استكشاف مشكلات L2L وشبكة VPN لبروتوكول IPsec للوصول عن بُعد الشائعة وإصلاحها

المحتويات

المقدمة

يصف هذا المستند الحلول الأكثر شيوعاً لمشكلات شبكات VPN لبروتوكول IPsec.

معلومات أساسية

تأتي الحلول الموضحة هنا مباشرة من طلبات الخدمة التي حلها الدعم الفني من Cisco.

يتم تنفيذ العديد من هذه الحلول قبل أستكشاف أخطاء اتصال VPN IPsec وإصلاحها بشكل متعمق.

يقدم هذا المستند ملخص الإجراءات الشائعة للمحاولة قبل بدء أستكشاف أخطاء الاتصال وإصلاحها.

على الرغم من أن أمثلة التكوين الواردة في هذا المستند مخصصة للاستخدام على الموجهات وأجهزة الأمان، فإن جميع هذه المفاهيم تقريبا تنطبق أيضا على شبكة VPN 3000 .

ارجع إلى أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها للحصول على شرح لأوامر تصحيح الأخطاء الشائعة التي يتم إستخدامها لاستكشاف أخطاء IPsec وإصلاحها على كل من برنامج Cisco IOS® و .

ملاحظة: لا يمرر ASA بحركة مرور البث المتعدد عبر أنفاق VPN IPsec.

تحذير: يمكن أن تؤدي العديد من الحلول المقدمة في هذا المستند إلى فقد مؤقت لجميع اتصال IPsec VPN على جهاز ما.

يوصى بتنفيذ هذه الحلول بحذر وبما يتوافق مع سياسة التحكم في التغيير التي تنتهجها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة تكوين VPN IPsec على أجهزة Cisco التالية:

- جهاز الأمان Cisco ASA 5500 Series Security Appliance
- موجهات Cisco IOS®

المكونات المستخدمة

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

- جهاز الأمان Cisco ASA 5500 Series Security Appliance
- برنامج Cisco IOS®

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 نصائح Cisco التقنيةللحصول على مزيد من المعلومات حول اصطلاحات المستندات.

تكوين VPN IPsec لا يعمل

المشكلة

لا يعمل حل IPsec VPN الذي تم تكوينه أو تعديله مؤخرا.

لم يعد تكوين VPN IPsec الحالي يعمل.

الحلول

يحتوي هذا القسم على حلول لمشاكل VPN IPsec الأكثر شيوعا.

على الرغم من أنها غير مدرجة بأي ترتيب معين، إلا أنه يمكن إستخدام هذه الحلول كقائمة إختيار للعناصر للتحقق منها أو المحاولة قبل الشروع في عملية إصلاح متعمقة.

تأتي جميع هذه الحلول مباشرة من طلبات خدمة TAC وقد حلت العديد من المشاكل.

- تمكين إجتياز NAT (#1 ra VPN الصادر)
- إختبار الاتصال بشكل صحيح

- تمكين ISAKMP
- تمكين/تعطيل PFS
- مسح اقترانات الأمان القديمة أو القائمة (الأنفاق)
- التحقق من عمر ISAKMP
- تمكين رسائل keepalives لبروتوكول ISAKMP أو تعطيلها
- إعادة ادخال مفاتيح مشتركة مسبقا أو إسترادها
- مفتاح مشترك مسبق غير متطابق
- إزالة خرائط التشفير وإعادة تطبيقها
- تحقق من وجود أوامر sysopt (/ASA فقط)
- التحقق من هوية ISAKMP
- التحقق من مهلة وضع الخمول/جلسة العمل
- التحقق من صحة قوائم التحكم في الوصول (ACL) وتثبيتها في خريطة التشفير
- التحقق من سياسات ISAKMP
- تحقق من صحة التوجيه
- تحقق من صحة مجموعة التحويل
- التحقق من أرقام تسلسل خريطة التشفير والسم
- التحقق من صحة عنوان IP للنظير
- التحقق من أسماء مجموعة النفق والمجموعة
- تعطيل مصادقة (Xauth) نظائر L2L
- استنفاد تجمع VPN
- مشاكل عمر زمن انتقال حركة مرور عميل VPN

ملاحظة: خفضت بعض الأوامر في هذه الأقسام إلى خط ثان بسبب الاعتبارات المكانية.

تمكين إجتياز NAT (#1 ra VPN إصدار)

يسمح NAT-Traversal (أو NAT-T) لحركة مرور VPN بالمرور من خلال NAT أو أجهزة PAT، مثل موجه Linksys SOHO.

إذا لم يتم تمكين NAT-T، فإن معظم مستخدمي عميل VPN للاتصال ب ASA دون مشكلة، ولكنهم غير قادرين على الوصول إلى الشبكة الداخلية خلف جهاز الأمان.

إن لا يمكن أنت ال NAT-T في ال nat/ضرب أداة، أنت يستطيع إستلمت `القانوني ترجمة يفشل خلق لبروتوكول 50 src داخل:10.0.1.26 dst خارج:10.9.69.4` أطخ ةلاسر في ال ASA.

بالمثل، إذا لم تكن قادرا على تسجيل الدخول بشكل متزامن من عنوان IP نفسه، `يتم إنهاء اتصال VPN الآمن محليا بواسطة العميل. السبب 412: لم يعد النظير البعيد يستجيب.` أطخ ةلاسر رهظت.

مكنت NAT-T في الرئيسي نهاية VPN أداة in order to حللت اذه أطخ.

ملاحظة: باستخدام برنامج Cisco IOS® الإصدار 12.2(13)T والإصدارات الأحدث، يتم تمكين NAT-T بشكل افتراضي في برنامج Cisco IOS®.

وفيما يلي الأمر لتمكين NAT-T على جهاز أمان Cisco. ال 20 (20) في اذه مثال ال keepalive وقت (رصيق).

ASA

<#root>

```
securityappliance(config)#

crypto isakmp nat-traversal 20
```

كما يتعين تعديل العملاء أيضا حتى يتسنى لهم العمل.

في عميل Cisco VPN، انتقل إلى أجهزة الاتصال وانقر فوق تعديل. إنه يفتح نافذة جديدة حيث يجب عليك إختيار TransportTab.

تحت اذه التبويب، انقر فوق تمكين النفق الشفاف وIPSec عبر UDP (nat / pat)زر الراديو. ثم انقر على SaveAnd اختبر الاتصال.

من المهم السماح ل UDP 4500 لمنافذ NAT-T و UDP 500 و ESP بواسطة تكوين قائمة التحكم في الوصول (ACL) لأن ASA يعمل كجهاز nat.

راجع تكوين نفق IPsec من خلال جدار حماية مع NATs للحصول على مزيد من المعلومات لمعرفة المزيد حول تكوين قائمة التحكم في الوصول في ASA.

إختبار الاتصال بشكل صحيح

من الناحية المثالية، يتم إختبار اتصال VPN من الأجهزة الموجودة خلف أجهزة نقطة النهاية التي تقوم بالتشفير، ومع ذلك يختبر العديد من المستخدمين اتصال VPN باستخدام الأمر التالي على الأجهزة التي تقوم بالتشفير.

في حين أن إختبار الاتصال يعمل بشكل عام لهذا الغرض، فمن المهم أن يتم توفير إختبار الاتصال الخاص بك من الواجهة الصحيحة.

إذا تم الحصول على اتصال VPN بشكل غير صحيح، فقد يبدو أن اتصال VPN فشل عندما يعمل بالفعل. هذا مثال واحد:

قائمة التحكم في الوصول (ACL) المشفرة للموجه A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

قائمة التحكم في الوصول (ACL) المشفرة للموجه B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

في هذه الحالة، يجب الحصول على المنفذ من الشبكة الداخلية خلف أي من الموجهين. وذلك لتكوين قوائم التحكم في الوصول (ACL) للتشفير فقط لتشفير حركة المرور نظرا باستخدام عناوين المصدر هذه.

لم يتم تشفير الوصول إلى المصدر من الواجهات الخارجية لأي من الموجهات. أستخدم الخيارات الموسعة للأمر في وضع EXEC ذي الامتيازات لمصادر إختبار اتصال من الواجهة الداخلية للموجه:

<#root>

```
routerA#

ping

Protocol [ip]:

Target IP address: 192.168.200.10

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.100.1

Type of service [0]:
Set DF bit in IP header? [no]:
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, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.100.1

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

تخيل أنه تم إستبدال الموجهات في هذه الطوبولوجيا بأجهزة أمان ASA. كما يمكن الحصول على

الاتصال الذي يتم إستخدامه لاختبار الاتصال من الواجهة الداخلية باستخدام الكلمة الألأساسية الداخلية:

<#root>

securityappliance#

ping inside 192.168.200.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ال يوصى باستهداف الواجهة الداخلية لجهاز الأمان باستخدام عملية إختبار الاتصال.

إذا كان يجب عليك إستهداف الواجهة الداخلية باستخدام عملية إختبار الاتصال، فيجب عليك تمكين الوصول إلى هذه الواجهة، أو أ الى موقع الجهاز بالدرل.

<#root>

securityappliance(config)#

management-access inside

عندما توجد مشكلة في الاتصال، فإن حتى المرحلة الأولى (1) من VPN ال تعمل.

في ASA، إذا فشل الاتصال، فإن إخراج SA ممائل لهذا المثال، والذي يشير إلى تكوين نظير تشفير غير صحيح محتمل و/أو تكوين اقتراح ISAKMP غير صحيح:

<#root>

Router#

show crypto isakmp sa

1   IKE Peer: XX.XX.XX.XX
    Type   : L2L   Role   : initiator
    Rekey   : no   State   : MM_WAIT_MSG2

يمكن أن تكون الحالة من MM_WAIT_MSG2 إلى MM_WAIT_MSG5، مما يشير إلى فشل تبادل الحالة المعني في الوضع الرئيسي (MM).

إخراج Crypto SA عندما تكون المرحلة 1 ألأعلى ممائل لهذا المثال:

<#root>

```
Router#
show crypto isakmp sa

1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

تمكين ISAKMP

إذا لم يكن هناك أي مؤشر على أن قفن IPsec VPN يعمل، فمن المحتمل أن ISAKMP لم يتم تمكينه. تأكد من تمكين ISAKMP على أجهزتك.

أستخدم أحد هذه الأوامر لتمكين ISAKMP على أجهزتك:

برنامج Cisco IOS®

```
<#root>
router(config)#
crypto isakmp enable
```

Cisco ASA (تغيير الواجهة الخارجية باستخدام الواجهة المطلوبة)

```
<#root>
securityappliance(config)#
crypto isakmp enable outside
```

أنت يستطيع أيضا حصلت هذه خطأ عندما أنت يمكن ال isakmp على القارن خارجي:

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

السبب من الخطأ يستطيع كنت أن يحصل الزبون خلف ASA ضرب إلى udp ميناء 500 قبل ضرب (مسح xlate)، ال isakmp يستطيع كنت تمكن على القارن. ما إن أزلت ترجمة ضرب أن يكون isakmp يستطيع كنت تمكن.

تحقق من أن أرقام منافذ UDP 500 و 4500 محجوزة للتفاوض على إتصالات ISAKMP مع النظير.

عندما ال يتم تمكين ISAKMP على الواجهة، يظهر عميل VPN رسالة خطأ مماثلة لهذه

الرسالة:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

لحل هذا الخطأ، قم بتمكين ISAKMP على واجهة التشفير لبوابة VPN.

تمكين/تعطيل PFS

في مفاوضات IPsec، تضمن سرية إعادة التوجيه الكاملة (PFS) عدم إرتباط كل مفتاح تشفير جديد بأي مفتاح سابق.

إما أن يمكنك أو أعجزت PFS على الكل من نظام النفق؛ وإلا، فإن نفق LAN إلى LAN (L2L) IPsec الذي تم إنشاؤه في موجه ASA / Cisco IOS®.

السرية المثالية لإعادة التوجيه (PFS) خاصة ب Cisco والتي تم دعمها على أجهزة الطرف الثالث.

ASA:

يتم تعطيل PFS بشكل افتراضي. لتمكين PFS، أستخدم الأمرpFFs مع الكلمة الأساسية الكلمة المفاتيح. دخلت in order to أعجزت PFS، ال disable في وضع تكوين نهج المجموعة.

```
<#root>

hostname(config-group-policy)#

pfs {enable | disable}
```

دخلت in order to أزلت ال PFS سمة من التشكيل، ال ام من شكل من هذا أمر.

يمكن أن يرث نهج المجموعة قيمة ل PFS من نهج مجموعة آخر. أدخل نموذج no من هذا الأمر لمنع نقل قيمة.

```
<#root>

hostname(config-group-policy)#

no pfs
```

الموجه Cisco IOS®:

لتحديد أنه يجب على IPsec طلب PFS عند طلب اقترانات أمان جديدة لإدخال خريطة التشفير هذا، أستخدم الأمر set pfscommand في وضع تكوين خريطة التشفير.

لتحديد أن IPsec يتطلب PFS عندما يستلم طلبات اقترانات أمان جديدة، أستخدم الأمر show pfsg هذا في وضع تكوين خريطة التشفير.

لتحديد أنه يجب على IPsec عدم طلب PFS، أستخدم الصيغة no من هذا الأمر. بشكل افتراضي، ال يتم طلب ملفات PFS. إذا لم يتم تحديد مجموعة باستخدام هذا الأمر، فسيتم إستخدام المجموعة 1 كافتراضي.

```
set pfs [group1 | group2]
no set pfs
```

بالنسبة لأمر مجموعة ملفات PFS:

- مجموعة1 — يحدد أنه يجب على IPsec إستخدام مجموعة وحدات Diffie-Hellman الأساسية ذات 768 بت عند إجراء تبادل Diffie-Hellman جديد.
- مجموعة2 — يحدد أنه يجب على IPsec إستخدام مجموعة وحدات Diffie-Hellman الأساسية ذات 1024 بت عند إجراء تبادل Diffie-Hellman جديد.

مثال:

```
<#root>

Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#

set pfs group2
```

مسح اقترانات الأمان القديمة أو الحالية (الأنفاق)

إذا حدثت رسالة الخطأ هذه في موجه Cisco IOS®®، فإن المشكلة هي أن SA قد انتهت صلاحيته أو تم مسحه.

ال يعرف جهاز نهاية النفق البعيد أنه يستخدم SA منتهي الصلاحية لإرسال حزمة (ليس حزمة إنشاء SA).

عند إنشاء مساعد خدمة جديد، يتم إستئناف الاتصال، لذلك ابدأ حركة المرور المهمة عبر النفق لإنشاء مساعد خدمة جديد وإعادة إنشاء النفق.

```
<#root>

%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA
```

إذا قمت بمسح اقترانات أمان ISAKMP (المرحلة الأولى) و IPsec (المرحلة الثانية) (SAs)، فهذا هو الحل الأكثر بساطة وغالبا الأفضل لحل مشاكل شبكات VPN الخاصة ب IPsec.

إذا قمت بمسح أسماء المجالات (SAs)، فيمكنك بشكل متكرر حل مجموعة كبيرة ومتنوعة من رسائل الخطأ والسلوكيات الغريبة دون الحاجة إلى أستكشاف الأخطاء وإصلاحها.

بينما يمكن إستخدام هذا الأسلوب بسهولة في أي حالة، إلا أنه غالبا ما يكون متطلبا مسح SAs بعد تغيير تكوين شبكة VPN IPsec الحالية وأ إضافته إلى هذا التكوين.

علاوة على ذلك، في حين أنه من الممكن مسح إرتباطات أمنية محددة فقط، إلا أن الفائدة الأكبر يمكن أن تتحقق عندما توقم بإلغاء تحديد معايير الخدمة (SAs) بشكل عام على الجهاز.

وبمجرد مسح الرابطات الأمنية، قد يكون من الضروري إرسال حركة المرور عبر النفق لإعادة إنشائها.

تحذير: إذا لم تحدد أي اقترانات أمان سيتم مسحها، يمكن للأوامر المدرجة هنا مسح جميع اقترانات الأمان على الجهاز. المتابعة بحذر إذا كانت أنفاق VPN الأخرى ل IPsec قيد الاستخدام.

1. عرض اقترانات الأمان قبل إزالتها

   a. برنامج Cisco IOS®

```
<#root>
router#
show crypto isakmp sa
router#
show crypto ipsec sa
```

   b. أجهزة أمان ASA من Cisco

```
<#root>
securityappliance#
show crypto isakmp sa
securityappliance#
show crypto ipsec sa
```

2. مسح اقترانات الأمان. يمكن إدخال كل أمر كما هو موضح بالأسود أو إدخاله بالخيارات المعروضة معه.

a. برنامج Cisco IOS®

a. ISAKMP (المرحلة الأولى)

<#root>

```
router#

clear crypto isakmp

 ?
  <0 - 32766>  connection id of SA
  <cr>
```

b. IPsec (المرحلة الثانية)

<#root>

```
router#

clear crypto sa

 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```

b. أجهزة أمان ASA من Cisco

a. ISAKMP (المرحلة الأولى)

<#root>

```
securityappliance#

clear crypto isakmp sa
```

b. IPsec (المرحلة الثانية)

<#root>

```
security appliance#

clear crypto ipsec sa

 ?

  counters  Clear IPsec SA counters
```

```
entry     Clear IPsec SAs by entry
map       Clear IPsec SAs by map
peer      Clear IPsec SA by peer
<cr>
```

التحقق من عمر ISAKMP

إذا تم قطع اتصال المستخدمين بشكل متكرر عبر نفق L2L، فقد تكون المشكلة هي مدة عمر ISAKMP SA التي تم تكوينها في البداية.

إذا حدث أي أختلاف في فترة عمر ISAKMP، فيمكنك تلقي ASA-5-713092: المجموعة = x.x.x.x، IP = x.x.x.x، الفشل أثناء المرحلة 1 لمحاولة إعادة المفاتيح بسبب رسالة خطأ التصادم في /ASA.

التقصير هو 86،400 ثاني أو 24 ساعة. وكقاعدة عامة، يوفر العمر الافتراضي الأقصر، يقوم مفاوضات ISAKMP الأكثر أمانا (حتى نقطة معينة)، ولكن مع فترات الحياة الأقصر، يقوم جهاز الأمان بإعداد عمليات IPsec المستقبلية بشكل أسرع.

يتم إجراء التطابق عندما تحتوي كل النهجين من النظيرين على نفس قيم معلمات التشفير والتجزئة والمصادقة و Diffie-Hellman، وعندما تحدد سياسة النظير البعيد فترة حياة أقل من العمر الافتراضي أو مساوية له في النهج المقارن.

وإذا كانت فترات الحياة غير متطابقة، تستعمل فترة الحياة الاقصر — من سياسة النظير البعيد. وفي حالة عدم العثور على تطابق مقبول، ترفض IKE التفاوض، ولا يتم إنشاء IKE SA.

تحديد مدة بقاء SA. تحدد هذه المثلة مدة حياة تبلغ 4 ساعات (14400 ثانية). التقصير 86400 ثاني (24 ساعة).

ASA

<#root>

```
hostname(config)#
```

isakmp policy 2 lifetime 14400

موجه IOS® من Cisco

<#root>

```
R2(config)#
```

crypto isakmp policy 10

```
R2(config-isakmp)#
```

lifetime 86400

إذا تم تجاوز الحد الأقصى لفترة الحياة التي تم تكوينها، فأنت تتلقى رسالة الخطأ هذه عند إنهاء اتصال VPN:

تم إنهاء اتصال VPN الآمن محليا بواسطة العميل. السبب 426: تجاوز الحد الأقصى لفترة البقاء التي تم تكوينها.

لحل رسالة الخطأ هذه، قم بتعيين قيمة الوقت إلى صفر (0) لتعيين عمر اقتران أمان IKE إلى ما لا نهاية. ال VPN دائما يكون ربطت والى ينهي.

```
hostname(config)#isakmp policy 2 lifetime 0
```

أنت يستطيع أيضا أعجزت rexauth في المجموعة-policy in order to حللت الإصدار.

تمكين رسائل keepalives لبروتوكول ISAKMP أو تعطيلها

إذا قمت بتكوين رسائل تنشيط ISAKMP، فإنها تساعد على منع السقوط العرضي لشبكة LAN إلى شبكة LAN أو شبكة VPN للوصول عن بعد، والتي تتضمن عملاء شبكة VPN والأنفاق والأنفاق التي يتم إسقاطها بعد فترة من عدم النشاط.

تتيح هذه الميزة لنقطة نهاية النفق مراقبة التواجد المستمر لنظير بعيد والإبلاغ عن وجوده الخاص لذلك النظير.

إذا أصبح النظير غير متجاوب، تزيل نقطة النهاية الاتصال.

لكي تعمل حزم ISAKMP keepalives، يجب أن تدعمها كل من نقاط نهاية شبكات VPN.

تكوين رسائل تنشيط ISAKMP في Cisco IOS® باستخدام هذا الأمر:

```
<#root>

router(config)#

crypto isakmp keepalive 15
```

أستخدم هذه الأوامر لتكوين رسائل تنشيط الاتصال ISAKMP على أجهزة أمان ASA:

Cisco ASA لمجموعة الأنفاق المسماة 10.165.205.222

```
<#root>

securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#
```

```
isakmp keepalive
   threshold 15 retry 10
```

في بعض الحالات، من الضروري تعطيل هذه الميزة لحل المشكلة، على سبيل المثال، إذا كان عميل VPN خلف جدار حماية يمنع حزم DPD.

Cisco ASA، لمجموعة الأنفاق المسماة 10.165.205.222

تعطيل معالجة IKE keepalive، والتي يتم تمكينها بشكل افتراضي.

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

تعطيل Keepalive لعميل Cisco VPN 4.x

انتقل إلى٪System Root٪ > Program Files (جذر النظام) > Cisco Systems > VPN Client (عميل الشبكة الخاصة الظاهرية) > ملفات التعريف على جهاز الكمبيوتر العميل الذي يواجه المشكلة لتعطيل IKE Keepalive، وتحرير ملف PCF، حيثما ينطبق ذلك، للاتصال.

تغيير ForceKeepAlives=0(الافتراضي) إلى ForceKeepAlives=1.

رسائل Keepalives خاصة من Cisco والمعتمدة أجهزة الطرف الثالث.

إعادة إدخال مفاتيح مشتركة مسبقا أو إستردادها

في العديد من الحالات، قد يكون خطأ مطبعي بسيط السبب في عدم عمل نفق IPsec VPN. على سبيل المثال، في جهاز الأمان، تصبح المفاتيح المشتركة مسبقا مخفية بمجرد إدخالها.

هذا التشويش يجعل من المستحيل معرفة ما إذا كان المفتاح غير صحيح. تأكد من إدخال أي مفاتيح مشتركة مسبقا بشكل صحيح على كل نقطة نهاية لشبكة VPN.

أعد إدخال مفتاح للتأكد من صحته، وهذا حل بسيط يمكن أن يساعد على تجنب أستكشاف الأخطاء وإصلاحها بشكل متعمق.

في VPN للوصول عن بعد، تحقق من إدخال اسم المجموعة الصحيح والمفتاح المشترك

مسبقا في عميل CiscoVPN.

أنت يستطيع واجهت اذه خطأ أن المجموعة إسم وأ مفتاح سابق التزامن غير مطابق بين ال VPN زبون والل head-end أداة.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

تحذير: إذا قمت بإزالة الأوامر المتعلقة بالشفرة، فمن المرجح أن توقت مع إسقاط واحد أو كل ك. أستخدم هذه الأوامر مع توخي الحذر والرجوع إلى دليل (VPN) الظاهرية الخاصة بشبكة أنفاق الشبكة الخاصة بمؤسستك قبل إزالة الأوامر المتعلقة بالشفرة.

أستخدم هذه الأوامر لإزالة KeySecretKey المشترك مسبقا وإعادة إدخاله للنظير 10.0.0.1 أو GroupVpnGroupPin Cisco IOS®:

شبكة VPN من Cisco LAN إلى LAN

```
<#root>

router(config)#

no crypto isakmp key secretkey
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

Cisco Remote Access VPN

<#root>

```
router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

أستخدم هذه الأوامر لإزالة KeySecretKey المشترك مسبقا وإعادة إدخاله لأجهزة الأمان النظيرة 10.0.0.1on /ASA:

Cisco 6.x

```
<#root>

(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x والإصدارات الأحدث

```
<#root>

securityappliance(config)#

tunnel-group 10.0.0.1
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key

securityappliance(config-tunnel-ipsec)#

ikev1


pre-shared-key
   secretkey
```

مفتاح مشترك مسبقا غير متطابق

يتم قطع اتصال بدء "نفق VPN". تحدث هذه المشكلة بسبب عدم تطابق مفتاح مشترك مسبقا أثناء مفاوضات المرحلة الأولى.

تشير الرسالة MM_WAIT_MSG_6 في الأمر AShow crypto isakmp إلى مفتاح مشترك مسبق غير متطابق كما هو موضح في هذا المثال:

<#root>

ASA#

show crypto isakmp sa

```
Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :
```

MM_WAIT_MSG_6

لحل هذه المشكلة، أعد إدخال المفتاح المشترك مسبق في كل الجهازين، ويجب أن يكون المفتاح المشترك مسبق فريدا ومطابق. راجع إعادة إدخال أو إستعادة Keysfor مزيد من المعلومات.

إزالة خرائط التشفير وإعادة تطبيقها

عند مسح إقترانات الأمان، ولا يقوم بحل مشكلة IPsec VPN، قم بإزالة خريطة التشفير ذات الصلة وإعادة تطبيقها لحل مجموعة متنوعة من المشاكل التي تتضمن عملاء السوق المتقطعة لنفق VPN وفشل بعض مواقع VPN في الظهور.

تحذير: إذا قمت بإزالة خريطة تشفير من واجهة، فسيقوم IPsec بتنزيل أي أنفاق IPsec المقترنة بخريطة التشفير هذه. انتقل بحذر إلى هذه الخطوات وتفكر في سياسة التحكم بالتغيير الخاصة بمؤسستك قبل المتابعة.

أستخدم هذه الأوامر لإزالة خريطة تشفير واستبدالها في Cisco IOS®:

ابدأ بإزالة خريطة التشفير من الواجهة. أستخدم الأمر no form of thecrypto mapcommand.

<#root>

```
router(config-if)#
```

no crypto map mymap

الاستمرار في إستخدام thenoform لإزالة خريطة تشفير بالكامل.

<#root>

```
router(config)#
```

```
no crypto map mymap 10
```

استبدلت ال crypto خريطة على قارن إثرنيت0/0 للنظير10.0.0.1. يوضح هذا المثال تكوين خريطة التشفير الأدنى المطلوب:

```
<#root>

router(config)#

crypto map mymap 10 ipsec-isakmp

router(config-crypto-map)#

match address 101

router(config-crypto-map)#

set transform-set mySET

router(config-crypto-map)#

set peer 10.0.0.1

router(config-crypto-map)#

exit

router(config)#

interface ethernet0/0

router(config-if)#

crypto map mymap
```

أستخدم هذه الأوامر لإزالة خريطة تشفير واستبدالها على ASA:

ابدأ بإزالة خريطة التشفير من الواجهة. أستخدم الأمر no form of thecrypto mapcommand.

```
<#root>

securityappliance(config)#

no crypto map mymap interface outside
```

تابع إستخدام thenoform لإزالة أوامر خريطة التشفير الأخرى.

```
<#root>

securityappliance(config)#

no crypto map mymap 10 match
   address 101
```

```
securityappliance(config)#

no crypto map mymap set
   transform-set mySET

securityappliance(config)#

no crypto map mymap set
   peer 10.0.0.1
```

استبدل خريطة التشفير للنظير 10.0.0.1. يوضح هذا المثال تكوين خريطة التشفير الأدنى المطلوب:

```
<#root>

securityappliance(config)#

crypto map mymap 10 ipsec-isakmp

securityappliance(config)#

crypto map mymap 10
   match address 101

securityappliance(config)#

crypto map mymap 10 set
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

إذا قمت بإزالة خريطة التشفير وإعادة تطبيقها، فهذا يعمل أيضا على حل مشكلة الاتصال إذا تم تغيير عنوان IP الخاص بالطرف الرئيسي.

تحقق من وجود أوامر sysopt (ASA فقط)

يسمح اتصال CommandSysptباتصال IPsec-vpnallow الجزم من نفق IPsec وحمولتها لتتجاوز قوائم التحكم في الوصول الخاصة بالواجهة على جهاز الأمان.

من المحتمل أن تفشل أنفاق IPsec التي يتم إنهاؤها على جهاز الأمان إذا لم يتم تكوين أحد هذه الأوامر.

في الإصدار 7.0 من برنامج جهاز الأمان والإصدارات الأقدم، فإن الأمر sysopt ذو الصلة أمر اتصال iSub لهذه الحالة.

في الإصدار 7.1(1) من برنامج جهاز الأمان والإصدارات الأحدث، الأمر sysopt ذي الصلة لهذه الحالة issysopt connection allowed-vpn.

في 6.x، هذه الوظيفة مطلوبة بشكل افتراضي. مع ASA 7.0(1) والإصدارات الأحدث، يتم تمكين هذه الوظيفة بشكل افتراضي. أستخدم الأوامر العرض التالية لتحديد ما إذا تم تمكين الأمر relatedsyffCommand على جهازك:

Cisco من ASA

```
<#root>

securityappliance#

show running-config all sysopt

no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret

sysopt connection permit-vpn


!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

استعملت هذا أمر in order to مكنت ال يصحيحsyffCommand لجهازك:

Cisco من ASA

```
<#root>

securityappliance(config)#

sysopt connection permit-vpn
```

إذا كنت ال ترغب في إستخدام الأمر هذاOpt Connection، فعليك السماح بشكل صريح بحركة المرور المفيدة المطلوبة من المصدر إلى الوجهة.

على سبيل المثال، من الشبكة المحلية (LAN) البعيدة إلى الشبكة المحلية للجهاز البعيد و"منفذ UDP 500" للواجهة الخارجية للجهاز البعيد إلى الواجهة الخارجية للجهاز المحلي، في قائمة التحكم في الوصول (ACL) الخارجية.

التحقق من هوية ISAKMP

إذا فشل نفق IPsec VPN ضمن تفاوض IKE، فقد يكون الفشل ناجما عن عدم قدرة النظير على التعرف على هوية النظير الخاص به أو عن عدم قدرته على ذلك.

عندما يستخدم إثنان من النظراء IKE لإنشاء اقترانات أمان IPsec، يرسل كل نظير هوية ISAKMP الخاصة به إلى النظير البعيد.

ووه لسري إما عنوان IP الخاص به أو اسم المضيف بناء على كيفية حصول كل واحد على مجموعة هوية ISAKMP الخاصة به.

بشكل افتراضي، يتم تعيين هوية ISAKMP لوحدة جدار الحماية على عنوان IP.

كقاعدة عامة، قم بتعيين جهاز الأمان وهوياته أقرانه بنفس الطريقة لتجنب فشل مفاوضات IKE.

لتعيين معرف المرحلة 2 الذي سيتم إرساله إلى النظير، استخدم الأمر identityIP في وضع التكوين العام.

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

أو

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

أو

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

يفشل نفق VPN في الظهور بعد نقل التكوين من ASA إلى ASA باستخدام أداة ترحيل تكوين ASA؛ تظهر هذه الرسائل في السجل:

[IKEv1]: المجموعة = x.x.x.x، IP = x.x.x.x، تم العثور على **PeerTblEntry**، إزالة!

[IKEv1]: المجموعة = x.x.x.x، IP = x.x.x.x، فشلت إزالة النظير من جدول أداة الربط، ال يوجد تطابق!

[IKEv1]: المجموعة = x.x.x.x، IP = x.x.x.x، construct_ipsec_delete(): ال يوجد SPI لتعريف المرحلة 2 SA!

[IKEv1]: المجموعة = x.x.x.x، IP = x.x.x.x، فشلت إزالة النظير من جدول أداة الربط، ال يوجد تطابق!

التحقق من مهلة وضع الخمول/جلسة العمل

إذا تم تعيين مهلة الخمول على 30 دقيقة (الافتراضي)، فهذا يعني أنها تسقط النفق بعد 30 دقيقة من عدم مرور البيانات خلاله.

يتم قطع اتصال عميل VPN بعد 30 دقيقة بغض النظر عن المعلمة المهلة الخاملة ويصادف خطأ PEER_DELETE-IKE_DELETE_UNSPECIFIED.

يتم تكوين المهلة الزمنية لجلسة عمل TimeOutasIn لإنشاء النفق دائما، وبالتالي لا يتم إسقاط النفق أبدا حتى عند إستخدام أجهزة الطرف الثالث.

ASA

ادخل تلك ال vpn-idle-timeoutcommand في مجموعة-policy تشكيل أسلوب أو في username تشكيل أسلوب in order to شكل تلك المستعمل مهلة فترة:

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-idle-timeout none
```

شكل تلك الحد الأقصى وقت ل VPN توصيل مع ال vpn-session-timeoutcommand في مجموعة-policy تشكيل أسلوب أو في username تشكيل أسلوب:

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-session-timeout none
```

عندما يتوفر لديك مهلة النفق-enabled، فأنت لا تحتاج إلى تكوين مهلة الخمول لأنه، حتى إذا قمت بتكوين مهلة VPN-Idle، فإنها لا تعمل لأن جميع حركة المرور تمر عبر النفق (منذ تكوين النفق-all).

لذلك، فإن حركة المرور المثيرة للاهتمام (أو حتى حركة المرور التي تم إنشاؤها بواسطة الكمبيوتر الشخصي) مثيرة للاهتمام ولا تسمح للمهلة الخاملة بالبدء في العمل.

موجه IOS® من Cisco

إستخدم الأمر thecrypto IPsec security-association idle-timeccommand في وضع التكوين العام أو وضع تكوين خريطة التشفير لتكوين مؤقت خمول IPsec SA.

مت ليطعت تاتقؤم لومخ IPsec SA بشكل افتراضي.

<#root>

```
crypto ipsec security-association idle-time
seconds
```

على ظافحلاب طشن ريغ ريظنل لماخلا تقؤملا حمسي يتلاو ،ينا‌وثلاب تقولا سايق متي SA. تحوارت ميقلا ةحلاصلا ةطيسوللو الثانية نم 60 إلى 86400.

التحقق نم ةحص مئاوق التحكم في الوصول (ACL) وتثبيتها في خريطة التشفير

ةمئاق ذفنم دحاو تلمعتسا .IPsec ل يجذومن VPN نيوكت يف نامدختست لوصو اتمئاق كانه نأ يعفي ةكرح رورم نأ نوكي دعم ل ل لا VPN نم قفن لا nat عمليةٍ.

مكحتلا ةمئاق نمضتي اذهو ،اهريفشت ديرت يتلا رورملا ةكرح ىرخألا لوصولا ةمئاق ددحت في الوصول (ACL) الخاصة بالتشفير في إعداد شبكة LAN إلى شبكة LAN وأ ةمئاق التحكم في الوصول (ACL) ذات النفق المنقسم في تكوين الوصول عن بعد.

عندما يتم تكوين مئاوق التحكم في الوصول (ACL) هذه وأ فقدها بشكل غير صحيح، فقد تتدفق حركة المرور في إتجاه واحد عبر نفق VPN، أو ال يتم إرسالها عبر النفق على الإطالق.

تأكد نم طبر ةمئاق التحكم في الوصول (ACL) للتشفير بخريطة التشفير باستخدام األمر crypto map match address في وضع التكوين العام.

تأكد نم تكوين جميع قوائم الوصول الضرورية إلكمال تكوين VPN IPsec وأن قوائم الوصول هذه تحدد حركة المرور الصحيحة.

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

تأكد نم 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 نم عدم تداخل قوائم التحكم في الوصول (ACL) هذه.

تأكد نم تكوين الجهاز الستخدام قائمة التحكم في الوصول (ACL) إلعفاء NAT. على جهاز تحديد، هذا يعني أن تستخدم theroute-mapcommand.

على ال ASA، هذا يعني أن تستخدم هذا األمر (0). يلزم وجود قائمة تحكم في الوصول (ACL) إلعفاء NAT لكل من اتصاالت تكوينات شبكة LAN والوصول عن بعد.

هنا، تشكل cisco ios ® جهاز تحديد أن يعفي حركة مرور أن يكون أرسلت بين 192.168.100.0 /24 و192.168.200.0 /24 أو192.168.1.0 /24 من nat. تخضع حركة المرور الموجهة إلى أي مكان آخر /24

إلى الحمل الزائد ل NAT:

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

تعمل قوائم التحكم في الوصول إلعفاء NAT فقط عم عنوان IP أو شبكات IP، مثل تلك المذكورة في الأمثلة (noNAT لقائمة الوصول)، ويجب أن تكون مطابقة لقوائم التحكم في الوصول (ACL) لخريطة التشفير.

ال تعمل قوائم التحكم في الوصول (ACL) الخاصة بإعفاء NAT مع أرقام المنافذ (على سبيل المثال، 23 و 25،...).

في بيئة VoIP، حيث تم توصيل المكالمات الصوتية بين الشبكات من خالل شبكة VPN، ال تعمل المكالمات الصوتية إذا لم يتم تكوين قوائم التحكم في الوصول إلى NAT 0 بشكل صحيح.

قبل أستكشاف الأخطاء وإصالحها، يقترح التحقق من حالة اتصال شبكة VPN لأن المشكلة قد تكون في التكوين الخاطئ لقوائم التحكم في الوصول (ACL) المعفاة من NAT.

يمكنك الحصول على رسالة الخطأ كما هو موضح إذا كان هناك عدم تكوين في قوائم التحكم في الوصول (ACLs) إلعفاء NAT (nat 0).

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

مثال غير صحيح:

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0

eq 25
```

إن ال يعمل إعفاء nat (nat 0)، بعد ذلك حاول إزالة أو أصدر الأمر nat 0 in order to عمل.

تأكد من أن قوائم التحكم في الوصول (ACL) لديك ليست معكوسة وأنها النوع الصحيح.

يجب كتابة قوائم التحكم في الوصول الخاصة بإستثناء التشفير و NAT لتكوينات شبكة LAN إلى شبكة LAN من منظور الجهاز الذي تم تكوين قائمة التحكم في الوصول عليه.

وهذا يعني أن قوائم التحكم في الوصول (ACL) يجب أن تصل إلى بعضها البعض. في هذا المثال، يتم إعداد نفق من شبكة LAN إلى شبكة LAN بين 192.168.100.0 /24 و192.168.200.0 /24.

قائمة التحكم في الوصول (ACL) المشفرة للموجه A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

قائمة التحكم في الوصول (ACL) المشفرة للموجه B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

على الرغم من أنه غير موضح هنا، إلا أن هذا المفهوم نفسه ينطبق على أجهزة أمان ASA.

في ASA، يجب أن تحدد قوائم التحكم في الوصول (ACL) للنفق المقسم لتكوينات الوصول عن بعد قوائم الوصول التي تسمح بحركة المرور إلى الشبكات التي يحتاج عملاء شبكة VPN إلى الوصول إليها.

يمكن لموجهات Cisco IOS® إستخدام قائمة التحكم في الوصول (ACL) الموسعة للنفق المنقسم. في قائمة الوصول الموسعة، يكون إستخدام 'any' في المصدر في قائمة التحكم في الوصول (ACL) للنفق المنقسم مماثلا لتعطيل النفق المنقسم.

أستخدم فقط الشبكات المصدر في قائمة التحكم في الوصول (ACL) الموسعة للنفق المقسم.

مثال صحيح:

<#root>

access-list 140 permit ip

10.1.0.0 0.0.255.255

10.18.0.0 0.0.255.255

مثال غير صحيح:

<#root>

access-list 140 permit ip

any

 10.18.0.0 0.0.255.255

برنامج Cisco IOS®

<#root>

router(config)#

access-list 10 permit ip 192.168.100.0

router(config)#

crypto isakmp client configuration group MYGROUP

router(config-isakmp-group)#

acl 10

ASA من Cisco

<#root>

securityappliance(config)#

access-list 10 standard
permit 192.168.100.0 255.255.255.0

securityappliance(config)#

group-policy MYPOLICY internal

securityappliance(config)#

group-policy MYPOLICY attributes

securityappliance(config-group-policy)#

split-tunnel-policy
tunnelspecified

securityappliance(config-group-policy)#

split-tunnel-network-list
value 10

تكوين إعفاء NAT في الإصدار 8.3 من ASA لنفق VPN من موقع إلى موقع:

يجب إنشاء شبكة خاصة ظاهرية (VPN) من موقع إلى موقع بين HOASA و BOASA مع كل من

ASAs بالإصدار 8.3. وبدء تكوين إستثناء NAT على Hoasa مماثل لهذا:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

التحقق من سياسات ISAKMP

إذا لم يكن نفق IPsec قيد التشغيل، فتحقق من تطابق نهج ISAKMP مع النظراء عن بعد. يتطابق نهج ISAKMP هذا على كل من موقع إلى موقع (L2L) وشبكة VPN الخاصة ب IPsec للوصول عن بعد.

إذا لم يتمكن عملاء Cisco VPN أو الشبكة الخاصة الظاهرية (VPN) من إنشاء النفق باستخدام الجهاز الطرفي البعيد، فتحقق من أن النظيرين يحتويان على قيم معلمات التشفير والتجزئة والمصادقة و Diffie-Hellman نفسها.

تحقق عندما يحدد نهج النظير البعيد فترة بقاء أقل من أو تساوي فترة البقاء في النهج الذي أرسله البادئ.

إذا كانت فترات الحياة غير متطابقة، يستخدم جهاز الأمان العمر الأقصر. في حالة عدم وجود تطابق مقبول، يرفض ISAKMP التفاوض، ولا يتم إنشاء SA.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

فيما يلي رسالة السجل التفصيلية:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

عادة ما تظهر هذه الرسالة بسبب سياسات ISAKMP غير المتطابقة أو جملة NAT 0 مفقودة.

بالإضافة إلى ذلك، تظهر هذه الرسالة:

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
```

```
P1 SA is complete.
```

تشير هذه الرسالة إلى أن رسائل المرحلة 2 موجودة في قائمة الانتظار بعد اكتمال المرحلة 1. ترجع رسالة الخطأ هذه إلى أحد الأسباب التالية:

- عدم التطابق في المرحلة على أي من الأقران
- تمنع قائمة التحكم في الوصول (ACL) النظر من إكمال المرحلة الأولى

عادة ما تأتي هذه الرسالة بعد فشل رسالة الخطأ **Remove peer** من جدول النظير.

إذا تعذر على عميل Cisco VPN توصيل الجهاز الطرفي، يمكن أن تكون المشكلة عدم تطابق سياسة ISAKMP. يجب أن يتطابق الجهاز الطرفي الرئيسي مع أحد اقتراحات IKE الخاصة بعميل Cisco VPN.

بالنسبة لنهج ISAKMP ومجموعة تحويل IPsec التي تم إستخدامها على ASA، الى يمكن لعميل Cisco VPN إستخدام سياسة باستخدام مجموعة من DES و SHA.

إذا كنت تستخدم DES، فأنت بحاجة إلى إستخدام MD5 لخوارزمية التجزئة، أو يمكنك إستخدام التركيبات الأخرى، 3DES مع SHA و 3DES مع MD5.

تحقق من صحة التوجيه

تأكد من أن أجهزة التشفير لديك مثل الموجهات وأجهزة أمان ASA تحتوي على معلومات التوجيه المناسبة لإرسال حركة مرور البيانات عبر نفق VPN الخاص بك.

إذا كانت هناك موجهات أخرى خلف جهاز العبارة الخاص بك، فتأكد من أن هذه الموجهات تعرف كيفية الوصول إلى النفق وما هي الشبكات الموجودة على الجانب الآخر.

يعد إدخال المسار العكسي (RRI) أحد المكونات الأساسية للتوجيه في نشر شبكة VPN.

يضع RRI الإدخالات الديناميكية للشبكات البعيدة أو عملاء VPN في جدول التوجيه لبوابة VPN.

وتكون هذه الموجهات مفيدة للجهاز الذي تم تثبيتها عليه، وكذلك لأجهزة الأخرى في الشبكة لأنه يمكن إعادة توزيع الموجهات التي تم تثبيتها بواسطة RRI من خلال بروتوكول توجيه مثل EIGRP أو OSPF.

في تكوين شبكة LAN إلى شبكة LAN، من المهم أن يكون لكل نقطة نهاية مسار أو مسارات إلى الشبكات التي من المفترض أن تقوم بتشفير حركة المرور لها.

في هذا المثال، يجب أن يحتوي الموجه A على مسارات إلى الشبكات خلف الموجه B من خلال 10.89.129.2. يجب أن يكون للموجه B مسار مماثل إلى 192.168.100.0 /24:

الطريقة الأولى لضمان أن كل موجه يعرف المسار (المسارات) المناسب هي تكوين المسارات الثابتة لكل شبكة وجهة. على سبيل المثال، يمكن أن يتم تكوين عبارات المسار هذه للموجه A:

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

إذا تم إستبدال الموجه A ب ASA، فقد يدي التكوين كما يلي:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

إذا وجد عدد كبير من الشبكات خلف كل نقطة نهاية، يصبح من الصعب الحفاظ على تكوين المسارات الثابتة.

ويدل من ذلك، يوصى باستخدام حقن المسار العكسي، كما هو موضح. يضع RRI مسارات جدول التوجيه لجميع الشبكات البعيدة المدرجة في قائمة التحكم في الوصول (ACL) للتشفير.

على سبيل المثال، يمكن أن تدل قائمة التحكم في الوصول (ACL) المشفرة وخريطة التشفير للموجه A بهذا الشكل:

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

reverse-route

```
 set transform-set mySET
 match address 110
```

إذا تم إستبدال الموجه A ب AH ASA، فقد يدي التكوين كما يلي:

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
```

```
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

crypto map mymap 10 set reverse-route

في تكوين الوصول عن بعد، لا تكون تغييرات التوجيه ضرورية دائما.

ومع ذلك، إذا كانت هناك موجهات أخرى خلف موجه عبارة VPN أو جهاز الأمان، فإن هذه الموجهات تحتاج إلى معرفة المسار إلى عملاء VPN بشكل ما.

في هذا المثال، لنفترض أن عملاء شبكة VPN تم منحهم عناوين في النطاق 10.0.0.0 /24عند إتصالهم.

إذا لم يكن هناك بروتوكول توجيه قيد الاستخدام بين البوابة والموجه (الموجهات) الآخر، يمكن إستخدام المسارات الثابتة على الموجهات مثل الموجه 2:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

إذا كان بروتوكول التوجيه مثل EIGRP أو OSPF قيد الاستخدام بين البوابة والموجهات الأخرى، فمن المستحسن إستخدام حقن المسار العكسي كما هو موضح.

يقوم RRI بإضافة مسارات لعميل الشبكة الخاصة الظاهرية (VPN) إلى جدول التوجيه البوابة. ويمكن بعد ذلك توزيع هذه المسارات على الموجهات الأخرى في الشبكة.

الموجه Cisco IOS®:

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

جهاز الأمان Cisco ASA Security Appliance:

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

crypto dynamic-map dynMAP 10 set reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

يحدث إصدار التوجيه إذا كان تجمع عناوين IP التي تم تعيينها لعملاء VPN متداخل مع الشبكات الداخلية للجهاز الطرفي الرئيسي. لمزيد من المعلومات، راجع قسم الشبكات المتداخلة الخاصة .

تحقق من صحة مجموعة التحويل

تأكد من أن تشفير IPsec وخوارزميات التجزئة التي سيتم إستخدامها من قبل مجموعة التحويل على كلا الطرفين هي نفسها.

راجع مرجع الأوامر دليل تكوين جهاز الأمان من Cisco للحصول على مزيد من المعلومات.

بالنسبة لنهج ISAKMP ومجموعة تحويل IPsec التي يتم إستخدامها على ASA، الكمية لعميل Cisco VPN إستخدام سياسة باستخدام مجموعة من DES و SHA.

إذا كنت تستخدم DES، فأنت بحاجة إلى إستخدام MD5 لخوارزمية التجزئة، أو يمكنك إستخدام التركيبات الأخرى، 3DES مع SHA و 3DES مع MD5.

تحقق من أرقام تسلسل خريطة التشفير والمسم وكذلك من تطبيق خريطة التشفير في الواجهة الكمنى التي يتم فيها بدء/نهاية نفق IPsec

إذا تم تكوين النظراء الثابتة والحركي على خريطة التشفير نفسها، فإن ترتيب إدخالات خريطة التشفير مهم للغاية.

يجب أن يكون الرقم التسلسلي لإدخال خريطة التشفير الديناميكية أعلى من جميع إدخالات خريطة التشفير الثابتة الأخرى.

إذا كانت الإدخالات الثابتة مرقمة أعلى من المدخل الديناميكي، فإن الاتصالات مع الأقران هؤلاء تفشل وتصحيح الأخطاء كما هو موضح ظهر.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

يسمح بخريطة تشفير ديناميكية واحدة فقط لكل واجهة في جهاز الأمان.

هنا مثال على خريطة تشفير مرقمة بشكل صحيح تحتوي على مدخل ثابت ومدخل ديناميكي. لاحظ أن الإدخال الديناميكي يحتوي على أعلى رقم تسلسلي وأنه قد تم ترك الغرفة لإضافة إدخالات ثابتة إضافية:

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
```

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe

أسماء خرائط التشفير حساسة لحالة الأحرف.

يمكن أيضا رؤية رسالة الخطأ هذه عندما يكون تسلسل رجل التشفير الديناميكي غير صحيح مما يتسبب في قيام النظير بالوصول إلى خريطة التشفير الخطأ.

وهذا يرجع أيضا إلى قائمة الوصول إلى التشفير غير المتطابق التي تحدد حركة المرور المثيرة للاهتمام:**%ASA-3-713042: لم يتمكن بادئ IKE من العثور على النهج:**

في سيناريو حيث يتم إنهاء أنفاق VPN متعددة في الواجهة نفسها، قم بإنشاء خريطة تشفير بنفس الاسم (يتم السماح بخريطة تشفير واحدة فقط لكل واجهة) ولكن باستخدام رقم تسلسلي مختلف.

ينطبق هذا على الموجه، و ASA.

وبالمثل، ارجع [إلى ASA: إضافة نفق جديد أو وصول عن بعد إلى شبكة VPN موجودة من الموقع2L -](#) Cisco للحصول على مزيد من المعلومات حول تكوين خريطة التشفير لكل من سيناريو L2L والوصول عن بعد VPN.

التحقق من صحة عنوان IP للنظير

قم بإنشاء قاعدة بيانات السجلات الخاصة بالاتصال ل IPsec وإدارتها.

للحصول على تكوين VPN ل ASA Security Appliance LAN-to-LAN (L2L) IPsec، حدد<name>مجموعة النفق كعنوان IP النظير البعيد (نهاية النفق البعيد) في مجموعة النفق <name> النوع ipSec-l2LCOMMAND.

يجب أن يتطابق عنوان IP النظير مع اسم مجموعة النفق وأوامر عناوين مجموعة خريطة التشفير.

بينما تقوم بتكوين شبكة VPN باستخدام ASDM، فإنها قامت بإنشاء اسم مجموعة النفق تلقائيا باستخدام عنوان IP للنظير الأبعد.

إذا لم يتم تكوين عنوان IP للنظير بشكل صحيح، يمكن أن تحتوي السجلات على هذه الرسالة، والتي يمكن حلها بواسطة التكوين السليم لعنوان IP للنظير.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

عندما لم يتم تكوين عنوان IP للنظير بشكل صحيح على تكوين تشفير ASA، لا يتمكن ASA من إنشاء نفق VPN ويتوقف في المرحلة MM_WAIT_MSG4 فقط.

تحقق in order to حلل هذا إصدار، النظير عنوان في التشكيل.

وفيما يلي إخراج الأمر show crypto isakmp عند تعليق نفق VPN في حالة mm_wait_msg4.

<#root>

hostname#

show crypto isakmp sa

1 IKE Peer: XX.XX.XX.XX
Type : L2L Role : initiator
Rekey : no State : MM_WAIT_MSG4

التحقق من أسماء مجموعة النفق والمجموعة

%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy

تظهر الرسالة عند إسقاط نفق لأن النفق المسموح به المحدد في نهج المجموعة يختلف عن النفق المسموح به في تكوين مجموعة النفق.

<#root>

group-policy hf_group_policy attributes
vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
vpn-tunnel-protocol l2tp-ipsec

Both lines read:

vpn-tunnel-protocol ipsec l2tp-ipsec

تمكين IPSec في نهج المجموعة الافتراضي للبروتوكولات الموجودة بالفعل في نهج المجموعة الافتراضي .

group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol L2TP-IPSec IPSec webvpn

تعطيل مصادقة (Xauth) نظائر L2L

إذا تم تكوين نفق من شبكة LAN إلى شبكة LAN ونفق وصول عن بعد VPN على خريطة التشفير نفسها، يتم مطالبة نظير شبكة LAN إلى شبكة LAN بمعلومات XAUTH، ويفشل نفق شبكة LAN إلى شبكة LAN باستخدام CONF_XAUTH" في إخراج أمر التشفير إلى isakmp هذا.

هنا مثال من ال SA إنتاج:

```
<#root>

Router#

show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

تنطبق هذه المشكلة فقط على Cisco IOS® في حين أن تأثر ASA بهذا الإصدار نظرا لأنه يستخدم مجموعات الأنفاق.

أستخدم theno-xauthkeyword عند إدخال مفتاح isakmp، لذلك ال موقوم الجهاز بمطالبة النظير بمعلومات XAUTH (اسم المستخدم وكلمة المرور).

توقوم هذه الكلمة الأساسية بتعطيل مصادقة (Xauth) نظائر IPsec الثابتة. دخلت أمر مماثل لإ على هذا الأداة أن يتلقى على حد سواء L2L و RA VPN يشكل على النفس تشفير خريطة:

```
<#root>

router(config)#

crypto isakmp key cisco123 address
   172.22.1.164 no-xauth
```

في السيناريو الذي يعمل فيه ASA كخادم Easy VPN، يتعذر على عميل VPN السهل الاتصال بالطرف الرئيسي بسبب مشكلة Xauth.

أعجزت المستعمل صحة هوية في ال ASA in order to حللت الإصدار كما هو موضح:

```
<#root>

ASA(config)#

tunnel-group example-group type ipsec-ra

ASA(config)#
```

```
tunnel-group example-group ipsec-attributes
ASA(config-tunnel-ipsec)#
isakmp ikev1-user-authentication none
```

راجع قسم MiseLaneossection في هذا المستند لمعرفة المزيد حول الأمر item ikev1-user-authentication.

استنفاد تجمع VPN

عندما يكون نطاق عناوين IP التي تم تعيينها إلى تجمع VPN كافياً، يمكنك توسيع نطاق عناوين IP بطريقتين:

1. قم بإزالة النطاق الموجود، ثم حدد النطاق الجديد. فيما يلي مثال:

```
<#root>
CiscoASA(config)#
no ip local pool testvpnpool 10.76.41.1-10.76.41.254
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. عندما تتم إضافة شبكات فرعية غير متتالية إلى تجمع VPN، يمكنك تعريف تجمعات VPN منفصلة ثم تحديدها بالترتيب أسفل "سمات مجموعة النفق". فيما يلي مثال:

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

الترتيب الذي تحدد به التجمعات مهم جدا لأن ASA يخصص العناوين من هذه التجمعات بالترتيب الذي تظهر فيه التجمعات في هذا الأمر.

تتجاوز إعدادات تجمعات العناوين الموجودة في الأمر group-policy address-pools دائما إعدادات التجمع المحلي في الأمر tunnel-group address-pool.

مشاكل بزمن انتقال حركة مرور عميل VPN

عندما تكون هناك مشاكل زمن وصول عبر اتصال VPN، فتحقق من هذه الشروط لحل هذه المشكلة:

1. تحقق ما إذا كان يمكن تقليل MSS للحزمة أكثر.
2. إذا تم إستخدام IPsec/tcp بدلا من IPsec/udp، فعندئذ يتم تكوين VPN-flow .
3. إعادة تحميل Cisco ASA.

يتعذر على عملاء VPN الاتصال ب ASA

المشكلة

يتعذر على عملاء شبكة VPN من Cisco المصادقة عند إستخدام مصادقة X-auth مع خادم RADIUS.

الحل

يمكن أن تكون المشكلة أن xauth times out. قم بزيادة قيمة المهلة لخادم AAA لحل هذه المشكلة.

على سبيل المثال:

```
<#root>

Hostname(config)#

aaa-server test protocol radius


hostname(config-aaa-server-group)#

aaa-server test host 10.2.3.4


hostname(config-aaa-server-host)#

timeout 10
```

المشكلة

يتعذر على عملاء شبكة VPN من Cisco المصادقة عند إستخدام مصادقة X-auth مع خادم RADIUS.

الحل

في البداية، تأكد من عمل المصادقة بشكل صحيح. لتقليص المشكلة، تحقق أولا من المصادقة باستخدام قاعدة البيانات المحلية على ASA.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

إذا نجح هذا بشكل جيد، فحينئذ تكون المشكلة متعلقة بتكوين خادم RADIUS.

تحقق من اتصال خادم Radius من ASA. إذا كان إختبار الاتصال يعمل دون أي مشكلة، فتحقق من التكوين المرتبط ب RADIUS على ASA وتكوين قاعدة البيانات على خادم RADIUS.

يمكنك إستخدام الأمر debug radioCommand لاستكشاف المشاكل المتعلقة بنصف القطر وإصلاحها. للحصول على sampledebug radiusoutput، راجع هذاSample Output.

قبل إستخدام الأمر debugcommand على ASA، ارجع إلى هذه الوثائق:رسالة التحذير.

يقوم عميل شبكة VPN بإسقاط الاتصال بشكل متكرر في المحاولة الأولى أو "إنهاء اتصال شبكة VPN الأمنية بواسطة النظير. السبب 433." أو "إنهاء اتصال VPN الآمن بواسطة النظير)"سبب النظير 433:(السبب غير المحدد بواسطة النظير

المشكلة

يتلقى مستخدم عميل Cisco VPN هذا الخطأ عندما يحاولون الاتصال بجهاز VPN الطرفي الرئيسي.

يقوم عميل شبكة VPN بإسقاط الاتصال بشكل متكرر في المحاولة الأولى

تم إنهاء اتصال VPN للأمان بواسطة النظير. السبب 433.

تم إنهاء اتصال VPN الآمن بواسطة سبب النظير 433:(السبب غير المحدد بواسطة النظير)

تمت محاولة تعيين عنوان IP للشبكة أو البث، لإزالة (x.x.x.x) من التجمع

الحل 1

يمكن أن تكون المشكلة مع تعيين تجمع IP إما من خلال ASA، خادم RADIUS، خادم DHCP أو من خادم RADIUS الذي يعمل كخادم DHCP.

أستخدم الأمر debug cryptocommand للتحقق من صحة قنوات الشبكة وعناوين IP. تحقق أيضا من أن التجمع ال يتضمن عنوان الشبكة وعنوان البث.

يجب أن تكون خوادم RADIUS قادرة على تعيين عناوين IP المناسبة للعملاء.

الحل 2

يقع هذا إصدار أيضا بسبب إخفاق من موسع صحة هوية. يجب التحقق من خادم AAA لاستكشاف أخطاء هذا الخطأ وإصلاحها.

تحقق من كلمة مرور مصادقة الخادم على الخادم والعميل. يمكن أن تحل إعادة تحميل خادم AAA هذه المشكلة.

الحل 3

آخر workaround ل هذا إصدار أن يعجز التهديد كشف سمة.

في بعض الأحيان التي يتم فيها إعادة الإرسال المتعدد لاتجاهات الأمان غير المكتملة (SAs)، يعتقد ASA الذي يتمتع بميزة اكتشاف التهديد أن هجوم مسح ضوئي قد حدث ويتم تمييز منافذ الشبكة الخاصة الظاهرية (VPN) على أنها الجاني الرئيسي.

حاول تعطيل ميزة اكتشاف التهديدات لأن ذلك يمكن أن يتسبب في كثير من التكاليف على معالجة ASA. استعملت هذا أمر in order to أعجزت التهديد كشف:

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

يمكن إستخدام هذا كحل بديل للتحقق مما إذا كان هذا سيقوم بإصلاح المشكلة الفعلية.

تأكد من أن تعطيل اكتشاف التهديد على Cisco ASA يتناقض فعليا مع العديد من ميزات الأمان مثل تخفيف محاولات المسح الضوئي، ورفض الخدمة (DoS) مع SPI غير صالح، والحزم التي تفشل فحص التطبيق، والجلسات غير المكتملة.

الحل 4

تحدث هذه المشكلة أيضا عندما ال يتم تكوين مجموعة توحيل بشكل صحيح. يقوم التكوين المناسب لمجموعة التوحيل بحل المشكلة.

يتصل مستخدمو Remote Access و EZvpn بشبكة VPN لكنهم ال يستطيعون الوصول إلى الموارد الخارجية

المشكلة

ال يتمتع مستخدمو الوصول عن بعد بإمكانية الاتصال بالإنترنت بمجرد اتصالهم بالشبكة الخاصة الظاهرية (VPN).

ال يمكن لمستخدمي الوصول عن بعد الوصول إلى المواد الموجودة خلف شبكات VPN الأخرى على الجهاز نفسه.

يمكن لمستخدمي الوصول عن بعد الوصول إلى الشبكة المحلية فقط.

الحلول

حاولت هذا حل in order to حللت هذا إصدار:

- تعذر الوصول إلى الخوادم في DMZ
- تعذر على عملاء VPN حل DNS
- انقسام النفق—غير قادر على الوصول إلى الإنترنت أو الشبكات المستبعدة
- الوصول إلى شبكة LAN المحلية
- الشبكات الخاصة المتداخلة

تعذر الوصول إلى الخوادم في DMZ

بمجرد إنشاء عميل VPN نفق IPsec مع جهاز الطرف الرئيسي لشبكة VPN (ASA / موجه CISCO IOS®)، يمكن لمستخدمي عميل شبكة VPN الوصول إلى موارد الشبكة الداخلية (10.10.10.0/24)، ولكنهم غير قادرين على الوصول إلى شبكة DMZ (10.1.1.0/24).

الرسم التخطيطي

تحقق من إضافة "نفق التقسيم"، دون تكوين nat في الجهاز الطرفي للوصول إلى الموارد في شبكة DMZ.

مثال:

تكوين ASA:

يبدي هذا تشكيل كيف أن لكل ال NAT إعفاء لشبكة DMZ in order to مكنت ال VPN مستعمل أن ينفذ ال DMZ شبكة:

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

عقب يضيف أنت جديد مدخل ل الـ nat تشكيل، يبرئ الـ nat ترجمة.

```
Clear xlate
Clear local
```

التحقق من الصحة:

إذا تم إنشاء النفق، فانتقل إلى عميل Cisco VPN واخترStatus > تفاصيل المسار للتحقق من أنه يتم عرض المسارات الآمنة لكل من الشبكات الداخلية و DMZ.

ارجع إلى ASA: إضافة نفق جديد أو وصول عن بعد إلى شبكة VPN موجودة L2L - Cisco للحصول على الخطوات المطلوبة إلضافة نفق VPN جديد أو شبكة VPN للوصول عن بعد إلى تكوين L2L VPN موجود بالفعل.

ارجع إلى ASA: السماح بانفاق النقسام لعملاء VPN على مثال تكوين ASA للحصول على تعليمات خطوة بخطوة حول كيفية السماح لعملاء VPN بالوصول إلى الإنترنت أثناء إنشاء قنوات لهم في جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5500.

يتعذر على عملاء VPN حل DNS

بعد إنشاء النفق، إذا تعذر على عملاء VPN حل DNS، يمكن أن تكون المشكلة هي تكوين خادم DNS في جهاز الطرف الرئيسي (ASA).

تحقق أيضا من الاتصال بين عملاء VPN وخادم DNS. يجب تكوين خادم DNS ضمن نهج المجموعة وتطبيقه ضمن نهج المجموعة في السمات العامة لمجموعة النفق؛ على سبيل المثال:

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a


group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com


!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.


tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

يتعذر على عملاء شبكة VPN توصيل الخوادم الداخلية بالاسم

يتعذر على عميل الشبكة الخاصة الظاهرية (VPN) إجراء اتصال المضيفين أو الخوادم

الخاصة بالشبكة الداخلية البعيدة أو شبكة الطرف الرئيسي بالاسم. أنت تحتاج أن يمكن ال split-dns يشكل على ASA in order to حللت هذا إصدار.

انقسام النفق—غير قادر على الوصول إلى الإنترنت أو الشبكات المستبعدة

يتيح تقسيم النفق لعملاء IPsec للوصول عن بعد توجيه الحزم بشروط عبر نفق IPsec فيه نموذج مشفر أو إلى واجهة شبكة في نموذج نص واضح، تم فك تشفيره، حيث يتم توجيههم إلى وجهة نهائية.

يتم تعطيل Split-Tunnel بشكل افتراضي، أي حركة مرور بيانات.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

يتم دعم الخيار المستبعد فقط لعملاء Cisco VPN، وليس عملاء EZvpn.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

ارجع إلى هذه المستندات للحصول على أمثلة التكوين التفصيلية للنفق المقسم:

- ASA: السماح بانفاق الانقسام لعملاء VPN على مثال تكوين ASA
- يسمح الموجه لعملاء VPN بتوصيل IPsec والإنترنت باستخدام مثال تكوين انقسام الاتصال النفقي

محلول مسمار الشعر

هذا سمة مفيد لـ VPN حركة مرور أن يدخل قارن غير أن بعد ذلك وجهت خارج أن القارن نفسه.

على سبيل المثال، في شبكة VPN محورية ومتحدثة، حيث يكون جهاز الأمان هو المحور وتكون شبكات VPN البعيدة فرعية، يجب أن تدخل حركة مرور الاتصال عبر المحادثة إلى جهاز الأمان ثم تخرج مرة أخرى إلى الأخرى التي يتم التحدث بها.

أستخدم تكوين name-security-traffic للسماح لحركة المرور بإدخال الواجهة نفسها والخروج منها.

<#root>

```
securityappliance(config)#
```

same-security-traffic permit intra-interface

الوصول إلى شبكة LAN المحلية

يتصل مستخدمو الوصول عن بعد بالشبكة الخاصة الظاهرية (VPN) وهم قادرون على الاتصال بالشبكة المحلية فقط.

للحصول على مثال تكوين أكثر تفصيلا، ارجع إلى ASA: السماح بوصول شبكة LAN المحلية لعملاء VPN.

الشبكات الخاصة المتداخلة

المشكلة

إذا لم تكن قادرا على الوصول إلى الشبكة الداخلية بعد إنشاء النفق، فتحقق من عنوان IP الذي تم تعيينه لعميل VPN الذي يتداخل مع الشبكة الداخلية خلف جهاز الطرف الرئيسي.

الحل

تحقق من أن عناوين IP في المجموعة التي سيتم تعيينها لعملاء الشبكة الخاصة الظاهرية (VPN) والشبكة الداخلية للجهاز الطرفي الرئيسي والشبكة الداخلية لعميل الشبكة الخاصة الظاهرية (VPN)، موجودة في شبكات مختلفة.

يمكنك تعيين الشبكة الرئيسية نفسها مع شبكات فرعية مختلفة، ولكن في بعض الأحيان تحدث مشاكل التوجيه.

للحصول على مزيد من الأمثلة، راجع DiagramandExample الخاص بعدم القدرة على الوصول إلى الخوادم في قسم DMZ.

يتعذر توصيل أكثر من ثلاثة من مستخدمي عميل شبكة VPN

المشكلة

يمكن لثلاثة عملاء فقط من شبكات VPN الاتصال بـ ASA/؛ يفشل اتصال العميل الرابع. عند الفشل، يتم عرض رسالة الخطأ هذه:

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

الحلول

في معظم الحالات، تتعلق هذه المشكلة بإعداد تسجيل دخول متزامن ضمن نهج المجموعة والحد الأقصى للجلسة.

حاولت هذا حل in order to حللت هذا إصدار:

- تكوين عمليات تسجيل الدخول المتزامنة
- تكوين ASA باستخدام CLI
- التكوين

تكوين عمليات تسجيل الدخول المتزامنة

في حالة تحديد خانة الاختيار Inherirs في ASDM، يتم السماح فقط بالعدد الافتراضي للإدخالات المتزامنة للمستخدم. القيمة الافتراضية لعمليات الإدخال المتزامنة هي ثلاثة (3).

لحل هذه المشكلة، قم بزيادة قيمة عمليات تسجيل الدخول المتزامنة.

1. قم بتشغيل ASDM ثم انتقل إلى التكوين > VPN > نهج المجموعة.
2. أختر منابسبGroupand انقر فوق Editbutton.
3. مرة واحدة في Generaltab، تراجع عن خانة الاختيار Inherirs لإعدادات LogInConnection المتزامنة. أختر قيمة مناسبة في الحقل.

   الحد الأدنى لقيمة هذا الحقل هو صفر (0)، وهو ما يعطل تسجيل الدخول ويمنع وصول المستخدم.

   عندما تقوم بتسجيل الدخول بنفس حساب المستخدم من كمبيوتر مختلف، يتم إنهاء الجلسة الحالية (الاتصال المنشأ من كمبيوتر آخر بنفس حساب المستخدم)، ويتم إنشاء الجلسة الجديدة.

هذا هو السلوك الافتراضي وهو مستقل عن عمليات تسجيل الدخول المتزامنة إلى VPN.

تكوين ASA باستخدام CLI

أكمل هذه الخطوات لتكوين العدد المطلوب من عمليات الدخول المتزامنة. في هذا المثال، تم إختيار 20 (20) كقيمة مرغوب فيها.

```
<#root>

ciscoasa(config)#

group-policy Bryan attributes

ciscoasa(config-group-policy)#

vpn-simultaneous-logins 20
```

لمعرفة المزيد حول هذا الأمر، ارجع إلى مرجع أمر جهاز الأمان من Cisco.

استعملت ال vpn-sessionDB max-session-limitCommand في شامل تشكيل أسلوب in order to حددت VPN جلسة إلى قيمة أقل من أن الأداة أمن يسمح.

أستخدم تجاوز هذا الأمر لإزالة حد جلسة العمل. أستخدم الأمر مرة أخرى من أجل الكتابة فوق الإعداد الحالي.

```
vpn-sessiondb max-session-limit {session-limit}
```

يوضح هذا المثال كيفية تعيين حد أقصى لجلسة VPN يبلغ 450:

<#root>

hostname#

vpn-sessiondb max-session-limit 450

التكوين

رسالة الخطأ

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

الحل

أتمت هذا steps in order to شكلت الرقم المرغوب من دخيل متزامن. أنت يستطيع أيضا حاولت أن يثبت ال login متزامن إلى 5 ل هذا SA:

أختر Configuration > إدارة المستخدم > مجموعات > تعديل 10.19.187.229 > عام > عمليات تسجيل الدخول المتزامنة، وقم بتغيير عدد عمليات تسجيل الدخول إلى5.

تعذر بدء جلسة العمل أو الطلب وبطء النقل بعد إنشاء النفق

المشكلة

بعد إنشاء نفق IPsec، ال يبدأ التطبيق أو جلسة العمل عبر النفق.

الحلول

أستخدم الأمر التالي للتحقق من الشبكة أو البحث عن إمكانية الوصول إلى خادم التطبيق من الشبكة.

هو يستطيع كنت مشكلة مع الأقصى قطعة حجم (MSS) للحزم العابرة أن يجتاز مسحاج وأ /ASA أداة، خصوصا TCP قسم مع ال syn بت مجموعة.

الموجه Cisco IOS®—تغيير قيمة MSS في الواجهة الخارجية (واجهة نهاية النفق) للموجه

قم بتشغيل هذه الأوامر لتغيير قيمة MSS في الواجهة الخارجية (واجهة نهاية النفق) للموجه:

```
<#root>

Router>

enable

Router#

configure terminal

Router(config)#

interface ethernet0/1


Router(config-if)#ip tcp adjust-mss 1300

Router(config-if)#

end
```

تظهر هذه الرسائل إخراج تصحيح الأخطاء ل TCP MSS:

```
<#root>

Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

يتم تعديل MSS إلى 1300 على الموجه كما تم تكوينه.

لمزيد من المعلومات، ارجع إلى ASA و Cisco IOS®: تجزئة VPN.

ASA —ارجع إلى /ASA Documentation

هناك عدم قدرة على الوصول إلى الإنترنت بشكل صحيح أو النقل البطيء عبر النفق لأنه يعطي رسالة خطأ حجم MTU ومشكلات MSS.

أحلت هذا وثيقة in order to حللت الإصدار:

- ASA و Cisco IOS®: تجزئة VPN

يتعذر بدء نفق VPN من ASA

المشكلة

أنت يعجز أن يبدأ ال VPN نفق من ASA قارن، وبعد النفق إنشاء، البعيد نهاية/VPN زبون يعجز أن يمسك القارن داخلي من ASA على ال VPN نفق.

على سبيل المثال، يمكن أن يكون عميل PN غير قادر على بدء اتصال SSH أو HTTP ب ASAs داخل الواجهة عبر نفق VPN.

الحل

ال يمكن قطع الواجهة الداخلية للواجهة من الطرف الآخر من النفق ما لم يتم تكوين الأمرidentity-access في وضع التكوين العام.

```
<#root>

ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

كما يساعد هذا الأمر في بدء SSH أو اتصال HTTP بالواجهة الداخلية ل ASA من خلال نفق VPN.

تنطبق هذه المعلومات على واجهة DMZ أيضا. على سبيل المثال، إذا كنت ترغب في إختبار اتصال واجهة DMZ ل /ASA أو ترى بدء نفق من واجهة DMZ، فيلزمك أمر Management-access DMZ.

```
<#root>
```

ASA-02(config)#

management-access DMZ

إذا لم يتمكن عميل شبكة VPN من الاتصال، فتأكد من فتح منافذ ESP و UDP.

ومع ذلك، إذا لم تكن هذه المنافذ مفتوحة، فحاول الاتصال على TCP 10000 بتحديد هذا المنفذ ضمن إدخال اتصال عميل شبكة VPN.

انقر بزر الماوس الأيمن فوق تعديل > علامة التبويب النقل > IPsec عبر TCP.

يتعذر تمرير حركة مرور البيانات عبر نفق VPN

المشكلة

أنت عاجز أن يمرر حركة مرور عبر VPN نفق.

الحل

كما يمكن أن تحدث هذه المشكلة عند حظر حزم ESP. in order to حللت هذا إصدار، أعدت ال VPN نفق.

يمكن أن تحدث هذه المشكلة عندما لا يتم تشفير البيانات، ولكن يتم فك تشفيرها فقط عبر نفق VPN كما هو موضح في هذا الإخراج:

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y


 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0
```

in order to حللت هذا إصدار، فحص هذا شرط:

1. إذا كانت قوائم الوصول إلى التشفير متطابقة مع الموقع البعيد، وكانت قوائم الوصول إلى NAT 0 صحيحة.

2. إذا كان التوجيه صحيحا وكانت حركة المرور تصل إلى الواجهة الخارجية التي تمر من الداخل. تظهر مخرجات النموذج أن فك التشفير تم، لكن التشفير لا يحدث.

3. إذا تم تكوين الأمر allowed allowed allowed allowed connection-vpn على ASA. إذا لم يتم تكوين هذا الأمر، فقم بتكوين هذا الأمر لأنه يسمح لـ ASA بإعفاء حركة مرور البيانات المشفرة/VPN من فحص قائمة التحكم في الوصول (ACL) للواجهة.

تكوين نظير النسخ الاحتياطي لنفق VPN على خريطة التشفير نفسها

المشكلة

تريد إستخدام العديد من نظائر النسخ الاحتياطي لنفق شبكة خاصة ظاهرية (VPN) واحد.

الحل

تكوين العديد من الأقران متوفير قائمة إحتياطية. يحاول جهاز الأمان التفاوض مع النظير الأول في القائمة لكل نفق.

وإذا لم يستجب ذلك النظير، فإن جهاز الأمان يعمل على خفض القائمة إلى أن يستجيب أي نظير أو ال يوجد المزيد من النظراء في القائمة.

يحتوي ASA على خريطة تشفير تم تكوينها بالفعل كنظير أساسي. ويمكن إضافة النظير الثانوي بعد النظير الأساسي.

يوضح مثال التكوين هذا النظير الأساسي كـ X.X.X.X والنظير الاحتياطي كـ Y.Y.Y.Y:

```
<#root>

ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

تعطيل/إعادة تشغيل نفق VPN

المشكلة

من أجل تعطيل نفق VPN أو إعادة تشغيل الخدمة، أكمل الإجراء الموضح في هذا القسم.

الحل

أستخدم الأمر thecypto map interfaceCommand في وضع التكوين العام لإزالة مجموعة خريطة تشفير معرفة مسبقا إلى واجهة.

أستخدم الصيغة اللونية لهذا الأمر لإزالة مجموعة خريطة التشفير من الواجهة.

<#root>

```
hostname(config)#

no crypto map

 map-name

interface

 interface-name
```

قفن لعجيو ةطشن نامأ زاهج ةهجاو يأ ىلع اهنييعت مت ريفشت ةطيرخ ةلازإب رمألا اذه موقي IPsec VPN ريغ طشن يف هذه الواجهة.

لإعادة تشغيل نفق IPsec على واجهة، يجب تعيين تعيين خريطة تشفير إلى واجهة قبل أن تتمكن هذه الواجهة من توفير خدمات IPsec.

<#root>

```
hostname(config)#

crypto map

 map-name

interface

 interface-name
```

بعض الأنفاق غير مشفرة

المشكلة

عند تكوين عدد كبير من الأنفاق على بوابة الشبكة الخاصة الظاهرية (VPN)، ال موقت بعض الأنفاق بتمرير حركة المرور. ال يتلقى ال ASA حزم مشفرة لتلك الأنفاق.

الحل

يقع هذا إصدار لأن ال ASA يفشل أن يرمي الربط يشفر من خلال الأنفاق. يتم إنشاء قواعد تشفير مكررة في جدول ASP.

خطأ:- %ASA-5-713904: المجموعة = DefaultRAGgroup، IP = x.x.x.x، ... تم إنهاء وضع المعاملة غير المعتمد v2 version.Tunnel.

المشكلة

تظهر رسالة إنهاء Error الخاصة ب%ASA-5-713904: Group = DefaultRAGgroup، IP = 192.0.2.0،... Non-Transaction Mode v2 version.Tunnel.

الحل

سبب رسالة الخطأ Transaction Mode v2 هو أن ASA يدعم وضع IKE Config V6 فقط والى يدعم إصدار وضع V2 القديم.

أستخدم إصدار IKE Mode Config V6 لحل هذا الخطأ.

خطأ:- %ASA-6-722036: مستخدم مجموعة عملاء المجموعة xxxx IP x.x.x.x يرسل الحزمة الكبيرة 1220 (الحد 1206)

المشكلة

تظهر رسالة الخطأ %ASA-6-722036: مجموعة </client-group>مستخدم < xxx > IP </x.x.x> التي ترسل حزمة كبيرة 1220 (الحد 1206) في سجلات ASA.

اذا يعني هذا السجل وكيف يمكن حل ذلك؟

الحل

تشير رسالة السجل هذه إلى أنه تم إرسال حزمة كبيرة إلى العميل. مصدر الحزمة ليس على دراية بحد MTU الخاص بالعميل.

قد يرجع ذلك أيضاً إلى ضغط البيانات غير القابلة للضغط. ال workaround أن يلتفت باتجاه إيقاف ضغط SVC مع طغض اذه غير أمر، أي يحل الإصدار.

رسالة خطأ عند تمكين جودة الخدمة في نهاية واحدة من نفق VPN

المشكلة

إذا قمت بتمكين جودة الخدمة في أحد طرفي نفق VPN، فيمكنك تلقي رسالة الخطأ هذه:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

الحل

وعادة ما يتم إرسال هذه الرسالة عندما يقوم أحد طرفي النفق بتنفيذ جودة الخدمة. يحدث ذلك عندما يتم اكتشاف حزمة غير مرتبة.

يمكنك تعطيل جودة الخدمة لإيقاف هذا الإجراء ولكن يمكن تجاهلها طالما أن حركة المرور قادرة على إجتياز النفق.

تحذير: إدخال خريطة التشفير غير مكتمل

المشكلة

عند تشغيل الأمرthecrypto map 20 ipSec-isakmpcommand، يمكنك تلقي هذا الخطأ:

```
تحذير: إدخال خريطة التشفير غير مكتمل
```

على سبيل المثال:

<#root>

```
ciscoasa(config)#
crypto map mymap 20 ipsec-isakmp
WARNING: crypto map entry incomplete
```

الحل

هذا تنبيه عادي عند تعريف خريطة تشفير جديدة؛ تذكير بأن المعلمات مثل قائمة الوصول (عنوان المطابقة) ومجموعة التحويل وعنوان النظير يجب تكوينها قبل أن تعمل.

من الطبيعي أيضا أن ال يظهر السطر الأول الذي تكتبه من أجل تحديد خريطة التشفير في التكوين.

خطأ:- %ASA-4-400024: IDS:2151 حزمة ICMP كبيرة من الواجهة إلى عليها في الخارج

المشكلة

يتعذر تمرير حزمة إختبار الاتصال الكبيرة عبر نفق VPN. عند محاولة تمرير حزم إختبار الاتصال الكبيرة، نحصل على الخطأ`%ASA-4-400024: المعرفات:2151 حزمة ICMP كبيرة من الواجهة إلى الخارج.`

الحل

قم بتعطيل التوقيعات 2150 و 2151 لحل هذه المشكلة.بمجرد تعطيل التوقيعات، يعمل ping بشكل صحيح.

استعمل هذا أمر in order to أعجز التوقيعات:

ASA(config)#ip تدقيق توقيع 2151 disable

ASA(config)#ip تدقيق توقيع 2150 يعجز

خطأ:- ٪ASA-4-402119: IPSec: استلم حزمة بروتوكول (SPI=SPI، الرقم التسلسلي= seq_num) من remote_ip (username) إلى local_ip التي فشلت في فحص مكافحة إعادة التشغيل.

المشكلة

إستلمت هذا خطأ في السجل رسالة من ال ASA:

خطأ:- ٪ASA-4-402119: IPSec: استلم حزمة بروتوكول (SPI=SPI، الرقم التسلسلي= seq_num) من remote_ip (username) إلى local_ip التي فشلت في فحص مكافحة إعادة التشغيل.

الحل

لحل هذا الخطأ، أستخدم الأمر Cisco IPsec Security-association replay window-size لتغيير حجم النافذة.

<#root>

hostname(config)#

crypto ipsec security-association replay window-size 1024

cisco يوصي أن يستعمل أنت ال 1024 نافذة حجم كامل أن يزيل أي مشكلة ضد إعادة التشغيل.

رسالة خطأ - ٪ASA-4-407001: رفض حركة مرور بيانات المضيف المحلي interface_name:inside_address، تجاوز حد الترخيص للعدد

المشكلة

ال يستطيع عدد قليل من البيئات المضيفة الاتصال بالإنترنت، وتظهر رسالة الخطأ هذه في syslog:

رسالة خطأ - ٪ASA-4-407001: رفض حركة مرور بيانات المضيف المحلي interface_name:inside_address، تجاوز حد الترخيص للعدد

الحل

يتم تلقي رسالة الخطأ هذه عندما يتجاوز عدد المستخدمين حد المستخدم للترخيص المستخدم. يمكن حل هذا الخطأ عن طريق ترقية الترخيص إلى عدد أكبر من المستخدمين.

يمكن أن يتضمن ترخيص المستخدم 50 وأ 100 وأ مستخدمين غير محدودين حسب الطلب.

رسالة خطأ - ٪VPN_HW-4-PACKET_ERROR:

المشكلة

تشير رسالة أخطاء - ٪VPN_HW-4-PACKET_ERROR:رسالة الخطأ إلى عدم تطابق حزمة ESP مع HMAC التي تم استقبالها بواسطة الموجه. يمكن أن يتسبب هذه الخطأ في هذه المشاكل:

- الوحدة النمطية VPN H/W المعيبة
- حزمة ESP تالفة

الحل

in order to حلل هذه خطأ رسالة:

- تجاهل رسائل الخطأ ما لم يكن هناك مقاطعة لحركة المرور.
- إذا كان هناك انقطاع في حركة المرور، فاستبدل الوحدة النمطية.

رسالة خطأ: رفض الأمر: حذف اتصال التشفير بين VLAN xxxx و xxxx، الأول.

المشكلة

تظهر رسالة الخطأ هذه عندما تحاول إضافة شبكة VLAN مسموح بها على منفذ خط الاتصال.. الأول، VLAN XXXX و VLAN XXXX بين تشفير اتصال حذف :رمز الأمر مرفوض:على محول

لا يمكن تعديل خط اتصال حافة WAN للسماح بشبكات VLAN إضافية. لذلك، لا يمكن إضافة شبكات VLAN في خط اتصال SPAIPsec VPN.

يتم رفض هذا الأمر لأنه ينتج عنه شبكة VLAN أولوية متصلة بتشفير تنتمي إلى قائمة VLAN المسموح بها، والتي تشكل خرقاً أمان IPSec المحتمل.

لاحظ أن هذا السلوك ينطبق على جميع منافذ خطوط الاتصال.

الحل

من الأمر switchport trunk allowed vlan (vlanlist)، أستخدم الأمر switchport trunk allowed vlan noCommand أو الأمر"switchport trunk allowed vlan remove (vlanlist)".

رسالة خطأ - ٪ FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: الحزمة المقسطة - خيار مقياس النافذة غير صالح لجلسة

x.x.x.x:27331 إلى x.x.x:23 [Initiator(Flag 0،Factor 0) Responder (Flag 1، Factor 2)]

المشكلة

يحدث هذا الخطأ عندما تحاول إستخدام Telnet من جهاز على الطرف البعيد من نفق VPN وأو عندما تحاول إستخدام Telnet من الموجه نفسه:

رسالة خطأ - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: الحزمة المسقطة - خيار مقياس نافذة غير صالح لجلسة x.x.x.x:27331 إلى x.x.x:23 [Initiator(Flag 0،Factor 0) Responder (Flag 1، Factor 2)]

الحل

يمكن أن يتضمن ترخيص المستخدم 50 أو 100 أو مستخدمين غير محدودين حسب الطلب. تمت إضافة وظيفة نطاق النافذة للسماح بالانتقال السريع للبيانات على شبكات الدهون الطويلة (LFN).

هذه هي الوصلات ذات عرض نطاق ترددي عال جدا، لكن أيضا زمن وصول مرتفع.

وتعد الشبكات ذات الاتصالات الساتلية مثالا واحدا على شبكة LFN، نظرا لأن الارتباطات الساتلية تحدث دائما تأخيرات كبيرة في النشر ولكن عادة ما تكون ذات نطاق ترددي عريض مرتفع.

لتمكين وظيفة نطاق النافذة لدعم شبكات LFN، يجب أن يكون حجم نافذة TCP أكثر من 65.535. يمكن حل رسالة الخطأ هذه إذا قمت بزيادة حجم نافذة TCP ليصبح أكثر من 65.535.

%ASA-5-305013: قواعد NAT غير المتماثلة متطابقة للإرسال والعكس . الرجاء تحديث تدفقات هذه المشكلة

المشكلة

تظهر رسالة الخطأ هذه بمجرد ظهور نفق VPN:

%ASA-5-305013: قواعد NAT غير المتماثلة متطابقة للإرسال والعكس . الرجاء تحديث تدفقات هذه المشكلة

الحل

in order to حللت هذه إصدار عندما ليس على الجهاز نفسه قارن بما أن المضيف مع NAT، استعملت العنوان خطط بدل من العنوان حقيقي أن يربط إلى المضيف.

بالإضافة إلى ذلك، قم بتمكين الأمرinspection إذا كان التطبيق يدمج عنوان IP.

%ASA-5-713068: تم إستلام رسالة إعلام غير روتينية: notify_type

المشكلة

تظهر رسالة الخطأ هذه إذا فشل نفق VPN في الارتفاع:

%ASA-5-713068: تم إستلام رسالة إعلام غير متوقعة: notify_type

الحل

تحدث هذه الرسالة بسبب التكوين الخاطئ (أي عندما لا يتم تكوين السياسات أو قوائم التحكم في الوصول لتكون نفسها على الأقران).

بمجرد مطابقة السياسات وقوائم التحكم في الوصول (ACL)، يأتي النفق دون أي مشكلة.

%ASA-5-720012: (VPN-Secondary) فشل تحديث بيانات وقت تشغيل زواج فشل IPSec على الوحدة الاحتياطية (أو) %ASA-6-720012: (وحدة VPN) فشل تحديث بيانات وقت تشغيل زواج فشل IPsec على الوحدة الاحتياطية

المشكلة

تظهر إحدى رسائل الخطأ التالية عند محاولة ترقية جهاز الأمان القابل للتكيف (ASA) من Cisco:

%ASA-5-720012: (VPN-Secondary) فشل تحديث بيانات وقت تشغيل زواج فشل IPSec على الوحدة الاحتياطية.

%ASA-6-720012: (وحدة VPN) فشل تحديث بيانات وقت تشغيل زواج فشل IPsec على الوحدة الاحتياطية.

الحل

رسائل الخطأ هذه هي أخطاء إعلامية. لا تؤثر الرسائل على وظيفة ASA أو VPN.

تظهر هذه الرسائل عندما يتعذر على النظام الفرعي الخاص بتجاوز فشل الشبكة الخاصة الظاهرية (VPN) تحديث بيانات وقت التشغيل ذات الصلة بـ IPsec بسبب حذف نفق IPsec ذي الصلة على الوحدة الاحتياطية.

لحل هذه المشاكل، قم بإصدار الأمر standbycommand على الوحدة النشطة.

خطأ:- %ASA-3-713063: لم يتم تكوين عنوان نظير IKE للوجهة 0.0.0.0

المشكلة

تظهر رسالة الخطأ **%ASA-3-713063: لم يتم تكوين عنوان نظير IKE لوجهة 0.0.0.0** وفشل النفق في الظهور.

الحل

تظهر هذه الرسالة عندما يتم تكوين عنوان نظير IKE لنفق L2L.

يمكن حل هذا الخطأ إذا قمت بتغيير الرقم التسلسلي لخريطة التشفير، ثم قمت بإزالة خريطة التشفير وإعادة تطبيقها.

خطأ: %ASA-3-752006: فشلت إدارة النفق في إرسال رسالة KEY_ACQUIRE.

المشكلة

The%ASA-3-752006: Tunnel Manager فشل في إرسال رسالة KEY_ACQUIRE.Likely mis-configuration الخاصة بخريطة التشفير أو مجموعة النفق. تم تسجيل رسالة الخطأ على Cisco ASA.

الحل

يمكن أن تحدث رسالة الخطأ هذه بسبب تكوين غير صحيح لخريطة التشفير أو مجموعة النفق. تأكد من تكوين كليهما بشكل صحيح. للحصول على مزيد من المعلومات حول رسالة الخطأ هذه، ارجع إلى Error 752006 .

وإليكم بعض الاجراءات التصحيحية:

- قم بإزالة قائمة التحكم في الوصول (ACL) للتشفير (على سبيل المثال، مرتبط بالخريطة الديناميكية).
- قم بإزالة التكوين المرتبط IKEv2 غير المستخدم، إن وجد.
- تحقق من مطابقة قائمة التحكم في الوصول (ACL) للتشفير بشكل صحيح.
- قم بإزالة إدخالات قائمة الوصول المكررة، إن وجدت.

خطأ: %ASA-4-402116: IPSec: تم تلقي حزمة ESP (SPI= 0x99554D4E، الرقم التسلسلي= 0x9E) من XX.XX.XX.XX (user= XX.XX.XX.XX) إلى YY.YY.YY.YY

في إعداد نفق VPN من شبكة LAN إلى شبكة LAN، يتم إستلام هذا الخطأ على ASA أحادي الطرف:

لا تتطابق الحزمة الداخلية المعطلة مع سياسة التفاوض في SA.

تحدد الحزمة وجهة على أنها 10.32.77.67، ومصدرها على شبكة 10.105.30.1، وبروتوكول على شبكة IP/0.

تحدد SA الوكيل المحلي الخاص بها على أنه 10.32.77.67/255.255.255.255/ip/0 و remote_proxy الخاص بها على أنه 10.105.42.192/255.255.255.224/ip/0.

الحل

أنت تحتاج أن تدقق الحركة مرور مهم منفذ قائمة ميالن إلى جانب يعين على كل نهاية من ال VPN نفق. يجب أن تتطابق كل منهما مع صورة متطابقة.

فشل تشغيل مثبت VA 64 بت لتمكين المحول الظاهري بسبب الخطأ 0xffffffff

المشكلة

فشل TheFailed في تشغيل مثبت VA 64-بت لتمكين المحول الظاهري بسبب خطأ 0xffffffflog يتم تلقي رسالة عندما يفشل AnyConnect في الاتصال.

الحل

أتمت هذا steps in order to حلل هذا إصدار:

1. انتقل إلى النظام > إدارة إتصالات الإنترنت > إعدادات إتصالات الإنترنت وتأكد من إيقاف تشغيل شهادات الجذر التلقائية المحدثة معطلة.
2. في حالة تعطيله، قم بتعطيل TemplatePart Administrative بالكامل من GPO المعين إلى الجهاز المتأثر ثم أعد الاختبار.

راجع إيقاف تشغيل تحديث شهادات الجذر التلقائية للحصول على مزيد من المعلومات.

عميل Cisco VPN لا يعمل مع بطاقة البيانات على Windows 7

المشكلة

لا يعمل عميل شبكة VPN من Cisco مع بطاقة البيانات على Windows 7.

الحل

لا يعمل عميل شبكة VPN من Cisco المثبت على نظام التشغيل Windows 7 مع إتصالات الجيل الثالث نظرا لأن بطاقات البيانات غير مدعومة على عملاء شبكات VPN المثبتة على جهاز يعمل بنظام التشغيل Windows 7.

تنبيه: "قد لا تعمل وظيفة الشبكة الخاصة الظاهرية (VPN) على الإطلاق"

المشكلة

أثناء محاولات تمكين isakmp على الواجهة الخارجية ل ASA، يتم تلقي رسالة التنبيه هذه:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

عند هذه النقطة، يمكن الوصول إلى ASA من خلال SSH. يتم إيقاف HTTPS كما يتأثر عمل SSL الآخرون.

الحل

ترجع هذه المشكلة إلى متطلبات الذاكرة من قبل وحدات مختلفة مثل المسجل والتشفير.

تأكد من عدم وجود الأمر Logging queue 0. يخلي حجم قائمة الانتظار ينضبط على 8192 وتزيد عمليات تخصيص الذاكرة.

في الأنظمة الأساسية مثل ASA5510، ASA5505 و ASA5505، يميل تخصيص الذاكرة هذه إلى حرمان وحدات أخرى من الذاكرة.

خطأ في إضافة IPSec

المشكلة

تم تلقي رسالة الخطأ هذه:

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

الحل

يقع الإصدار لأن IPSec VPN يفاوض دون خوارزمية تجزئة. تضمن تجزئة الحزمة التحقق من التكامل لقناة ESP.

لذلك، دون تجزئة، يتم قبول الحزم التي تم تكوينها بشكل غير صحيح دون اكتشاف بواسطة Cisco ASA ويحاول فك تشفير هذه الحزم.

مع ذلك، لأن هذه الحزم تم تكوينها بشكل غير صحيح، يجد ASA الأخطاء أثناء فك تشفير الحزمة. هذا يسبب الحشو رسالة خطأ أن يكون رأيت.

التوصية هي تضمين خوارزمية تجزئة في مجموعة التحويل الخاصة بالشبكة الخاصة الظاهرية (VPN) وضمان أن الارتباط بين الأقران يحتوي على الحد الأدنى من تشويه الحزمة.

يتم قطع اتصال نفق VPN بعد 18 ساعة

المشكلة

يتم قطع اتصال نفق الشبكة الخاصة الظاهرية (VPN) بعد كل 18 ساعة على الرغم من تعيين العمر الافتراضي على 24 ساعة.

الحل

مدة البقاء هي الحد الأقصى للوقت الذي يمكن فيه إستخدام SA للمفاتيح. القيمة التي أدخلتها في التكوين لأن العمر الافتراضي يختلف عن وقت المفاتيح ل SA.

لذلك، من الضروري التفاوض على زوج SA جديد (أو زوج SA في حالة IPsec) قبل انتهاء صلاحية الزوج الحالي.

يجب أن يكون وقت المفاتيح دائما أصغر من العمر للسماح لمحاولات متعددة في حالة فشل محاولة إعادة المفاتيح الأولى.

ال تحدد وحدات RFC كيفية حساب وقت إعادة التخزين. ويترك ذلك لتقدير المنفذين.

لذلك، يختلف الوقت حسب النظام الأساسي. يمكن لبعض عمليات التنفيذ إستخدام عامل عشوائي لحساب موقت rekey.

على سبيل المثال، إذا قام ASA بتهيئة النفق، ثم من الطبيعي أنه يبقى في 64800 ثاني = 75٪ من 86400.

إذا قام الموجه بالبدء، فيمكن حينئذ ل ASA الانتظار لمدة أطول لمنح النظير وقتا أطول لبدء المفاتيح.

لذلك، من الطبيعي قطع اتصال جلسة عمل الشبكة الخاصة الظاهرية (VPN) كل 18 ساعة (VPN). يجب أن يتسبب هذا في استخدام مفاتيح آخر للتفاوض على الشبكة الخاصة الظاهرية (VPN) في أي إسقاط لشبكة VPN أو مشكلة.

ال يتم الحفاظ على تدفق حركة المرور بعد إعادة التفاوض على نفق LAN إلى LAN

المشكلة

ال يتم الحفاظ على تدفق حركة المرور بعد إعادة التفاوض على نفق LAN إلى LAN.

الحل

يراقب ASA كل اتصال يمر خلاله ويحتفظ بإدخال في جدول حالته وفقا لميزة فحص التطبيق.

يتم الاحتفاظ بتفاصيل حركة المرور المشفرة التي تمر عبر شبكة VPN في شكل قاعدة بيانات اقتران الأمان (SA). بالنسبة لاتصالات LAN إلى LAN VPN، يحافظ على تدفقات حركة مرور مختلفة.

الأول هو حركة المرور المشفرة بين بوابات الشبكة الخاصة الظاهرية (VPN). والآخر هو تدفق حركة المرور بين مورد الشبكة خلف بوابة VPN والمستخدم النهائي خلف الطرف الآخر.

عندما يتم إنهاء شبكة VPN، يتم حذف تفاصيل التدفق الخاصة ب SA هذا المعين.

وعم ذلك، يصبح إدخال جدول الحالة الذي يتم الاحتفاظ به من قبل ASA لاتصال TCP هذا جامدا بسبب عدم وجود نشاط، مما يعيق التنزيل.

هذا يعني أن ASA ال يزال يحتفظ باتصال TCP لذلك التدفق المعين بينما ينتهي تطبيق المستخدم.

وعم ذلك، تصبح إتصالات TCP شاردة وفي نهاية المطاف مهلة بعد انتهاء صلاحية المؤقت الخامل ل TCP.

تم حل هذه المشكلة باستخدام إدخال ميزة تسمى التدفقات النفقي الثابتة ل IPSec.

تم دمج أمر جديد، اتصال sysopt المحافظة على تدفقات VPN، في Cisco ASA من أجل الاحتفاظ بمعلومات جدول الحالة في إعادة التوافق على نفق VPN.

بشكل افتراضي، يتم تعطيل هذا الأمر. لتمكين هذا، يحتفظ Cisco ASA بمعلومات جدول حالة TCP عند إستدراد L2L VPN من التعطيل وإعادة إنشاء النفق.

تشير رسالة الخطأ إلى أن النطاق الترددي تم الوصول إليه لوظيفة التشفير

المشكلة

يتم تلقي رسالة الخطأ هذه على موجه السلسلة 2900:

```
خطأ: تم الوصول إلى الحد الأقصى لعرض نطاق ترددي لـ Tx والذي يبلغ 85000 كيلوبت/ثانية لوظيفة التشفير
CERM-4-TX_BW_LIMIT: تم الوصول إلى الحد الأقصى لنطاق SecurityYk9 في ترخيص حزمة تقنية باستخدام
Tx والذي يبلغ 85000 كيلوبت/ثانية.
```

الحل

هذه قضية معروفة تحدث بسبب التعليمات الصارمة التي أصدرتها حكومة الولايات المتحدة.

وفقا لذلك، يمكن أن يسمح ترخيص securityK9 بتشفير الحمولة حتى معدلات تصل إلى 90 ميجابت في الثانية ويحد من عدد الأنفاق المشفرة/جلسات عمل TLS على الجهاز.

لمزيد من المعلومات حول قيود تصدير التشفير، ارجع إلى ترخيص Cisco ISR G2 SEC و HSEC.

في حالة أجهزة Cisco، يتم اشتقاقها لتكون أقل من حركة مرور أحادية الإتجاه بسرعة 85 ميجابت في الثانية أو خارج الموجه ISR G2، مع إجمالي ثنائي الإتجاه بسرعة 170 ميجابت في الثانية.

ينطبق هذا المتطلب على الأنظمة الأساسية ISR G2 1900 و 2900 و 3900 من Cisco. يساعد هذا الأمر في عرض هذه القيود:

```
<#root>

Router#

show platform cerm-information

Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)          85000                  85000
 Rx Bandwidth(in kbps)          85000                  85000
 Number of tunnels                225                    225
 Number of TLS sessions          1000                   1000
---Output truncated----
```

لتجنب هذه المشكلة، قم بشراء ترخيص HSECK9. يوفر ترخيص الميزات "hseck9" وظيفة تشفير الحمولة المحسنة مع زيادة عدد فتحات VPN النفقية وجلسات الصوت الآمنة.

لمزيد من المعلومات حول ترخيص موجه Cisco ISR، ارجع إلى تنشيط البرامج.

مشكلة: فشل حركة مرور التشفير الصادر في نفق IPsec، حتى إذا كانت حركة مرور فك التشفير الواردة تعمل.

الحل

تمت مالحظة هذه المشكلة على اتصال IPsec بعد عدة قرائن، ولكن شرط المشغل غير واضح.

يمكن إنشاء وجود هذه المشكلة إذا قمت بالتحقق من إخراج الأمر show asp drop والتحقق من زيادة عداد سياق VPN الذي انتهت صالحيته لكل حزمة صادرة مرسلة.

منوعات

تظهر رسالة AG_INIT_EXCH في إخراج الأوامر "show crypto isakmp sa" و"debug"

إذا لم يتم بدء النفق، تظهر رسالة **AG_INIT**_EXCHmessage في إخراج الأمر show crypto isakmp command وindebugoutput أيضا.

السبب يستطيع كنت بسبب حالة عدم توافق من isakmp سياسة أو إن ميناء UDP 500 يحصل حجبت على الطريق.

تظهر رسالة تصحيح الأخطاء "تلقت رسالة IPC أثناء حالة غير صحيحة"

هذه الرسالة هي رسالة إعلامية وليس لها أي عالقة بانقطاع نفق VPN.

معلومات ذات صلة

- ASA و Cisco IOS®: تجزئة VPN

- أجهزة الأمان Cisco ASA 5500 Series Security Appliances
- مفاوضة IPSec/بروتوكولات IKE
- 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).