دليل أستكشاف أخطاء GetVPN وإصلاحها

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
منهجية أستكشاف أخطاء GetVPN وإصلاحها
طوبولوجيا مرجعية
التكوينات المرجعية
مصطلحات
إعداد مرافق التسجيل وأفضل الممارسات الأخرى
أستكشاف أخطاء مستوى التحكم في GETVPN وإصلاحها
أفضل ممارسات تصحيح أخطاء مستوى التحكم
أدوات أستكشاف أخطاء مستوى التحكم وإصلاحها في GetVPN
أوامر عرض GetVPN
رسائل GetVPN Syslog
التشفير العام وتصحيح أخطاء GDOI
تصحيح الأخطاء الشرطي ل GDOI
آثار حدث GDOI
نقاط التفتيش على مستوى التحكم في GetVPN والمشاكل الشائعة
إعداد COOP وإنشاء السياسة
إعداد IKE
التسجيل، تنزيل النهج، وتثبيت SA
ريكي
التحقق من ترحيل مستوى التحكم
مشاكل تجزئة حزمة مستوى التحكم
مشكلات قابلية التشغيل البيني ل GDOI
أستكشاف أخطاء مستوى بيانات GETVPN وإصلاحها
أدوات أستكشاف أخطاء مستوى بيانات GetVPN وإصلاحها
عدادات التشفير/فك التشفير
Netflow
تمييز أسبقية DSCP/IP
التقاط حزمة مضمنة
تتبع حزمة IOS-XE من Cisco
المشاكل الشائعة لمستوى بيانات GetVPN
مشاكل مستوى بيانات IPsec العامة
مشكلات معروفة
أستكشاف أخطاء GETVPN وإصلاحها على الأنظمة الأساسية التي تعمل بنظام التشغيل Cisco IOS-XE
أوامر استكشاف الأخطاء وإصلاحها
القضايا المشتركة ل ASR1000
فشل تثبيت نهج IPsec (إعادة التسجيل المستمرة)

مشكلات شائعة تتعلق بالترحيل/الترقية
تحديد شريط ASR1000
مسألة تصنيف ISR4x00
معلومات ذات صلة

المقدمة

هذا وثيقة أن يقدم هيكل تحريري منهجية و أداة مفيد أن يساعد عينت وعزلت مجموعة يشفر نفق VPN (GETVPN) مشكلة وأن يوزي حل ممكن.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Getvpn
  دليل تكوين GETVPN الرسمي
  الدليل الرسمي لتصميم GETVPN وتنفيذه

- إستخدام خادم Syslog

المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

منهجية أستكشاف أخطاء GetVPN وإصلاحها

كما هو الحال مع معظم أستكشاف أخطاء التقنية المعقدة وإصلاحها، فإن المفتاح هو أن يكون قادرا على عزل المشكلة لميزة أو ظاهر فرعي أو مكون معين. يتكون حل GETVPN من عدد من مكونات الميزات، وعلى وجه التحديد:

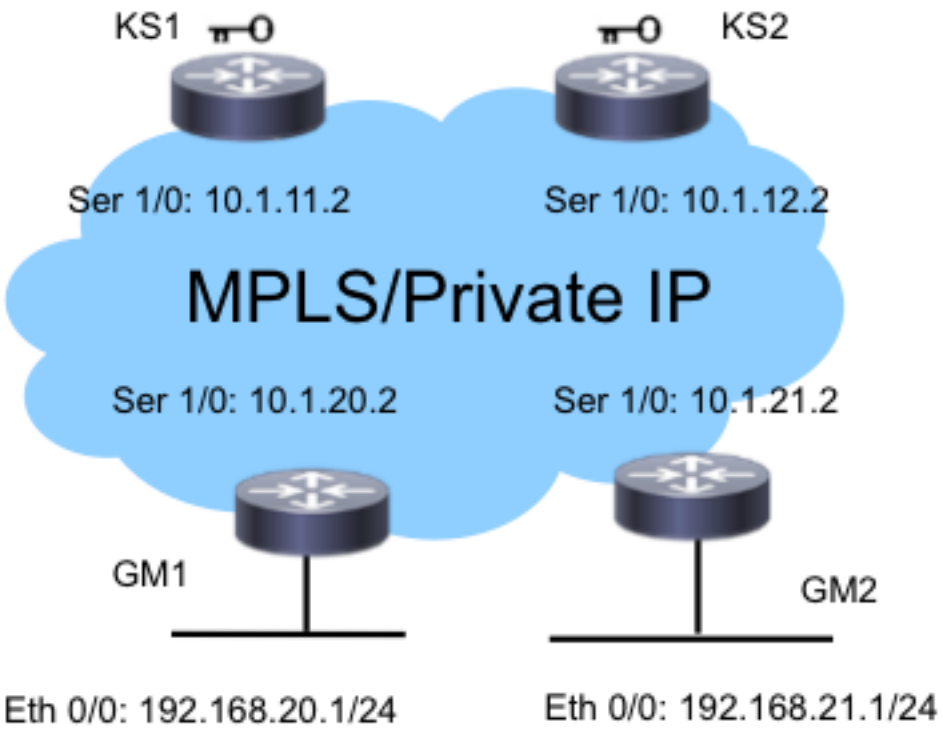
- تبادل مفاتيح الإنترنت (IKE) - يستخدم بين عضو المجموعة (GM) وخادم المفاتيح (KS)، وبين مجموعات المفاتيح والنسخ (KS) للبروتوكول التعاوني (COOP) لمصادقة مستوى التحكم وحمايته.
- مجال المجموعة للتفسير (GDOI) - البروتوكول المستخدم ل KS من أجل توزيع مفاتيح المجموعة وتوفير الخدمة الأساسية مثل rekey إلى جميع GMs.
- COOP - بروتوكول مستخدم ل KSs in order to اتصلت مع بعضهم بعضا ووفرت تكرار.
- حفظ الرأس - IPsec في وضع النفق الذي يحافظ على رأس حزمة البيانات الأصلية لتوصيل حركة المرور من نهاية إلى نهاية.
- مكافحة إعادة التشغيل المستندة إلى الوقت (TBAR) - آلية كشف إعادة التشغيل المستخدمة في بيئة مفتاح مجموعة.

كما توفر مجموعة شاملة من أدوات أستكشاف الأخطاء وإصلاحها من أجل تسهيل عملية

أستكشاف الأخطاء وإصلاحها. من المهم فهم أي من هذه الأدوات متوفر، ومتى تكون مناسبة لكل مهمة أستكشاف الأخطاء وإصلاحها. وعند أستكشاف المشكلات وحلها، فدائما ما تكون فكرة جيدة البدء باألساليب الأقل تدخال حتى ال تتأثر بيئة الإنتاج سلبا. إن مفتاح عملية أستكشاف الأخطاء وإصلاحها المنظمة هذه هو أن تكون قادرا على حل المشكلة إما إلى مشكلة في مستوى التحكم أو مستوى البيانات. يمكنك تنفيذ هذا الإجراء إذا كنت تتبع البروتوكول أو تدفق البيانات وتستخدم الأدوات المختلفة المقدمة هنا للتحقق من صحتها.

طوبولوجيا مرجعية

يتم إستخدام مخطط GETVPN والعنونة هذا في باقي مستند أستكشاف الأخطاء وإصلاحها هذا.



التكوينات المرجعية

- KS1

```
crypto gdoi group G1
identity number 3333
server local
rekey authenmypubkeyrsa get
rekey transport unicast
sa ipsec 1
profile gdoi-p
match address ipv4ENCPOL
address ipv4 10.1.11.2
redundancy
local priority 10
peer address ipv4 10.1.12.2
```

- GM1

```
crypto gdoi group G1
identity number 3333
server address ipv4 10.1.11.2
server address ipv4 10.1.12.2
!
crypto map gm_map 10 gdoi
set group G1
!
interface Serial1/0
crypto map gm_map
```

ةظحالم: ال يتم تضمين اوماصفات KS2 و GM2 هنا للإيجاز.

مصطلحات

- **KS** - الخادم الرئيسي
- **GM** - عضو المجموعة
- **لالبروتوكول** التعاوني
- **TBAR** - مقاومة إعادة التشغيل المستندة إلى الوقت
- **KEK** - مفتاح التشفير
- **TEK** - مفتاح تشفير حركة مرور البيانات

إعداد مرافق التسجيل وأفضل الممارسات الأخرى

قبل البدء في أستكشاف الأخطاء وإصلاحها، تأكد من أنك قد قمت بإعداد منشأة التسجيل كما هو موضح هنا. وتدرج هنا أيضا بعض أفضل الممارسات:

- تحقق من مقدار الموجه للذاكرة الحرة، وقم بتكوين **تصحيح الأخطاء المخزن مؤقتا** للتسجيل إلى قيمة كبيرة (10 ميجابت أو أكثر إن أمكن).

- تعطيل التسجيل إلى خوادم وحدة التحكم والمراقبة و syslog.

- قم باسترداد محتوى المخزن المؤقت للتسجيل باستخدام الأمر **show log** على أساس زمنية منتظمة، كل 20 دقيقة إلى ساعة، لمنع فقدان السجل بسبب إعادة إستخدام المخزن المؤقت.

- أيا كان ما يحدث، فأدخل الأمر **show tech** من GMs و KSs المتأثرة، وفحص إخراج الأمر **show ip route** في الوضع العام وكل توجيه ظاهري (VRF) متوطن، إذا كان هناك حاجة إلى أي منهما.

- أستخدم بروتوكول وقت الشبكة (NTP) لمزامنة الساعة بين جميع الأجهزة التي تم تصحيح أخطائها. تمكين الطوابع الزمنية بالملي ثانية (msec) لكل من رسائل تصحيح الأخطاء والسجل:

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- تأكد من أن مخرجات أمر العرض مختومة بختم الوقت.

```
Router#terminal exec prompt timestamp
```

- عندما تقوم بتجميع مخرجات الأمر show لأحداث مستوى التحكم أو عدادات مستوى

البيانات، قم دائما بتجميع تكرارات متعددة من نفس الإخراج.

أستكشاف أخطاء مستوى التحكم في GETVPN وإصلاحها

مستوى التحكم يعني جميع أحداث البروتوكول التي أدت إلى إنشاء اقتران الأمان (SA) والسياسة على GM حتى تصبح جاهزة لتشفير حركة مرور مستوى البيانات وفك تشفيرها. بعض نقاط التفتيش الرئيسية في مستوى التحكم في GETVPN هي:

أفضل ممارسات تصحيح أخطاء مستوى التحكم

أفضل ممارسات أستكشاف الأخطاء وإصلاحها هذه ليست خاصة ب GETtvpn؛ بل تنطبق على أي تصحيح أخطاء لمستوى التحكم تقريبا. من المهم للغاية اتباع أفضل الممارسات هذه لضمان أكثر عمليات أستكشاف الأخطاء وإصلاحها فعالية:

- قم بإيقاف تشغيل تسجيل وحدة التحكم واستخدام المخزن المؤقت للتسجيل أو syslog لجمع تصحيح الأخطاء.
- أستخدم NTP لمزامنة ساعات الموجه على جميع الأجهزة التي تم تصحيحها.
- تمكين ختم وقت msec لتصحيح الأخطاء ورسائل السجل:

```
service timestamp debug datetime msec
service timestamp log datetime msec
```

- تأكد من أن مخرجات أمر العرض مختومة بختم زمني بحيث يمكن ربطها بمخرج تصحيح الأخطاء:

```
terminal exec prompt timestamp
```

- أستخدم تصحيح الأخطاء الشرطي في بيئة المقياس إن أمكن.

أدوات أستكشاف أخطاء مستوى التحكم وإصلاحها في GetVPN

أوامر عرض GetVPN

كقاعدة عامة، هذه هي مخرجات الأمر التي يجب عليك جمعها تقريبا لكل مشاكل GETVPN.

كس

```
show crypto gdoi
show crypto gdoi ks coop
show crypto gdoi ks members
show crypto gdoi ks rekey
show crypto gdoi ks policy
```

جي إم

```
show crypto eli
show crypto gdoi rekey sa
```

```
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

رسائل GetVPN Syslog

يوفر GETtvpn مجموعة واسعة من رسائل syslog لأحداث البروتوكول الهامة وحالات الخطأ. يجب أن يكون syslog دائما أول مكان يظهر فيه عند إجراء أستكشاف أخطاء GETVPN وإصلاحها.

رسائل syslog المشتركة ل KS

رسائل Syslog	الشرح
coop_config_mismatch	التكوين بين خادم المفاتيح الأساسية الأساسية وخادم المفاتيح الثانوية غير متطابق.
COOP_KS_ELECTION	دخل خادم المفتاح المحلي عملية الاختيار في مجموعة.
coop_ks_reach	تم إستعادة إمكانية الوصول بين خوادم المفاتيح التعاونية التي ت تكوينها.
coop_ks_trans_to_pri	تم تحويل خادم المفتاح المحلي إلى دور أساسي من كونه ملقم ثانوي مجموعة.
Coop_KS_Unauth	حاول خادم بعيد معتمد الاتصال بخادم المفاتيح المحلي في مجموعة، و يمكن اعتباره حدث معادي.
coop_ks_unreach	تم فقد إمكانية الوصول بين خوادم المفاتيح التعاونية التي تم تكوينها، مما يمكن اعتباره حدث عدائي.
KS_GM_REVOKED	أثناء بروتوكول إعادة المفاتيح، حاول عضو غير مصرح له الانضمام إل مجموعة، وهو ما يمكن اعتباره حدث عدائي.
KS_SEND_MCAST_REKEY	إرسال مفتاح البث المتعدد.
KS_SEND_UNICAST_REKEY	إرسال مفتاح إعادة البث الأحادي.
KS_غير مصرح به	وخلال بروتوكول التسجيل في الهيئة، حاول عضو غير مأذون له الانض إلى مجموعة، الأمر الذي يمكن اعتباره حدث عدائيا.
UNAUTHORIZED_IPADDR	تم إسقاط طلب التسجيل لأن الجهاز الطالب غير مخول للانضمام إلى المجموعة.

رسائل syslog الشائعة ل GM

رسائل Syslog	الشرح
GM_CLEAR_Register	تم تنفيذ الأمر **clear crypto gdoi** بواسطة عضو المجموعة المحلية.
gm_cm_attach	تم إرفاق خريطة تشفير لعضو المجموعة المحلية.
GM_CM_DETACH	تم فصل خريطة تشفير لعضو المجموعة المحلي.&
gm_re_register	ربما انتهت صلاحية IPsec SA الذي تم إنشاؤه لمجموعة واحدة أو تم م الحاجة إلى إعادة التسجيل إلى الخادم الرئيسي.
GM_RECV_REKEY	تم تلقي Rekey.
GM_REGS_COMPL	اكتمل التسجيل.
GM_REKEY_TRANS_2_MULTI	انتقل عضو المجموعة من إستخدام آلية إعادة مفتاح البث الأحادي إل إستخدام آلية البث المتعدد.
GM_REKEY_TRANS_2_UNI	انتقل عضو المجموعة من إستخدام آلية إعادة مفتاح البث المتعدد إ إستخدام آلية البث الأحادي.
pseudo_time_large	تلقى عضو المجموعة وقتا زائفا بقيمة مختلفة إلى حد كبير عن و الزائف.
Replay_Failed	فشل أحد أعضاء المجموعة أو خادم المفاتيح في إجراء التحقق من عدم التشغيل.

ملاحظة: الرسائل التي يتم إبرازها باللون الأحمر هي الرسائل الأكثر شيوعا أو أهمية التي يتم رؤيتها في بيئة GETVPN.

التشفير العام وتصحيح أخطاء GDOI

يتم تقسيم عمليات تصحيح أخطاء GetVPN:

1. أولا بواسطة الجهاز الذي يتم استكشاف الأخطاء وإصلاحها عليه.
```
F340.06.15-2900-18#debug cry gdoi ?
 all-features  All features in GDOI
 condition     GDOI Conditional Debugging
 gm            Group Member
 ks            Key Server
```
2. ثانيا حسب نوع المشكلة إلى مع تستكشف فيها الأخطاء وإصلاحها.
```
GM1#debug cry gdoi gm ?
 all-features    All Group Member features
 infrastructure  GM Infrastructure
 registration    GM messages related to registration
 rekey           GM messagese related to Re-Key
 replay          Anti Replay
```
3. ثالثا حسب مستوى تصحيح الأخطاء المطلوب تمكينه. في الإصدار 15.1(3)T والإصدارات الأحدث، تم توحيد جميع عمليات تصحيح أخطاء ميزات GDOI للحصول على مستويات تصحيح الأخطاء هذه. تم تصميم هذا للمساعدة في أستكشاف أخطاء بيئات GETVPN واسعة النطاق وإصلاحها بما يكفي من تحديد تصحيح الأخطاء. عندما يتم تصحيح مشاكل GETVPN، من المهم إستخدام مستوى تصحيح الأخطاء المناسب. كقاعدة عامة، ابدأ بأدنى مستوى تصحيح أخطاء، وهو مستوى الخطأ، وقم بزيادة دقة تصحيح الأخطاء عند الحاجة.
```
GM1#debug cry gdoi gm all-features ?
 all-levels  All levels
 detail      Detail level
 error       Error level
 event       Event level
 packet      Packet level
 terse       Terse level
```

تصحيح الأخطاء الشرطي ل GDOI

في الإصدار 15.1(3)T من Cisco IOS® والإصدارات الأحدث، تمت إضافة تصحيح الأخطاء المشروط ل GDOI للمساعدة في أستكشاف أخطاء GETVPN وإصلاحها في بيئة واسعة النطاق. لذلك يمكن الآن تشغيل جميع "أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) وتصحيح أخطاء GDOI باستخدام عامل تصفية شرطي استنادا إلى المجموعة أو عنوان IP النظير. لمعظم مشاكل GETtvpn، من الجيد تمكين كل من تصحيح أخطاء ISAKMP و GDOI باستخدام المرشح الشرطي المناسب، نظرا لأن تصحيح أخطاء GDOI يعرض فقط العمليات الخاصة ب GDOI. لاستخدام تصحيح الأخطاء المشروط ISAKMP و GDOI، أكمل هاتين الخطوتين البسيطتين:

1. ضبط المرشح الشرطي.
2. قم بتمكين ISAKMP و GDOI المعنيين كالمعتاد.

على سبيل المثال:

```
KS1# debug crypto gdoi condition peer add ipv4 10.1.20.2
% GDOI Debug Condition added.
```

```
KS1#
KS1# show crypto gdoi debug-condition
GDOI Conditional Filters:
Peer Address 10.1.20.2
Unmatched NOT set

KS1#debug crypto gdoi ks registration all-levels
GDOI Key Server Registration Debug level: (Packet, Detail, Event, Terse, Error)
```

ةظحالم: طاقتلا لجأ نم ،GDOI و ISAKMP يطرشلا ءاطخألا حيحصت نم لك مادختساب ليبس ىلع ،يطرشلا حشرملا تامولعم ىلع يوتحت ال دق يتلا ءاطخألا حيحصت لئاسر ،لاثملا ناونع IP يف راسم حيحصت ءاطخألا، نكمي نيكمت نيلعالا ةمالع **ريغ** ةقباطملا. عمو ،كلذ بجي مادختسإ اذه رمألا رذحب نأل هنكمي نأ جتني ةيمك ةريبك نم تامولعم حيحصت ءاطخألا.

GDOI ثدح راثآ

و ثادحألا امئادو نزولا فيفخ عبتت ثادحألا عبتت رفوي .15.1(3)T رادصإلا يف كلذ فيضأو ءاطخأ GDOI ةمهملا. كلذك اضيأ عبتت راسم جورخلا عم نيكمت traceback فورظل ءانثتسالا. يف نكمي نأ رفوت راثآ ثادحألا تامولعم لوح تاظوفحم ثادحأ GETVPN رثكأ نم تاططخم ماظنلا ةيديلقتلا.

عبتتلل تقؤملا نزخملا نم اهدادرتسإ نكميو يضارتفا لكشب GDOI ثادحأ راثآ نيكمت متي رمألا مادختساب **show monitor even-trace**.

```
GM1#show monitor event-trace gdoi ?
all Show all the traces in current buffer
back Show trace from this far back in the past
clock Show trace from a specific clock time/date
coop GDOI COOP Event Traces
exit GDOI Exit Traces
from-boot Show trace from this many seconds after booting
infra GDOI INFRA Event Traces
latest Show latest trace events since last display
merged Show entries in all event traces sorted by time
registration GDOI Registration event Traces
rekey GDOI Rekey event Traces

GM1#show monitor event-trace gdoi rekey all
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
```

رفوي عبتت راسم جورخلا تامولعم ةيليصفت لوح راسم جورخلا، يأ تالاح ءانثتسالاو ءاطخألا، عم نيكمت رايخ traceback لكشب يضارتفا. دعب كلذ نكمي مادختسإ traceback in order to كف زيمرت لسلست زمرلا قيقدلا يذلا ىدأ ىلإ ةلاح راسم جورخلا. مدختسأ رايخ **ليصافتلا** دادرتسال traceback نم نزخملا تقؤملا عبتتلل:

```
GM1#show monitor event-trace gdoi exit all detail
*Nov 6 15:15:25.611: NULL_VALUE_FOUND:Invalid GROUP Name
-Traceback= 0xCA51318z 0xCA1F4DBz 0xC9B2707z 0xCA1ED4Ez 0x97EB018z
```

```
0x97EA960z 0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez
*Nov 6 15:15:25.611: MAP_NOT_APPLIED_IN_ANY_INTERFACE:
-Traceback= 0xCA51318z 0xCA46718z 0xCA1EF79z 0x97EB018z 0x97EA960z
0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez 0xA01FD52z
*Nov 6 15:15:25.650: NULL_VALUE_FOUND:NULL Parameters passed idb or ipaddress
when idb ipaddress is changed
-Traceback= 0xCA51318z 0xCA22430z 0xA09A8DCz 0xA09D8F6z 0xA0F280Fz
0xBA1D1F4z 0xBA1CACCz 0xBA1C881z 0xBA1C5BBz 0xA0F494Az
```

تناك اذإ ايفاك اذه نوكي ال دقو ،الاخدإ 512 وه يضارتفالا تقؤملا عبتتلا نزخم مجح نيوكت تاملعم رييغت نكمي ،اذه يضارتفالا عبتتلا لاخدإ مجح ةدايزل .ةعطقتم ةلكشملا عبتت ثادحألا امك وه حضوم انه:

```
GM1#show monitor event-trace gdoi rekey parameters
Trace has 512 entries
Stacktrace is disabled by default

GM1#
GM1#config t
Enter configuration commands, one per line. End with CNTL/Z.
GM1(config)#monitor event-trace gdoi rekey size ?
<1-1000000> Number of entries in trace
```

نقاط التفتيش على مستوى التحكم في GetVPN والمشاكل الشائعة

فيما يلي بعض من مشاكل مستوى التحكم الشائعة ل GetVPN. لإعادة التكرار، متي فيرعت مستوى التحكم على أنه يجمع عيمج تانوكم ةزيم GETVPN المطلوبة لتمكين تشفير مستوى البيانات وكف تشفيرها على GMs. وعلى مستوى عال، يتطلب ذلك تسجيل GM بنجاح، وسياسة أمان، وتنزيل/تثبيت SA، وما يليه من إعادة إدخال KEK/TEK.

إعداد COOP وإنشاء السياسة

للتحقق من قيام KS بإنشاء نهج الأمان بنجاح و KEK/TEK المقترن والتحقق من ذلك، أدخل:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4
```

```
Replay Value 442843.29 secs
```

مت ةفلتخم تاسايس كانه نوكت امدنع يه KS جهن دادعإ عم ةكرتشم ةدحاو ةلكشم دجوت تكوينواه نيب KSs الأساسية والثانوية. دق يؤدي ذلك إلى سلوك KS ريغ عقوتم وسيتم الإبلاغ نع اذه الخطأ:

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNNING: replay method configuration between
Primary KS and Secondary KS are mismatched
```

ال دجوت ايلاح ةنمازم نيوكت ةيئاقلت نيب KSs الأساسية والثانوية، لذلك بجي تصحيحها يدويا.

نأل COOP وه نيوكت جرح (ودائما تقريبا إلزامي) ل GETVPN، نمف الأساسي التأكد نم لمع COOP لكشب حيحص نأو أدوار COOP KS صحيحة:

```
KS1#show crypto gdoi ks coop
Crypto Gdoi Group Name :G1
Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 10.1.11.2
Local Priority: 200
 Local KS Role: Primary   , Local KS Status: Alive
Local KS version: 1.0.4
Primary Timers:
Primary Refresh Policy Time: 20
Remaining Time: 10
Antireplay Sequence Number: 40

Peer Sessions:
Session 1:
Server handle: 2147483651
Peer Address: 10.1.12.2
Peer Version: 1.0.4
Peer Priority: 100
Peer KS Role: Secondary , Peer KS Status: Alive
Antireplay Sequence Number: 0

IKE status: Established
Counters:
Ann msgs sent: 31
Ann msgs sent with reply request: 2
Ann msgs recv: 64
Ann msgs recv with reply request: 1
Packet sent drops: 7
Packet Recv drops: 0
Total bytes sent: 20887
Total bytes recv: 40244
```

في إعداد البروتوكول الاختياري الوظيفي، بجي ملاحظة تدفق البروتوكول هذا:

IKE Exchange > ANN مع أولويات COOP المتبادلة > إختيار COOP > ANN نم KS الأساسي إلى الثانوي (السياسة وقاعدة بيانات GM والمفاتيح)

عندما ال يعمل COOP لكشب حيحص، أو إذا كان ناك كانه ميسقت COOP، لثم نأ حبصت KSs ةددعتم KS الأساسية، فيجب تجميع تصحيح الأخطاء هذه الاستكشاف الأخطاء وإصلاحها:

```
debug crypto isakmp
debug crypto gdoi ks coop all-levels
show crypto isakmp sa
```

```
show crypto gdoi ks coop
```

إعداد IKE

يطلب تبادل IKE ل GETVPN تأمين قناة التحكم للنهج القالب وتنزيل SA. وفي نهاية عملية تبادل IKE الناجحة، يتم إنشاء SA ل GDOI_REKEY.

في الإصدارات الأقدم من Cisco IOS 15.4(1)T، يمكن عرض gdoi_REKEY باستخدام الأمر **show crypto isakmp sa**:

```
GM1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.1.13.2 10.1.11.2 GDOI_REKEY        1075 ACTIVE
10.1.11.2 10.1.13.2 GDOI_IDLE         1074 ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
```

في الإصدار 15.4(1)T من Cisco IOS 15.4(1)T والإصدارات الأحدث، يتم عرض الأمر gdoi_REKEY هذا باستخدام الأمر **show crypto gdoi rekey sa**:

```
GM1#show crypto gdoi rekey sa
GETVPN REKEY SA
dst             src             conn-id         status
10.1.13.2       10.1.11.2       1114            ACTIVE
```

> **ملاحظة**: بمجرد اكتمال عملية التبادل الأولية لنموذج IKE، **يتم دفع** السياسات والمفاتيح اللاحقة من نظام KS إلى نظام GM باستخدام GDOI_REKEY SA. لذلك فإنه لا يمكن الحصول على مفتاح لحالة عدم انتظام العمل في الدليل عندما تنتهي مدة صلاحيتها. ومع ذلك، يجب أن يكون هناك دائما SA GDOI_REKEY على GM لكي يتلقى الدورق.

لا يختلف تبادل IKE ل GETVPN عن IKE المستخدم في أي أنفاق IPsec التقليدية من نقطة إلى نقطة، لذلك ظل طريقة استكشاف الأخطاء وإصلاحها كما هي. يجب تجميع عمليات تصحيح الأخطاء هذه لاستكشاف أخطاء مصادقة IKE وإصلاحها:

```
debug crypto isakmp
debug crypto isakmp error
debug crypto isakmp detail (hidden command, if detailed isakmp exchange information
is needed)
debug crypto isakmp packet (hidden command, if packet level isakmp information is needed)
```

التسجيل، تنزيل النهج، وتثبيت SA

بمجرد نجاح مصادقة IKE، يتم تسجيل GM باستخدام KS. من المتوقع رؤية رسائل syslog هذه عندما يحدث هذا بشكل صحيح:

```
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to Unicast Rekey.
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.2 complete for group G1 using
address 10.1.13.2
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies
```

from KS 10.1.12.2 for group G1 & gm identity 10.1.13.2

يمكن التحقق من النهج والمفاتيح باستخدام هذا الأمر:

```
GM1#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 1
IPSec SA Direction : Both

Group Server list : 10.1.11.2
10.1.12.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.12.2
Re-registers in       : 139 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 10.1.11.2
Last rekey seq num : 0
Unicast rekey received: 1
Rekey ACKs sent : 1
Rekey Rcvd(hh:mm:ss)  : 00:05:20
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 1
After latest register : 1
Rekey Acks sents : 1

ACL Downloaded From KS 10.1.11.2:
access-list deny icmp any any
access-list deny eigrp any any
access-list deny ip any 224.0.0.0 0.255.255.255
access-list deny ip 224.0.0.0 0.255.255.255 any
access-list deny udp any port = 848 any port = 848
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 878
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (200)
Anti-Replay(Time Based) : 4 sec interval
```

```
GM1#
GM1#
GM1#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: gm1map, local addr 10.1.13.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x8BF147EF(2347845615)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
GM1#
```

ملاحظة: باستخدام GETVPN، تستخدم شبكات SA الواردة والصادرة نفس SPI.

عم تسجيل GETVPN وعون تثبيت السياسة من المشاكل، تكون هناك حاجة إلى عمليات تصحيح الأخطاء وإصلاحها:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

ملاحظة: قد تكون هناك حاجة إلى مزيد من تصحيح الأخطاء بعد النتائج هذه.

بما أن تسجيل GETVPN يحدث عادة بعد إعادة تحميل GM مباشرة، فقد يكون برنامج IM النصي هذا مفيدا لجمع تصحيح الأخطاء هذه:

```
event manager applet debug
event syslog pattern "RESTART"
action 1.0 cli command "enable"
action 2.0 cli command "debug crypto gdoi all all"
```

ريكي

بمجرد تسجيل GMs إلى KS وإعداد شبكة GETVPN بشكل صحيح، تكون KS الأساسية مسؤولة عن إرسال رسائل rekey إلى جميع GMs المسجلة إليها. يتم إستخدام رسائل rekey لمزامنة كل السياسات والمفاتيح والأقفال الزائفة على GMs. يمكن إرسال رسائل rekey من خلال أسلوب بث أحادي أو متعدد.

رأيت هذه syslog رسالة على ال KS عندما ال rekey رسالة أرسلت:

```
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group G1 from address
10.1.11.2 with seq # 11
```

على ال GMs، هذا هو syslog أن يرى عندما يستلم هو المفاتيح:

```
%GDOI-5-GM_RECV_REKEY: Received Rekey for group G1 from 10.1.11.2 to 10.1.20.2
with seq # 11
```

متطلبات وجود مفاتيح RSA ل rekey على KS

تتطلب وظيفة Rekey وجود مفاتيح RSA على KS. يوفر KS المفاتيح العام لزوج مفاتيح RSA إلى GM من خلال هذه القناة المؤمنة أثناء التسجيل. ثم يقوم مكتب الأخلاقيات بتوقيع رسائل GDOI المرسلة إلى GM مع مفاتيح RSA الخاص في حمولة GDOI SIG. تتلقى GM رسائل GDOI وتستخدم مفاتيح RSA العام للتحقق من الرسالة. يتم تشفير الرسائل بين KS و GM باستخدام KEK، والتي يتم توزيعها أيضا على GM أثناء التسجيل. وبمجرد اكتمال التسجيل، يتم تشفير المفاتيح التالية باستخدام KEK وتوقيعها باستخدام مفاتيح RSA الخاص.

إذا لم يكن مفاتيح RSA موجودا على KS أثناء تسجيل GM، تظهر هذه الرسالة على syslog:

```
%GDOI-1-KS_NO_RSA_KEYS: RSA Key - get : Not found, Required for group G1
```

عندما ال تكون المفاتيح موجودة على KS، تسجل GM أول مرة، ولكن المفاتيح الرئيسية التالية في شل من KS. في انتهاء المطاف تنتهي صلاحية المفاتيح الموجودة على GM، ويتم إعادة تسجيلها مرة أخرى.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may have expired/been
cleared, or didn't go through. Re-register to KS.
```

ونظرا لأن ه يتم إستخدام زوج مفاتيح RSA لتوقيع رسائل rekey، **فيجب أن** تكون **هذه الرسائل** هي نفسها بين كل وحدات KS الأساسية والثانوية. وهذا يضمن أن ه خلال فشل KS أساسي، لا يزال بالإمكان التحقق من صحة المفاتيح المرسلة من قبل KS ثانوي (KS الأساسي الجديد) بشكل صحيح بواسطة GMs. عندما يقوم بإنشاء زوج مفاتيح RSA على KS الأساسية، يجب إنشاء زوج المفاتيح باستخدام الخيار **القابل للتصدير** حتى يمكن تصديره إلى جميع KSs الثانوية من أجل تلبية هذا المتطلب.

تحليل مشاكل إعادة المفاتيح

فشل إعادة توجيه KEK/TEK هو أحد أكثر مشاكل GETVPN شيوعا التي تتم مواجهتها في عمليات نشر العملاء. يجب أن تتبع المشكلات المتعلقة بحل المشكلات الرئيسية الخطوات الأساسية كما هو موضح هنا:

1. هل تم إرسال القدرة من قبل KS؟

 يمكن التحقق من هذا الإجراء بواسطة أحد المراقبين لرسالة syslog الخاصة ب %GDOI-5-KS_SEND_UNICAST_REKEY أو بشكل أكثر دقة باستخدام هذا الأمر:

```
KS1#show crypto gdoi ks rekey
Group G1 (Unicast)
Number of Rekeys sent                 : 341
Number of Rekeys retransmitted        : 0
KEK rekey lifetime (sec) : 1200
Remaining lifetime (sec) : 894
Retransmit period : 10
Number of retransmissions : 5
IPSec SA 1 lifetime (sec) : 900
Remaining lifetime (sec) : 405
```

 يشير عدد القرود التي أعيد نقلها إلى حزم إقرار إعادة المفاتيح التي لم تستلمها KS وبالتالي يشير إلى مشاكل إعادة المفاتيح المحتملة. مع الأخذ في الاعتبار أن مفاتيح GDOI يستخدم بروتوكول UDP كآلية نقل لا يمكن الاعتماد عليها، لذلك قد يتوقع حدوث بعض حالات انخفاض الباب اعتمادا على موثوقية شبكة النقل الأساسية، ولكن ينبغي التحقيق دائما في أي اتجاه زيادة إعادة نقل المفاتيح.

 ويمكن أيضا الحصول على إحصاءات أكثر تفصيلا عن كل عملية تغيير نوعية. هذا هو عادة أول مكان للبحث عن القضايا الأساسية المحتملة.

```
KS1#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group G1 : 346

Group Member ID : 10.1.14.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.11.2
 Rekeys sent       : 346
Rekeys retries : 0
```

```
Rekey Acks Rcvd : 346
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1

Group Member ID : 10.1.13.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.12.2
 Rekeys sent       : 340
Rekeys retries : 0
Rekey Acks Rcvd : 340
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1
```

2. هل تم تسليم حزم rekey في شبكة البنية الأساسية الأساسية؟

   يجب اتباع أستكشاف أخطاء IP وإصلاحها بشكل قياسي على مسار إعادة توجيه إعادة توجيه للمفاتح لضمان عدم إسقاط حزم rekey في شبكة النقل بين KS و GM. بعض أدوات أستكشاف الأخطاء وإصلاحها الشائعة المستخدمة هي قوائم التحكم في الوصول إلى الإدخال/الإخراج (ACLs) و NetFlow والتقاط الحزم في شبكة النقل.

3. هل وصلت حزم rekey إلى عملية GDOI لمعالجة إعادة المفاتح؟

   تحقق من إحصائيات مفاتح GM:

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
Number of Rekey Acks sent : 340
```

4. هل عادت حزمة إقرار إعادة المفاتح إلى KS؟

   اتبع الخطوات من 1 إلى 3 لتتبع حزمة إقرار إعادة المفاتح من GM مرة أخرى إلى KS.

مفاتح البث المتعدد

يختلف مفاتح إعادة البث المتعدد عن إعادة مفاتح البث الأحادي في هذه الجوانب:

- بما أن multicast استعملت in order to نقلت هذا rekey ربط من ال KS إلى ال GMs، ال k ال يحتاج أن يكرر ال rekey ربط نفسه. يرسل KS نسخة واحدة فقط من حزمة rekey، وتم نسخها في الشبكة التي تم تمكين البث المتعدد.
- ال توجد آلية للإقرار لمفاتح إعادة البث المتعدد، لذلك إذا لم تستلم GM حزمة المفاتح، فلن يكون ل KS معرفة به، وبالتالي لن يزيل GM من قاعدة بيانات GM الخاصة به. ونظرا لعدم وجود إقرار، فإن KS سيقوم دائما بإعادة إرسال حزم rekey استنادا إلى تكوين إعادة نقل المفاتح الخاص به.

تعد مشكلة إعادة مفاتح البث المتعدد الأكثر شيوعا هي عندما ال يتم تلقي المفاتح على GM. قد يكون هناك عدد من الأسباب المحتملة لذلك، مثل:

- مشكلة تسليم الحزمة داخل البنية الأساسية لتوجيه البث المتعدد

- لم يتم تمكين التوجيه من نهاية إلى نهاية للبث المتعدد داخل الشبكة

الخطوة الأولى لاستكشاف أخطاء إحدى المشاكل مع إعادة مفتاح البث المتعدد وإصلاحها هي معرفة ما إذا كانت إعادة المفتاح تعمل عند التبديل من البث المتعدد إلى طريقة البث الأحادي.

ما إن يعين أنت أن الإصدار خاص إلى multicast rekey، دققت أن KS يرسل المفتاح إلى ال multicast عنوان يعين.

```
%GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group G1 from address
10.1.11.2 to 226.1.1.1 with seq # 6
```

اختبر اتصال البث المتعدد بين KS و GM مع طلب بروتوكول رسائل التحكم في الإنترنت (ICMP) إلى عنوان البث المتعدد. يجب أن ترد جميع GMs التي تعد جزءا من مجموعة البث المتعدد على إختبار الاتصال. تأكد من إستثناء ICMP من نهج تشفير KS لهذا الاختبار.

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

إذا فشل إختبار اتصال البث المتعدد، فيجب تنفيذ أستكشاف أخطاء البث المتعدد وإصلاحها، وهو خارج نطاق هذا المستند.

التحقق من ترحيل مستوى التحكم

عرض

عندما يقوم العملاء بترقية GM الخاص بهم إلى إصدار جديد من Cisco IOS، فقد يواجهون حالات فشل إعادة مفتاح KEK مع ظهور هذه الرسالة في syslog:

```
%GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 1 in seq payload for
group G1, last seq # 11
%GDOI-3-GDOI_REKEY_FAILURE: Processing of REKEY payloads failed on GM 10.1.13.2 in the group G1,
with peer at 10.1.11.2
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of GDOI mode failed with peer at 10.1.11.2
```

يحدث هذا السلوك بسبب مشكلة قابلية التشغيل البيني التي تم تقديمها مع التحقق من عدم إعادة التشغيل الذي تمت إضافته لرسائل مستوى التحكم. وعلى وجه التحديد، سيقوم KS الذي يقوم بتشغيل التعليمات البرمجية القديمة بإعادة تعيين رقم تسلسل إعادة مفتاح KEK إلى 1، وسيتم إسقاط هذا من قبل GM الذي يقوم بتشغيل التعليمات البرمجية الجديدة عند تفسيرها على أنها حزمة rekey معاد تشغيلها. للحصول على مزيد من التفاصيل، راجع معرف تصحيح الأخطاء من Cisco CSCta05809 (GETVPN: مستوى تحكم GETVPN معقول لإعادة التشغيل)، وقيود تكوين GETVPN.

الخلفية

باستخدام GETVPN، يمكن أن تحمل رسائل مستوى التحكم معلومات حساسة للوقت لتوفير خدمة التحقق من عدم إعادة التشغيل المستندة إلى الوقت. وبالتالي، تتطلب هذه الرسائل حماية مضادة لإعادة التشغيل نفسها من أجل ضمان الاستفادة من الوقت. هذه الرسائل هي:

- **إعادة تكوين الرسائل** من KS إلى GM
- **رسائل إعلان التعاون** بين KSs

كجزء من تنفيذ الحماية ضد إعادة التشغيل هذا، تمت إضافة تحققات الرقم التسلسلي من أجل حماية الرسائل التي تم إعادة تشغيلها، بالإضافة إلى التحقق من الوقت الكاذب عند تمكين TBAR.

الحل

لحل هذه المشكلة، يجب ترقية كل من GM و KS إلى إصدارات Cisco IOS بعد ميزة التحقق من إعادة تشغيل مستوى التحكم. باستخدام رمز Cisco IOS الجديد، الـ يقوم KS بإعادة تعيين رقم التسلسل مرة أخرى إلى 1 لمفاتيح KEK، ولكنه بدلاً من ذلك يستمر في استخدام رقم التسلسل الحالي ويقوم فقط بإعادة تعيين رقم التسلسل لمفاتيح TEK.

تتضمن إصدارات Cisco IOS هذه ميزات التحقق من إعادة التشغيل:

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M والإصدارات الأحدث

مشاكل أخرى ذات صلة بإعادة التشغيل

- فشل البرنامج بسبب رسائل فشل التحقق من إعادة التشغيل (معرف تصحيح الأخطاء من Cisco CSCtc52655)

أخطاء إعادة تشغيل مستوى التحكم

بالنسبة لعمليات فشل إعادة تشغيل مستوى التحكم الأخرى، قم بجمع هذه المعلومات وتأكد من مزامنة الأوقات بين KS و GM.

- Syslog من GM و KS
- تصحيح أخطاء ISAKMP
- تصحيح أخطاء GDOI (rekey and replay) من كل من KS و GM

مشاكل تجزئة حزمة مستوى التحكم

مع GETVPN، يعد تجزئة حزمة مستوى التحكم مشكلة مشتركة، ويمكن أن تظهر نفسها في أحد السيناريوهين عندما تكون حزم مستوى التحكم كبيرة بشكل يكفي أنها ستتطلب تجزئة IP:

- حزم إعلان بروتوكول GetVPN
- حزم مفتاح GetVPN

حزم إعلان COOP

تحمل حزم إعلان COOP معلومات قاعدة بيانات GM، وبالتالي يمكن أن تنمو بشكل كبير في نشر GETVPN كبير. من التجربة السابقة، ستنتج شبكة GETVPN التي تتكون من 1500+ GMs حزم إعلان أكبر من 18024 بايت، وهو حجم المخزن المؤقت الضخم الافتراضي من Cisco IOS. عندما يحدث هذا، يفشل KS في تخصيص مخزن مؤقت كبير بما يكفي للإرسال حزم ANN مع هذا الخطأ:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 18872 -Process= "Crypto IKMP", ipl= 0, pid= 183
```

لتصحيح اذه الشرط، يوصى بتوليف المخزن المؤقت اذه:

```
buffers huge permanent 10
buffers huge size 65535
```

إعادة مفاتيح الحزم

كما يمكن أن تتجاوز الحزم المنمطية ل GetVPN حجم وحدة الاتصال الأقصى ل IP (MTU) المنموذجي 1500 عندما يكون تشفير كبير، مثل السياسة التي تتكون من 8+ سطر من إدخالات التحكم في الوصول (ACEs) في قائمة التحكم في الوصول (ACL) للتشفير.

مشكلة التجزئة والتعريف

في كل السيناريوهين السابقين، يجب أن يكون GETVPN قادرا على إرسال واستقبال حزم UDP المجزأة بشكل صحيح in order to عمل COOP أو GDOI rekey بشكل صحيح. يمكن أن يكون تجزئة IP مشكلة في بعض بيئات الشبكة. على سبيل المثال، تتطلب الشبكة التي تتكون من مستوى إعادة توجيه متعدد المسارات (ECMP) ذي تكلفة متساوية، وبعض الأجهزة في مستوى إعادة التوجيه، إعادة تجميع ظاهرية لحزم IP المجزأة، مثل إعادة تجميع التجزئة الظاهرية (VFR).

لتحديد المشكلة، تحقق من أخطاء إعادة التجميع على الجهاز حيث يشتبه في أن حزم UDP 848 المجزأة لم يتم استقبالها بشكل صحيح:

```
KS1#show ip traffic | section Frags
Frags: 10 reassembled, 3 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
```

إذا إستمرت حالات انتهاء المهلة لإعادة التجميع في الزيادة، أستخدم الأمر **debug ip error** لتأكيد ما إذا كان الإسقاط عجز من دقق حزمة rekey/COOP. وبمجرد التأكد من ذلك، يجب تنفيذ أستكشاف أخطاء إعادة توجيه IP وإصلاحها بشكل طبيعي لعزل الجهاز الدقيق في مستوى إعادة التوجيه الذي قد يكون قد أسقط الحزم. تتضمن بعض الأدوات الشائعة الاستخدام ما يلي:

- التقاط الحزمة
- إحصائيات إعادة توجيه حركة المرور
- إحصائيات ميزة الأمان (جدار الحماية، IPS)
- إحصائيات VFR

مشكلات قابلية التشغيل البيني ل GDOI

تم العثور على العديد من مشاكل قابلية التشغيل البيني مع GETVPN على مر السنوات، ومن المهم ملاحظة إصدارات برنامج Cisco IOS بين KS و GM وبين KSs لمسائل قابلية التشغيل البيني.

من بين المشاكل الأخرى المعروفة الخاصة بقابلية التشغيل البيني ل GETVPN:

- التحقق من ترحيل مستوى التحكم
- تغيير سلوك مفتاح GetVPN KEK
- معرف تصحيح الأخطاء من Cisco CSCub42920 (GETVPN: KS يفشل في التحقق من صحة

التجزئة في ACK rekey من إصدارات GM السابقة)

- معرف تصحيح الأخطاء من Cisco CSCuw48400 (GetVPN GM يعجز عن التسجيل أو يفشل rekey - sig-hash > default SHA-1)
- معرف تصحيح الأخطاء من Cisco CSCvg19281 (يتعدد GETVPN GM يتعطل بعد الترحيل إلى 3.16 أو إلى زوج KS جديد؛ إذا كان إصدار GM أقدم من 3.16، وتمت ترقية KS من رمز سابق إلى 3.16 أحدث، يمكن أن تحدث هذه المشكلة)

إجراء ترقية IOS ل GetVPN

يجب اتباع إجراء ترقية Cisco IOS هذا عندما يلزم إجراء ترقية رمز Cisco IOS في بيئة GETVPN:

1. قم بترقية KS الثانوي أو انتظر حتى اكتمال عملية إختيار COOP KS.
2. كرر الخطوة 1 لجميع KSs الثانوية.
3. ترقية KS الأساسية.
4. ترقية GMs.

أستكشاف أخطاء مستوى بيانات GETVPN وإصلاحها

بالمقارنة مع مشاكل مستوى التحكم، فإن مشاكل مستوى بيانات GETVPN هي مشاكل حيث تحتوي GM على السياسة والمفاتيح لإجراء تشفير مستوى البيانات وفك تشفيرها، ولكن لسبب ما ال يعمل تدفق حركة مرور البيانات من نهاية إلى نهاية. تتعلق معظم مشاكل مستوى البيانات ل GETVPN بإعادة توجيه IPsec العامة، وليست خاصة ب GETtvpn. لذلك ينطبق معظم نهج أستكشاف الأخطاء وإصلاحها الموصوف هنا على مشاكل حوكمة بيانات IPsec العامة أيضا.

مع مشاكل التشفير (على أساس المجموعة أو الأنفاق على مستوى الكبل)، من المهم أستكشاف المشكلة وإصلاحها وعزل المشكلة إلى جزء معين من DataPath. وعلى وجه التحديد، فإن نهج أستكشاف الأخطاء وإصلاحها المذكور هنا يهدف إلى مساعدتك على الإجابة على هذه الأسئلة:

- ما هو الجهاز المسؤول - تشفير الموجه أو فك تشفير الموجه؟
- في أي إتجاه تحدث المشكلة - مدخل أو مخرج؟

أدوات أستكشاف أخطاء مستوى بيانات GetVPN وإصلاحها

يختلف أستكشاف أخطاء مستوى بيانات IPsec وإصلاحها تماما عن تلك الخاصة بمستوى التحكم. باستخدام مستوى البيانات، ال توجد عادة أي تصحيح أخطاء يمكنك تشغيله، أو على الأقل تشغيله بأمان في بيئة إنتاج. لذلك، يعتمد أستكشاف الأخطاء وإصلاحها في بشكل كبير على عدادات مختلفة وإحصاءات حركة مرور البيانات التي يمكنها المساعدة في تتبع الحزمة على مسار إعادة التوجيه. تتمثل الفكرة في القدرة على تحويل مجموعة من نقاط التفتيش للمساعدة في عزل الأماكن التي قد يتم فيها إسقاط الحزم كما هو موضح هنا:

فيما يلي بعض أدوات تصحيح أخطاء مستوى البيانات:

- قوائم الوصول
- محاسبة أسبقية IP
- Netflow
- عدادات الواجهة
- عدادات التشفير
- عدادات الإسقاط العامة لكل ميزة وإعادة التوجيه السريع IP Cisco Express Forwarding (CEF)
- التقاط الحزمة المضمنة (EPC)
- تصحيح أخطاء مستوى البيانات (تصحيح أخطاء حزم IP و CEF)

يمكن التحقق من نقاط التفتيش الموجودة في قاعدة البيانات في الصورة السابقة باستخدام الأدوات التالية:

تشفير GM

- واجهة Ingress LAN
  قائمة التحكم في الوصول (ACL) للإدخال
  Ingress NetFlow
  التقاط حزمة مضمنة
  محاسبة أسبقية الإدخال

- محرك التشفير
  show crypto ipsec sa
  إظهار تفاصيل IPsec للتشفير
  إظهار إحصائيات مسرع محرك التشفير

- واجهة Egress WAN
  Egress NetFlow
  التقاط حزمة مضمنة
  محاسبة أسبقية المخرجات

فك تشفير GM

- واجهة WAN للمدخل
  قائمة التحكم في الوصول (ACL) للإدخال
  Ingress NetFlow
  التقاط حزمة مضمنة
  محاسبة أسبقية الإدخال

- محرك التشفير
  show crypto ipsec sa

عرض تفاصيل IPsec للتشفير
إظهار إحصائيات عرض حركة التشفير

- واجهة Egress LAN
  Egress NetFlow
  ضمن حزمة طاقتل

يتبع رسم الإرجاع نفس تدفق حركة المرور. تحتوي الأقسام التالية على بعض الأمثلة على أدوات مستوى البيانات هذه قيد الاستخدام.

عدادات التشفير/فك التشفير

تستند عدادات التشفير/فك التشفير على الموجه إلى تدفق IPsec. للأسف ال يعمل هذا بشكل جيد مع GETVPN نظرا لأن GETVPN عادة موقي بنشر سياسة تشفير "السماح ip any" التي توقع بتشفير كل شيء. لذلك إذا تحدث المشكلة فقط لبعض التدفقات وليس الكل، فإن هذه العدادات يمكن أن تكون عونا ما صعبة االستخدام من أجل التقييم الصحيح إذا تم تشفير الحزم أو فك تشفيرها عندما يكون هناك ما يكفي من حركة مرور بيانات خلفية مهمة لعمل.

```
GM1#show crypto ipsec sa | in encrypt|decrypt
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
```

Netflow

يمكن إستخدام NetFlow لمراقبة كل من حركة مرور المدخل والمخرج على كل GMs. مع الحظ سماح GETVPN **بالإيصال أي** سياسة، ويتم تجميع حركة المرور التي تم تشفيرها والمعلومات لكل تدفق. بعد ذلك، سيتعين تجميع المعلومات لكل تدفق مع وضع عالمة أسبقية/أسبقية DSCP الموضحة الحقا.

في هذا المثال، يتم عرض NetFlow ل 100 عملية إختبار اتصال من مضيف خلف GM1 إلى مضيف خلف GM2 في نقاط التفتيش المختلفة.

تشفير GM

تكوين Netflow:

```
interface Ethernet0/0
description LAN
ip address 192.168.13.1 255.255.255.0
ip flow ingress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.13.2 255.255.255.252
ip flow egress
ip pim sparse-dense-mode
crypto map gm1map
```

إخراج Netflow:

```
GM1#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
```

```
Et0/0 192.168.13.2 Se1/0* 192.168.14.2 32 8DE1 6523   100
Et0/0 192.168.13.2 Se1/0 192.168.14.2 01 0000 0800   100
GM1#
```

ملاحظة: في المخرج السابق، * يشير إلى حركة مرور المخرج. يعرض الخط الأول حركة مرور البيانات المشفرة للخروج (مع البروتوكول 0x32 = ESP) من واجهة WAN، والسطر الثاني مدخل ICMP حركة مرور الوصول إلى واجهة LAN.

فك تشفير GM

التكوين:

```
interface Ethernet0/0
description LAN interface
ip address 192.168.14.1 255.255.255.0
ip flow egress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.14.2 255.255.255.252
ip flow ingress
ip pim sparse-dense-mode
crypto map gm1map
```

إخراج Netflow:

```
GM2#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Se1/0 192.168.13.2 Et0/0 192.168.14.2 32 8DE1 6523   100
Se1/0 192.168.13.2 Et0/0* 192.168.14.2 01 0000 0800   100
GM2#
```

تمييز أسبقية DSCP/IP

التحدي مع أستكشاف أخطاء التشفير وإصلاحها هو أنه بمجرد تشفير الحزمة تفقد إمكانية الرؤية في الحمولة، وهو ما يفترض أن يفعله التشفير، وهذا يجعل من الصعب تتبع الحزمة لتدفق IP معين. هناك طريقتان لمعالجة هذا الحد عندما يتعلق الأمر باستكشاف مشكلة IPsec وإصلاحها:

- إستخدام ESP-NULL كتحويل IPsec. الا يزال IPsec يجري تضمين ESP ولكن ال يتم تطبيق أي تشفير على الحمولة، لذلك فإنها تكون مرئية في التقاط الحزمة.
- وضع علامة على تدفق IP باستخدام نقطة رمز خدمات مميزة (DSCP)/وضع علامة أسبقية استنادا إلى خصائص L3/L4 الخاصة بها.

يتطلب ESP-NULL تغييرات على كل نقطتي نهاية النفق وغالبا ال يتم السماح به بناء على نهج أمان العميل. لذلك، توصي Cisco عادة باستخدام تمييز أسبقية/DSCP بدال من ذلك.

المخطط المرجعي لألسبقية/DSCP

ToS (hex)	ToS(عشري)	أسبقية IP	DSCP	ثنائي
0xE0	224	التحكم في الشبكة 7	56 وحدة التحكم CS7	11100000
0xC0	192	التحكم في الشبكة البينية 6	48 CS6	11000000
0xB8	184	5 جرح	46 فولت	10111000
0xA0	160		40 CS5	10100000

0x88	136	تجاوز 4 فلاش	34 أف-41	10001000
0x80	128		32 وحدة التحكم CS4	10000000
0x68	104	3 فلاش	26 أف 31	01101000
0x60	96		24 CS3	01100000
0x48	72	منفذان فوريان	18 أف 21	01001000
0x40	64		16 وحدة التحكم CS2	01000000
0x20	32	أولوية واحدة	8 CS1	00100000
0x00	0	روتين 0	0 DFLT	00000000

تمييز الحزم باستخدام DSCP/أسبقية

يتم إستخدام هذه الطرق بشكل نموذجي لوضع علامات على الحزم بعلامات DSCP/أسبقية محددة.

بي بي آر

```
interface Ethernet1/0
ip policy route-map mark
!
access-list 150 permit ip host 172.16.1.2 host 172.16.254.2
!
route-map mark permit 10
match ip address 150
set ip precedence flash-override
```

MQC

```
class-map match-all my_flow
match access-group 150
!
policy-map marking
class my_flow
set ip precedence 4
!
interface Ethernet1/0
service-policy input marking
```

إختبار اتصال الموجه

```
GM1-host#ping ip
Target IP address: 192.168.14.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 136
...
<snip>
```

ملاحظة: من الأفضل دائما مراقبة تدفق حركة المرور العادي وملف تعريف أسبقية DSCP قبل تطبيق التمييز بحيث يكون تدفق حركة المرور المميز فريدا.

مراقبة الحزم المميزة

محاسبة أسبقية IP

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip accounting precedence input
```

```
middle_router#show interface precedence
Ethernet0/0
Input
Precedence 4: 100 packets, 17400 bytes
```

قائمة التحكم في الوصول (ACL) للواجهة

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

التقاط حزمة مضمنة

التقاط الحزم المضمن (EPC) هو أداة مفيدة لالتقاط الحزم على مستوى الواجهة لتحديد ما إذا كانت الحزمة قد وصلت إلى جهاز معين. تذكر أن EPC يعمل جيدا لحركة مرور النص الواضح، ولكنه يمكن أن يكون تحديا عندما يتم تشفير الحزم التي يتم التقاطها. لذلك يجب إستخدام تقنيات مثل تمييز DSCP/أسبقية التي تمت مناقشتها سابقا وأ حرف IP الأخرى، مثل طول حزمة IP، مع EPC لجعل أستكشاف الأخطاء وإصلاحها أكثر فعالية.

تتبع حزمة IOS-XE من Cisco

هذه ميزة مفيدة لتتبع مسار إعادة توجيه الميزات على جميع الأنظمة الأساسية التي تعمل بنظام التشغيل Cisco IOS-XE، مثل ISR4451-X و ASR1000 و CSR1000V.

المشاكل الشائعة لمستوى بيانات GetVPN

ال يختلف أستكشاف أخطاء مستوى بيانات IPsec ل GETtvpn وإصلاحها غالبا عن أستكشاف أخطاء مستوى بيانات IPsec التقليدية وإصلاحها من نقطة إلى نقطة، مع إستثنائين. بسبب خصائص مستوى البيانات الفريدة هذه ل GETtvpn.

فشل مكافحة إعادة التشغيل المستند إلى الوقت

في شبكة GETVPN، غالبا ما يكون من الصعب أستكشاف أخطاء TBAR وإصلاحها نظرا لعدم وجود أنفاق مزودة الحكمة بعد ذلك. لاستكشاف أخطاء GETvpn TBAR وإصلاحها، أكمل الخطوات التالية:

1. تعرف على الحزمة التي يتم إسقاطها بسبب فشل شريط الفيديو ثم حدد تشفير GM بعد ذلك.

قبل الإصدار 15.3(2)T، لم يقم syslog لفشل TBAR بطباعة عنوان المصدر للحزمة الفاشلة، لذلك يجعل هذا من الصعب جدا تحديد الحزمة التي فشلت. وقد تم تحسين هذا بشكل ملحوظ في الإصدار 15.3(2)T والإصدارات الأحدث، حيث يطبع Cisco IOS هذا:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=13, sequence number=1

%GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in group G1:
my_pseudotime = 620051.84 secs, peer_pseudotime = 619767.09 secs, replay_window =
4 (sec), src_ip = 192.168.13.2, dst_ip = 192.168.14.2
```

تم تنفيذ محفوظات TBAR أيضا في هذا الإصدار:

```
GM2#show crypto gdoi gm replay
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value : 621388.66 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs


TBAR Error History (sampled at 10pak/min):
19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
peer_pst=619767.09 secs; win=4
```

ملاحظة: تم تنفيذ التحسينات المذكورة سابقا في Cisco IOS-XE بواسطة فرع تصحيح الأخطاء من Cisco [CSCun49335](https://tools.cisco.com/bugsearch/bug/CSCun49335) وفي Cisco IOS بواسطة فرع تصحيح الأخطاء من Cisco [CSCub91811](https://tools.cisco.com/bugsearch/bug/CSCub91811).
بالنسبة لإصدارات Cisco IOS التي لم تحتوي على هذه الميزة، يمكن **أن** يوفر أيضا **إعادة تشغيل لتفاصيل** Debug crypto gdoi gm هذه المعلومات، رغم أن تصحيح الأخطاء هذا يطبع معلومات TBAR لجميع حركة المرور (وليس فقط الحزم التي تم إسقاطها بسبب فشل TBAR)، لذلك قد لا يكون من الممكن تشغيلها في بيئة إنتاج.

```
GDOI:GM REPLAY:DET:(0):my_pseudotime is 621602.30 (secs), peer_pseudotime is 621561.14
(secs), replay_window is 4 (secs), src_addr = 192.168.14.2, dest_addr = 192.168.13.2
```

2. بمجرد تحديد مصدر الحزمة، يجب أن تكون على إدراك على العثور على تشفير GM. ثم ينبغي مراقبة الطابع الزمني الزائف على كل من تشفير أو فك تشفير الآلية العالمية من أجل أي انحراف ممكن في الزمن الزجري. وأفضل طريقة للقيام بذلك هي مزامنة كل من GMs و KS مع NTP، وتجميع معلومات الوقت الزائف بصورة دورية مع ساعة ماظم مرجعي عليها لك لتحديد ما إذا كانت المشكلة ناجمة عن انحراف الساعة على GMs.

GM1

```
GM1#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.469 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.26 secs
Input Packets : 0 Output Packets : 0
```

```
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

جي إم 2

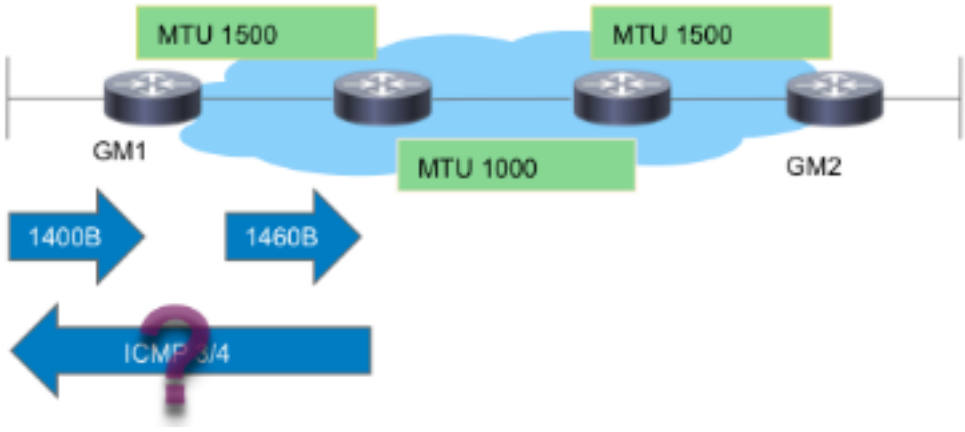
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

في المثال السابق، إذا كان الوقت الكاذب (كما تشير إليه قيمة الإعادة) مختلف بشكل كبير بين GMs عندما يتم التقاط المخرجات بنفس الوقت المرجعي، ثم يمكن أن تعزى المشكلة إلى انحراف الساعة.

> **ملاحظة**: في النظام الأساسي لموجه الخدمات المجمعة (Cisco) 1000 Series، بسبب بنية النظام الأساسي، يشير datapath الموجود على معالج تدفق الكم (QFP) بالفعل إلى ساعة الحائط لعد حزم الوقت الكاذب. وقد تسبب ذلك في حدوث مشاكل مع TBAR عندما يتغير وقت ساعة الحائط بسبب مزامنة NTP. وثقت هذه المشكلة مع cisco ق id CSCum37911.

حفظ رأس PMTUD و GETVPN

باستخدام GETtvpn، العمل الكشاف MTU للمسار (PMTUD) بين تشفير GMs وفك تشفيرها، ويمكن للحزم الكبيرة باستخدام مجموعة بت عدم التجزئة (DF) أن تصبح سوداء. يرجع السبب في أن هذا العمل إلى حفظ رأس GETVPN حيث يتم الاحتفاظ بعناوين مصدر/وجهة البيانات في رأس تضمين ESP. وهذا موضح في هذه الصورة:



كما تظهر الصورة، ينهار PMTUD مع GETVPN مع هذا التدفق:

1. تصل حزمة البيانات الكبيرة على تشفير GM1.
2. تتم إعادة توجيه حزمة ESP بعد التشفير من GM1 وتتم تسليمها إلى الوجهة.
3. إذا كان هناك إرتباط عبور مع IP MTU بقيمة 1400 بايت، فسيتم إسقاط حزمة ESP، وسيتم إرسال حزمة ICMP 3/4 ذات رسالة كبيرة للغاية نحو مصدر الحزمة، وهو مصدر حزمة البيانات.
4. يتم إسقاط حزمة ICMP3/4 إما بسبب عدم إستبعاد ICMP من نهج تشفير GETVPN، أو

إسقاطه من قبل المضيف الطرفي لأنه لا يعرف أي شيء حول حزمة ESP (حمولة غير مصدق عليها).

وباختصار، لا يعمل PMTUD مع GETVPN اليوم. in order to عملت حول هذا إصدار، cisco يوصي هذا steps:

1. قم بتنفيذ "ip tcp adjust-mss" لتقليل حجم مقطع حزمة TCP لعدد مرات الاستيعاب مصروفات التشفير العامة والحد الأدنى للمسار MTU في شبكة النقل.
2. امسح بت DF في حزمة البيانات عند وصولها إلى تشفير GM لتجنب PMTUD.

مشاكل مستوى بيانات IPsec العامة

يشبه معظم أستكشاف أخطاء مستوى بيانات IPsec وإصلاحها أنفاق IPsec التقليدية من نقطة إلى نقطة. إحدى المشكلات الشائعة هي ٪CRYPTO-4-RECVD_PKT_MAC_ERR. راجع syslog "٪CRYPTO-4-RECVD_PKT_MAC_ERR:" رسالة الخطأ مع فقدان إختبار الاتصال عبر أستكشاف أخطاء نفق IPsec وإصلاحها للحصول على مزيد من تفاصيل أستكشاف الأخطاء وإصلاحها.

مشكلات معروفة

يمكن إنشاء هذه الرسالة عند إستلام حزمة IPsec لا تطابق SPI في SADB. راجع معرف تصحيح الأخطاء من Cisco CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPsec الذي تم الإعلام عنه ل PKT الذي لا يطابق التدفق. مثال على ذلك:

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
vrf/dest_addr= /192.168.14.2, src_addr= 192.168.13.2, prot= 50
```

يجب أن تكون هذه الرسالة ٪CRYPTO-4-RECVD_PKT_INV_SPI، وهو ما يتم الإبلاغ عنه ل IPsec التقليدي وكذلك على بعض الأنظمة الأساسية للأجهزة مثل ASR. تم إصلاح هذه المشكلة التجميلية بواسطة معرف تصحيح الأخطاء من Cisco CSCup80547: خطأ في إرسال تقرير CRYPTO-4-RECVD_PKT_NOT_IPsec ل ESP PAK.

ملاحظة: يمكن أن تظهر هذه الرسائل أحيانا بسبب خطأ GETvpn آخر CSCup34371: موقع GETVPN GM بإيقاف إلغاء تجزئة حركة المرور بعد مفتاح TEK.

في هذه الحالة، لا يمكن ل GM فك تشفير حركة مرور GETtvpn، رغم أن لها IPsec SA صالح في SADB (يتم إعادة تكوين SA). تختفي المشكلة بمجرد انتهاء صلاحية SA وإزالتها من SADB. تتسبب هذه المشكلة في انقطاع كبير، لأن مفتاح TEK يتم أداؤه مسبقا. على سبيل المثال، يمكن أن يكون الانقطاع 22 دقيقة في حالة مدة بقاء TEK التي تبلغ 7200 ثانية. راجع وصف الخطأ للشرط المحدد الذي يجب تلبيته لمواجهة هذا الخطأ.

أستكشاف أخطاء GETVPN وإصلاحها على الأنظمة الأساسية التي تعمل بنظام التشغيل Cisco IOS-XE

أوامر استكشاف الأخطاء وإصلاحها

تحتوي الأنظمة الأساسية التي تعمل بنظام Cisco IOS-XE على عمليات تنفيذ خاصة بالأنظمة الأساسية، وغالبا ما تتطلب تصحيح بيانات خاص بالنظام الأساسي لمشاكل GetVPN. فيما يلي قائمة بالأوامر المستخدمة عادة لاستكشاف أخطاء GETVPN وإصلاحها

عل ى الأنظمة الأساسية التالية:

show crypto eli all

إظهار إحصائيات نوع IPsec لبرنامج النظام الأساسي

إظهار المخزون النشط ل IPsec لبرنامج النظام الأساسي

إظهار ميزة QFP النشطة ل IPsec على جهاز النظام الأساسي الكل

إظهار إحصائيات QFP النشطة لأجهزة النظام الأساسي واضحة

إظهار ميزة QFP النشطة لأجهزة النظام الأساسي واضح

show crypto ipsec sa

show crypto gdoi

إظهار التشفير الداخلي ل IPsec

debug crypto ipSec

خطأ تصحيح أخطاء التشفير في بروتوكول IPsec

حالات تصحيح أخطاء التشفير إلى ipSec

رسالة تصحيح أخطاء التشفير إلى ipSec

debug crypto ipSec hw-req

تفاصيل تصحيح أخطاء تشفير gdoi تحت الحمراء

debug crypto gdoi gm rekey detail

القضايا المشتركة ل ASR1000

فشل تثبيت نوع IPsec (إعادة التسجيل المستمرة)

قد يستمر ASR1000 GM في التسجيل إلى الخادم الرئيسي إذا لم يدعم محرك التشفير سياسة IPsec أو الخوارزمية التي تم تلقيها. على سبيل المثال، في منصات ASR المستندة إلى Nitrox (مثل ASR1002)، ال يتم دعم سياسات Suite-B أو SHA2 وهذا يمكن أن يتسبب في أعراض إعادة التسجيل المستمرة.

مشكلات شائعة تتعلق بالترحيل/الترقية

تحديد شريط ASR1000

على النظام الأساسي ASR1000، قدم إصلاح معرف الأخطاء من Cisco CSCum37911 قيد على هذا النظام الأساسي حيث يكون وقت الشريط أقل من 20 ثانية غير مدعوم. راجع قيود GetVPN على IOS-XE.

تم فتح أطخ التعزيز هذا لرفع هذا التقييد، معرف تصحيح الأخطاء من Cisco CSCuq25476 - يحتاج ASR1k إلى دعم حجم نافذة شريط GETVPN أقل من 20 ثانية.

تحديث: تم رفع هذا التقييد منذ ذلك الحين مع إصلاح معرف تصحيح الأخطاء من Cisco CSCur57558، ولم يعد قيد في XE3.13.2 و XE3.10.5 والرمز اللاحق.

لاحظ أيضا، ل GM الذي يعمل على cisco IOS-XE منصة (ASR1k أو ISR4k)، من المستحسن بشدة أن يركض الجهاز إصدارا مع الإصلاح لهذه المشكلة إذا تم تمكين TBAR؛ معرف تصحيح الأخطاء من Cisco CSCut91647 - GETVPN على IOS-XE: GM يسقط الحزم بشكل غير صحيح بسبب فشل TBAR.

مسألة تصنيف ISR4x00

تم العثور على تراجع على النظام الأساسي ISR4x00 حيث يتم تجاهل سياسات الرفض. لمزيد من التفاصيل، راجع معرف تصحيح الأخطاء من Cisco CSCut14355 - GETVPN - ISR4300 GM يتجاهل سياسة الرفض.

معلومات ذات صلة

- Cisco Group Encrypted Transport VPN (GET VPN) - أنظمة
- 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).