Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" رسالة الخطأ أستكشاف الأخطاء وإصلاحها عبر نفق IPsec Loss

المحتويات

المقدمة

يوضح هذا المستند كيفية حل فقدان إختبار الاتصال عبر نفق IPsec المقترن برسائل "%CRYPTO-4-RECVD_PKT_MAC_ERR" في syslog كما هو موضح في المربع:

```
:May 23 11:41:38.139 GMT: %CRYPTO-4-RECVD_PKT_MAC_ERR
decrypt: mac verify failed for connection
id=2989 local=172.16.200.18 remote=172.16.204.18 spi=999CD43B
seqno=00071328
```

وتعتبر نسبة مئوية صغيرة من حالات السقوط هذه أمرا طبيعيا. ومع ذلك، يمكن أن يؤثر معدل الإسقاط المرتفع بسبب هذه المشكلة على الخدمة وقد يتطلب اهتمام مشغل الشبكة. لاحظ أن هذه الرسائل المبلغ عنها في syslogs محدودة بمعدل 30 ثانية لفواصل زمنية، لذلك لا تشير رسالة سجل واحد دائما إلى أنه تم إسقاط حزمة واحدة فقط. للحصول على عدد صحيح من عمليات الإسقاط هذه، قم بإصدار الأمر **show crypto ipSec detail**، وانظر إلى SA المجاور لمعرف الاتصال الذي يظهر في السجلات. من بين عدادات SA، **يتحقق pkts من** حسابات عداد الأخطاء **الفاشلة** لإجمالي إسقاط الحزمة بسبب فشل التحقق من رمز مصادقة الرسالة (MAC).

```
interface: GigabitEthernet0/1
Crypto map tag: MPLSWanGREVPN, local addr 172.16.204.18

(protected vrf: (none
(local ident (addr/mask/prot/port): (172.16.204.18/255.255.255.255/47/0
(remote ident (addr/mask/prot/port): (172.16.205.18/255.255.255.255/47/0
current_peer 172.16.205.18 port 500
{,PERMIT, flags={origin_is_acl
pkts encaps: 51810, #pkts encrypt: 51810, #pkts digest: 51810#
pkts decaps: 44468, #pkts decrypt: 44468, #pkts verify: 44468#
pkts compressed: 0, #pkts decompressed: 0#
```

```
                                pkts not compressed: 0, #pkts compr. failed: 0#
                            pkts not decompressed: 0, #pkts decompress failed: 0#
                                   pkts no sa (send) 0, #pkts invalid sa (rcv) 0#
                         pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0#
                               pkts invalid prot (recv) 0, #pkts verify failed: 8#
                        pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0#
                    pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0#
                                                pkts replay failed (rcv): 0#
                         pkts internal err (send): 0, #pkts internal err (recv) 0#

      local crypto endpt.: 172.16.204.18, remote crypto endpt.: 172.16.205.18
                      path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
                                    (current outbound spi: 0xD660992C(3596654892

                                                                :inbound esp sas
                                                       (spi: 0x999CD43B(2577191995
                                                , transform: esp-3des esp-sha-hmac
                                                   { ,in use settings ={Transport
          ,conn id: 2989, flow_id: AIM-VPN/SSL-3:2989, sibling_flags 80000006
                                                     crypto map: MPLSWanGREVPN
                                (sa timing: remaining key lifetime (k/sec): (4257518/24564
                                                                IV size: 8 bytes
                                                     replay detection support: N
                                                                  Status: ACTIVE

                                                                :outbound esp sas
                                                       (spi: 0xD660992C(3596654892
                                                , transform: esp-3des esp-sha-hmac
                                                   { ,in use settings ={Transport
          ,conn id: 2990, flow_id: AIM-VPN/SSL-3:2990, sibling_flags 80000006
                                                     crypto map: MPLSWanGREVPN
                                (sa timing: remaining key lifetime (k/sec): (4199729/24564
                                                                IV size: 8 bytes
                                                     replay detection support: N
                                                                  Status: ACTIVE
```

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الاختبارات التي تم إجراؤها على الإصدار M4(4)15.1 من Cisco IOS®. وعلى الرغم من عدم إختبارها بعد، إلا أنه يجب أن تعمل البرامج النصية والتكوين مع إصدارات برامج Cisco IOS السابقة أيضا لأن كلا التطبيقين يستخدمان الإصدار 3.0 من IM (والذي يتم دعمه في الإصدار T(22)12.4 أو إصدارا أعلى) من 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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات الميزة

يتضمن "CRYPTO-4-RECVD_PKT_MAC_ERR:Decrypt%" أنه تم تلقي حزمة مشفرة فشلت في التحقق من MAC. هذا التحقق هو نتيجة لمجموعة تحويل المصادقة التي تم تكوينها:

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5-hmac
```

في المثال المذكور أعلاه، يحدد *ESP-AES 256* خوارزمية التشفير على أنها AES من فئة 256 بت، وتعرف *esp-"* MD5 *md5"* (متغير HMAC) على أنها خوارزمية التجزئة المستخدمة للمصادقة. يتم إستخدام خوارزميات التجزئة مثل MD5 عادة لتوفير بصمة رقمية لمحتويات الملف. غالبا ما يتم إستخدام بصمة الإصبع الآلية لضمان عدم تغيير الملف بواسطة متسلل أو فيروس. لذلك فإن حدوث رسالة الخطأ هذه غالبا ما يعني إما:

- تم إستخدام المفتاح الخطأ لتشفير الحزمة أو فك تشفيرها. هذا الخطأ نادر جدا ويمكن أن يكون بسبب خطأ في البرنامج.

-أو-

- تم التلاعب بالحزمة أثناء النقل. قد يرجع سبب هذا الخطأ إلى وجود دائرة قذرة أو حدث عدائي.

منهجية أستكشاف الأخطاء وإصلاحها

بما أن رسالة الخطأ هذه يسببها عادة تلف الحزمة، فإن الطريقة الوحيدة لعمل تحليل سبب جذري هي إستخدام EPC للحصول على لقطات كاملة للحزم من جانب WAN على كلا نقطتي نهاية النفق ومقارنتهم. قبل الحصول على عمليات الالتقاط، من الأفضل تحديد نوع حركة المرور التي تشغل هذه السجلات. وفي بعض الحالات، يمكن أن يكون ذلك نوعا محددا من حركة المرور؛ وفي حالات أخرى، قد يكون عشوائيا ولكنه يمكن تكراره بسهولة (مثل قطرة 5-7 كل 100 تجسر). وفي مثل هذه الحالات، يصبح من الأسهل قليلا تحديد هذه المسألة. أفضل طريقة لتحديد المشغل هي تمييز حركة مرور الاختبار بعلامات DSCP والتقاط الحزم. يتم نسخ قيمة DSCP إلى رأس ESP ومن ثم يمكن تصفيتها باستخدام Wireshark. يمكن إستخدام هذا التكوين، والذي يفترض إجراء إختبار باستخدام 100 إختبار، لتعليم حزم ICMP:

```
ip access-list extended VPN_TRAFFIC
<permit icmp <source> <destination
class-map match-all MARK
match access-group name VPN_TRAFFIC
policy-map MARKING
class MARK
set dscp af21
```

يجب تطبيق هذا النهج الآن على واجهة الدخول حيث يتم تلقي حركة مرور البيانات الواضحة على موجه التشفير:

```
interface GigabitEthernet0/0
service-policy MARKING in
```

بدلا من ذلك، قد ترغب في تشغيل هذا الاختبار باستخدام حركة مرور يتم إنشاؤها بواسطة الموجه. لهذا، لا يمكنك إستخدام جودة الخدمة (QoS) لتعليم الحزم، ولكن يمكنك إستخدام التوجيه المستند إلى السياسة (PBR).

ملاحظة: لتحديد موقع علامات DSCP الهامة (5)، أستخدم عامل تصفية Wireshark **ip.dsfield.dscp == 0x28**.

```
ip access-list extended VPN_TRAFFIC
<permit icmp <source> <destination
route-map markicmp permit 10
match ip address vpn
set ip precedence critical
ip local policy route-map markicmp
```

بمجرد تكوين تمييز جودة الخدمة لحركة مرور ICMP لديك، يمكنك تكوين التقاط الحزمة المضمنة:

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host

Router(config)# permit ip host

.Router(config)#  exit //the capture is only configured in enable mode
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
.Router# monitor capture point start capo //starts the capture
"To stop replace the "start" keyword with "stop
```

ملاحظة: تم تقديم هذه الميزة في الإصدار 12.4(20)T من Cisco IOS. راجع التقاط الحزمة المضمنة للحصول على مزيد من المعلومات حول EPCs.

يتطلب إستخدام التقاط حزمة لاستكشاف أخطاء هذا النوع من المشاكل وإصلاحها التقاط الحزمة بالكامل، وليس مجرد جزء منها. تحتوي ميزة EPC في إصدارات Cisco IOS التي تسبق الإصدار 15.0(1)M على حد مخزن مؤقت يبلغ 512 كيلوبايت بحد أقصى لحجم الحزمة يبلغ 1024 بايت. لتجنب هذا التحديد، قم بالترقية إلى 15.0(1)M أو التعليمات البرمجية الأحدث، والتي تدعم الآن حجم مخزن الالتقاط المؤقت الذي يبلغ 100 متر بحد أقصى لحجم الحزمة يبلغ 9500 بايت.

إذا كان من الممكن نسخ المشكلة بشكل موثوق مع كل 100 إختبار اتصال، فإن أسوأ سيناريو هو جدولة نافذة صيانة للسماح فقط لحركة مرور ping كإختبار متحكم به والتقاط الصور. يجب ألا تستغرق هذه العملية سوى دقائق قليلة، ولكنها تتسبب في تعطيل حركة مرور الإنتاج لتلك الفترة. إذا كنت تستخدم تمييز جودة الخدمة، فيمكنك التخلص من متطلبات تقييد الحزم فقط على إختبارات الاتصال. in order to على قبض all the ping ربط في واحد مصد، أنت ينبغي ضمنت أن الاختبار لا ينجز أثناء ساعات الذروة.

إذا لم تكن المشكلة سهلة التوليد، أنت يستطيع استعملت IM نصي أن يدير الربط التقاط. النظرية هي أن تبدأ التقاط على كلا الجانبين في عازل دائري واستخدام IM لوقف الأسر على جانب واحد. وفي الوقت نفسه، توقف IM التقاط، جعلها ترسل فخ SNMP إلى النظير، الذي يوقف التقاطها. قد تنجح هذه العملية. ولكن إذا كان الحمل ثقيلا، فقد لا يستجيب الموجه الثاني بالسرعة الكافية لوقف الأسر. يفضل إجراء إختبار مضبوط. وفيما يلي نصوص البرنامج التنفيذي للعمليات المتكاملة التي ستنفذ العملية:

```
Receiver
========
event manager applet detect_bad_packet
"event syslog pattern "RECVD_PKT_MAC_ERR
"action 1.0 cli command "enable
"action 2.0 cli command "monitor capture point stop test
"!action 3.0 syslog msg "Packet corruption detected and capture stopped
"" action 4.0 snmp-trap intdata1 123456 strdata

Sender
======
```

```
event manager applet detect_bad_packet
.event snmp-notification oid 1.3.6.1.4.1.9.10.91.1.2.3.1.9
oid-val "123456" op eq src-ip-address 20.1.1.1
"action 1.0 cli command "enable
"action 2.0 cli command "monitor capture point stop test
"!action 3.0 syslog msg "Packet corruption detected and capture stopped
```

لاحظ أن الرمز الموجود في المربع السابق هو تكوين تم إختباره باستخدام M(1)15.0. قد تحتاج إلى إختباره باستخدام إصدار Cisco IOS المحدد الذي يستخدمه العميل قبل تنفيذه في بيئة العميل.

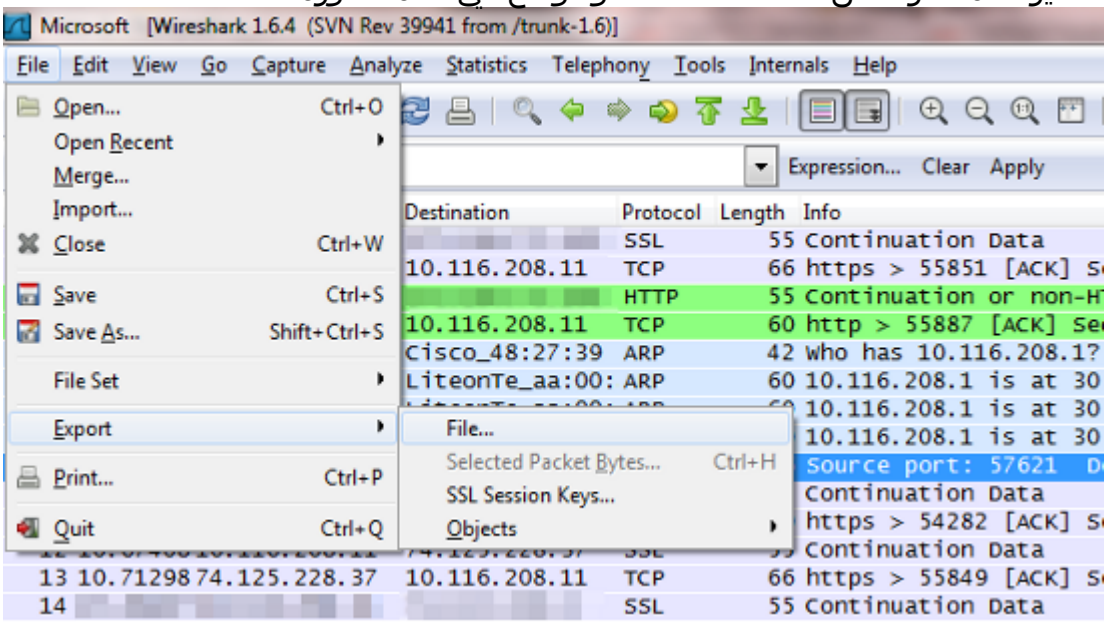
تحليل البيانات

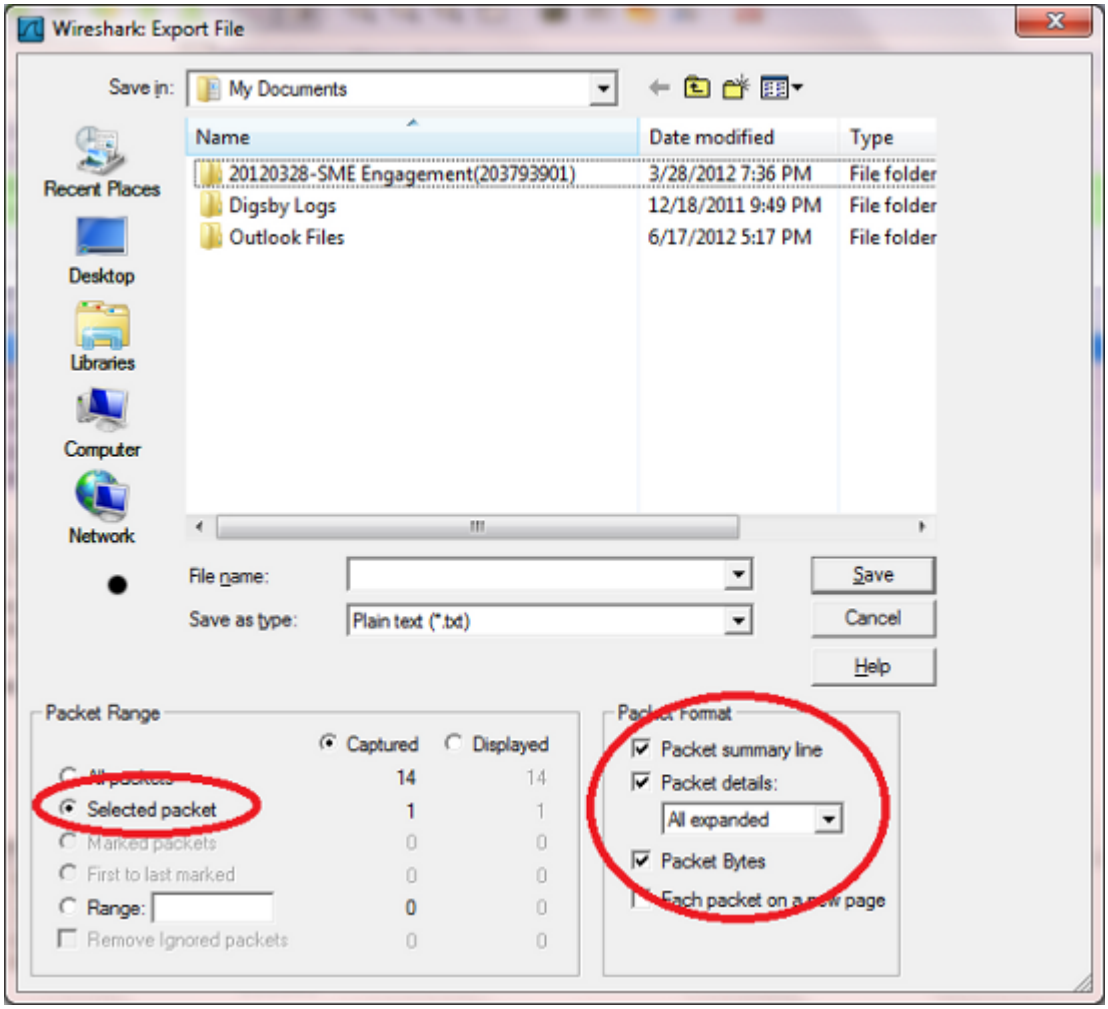
1. بمجرد اكتمال عمليات الالتقاط، أستخدم TFTP لتصديرها إلى جهاز كمبيوتر شخصي.
2. افتح الالتقاط باستخدام محلل بروتوكول شبكة (مثل Wireshark).
3. إذا تم إستخدام تمييز جودة الخدمة، قم بتصفية الحزم المقابلة.

```
ip.dsfield.dscp==0x08
```

"0x08" خاصة بقيمة AF21 لبروتوكول DSCP. إذا تم إستخدام قيمة DSCP مختلفة، يمكن الحصول على القيمة الصحيحة من التقاط الحزمة نفسها أو من قائمة مخطط تحويل قيم DSCP. راجع DSCP وقيم الأولوية للحصول على مزيد من المعلومات.

4. حدد إختبار الاتصال الذي تم إسقاطه على عمليات الالتقاط من المرسل، وحدد موقع الحزمة على عمليات الالتقاط على كل من جانب المستلم وجانب المرسل.
5. تصدير هذه الحزمة من كلا الالتقاط كما هو موضح في هذه الصورة:





6. عقد مقارنة ثنائية بين الاثنين. إذا كانت متطابقة، فلن تكون هناك أخطاء أثناء النقل وقد قام برنامج Cisco IOS بإلقاء قيمة سلبية خاطئة على الطرف المتلقي أو إستخدام المفتاح الخطأ على نهاية المرسل. في كلتا الحالتين، الإصدار هو خطأ Cisco IOS. إن يكون الربط مختلف، بعد ذلك الربط كنت عبثت مع في بيث.

هنا الربط بما أن هو ترك ال crypto محرك على ال FC:

```
                                :Mar  1 00:01:38.923: After encryption*
                                  .......05F032D0: 45000088 00000000 E
 .05F032E0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a
$.05F032F0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z
05F03300: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
05F03310: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
+05F03320: 09CE001B 70CC56AB 746D6A3A 63C2652B .N..pLV+tmj:cBe
05F03330: 1992E8AF 2CE2A279 46367BDB 660854ED ..h/,b"yF6{[f.Tm
.05F03340: 77B69453 83E47778 1470021F 09436285 w6.S.dwx.p...Cb
.!].05F03350: CB94AEF5 20A65B1F 480D86F6 125BA12E K..u &[.H..v
```

هنا نفس الربط كما إستلمت على النظير:

```
.......4F402C90:                    45000088 00000000          E
 .4F402CA0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a
$.4F402CB0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z
4F402CC0: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
4F402CD0: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
........+4F402CE0: 09CE001B 70CC56AB 00000000 00000000 .N..pLV
................ 4F402CF0: 00000000 00000000 00000000 00000000
................ 4F402D00: 00000000 00000000 00000000 00000000
................ 4F402D10: 00000000 00000000 00000000 00000000
```

عند هذه النقطة، من المرجح أن تكون مشكلة موفر خدمة الإنترنت (ISP)، ويجب أن تشارك هذه المجموعة في أستكشاف الأخطاء وإصلاحها.

مشاكل مشتركة

- يصف معرف تصحيح الأخطاء من CSCed87408 Cisco مشكلة في الجهاز مع محرك التشفير على 83xs حيث تكون الحزم الصادرة العشوائية تالفة أثناء التشفير، مما يؤدي إلى أخطاء المصادقة (في الحالات التي يتم فيها إستخدام المصادقة) وحالات إسقاط الحزم على نهاية الاستلام. من المهم أن تدرك أنك لن ترى هذه الأخطاء على 83x نفسها، ولكن على جهاز الاستقبال.

- في بعض الأحيان تظهر الموجهات التي تشغل التعليمات البرمجية القديمة هذا الخطأ. يمكنك الترقية إلى إصدارات الرموز الأحدث مثل 15.1(4) M4 لحل المشكلة.

- أعجزت in order to دققت إن المشكلة يكون جهاز أو برمجية إصدار، جهاز تشفير. إذا إستمرت رسائل السجل، فستكون هناك مشكلة في البرنامج. وإذا لم تكن هناك مساحة، فيجب أن تقوم وحدة الإدارة عن بعد بحل المشكلة.
تذكر أنه إذا قمت بتعطيل تشفير الأجهزة، فقد يؤدي ذلك إلى انخفاض حاد في الشبكة الخاصة بأنفاق الشبكة الخاصة الظاهرية (VPN) المحملة بشكل كبير. لذلك، توصي Cisco بمحاولة الإجراءات الموضحة في هذا المستند أثناء نافذة صيانة.

معلومات ذات صلة

- 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).