تكوين أنفاق IKEv1 IPsec من موقع إلى موقع باستخدام ASDM أو CLI على ASA

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نفق تبادل مفتاح الإنترنت الإصدار 1 (IKEv1) IPsec من موقع إلى موقع بين جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5515-X Series الذي يشغل الإصدار 9.2.x من البرنامج و Cisco 5510 Series ASA الذي يشغل الإصدار 8.2.x من البرنامج.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- يجب إنشاء اتصال IP الشامل
- يجب السماح بهذه البروتوكولات:
  بروتوكول مخطط بيانات المستخدم (UDP) 500 و 4500 لمستوى التحكم في IPsecبروتوكول IP لحمولة أمان التضمين (ESP) 50 لمستوى بيانات IPsec

المكونات المستخدمة

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

- Cisco 5510 Series ASA أن يركض برمجية صيغة 8.2
- Cisco 5515-X ASA الذي يشغل البرنامج صيغة 9.2

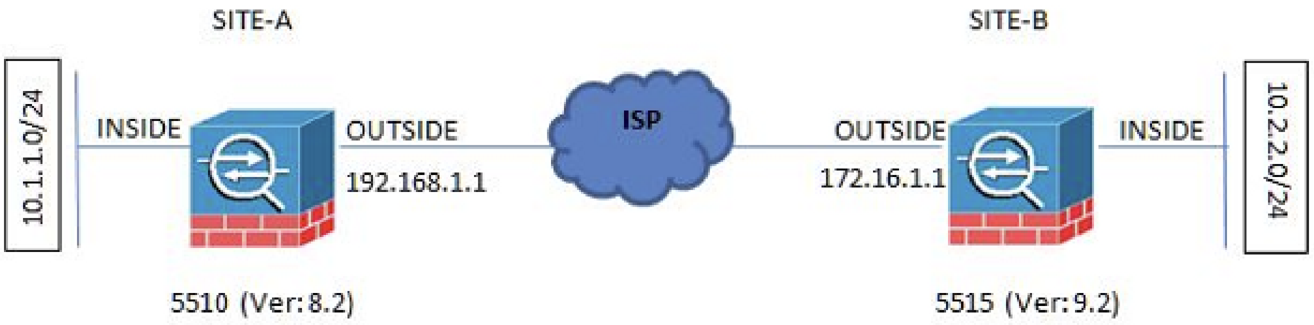
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يصف هذا القسم كيفية تكوين نفق VPN من موقع إلى موقع من خلال معالج Adaptive Security Device Manager (ASDM) VPN أو من خلال CLI (واجهة سطر الأوامر).

الرسم التخطيطي للشبكة

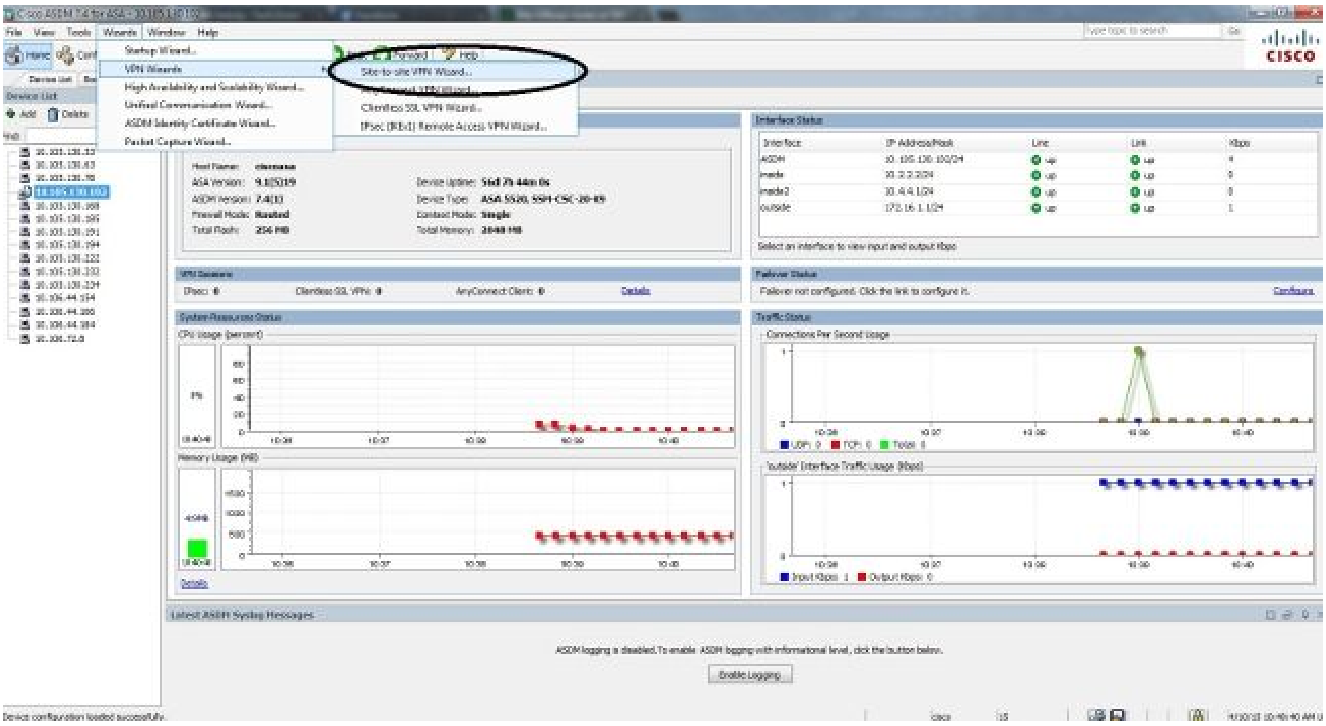
يتم إستخدام هذا المخطط للأمثلة في هذا المستند:



التكوين عبر معالج ASDM VPN

أكمل الخطوات التالية لإعداد نفق VPN من موقع إلى موقع من خلال معالج ASDM:

1. فتح ASDM والانتقال إلى Wizards > VPN Wizards > Site-to-site VPN Wizard.


File View Tools Wizards Window Help
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
ASDM Identity Certificate Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
Device List
Add Delete
Interface Status
VPN Sessions
Failover Status
System Resources Status
Traffic Status
Latest ASDM Syslog Messages
Enable Logging
CISCO

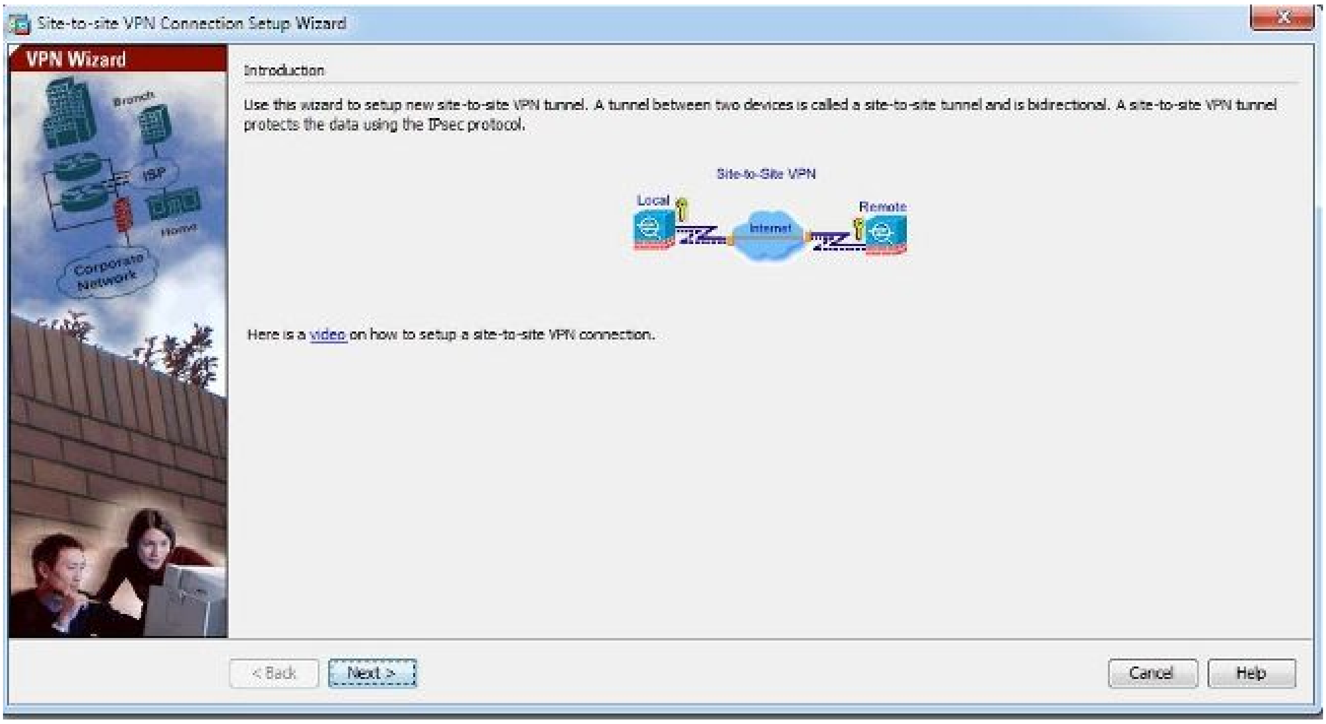
Host Name: ciscoasa
ASA Version: 9.1(5)19
ASDM Version: 7.4(1)
Firewall Mode: Routed
Total Flash: 256 MB
Device Uptime: 56d 7h 44m 0s
Device Type: ASA 5520, SSM-CSC-20-K9
Context Mode: Single
Total Memory: 2048 MB

Failover not configured. Click the link to configure it.

ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.

Device configuration loaded successfully.

2. انقر Next بمجرد الوصول إلى الصفحة الرئيسية للمعالج.



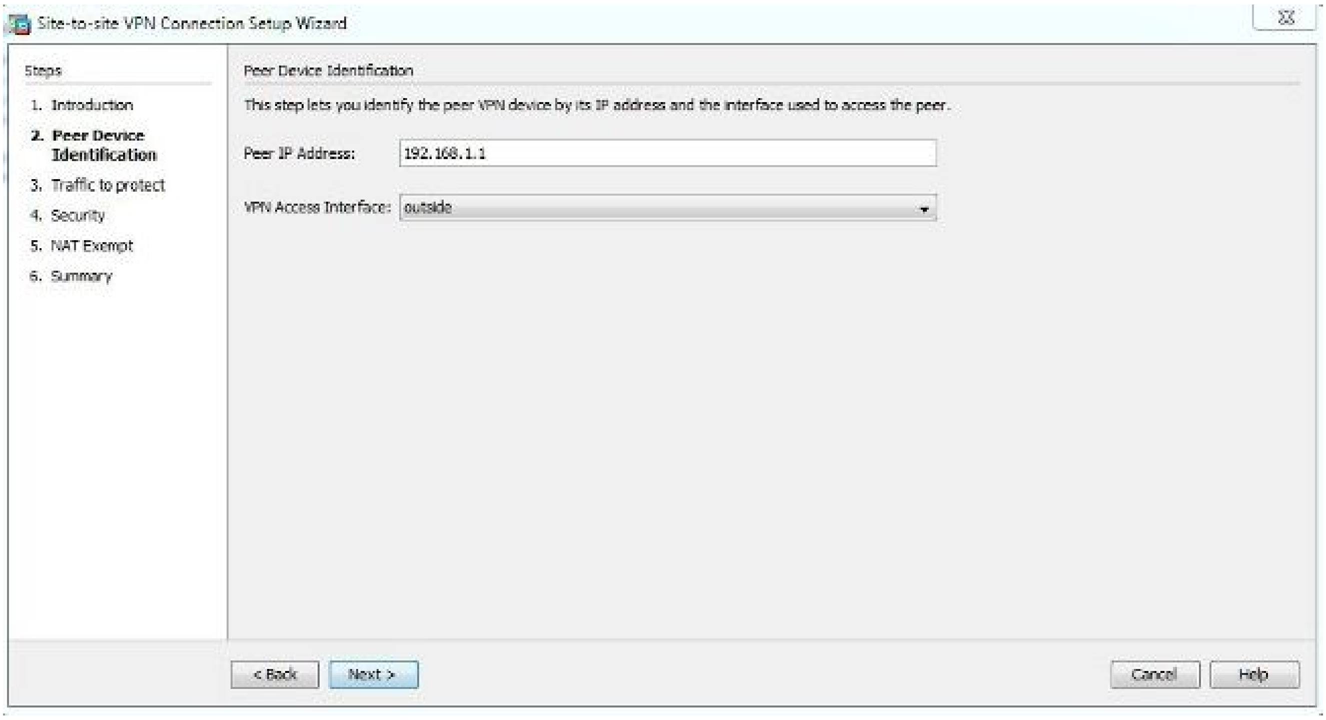
Introduction

Use this wizard to setup new site-to-site VPN tunnel. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.

Here is a video on how to setup a site-to-site VPN connection.

ملاحظة: توفر أحدث إصدارات ASDM إرتباط إلى فيديو يشرح هذا التكوين.

3. قم بتكوين عنوان IP للنظير. في هذا المثال، يتم تعيين عنوان IP للنظير على 192.168.1.1 في الموقع (ب). إذا قمت بتكوين عنوان IP للنظير على الموقع (أ)، فيجب تغييره إلى 172.16.1.1. كما تم تحديد الواجهة التي يمكن من خلالها الوصول إلى الطرف البعيد. انقر Next بمجرد الاكتمال.



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. **Peer Device Identification**
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary

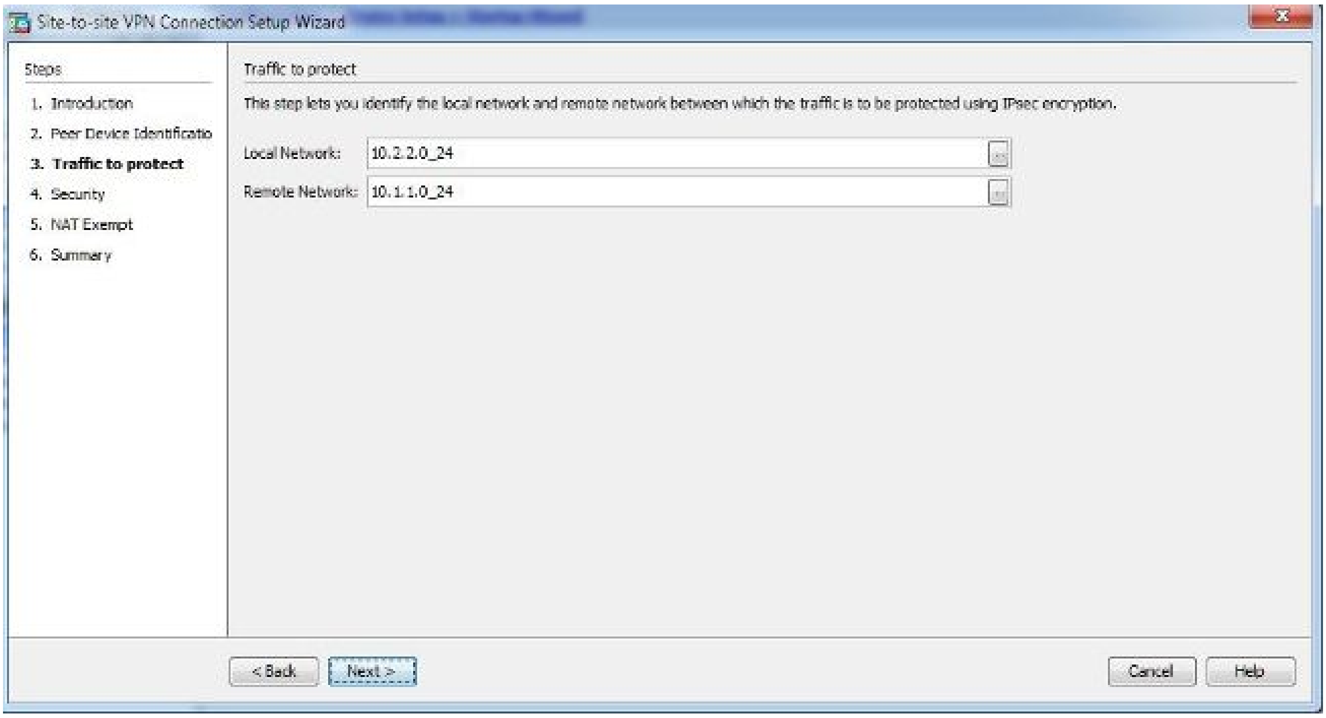
Peer Device Identification

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 192.168.1.1

VPN Access Interface: outside

4. قم بتكوين الشبكات المحلية والبعيدة (مصدر حركة المرور والوجهة). تعرض هذه الصورة تكوين الموقع (ب) (ينطبق العكس على الموقع (أ).



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identificatio
3. **Traffic to protect**
4. Security
5. NAT Exempt
6. Summary

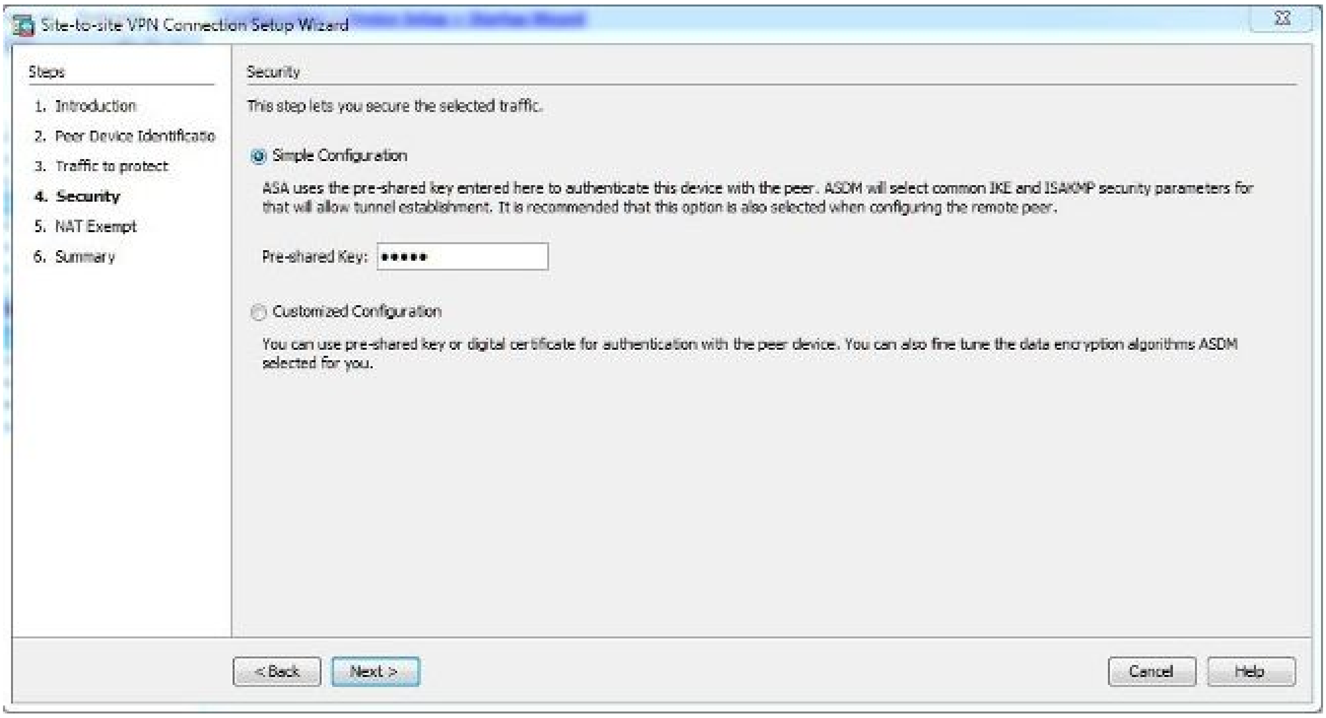
Traffic to protect

This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

Local Network: 10.2.2.0_24

Remote Network: 10.1.1.0_24

5. في صفحة الأمان، قم بتكوين المفتاح المشترك مسبقا (يجب أن يتطابق على كلا النهايتين). انقر Next بمجرد الاكتمال.



Security

This step lets you secure the selected traffic.

● Simple Configuration

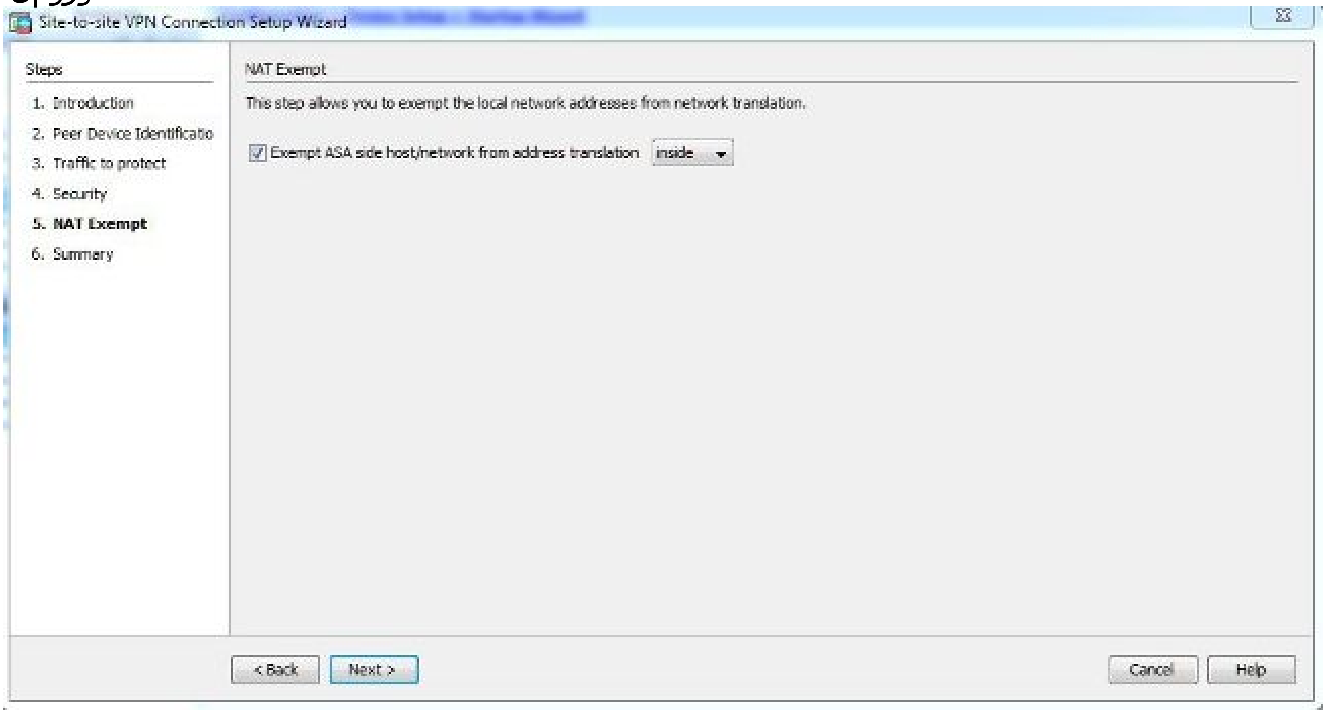
ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.

Pre-shared Key: •••••

○ Customized Configuration

You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

6. شكلت المصدر قارن لحركة مرور على ال ASA. يقوم ASDM تلقائيا بإنشاء قاعدة ترجمة عنوان الشبكة (NAT) استنادا إلى إصدار ASA ويدفعها مع بقية التكوين في الخطوة النهائية. **ملاحظة**: على سبيل المثال المستخدم في هذا المستند، يمثل "الداخل" مصدر حركة
المرور.

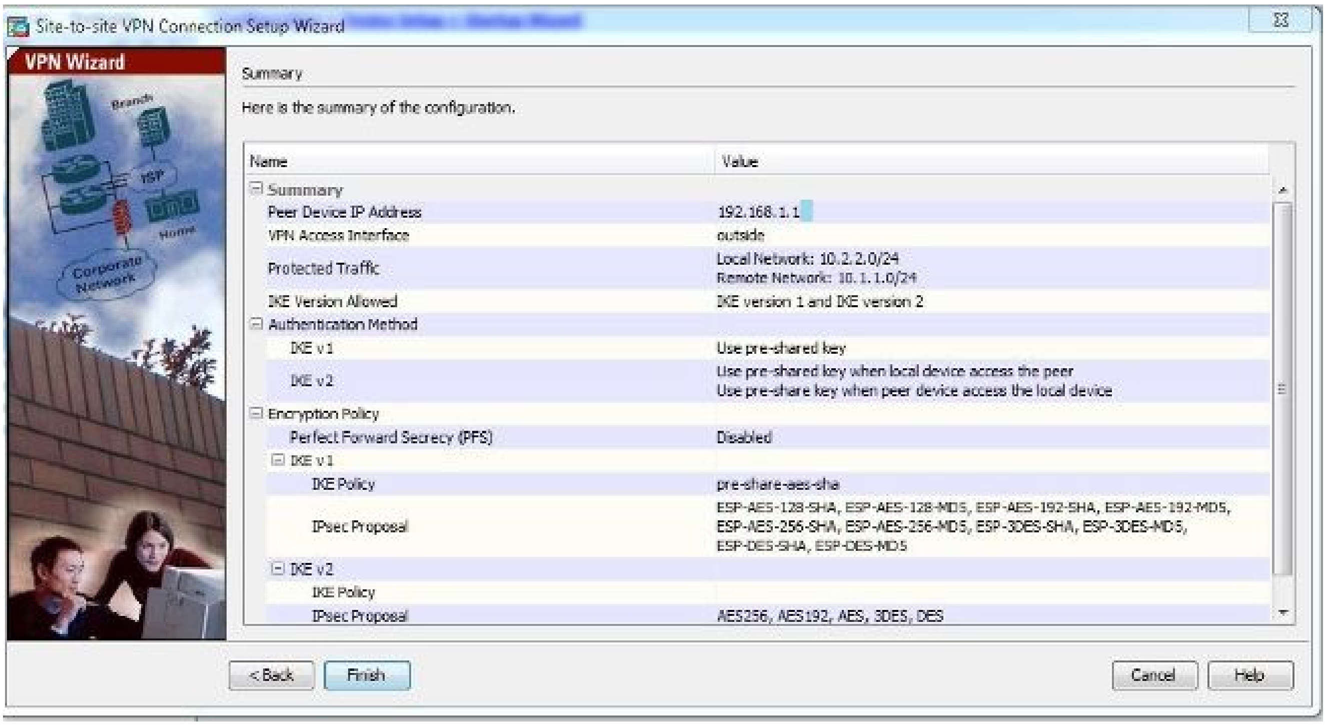


NAT Exempt

This step allows you to exempt the local network addresses from network translation.

☑ Exempt ASA side host/network from address translation: inside

7. يوفر المعالج الآن ملخصا للتكوين الذي يتم دفعه إلى ASA. راجعت ودققت التشكيل عملية إعداد، ثم طقطقت Finish.



Summary

Here is the summary of the configuration.

Name	Value
⊟ Summary	
Peer Device IP Address	192.168.1.1
VPN Access Interface	outside
Protected Traffic	Local Network: 10.2.2.0/24 Remote Network: 10.1.1.0/24
IKE Version Allowed	IKE version 1 and IKE version 2
⊟ Authentication Method	
IKE v1	Use pre-shared key
IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
⊟ Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
⊟ IKE v1	
IKE Policy	pre-share-aes-sha
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
⊟ IKE v2	
IKE Policy	
IPsec Proposal	AES256, AES192, AES, 3DES, DES

التكوين عبر واجهة سطر الأوامر (CLI)

يوضح هذا القسم كيفية تكوين نفق IKEv1 IPsec من موقع إلى موقع عبر CLI (واجهة سطر الأوامر).

تكوين الموقع B لإصدارات ASA 8.4 والإصدارات الأحدث

في إصدارات ASA 8.4 والإصدارات الأحدث، تم تقديم دعم لكل من IKEv1 و Internet Key Exchange الإصدار 2 (IKEv2).

> **تلميح**: للحصول على مزيد من المعلومات حول الفروق بين الإصدارين، ارجع إلى قسم لماذا الترحيل إلى IKEv2؟ من الترحيل السريع ل IKEv1 إلى تكوين نفق IKEv2 L2L على مستند ASA 8.4 Code من Cisco.

> **تلميح**: للحصول على مثال تكوين IKEv2 مع ASA، ألق نظرة على نفق IKEv2 من موقع إلى موقع بين ASA وأمثلة تكوين الموجه مستند Cisco.

المرحلة 1 (IKEv1)

أكمل الخطوات التالية لتكوين المرحلة 1:

1. دخلت هذا أمر داخل ال CLI in order to مكنت IKEv1 على القارن خارجي:

```
crypto ikev1 enable outside
```

2. إنشاء سياسة IKEv1 التي تحدد الخوارزميات/الطرق التي سيتم إستخدامها للتجزئة والمصادقة ومجموعة Diffie-Hellman ودورة الحياة والتشفير:

```
crypto ikev1 policy 1
```

```
!The 1 in the above command refers to the Policy suite priority
(1 highest, 65535 lowest)
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. قم بإنشاء مجموعة أنفاق تحت سمات IPsec وقم بتكوين عنوان IP للنظير ومفتاح النفق المشترك مسبقا:

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
! Note the IKEv1 keyword at the beginning of the pre-shared-key command.
```

المرحلة 2 (IPsec)

أكمل الخطوات التالية لتكوين المرحلة 2:

1. قم بإنشاء قائمة وصول تحدد حركة المرور التي سيتم تشفيرها وإنشاء قنوات لها. في هذا المثال، حركة مرور المصلحة هي حركة المرور من النفق الذي يتم الحصول عليه من الشبكة الفرعية 10.2.2.0 إلى 10.1.1.0. ويمكن أن يحتوي على إدخالات متعددة إذا كانت هناك شبكات فرعية متعددة مشتركة بين المواقع.

   في الإصدارات 8.4 والإصدارات الأحدث، يمكن إنشاء كائنات أو مجموعات كائنات تعمل كحاويات للشبكات أو الشبكات الفرعية أو عناوين IP للمضيف أو كائنات متعددة. قم بإنشاء كائنين يحتويان على شبكات فرعية محلية وبعيدة واستخدامهما لكل من قائمة التحكم في الوصول (ACL) للتشفير وجمل NAT.

```
object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

2. تكوين مجموعة التحويل (TS)، والتي يجب أن تتضمن الكلمة الأساسية IKEv1. يجب إنشاء TS مطابق على الطرف البعيد أيضا.

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

3. قم بتكوين خريطة التشفير، والتي تحتوي على المكونات التالية:
   عنوان IP النظيرقائمة الوصول المعرفة التي تحتوي على حركة مرور الفائدةتتي
   إسإعداد سرية إعادة التوجيه الكاملة الاختيارية (PFS)، التي تنشئ زوج جديد من مفاتيح Diffie-Hellman التي يتم إستخدامها لحماية البيانات (يجب تمكين كلا الجانبين من PFS قبل ظهور المرحلة 2)

4. تطبيق خريطة التشفير على الواجهة الخارجية:

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
```

```
     crypto map outside_map 20 set pfs
     crypto map outside_map interface outside
```

إستثناء NAT

تضمن أن لا يخضع الـ VPN حركة مرور إلى أي قاعدة nat آخر. هذه هي قاعدة NAT التي يتم إستخدامها:

```
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

> **ملاحظة**: عند إستخدام شبكات فرعية متعددة، يجب عليك إنشاء مجموعات كائنات باستخدام جميع الشبكات الفرعية للمصدر والوجهة واستعمالها في قاعدة NAT.

```
object-group  network 10.x.x.x_SOURCE
network-object 10.4.4.0 255.255.255.0
network-object 10.2.2.0 255.255.255.0

object network 10.x.x.x_DESTINATION
network-object 10.3.3.0 255.255.255.0
network-object 10.1.1.0 255.255.255.0

nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination
static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

إكمال نموذج التكوين

فيما يلي التكوين الكامل للموقع B:

```
crypto ikev1 enable outside

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

tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
!Note the IKEv1 keyword at the beginning of the pre-shared-key command.

object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24

crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

تكوين الموقع A لإصدارات ASA 8.2 والإصدارات الأقدم

يوضح هذا القسم كيفية تكوين الموقع A لإصدارات ASA 8.2 والإصدارات الأقدم.

المرحلة 1 (ISAKMP)

أكمل الخطوات التالية لتكوين المرحلة 1:

1. دخلت هذا أمر داخل ال CLI in order to مكنت إنترنت أمن اقتران ومفتاح إدارة بروتوكول (ISAKMP) على القارن خارجي:

   ```
   crypto isakmp enable outside
   ```

   ملاحظة: نظرا لأن الإصدارات المتعددة من IKE (IKEv1 و IKEv2) لم تعد مدعومة، يتم إستخدام ISAKMP للإشارة إلى المرحلة 1.
2. إنشاء سياسة ISAKMP التي تحدد الخوارزميات/الطرق التي سيتم إستخدامها لبناء المرحلة الأولى.

   ملاحظة: في مثال التكوين هذا، تكون الكلمة الأساسية IKEv1 من الإصدار 9.x يتم إستبداله ب ISAKMP.

   ```
   crypto isakmp policy 1
   authentication pre-share
   encryption aes
   hash sha
   group 2
   lifetime 86400
   ```
3. قم بإنشاء مجموعة أنفاق لعنوان IP للنظير (عنوان IP الخارجي لعام 5515) باستخدام المفتاح المشترك مسبقا:

   ```
    tunnel-group 172.16.1.1 type ipsec-l2l
   tunnel-group 172.16.1.1 ipsec-attributes
   pre-shared-key cisco
   ```

المرحلة 2 (IPsec)

أكمل الخطوات التالية لتكوين المرحلة 2:

1. وكما هو الحال مع التكوين في الإصدار 9.x، يجب عليك إنشاء قائمة وصول موسعة لتحديد حركة مرور البيانات ذات الاهتمام.

   ```
   access-list 100 extended permit ip 10.1.1.0 255.255.255.0
   10.2.2.0 255.255.255.0
   ```

2. قم بتحديد ts يحتوي على جميع خوارزميات التشفير والتجزئة المتوفرة (تتضمن المشكلات المعروضة علامة إستفهام). تأكد من أنه مطابق للجانب الآخر الذي تم تكوينه.

   ```
   crypto ipsec transform-set myset esp-aes esp-sha-hmac
   ```
3. تكوين خريطة تشفير، تحتوي على المكونات التالية:
   عنوان IP النظيرقائمة الوصول المعرفة التي تحتوي على حركة مرور الفائدةتي إسإعداد PFS إختياري، الذي ينشئ زوج جديد من مفاتيح Diffie-Hellman التي يتم إستخدامها لحماية البيانات (يجب أن يكون كلا الجانبين متوافقين مع PFS بحيث تظهر المرحلة 2)
4. تطبيق خريطة التشفير على الواجهة الخارجية:

   ```
   crypto map outside_map 20 set peer 172.16.1.1
   crypto map outside_map 20 match address 100
   crypto map outside_map 20 set transform-set myset
   crypto map outside_map 20 set pfs
   crypto map outside_map interface outside
   ```

إستثناء NAT

قم بإنشاء قائمة وصول تحدد حركة المرور التي سيتم إعفاؤها من تحققات nat. في هذا إصدار، يظهر مماثل إلى قائمة الوصول أن أنت عينت لحركة مرور الفائدة:

```
access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0  255.255.255.0
```

عند إستخدام شبكات فرعية متعددة، أضف خطا آخر إلى قائمة الوصول نفسها:

```
access-list nonat line 1 extended permit ip 10.3.3.0 255.255.255.0
10.4.4.0 255.255.255.0
```

يتم إستخدام قائمة الوصول مع NAT، كما هو موضح هنا:

```
nat (inside) 0 access-list nonat
```

> **ملاحظة**: يشير 'inside' هنا إلى اسم الواجهة الداخلية التي يستلم ASA عليها حركة مرور البيانات التي تطابق قائمة الوصول.

إكمال نموذج التكوين

فيما يلي التكوين الكامل للموقع A:

```
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption aes
```

```
hash sha group 2
lifetime 86400

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco

access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 set peer
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0

nat (inside) 0 access-list nonat
```

نهج المجموعة

يتم إستخدام نهج المجموعة لتحديد إعدادات معينة تنطبق على النفق. يتم إستخدام هذه السياسات بالاقتران مع مجموعة النفق.

يمكن تعريف نهج المجموعة على أنه إما داخلي، مما يعني أن السمات يتم سحبها من السمات المحددة على ASA، أو يمكن تعريفها على أنها خارجية، حيث يتم الاستعلام عن السمات من خادم خارجي. هذا هو الأمر الذي يتم إستخدامه لتحديد سياسة المجموعة:

```
group-policy SITE_A internal
```

> **ملاحظة**: يمكنك تعريف سمات متعددة في نهج المجموعة. للحصول على قائمة بكافة السمات الممكنة، ارجع إلى قسم تكوين سياسات المجموعة" في إجراءات تكوين VPN المحددة ل ASDM ل سلسلة Cisco ASA 5500، الإصدار 5.2.

سمات إختيارية لنهج المجموعة

يعرض الأمر vpn-tunnel-protocol تحدد السمة نوع النفق الذي يجب تطبيق هذه الإعدادات عليه. في هذا المثال، يتم إستخدام IPsec:

```
vpn-tunnel-protocol ?
group-policy mode commands/options:
IPSec IP Security Protocol l2tp-ipsec L2TP using IPSec for security
svc SSL VPN Client
webvpn WebVPN

vpn-tunnel-protocol ipsec - Versions 8.2 and prior
vpn-tunnel-protocol ikev1 - Version 8.4 and later
```

لديك الخيار لتكوين النفق حتى يظل في وضع الخمول (بدون حركة مرور) ولا يتوقف.

لتكوين هذا الخيار، فإن vpn-idle-timeout يجب أن تستخدم قيمة السمة الدقائق، أو يمكنك تعيين القيمة إلى none، ما يعني أن النفق لا يسقط أبدا.

فيما يلي مثال:

```
group-policy SITE_A attributes
vpn-idle-timeout ?
group-policy mode commands/options:
<1-35791394> Number of minutes
none IPsec VPN: Disable timeout and allow an unlimited idle period;
```

يعرض الأمر default-group-policy يقوق موو الأمر الموجود تحت السمات العامة لمجموعة النفق بتعريف نهج المجموعة الذي يتم إستخدامه لدفع بعض إعدادات النهج للنفق الذي تم إنشاؤه. يتم أخذ الإعدادات الافتراضية للخيارات التي لم تقم بتعريفها في نهج المجموعة من نهج مجموعة افتراضي عمومي:

```
tunnel-group 172.16.1.1 general-attributes
default-group-policy SITE_A
```

التحقق من الصحة

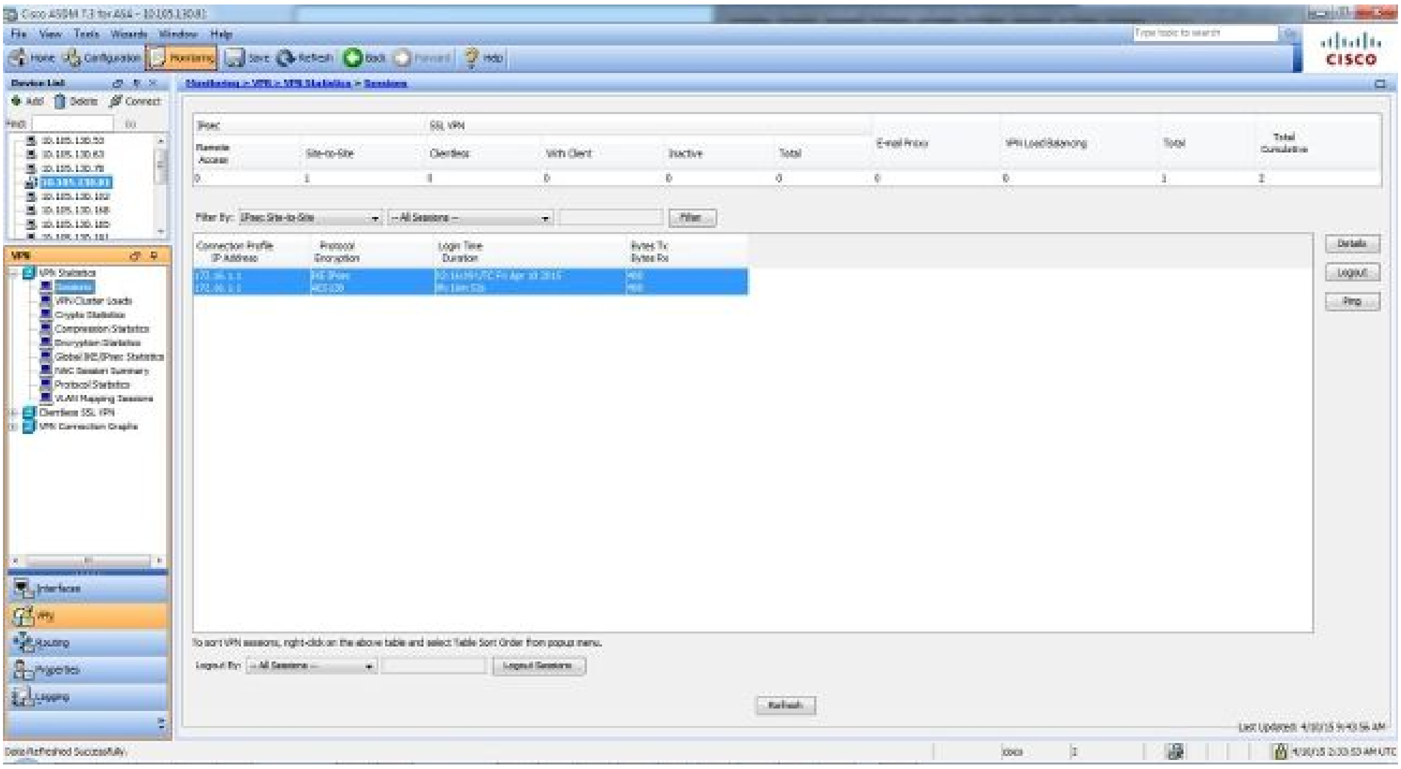
أستخدم المعلومات المقدمة في هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

ASDM

لعرض حالة النفق من ASDM، انتقل إلى Monitoring > VPN. يتم توفير هذه المعلومات:

- عنوان IP النظير
- البروتوكول الذي يتم إستخدامه لإنشاء النفق
- خوارزمية التشفير التي يتم إستخدامها
- الوقت الذي خرج فيه النفق و الوقت
- عدد الحزم التي يتم إستلامها ونقلها

تلميح: انقر Refresh لعرض أحدث القيم، حيث أن البيانات لا يتم تحديثها في الوقت الحقيقي.



Monitoring > VPN > VPN Statistics > Sessions

IPsec		SSL VPN							
Remote Access	Site-to-Site	Clientless	With Client	Inactive	Total	E-mail Proxy	VPN Load Balancing	Total	Total Cumulative
0	1	0	0	0	0	0	0	1	2

Filter By: IPsec Site-to-Site -- All Sessions --

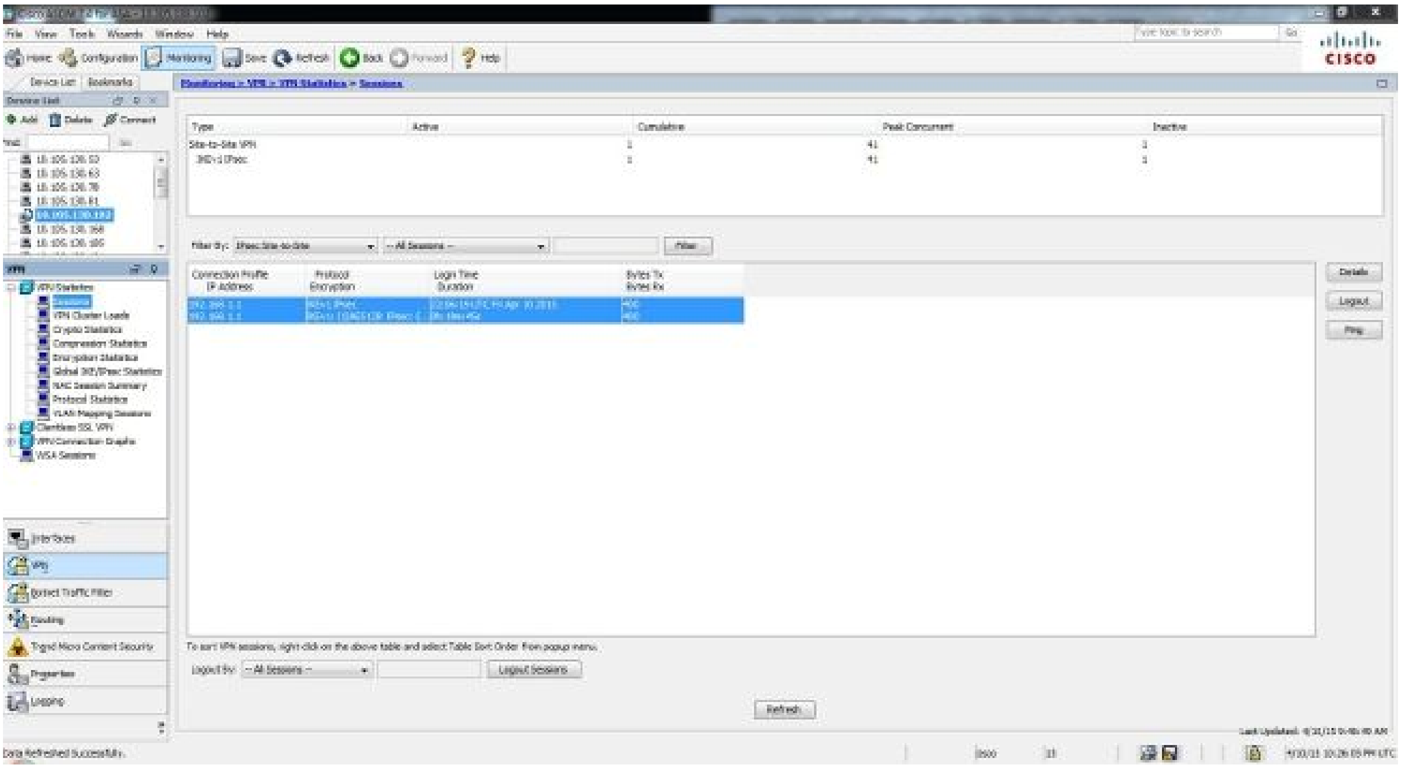
Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
172.16.1.1 172.16.1.1	IKE IPsec AES128	02:16:09 UTC Fri Apr 10 2015 0h:16m:53s	400 400

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Last Updated: 4/10/15 9:43:56 AM

Data Refreshed Successfully.



Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN		1	41	1
IKEv1 IPsec		1	41	1

Filter By: IPsec Site-to-Site -- All Sessions --

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
192.168.1.1 192.168.1.1	IKEv1 IPsec IKEv1: (1)AES128 IPsec: (	22:06:15 UTC Fri Apr 10 2015 0h:18m:45s	400 400

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Data Refreshed Successfully.

CLI

يوضح هذا القسم كيفية التحقق من التكوين الخاص بك عبر واجهة سطر الأوامر.

المرحلة الأولى

أدخل هذا الأمر في واجهة سطر الأوامر (CLI) للتحقق من تكوين المرحلة 1 على جانب الموقع (5515):

```
show crypto ikev1 sa

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: 192.168.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

أدخل اذه الأمر في واجهة سطر الأوامر (CLI) للتحقق من تكوين المرحلة 1 على الجانب (5510) للموقع A:

```
show crypto isakmp sa

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: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

المرحلة الثانية

يعرض الأمر show crypto ipsec sa يعرض الأمر رسائل IPsec SAs التي تم إنشاؤها بين الأقران. يتم إنشاء النفق المشفر بين عناوين IP 192.168.1.1 و 172.16.1.1 لحركة المرور التي تتدفق بين الشبكات 10.1.1.0 و 10.2.2.0. يمكنك رؤية وحدتي ESP اللتين تم إنشاؤهما لحركة المرور الواردة والصادرة. لا يتم إستخدام رأس المصادقة (AH) نظرا لعدم وجود رسائل AH SA.

أدخل اذه الأمر في واجهة سطر الأوامر (CLI) للتحقق من تكوين المرحلة 2 على جانب الموقع (B) (5515):

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
 local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
 current_peer: 192.168.1.1
PERMIT, flags={origin_is_acl,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
   local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
      transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
      sa timing: remaining key lifetime (k/sec): (4608000/52)
```

```
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
      transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
      sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

أدخل هذا الأمر في واجهة سطر الأوامر (CLI) للتحقق من تكوين المرحلة 2 على الجانب (5510) للموقع A:

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 192.168.1.1
  local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  current_peer: 172.16.1.1
PERMIT, flags={origin_is_acl,}
   #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
    local crypto endpt.: 192.168.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
       transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
       transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

استكشاف الأخطاء وإصلاحها

استعملت المعلومة أن يكون زود تد في هذا قسم in order to تحريت تشكيل إصدار.

ASA الإصدارات 8.4 والإصدارات الأحدث

أدخل أوامر تصحيح الأخطاء هذه لتحديد موقع فشل النفق:

- debug crypto ikev1 127 (المرحلة 1)
- debug crypto ipsec 127 (المرحلة 2)

هنا مثال كامل من يضبط إنتاج:

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver RFC payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE
fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA_KE payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco
VPN3000/Cisco ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
!
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group
192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating
keys for Initiator...
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing
ID payload
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing
hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing
hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive
payload: proposal=32767/32767 sec.
!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms
ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing dpd vid payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT
Detection Status: Remote end is NOT behind a NAT device This end is NOT behind
a NAT device
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing
ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR ID received 192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing
hash for ISAKMP
```

```
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received
DPD VID
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group
192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley
begin quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE
Initiator starting QM: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1
rekey timer: 73440 seconds.
IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
IKE got SPI from key engine: SPI = 0x03fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
oakley constucting quick mode
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing blank hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing IPSec SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing IPSec nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing proxy ID
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Transmitting Proxy Id:
Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
IKE Initiator sending Initial Contact
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1,
IP = 192.168.1.1, constructing qm hash payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1,
IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 200
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
total length : 172
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
loading all IPSEC SAs
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
NP encrypt rule look up for crypto map outside_map 20 matching ACL
100: returned cs_id=6ef246d0; encrypt_rule=752972d0;
tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x6f0e03f0,
SCB: 0x75B6DD00,
Direction: outbound
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x1BA0C55C
IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: New outbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
```

```
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
```

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0; encrypt_rule=752972d0; tunnelFlow_rule=75ac8020

```
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation
complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7,
Outbound SPI = 0x1ba0c55c
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley
constructing final quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator
sending 3rd QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + NONE (0) total length : 76
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY_ADD
msg for SA: SPI = 0x1ba0c55c
IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x03FC9DB7
IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000006
SA : 0x75298588
SPI : 0x03FC9DB7
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000F614
SCB : 0x0B4707C7
Channel: 0x6ef0a5c0
IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x00011f6c
IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00011F6C
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7
Rule ID: 0x74e1b4a0
IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de830
IPSEC: New inbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de8d8
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher:
received KEY_UPDATE, spi 0x3fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting
P2 rekey timer: 24480 seconds.
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2
COMPLETED (msgid=4c073b21)
```

ASA الإصدارات 8.3 والإصدارات الأقدم

أدخل أوامر تصحيح الأخطاء هذه لتحديد موقع فشل النفق:

- debug crypto isakmp 127 (المرحلة 1)
- debug crypto ipsec 127 (المرحلة 2)

هنا مثال كامل من يضبط إنتاج:

```
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Oakley proposal is acceptable
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 02 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 03 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal RFC VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Fragmentation VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: True
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing IKE SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE SA Proposal # 1, Transform # 1
acceptable Matches global IKE entry # 1
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ISAKMP SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Traversal VID ver
02 payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 132
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ke payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ISA_KE payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Cisco Unity client VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received xauth V6 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing VPN3000/ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ke payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Cisco Unity VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing xauth V6 VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send IOS VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing ASA spoofing IOS Vendor
ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send Altiga/Cisco VPN3000/Cisco
```

```
ASA GW VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys
for Responder...
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)
total length : 96
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR
ID received 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing
hash for ISAKMP
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection
Status: Remote end is NOT behind a NAT device This end is NOT behind
a NAT device
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing ID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
Computing hash for ISAKMP
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing dpd vid payload
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)
total length : 96
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1
rekey timer: 82080 seconds.
Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id =
4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +
ID (5) + NOTIFY (11) + NONE (0) total length : 200
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP
```

```
Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0,
Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP
Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
notify payload
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa
not found by addr
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map
check, checking map = outside_map, seq = 20...
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map
check, map outside_map, seq = 20 is a successful match
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer
configured for crypto map: outside_map
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
IPSec SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPSec SA
Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0xAB5C63A8,
SCB: 0xABD54E98,
Direction: inbound
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI
from key engine: SPI = 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley
constucting quick mode
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
blank hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
proxy ID
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting
Proxy Id:
Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
qm hash payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder
sending 2nd QM pkt: msg id = 4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +
ID (5) + NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all
IPSEC SAs
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating
Quick Mode Key!
```

```
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt
rule look up for crypto map outside_map 20 matching ACL 100: returned
cs_id=ab9302f0; rule=ab9309b0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating
Quick Mode Key!
IPSEC: New embryonic SA created @ 0xAB570B58,
SCB: 0xABD55378,
Direction: outbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x03FC9DB7
IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: New outbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
```

```
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0;
rule=ab9309b0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,
Outbound SPI = 0x03fc9db7
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a
KEY_ADD msg for SA: SPI = 0x03fc9db7
IPSEC: Completed host IBSA update, SPI 0x1BA0C55C
IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C
Flags: 0x00000006
SA : 0xAB5C63A8
SPI : 0x1BA0C55C
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000F99C
SCB : 0x0150B419
Channel: 0xA7A98400
IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0001169C
IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7
Flags: 0x00000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x0001169C
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x1BA0C55C
Rule ID: 0xAB8D98A8
IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
```

```
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C
Rule ID: 0xABD55CB0
IPSEC: New inbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C
Rule ID: 0xABD55D48
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received
KEY_UPDATE, spi 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey
timer: 27360 seconds.
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED
(msgid=4c073b21)
```

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).