أستكشاف مشاكل GETVPN الشائعة وإصلاحها

المحتويات

المقدمة

يصف هذا وثيقة ما تصحيح الأخطاء أن يجمع لأغلب المجموعة المشتركة يشفر نقل GETVPN) VPN) إصدار.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Getvpn
- إستخدام خادم Syslog

المكونات المستخدمة

لا 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.

معلومات أساسية - أدوات أستكشاف أخطاء GetVPN وإصلاحها

يوفر GETtvpn مجموعة شاملة من أدوات أستكشاف الأخطاء وإصلاحها لتسهيل 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 بالأساليب الأقل تدخلا، حتى لا تتأثر بيئة الإنتاج سلبا. وللمساعدة في هذه العملية، يصف هذا القسم بعض الأدوات المتاحة الشائعة الاستخدام:

أدوات تصحيح أخطاء مستوى التحكم

إظهار الأوامر

يتم إستخدام أوامر العرض بشكل شائع لعرض عمليات وقت التشغيل في بيئة GETVPN.

Syslogs

يحتوي GETtvpn على مجموعة محسنة من رسائل syslog لأحداث البروتوكول الهامة وحالات الخطأ. يجب أن يكون هذا دائما أول مكان للبحث قبل تشغيل أي تصحيح أخطاء.

تتبع أحداث أحداث GDOI) Group domain of Interpretation)

تمت إضافة هذه الميزة في الإصدار T(3)15.1. يوفر تتبع الأحداث إمكانية تتبع منخفضة الوزن ودائمة لأحداث GDOI وأخطائها المهمة. هناك أيضا تتبع مسار الخروج مع تمكين traceback لظروف الاستثناء.

تصحيح الأخطاء الشرطي ل GDOI

تمت إضافة هذه الميزة في الإصدار T(3)15.1. وهو يسمح بتصحيح الأخطاء التي تمت تصفيتها لجهاز معين استنادا إلى عنوان النظير، ويجب إستخدامه دائما عند الإمكان، وخاصة على الخادم الرئيسي.

التشفير العام وتصحيح أخطاء GDOI

هذه هي كل عمليات تصحيح أخطاء GETVPM المختلفة. يجب على المسؤولين توخي الحذر عند تصحيح الأخطاء في البيئات واسعة النطاق. مع تصحيح أخطاء GDOI، يتم توفير خمسة مستويات تصحيح أخطاء لمزيد من تصحيح التحبب:

```
? GM1#debug crypto gdoi gm rekey
          all-levels All levels
            detail Detail level
              error Error level
              event Event level
            packet Packet level
              terse Terse level
```

مستوى تصحيح الأخطاء	ما ستحصل عليه
الخطأ	شروط الخطأ
خرشنة	رسائل هامة إلى المستخدم ومشكلات البروتوكول
حدث	حالات الانتقال والأحداث مثل مفاتيح الإرسال والاستقبال
التفاصيل	معلومات رسائل تصحيح

الأخطاء الأكثر تفصيلا يتضمن تفريغ معلومات الحزمة التفصيلية	حزمة
كل ما سبق	الكل

أدوات تصحيح أخطاء مستوى البيانات

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 CEF) IP Cisco Express Forwarding)
- التقاط الحزمة المضمنة (EPC)
- تصحيح أخطاء مستوى البيانات (تصحيح أخطاء حزم IP و CEF)

استكشاف الأخطاء وإصلاحها

إعداد مرافق التسجيل وأفضل الممارسات الأخرى

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

تحقق من مقدار الموجه للذاكرة الحرة، وقم بتكوين **تصحيح الأخطاء المخزن مؤقتا للتسجيل** إلى قيمة كبيرة (40 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 فواصل زمنية منتظمة، كل 20 دقيقة إلى ساعة، لمنع فقدان السجل بسبب إعادة إستخدام المخزن المؤقت.

- أيا كان ما يحدث، فأدخل الأمر **show tech** من أعضاء المجموعة المتأثرة (GM) والخوادم الأساسية (KSs)، وفحص إخراج الأمر **show ip route** في الوضع العام وكل توجيه وإعادة توجيه ظاهري (VRF) متضمن، إذا كان هناك حاجة إلى أي منهما.

- أستخدم بروتوكول وقت الشبكة (NTP) لمزامنة الساعة بين جميع الأجهزة التي تم تصحيح أخطائها. تمكين الطوابع الزمنية بالمللي 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 إنشاء IKE وإصلاحها

عندما تبدأ عملية التسجيل، تتفاوض GMs و KSs على جلسات تبادل مفتاح الإنترنت (IKE) من أجل حماية حركة مرور GDOI.

- تحقق من إنشاء IKE بنجاح على GM:

```
gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
GDOI_REKEY 1068 ACTIVE 172.16.1.1 172.16.1.9
GDOI_IDLE 1067 ACTIVE 172.16.1.9 172.16.1.1
```

ملاحظة: تنقطع حالة خمول_GDOI، التي هي أساس التسجيل، بسرعة وتختفي لأنه لم تعد هناك حاجة إليها بعد التسجيل الأولي.

- على KS، يجب أن ترى:

```
ks1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
GDOI_IDLE 1001 ACTIVE 172.16.1.9 172.16.1.1
```

ملاحظة: لا تظهر جلسة المفتاح إلا عندما تكون هناك حاجة إليها على KS.

أتمت هذا steps إن لا يبلغ أنت أن حالة:

- للحصول على رؤية حول سبب الفشل، تحقق من مخرجات هذا الأمر:
  `router# show crypto isakmp statistics`
- إذا كانت الخطوة السابقة غير مفيدة، فيمكنك الحصول على رؤى على مستوى البروتوكول إذا قمت بتمكين عمليات تصحيح أخطاء IKE المعتادة:
  `router# debug crypto isakmp`

ملاحظات:

* على الرغم من إستخدام IKE، فإنه لا يستخدم على المنفذ UDP/500 المعتاد، بل على المنفذ UDP/848.

* إذا واجهت مشكلة في هذا المستوى، فقم بتوفير تصحيح الأخطاء لكل من KS و GM المتأثرة.

- نظرا للاعتماد على موقعي Rivest-Shamir-Adleman (RSA) لمفاتيح المجموعة، **يجب أن يكون** ل KS مفتاح RSA تم تكوينه، ويجب أن يكون له نفس الاسم كالذي تم تحديده في تكوين المجموعة.

دخلت in order to فحصت هذا، هذا أمر:

```
ks1# show crypto key mypubkey rsa
```

أستكشاف أخطاء التسجيل الأولي وإصلاحها

على GM، للتحقق من حالة التسجيل، قم بفحص إخراج هذا الأمر:

```
gm1# show crypto gdoi | i Registration status
Registration status  : Registered
gm1#
```

إذا كان الإخراج يشير إلى أي شيء غير **مسجل**، فأدخل الأوامر التالية:

حول جنرال موتورز:

- إيقاف تشغيل الواجهات التي تم تمكين التشفير عليها.
تحذير: من المتوقع تمكين الإدارة خارج النطاق.

- تمكين تصحيح الأخطاء التالي:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
```

- قم بتمكين تصحيح الأخطاء على جانب KS (راجع القسم التالي).

- عندما تكون أخطاء KS جاهزة، قم بإلغاء تشغيل الواجهات التي تم تمكين التشفير، وانتظر التسجيل (من أجل تسريع العملية، قم بإصدار الأمر **clear crypto gdoi** على GM).

على KSs:

- تحقق من وجود مفتاح RSA على KS:

```
ks1# show crypto key mypubkey rsa
```

- تمكين تصحيح الأخطاء التالي:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
```

أستكشاف المشاكل المتعلقة بالسياسة وإصلاحها

تحدث مشكلة في النهج قبل التسجيل (المرتبط بنهج إغلاق الفشل)

هذا إصدار فقط يؤثر GMs، لذلك جمع هذا إنتاج من ال GM:

```
gm1# show crypto ruleset
```

ملاحظة: في Cisco IOS-XE؟، يكون هذا الإخراج دائما فارغا نظرا لأن تصنيف الحزمة لم يتم في البرنامج.

يوفر إخراج الأمر **show tech** من الجهاز المتأثر باقي المعلومات المطلوبة.

تحدث مشكلة في النهج بعد التسجيل، وتتصل بالنهج العام الذي يتم دفعه

وهناك عادة طريقتان تتجلى فيهما هذه المشكلة:

- ولا يستطيع بنك إنجلترا أن يدفع السياسات إلى الآلية العالمية.
- وهناك تطبيق جزئي لهذه السياسة فيما بين الآلية العالمية.

للمساعدة على أستكشاف أخطاء أي من هذه المشاكل وإصلاحها، أكمل الخطوات التالية:

1. اجمع هذا الناتج على GM المتضرر:

```
gm1# show crypto gdoi acl
gm1# show crypto ruleset
```

2. تمكين تصحيح الأخطاء التالي على GM:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm acls packet
```

3. على KS التي تسجل فيها الآلية العالمية المتأثرة، اجمع هذا الناتج:

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks policy
```

ملاحظة: لتحديد أي KS يتصل به GM، أدخل أمر **show crypto gdoi group**.

4. على ال نفسه KS، مكنت هذا يضبط:

```
ks1# debug crypto gdoi infra packet
```

```
ks1# debug crypto gdoi ks acls packet
```

5. إجبار GM على التسجيل مع هذا الأمر على GM:

```
clear crypto gdoi
```

تحدث مشكلة في النهج بعد التسجيل، وتتعلق بدمج النهج العام والتخطيات المحلية

عادة ما تظهر هذه المشكلة في شكل رسائل تشير إلى تلقي حزمة مشفرة تشير السياسات المحلية لها إلى أنه لا يفترض تشفيرها والعكس صحيح. جميع البيانات المطلوبة في القسم السابق ومطلوب **إخراج** الأمر **show tech** في هذه الحالة.

أستكشاف مشاكل مفتاح الإصلاح وإصلاحها

حول جنرال موتورز:

- تجميع تصحيح الأخطاء التالي:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- أدخل هذا الأمر للتحقق من أن GM لا يزال لديه اقتران أمان IKE (SA) من النوع gdoi_REKEY:

```
gm1# show crypto isakmp sa
```

على KSs:

- قم بتجميع إخراج الأمر **show crypto key mypubkey rsa** من **كل** KS. من المتوقع أن تكون المفاتيح **متطابقة**.

- دخلت هذا يضبط in order to شاهدت ما يقع على ال KS:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

أستكشاف أخطاء مكافحة إعادة التشغيل المستندة إلى الوقت وإصلاحها (TBAR)

تتطلب ميزة TBAR حفظ الوقت عبر المجموعات، وبالتالي تتطلب إعادة ضبط ساعات الوقت الزائفة ل GMs بشكل مستمر. ويتم ذلك خلال عملية التفكير أو كل ساعتين، أيهما يأتي أولا.

ملاحظة: يجب تجميع جميع المخرجات وتصحيح الأخطاء في نفس الوقت من كل من الآلية العالمية والهيئة كيما يمكن ربطها بشكل مناسب.

من أجل التحقيق في المشاكل التي تحدث على هذا المستوى، قم بجمع هذا الإخراج.

- حول جنرال موتورز:

```
gm1# show crypto gdoi
gm1# show crypto gdoi replay
```

- على KS:

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks replay
```

من أجل التحقيق في حفظ وقت TBAR بطريقة أكثر ديناميكية، قم بتمكين تصحيح الأخطاء التالية:

- عن مجلة موتورز:

```
gm1# debug crypto gdoi gm rekey packet
(gm1# debug crypto gdoi replay packet (verbosity might need to be lowered
```

- على KS:

```
ks1# debug crypto gdoi ks rekey packet
(ks1# debug crypto gdoi replay packet (verbosity might need to be lowered
```

اعتبارا من الإصدار T(3)15.2 من Cisco IOS، تمت إضافة القدرة على تسجيل أخطاء tbar، مما يسهل اكتشاف هذه الأخطاء. على ال GM، أستخدم هذا أمر in order to فحصت إن هناك أي خطأ TBAR:

```
R103-GM#show crypto gdoi gm replay
Anti-replay Information For Group GETVPN:
Timebased Replay:
Replay Value : 512.11 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00secs

TBAR Error History (sampled at 10pak/min):
No TBAR errors detected
```

للحصول على مزيد من المعلومات حول كيفية أستكشاف أخطاء TBAR وإصلاحها، ارجع إلى فشل مكافحة إعادة التشغيل المستند إلى الوقت.

أستكشاف أخطاء KS المتكررة وإصلاحها

وتشئ تعاونية (COOP) جلسة للمعهد من أجل حماية الاتصالات فيما بين شبكات الاتصالات السلكية واللاسلكية، ولذلك فإن أسلوب أستكشاف الأخطاء وإصلاحها الذي سبق وصفه لإنشاء هذا النظام ينطبق هنا أيضا.

يتضمن أستكشاف أخطاء COOP الخاصة وإصلاحها عمليات التحقق من إخراج هذا الأمر على جميع KSs المعنية:

```
ks# show crypto gdoi ks coop
```

ملاحظة: إن الخطأ الأكثر شيوعا الذي حدث عند نشر COOP KSs هو نسيان إستيراد مفتاح RSA نفسه (الخاص والعام) للمجموعة على جميع KSs. يسبب ذلك مشاكل أثناء القرود. للتحقق من المفاتيح العامة ومقارنتها بين KS، قارن إخراج الأمر **show crypto key mypubkey rsa** من كل KS.

إذا كان أستكشاف الأخطاء وإصلاحها على مستوى البروتوكول مطلوبا، فقم بتمكين تصحيح الأخطاء هذا على جميع KSs المعنية:

```
ks# debug crypto gdoi ks coop packet
```

أسئلة شائعة

لماذا ترى رسالة الخطأ هذه "تم رفض مصادقة إعادة المفتاح لتعيين ٪٪"؟

ترى رسالة الخطأ هذه عندما تقوم بتكوين KS بعد إضافة هذا السطر:

```
KS(gdoi-local-server)#rekey authentication mypubkey rsa GETVPN_KEYS
.Setting rekey authentication rejected %
```

سبب رسالة الخطأ هذه عادة لأن المفتاح المسمى GETVPN_KEYS غير موجود. لإصلاح ذلك، قم بإنشاء مفتاح بتسمية صحيحة باستخدام الأمر:

```
<crypto key generate rsa mod <modulus> label <label_name
```

ملاحظة: أضف الكلمة الأساسية القابلة للتصدير في النهاية إذا كان هذا نشر COOP ثم استورد نفس المفتاح في KS الأخرى

هل يمكن أن يعمل أيضا الموجه الذي تم تكوينه ك KS لمجموعة GETVPN واحدة ك GM لنفس المجموعة؟

لا. تتطلب جميع عمليات نشر GETVPN وجود KS مخصصة لا يمكن أن تشارك ك GM لنفس المجموعات. هذه الميزة غير مدعومة، نظرا لأن إضافة وظائف GM إلى KS مع جميع التفاعلات المحتملة مثل التشفير والتوجيه وجودة الخدمة (QoS) وما إلى ذلك، ليست مثالية لسلامة جهاز الشبكة الهام هذا. يجب أن يكون متوفرا في جميع الأوقات حتى يعمل نشر GETVPN بأكمله.

معلومات ذات صلة

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