أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: نظرة عامة

المحتويات

المقدمة

الغرض من هذا الدليل هو المساعدة في التعرف بسرعة على ما إذا كان جهاز الدفاع عن تهديد الطاقة النارية (FTD) أو جهاز الأمان القابل للتكيف (ASA) مع خدمات FirePOWER يتسبب في مشكلة مع حركة مرور الشبكة. كما تساعد في تضييق المكون (المكونات) الخاصة بالمشكلة وجمع البيانات التي يجب التحقق فيها والبيانات التي يجب جمعها قبل إشراك مركز المساعدة التقنية (TAC) من Cisco.

تنطبق هذه المقالة على جميع منصات سلسلة أستكشاف أخطاء مسار بيانات Firepower وإصلاحها.

المرحلة 1 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: مدخل الحزمة

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

المرحلة 2 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: طبقة DAQ
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

المرحلة 3 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: ذكاء الأمان

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

المرحلة 4 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: سياسة التحكم في الوصول
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

المرحلة 5 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: نهج SSL
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

المرحلة 6 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: المصادقة النشطة
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

المرحلة 7 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: نهج الاقتحام
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

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

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

المتطلبات الأساسية

- تفترض هذه المقالة أن الشخص لديه فهم أساسي لمنصات FTD و ASA.
- يوصى بالمعرفة عن شخ المصدر المفتوح، على الرغم من أنه غير مطلوب.

للحصول على قائمة كاملة بوثائق FirePOWER، بما في ذلك أدلة التكوين والتثبيت، يرجى زيارة صفحة مخطط مسار الوثائق.

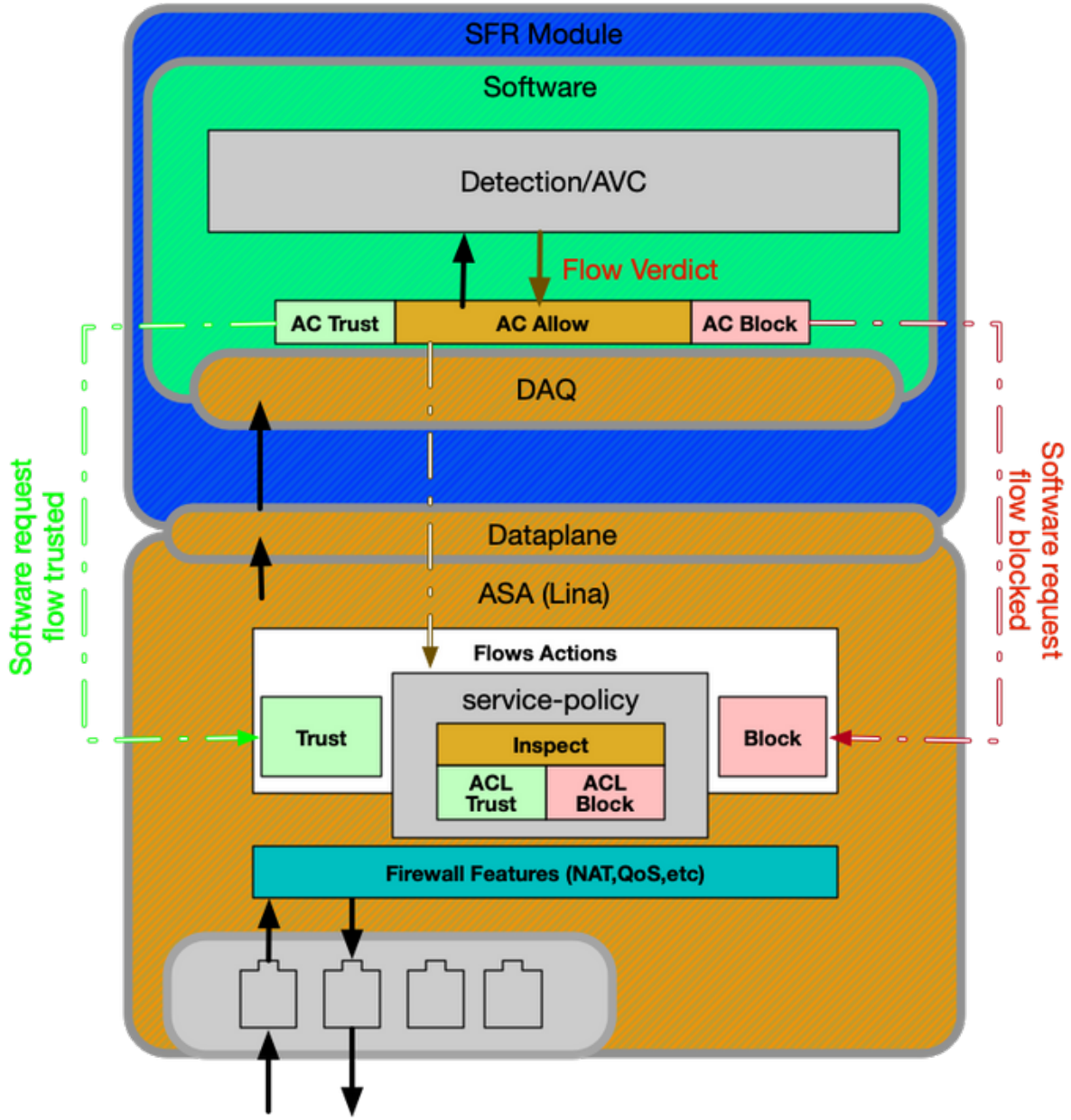
نظرة عامة معمارية لمسار البيانات

ينظر القسم التالي إلى مسار بيانات البنية للعديد من منصات FirePOWER. مع وضع الهندسة المعمارية في الاعتبار، سننتقل بعد ذلك إلى كيفية تحديد ما إذا كان جهاز FirePOWER يمنع تدفق حركة المرور أم لا.

> **ملاحظة**: لا تغطي هذه المقالة أجهزة السلسلة Firepower 7000 و 8000 القديمة والنظام الأساسي الظاهري NGIPS (غير FTD). لمزيد من المعلومات حول أستكشاف هذه الأنظمة وإصلاحها، يرجى زيارة صفحة TechNotes الخاصة بنا.

ASA مع النظام الأساسي لخدمات FirePOWER (وحدة SFR)

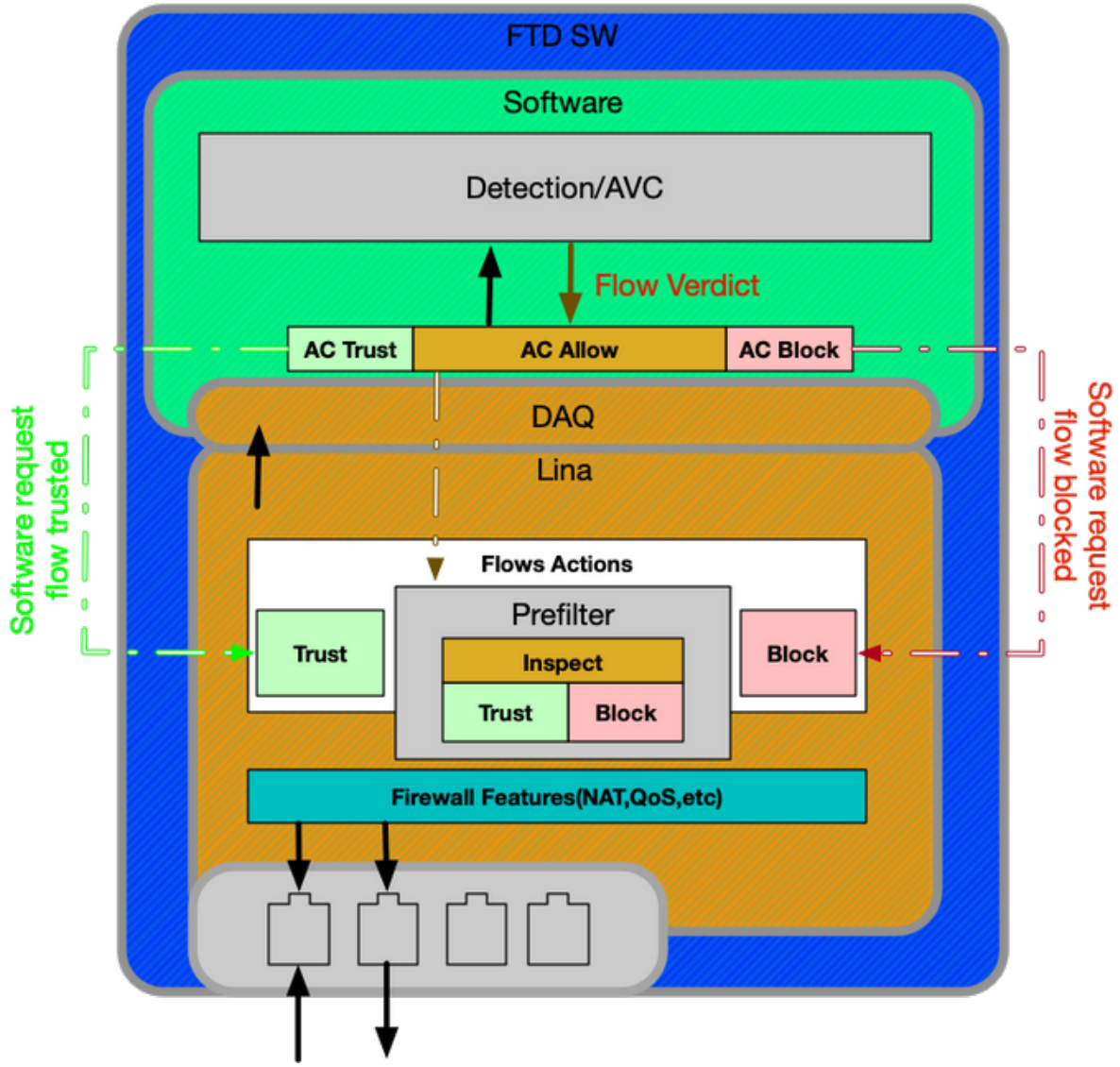
ويشار أيضا إلى النظام الأساسي لخدمات FirePOWER باسم وحدة SFR. هذا في الأساس جهاز افتراضي يعمل على 5500-X ASA منصة.



يحدد نهج الخدمة على ASA حركة مرور البيانات التي يتم إرسالها إلى وحدة SFR النمطية. هناك طبقة مستوى بيانات والتي يتم إستخدامها للاتصال بمحرك الحصول على بيانات FirePOWER (DAQ)، والذي يتم إستخدامه لترجمة الحزم بطريقة يمكن للشخير فهمها.

الدفاع ضد تهديد Firepower على منصة ASA500-X و Virtual FTD

يتكون نظام FTD الأساسي من صورة واحدة تحتوي على كل من Lina (ASA) و FirePOWER. الفرق الرئيسي بين هذا وبين ASA مع SFR وحدة منصة هو أن هناك إتصالات أكثر فعالية بين Lina و snort.

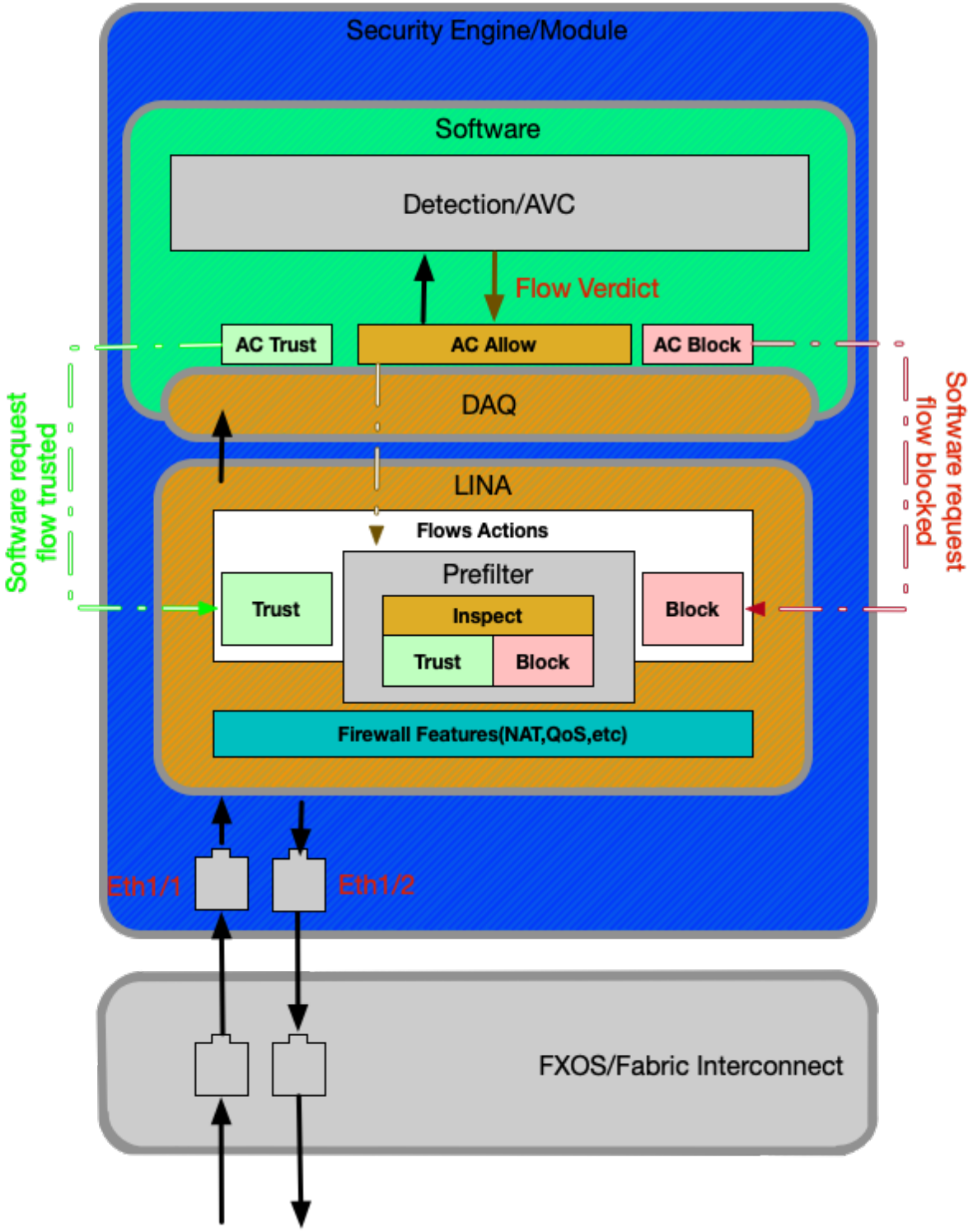


FTD على منصات SSP

في طرز الأنظمة الأساسية لخدمات الأمان (SSP)، يعمل برنامج FTD فوق النظام التشغيلي Firepower Xsible Operation System (المعروف إختصارا باسم FXOS)، وهو عبارة عن نظام تشغيل أساسي (OS) يستخدم لإدارة أجهزة الهيكل واستضافة تطبيقات مختلفة تعرف باسم الأجهزة المنطقية.

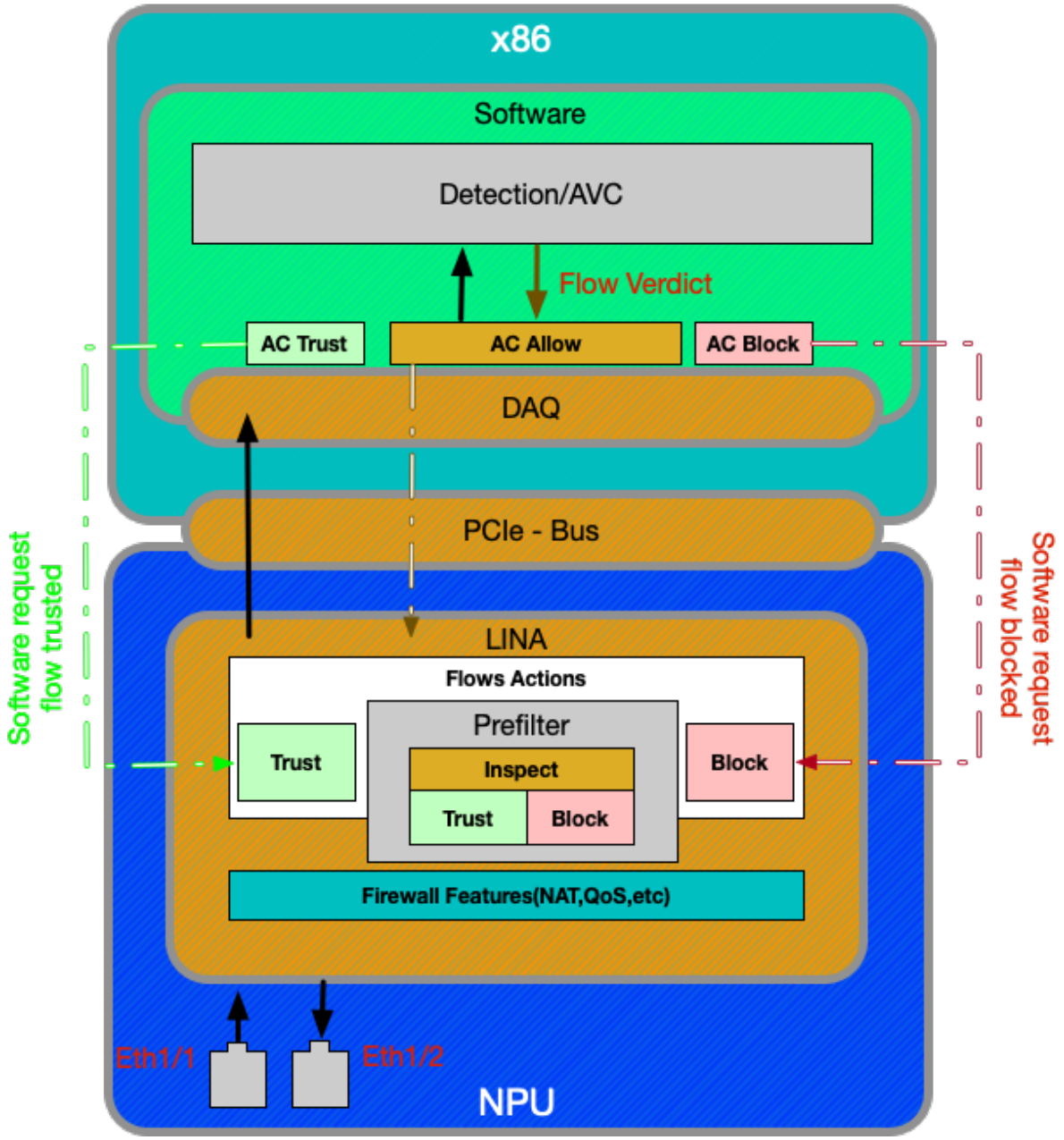
داخل النظام الأساسي لبروتوكول طبقة الأمان (SSP)، هناك بعض الاختلافات عبر الطرز، كما هو موضح في الرسوم البيانية والأوصاف أدناه.

أجهزة Firepower 9300 و 4100



على الأنظمة الأساسية Firepower 9300 و 4100، يتم التعامل مع حزم الإدخال والإخراج بواسطة محول يتم تشغيله بواسطة البرنامج الثابت FXOS (الاتصال البيني النسيجي). يتم بعد ذلك إرسال الحزم إلى الواجهات المعينة إلى الجهاز المنطقي (في هذه الحالة، FTD). بعد ذلك، تكون معالجة الحزم هي نفسها كما هو الحال على منصات FTD غير SSP.

أجهزة Firepower 2100



يعمل الجهاز Firepower 2100 بشكل يشبه كثيرا الأنظمة الأساسية FTD غير الخاصة ب SSP. والتي تحتوي على طبقة اتصال البنية البيني الموجودة في الطرازين 4100 و 9300. ومع ذلك، هناك فرق كبير في أجهزة السلسلة 2100 مقارنة بالأجهزة الأخرى، ألا وهو وجود الدائرة المدمجة الخاصة بالتطبيق (ASIC). يتم تشغيل جميع ميزات ASA التقليدية (LINA) على ASIC، كما يتم تشغيل جميع ميزات جدار الحماية (NGFW) من الجيل التالي (snort، وتصفية عنوان URL، وما إلى ذلك) على بنية x86 التقليدية. الطريقة التي تتصل بها Lina و Snort على هذا النظام الأساسي هي من خلال Peripheral Component Interconnect Express (PCIe) عبر قائمة انتظار الحزم، مقارنة بالأنظمة الأساسية الأخرى التي تستخدم الوصول المباشر إلى الذاكرة (DMA) لوضع الحزم في قائمة الانتظار حتى الشخير.

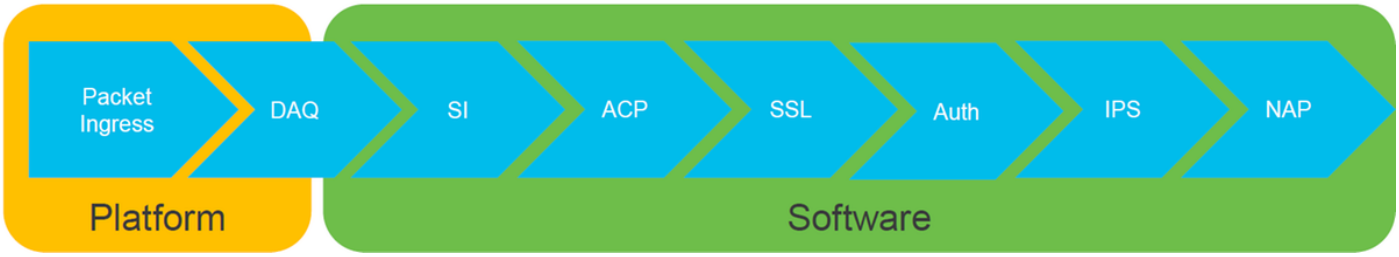
ملاحظة: سيتم اتباع الأساليب نفسها لاستكشاف أخطاء أنظمة FTD غير الخاصة ب SSP وإصلاحها على النظام الأساسي FPR-2100.

العملية الموصى بها لاستكشاف أخطاء مسار بيانات Firepower وإصلاحها

الآن وقد غطينا كيفية تحديد حركة المرور الفريدة بالإضافة إلى بنية مسار البيانات

الأساسي في منصات FirePOWER، فإننا ننظر الآن إلى الأماكن المحددة التي يمكن إسقاط الحزم فيها. هناك ثمانية مكونات أساسية يتم تغطيتها في مقالات مسار البيانات، والتي يمكن أستكشاف الأخطاء وإصلاحها بشكل منهجي لتحديد عمليات إسقاط الحزم المحتملة. وتشمل هذه التدابير ما يلي:

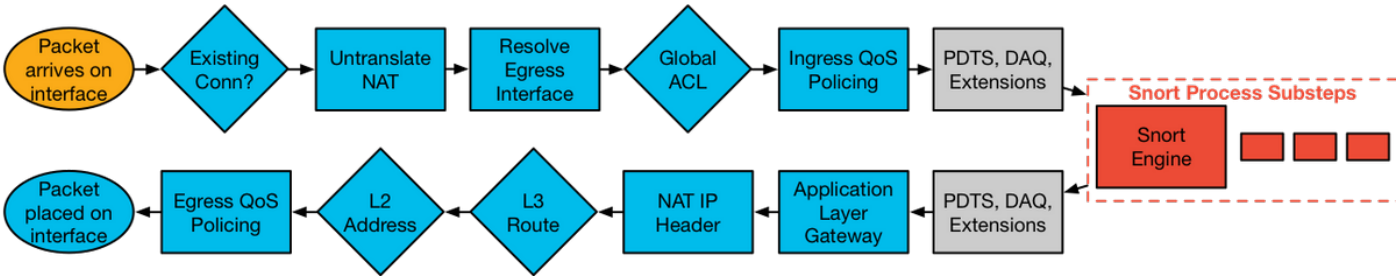
1. مدخل الحزمة
2. طبقة DAQ Firepower
3. الإستخبارات الأمنية
4. سياسة التحكم في الوصول
5. نهج SSL
6. ميزات المصادقة النشطة
7. سياسة التسلل (قواعد IPS)
8. نهج تحليل الشبكة (إعدادات معالج ما قبل الشبكة)



ملاحظة: هذه المكونات غير مدرجة بترتيب العمليات في معالجة FirePOWER على وجه الدقة، ولكنها مطلوبة وفقا لسير العمل الموصى به لاستكشاف الأخطاء وإصلاحها. راجع الرسم التوضيحي أدناه للمسار الفعلي لمخطط الحزمة.

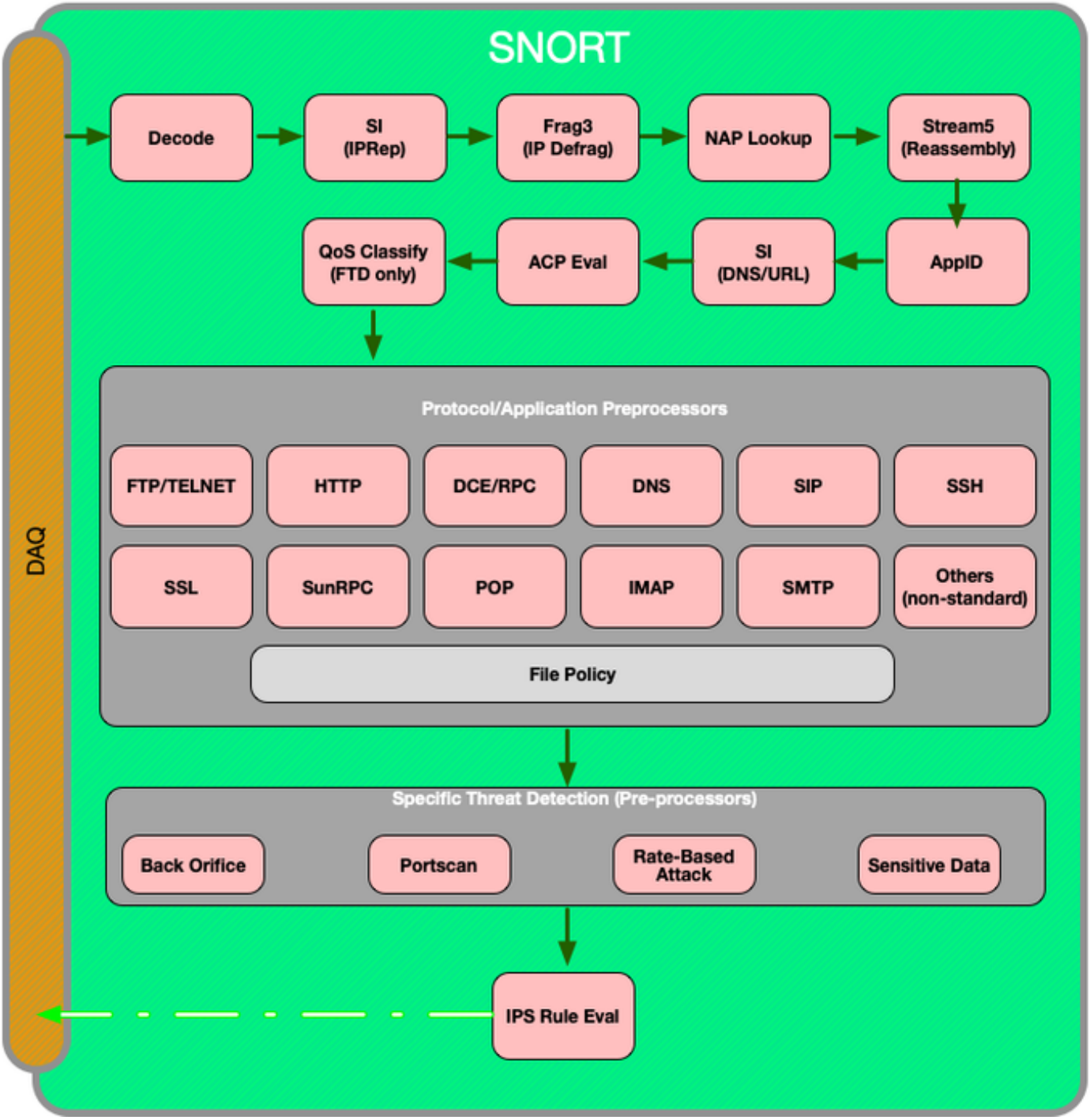
المسار الفعلي للحزمة عبر FTD

يوضح الرسم التوضيحي التالي المسار الفعلي للحزمة عند إجتيازها خلال FTD.



مسار حزمة الشورت

يوضح الرسم التوضيحي التالي مسار الحزمة من خلال محرك الشخير.



الدخول والخروج للحزم

أولى خطوات أستكشاف أخطاء مسار البيانات وإصلاحها هي التأكد من عدم حدوث أي عمليات إسقاط في مرحلة الدخول أو الخروج لمعالجة الحزمة. إذا كانت الحزمة تدخل ولكنها لا تدخل، بعد ذلك يمكنك التأكد من أن الحزمة يتم إسقاطها بواسطة الجهاز في مكان ما داخل مسار البيانات.

تتطرق هذه المقالة إلى كيفية أستكشاف أخطاء دخول الحزم وخروجها إلى أنظمة FirePOWER وإصلاحها.

طبقة DAQ Firepower

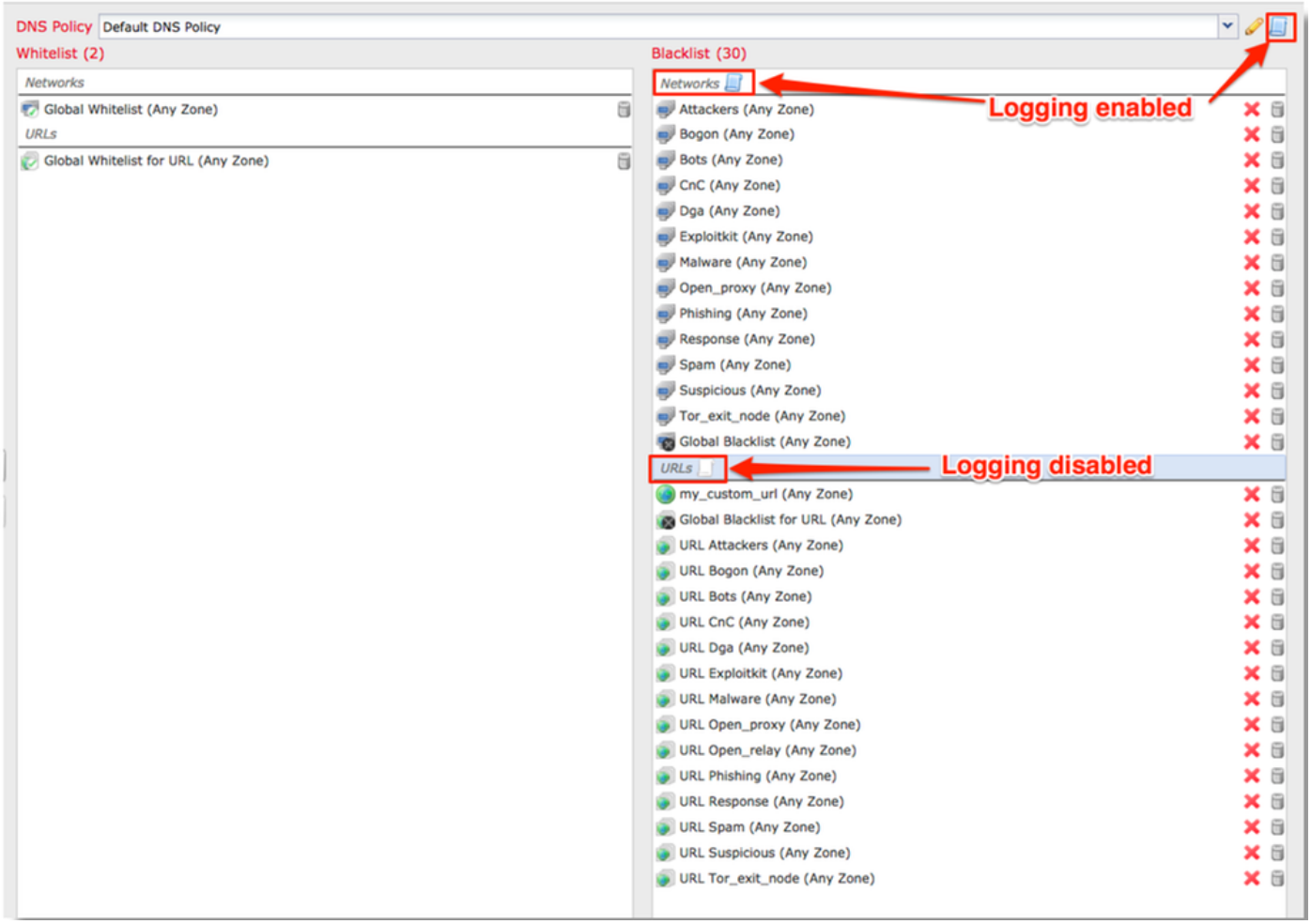
إذا تم تحديد أن الحزمة قيد الإتجاه ولكن ليس الإتجاه، فإن الخطوة التالية في أستكشاف أخطاء مسار البيانات وإصلاحها يجب أن تكون في طبقة FirePOWER DAQ (اكتساب البيانات) للتأكد من إرسال حركة المرور المعنية إلى FirePOWER للتفتيش وإذا كان الأمر كذلك، إذا تم إسقاطها أو تعديلها.

تبحث هذه المقالة في كيفية أستكشاف أخطاء المعالجة الأولية لحركة المرور بواسطة FirePOWER بالإضافة إلى المسار الذي تسلكه عبر الجهاز وإصلاحها.

كما يغطي كيفية تجاوز جهاز FirePOWER تمامًا لتحديد ما إذا كان مكون FirePOWER مسؤولاً عن مشكلة حركة المرور.

الإستخبارات الأمنية

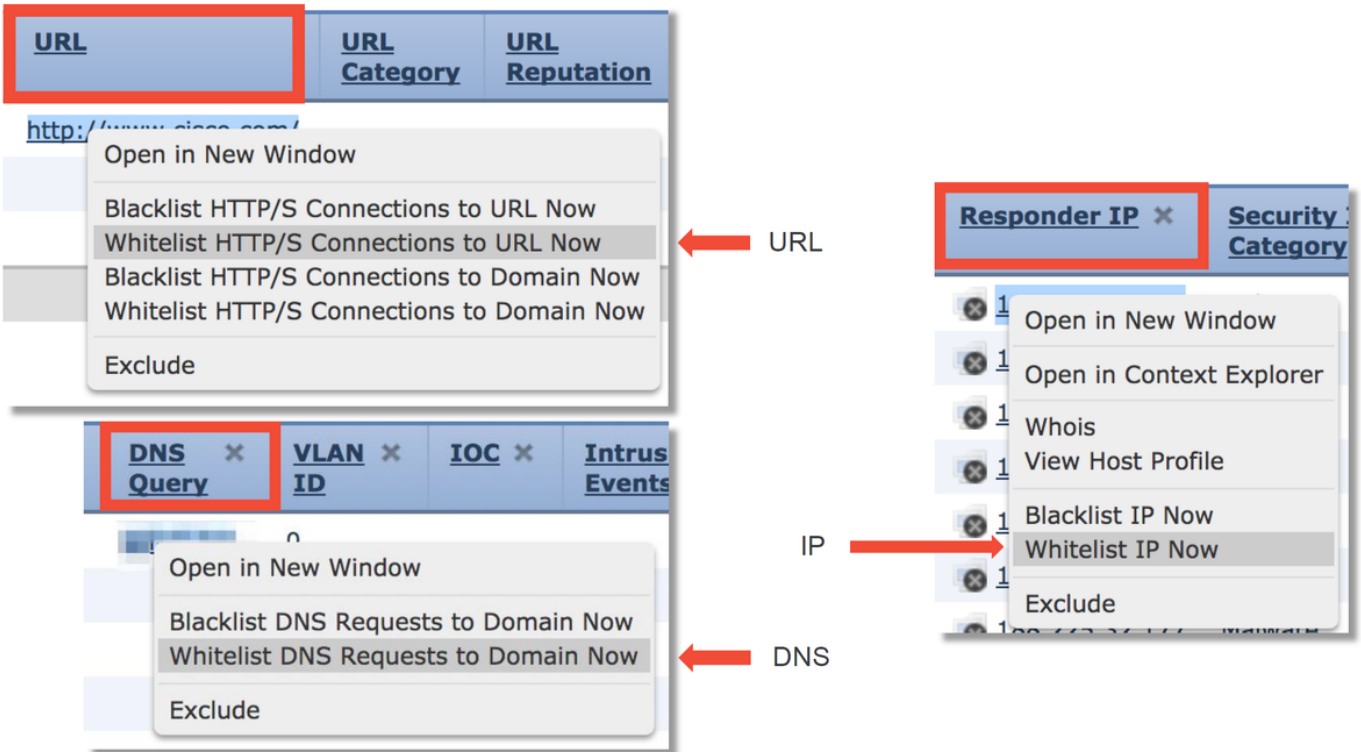
وذكاء الأمان هو أول مكون داخل FirePOWER لفحص حركة المرور. الكتل في هذا المستوى سهلة جدا لتحديد ما دام التسجيل ممكنا. ويمكن تحديد ذلك على واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم **في** الوصول (FMC) من خلال الانتقال إلى **السياسات > التحكم في الوصول > سياسة التحكم في الوصول**. بعد النقر فوق رمز التحرير الموجود بجانب النهج قيد البحث، انتقل إلى علامة التبويب **معلومات الأمان**.



بمجرد تمكين التسجيل، يمكنك عرض أحداث ذكاء الأمان تحت **التحليل > الاتصالات > أحداث ذكاء الأمان**. يجب أن يكون واضحا سبب منع حركة المرور.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

كخطوة تخفيف سريعة، يمكنك النقر بزر الماوس الأيمن على IP أو URL أو استعلام DNS الذي يتم حظره بواسطة ميزة "معلومات الأمان" واختيار خيار البيانات البيضاء.



إذا كنت تشك في أن شيئا ما تم وضعه بشكل غير صحيح على القائمة السوداء، وإذا كنت ترغب في طلب تغيير السمعة، يمكنك فتح تذكرة مباشرة مع Cisco Talos على الرابط التالي:

https://www.talosintelligence.com/reputation_center/support

يمكنك أيضا توفير البيانات إلى TAC للإبلاغ عن ما تم حظره وربما إزالة إدخال من القائمة السوداء.

للحصول على معلومات تفصيلية حول أستكشاف أخطاء مكون "معلومات الأمان" وإصلاحها، الرجاء مراجعة مقال أستكشاف أخطاء مسار البيانات وإصلاحها ذات الصلة.

سياسة التحكم في الوصول

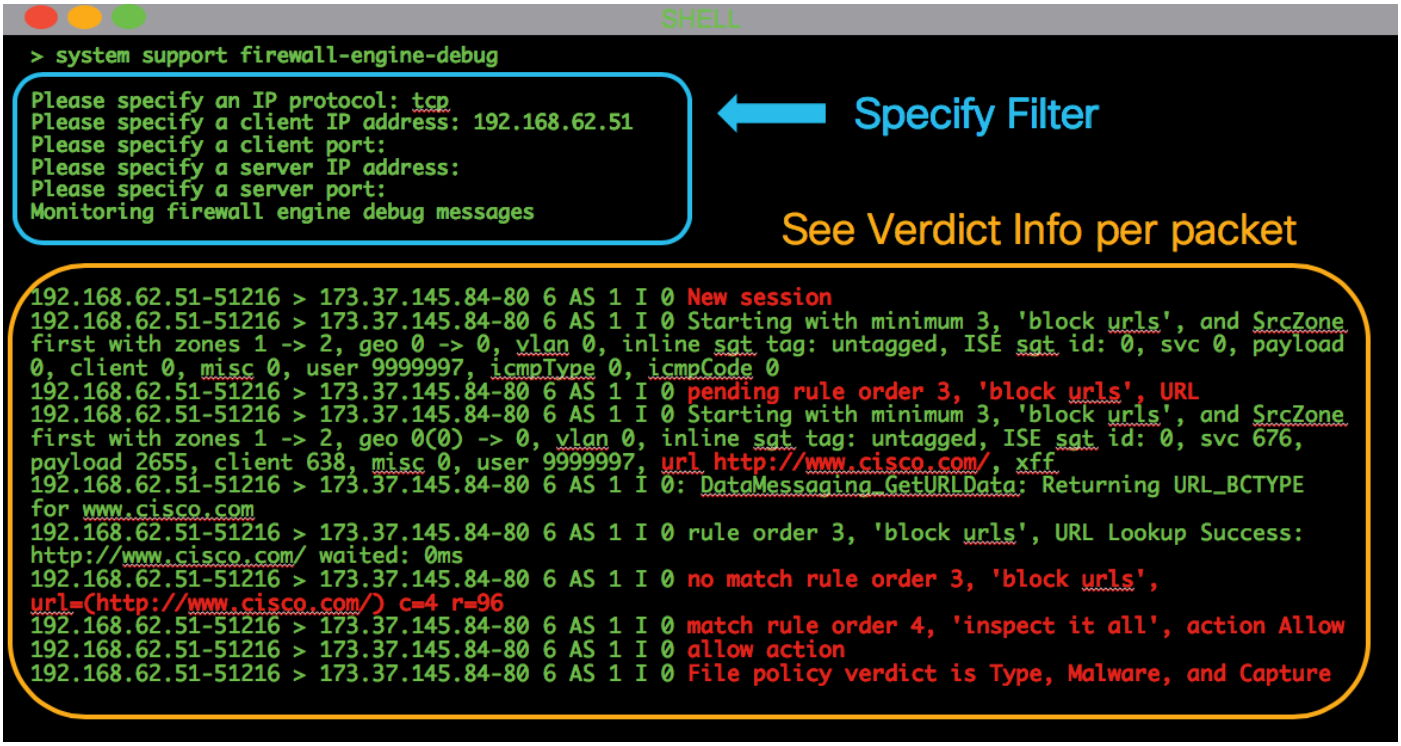
إذا تم تحديد أن ميزة "معلومات الأمان" ال تقوم بحظر حركة المرور، فإن الخطوة التالية المنصوص بها هي أستكشاف أخطاء قواعد "سياسة التحكم في الوصول" وإصلاحها لمعرفة ما إذا كانت إحدى القواعد التي تتضمن إجراء "الحظر" تقوم بإسقاط حركة المرور.

يوصى بدء إستخدام الأمر "firewall-engine-debug" أو الالتقاط بالتتبع. عموما، يمكن لهذه

الادوات ان تعطيك الجواب فورا وتخبرك ما هي القاعدة التي تضربها حركة المرور، ولأي أسباب.

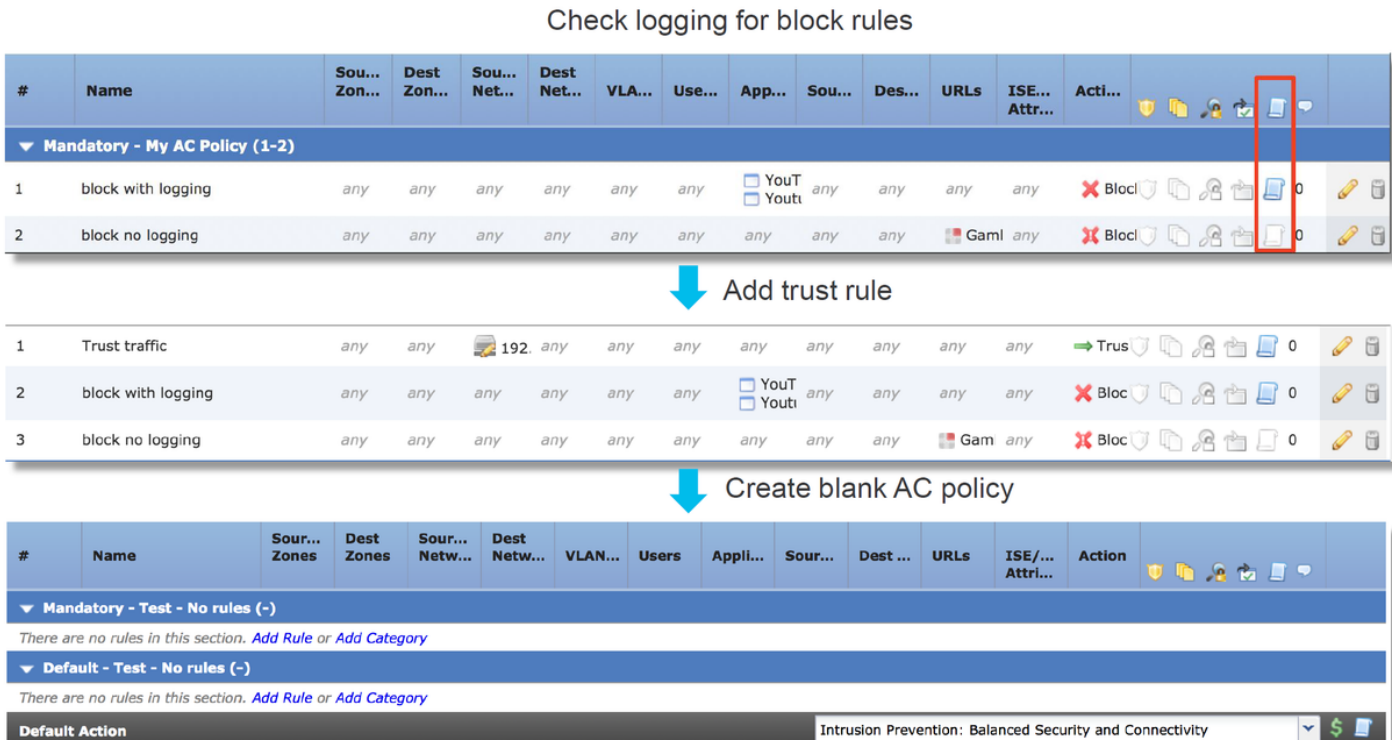
- قم بتشغيل تصحيح الأخطاء على Firepower CLI لمعرفة القاعدة التي تمنع حركة المرور (تأكد من إدخال أكبر عدد ممكن من المعلمات) من خلال الأمر التالي: **> دعم النظام جدار الحماية-المحرك-تصحيح الأخطاء**
- يمكن توفير إخراج تصحيح الأخطاء إلى TAC للتحليل

فيما يلي بعض المخرجات النموذجية، التي تصف تقييم القاعدة لحركة المرور التي تطابق قاعدة التحكم في الوصول مع الإجراء "السماح":



إذا لم تكن قادرا على تحديد أي من قواعد التحكم في الوصول (AC) التي تتم مطابقتها، أو لم تكن قادرا على تحديد ما إذا كانت سياسة التجار المتردد هي المشكلة باستخدام الأدوات الواردة أعلاه، فيما يلي بعض الخطوات الأساسية الاستكشاف أخطاء سياسة التحكم في الوصول وإصلاحها (لاحظ أن هذه الخيارات ليست الخيار الأول لأنها تتطلب تغييرات/عمليات نشر للسياسة):

- تمكين التسجيل لأي قواعد مع إجراء "حظر"
- إذا كنت لا تزال لا ترى أحداث الاتصال لحركة المرور ويتم حظرها، قم بعد ذلك بإنشاء قاعدة ثقة لحركة المرور المعنية كخطوة تخفيف
- إذا كانت قاعدة الثقة لحركة المرور لا تزال لا تحل المشكلة لكنك لا تزال تشك في أن سياسة التجار المتردد موجودة على أطر، بعد ذلك، قم بإنشاء نهج جديد فارغ للتحكم في الوصول إن أمكن، باستخدام إجراء افتراضي غير "حظر لكل حركة المرور"

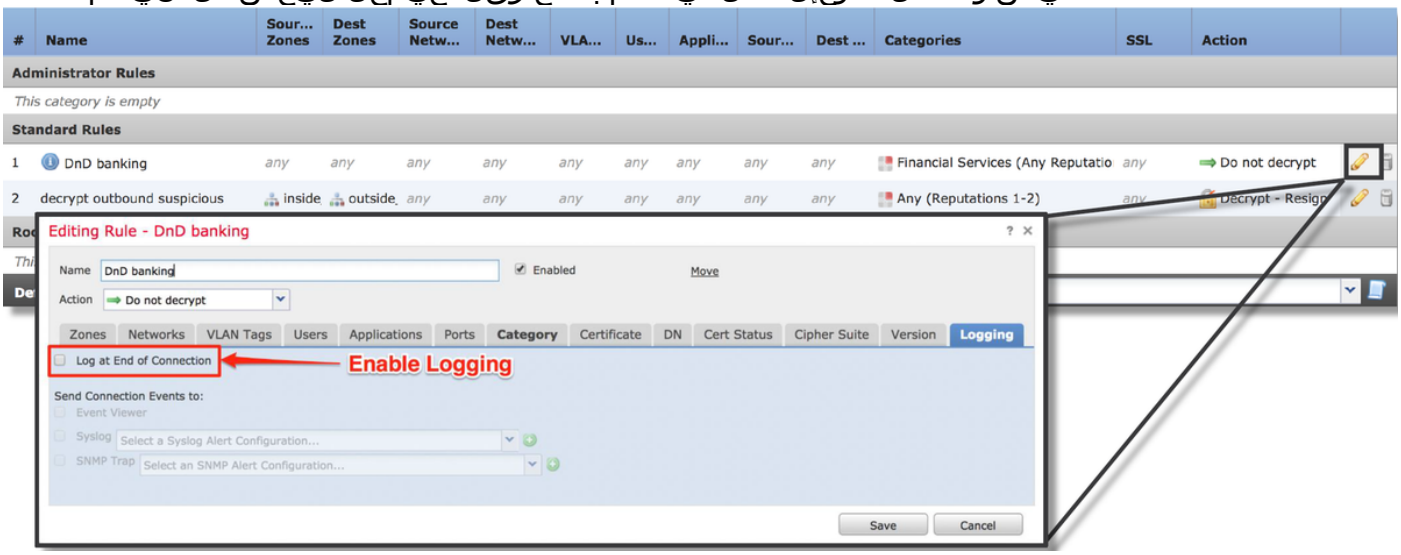


للحصول على معلومات مفصلة حول أستكشاف أخطاء سياسة التحكم بالوصول وإصلاحها، الرجاء مراجعة مقالة أستكشاف أخطاء مسار البيانات وإصلاحها ذات الصلة.

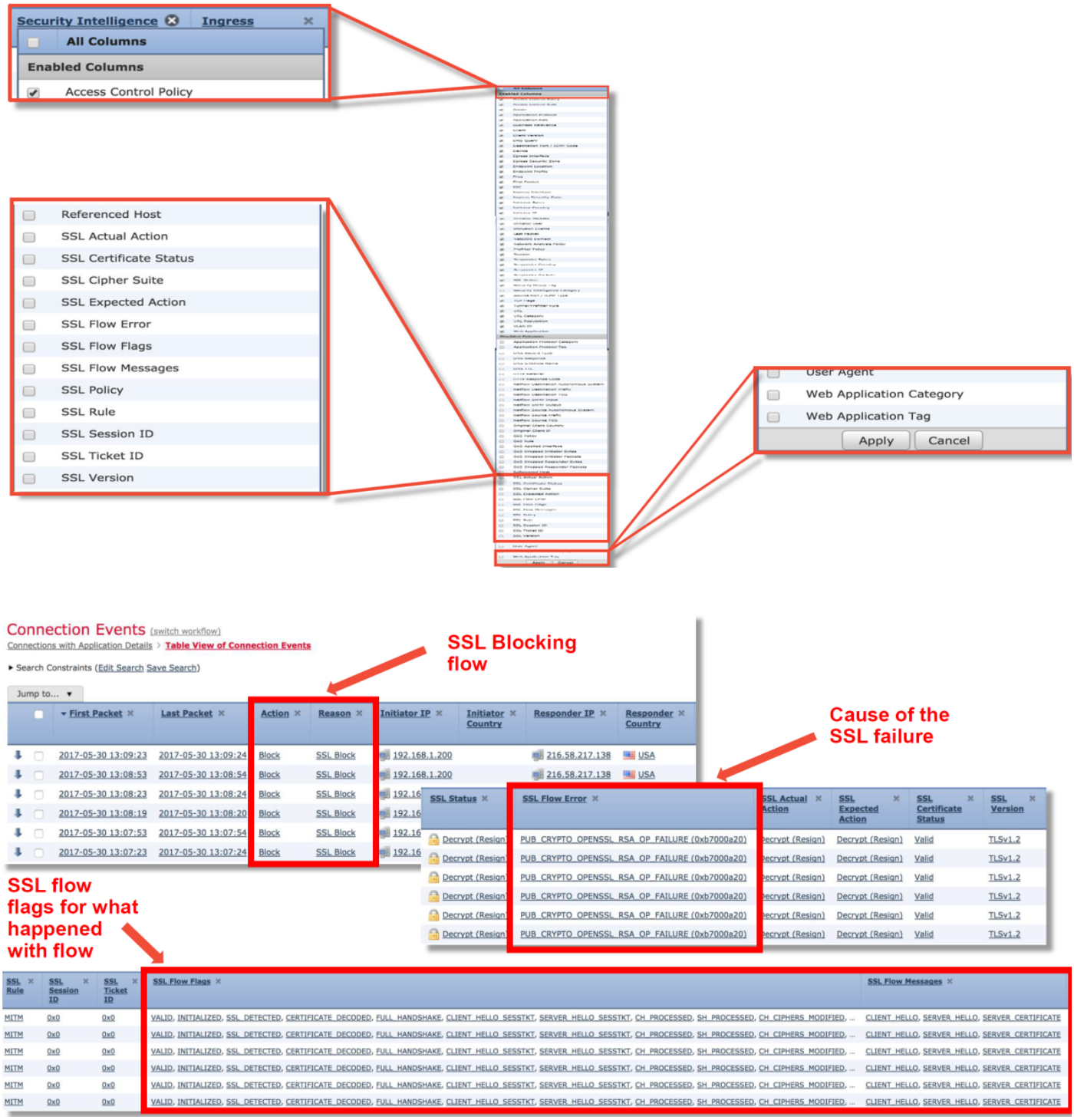
نهج SSL

إذا كان نهج SSL قيد الاستخدام، فمن المحتمل أن يكون قد قام بحظر حركة المرور. فيما يلي بعض الخطوات الأساسية لاستكشاف أخطاء سياسة SSL وإصلاحها:

- تمكين التسجيل لجميع القواعد، بما في ذلك 'الإجراء الافتراضي'



- تحقق من علامة التبويب إجراءات إلغاء التشفير لمعرفة ما إذا تم تعيين خيار لحظر حركة المرور
- في قسم "أحداث الاتصال"، تحقق من كافة الحقول التي تحتوي على 'SSL' في الاسم يتم تعطيل معظم المستخدمين بشكل افتراضي ويجب تمكينهم في عارض "أحداث الاتصال" بالنقر فوق الصليب الموجود بجوار أي اسم عمود



- إنشاء سياسة SSL فارغة مع عدم فك التشفير كإجراء افتراضي كخطوة تخفيف
- إزالة نهج SSL من نهج التحكم في الوصول كخطوة تخفيف
  تم تعيين ذلك في علامة التبويب متقدم

يشتبه في أن نهج SSL الخاص ب IT يقوم بإسقاط حركة المرور، ويمكن إرسال أحداث الاتصال بالإضافة إلى تكوين النهج إلى TAC.

للحصول على مزيد من التفاصيل حول أستكشاف أخطاء سياسة SSL وإصلاحها، الرجاء مراجعة مقالة أستكشاف أخطاء مسار البيانات وإصلاحها ذات الصلة.

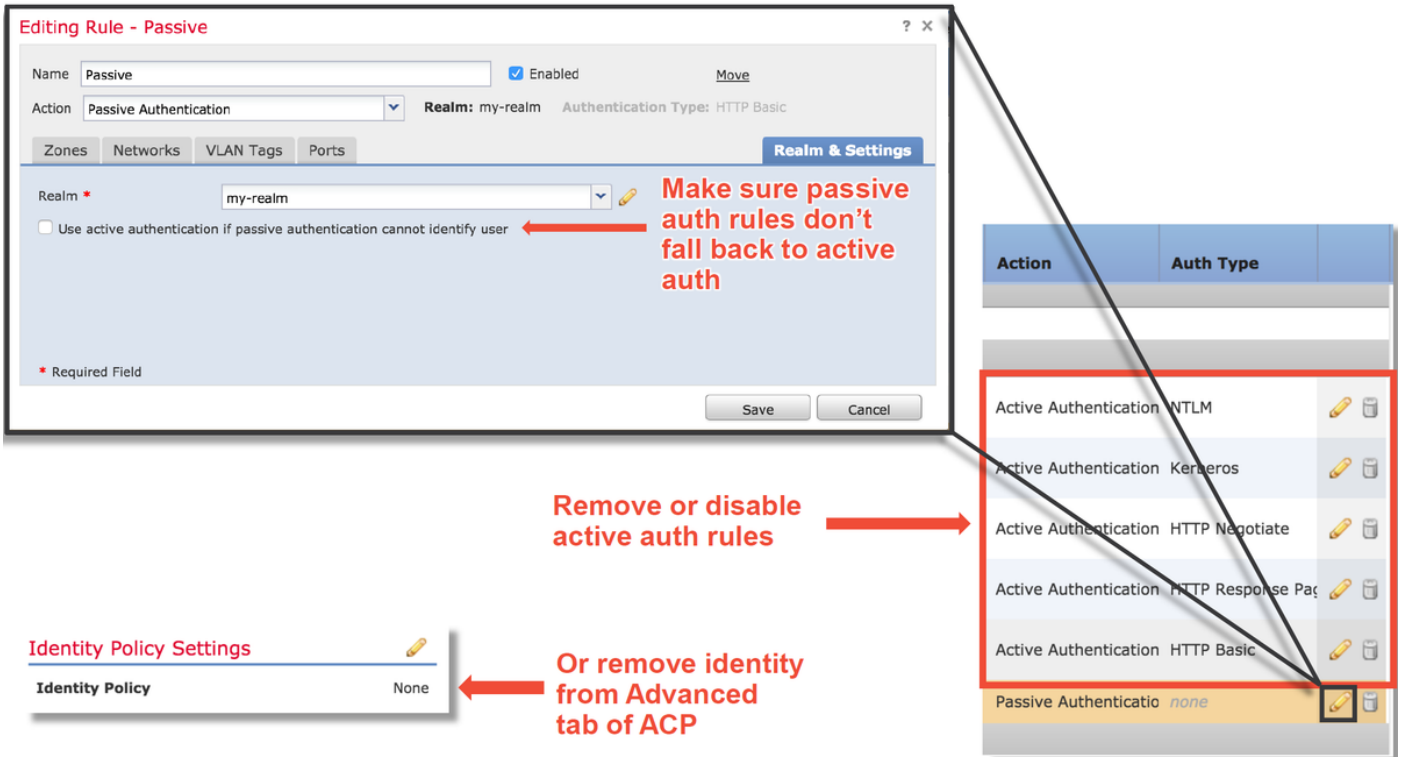
المصادقة النشطة

عند الاستخدام في نهج الهوية، يكون للمصادقة النشطة القدرة على إسقاط حركة المرور

التي يجب السماح بها في حالة حدوث خطأ. يمكن أن تؤثر ميزة المصادقة النشطة نفسها مباشرة على جميع حركة مرور HTTP/HTTPS لأنه إذا تم تحديد حاجتنا إلى مصادقة مستخدم، يحدث كل هذا عبر بروتوكول HTTP فقط. وهذا يعني أن المصادقة النشطة لا ينبغي أن تؤثر على خدمات الشبكة الأخرى (مثل DNS و ICMP وما إلى ذلك) ما لم تكن لديك قواعد محددة للتحكم في الوصول تقوم على الحظر بناء على المستخدم، ولا يمكن للمستخدمين المصادقة من خلال خدمات المصادقة النشطة على FTD. ومع ذلك، لن يكون هذا مشكلة مباشرة لميزة المصادقة النشطة، ولكن نتيجة لعدم قدرة المستخدمين على المصادقة ووجود نهج يمنع المستخدمين غير المصدق عليهم.

تتمثل إحدى خطوات التخفيف السريعة في تعطيل أي قاعدة ضمن نهج الهوية باستخدام إجراء "المصادقة النشطة".

تأكد أيضا من أن أي قواعد مع إجراء "المصادقة الخاملة" لا تحتوي على خيار "إستخدام المصادقة النشطة إذا لم تتمكن المصادقة الخاملة من تحديد المستخدم" الذي تم فحصه.



مزيد من التفاصيل حول أستكشاف أخطاء المصادقة النشطة وإصلاحها، الرجاء مراجعة مقالة أستكشاف أخطاء مسار البيانات وإصلاحها ذات الصلة.

سياسة القاحام

قد تؤدي سياسة التسلل إلى إسقاط حركة المرور أو التسبب في تأخير الشبكة. يمكن إستخدام سياسة التسلل في أحد الأماكن الثلاثة التالية ضمن سياسة التحكم بالوصول:

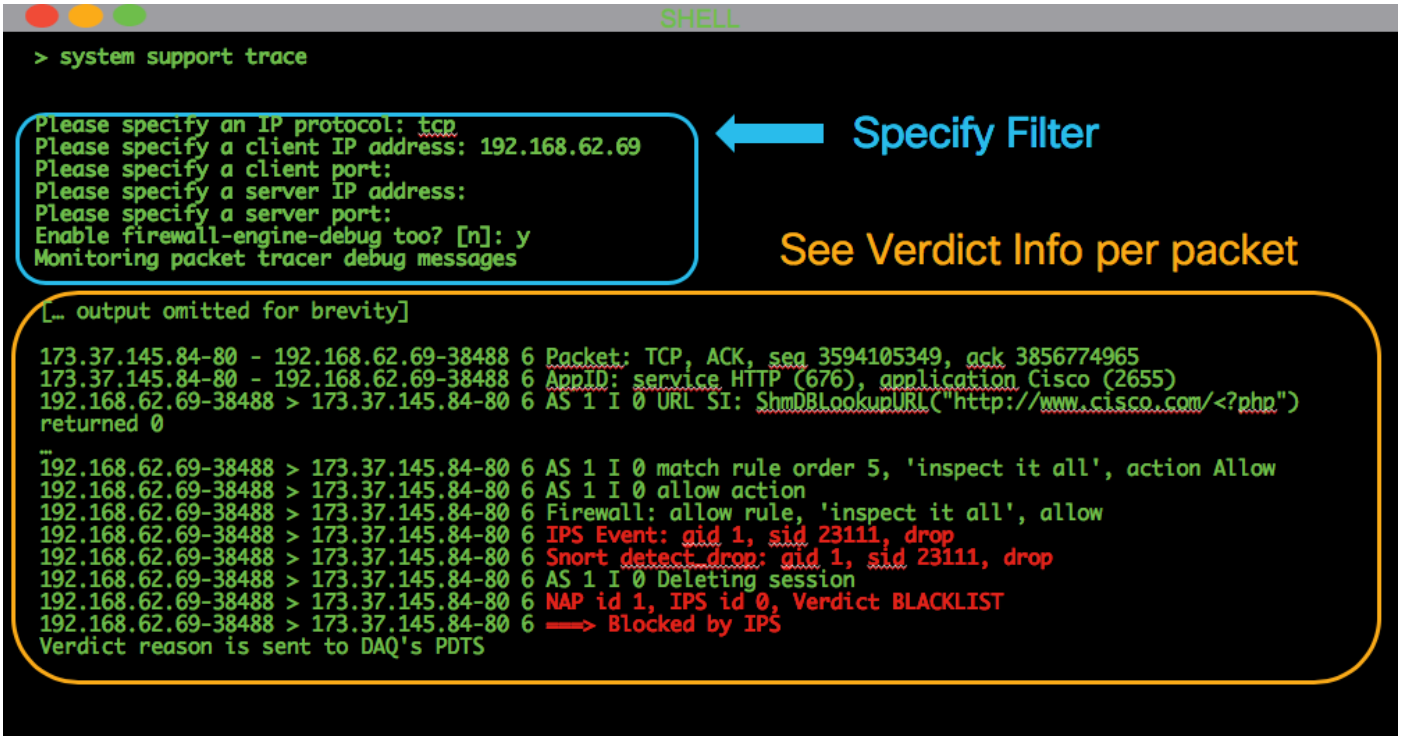
- في قاعدة التحكم بالوصول، ضمن علامة التبويب "فحص"
- في الإجراء الافتراضي
- في علامة التبويب خيارات متقدمة، في **قسم تحليل الشبكة وسياسات الاختراق > سياسة الاختراق المستخدمة قبل تحديد قاعدة التحكم في الوصول**

لمعرفة ما إذا كانت قاعدة سياسة القاحام تقوم بحظر حركة المرور، انتقل إلى **صفحة تحليل > القاحام > الأحداث** في وحدة التحكم في الإدارة الأساسية (FMC). توفر طريقة عرض **جدول أحداث التسلل** معلومات حول الأجهزة المضيفة المشاركة في الأحداث. يرجى الاطلاع

على مقالة أستكشاف أخطاء مسار البيانات وإصلاحها المتعلقة بالمعلومات المتعلقة بتحليل الحدث.

تتمثل الخطوة الأولى الموصى بها لتحديد ما إذا كان توقيع سياسة الاقتحام (IPS) يقوم بحظر حركة المرور في إستخدام ميزة **تتبع دعم الظاهر** من واجهة سطر الأوامر (CLI) الخاصة بـ FTD. يعمل أمر تصحيح الأخطاء هذا بطريقة مشابهة لجدار الحماية-engine-debug، كما أنه يتيح لك خيار تمكين تصحيح أخطاء محرك جدار الحماية بجانب التتبع.

يوضح الرسم التوضيحي التالي مثال لاستخدام أداة تتبع دعم النظام حيث أظهرت النتيجة أنه تم حظر الحزمة بسبب قاعدة التطفل. وهذا يمنحك جميع التفاصيل مثل معرف IPS ومعرف NAP (نهج تحليل الشبكة) ومعرف SID (معرف التوقيع) ومعرف GID (المجموعة) حتى يمكنك الاطلاع على النهج/القاعدة التي تمنع حركة المرور هذه.

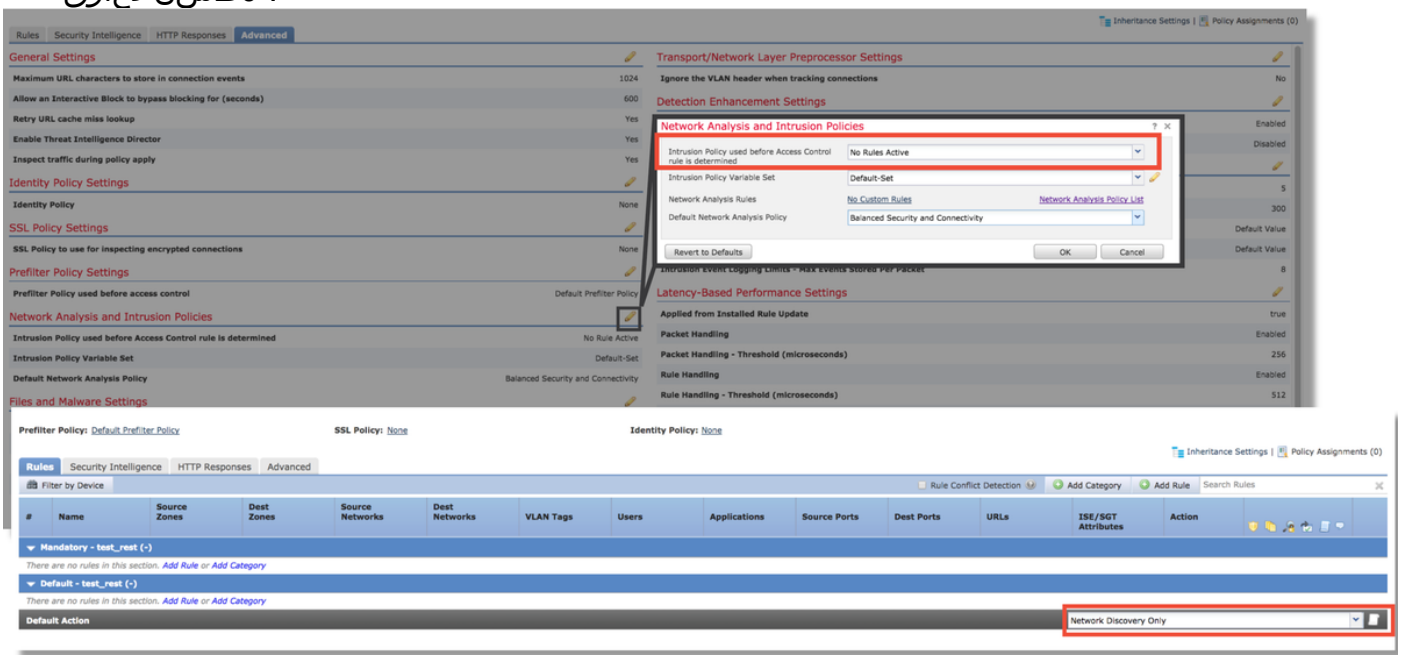


إذا لم تكن قادرا على تحديد أن IPS تقوم بحظر إخراج التتبع، ولكنك تشك في أنه يتم إسقاط IPS بسبب سياسة منع الوصول المخصصة، فيمكنك إستبدال سياسة منع الوصول بنهج "الأمان والاتصال المتوازن" أو نهج "الاتصال عبر الأمان". هذه هي سياسات الاقتحام التي توفرها Cisco. إذا تم إجراء هذا التغيير، فإنه يعمل على حل المشكلة، ومن ثم يمكن أن يكون نهج الاقتحام المخصص المستخدم مسبقا مزعجا من قبل TAC. إذا تم إستخدام سياسة Cisco الافتراضية بالفعل، فيمكنك محاولة تغيير الإعداد الافتراضي إلى نهج أقل أمانا لأن هذه القواعد تحتوي على قواعد أقل، لذلك قد تساعد في تضييق النطاق. على سبيل المثال، إذا تم حظر حركة المرور وأنت تستخدم سياسة متوازنة، ثم تقوم بالتبديل إلى الاتصال عبر سياسة الأمان وتزول المشكلة، فمن المحتمل أن يكون هناك قاعدة في السياسة المتوازنة تسقط حركة المرور التي لم يتم تعييناها للإفلات من الاتصال عبر سياسة الأمان.

يمكن إجراء التغييرات التالية ضمن "نهج التحكم بالوصول" لإزالة جميع إمكانيات كتل فحص نهج التسلل" (ويوصى بإجراء أقل قدر ممكن من التغييرات لعدم تغيير فعالية الأمان، لذا يوصى بوضع قواعد تيار متردد مستهدفة لحركة المرور المعنية، بدلا من تعطيل IPS في السياسة بأكملها):

- في جميع قواعد التحكم بالوصول (أو فقط القاعدة (القواعد) التي تطابق حركة مرور معينة والتي تتأثر)، قم بإزالة سياسة التسلل من علامة التبويب "فحص"
- في علامة التبويب خيارات متقدمة، في **تحليل الشبكة وسياسات الاختراق > نهج**

الاختراق المستخدم قبل تحديد قسم قاعدة التحكم في الوصول، أختر النهج "ال توجد قواعد نشطة".



إذا لم يحل هذا المشكلة بعد، فتقدم إلى أستكشاف أخطاء نهج تحليل الشبكة وإصلاحها.

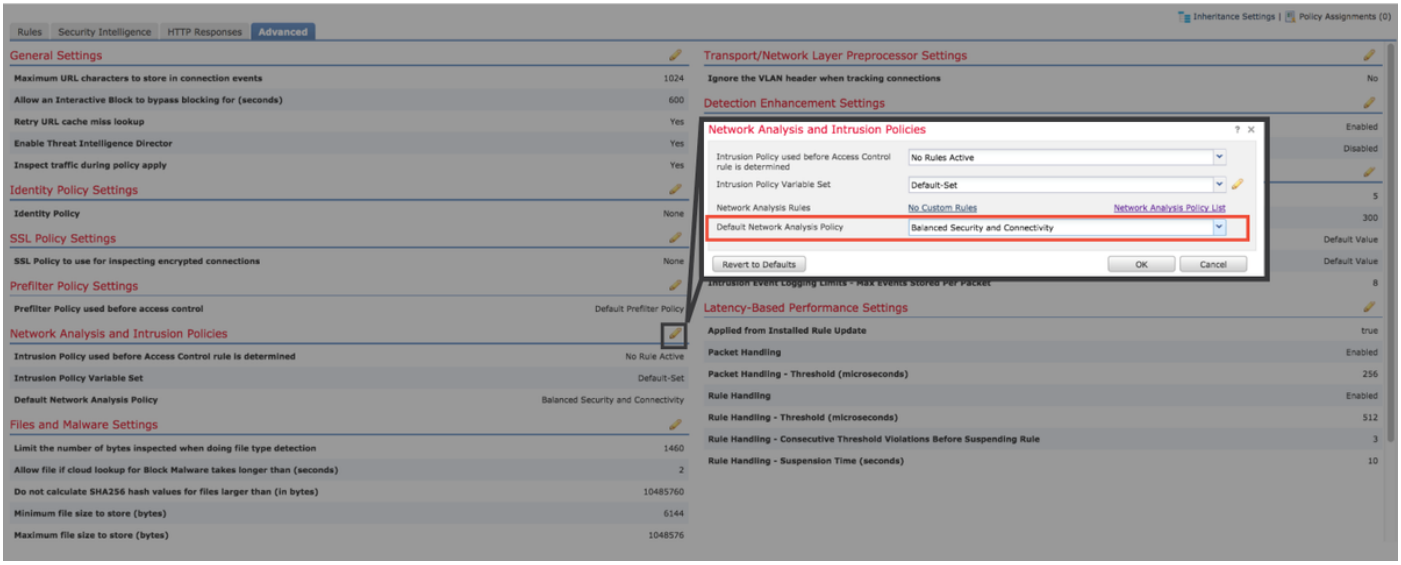
المزيد من التفاصيل حول أستكشاف أخطاء ميزة "سياسة التسلل" وإصلاحها، الرجاء مراجعة مقالة أستكشاف أخطاء مسار البيانات وإصلاحها ذات الصلة.

سياسة تحليل الشبكة

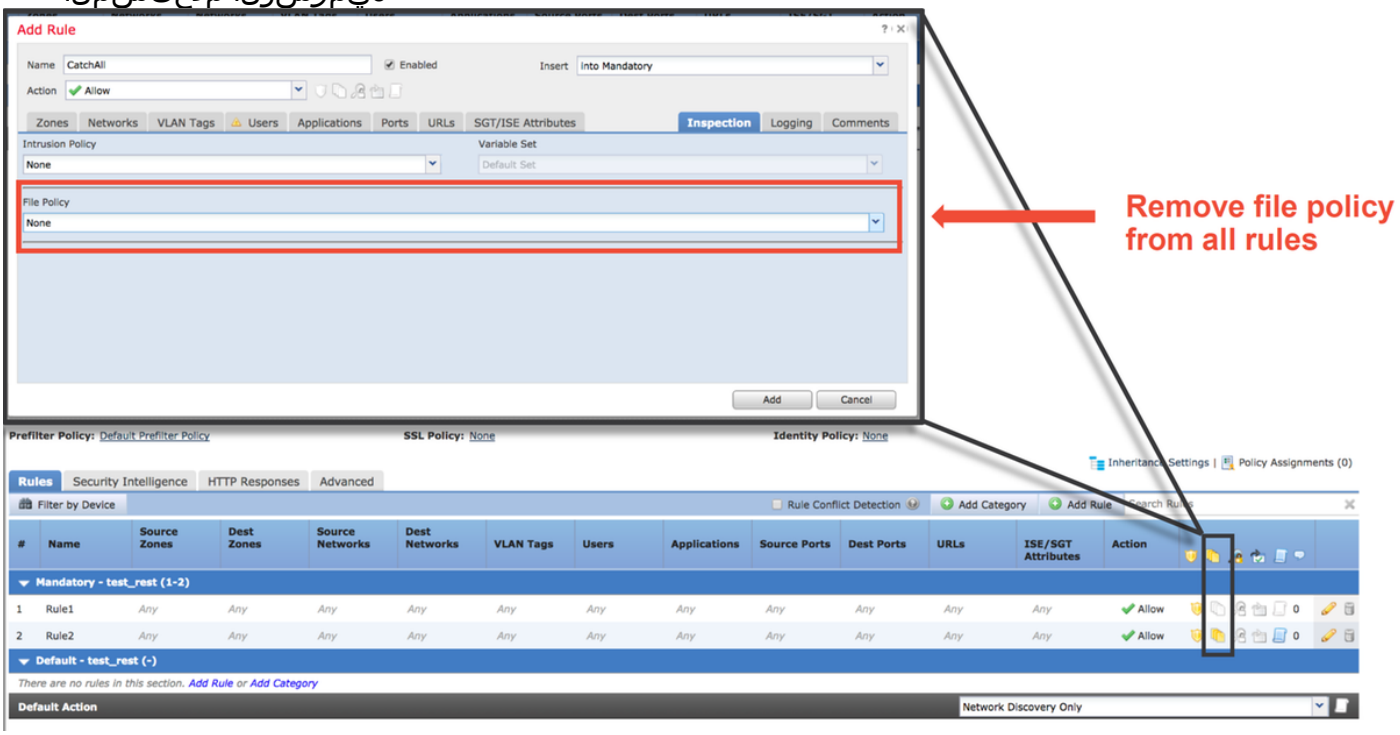
يحتوي نهج تحليل الشبكة (NAP) على إعدادات المعالج المسبق ل FirePOWER، والتي يمكن لبعضها إسقاط حركة المرور. تعد الخطوة الأولى الموصى بها لاستكشاف الأخطاء وإصلاحها هي نفسها كما هو الحال بالنسبة لاستكشاف أخطاء IPS وإصلاحها، والتي تتمثل في إستخدام أداة **> تعقب دعم النظام** لمحاولة العثور على ما يوجد في الخادم الذي يمنع حركة مرور البيانات. راجع قسم "سياسة الاقتحام" أعلاه للحصول على مزيد من المعلومات حول هذه الأداة ومثال الاستخدام.

من أجل تخفيف المشكلات المحتملة المتعلقة ببرنامج العمل الوطني على وجه السرعة، يمكن تنفيذ الخطوات التالية:

- في حالة إستخدام برنامج حماية مستوى التحكم المخصص، استبدل هذا النهج بنهج "الأمان والاتصال المتوازنين" 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، يمكن لإزالته مؤقتا كنهج ملف تمكين إعدادات المعالج المسبق على الطرف الخلفي والتي لن تنعكس في واجهة المستخدم الرسومية



يمكن مراجعة المزيد من التفاصيل حول أستكشاف أخطاء سياسة تحليل الشبكة وإصلاحها في هذه الوثيقة.

معلومات ذات صلة

ارتباطات لوثائق FirePOWER

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

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).