المرحلة 8 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: نهج تحليل الشبكة

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 النظرة العامة للحصول على معلومات حول بنية الأنظمة الأساسية FirePOWER والأجهزة الخاصة بمقالات أستكشاف أخطاء مسارات البيانات وإصلاحها الأخرى.

تغطي هذه المقالة المرحلة الثامنة من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها، وهي ميزة "سياسة تحليل الشبكة".

المتطلبات الأساسية

- تنطبق هذه المقالة على جميع منصات Firepower
  ال تتوفر ميزة **التتبع** إلا في الإصدار 6.2.0 من البرنامج وما بعده للنظام الأساسي للدفاع عن تهديد FirePOWER (FTD) فقط.
- معرفة مصدر الشخ المفتوح مفيدة، على الرغم من أنها غير مطلوبة لمزيد من المعلومات حول برنامج Open Source Snort، يرجى زيارة موقع https://www.snort.org/

أستكشاف أخطاء ميزة نهج تحليل الشبكة وإصلاحها

يحتوي نهج تحليل الشبكة (NAP) على إعدادات للمعالج المسبق تقوم بعمليات فحص

لحركة المرور، بناء على التطبيق المحدد. للمعالجات السابقة القدرة على إسقاط حركة المرور، بناء على التكوين. تتناول هذه المقالة كيفية التحقق من تكوين NAP والتحقق من حالات السقوط السابقة للمعالج.

> **ملاحظة**: تحتوي قواعد المعالج الأولي على معرف المولد (GID) بخلاف '1' أو '3' (أي 129 و 119 و 124). يمكن العثور على مزيد من المعلومات حول GID إلى تعيينات المعالجات السابقة في أدلة تكوين FMC.

إستخدام أداة "التتبع" للعثور على عمليات إسقاط المعالج الأولي (في FTD فقط)

يمكن إستخدام أداة **تتبع دعم النظام** لاكتشاف حالات السقوط التي تم إجراؤها على مستوى المعالجات السابقة.

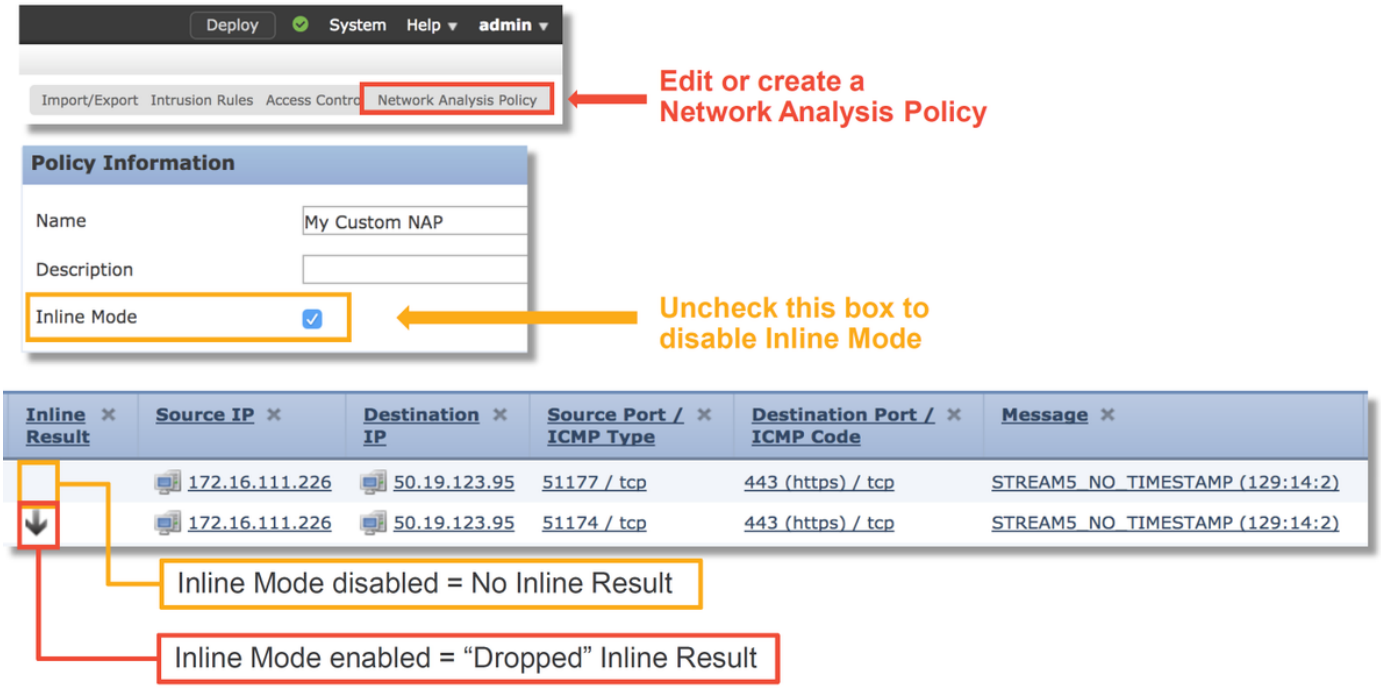
في المثال التالي، اكتشف معالج TCP المسبق للتطبيع وجود حالة شاذة. ونتيجة لذلك، يتم إسقاط حركة المرور بواسطة القاعدة **129:14**، والتي تبحث عن الطوابع الزمنية المفقودة داخل تدفق TCP.

```
> system support trace

[omitted for brevity…]

172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 - 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or
unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 AppID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 Starting with minimum 3, 'block urls', and SrcZone first with zones -1 -> -1, geo 0 ->
0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ===> Blocked by Stream
```

> **ملاحظة**: على الرغم من أن المعالج المسبق **لتكوين تدفق TCP** يقوم بإسقاط حركة المرور، إلا أنه قادر على القيام بذلك لأن المعالج المسبق **للتطبيع** داخل **الخط** تم تمكينه أيضا. لمزيد من المعلومات حول التطبيع الداخلي، يمكنك قراءة هذه المقالة.

التحقق من تكوين NAP

في واجهة المستخدم الخاصة بمركز إدارة Firepower (FMC)، يمكن عرض حماية الوصول (NAP) ضمن **السياسات > التحكم في الوصول > التطفل**. بعد ذلك، انقر فوق خيار **تحليل نوع الشبكة** في أعلى اليمين، وبعد ذلك يمكنك عرض برامج العمل الوطنية وإنشاء برامج جديدة وتحرير البرامج الموجودة.

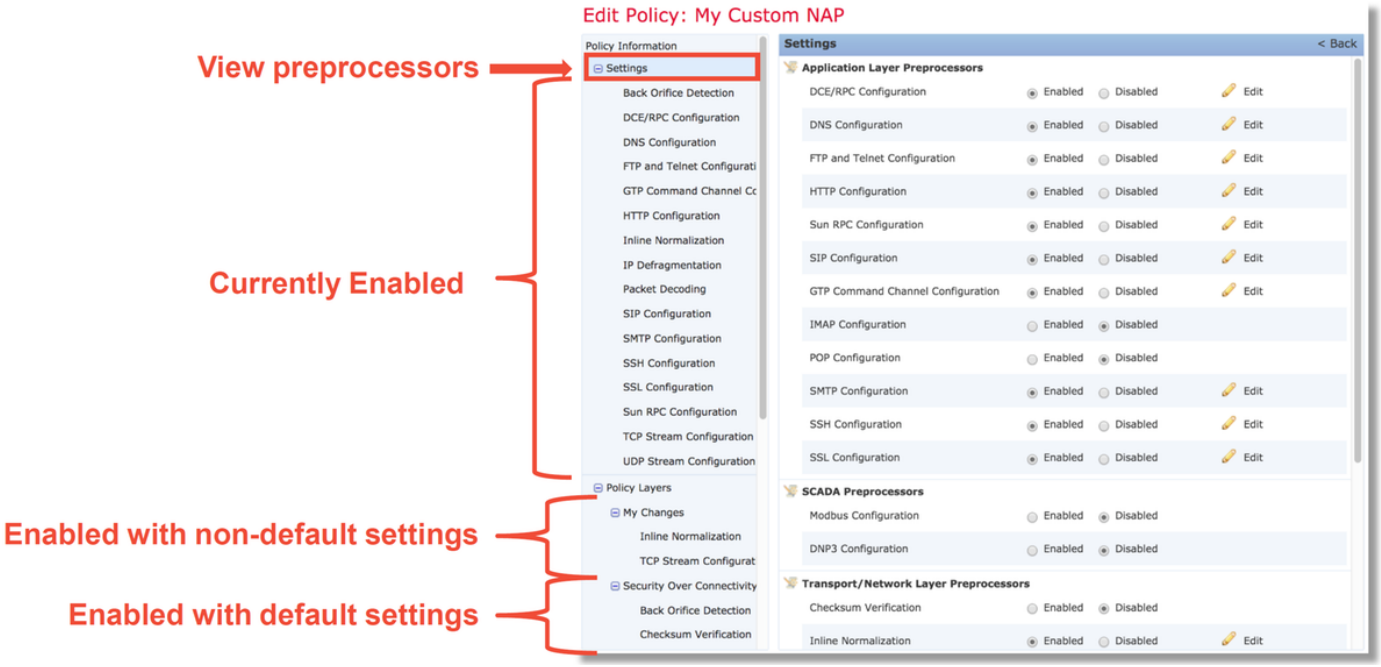


وكما هو موضح في الرسم التوضيحي أعلاه، تحتوي برامج العمل الوطنية على ميزة "الوضع الداخلي"، والتي تعادل خيار "إسقاط عندما تكون داخل السطر" في نهج التسلل. قد تكون خطوة تخفيف سريعة لمنع NAP من إسقاط حركة المرور هي إلغاء تحديد **الوضع المضمن**. ال تعرض أحداث التطفل التي تم إنشاؤها بواسطة NAP أي شيء في علامة التبويب **نتائج في السطر** مع تعطيل **الوضع المضمن**.

عرض إعدادات NAP

ضمن NAP، يمكنك عرض الإعدادات الحالية. يتضمن ذلك إجمالي معالجات Preprocessors المهيئة، متبوعا ب

معالجات مسبقة متاحة بإعدادات غير افتراضية (تلك التي تم نسخها يدويا) وتلك التي يتم تمكينها بالإعدادات الافتراضية، كما يرى في الرسم التوضيحي أدناه.

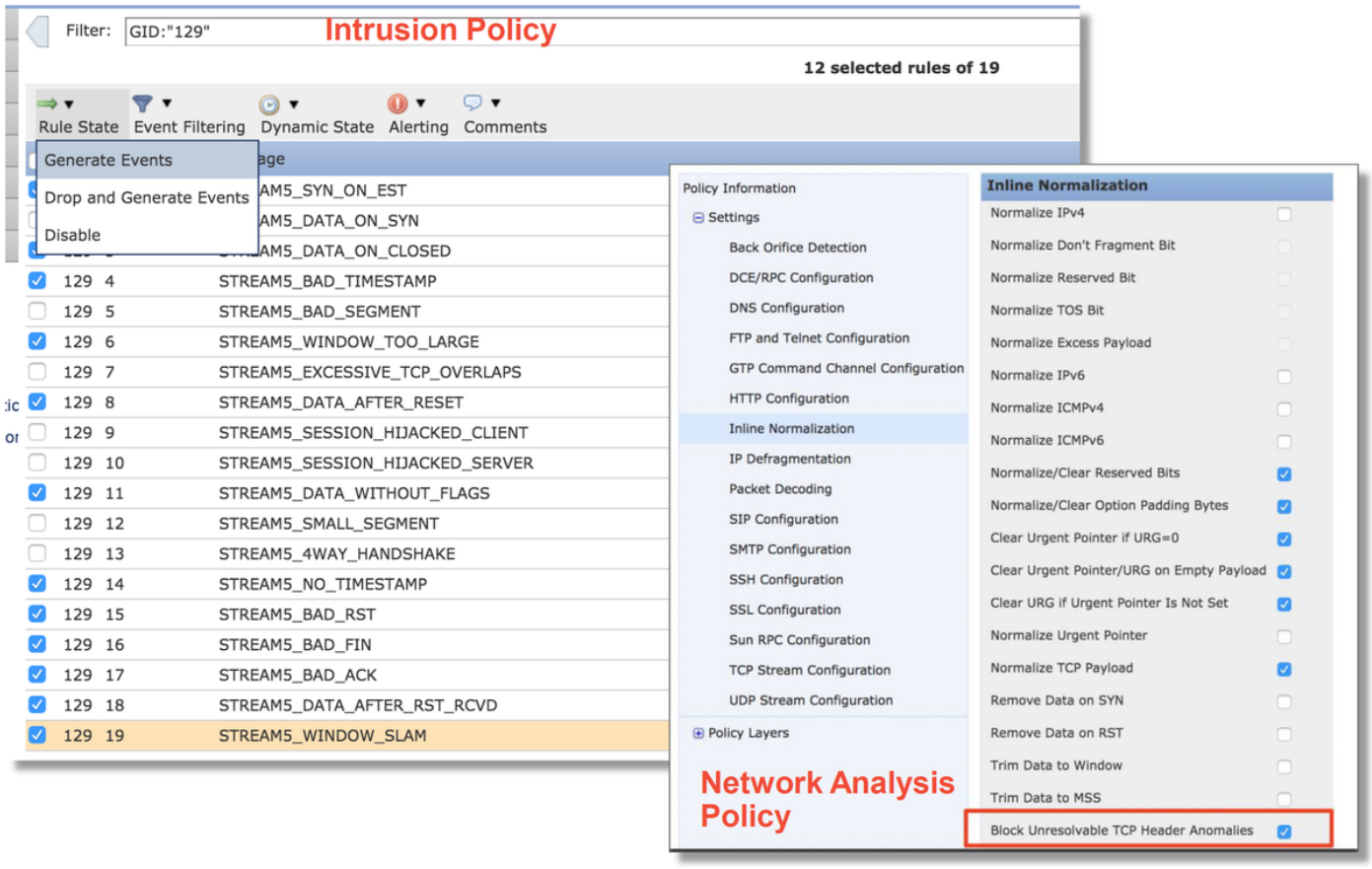


إعدادات NAP التي يمكن أن تتسبب في حالات السقوط الصامت

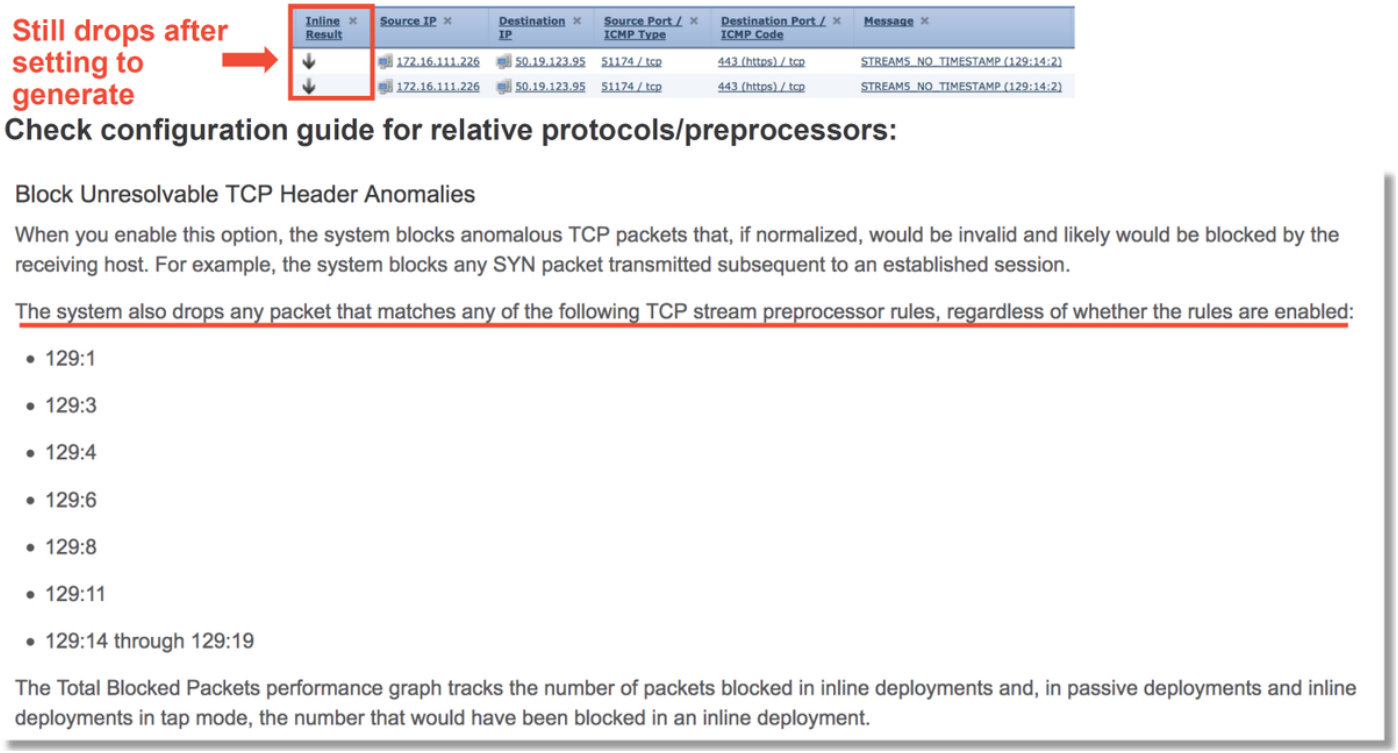
في المثال المذكور في قسم التتبع، تقوم قاعدة تكوين تدفق TCP **129:14** بإسقاط حركة المرور. ويتم تحديد ذلك من خلال النظر في مخرجات **تتبع دعم النظام**. ومع ذلك، إذا لم يتم تمكين القاعدة المذكورة ضمن سياسة الاقتحام المعنية، فلن يتم إرسال أي أحداث إقتحام إلى FMC.

يرجع السبب وراء حدوث هذا إلى إعداد داخل المعالج المسبق **للتسوية المضمنة** يسمى **منع حالات الشذوذ غير القابلة للحل الخاصة برأس TCP**. يتيح هذا الخيار بشكل أساسي لـ SNORT تنفيذ إجراء حظر عندما تكتشف بعض قواعد GID 129 حالات شاذة في تدفق TCP.

إذا تم تمكين **منع حالات عدم التناسب غير القابلة للحل الخاصة برأس TCP**، فمن المستحسن تشغيل قواعد GID 129 وفقا للتوضيح أدناه.



يؤدي تشغيل قواعد GID 129 إلى إرسال أحداث التطفل إلى FMC عند إتخاذ إجراء بشأن حركة المرور. ومع ذلك، طالما تم تمكين **حالات** عدم حل **رأس TCP**، فلا يزال إمكانية هذه الحالة إسقاط حركة المرور حتى إذا تم تعيين **حالة القاعدة** في نهج التسلل على **إنشاء الأحداث** فقط. ويتم شرح هذا السلوك في أداة تكوين FMC.



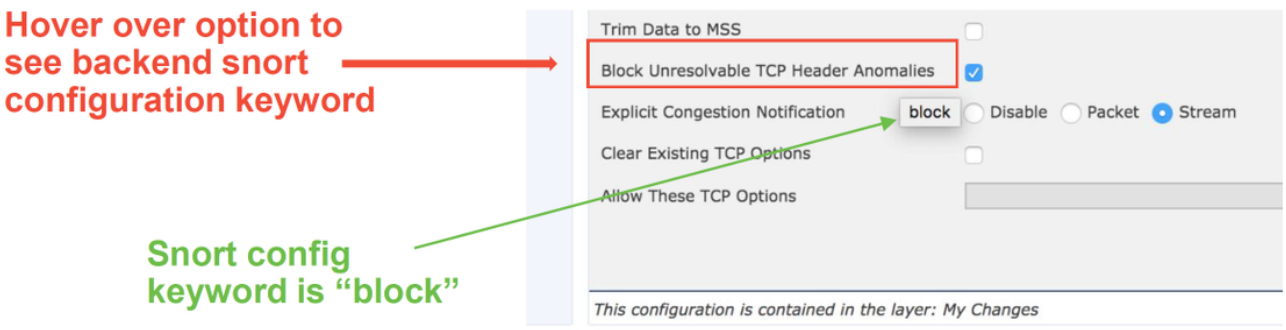
يمكن العثور على الوثائق المذكورة أعلاه في هذه الدفعة (للإصدار 6.4، الذي يعد أحدث إصدار في وقت نشر هذه المقالة).

التحقق من تكوين الطرف الخلفي

تتم إضافة طبقة أخرى من التعقيد إلى سلوك المعالج الأولي من خلال تمكين إعدادات معينة على الطرف الخلفي، دون أن تنعكس في FMC. هذه بعض الأسباب المحتملة.

- الخصائص الممكنة الأخرى لها القدرة على فرض تمكين إعدادات ما قبل المعالج (علما بأن الخصائص الرئيسية هي سياسة الملف)
- تتطلب بعض قواعد سياسة الاقتحام خيارات معينة للمعالج الأولي لإجراء الكشف
- قد يؤدي عيب ما إلى السلوك لقد رأينا مثالا واحدا على ذلك: CSCuz50295 - "سياسة الملف مع حظر البرامج الضارة تمكن TCP من التطبيع مع علامة الحظر"

قبل النظر إلى تكوين الطرف الخلفي، لاحظ أنه يمكن رؤية كلمات النورط الأساسية، المستخدمة في ملفات تكوين جهاز التنفس الخلفي، من خلال التحويم فوق إعداد محدد داخل برنامج NAP. يرجى الرجوع إلى الرسم التوضيحي التالي.



يترجم خيار **منع حالات عدم** توسيع **رأس TCP** في علامة التبويب NAP إلى الكلمة الأساسية **block** في الطرف الخلفي. مع وضع هذه المعلومات في الاعتبار، يمكن التحقق من تكوين الطرف الخلفي من طبقة الخبراء.

```
root@ciscoasa:~# de_info.pl

DE Name         : Primary Detection Engine (c9ef19d6-e187-11e6-ba76-99617d53da68)
DE Type         : ids
DE Description  : Primary detection engine for device c9ef19d6-e187-11e6-ba76-99617d53da68
DE Resources    : 1
DE UUID         : 0d82120c-e188-11e6-8606-a4827d53da68

root@ciscoasa:~# cd /var/sf/detection_engines/0d82120c-e188-11e6-8606-a4827d53da68/network_analysis/
root@ciscoasa: network_analysis# ls
b50f27b0-e31a-11e6-b866-dd9e65c01d56  object_b50f27b0-e31a-11e6-b866-dd9e65c01d56  snort.conf.b50f27b0-e31a-11e6-b866-
dd9e65c01d56  snort.conf.b50f27b0-e31a-11e6-b866-dd9e65c01d56.default
root@ciscoasa: network_analysis# cat b50f27b0-e31a-11e6-b866-dd9e65c01d56/normalize.conf
#
# generated from My Changes
#
preprocessor normalize_tcp: ips, rsv, pad, req_urg, req_pay, req_urp, block
```

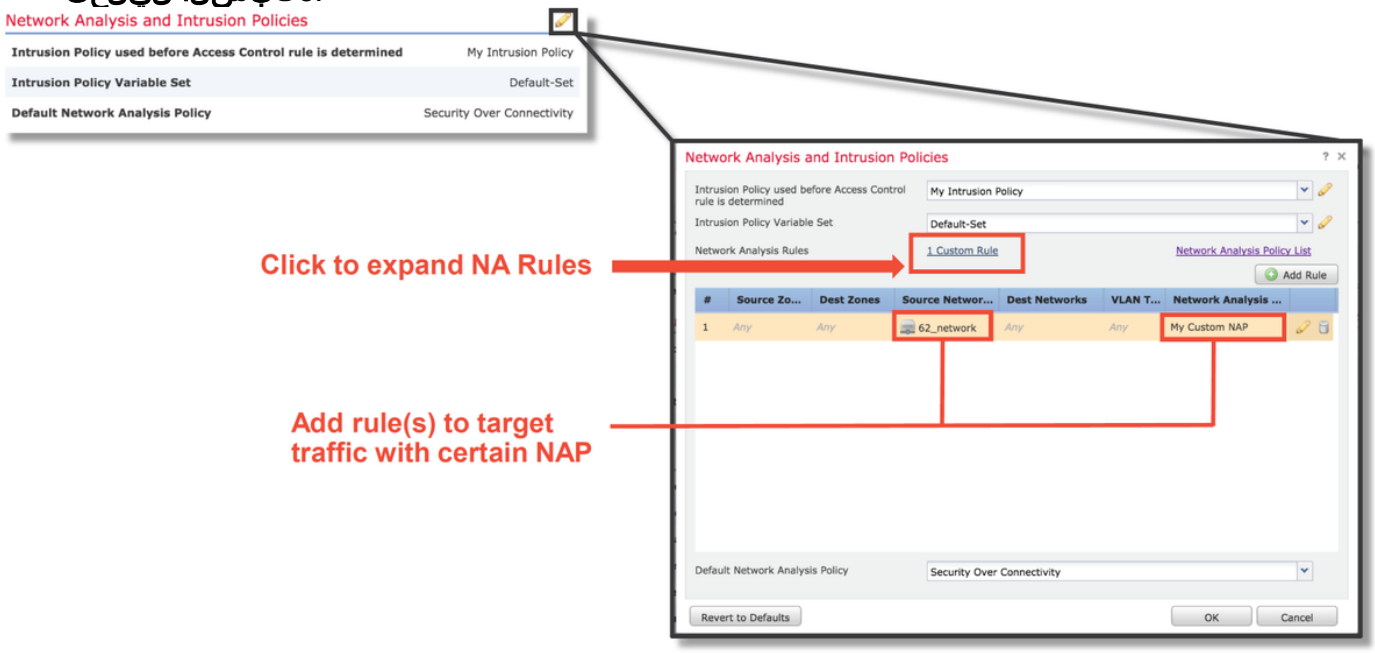
"block" option is enabled in normalize.conf

إنشاء قيلولة مستهدفة

إذا كانت بعض الأجهزة المضيفة تقوم بتشغيل أحداث سابقة للمعالج، يمكن إستخدام NAP مخصص لفحص حركة المرور من وإلى الأجهزة المضيفة المذكورة. يمكن تعطيل الإعدادات التي تتسبب في حدوث مشاكل ضمن NAP المخصص.

وهذه هي الخطوات اللازمة لتنفيذ برنامج عمل وطني مستهدف.

1. قم بإنشاء NAP وفقا للتعليمات المذكورة في قسم "التحقق من تكوين NAP" في هذه المقالة.
2. في علامة التبويب **خيارات متقدمة** بنهج التحكم في الوصول، انتقل إلى قسم **تحليل الشبكة وسياسات الاقتحام**. انقر فوق **إضافة قاعدة** وإنشاء قاعدة، باستخدام البيئات المضيفة المستهدفة واختر NAP التي تم إنشاؤها حديثا في قسم **نهج تحليل الشبكة**.



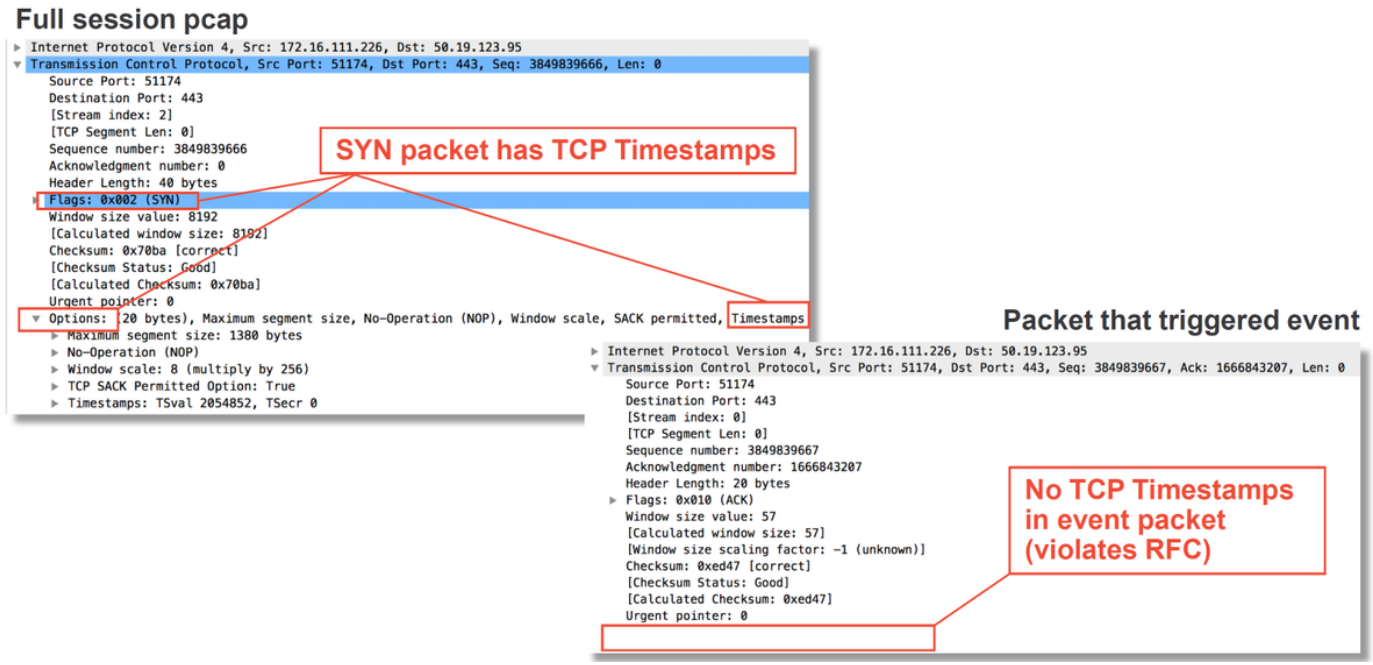
تحليل إيجابي كاذب

التحقق من الإيجابيات الخاطئة في أحداث التطفل لقواعد ما قبل المعالج مختلف تماما عن

قواعد الشخر المستخدمة لتقييم القاعدة (والتي تحتوي على GID 1 و 3).

لإجراء تحليل إيجابي خاطئ لأحداث قاعدة المعالج الأولي، يلزم التقاط جلسة عمل كاملة للبحث عن حالات شاذة داخل تدفق TCP.

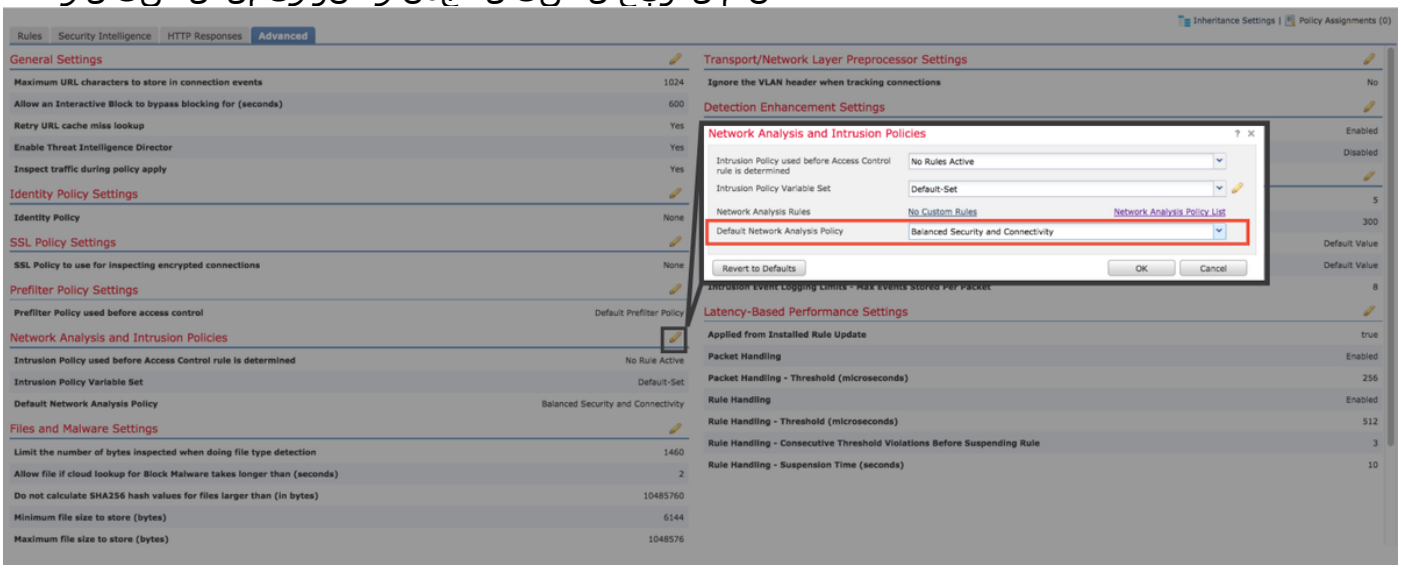
في المثال التالي، يتم إجراء تحليل إيجابي كاذب على القاعدة **129:14**، التي يتبين أنها تقوم بإسقاط حركة المرور في الأمثلة الواردة أعلاه. بما أن **129:14** تبحث عن تدفقات TCP التي تكون الطوابع الزمنية مفقودة فيها، يمكنك أن ترى بوضوح لماذا تم تشغيل القاعدة لكل تحليل التقاط الحزمة الموضح أدناه.



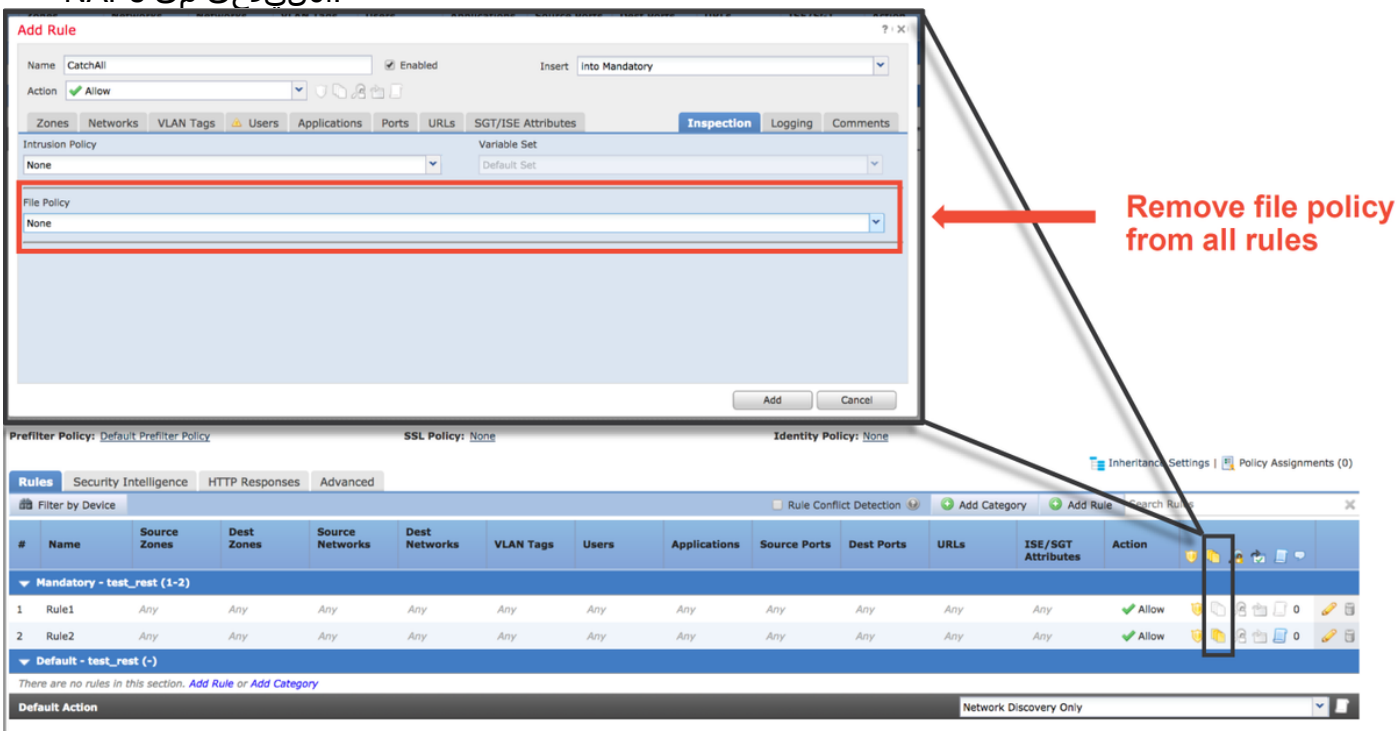
خطوات التخفيف

وللتخفيف بسرعة من المشاكل المحتملة في برنامج العمل الوطني، يمكن تنفيذ الخطوات التالية.

- في حالة إستخدام برنامج NAP مخصص وأنت غير متأكد مما إذا كان إعداد NAP يؤدي إلى إسقاط حركة المرور لكنك تشك في أنه قد يحدث، يمكنك محاولة إستبداله بنهج "الأمان والاتصال المتوازن" أو نهج "الاتصال عبر الأمان".



- في حالة إستخدام أي "قواعد مخصصة"، تأكد من تعيين NAP إلى أحد الافتراضيات المذكورة أعلاه
- إذا كانت أي من قواعد التحكم في الوصول تستخدم "نهج ملف"، فقد تحتاج إلى محاولة إزالته مؤقتا حيث أن "نهج الملف" يمكن أن يمكن إعدادات ما قبل المعالج على الطرف الخلفي التي لا تنعكس في FMC، وهذا يحدث على مستوى "عام"، مما يعني أن جميع NAPs تم تعديلها.



يحتوي كل بروتوكول على معالج مسبق مختلف، ويمكن أن يكون أستكشاف المشكلات وحلها خاصا بالمعالج الأولي. لا تغطي هذه المقالة جميع إعدادات المعالج المسبق وطرق أستكشاف الأخطاء وإصلاحها لكل منها.

يمكنك فحص الوثائق لكل معالج مسبق للحصول على فكرة أفضل عما يفعله كل خيار، وما يساعد عند أستكشاف أخطاء معالج مسبق معين وإصلاحها.

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 الملف وإصلاحها من جهاز Firepower
http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-appliar	التقاط حزمة الجلسة الكاملة من جهاز FirePOWER

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).