المرحلة 5 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: نهج SSL

المحتويات

المقدمة

هذه المقالة هي جزء من سلسلة مقالات توضح كيفية أستكشاف مسار البيانات في أنظمة FirePOWER وإصلاحها بشكل منهجي لتحديد ما إذا كانت مكونات FirePOWER قد تؤثر على حركة المرور. يرجى الرجوع إلى مقالة "نظرة عامة" للحصول على معلومات حول بنية الأنظمة الأساسية FirePOWER وارتباطاتها بمقالات "أستكشاف أخطاء مسارات البيانات وإصلاحها" الأخرى.

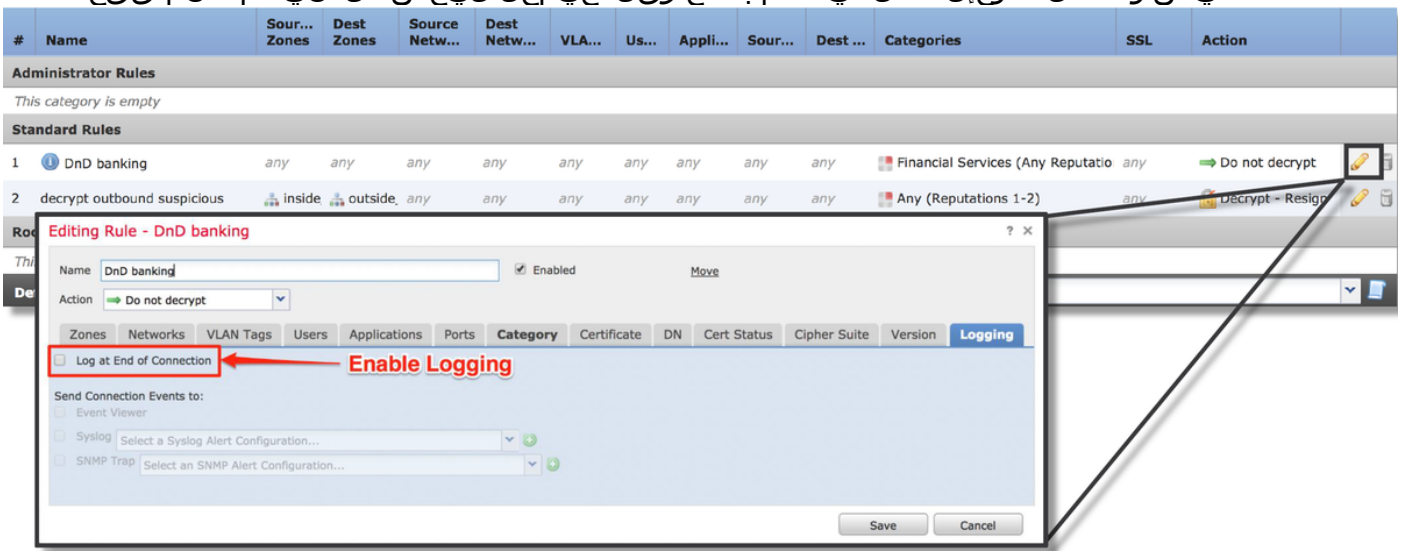
تغطي هذه المقالة المرحلة الخامسة من أستكشاف أخطاء مسار بيانات FirePOWER وإصلاحها، وهي ميزة نهج طبقة آخذ التوصيل الآمنة (SSL).

المتطلبات الأساسية

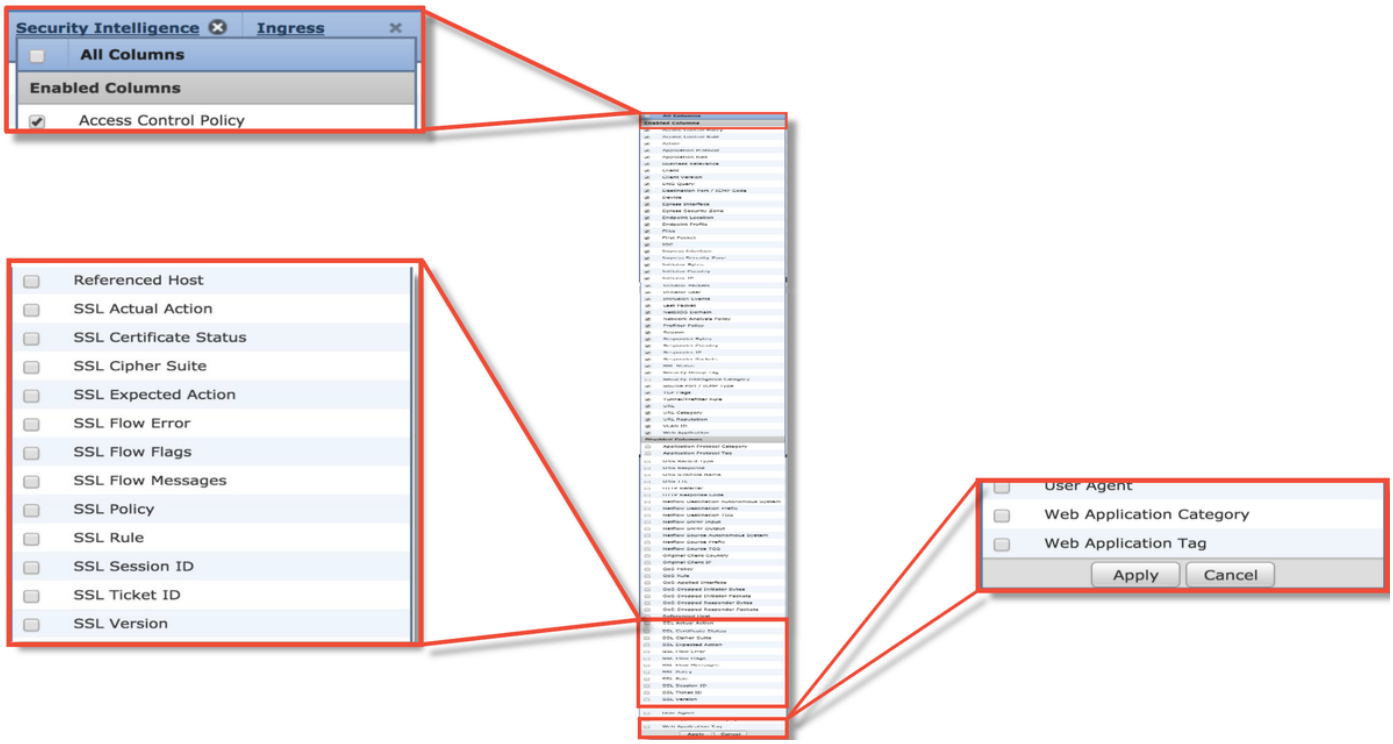
- تنطبق المعلومات الواردة في هذه المقالة على أي منصة Firepower كفك تشفير SSL متوفر فقط في جهاز الأمان القابل للتكيف (ASA) مع خدمات FirePOWER (وحدة SFR) في 6.1+ ميزة "تعديل ترحيب العميل" متوفرة في الإصدار 6.0+

- تأكيد إستخدام نهج SSL في نهج التحكم في الوصول

- تحقق من تمكين التسجيل لجميع القواعد، بما في ذلك "الإجراء الافتراضي"



- تحقق من علامة التبويب إجراءات إلغاء التشفير لمعرفة ما إذا تم تعيين أي خيار لحظر حركة المرور
- في أحداث الاتصال، عندما تكون في طريقة عرض الجدول لأحداث الاتصال، قم بتمكين كافة الحقول ذات 'SSL' في الاسم
  يتم تعطيل معظم هذه الخدمات بشكل افتراضي ويجب تمكينها في عارض أحداث الاتصال



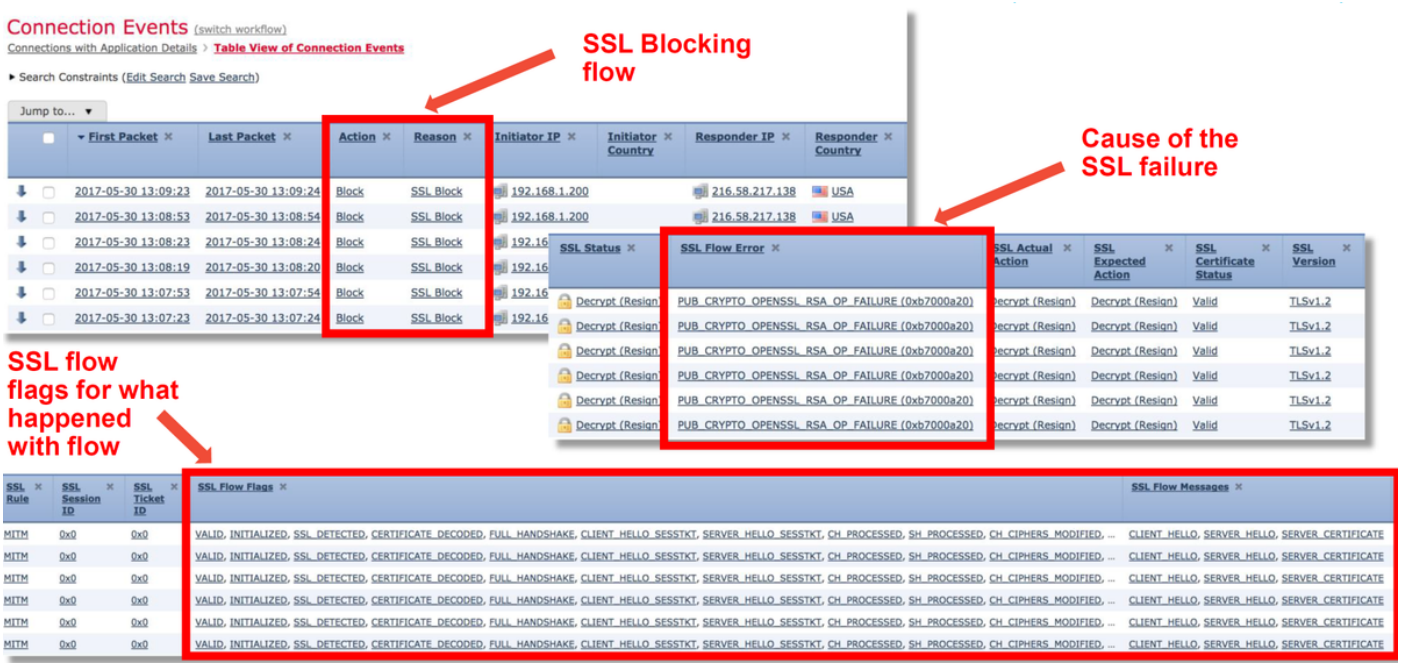
أستكشاف أخطاء مرحلة نهج SSL وإصلاحها

يمكن اتباع خطوات محددة للمساعدة في فهم لماذا قد تقوم سياسة SSL بإسقاط حركة المرور المتوقع السماح بها.

التحقق من حقول SSL في أحداث الاتصال

إذا كان يشتبه في أن سياسة SSL تتسبب في مشاكل في حركة المرور، فإن المكان الأول الذي يجب فحصه وهو قسم أحداث الاتصال (تحت **التحليل > الاتصالات > الأحداث**) بعد تمكين جميع حقول SSL، كما هو موضح أعلاه.

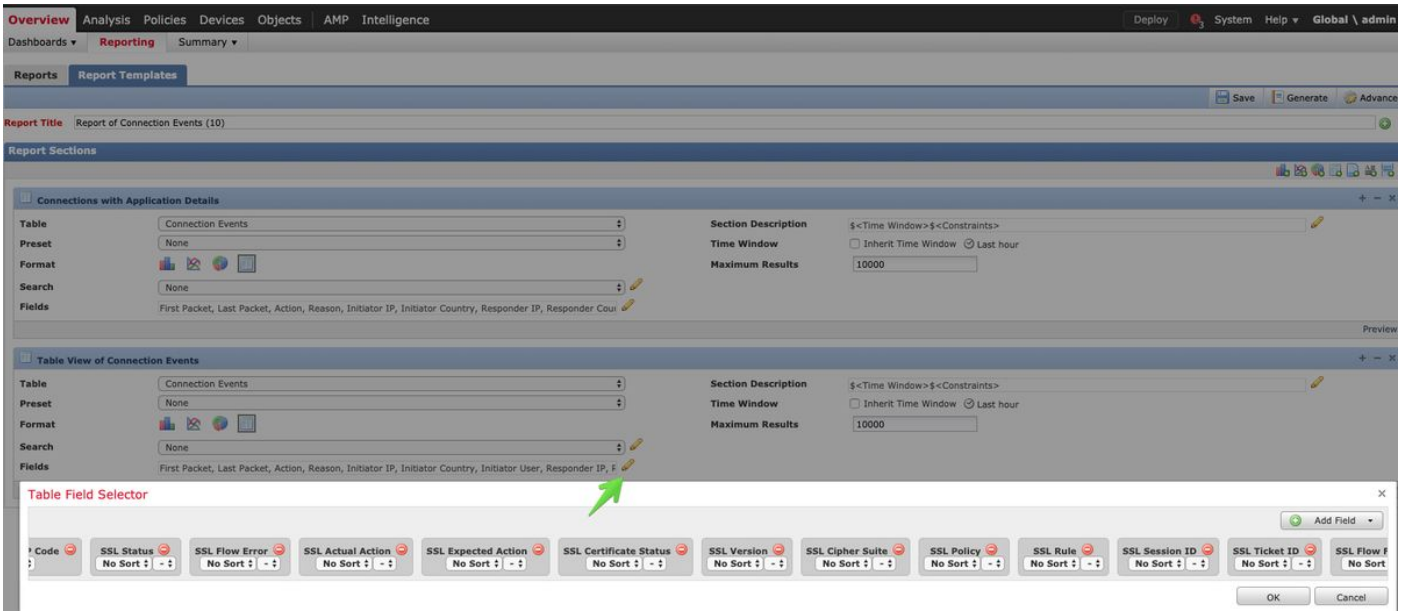
إذا كان نهج SSL يمنع حركة المرور، يعرض حقل **السبب** "كتلة SSL". يحتوي عمود خطأ تدفق **SSL** على معلومات مفيدة حول سبب حدوث الكتلة. تحتوي حقول SSL الأخرى على معلومات حول بيانات SSL التي اكتشفها FirePOWER في التدفق.



يمكن توفير هذه البيانات إلى مركز المساعدة التقنية (TAC) من Cisco عند فتح حالة لسياسة SSL. من أجل تصدير هذه المعلومات بسهولة، يمكن إستخدام زر **مصمم التقرير** الموجود في الركن العلوي الأيمن.

إذا تم النقر فوق هذا الزر من قسم "أحداث الاتصال"، يتم نسخ المرشحات وخيارات الإطار الزمني إلى قالب التقرير تلقائيا.

تأكد من إضافة كافة حقول SSL المذكورة في القسم "الحقل".



انقر على **إنشاء** لإنشاء تقرير عن تنسيقات PDF أو CSV.

تصحيح نهج SSL

إذا لم تحتوي أحداث الاتصال على معلومات كافية حول التدفق، يمكن تشغيل تصحيح SSL على واجهة سطر أوامر Firepower (CLI).

ملاحظة: يستند كل محتوى تصحيح الأخطاء أدناه إلى فك تشفير SSL الذي يحدث في البرنامج على بنية x86. الـ يتضمن هذا المحتوى تصحيح أخطاء من ميزات إلغاء تحميل أجهزة SSL التي تمت إضافتها في الإصدار 6.2.3 وما بعده، والتي تختلف.

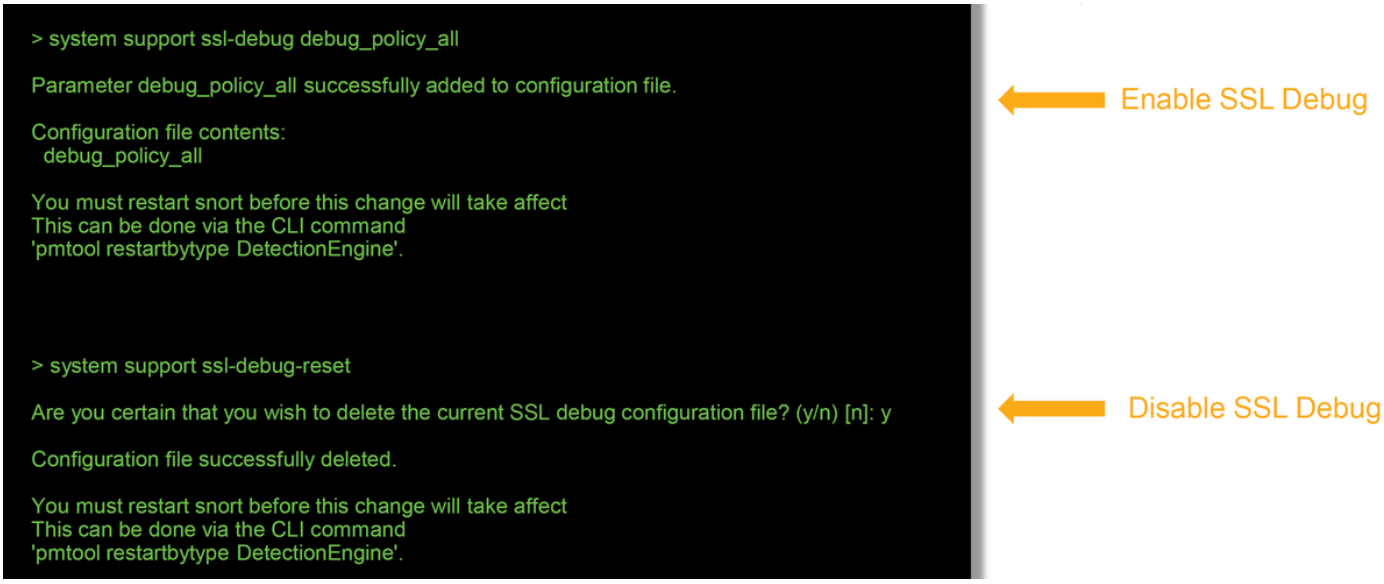
ملاحظة: في النظام الأساسي Firepower 9300 و 4100، يمكن الوصول إلى القشرة المعينة من خلال الأوامر التالية:

 # وحدة تحكم الوحدة النمطية Connect 1
Firepower-module1> **Connect ftd**
>

باالنسبة للمثيالت المتعددة، يمكن الوصول إلى واجهة سطر الأوامر (CLI) الخاصة بالجهاز المنطقي باستخدام الأوامر التالية.
 # Connect Module 1 telnet
Firepower-module1> **Connect ftd ftd1**
يتم الآن الاتصال بوحدة تحكم ftd(ftd1) للحاوية... أدخل "exit" للعودة إلى واجهة سطر الأوامر (CLI) الخاصة بالتمهيد
>

يمكن تشغيل الأمر **System support ssl-debug debug_policy_all** لإنشاء معلومات تصحيح الأخطاء لكل تدفق تتم معالجته بواسطة نهج SSL.

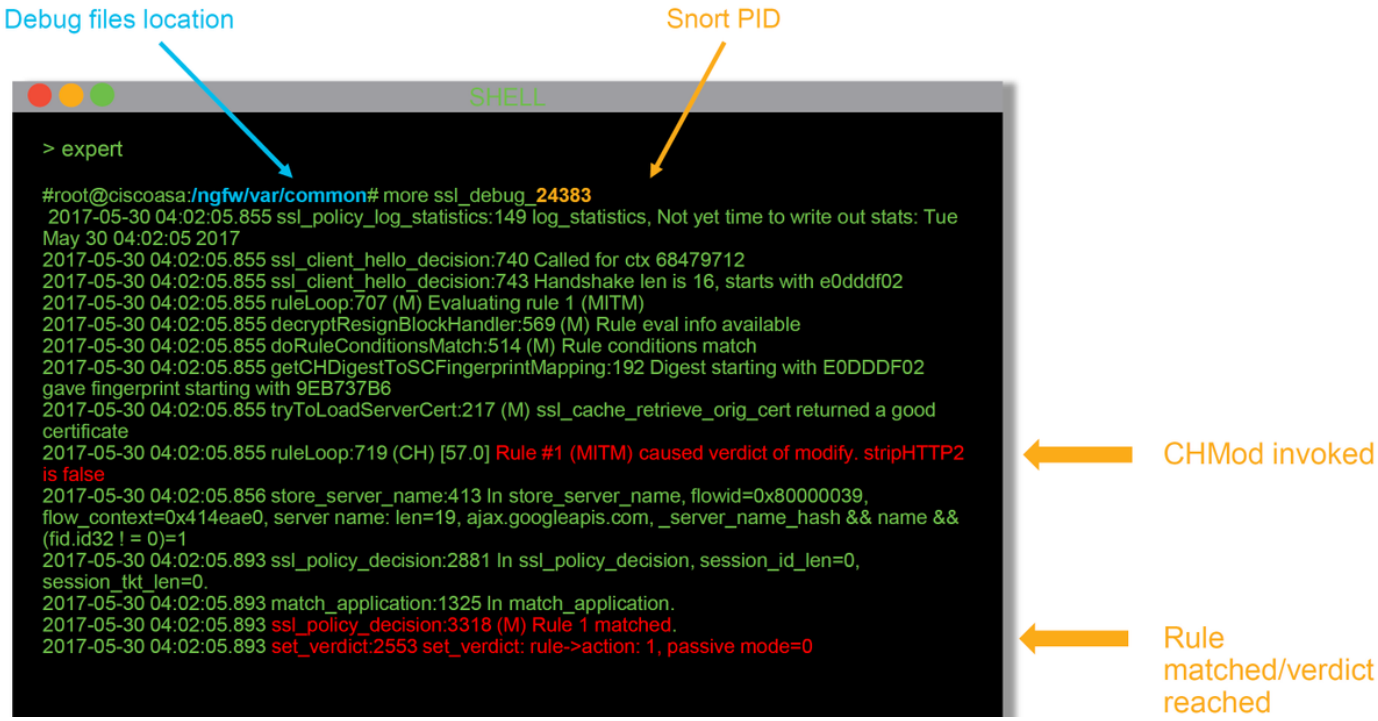
تحذير: يجب إعادة تشغيل عملية النموذج قبل تشغيل تصحيح أخطاء SSL وبعد تشغيله، مما يمكن أن يتسبب في إسقاط بعض الحزم وفقا لسياسات النموذج والنشر المستخدمة. سيتم إعادة إرسال حركة مرور TCP، ولكن يمكن أن تتأثر حركة مرور UDP بشكل سلبي إذا لم تتسامح التطبيقات التي تمر عبر جدار الحماية مع الحد الأدنى من فقدان الحزمة.



تحذير: لا تنس إيقاف تشغيل تصحيح الأخطاء بعد تجميع البيانات الضرورية باستخدام الأمر **system support ssl-debug-reset**.

سيكون هناك ملف مكتوب لكل عملية شخير قيد التشغيل على جهاز FirePOWER. سيكون موقع الملفات:

- **/var/log/** للأنظمة الأساسية غير FTD
- **/ngfw/var/common/** لأنظمة FTD



هذه بعض الحقول المفيدة في سجلات تصحيح الأخطاء.

```
...
2017-05-30 04:02:05.893  Verdict callback.
 Logstr: ssl_policy_decision: Found matching rule.
   Process ID: 24383
   Flow context: 0x414eae0
   Flow info: 0x7ffea4b8ccf0
     flowid: 0x80000039
     error: 0x00000000
     cipher_suite: 49199 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     ssl_version: TLS1.2
     server_cert_h: 89
        cert summary: CN=*.googleapis.com;O=Google Inc;
     flags: 0x40820004048181c3/0x00000088c0000000
  Connection Event: 0x7ffea4b8c9e8 messages: 0x00000038
  Policy ID: 93a182e8-1d00-11e6-9e03-b6d00120637b
     Rule ID: 1
     Logging is on: 1
     Cipher Suite: 49199 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     SSL Version: 16 - TLS1.2
     Server Cert Status: 2 - valid ca chain,
     URL Category Matched: 0
     App ID Matched: 0
     Client Hello Server Name: (null)
     Actual Action: 6 - Decrypt and resign.
     Expected Action: 6 - Decrypt and resign.
     SSL Flow Status: 2 - success - SSL Rule successfully applied.
     SSL Flow Error: 0x00000000 - NSLIB:Logging [0x00000000;code:0;sub:0] Success;
     SSL Flow Messages: 0x00000038 - CLIENT_HELLO,SERVER_HELLO,SERVER_CERTIFICATE
```

Certificate summary can help identify the flow

Validate that Expected and Actual actions are the same

```
...
    SSL Flow Flags: 0x00000088c48181c3 -
VALID,INITIALIZED,SSL_DETECTED,CERTIFICATE_DECODED,FULL_HANDSHAKE,CLIENT_HELL
O_SESSTKT,SERVER_HELLO_SESSTKT,CH_PROCESSED,SH_PROCESSED,CH_CIPHERS_MO
DIFIED,CH_CURVES_MODIFIED,CH_EXTENSION_REMOVED,CH_ALPN_HAS_H2
    SSL Session ID:
    SSL Session Ticket:

  Network parameters:
     src_addr: 192.168.1.200
     src_port: 55113
     src_intf: 3
     src_zone: -1
     dst_addr: 216.58.218.234
     dst_port: 443
     dst_intf: 2
     dst_zone: -1
     vlan: 0
  Matching Rule:
     ordinal rule id: 1
     rule id: 1
     rule name: MITM
  Verdict:
      Flow action: 6 - Decrypt and resign.
      Error action: 2 - Block.
```

Verdict the flow reached

```
...
2017-05-30 04:02:05.894  Error callback.
 Logstr: ssl_policy_error_callback
   Process ID: 24383
   Flow context: 0x414eae0
   Flow info: 0x7ffea4b8d3a0
      flowid: 0x80000039
      error: 0xb7000a20
      FLOW ERROR FOUND:
          - NSE:PubCrypto [0xb7000a20;code:32;sub:10] OpenSSL RSA operation failure;
      cipher_suite: 65535 - Unknown
      ssl_version: UNKNOWN
      server_cert_h: -1
      flags: 0xca4a0407068181c5/0x00000088c0000000
     messages: 0x00000078
  Connection Event: 0x7ffea4b8d290
     Policy ID: 93a182e8-1d00-11e6-9e03-b6d00120637b
    [ ...Omitting for brevity ]
    SSL Flow Status: 10 - decryption_error - Error found during SSL flow after server certificate.
    SSL Flow Error: 0xb7000a20 - NSE:PubCrypto [0xb7000a20;code:32;sub:10] OpenSSL RSA
operation failure;
...
```

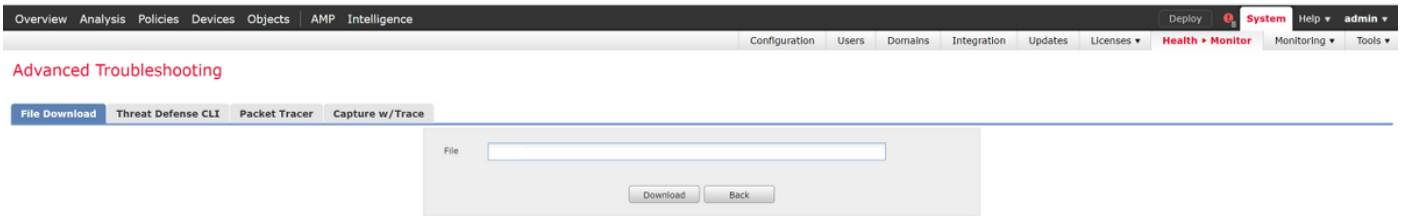
SSL Errors potentially causing drop

ملاحظة: في حالة حدوث خطأ في فك التشفير بعد بدء FirePOWER في فك التشفير، يجب إسقاط حركة مرور البيانات نظرا لأن جدار الحماية قد قام بالفعل بتعديل/إيقاف

جلسة العمل عن العمل عن بعد، لذا ال يمكن للعميل والخادم إستئناف الاتصال نظرا لوجود مكدسات TCP مختلفة لديهم وكذلك مفاتيح تشفير مختلفة مستخدمة في التدفق.

يمكن نسخ ملفات تصحيح الأخطاء من جهاز FirePOWER من موجه الأمر > باستخدام الاتجاهات الواردة في هذه المقالة.

بدلا من ذلك، هناك خيار على FMC في FirePOWER الإصدار 6.2.0 أو أكبر. للوصول إلى أداة UI المساعدة هذه على FMC، انتقل إلى **الأجهزة > إدارة الأجهزة**. ثم انقر فوق الرمز الموجود بجوار الجهاز المعني، يتبعه **أستكشاف الأخطاء وإصلاحها المتقدم > تنزيل الملف**. يمكنك بعد ذلك إدخال اسم الملف محل التساؤل والنقر فوق تنزيل.

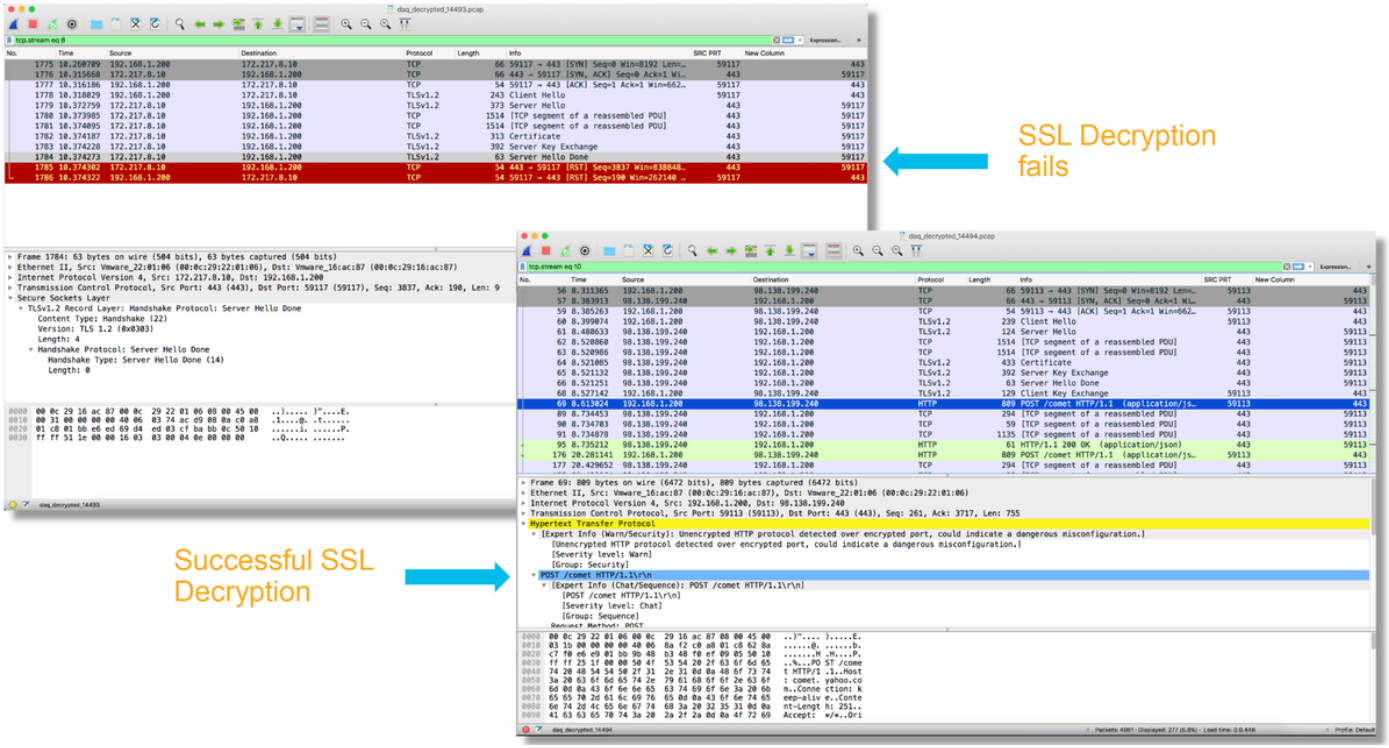


إنشاء التقاط حزمة تم فك تشفيرها

من الممكن تجميع التقاط حزمة غير مشفر لجلسات العمل التي يتم فك تشفيرها بواسطة FirePOWER. الأمر هو **دعم النظام debug-DAQ debug_daq_write_pcap**

تحذير: يجب إعادة تشغيل عملية الشخير قبل إنشاء التقاط الحزمة التي تم فك تشفيرها، والذي يمكن أن يتسبب في إسقاط بعض الحزم. يتم إعادة إرسال البروتوكولات المعبرة عن الحالة مثل حركة مرور TCP، ولكن يمكن أن تتأثر حركة المرور الأخرى، مثل UDP، سلبا.

```
> system support debug-DAQ debug_daq_write_pcap

Parameter debug_daq_write_pcap successfully added to configuration file.

Configuration file contents:
  debug_daq_write_pcap

You must restart snort before this change will take affect
This can be done via the CLI command
'system support pmtool restartbytype DetectionEngine'.

> system support pmtool restartbytype DetectionEngine

> expert
admin@firepower:~$ cd /var/common/
admin@firepower:/var/common$ ls
daq_decrypted_15903.pcap  daq_decrypted_15909.pcap

admin@firepower:/var/common$ tar pczf daq_pcaps.tgz daq_decrypted_*
```

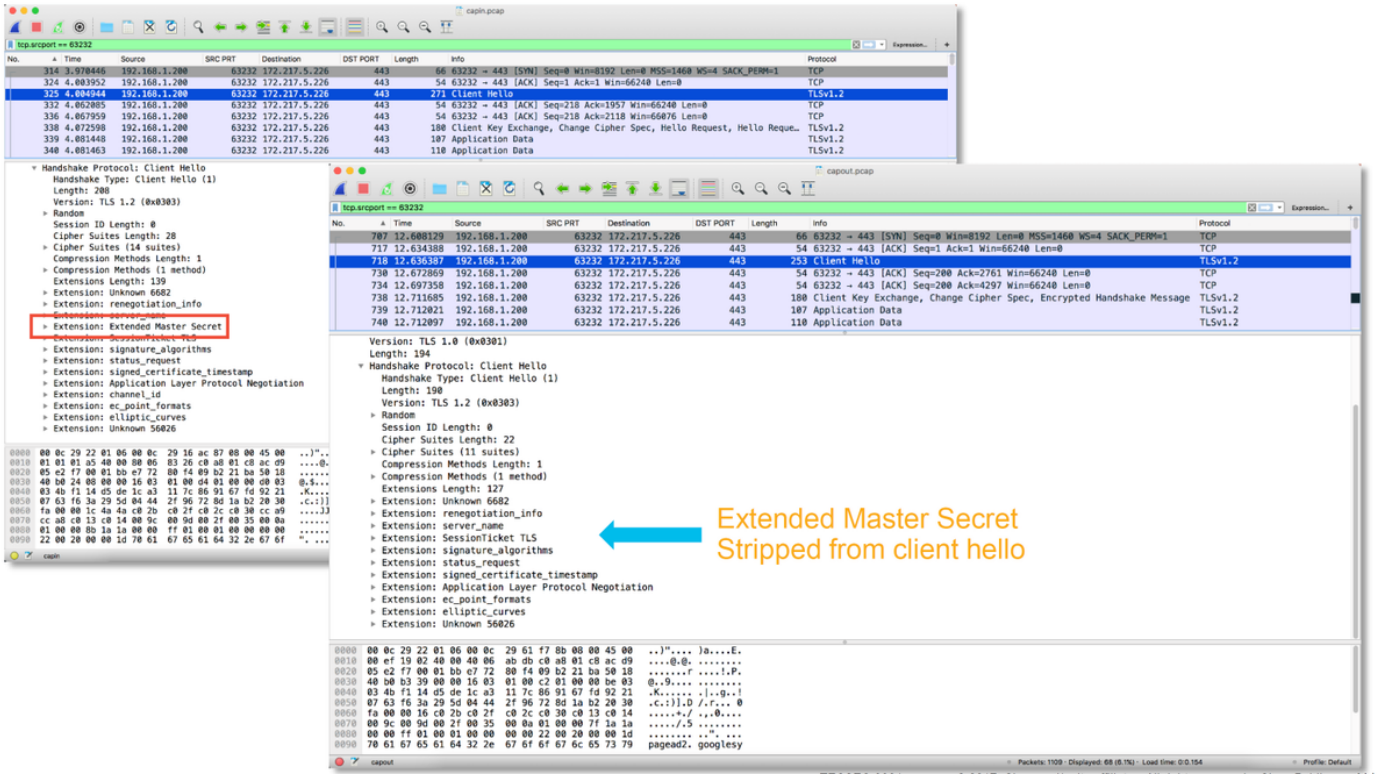


تحذير: قبل إرسال التقاط PCAP تم فك تشفيرها إلى TAC، يوصى بتصفية ملف الالتقاط وحده إلى التدفقات المسببة للمشاكل، لتجنب الكشف عن أي بيانات حساسة دون داع.

البحث عن تعديلات ترحيب العميل (CHMod)

يمكن أيضا تقييم التقاط الحزمة لمعرفة ما إذا كان أي تعديل على ترحيب العميل يحدث.

يصور التقاط الحزمة على اليسار ترحيب العميل الأصلي. تظهر تلك الموجودة على اليمين الحزم من جانب الخادم. لاحظ أنه قد تمت إزالة السر الرئيسي الموسع عبر ميزة CHMod في FirePOWER.



تأكد من أن العميل يثق في المرجع المصدق المستقيل لفك التشفير/الاستقالة

بالنسبة لقواعد سياسة SSL مع إجراء "فك تشفير - إستقالة"، تأكد من أن مضيفي العميل يثقون في "المرجع المصدق" (CA) المستخدم ك CA المستقيل. والـ ينبغي أن يكون لدى المستخدمين النهائيين أي إشارة إلى أنهم أصبحوا على وشك الدخول في حوار من خالل جدار الحماية. يجب أن يثقوا ب CA التوقيع. يتم فرض ذلك بشكل شائع من خالل نهج مجموعة Active Directory (AD) ولكنه يعتمد على سياسة الشركة والبنية الأساسية AD.

لمزيد من المعلومات، يمكنك مراجعة المقالة التالية، والتي تحدد كيفية إنشاء سياسة SSL.

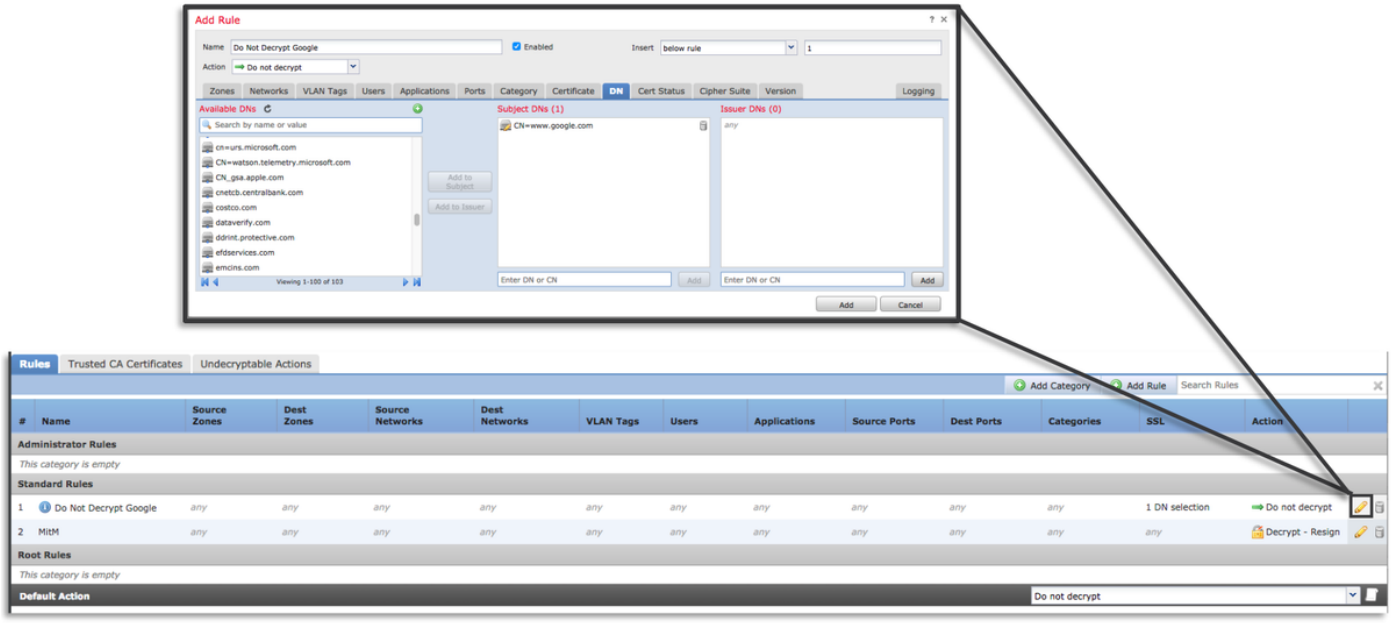
خطوات التخفيف

يمكن اتباع بعض خطوات التخفيف الأساسية من أجل:

- إعادة تكوين نهج SSL لعدم فك تشفير حركة مرور معينة
- إخراج بيانات معينة من حزمة ترحيب العميل حتى يتجح فك التشفير

إضافة قواعد عدم فك التشفير (DNd)

في سيناريو المثال التالي، تم تحديد أن حركة المرور إلى google.com تنكسر عند المرور عبر فحص سياسة SSL. تتم إضافة قاعدة، بناء على السم الشائع (CN) في شهادة الخادم حتى ال يتم فك تشفير حركة المرور إلى google.com.



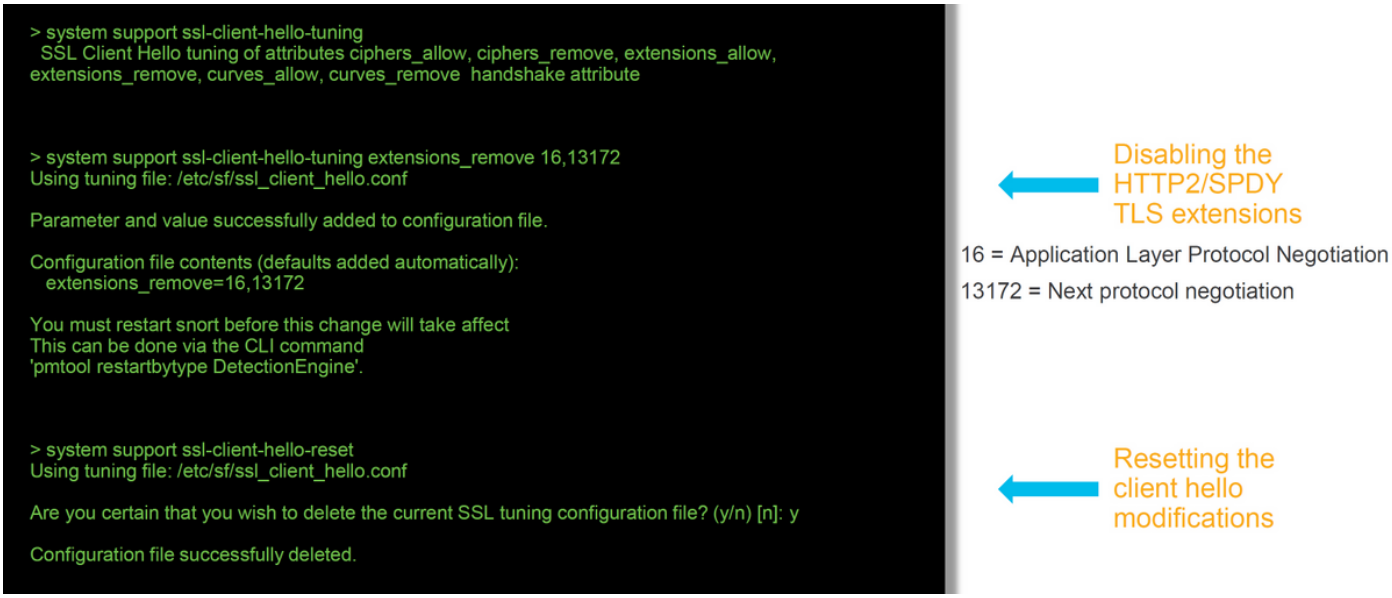
بعد حفظ النهج ونشره، يمكن اتباع خطوات أستكشاف الأخطاء وإصلاحها الموضحة أعلاه مرة أخرى لمعرفة ما يقوم به FirePOWER مع حركة المرور.

ضبط تعديل HELLO للعميل

في بعض الحالات، يمكن أن يكشف أستكشاف الأخطاء وإصلاحها عن وجود مشكلة في FirePOWER تتعلق بفك تشفير حركة مرور معينة. يمكن تشغيل الأداة المساعدة **لدعم النظام ssl-client-hello-tuning** على واجهة سطر الأوامر (CLI) لجعل FirePOWER يزيل بيانات معينة من حزمة HELLO الخاصة بالعميل.

في المثال التالي، تتم إضافة تكوين حتى تتم إزالة ملحقات TLS معينة. يتم العثور على المعرفات الرقمية من خلال البحث عن معلومات حول ملحقات TLS ومعاييرها.

> **تحذير**: يجب إعادة تشغيل عملية النخر قبل أن تصبح تغييرات تعديل ترحيب العميل سارية المفعول، والتي يمكن أن تتسبب في إسقاط بعض الحزم. يتم إعادة إرسال البروتوكولات المعبرة عن الحالة مثل حركة مرور TCP، ولكن يمكن أن تتأثر حركة المرور الأخرى، مثل UDP، سلبا.



لاستعادة أي تغييرات تم إجراؤها على إعدادات تعديل مرحبا للعميل، يمكن تنفيذ الأمر **system support ssl-client-hello-reset**.

البيانات التي سيتم تقديمها إلى TAC

تعليمات	البيانات
http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn	أستكشاف أخطاء الملفات وإصلاحها من مركز إدارة Firepower (FMC) وأجهزة FirePOWER
طالع هذه المقالة للحصول على تعليمات	تصحيح أخطاء SSL التقاط حزمة جلسة عمل كاملة (من جانب العميل وجهاز FirePOWER نفسه وجانب الخادم عند الإمكان)
http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-appliar	
طالع هذه المقالة للحصول على تعليمات	لقطات شاشة أو تقارير حدث الاتصال

الخطوة التالية

إذا تم تحديد أن مكون سياسة SSL ليس هو سبب المشكلة، فإن الخطوة التالية ستكون استكشاف أخطاء ميزة المصادقة النشطة وإصلاحها.

انقر هنا لمتابعة المقالة التالية.

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).