فهم أوامر التصحيح واستخدامها الاستكشاف أخطاء IPsec وإصلاحها

المحتويات

المقدمة

يصف هذا المستند أوامر تصحيح الأخطاء الشائعة المستخدمة لاستكشاف أخطاء IPsec وإصلاحها على كل من برنامج Cisco IOS® وPIX/ASA.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أنك قمت بتكوين IPsec. راجع [مفاوضة IPSec/بروتوكولات IKE](#) للحصول على مزيد من التفاصيل.

المكونات المستخدمة

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

- برنامج Cisco IOS®
  - مجموعة ميزات IPsec.
  - 56i—يشير إلى أحادي Data Encryption Standard (DES) (على برنامج Cisco IOS® الإصدار 11.2 والإصدارات الأحدث).
  - k2—يشير إلى ميزة DES الثلاثية (على برنامج Cisco IOS® الإصدار 12.0 والإصدارات الأحدث). يتوفر DES الثلاثي على السلسلة Cisco 2600 والإصدارات الأحدث.
- PIX-V5.0 والإصدارات الأحدث، والتي تتطلب مفتاح ترخيص DES فردي أو ثلاثي من أجل التنشيط.

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

ارجع إلى Remote Access IPsec و L2L لـ اهصالحإو VPN عاطخأ فاشكتسأ لولح للحصول على معلومات حول الحلول الأكثر شيوعا لمشاكل VPN لـ IPsec.

وهو يحتوي على قائمة تحقق من الإجراءات الشائعة التي يمكنك تجربتها قبل البدء في أستكشاف أخطاء الاتصال وإصلاحها واستدعاء دعم Cisco التقني.

تصحيح أخطاء برنامج Cisco IOS®

تصف المواضيع الواردة في هذا القسم أوامر تصحيح أخطاء برنامج Cisco IOS®. راجع مفاوضة IKE تالوكوتورب/IPSec للحصول على مزيد من التفاصيل.

show crypto isakmp sa

يوضح هذا الأمرInternet Security Association Management Protocol (ISAKMP) Security Associations (SAs)مبنية بين الأقران.

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

show crypto ipsec sa

يعرض هذا الأمر رسائل IPsec SAs التي تم إنشاؤها بين الأقران. يتم إنشاء النفق المشفر بين 10.1.1.0 و 10.1.0.0 تلك المرور التي تنتقل بين الشبكات 10.1.0.2 و 10.1.0.1.

يمكن رؤية اثنين Encapsulating Security Payload (ESP) تم إنشاء SAs داخلي وخارجي. ال تم إستخدام رأس المصادقة (AH) أظهر عدم وجود أي من رسائل AH SA.

يوضح هذا الإخراج مثال على**show crypto ipsec sa**erasecat4000_flash:.

<#root>

```
  interface: FastEthernet0
    Crypto map tag: test, local addr.
```

10.1.0.1

```
   local  ident (addr/mask/prot/port): (
```

10.1.0.0/255.255.255.0/0/0

```
)
   remote ident (addr/mask/prot/port): (
```

10.1.1.0/255.255.255.0/0/0

)
   current_peer:

10.1.0.2

     PERMIT, flags={origin_is_acl,}

#pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
**   #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382**

    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2

     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound

esp

 sas:
      spi: 0x136A010F(325714191)
        transform:

esp-3des esp-md5-hmac

 ,
        in use settings ={

Tunnel

, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        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-3des esp-md5-hmac

 ,
    in use settings ={

Tunnel

, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test

```
    sa timing:

 remaining key lifetime (k/sec): (4608000/52)

    IV size: 8 bytes
    replay detection support: Y
outbound

ah

 sas:
outbound pcp sas:
```

show crypto engine connection active

يعرض هذا الأمر لكل مرحلة 2 SA بنيت ومقدار حركة المرور المرسلة.

لأن المرحلة الثانية Security Associations (SAs)أحادي الإتجاه، لكل SA يدي حركة مرور في إتجاه واحد فقط (التشفير صادر، فك التشفير وارد).

debug crypto isakmp

يوضح هذا الإخراج مثال على **debug crypto isakmp** erasecat4000_flash:.

<#root>

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
    encryption DES-CBC
          hash SHA
    default group 2
    auth pre-share
    life type in seconds
    life duration (basic) of 240

atts are acceptable

. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debug crypto ipSec

يعرض هذا الأمر مصدر نقاط نهاية نفق IPsec ووجهة هذه النقاط.Src_proxy و dest_proxyهي الشبكات الفرعية للعميل.

إثنينsa createdظهر الرسائل مع رسالة في كل إتجاه. (ظهر أربع رسائل إذا تم أداء ESP و

AH.)

يوضح هذه الإخراج مثال على **debug crypto ipsec**erasecat4000_flash:.

<#root>

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
    encaps is 1
    SA life type in seconds
    SA life duration (basic) of 3600
    SA life type in kilobytes
    SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
```

atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
** not acceptable".**

```
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest=
```

10.1.0.2

, src=

10.1.0.1

,

dest_proxy= 10.1.1.0/255.255.255.0/0/0,
**   src_proxy= 10.1.0.0/255.255.255.0/0/0,**

      protocol=

ESP

```
, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=
```

10.1.0.2

, dest=

10.1.0.1,

```
 src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,

      protocol=
```

ESP

```
, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa):
```

sa created

```
,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa):
```

sa created

```
,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

نموذج رسائل الخطأ

تم إنشاء رسائل الخطأ هذه العينة من أوامر تصحيح الأخطاء المدرجة هنا:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

فشل التحقق من إعادة التشغيل

يوضح هذا الإخراج مثال على"Replay Check Failed"الخطأ :

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

هذا الخطأ هو نتيجة لإعادة الترتيب في وسط الإرسال (خاصة إذا كانت المسارات المتوازية موجودة)، أو المسارات غير المتكافئة للحزمة التي تمت معالجتها داخل Cisco IOS® للحزم الكبيرة مقابل الحزم الصغيرة بالإضافة إلى الحمل الزائد.

قم بتغيير مجموعة التحويل لتعكس هذا. يعرض الأمر reply check نرى فقط عندما transform-set esp-md5-hmac ممكن. أعجزت in order to ضغط هذا خطأ رسالة، esp-md5-hmac و بتعمل تشفير بس.

أحلت cisco بق idcscDP19680 (يسجل زبون فقط).

خطأ QM FSM

ال يظهر نفق IPsec L2L VPN على جدار حماية PIX أو ASA، وتظهر رسالة خطأ QM FSM.

أحد الأسباب المحتملة هو الهويات الوكيلة، مثل حركة المرور غير العادية،Access Control List (ACL),أو قائمة التحكم في الوصول (ACL) المشفرة، ال تتطابق على كل الطرفين.

تحقق من التكوين على كل الجهازين، وتأكد من مطابقة قوائم التحكم في الوصول (ACL) للتشفير.

سبب آخر ممكن وهو عدم تطابق معلمات مجموعة التحويل. تحقق من أنه في كل طرفي الشبكة الخاصة الظاهرية (VPN)، تستخدم بوابات الشبكة الخاصة الظاهرية (VPN) نفس مجموعة التحويل باستخدام نفس المعلمات تمامًا.

عنوان محلي غير صالح

يوضح هذا الإخراج مثال لرسالة الخطأ:

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

تنسب رسالة الخطأ هذه إلى إحدى هاتين المشكلتين المشتركتين:

- يعرض الأمرcrypto map map-name local-address interface-idيتسبب الأمر في أن يستخدم الموجه عنوانا غير صحيح كهوية لأنه يفرض على الموجه إستخدام عنوان محدد.
- Crypto map تم تطبيقه على الواجهة الخطأ أو لم يتم تطبيقه على الإطلاق. تحقق من التكوين لضمان تطبيق خريطة التشفير على الواجهة الصحيحة.

فشلت رسالة IKE من X.X.X.X في التحقق من سلامة النظام أو تم تكوينها بشكل غير صحيح

يظهر خطأ تصحيح الأخطاء هذا إذا لم تتطابق المفاتيح المشتركة مسبقا على الأقران. لحل هذه المشكلة، تحقق من المفاتيح المشتركة مسبقا على كل الجانبين.

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

فشلت عملية الوضع الرئيسي مع النظير

هذا مثال علىMain Modeرسالة الخطأ. يشير فشل الوضع الرئيسي إلى أن سياسة المرحلة الأولى غير متطابقة على كلا الجانبين.

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

يظهر الأمر show crypto isakmp sa وجود ISAKMP SA فيMM_NO_STATE. هذا يعني أيضا أن الوضع الرئيسي فشل.

```
dst          src        state              conn-id         slot
10.1.1.2  10.1.1.1   MM_NO_STATE        1           0
```

تحقق من أن نهج المرحلة 1 موجود على كلا الأقران، وتأكد من مطابقة جميع السمات.

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

هويات الوكيل غير مدعومة

تظهر هذه الرسالة في تصحيح الأخطاء إذا لم تتطابق قائمة الوصول لحركة مرور IPsec.

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

تحتاج قوائم الوصول لكل نظير إلى النسخ المتطابق (يلزم عكس جميع الإدخالات). يوضح هذا المثال هذه النقطة.

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

مقترح التحويل غير مدعوم

تظهر هذه الرسالة إذا لم تتطابق المرحلة 2 (IPsec) على كل الجانبين. يحدث هذا بشكل شائع في حالة وجود عدم تطابق أو عدم توافق في مجموعة التحويل.

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

تحقق من تطابق مجموعة التحويل على كل الجانبين:

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

لا توجد أية شهادة أو مفاتيح مع النظير البعيد

تشير هذه الرسالة إلى أن عنوان النظير الذي تم تكوينه على الموجه غير صحيح أو تم تغييره. تحقق من صحة عنوان النظير ومن إمكانية الوصول إلى العنوان.

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

لم يتم العثور على عنوان النظير x.x.x.x

تظهر رسالة الخطأ هذه بشكل طبيعي مع VPN 3000 Concentrator رسالة الخطأ "Message: No proposal chosen(14)". وذلك لأن الاتصالات من مضيف إلى مضيف.

يتضمن تكوين الموجه مقترحات IPsec بالترتيب الذي يتطابق فيه الاقتراح المختار للموجه مع قائمة الوصول، وليس النظير.

تحتوي قائمة الوصول على شبكة أكبر تتضمن المضيف الذي يتقاطع مع حركة المرور. لتصحيح هذا الأمر، ضع اقتراح الموجه الاتصال المركز إلى الموجه هذا أولا في السطر.

وهذا يسمح لها بمطابقة المضيف المحدد أو الـ.

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

حزمة IPsec تحتوي على SPI غير صالح

هذا الإخراج مثال على رسالة الخطأ:

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

تحدد حزمة IPsec المستلمة Security Parameters Index (SPI) غير موجودة في Security Associations Database (SADB). قد يكون هذا حالة مؤقتة بسبب:

- فرق طفيفة في قدم Security Sssociations (SAs) بين نظائر IPsec.
- تم مسح أسماء الخدمات المحلية.
- حزم غير صحيحة مرسلة بواسطة نظير IPsec.

من المحتمل أن يكون هذا هو.

الإجراء الموصى به:

قد لا يقر النظير بأنه قد تم مسح SAs المحلية. إذا تم إنشاء اتصال جديد من الموجه المحلي، فيمكن بعد ذلك لكل الأقران إعادة الإنشاء بنجاح. وإلا، إذا تحدث المشكلة لأكثر من فترة وجيزة، فإما أن تحاول إنشاء اتصال جديد أو اتصل بمسؤول ذلك النظير.

PSEC(initialize_sas): معرفات وكيل غير صالحة

الخطأ "21:57:57: IPSEC(initialize_sas): invalid proxy IDs" تشير إلى أن هوية الوكيل المستلمة لا تطابق هوية الوكيل التي تم تكوينها وفقا لقائمة الوصول.

للتأكد من مطابقتها مع، تحقق من الإخراج من الأمر debug.

في إخراج الأمر debug من طلب الاقتران، تطابق قائمة الوصول 103 مع السماح ip 10.1.1.0.0.0.255 10.1.0.0.0.0.255.

تكون قائمة الوصول خاصة بالشبكة من طرف واحد ومضيفة محددة من جهة أخرى.

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

5 المرحلة ليس صفرا على الحمولة مرجوز

هذا يعني أن مفاتيح ISAKMP غير متطابقة. قم بإعادة المفاتيح/إعادة الضبط لضمان الدقة.

ال تتطابق خوارزمية التجزئة المقدمة مع النهج

إذا لم تتطابق سياسات ISAKMP التي تم تكوينها مع السياسة المقترحة بواسطة النظير البعيد، فسيحاول الموجه النهج الافتراضي ل 65535.

إذا لم يتطابق ذلك مع أي من هذه، فإن فشل تفاوض ISAKMP.

يتلقى المستخدم إما "Hash algorithm offered does not match policy!" أو "Encryption algorithm offered does not match policy!" رسالة خطأ على الموجهات.

<#root>

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1):
```

Checking ISAKMP transform 1 against priority 1 policy

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):
```

Hash algorithm offered does not match policy!

```
ISAKMP (0:1):
```

atts are not acceptable. Next payload is 0

```
=RouterB=
ISAKMP (0:1):
```

Checking ISAKMP transform 1 against priority 65535 policy

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
```

```
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):

Encryption algorithm offered does not match policy!

ISAKMP (0:1):

atts are not acceptable. Next payload is 0

ISAKMP (0:1):

 no offers accepted!

ISAKMP (0:1):

phase 1 SA not acceptable!
```

فشل التحقق من HMAC

يتم الإبلاغ عن رسالة الخطأ هذه عندما يكون هناك فشل في التحقق من Hash Message Authentication Code على حزمة IPsec. يحدث هذا عادة عندما تكون الحزمة تالفة بأي طريقة.

<#root>

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39:

%MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure

Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39:

%MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                  PktEngReturn_MACMiscompare
```

إذا صادفت رسالة الخطأ هذه من حين إلى آخر، فيمكنك تجاهلها. مهما، إن يصبح هذا كثير، بعد ذلك أنت تحتاج أن يتحرى مصدر الفساد من الرابط. يمكن أن يكون هذا بسبب خلل في مسرع التشفير.

النظير البعيد لا يستجيب

تمت مصادفة رسالة الخطأ هذه عندما يكون هناك عدم تطابق في مجموعة تحويل. تأكد من تكوين مجموعات التحويل المطابقة على كل النظيرين.

جميع مقترحات IPSec SA غير مقبولة

تحدث رسالة الخطأ هذه عندما تكون معلمات Phase 2 IPSec غير متطابقة بين الأقران المحلية والأقران البعيدة.

in order to حللت هذه إصدار، عينت لا نفس معلم في التحويل مجموعة so that هم يطابقون وينجح VPN يثبت.

خطأ في تشفير/فك تشفير الحزمة

هذا الإخراج مثال على رسالة الخطأ:

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

قد يرجع سبب رسالة الخطأ هذه إلى أحد الأسباب التالية:

- التجزئة — يتم تحويل حزم التشفير المجزأة، والذي يفرض إرسال الحزم سريعة التحويل إلى بطاقة VPN قبل الحزم التي يتم تحويلها للعملية.

إذا تمت معالجة عدد كاف من الحزم المحولة بسرعة قبل الحزم المحولة للعملية، فسيتعرض رقم تسلسل ESP أو AH للحزمة المحولة للعملية للفشل، وعندما تصل الحزمة إلى بطاقة VPN، فسيكون الرقم التسلسلي الخاص بها خارج نافذة إعادة التشغيل.

وهذا يتسبب في أخطاء رقم تسلسل AH أو ESP (4615 و4612، على التوالي)، وفقا لأي عملية كبسلة تستخدمها.

- إدخالات ذاكرة التخزين المؤقت القديمة — هناك مثيل آخر يمكن أن يحدث فيه هذا وهو عندما يصبح إدخال ذاكرة التخزين المؤقت للمحول السريع خاطئا ويتم تحويل الحزمة الأولى التي تحتوي على ذاكرة تخزين مؤقت مفقودة إلى عملية.

الحلول

1. قم بإيقاف تشغيل أي نوع من المصادقة على مجموعة تحويل 3DES، واستخدم ESP-DES/3DES. يؤدي هذا بشكل فعال إلى تعطيل حماية المصادقة/مكافحة إعادة التشغيل، والتي (بدورها) تمنع أخطاء إسقاط الحزم المتعلقة بحركة مرور IPsec غير المطلوبة (المختلطة) %HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615.

2. أحد الحلول التي تنطبق على السبب المذكور هنا هو تعيين Maximum Transmission Unit (MTU) حجم التدفقات الواردة إلى أقل من 1400 بايت. أدخل هذا الأمر لتعيين الحد الأقصى لحجم وحدة الإرسال (MTU) للتدفقات الواردة إلى أقل من 1400 بايت:

   ```
   ip tcp adjust-mss 1300
   ```

3. تعطيل بطاقة AIM.

4. قم بإيقاف تشغيل التحويل السريع/CEF على واجهات الموجه. لإزالة التحويل السريع، أستخدم هذا الأمر في وضع تكوين الواجهة:

   ```
   no ip route-cache
   ```

خطأ في إستقبال الحزم بسبب فشل تسلسل ESP

هنا مثال من الخطأ رسالة:

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

تشير رسالة الخطأ هذه عادة إلى أحد هذه الشروط المحتملة:

- تتم إعادة توجيه الحزم المشفرة IPsec خارج الأمر بواسطة الموجه المشفر بسبب آلية جودة الخدمة التي تم تكوينها بشكل غير صحيح.
- تكون حزم IPsec التي يتم استقبالها بواسطة موجه فك التشفير خارج الترتيب بسبب إعادة ترتيب الحزمة في جهاز متوسط.
- تمت تجزئة حزمة IPsec المستلمة وتتطلب إعادة التجميع قبل التحقق من المصادقة وفك التشفير.

الحل

1. قم بتعطيل جودة الخدمة لحركة مرور IPsec على الموجهات المتوسطة أو المشفرة.
2. تمكين التجزئة المسبقة ل IPsec على موجه التشفير.

```
<#root>

Router(config-if)#

crypto ipsec fragmentation before-encryption
```

3. قم بتعيين قيمة MTU إلى حجم ال يلزم تجزئته.

```
<#root>

Router(config)#

interface type [slot_#/]port_#
```

```
<#root>

Router(config-if)#

ip mtu MTU_size_in_bytes
```

4. قم بترقية صورة Cisco IOS® إلى أحدث صورة مستقرة متوفرة في ذلك القطار.

إذا تم تغيير حجم وحدة الحد الأقصى للنقل (MTU) على أي موجه، فيجب إسقاط جميع الأنفاق التي تم إنهاؤها على تلك الواجهة.

قم بالتخطيط لإكمال هذا الحل خلال وقت التوقف عن العمل المجدول.

حدث خطأ أثناء محاولة إنشاء نفق VPN على موجه من السلسلة 7600

يتم تلقي هذا الخطأ عندما تحاول إنشاء نفق VPN على موجهات من السلسلة 7600:

```
crypto_engine_select_crypto_engine: can't handle any more
```

يحدث هذا الخطأ لأن تشفير البرامج غير مدعوم على موجهات سلسلة 7600. لا تدعم الموجهات من السلسلة 7600 إنهاء نفق IPsec بدون أجهزة SPA من IPsec. يتم دعم شبكة VPN فقط مع بطاقة IPSec-SPA في موجهات 7600.

تصحيح أخطاء PIX

show crypto isakmp sa

يوضح هذا الأمر ISAKMP SA الذي تم إنشاؤه بين الأقران.

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

في إخراج التشفير isakmp sa، يجب أن تكون الحالة دائما QM_IDLE. إذا كانت الحالة MM_KEY_EXCH، فهذا يعني إما أن المفاتيح الذي تم تكوينه مسبقا غير صحيح أو أن عناوين IP الخاصة بالنظير مختلفة.

<#root>

```
PIX(config)#
```

show crypto isakmp sa

```
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

أنت يستطيع صحح اذه عندما يشكل أنت العنوان صحيح وأ مفتاح مشترك مسبقا.

show crypto ipsec sa

يعرض هذا الأمر رسائل IPsec SAs التي تم إنشاؤها بين الأقران. يتم إنشاء نفق مشفر بين 10.1.0.0 و 10.1.1.0. تحركة المرور التي تنتقل بين الشبكات 10.1.0.2 و 10.1.0.1.

يمكنك مشاهدة نظام خدمة ESP الذين تم إنشاؤهما داخليا وخارجيا. AH غير مستعمل بما أنه لا يوجد AH SAs.

مثال علىshow crypto ipsec saيتم عرض الأمر في هذا الإخراج.

<#root>

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (
```

10.1.0.0/255.255.255.0/0/0

```
)
   remote ident (addr/mask/prot/port): (
```

10.1.0.2/255.255.255.255/0/0

```
)
   current_peer: 10.2.1.1
```

dynamic allocated peer ip: 10.1.0.2

```
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #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.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound
```

esp

```
 sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={
```

Tunnel

```
, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:
```

```
     outbound
```

esp

```
 sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={
```

Tunnel

```
, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debug crypto isakmp

يعرض هذا الأمر معلومات تصحيح الأخطاء حول إتصالات IPsec ويعرض المجموعة الأولى من السمات التي يتم رفضها بسبب عدم التوافق على كل النهايتين.

المحاولة الثانية للمطابقة (لتجربة 3DES بدلا من DES وSecure Hash Algorithm (SHA)مقبول، وتم إنشاء ISAKMP SA.

يأتي تصحيح الأخطاء هذا أيضا من عميل طلب هاتفي يقبل عنوان IP (10.32.8.1) من تجمع محلي. بمجرد إنشاء ISAKMP SA، يتم التفاوض على سمات IPsec ويتم العثور عليها مقبولة.

وبعد ذلك يقوم PIX بإعداد أسماء IPsec كما هو موضح هنا. يوضح هذا الإخراج المأخوذ على**debug crypto isakmp**erasecat4000_flash:.

<#root>

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are not acceptable

```
. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are acceptable

```
. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0):
```

peer accepted the address!

```
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0):
```

atts not acceptable.

```
 Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0):
```

atts are acceptable.

```
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipSec

يعرض هذا الأمر معلومات تصحيح الأخطاء حول إتصالات IPsec.

<#root>

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
```

```
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0):

Creating IPSec SAs
        inbound SA from  10.1.0.2  to  10.1.0.1
           (proxy 10.32.8.1 to  10.1.0.1.)
        has spi 3576885181 and conn_id 2 and flags 4
        outbound SA from  10.1.0.1  to  10.1.0.2
           (proxy 10.1.0.1 to 10.32.8.1)
        has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
           got a queue event...
IPSEC(initialize_sas

): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(

initialize_sas

): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

مشاكل عميل شبكة VPN إلى الموجه الشائع

عدم القدرة على الوصول إلى الشبكات الفرعية خارج نفق VPN: تقسيم النفق

يوضح إخراج تكوين موجه العينة هذه كيفية تمكين نفق تقسيم لاتصالات VPN.

يعرض الأمر **split tunnel**الأمر مرتبط بالمجموعة كما تم تكوينها في**crypto isakmp client configuration group hw-client-groupname**erasecat4000_flash:.

وهذا يسمحCisco VPN Client لاستخدام الموجه للوصول إلى شبكة فرعية إضافية ليست جزءا من نفق VPN.

ويتم القيام بذلك دون التضحية بأية ميزات في أمان اتصال IPsec. يتم تكوين النفق على شبكة 192.0.2.18.

تتدفق حركة المرور غير مشفرة إلى الأجهزة غير المعرفة في**access list 150**أمر، مثل الإنترنت.

<#root>

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool

acl 150

!
!
access-list 150 permit ip 192.0.2.18 0.0.0.127 any
!
```

مشكلات عميل PIX-to-VPN الشائعة

تعالج المواضيع الموجودة في هذا القسم المشاكل الشائعة التي تواجهها عند تكوين PIX إلى IPsec باستخدام تعليمات عميل VPN 3.x. تعتمد عمليات تكوين نموذج PIX على الإصدار 6.x.

لا تتدفق حركة المرور بعد إنشاء النفق: لا يمكن إختبار الاتصال داخل الشبكة خلف PIX

هذه مشكلة عامة مرتبطة بالتوجيه. تأكد من أن PIX به مسار للشبكات الموجودة بالداخل وغير المتصلة مباشرة بنفس الشبكة الفرعية.

كما تحتاج الشبكة الداخلية إلى الحصول على مسار مرة أخرى إلى PIX للعناوين الموجودة في تجمع عناوين العملاء.

تعرض هذه المخرجات مثالا.

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on the inside

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1

 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client for the I

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then the route

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

بعد تشغيل النفق، يتعذر على المستخدم إستعراض إنترنت: تقسيم النفق

السبب الأكثر شيوعا لهذه المشكلة هو أنه، مع نفق IPsec من عميل VPN إلى PIX، يتم إرسال جميع حركة مرور البيانات عبر النفق إلى جدار حماية PIX.

ال تسمح وظيفة PIX بإعادة حركة المرور إلى الواجهة التي تم استقبالها بها. لذلك، ال تعمل حركة المرور الموجهة إلى الإنترنت.

لحل هذه المشكلة، أستخدم**split tunnel**erasecat4000_flash:. الفكرة من وراء هذا الإصلاح أن واحد فقط يرسل حركة مرور معينة عبر النفق وباقي الحركة تذهب مباشرة إلى الإنترنت، وليس من خلال النفق.

<#root>

vpngroup vpn3000 split-tunnel 90

```
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

يعرض الأمر**vpngroup vpn3000 split-tunnel 90**الأمر يمكن النفق المقسم باستخدامaccess-list number 90.

يعرض الأمر**access-list number 90**يحدد الأمر حركة المرور التي تتدفق عبر النفق، ويتم رفض الباقي في نهاية قائمة الوصول.

يجب أن تكون قائمة الوصول هي نفسها لرفضها Network Address Translation (NAT)على PIX.

بعد تشغيل النفق، ال تعمل بعض التطبيقات: تعديل MTU على العميل

بعد إنشاء النفق، وعلى الرغم من إمكانية إختبار اتصال الأجهزة الموجودة على الشبكة خلف جدار حماية PIX، يتعذر عليك إستخدام تطبيقات معينة مثل Microsoft

كوآت

المشكلة الشائعة هي الحد الأقصى لحجم وحدة النقل (MTU) للحزم. يمكن أن يصل رأس IPsec إلى 50 إلى 60 بايت، والذي تتم إضافته إلى الحزمة الأصلية.

إذا أصبح حجم الحزمة أكثر من 1500 (الإعداد الافتراضي للإنترنت)، فيجب على الأجهزة تجزئته. بعد إضافة رأس IPsec، ال يزال الحجم أقل من 1496، وهو الحد الأقصى ل IPsec.

يعرض الأمر **show interface**يعرض الأمر MTU الخاص بتلك الواجهة المحددة على الموجهات التي يمكن الوصول إليها أو على الموجهات في المباني الخاصة بك.

لتحديد الحد الأقصى للنقل (MTU) للمسار بأكمله من المصدر إلى الوجهة، يتم إرسال مخططات البيانات من أحجام مختلفة مع Do Not Fragment (DF)تعيين البت بحيث، إذا كان مخطط البيانات المرسل أكثر من MTU، يتم إرسال رسالة الخطأ هذه إلى المصدر:

```
frag. needed and DF set
```

يوضح هذا الإخراج مثالا لكيفية العثور على وحدة الحد الأقصى للنقل (MTU) للمسار بين 172.16.1.56. و 10.1.1.2 IP عناوين على تحتوي التي المضيفة الأجهزة.

<#root>

```
Router#
```

debug ip icmp

```
ICMP packet debugging is on


!--- Perform an extended ping.

Router#
```

ping

```
Protocol [ip]:
Target IP address:
```

172.16.1.56

```
Repeat count [5]:
Datagram size [100]:
```

1550

```
Timeout in seconds [2]:


!--- Make sure you enter y for extended commands.

Extended commands [n]:
```

y

```
Source address or interface:
```

10.1.1.2

```
Type of service [0]:


!--- Set the DF bit as shown.


Set DF bit in IP header? [no]:
```

y

```
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
```

```
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)


!--- Reduce the datagram size further and perform extended ping again.

Router#

ping

Protocol [ip]:
Target IP address:

172.16.1.56

Repeat count [5]:
Datagram size [100]:

1500

Timeout in seconds [2]:
Extended commands [n]:

y

Source address or interface:

10.1.1.2

Type of service [0]:
Set DF bit in IP header? [no]:

y

Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

أي عميل شبكة VPN مزود بأداة مساعدة لضبط وحدة الحد الأقصى للنقل (MTU) تتيح للمستخدم ضبط وحدة الحد الأقصى للنقل (MTU) لعميل Cisco VPN.

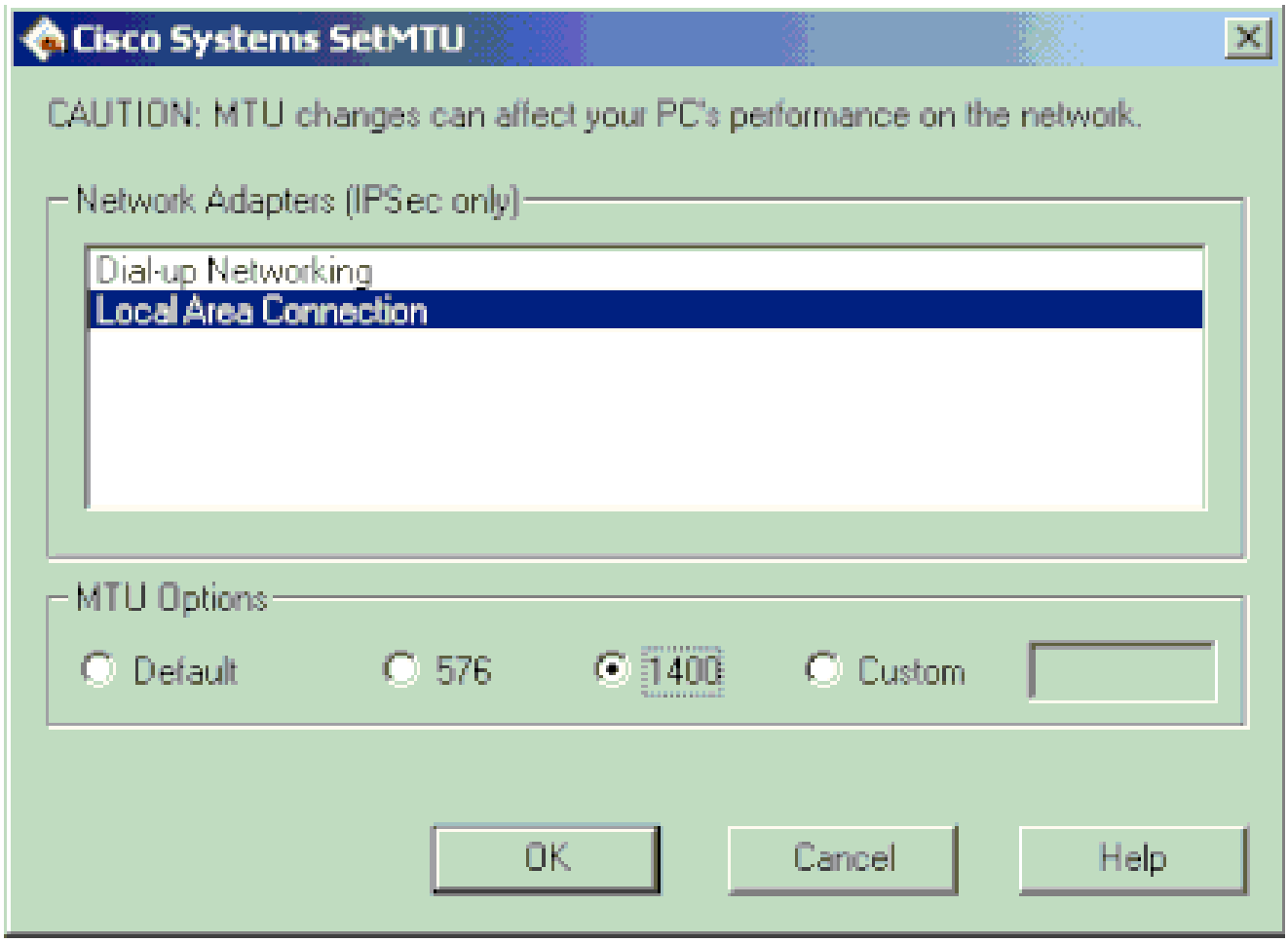
في حالة مستخدمي عميل PPP عبر الإيثرنت (PPPoE)، قم بضبط MTU لمهايئ PPPoE.

أكمل هذه الخطوات لضبط أداة MTU المساعدة لعميل الشبكة الخاصة الظاهرية (VPN).

1. اختر **Start** > **Programs** > **Cisco System VPN Client** > **Set MTU**.

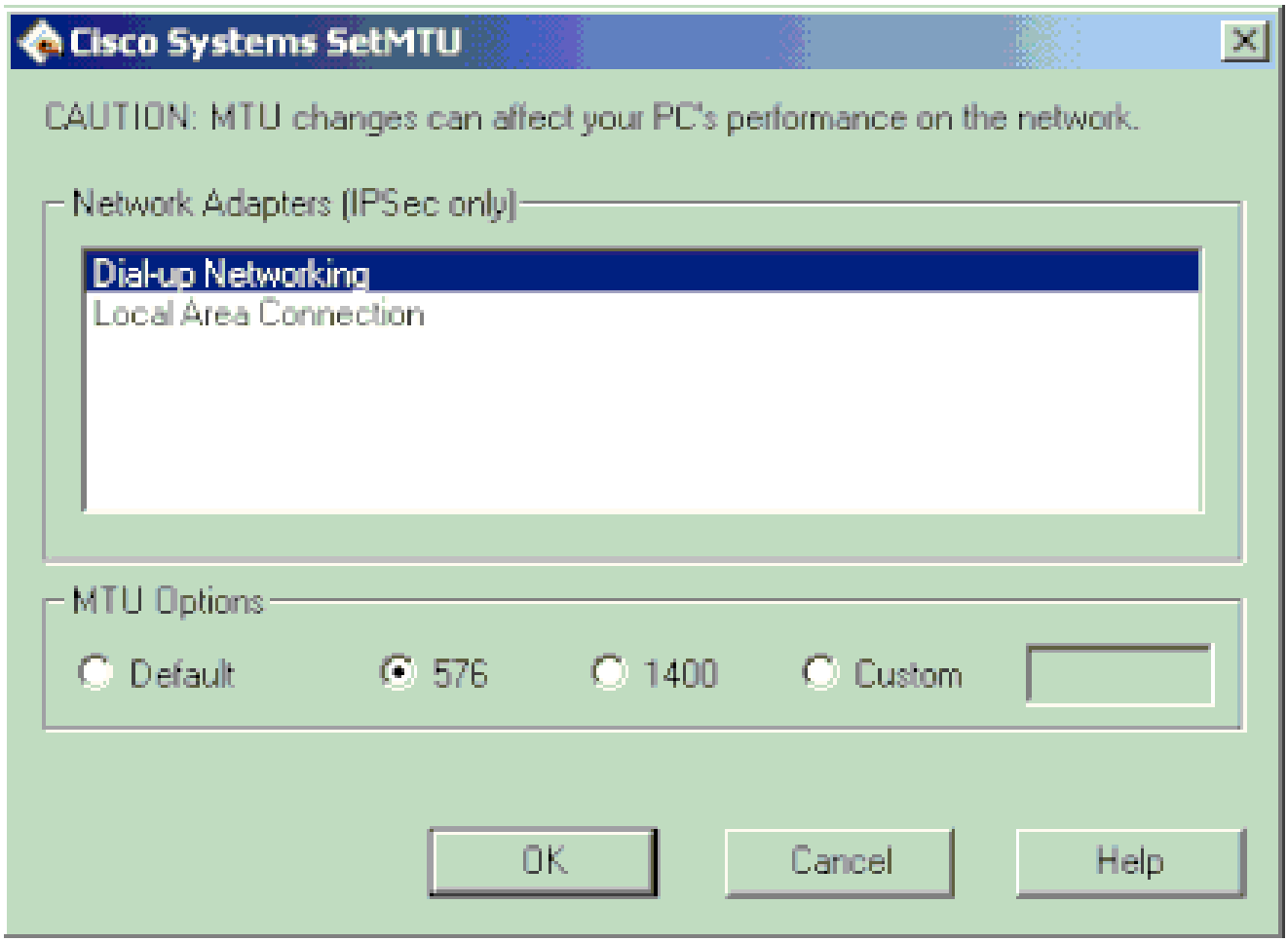
2. تحديدLocal Area Connectionثم انقر زر راديو 1400.

3. انقرOK.



4. كرر الخطوة 1، وحددDial-up Networking.

5. انقر فوق الطرازات576، ثم انقرOK.



أنسى أمر السيوبت

أستخدم **sysopt connection permit-ipsec**لأمر في تكوينات IPsec على PIX للسماح لحركة مرور IPsec بالمرور عبر جدار حماية PIX دون فحص**conduit** أو**access-list**تصريحات القيادة.

بشكل افتراضي، يجب أن يتم السماح بأي جلسة واردة بشكل صريح بواسطة **conduit** أو **access-list**بيان القيادة. باستخدام حركة مرور البيانات المحمية عبر بروتوكول IPsec، يمكن أن يكون التحقق من قائمة الوصول الثانوية زائدا.

لتمكين جلسات عمل IPsec الواردة المصدق عليها/المشفرة ليتم السماح بها دائما، أستخدم**sysopt connection permit-ipsec**erasecat4000_flash:.

التحقق من قوائم التحكم في الوصول (ACL)

هناك قائمتا وصول تستخدمان في تكوين VPN نموذجي ل IPsec. استعملت واحد منفذ قائمة أن يعفي حركة مرور أن يكون معد ل ل ال VPN نفق من ال nat عملية.

تحدد قائمة الوصول الأخرى حركة المرور التي سيتم تشفيرها. وهذا يتضمن قائمة تحكم في الوصول (ACL) التشفير في إعداد شبكة LAN إلى شبكة LAN أو قائمة التحكم في الوصول (ACL) ذات النفق المنقسم في تكوين الوصول عن بعد.

عندما يتم تكوين قوائم التحكم في الوصول (ACL) هذه أو فقدها بشكل غير صحيح، قد تتدفق حركة المرور في إتجاه واحد فقط عبر نفق VPN، أو لم يتم إرسالها عبر النفق على الإطلاق.

تأكد من تكوين جميع قوائم الوصول الضرورية لإكمال تكوين VPN IPsec وأن قوائم الوصول هذه تحدد حركة المرور الصحيحة.

تحتوي هذه القائمة على عناصر للتحقق منها عند الشك في أن قائمة التحكم في الوصول (ACL) هي سبب المشاكل في شبكة VPN الخاصة ب IPsec.

- تأكد من أن قوائم التحكم في الوصول إلى التشفير وإعفاء NAT تحدد حركة المرور الصحيحة.
- إذا كان لديك أنفاق متعددة للشبكة الخاصة الظاهرية (VPN) وقوائم تحكم في الوصول (ACL) المشفرة المتعددة، فتأكد من عدم تداخل قوائم التحكم في الوصول (ACL) هذه.
- لا تستخدم قوائم التحكم في الوصول (ACL) مرتين. حتى إذا كانت قائمة التحكم في الوصول الخاصة بإعفاء NAT وقائمة التحكم في الوصول (ACL) الخاصة بك المشفرة تحدد نفس حركة المرور، فاستخدم قائمتي وصول مختلفتين.
- تأكد من تكوين الجهاز لديك لاستخدام قائمة التحكم في الوصول (ACL) لإعفاء NAT. أي إستخدامroute-mapأمر على الموجه، أستخدمnat (0)أمر على ال PIX أو ASA. يلزم وجود قائمة تحكم في الوصول (ACL) لإعفاء NAT لكل من تكوينات الاتصال من شبكة LAN إلى شبكة LAN وعملاء تكوين الوصول عن بعد.

لمعرفة المزيد حول كيفية التحقق من عبارات قائمة التحكم في الوصول (ACL)، ارجع إلى [التحقق من أن قوائم التحكم في الوصول هي](#) Correctsection [في حلول أستكشاف الأخطاء وإصلاحها ل L2L و Remote Access IPsec VPN الشائعة للغاية](#).

معلومات ذات صلة

- [مفاوضة IPsec/صفحة دعم بروتوكول IKE](#)
- [صفحة دعم PIX](#)
- [الملاحظات الفنية](#)
- [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).