المرحلة 4 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: سياسة التحكم في الوصول

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 وارتباطها بمقالات "أستكشاف أخطاء مسارات البيانات وإصلاحها" الأخرى.

يغطي هذا المقال المرحلة الرابعة من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها، وهي سياسة التحكم في الوصول (ACP). تنطبق هذه المعلومات على جميع الأنظمة الأساسية وإصدارات FirePOWER المدعومة حاليا.

أستكشاف أخطاء مرحلة سياسة التحكم في الوصول (ACP) وإصلاحها

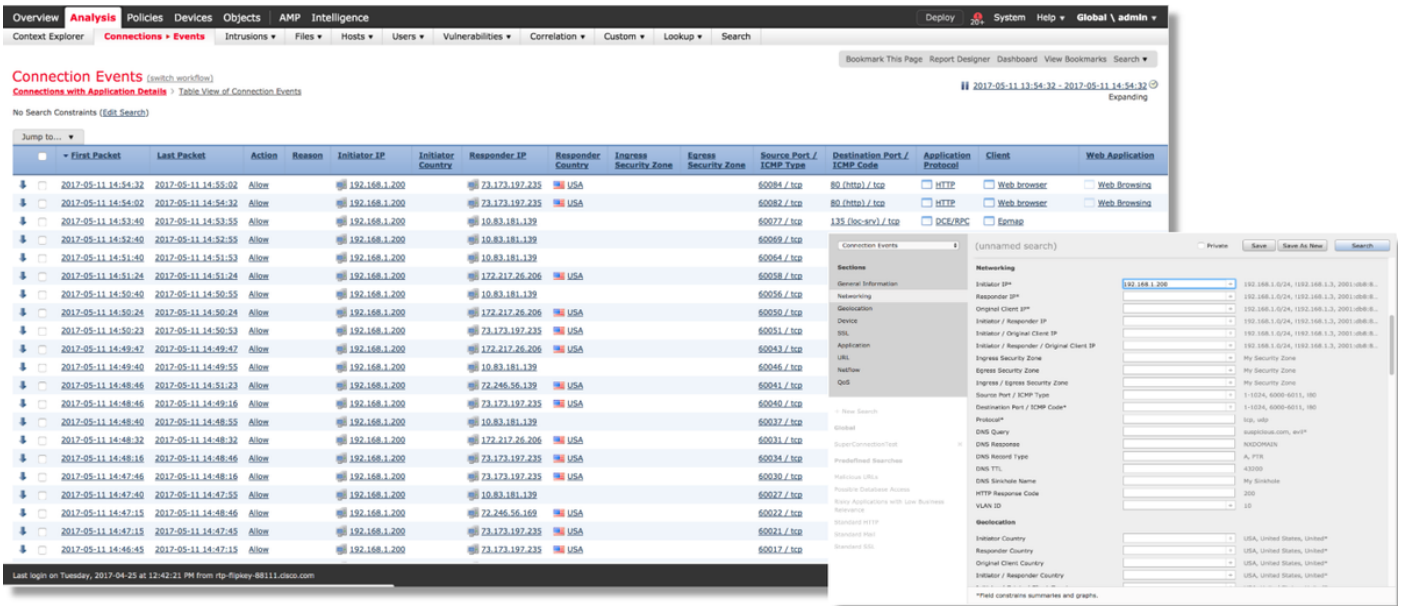
بشكل عام، يجب أن يكون تحديد قاعدة ACP التي يتوافق معها التدفق أمرا مباشرا إلى الأمام. يمكن مراجعة "أحداث الاتصال" لمعرفة القاعدة/الإجراء الذي يتم فرضه. إذا لم يظهر ذلك بوضوح ما تقوم به قائمة التحكم في الوصول (ACP) مع حركة المرور، يمكن تنفيذ تصحيح الأخطاء على واجهة سطر أوامر FirePOWER (CLI).

التحقق من أحداث الاتصال

بعد الحصول على فكرة عن واجهة الدخول والخروج يجب أن تكون حركة المرور مطابقة وكذلك

معلومات التدفق، الخطوة الأولى لتحديد ما إذا كان FirePOWER يمنع التدفق ستكون للتحقق من أحداث الاتصال لحركة المرور المعنية. ويمكن عرض هذه العناصر في مركز إدارة FirePOWER التابع **لتحليل > اتصالات > أحداث.**

ملاحظة: قبل التحقق من أحداث الاتصال، تأكد من تمكين التسجيل في قواعد ACP الخاصة بك. يتم تكوين التسجيل في علامة التبويب "التسجيل" داخل كل قاعدة من قواعد سياسة التحكم في الوصول بالإضافة إلى علامة التبويب "معلومات الأمان". تأكد من تكوين قواعد المشتبه بهم لإرسال السجلات إلى "عارض الأحداث". ينطبق هذا أيضا على الإجراء الافتراضي.



بالنقر فوق "تحرير البحث" وتصفية ملف IP لمصدر فريد (البادئ) يمكنك رؤية التدفقات التي تم اكتشافها بواسطة FirePOWER. يظهر عمود "الإجراء" "السماح" لحركة مرور هذا المضيف.

وإذا كانت قوة النيران تمنع حركة المرور عمدا، فسيتضمن الإجراء كلمة "حظر". يؤدي النقر فوق "عرض جدول أحداث الاتصال" إلى توفير مزيد من البيانات. يمكن مراجعة الحقول التالية في "أحداث الاتصال" إذا كان الإجراء "كتلة":

- السبب

- قاعدة التحكم بالوصول

خطوات التخفيف السريعة

من أجل تخفيف مشكلة يعتقد أنها ناجمة عن قواعد ACP بسرعة، يمكن القيام بما يلي:

- إنشاء قاعدة مع إجراء "الثقة" أو "السماح" لحركة المرور المعنية ووضعها في أعلى قائمة ACP، أو فوق كل قواعد الحظر.
- تعطيل أي قواعد مؤقتا مع إجراء يحتوي على كلمة "حظر"
- إذا تم تعيين الإجراء الافتراضي على "حظر كل حركة المرور"، قم بتحويلها مؤقتا إلى "اكتشاف الشبكة فقط"

ملاحظة: تتطلب هذه التخفيف السريع تغييرات في السياسات قد لا تكون ممكنة في جميع البيئات. يوصى أولا بمحاولة إستخدام تتبع دعم النظام لتحديد القاعدة

التي تتطابق مع حركة المرور قبل إجراء تغييرات النهج.

تصحيح أخطاء ACP

يمكن تنفيذ المزيد من أستكشاف الأخطاء وإصلاحها مقابل عمليات قائمة التحكم في الوصول (ACP) عبر الأداة المساعدة لواجهة سطر الأوامر (CLI) **>دعم النظام** Firewall-**engine-debug**.

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

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

بالنسبة للمثيلات 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
>

تحتوي الأداة المساعدة **لدعم النظام** Firewall-**engine-debug** على إدخال لكل حزمة يتم تقييمها بواسطة ACP. إنها تظهر عملية تقييم القاعدة الجارية، مع لماذا تتوافق القاعدة أو لا تتطابق.

ملاحظة: في الإصدار 6.2 وما بعده، يمكن تشغيل أداة **تتبع دعم النظام**. وهو يستخدم نفس المعلمات ولكنه يتضمن مزيدا من التفاصيل. تأكد من إدخال "y" عند طلبها باستخدام **تمكين جدار الحماية-engine-debug أيضا؟** .

مثال 1: حركة المرور تطابق قاعدة ثقة

في المثال التالي، يتم تقييم إنشاء جلسة عمل SSH باستخدام **تصحيح أخطاء محرك-جدار حماية دعم النظام**.

هذه هي ACP التي يتم تشغيلها على جهاز FirePOWER.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

مجموعة دول أفريقيا والكاريبي والمحيط الهادئ لديها ثلاثة قواعد.

1. القاعدة الأولى هي الثقة في أي حركة مرور من 192.168.0.7 مع منافذ الوجهة المستخدمة من قبل SSH.

2. تفحص القاعدة الثانية كل حركة المرور المستمدة من 10.0.0.0/8 حيث تتطابق معايير الشبكة بناء على بيانات رأس XFF (كما هو موضح بواسطة الرمز الموجود بجوار كائن الشبكة)
3. القاعدة الثالثة تثق في كل حركة المرور من 192.168.62.3 إلى 10.123.175.22

في سيناريو أستكشاف الأخطاء وإصلاحها، يتم تحليل اتصال SSH من 192.168.62.3 إلى 10.123.175.22.

من المتوقع أن تتطابق جلسة العمل مع قاعدة AC 3 "النسخ الاحتياطي لخادم الثقة". السؤال هو، كم عدد الحزم التي يجب أن تستغرقها جلسة العمل هذه لمطابقة هذه القاعدة. هل جميع المعلومات اللازمة في الحزمة الأولى لتحديد قاعدة AC أو الحزم المتعددة مطلوبة، وإذا كان الأمر كذلك، فما هو الرقم؟

على واجهة سطر أوامر (CLI) Firepower، تم إدخال ما يلي لرؤية عملية تقييم قاعدة قائمة التحكم في الوصول (ACP).

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **تلميح**: من الأفضل تعبئة أكبر عدد ممكن من المعلمات عند تشغيل **تصحيح أخطاء محرك جدار الحماية**، بحيث تتم طباعة رسائل تصحيح الأخطاء المثيرة فقط على الشاشة.

في إخراج تصحيح الأخطاء أدناه، ترى الحزم الأربع الأولى من الجلسة التي يتم تقييمها.

سين

سين، آك

آكلة

حزمة SSH الأولى (من عميل إلى خادم)

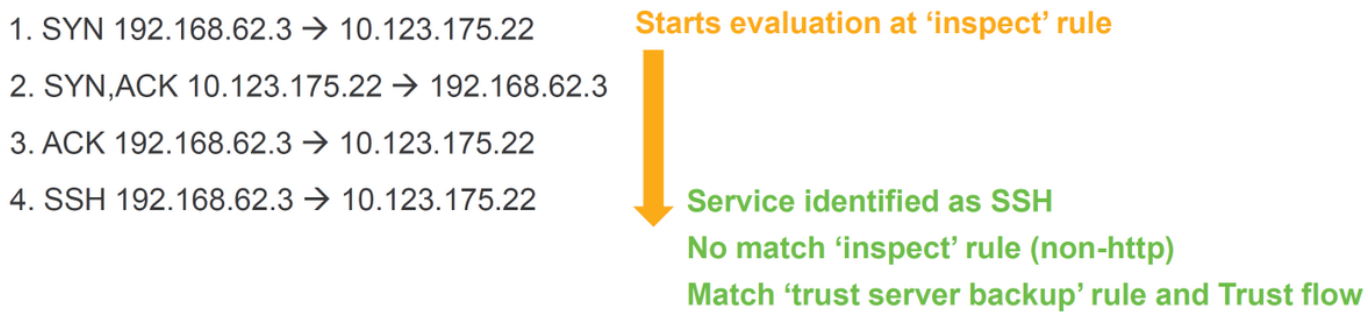
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

هذا رسم بياني يوضح منطق تصحيح الأخطاء بشكل أكبر.



بالنسبة لهذا التدفق، يلزم 4 حزم للجهاز لمطابقة القاعدة.

هذا شرح تفصيلي لمخرج تصحيح الأخطاء.

- تبدأ عملية تقييم ACP في قاعدة "فحص" لأن قاعدة "trust ssh for host" لم تتطابق لأن عنوان IP لم يتطابق مع المتطلبات. هذه مطابقة سريعة بسبب جميع المعلومات اللازمة لتحديد ما إذا كان يجب أن تتطابق هذه القاعدة موجودة في الحزمة الأولى (IPs والمنافذ)
- لا يمكن تحديد ما إذا كانت حركة المرور تطابق قاعدة "فحص" حتى يتم تحديد التطبيق، نظرًا لوجود معلومات X-Forwarding-for (XFF) في حركة مرور تطبيق HTTP، فإن التطبيق غير معروف بعد، لذلك فإن هذا يضع جلسة العمل في حالة معلقة للقاعدة 2، في انتظار بيانات التطبيق.
- بمجرد تحديد التطبيق في الحزمة الرابعة، ينتج عن قاعدة "الفحص" عدم تطابق، نظرًا لأن التطبيق هو SSH، بدلا من HTTP
- ثم تتم مطابقة قاعدة "النسخ الاحتياطي للخادم الموثوق به"، استنادا إلى عناوين IP.

باختصار، يتطلب الاتصال 4 حزم لمطابقة جلسة العمل لأنه يجب عليه انتظار جدار الحماية لتحديد التطبيق نظرا لأن القاعدة 2 تحتوي على قيد تطبيق فيها.

إذا كانت القاعدة 2 تتضمن شبكات مصدر فقط ولم تكن XFF، لكان قد تطلب ذلك حزمة واحدة لمطابقة الجلسة.

يجب دائما وضع التطابقات 1-4 فوق كل القواعد الأخرى في السياسة عندما يكون ذلك ممكنا لأن هذه القواعد تتطلب عادة حزمة واحدة لاتخاذ قرار. ومع ذلك، قد تلاحظ أيضا أنه حتى مع وجود التطابقات 1-4 المسطرة فقط، قد يكون أكثر من حزمة واحدة فقط لمطابقة قاعدة تاي متردد، وسبب ذلك هو ذكاء أمان URL/DNS. إذا كان لديك أي من هذين الممكنين، فيجب على جدار الحماية تحديد التطبيق لجميع الجلسات التي يتم تقييمها بواسطة نوع AC لأنه يجب أن يحدد ما إذا كانت HTTP أو DNS. وبعد ذلك، يجب أن تحدد ما إذا كان ينبغي لها أن تسمح بالجلسة استنادا إلى القواعد السوداء.

فيما يلي إخراج مقتطع من الأمر **firewall-engine-debug**، والذي يحتوي على الحقول ذات الصلة مبرزة بالأحمر. لاحظ الأمر المستخدم للحصول على اسم التطبيق المعرف.

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[...omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

المثال 2: تم حظر حركة المرور المطابقة لقاعدة ثقة

في بعض السيناريوهات، يمكن حظر حركة المرور على الرغم من مطابقة قاعدة ثقة في ACP. يقيم المثال التالي حركة المرور باستخدام نفس نهج التحكم في الوصول والأجهزة المضيفة.

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, 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
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

كما يظهر أعلاه، يظهر إخراج **جدار الحماية-المحرك-تصحيح الأخطاء** أن حركة المرور تطابق مع "ثقة"، في حين تظهر أحداث الاتصال إجراء **الحظر** بسبب قاعدة سياسة التسلل (محددة لأن عمود السبب يعرض **كتلة التسلل**).

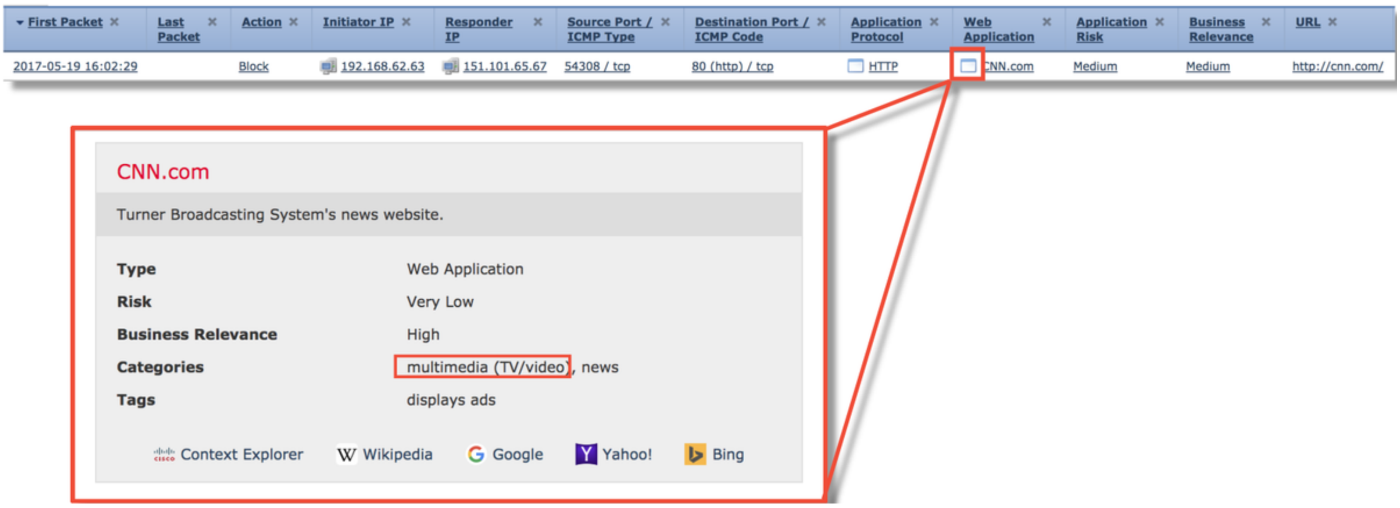
يرجع سبب حدوث ذلك إلى **نهج القاحة المستخدم قبل تحديد** الإعداد **لقاعدة التحكم في الوصول** في عالمة التبويب **خيارات متقدمة** في قائمة التحكم في الوصول (ACP). قبل إمكانية الوثوق بحركة المرور وفقا لإجراء القاعدة، يقوم نهج التسلل المعني بتعريف تطابق النمط وإسقاط حركة المرور. ومع ذلك، ينتج عن تقييم قاعدة ACP تطابق قاعدة الثقة، نظرا لأن عناوين IP تطابق معايير قاعدة "النسخ الاحتياطي لخادم الثقة".

وحتى لا تخضع حركة المرور للتفتيش على سياسة القاحة، يمكن وضع قاعدة الثقة فوق قاعدة "التفتيش"، التي ستكون أفضل ممارسة في كلتا الحالتين. ونظرا لأن تعريف التطبيق ضروري لمطابقة قاعدة "الفحص" وعدم مطابقتها، فإن **سياسة التسلل المستخدمة قبل تحديد قاعدة التحكم في الوصول** يتم إستخدامها لحركة المرور التي يتم تقييمها من قبل نفس المجموعة. يؤدي وضع قاعدة "النسخ الاحتياطي لخادم الثقة" فوق قاعدة "الفحص" إلى مطابقة حركة مرور البيانات للقاعدة عند رؤية الحزمة الأولى نظرا لأن القاعدة تستند إلى عنوان IP، والذي يمكن تحديده في الحزمة الأولى. لذلك، ال يلزم إستخدام **سياسة التسلل المستخدمة قبل تحديد قاعدة التحكم في الوصول**.

السيناريو 3: حظر حركة المرور بواسطة رقم التطبيق

في هذا السيناريو، يبلغ المستخدمون عن أنه يتم حظر cnn.com. غير أنه لا توجد قاعدة محددة تمنع السي ان ان. تظهر أحداث الاتصال، بالاقتران مع إخراج **جدار الحماية-engine-debug**، سبب الحظر.

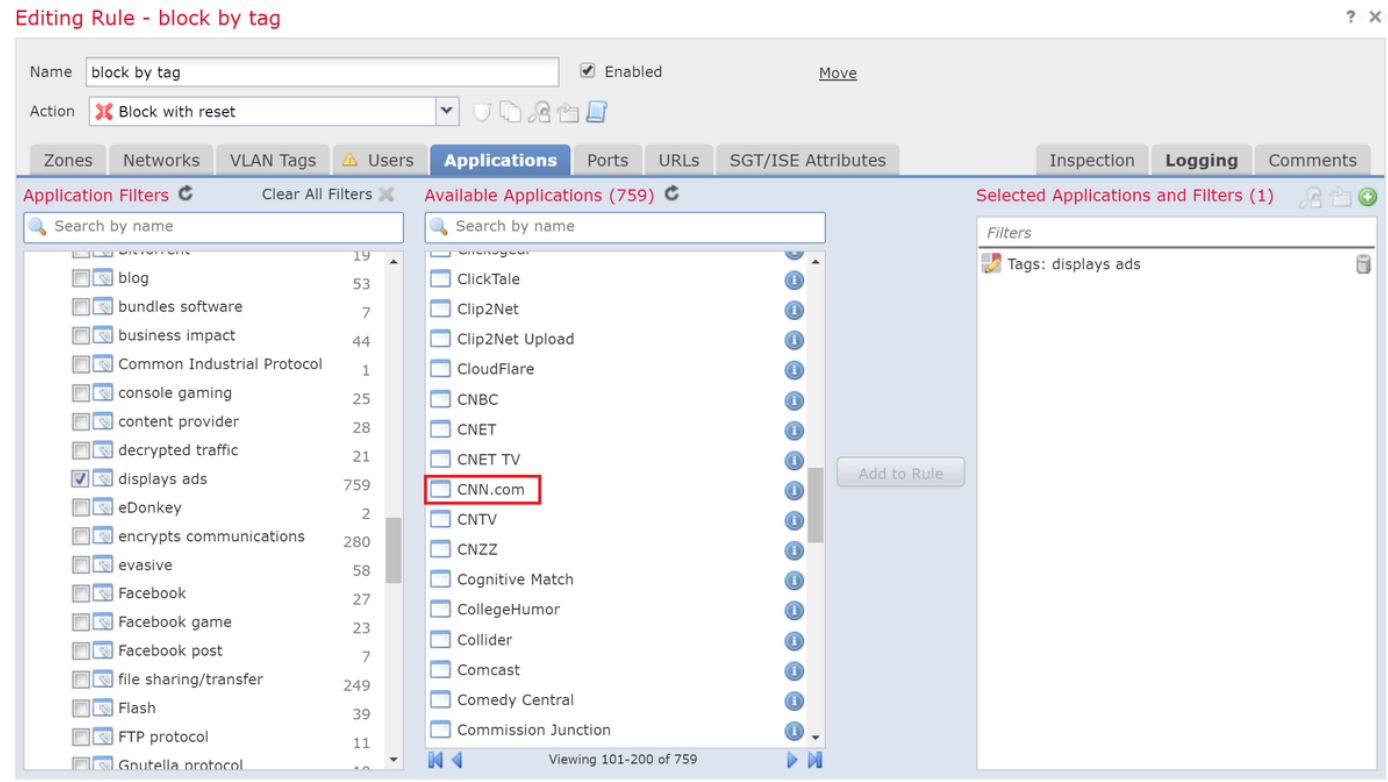
أولا، تحتوي "أحداث الاتصال" على مربع معلومات بجوار حقول التطبيق تظهر معلومات حول التطبيق بالإضافة إلى كيفية تصنيف FirePOWER للتطبيق المذكور.



بوضع هذه المعلومات في الاعتبار، يتم تشغيل **جدار الحماية-المحرك-تصحيح الأخطاء**. في إخراج تصحيح الأخطاء، يتم حظر حركة المرور استنادا إلى علامة التطبيق.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

على الرغم من عدم وجود قاعدة تمنع بشكل صريح http://cnn.com، يتم حظر **إعلانات العرض** التي تم وضع علامة عليها داخل علامة التبويب **تطبيقات** لقاعدة ACP.



البيانات التي سيتم تقديمها إلى TAC

البيانات	تعليمات
أستكشاف أخطاء الملف وإصلاحها من جهاز FirePOWER الذي يقوم بفحص حركة المرور	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1
خرج **جدار الحماية-المحرك-تصحيح الأخطاء ودعم النظام**-trtrace	طالع هذه المقالة للحصول على تعليمات
تصدير سياسة التحكم بالوصول	انتقل إلى **نظام > أدوات > إستيراد / تصدير**، حدد سياسة التحكم في الو

تحذير: إذا كانت قائمة التحكم في الوصول (ACP) تحتوي على سياسة SSL، فقم بإزالة سياسة SSL من قائمة التحكم في الوصول (ACP) قبل التصدير لتجنب الكشف عن معلومات PKI الحساسة

الخطوة التالية: أستكشاف أخطاء طبقة نهج SSL وإصلاحها

إذا كان نهج SSL قيد الاستخدام ولم يكشف أستكشاف أخطاء نهج التحكم في الوصول عن المشكلة، فإن الخطوة التالية هي أستكشاف أخطاء نهج SSL 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).