Firepower資料路徑故障排除第4階段：訪問控制策略

目錄

簡介

本文是一系列文章的一部分，這些文章介紹了如何對Firepower系統的資料路徑進行系統故障排除，以確定Firepower的元件是否影響流量。請參閱概述文章，瞭解有關Firepower平台架構的資訊，以及指向其他資料路徑故障排除文章的連結。

本文涵蓋Firepower資料路徑故障排除的第四階段，即訪問控制策略(ACP)。 此資訊適用於當前所有支援的Firepower平台和版本。

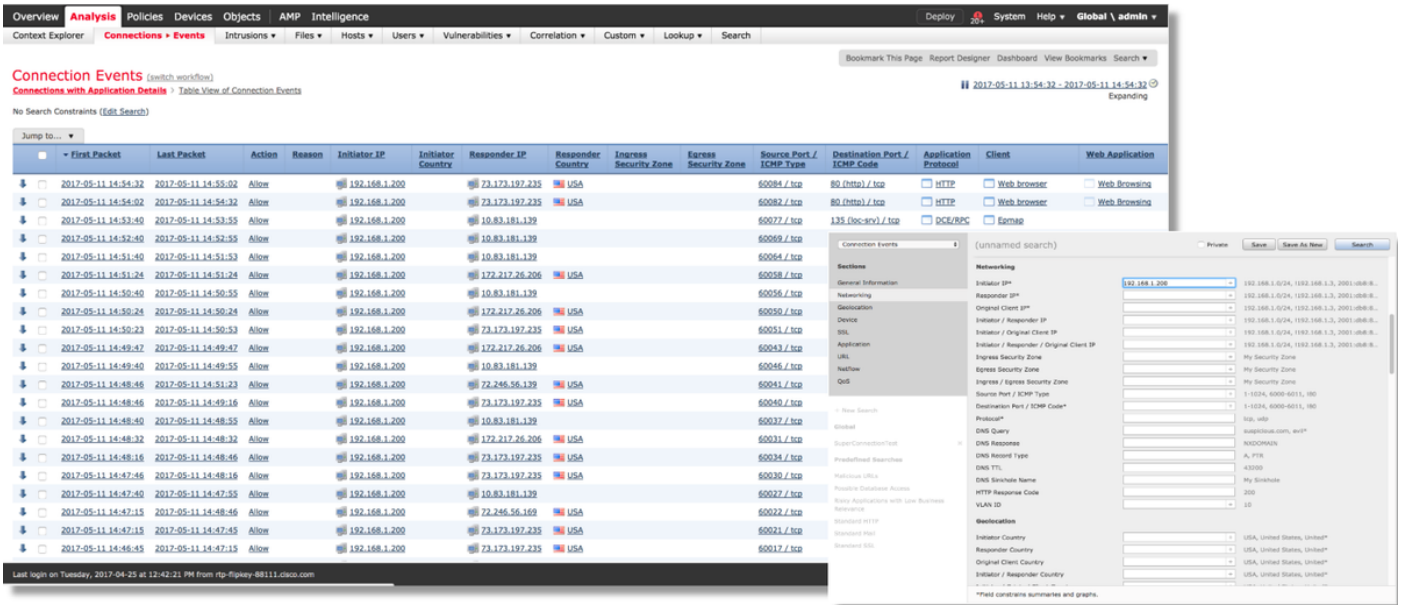
訪問控制策略(ACP)階段故障排除

一般來說，確定一個流匹配的ACP規則應該非常直觀。可以檢視「連線事件」，以檢視正在執行哪個規則/操作。如果這沒有清楚地顯示ACP對流量執行的操作，則可以在Firepower命令列介面(CLI)上執行調試。

檢查連線事件

瞭解了入口和出口介面後，流量應匹配以及流量資訊，識別Firepower是否阻止流量的第一步是檢查相關流量的連線事件。可在Firepower管理中心的**分析>連線>事件**下檢視這些資訊。

> **附註**：檢查連線事件之前，請確保在ACP規則中啟用日誌記錄。日誌記錄在每個訪問控制策略規則中的「日誌記錄」頁籤以及安全情報頁籤中配置。確保將可疑規則配置為將日誌傳送到「事件檢視器」。 這也適用於預設操作。



通過按一下「編輯搜尋」並按唯一的源（啟動器）IP進行過濾，您可以看到Firepower檢測到的流。「操作」列對此主機的流量顯示「允許」。

如果Firepower有意阻止流量，則操作將包含「阻止」一詞。 按一下「連線事件的表檢視」可提供更多資料。如果操作為「Block」，則可以檢視連線事件中的以下欄位：

— 原因

— 訪問控制規則

快速緩解步驟

為了快速緩解據信由ACP規則引起的問題，可以執行以下操作：

- 為相關流量建立具有「信任」或「允許」操作的規則，並將其置於ACP的最頂端，或者在所有塊規則之上。
- 使用包含「Block」一詞的操作暫時禁用所有規則
- 如果Default Action設定為「Block All Traffic」，請暫時將其切換到「Network Discovery Only」

> **附註**：這些快速緩解需要策略更改，而並非在所有環境中都如此。建議先嘗試使用系統支援跟蹤來確定流量匹配的規則，然後再進行策略更改。

調試ACP

通過> system support firewall-engine-debug CLI實用程式可以針對ACP操作執行進一步的故障排除。

> **附註**：在Firepower 9300和4100平台上，可以通過以下命令訪問有關外殼：
>
> **# connect module 1主控台**
> Firepower-module1> **connect ftd**
> **>**

對於多例項，可以使用以下命令訪問邏輯裝置CLI。
 # connect module 1 telnet
Firepower-module1> **connect ftd ftd1**
正在連線到容器ftd(ftd1)控制檯……輸入「exit」以返回啟動CLI
>

system support firewall-engine-debug實用程式包含由ACP評估的每個資料包的條目。它顯示發生的規則評估過程，以及規則匹配或不匹配的原因。

附註：在6.2及更高版本中，可以運行**系統支援跟蹤**工具。它使用相同的引數，但包含更多詳細資訊。當提示輸入「**Enable firewall-engine-debug too？**」時，請務必輸入「y」。

範例 1：流量匹配信任規則

在下面的示例中，使用**system support firewall-engine-debug**評估SSH會話的建立。

這是Firepower裝置上運行的ACP。

#	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

ACP有三個規則。

1. 第一條 規則是信任來自192.168.0.7的所有流量與SSH使用的目標埠。
2. 第二個規則根據XFF報頭資料檢查源自10.0.0.0/8的所有流量（如網路對象旁邊的圖示所示），其中網路條件匹配
3. 第三條 規則信任從192.168.62.3到10.123.175.22的所有流量

在故障排除場景中，正在分析從192.168.62.3到10.123.175.22的SSH連線。

預期會話與AC規則3「信任伺服器備份」匹配。 問題在於，此作業階段需要多少封包才能與此規則相符。第一個資料包中是否需要所有資訊來確定AC規則或需要多個資料包？如果是，需要多少個資料包？

在Firepower CLI上，輸入以下內容以檢視ACP規則評估流程。

```
>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
```

提示：最好在運行**firewall-engine-debug**時填寫儘可能多的引數，以便僅顯示感興趣的調試消

息。

在下面的調試輸出中，您會看到正在評估的會話的前四個資料包。

SYN

SYN，ACK

ACK

第一個SSH資料包（客戶端到伺服器）

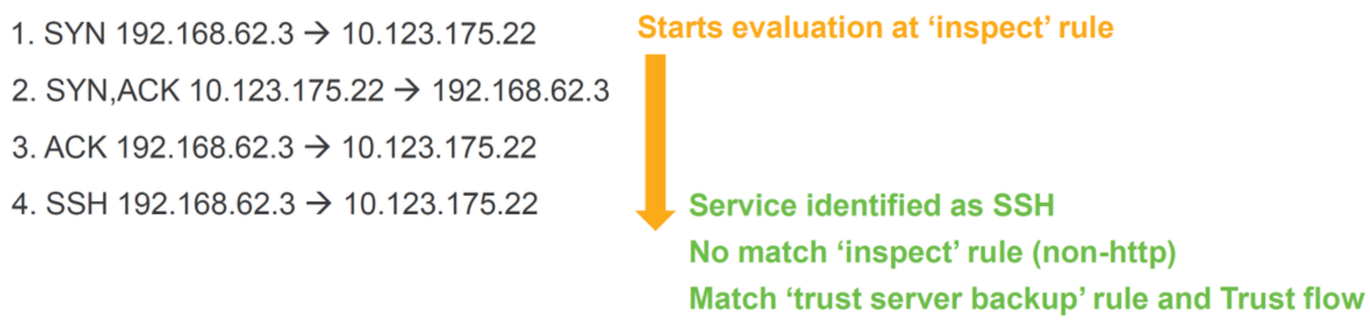
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType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

這是一個進一步說明調試邏輯的圖表。



對於此流，裝置需要4個資料包才能匹配規則。

以下是偵錯輸出的詳細說明。

- ACP評估過程從「檢查」規則開始，因為「主機的信任ssh」規則不匹配，因為IP地址不符合要求。這是一個快速匹配，因為判斷此規則是否匹配所需的所有資訊都存在於第一個資料包（IP和埠）中
- 在識別應用之前，無法確定流量是否與「inspect」規則匹配，因為在HTTP應用流量中發現X-Forwarded-For(XFF)資訊，但應用尚未知，因此這會將規則2的會話置於掛起狀態，掛起應用資料。
- 在第四個資料包中標識應用後，「inspect」規則將產生不匹配結果，因為應用是SSH而不是HTTP
- 然後根據IP地址匹配「信任伺服器備份」規則。

總之，連線需要4個資料包來匹配會話，因為它必須等待防火牆識別應用程式，因為規則2中含有應用程式約束。

如果規則2隻有來源網路，而不是XFF，則這將需要1個封包來匹配作業階段。

在可能的情況下，應始終將第1-4層規則置於策略中的所有其他規則之上，因為這些規則通常需要1個資料包才能做出決定。但是，您可能也注意到，即使僅使用第1-4層規則，匹配交流規則可能也不會只使用1個資料包，這是因為URL/DNS安全情報。如果其中任何一個啟用，防火牆必須確定由AC策略評估的所有會話的應用程式，因為它必須確定它們是HTTP還是DNS。然後，它必須根據黑名單確定是否允許會話。

以下是**firewall-engine-debug**命令的截斷輸出，其中相關欄位以紅色突出顯示。記下用於獲取已標識的應用程式名稱的命令。

```
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
```

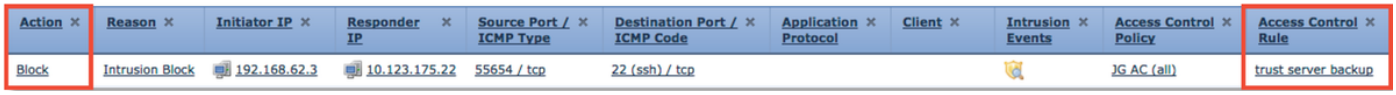
範例 2：與信任規則匹配的流量被阻止

在某些情況下，儘管匹配了ACP中的信任規則，仍可以阻止流量。以下示例評估具有相同訪問控制策略和主機的流量。

```
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

如上所示，**firewall-engine-debug**輸出顯示流量與「信任」匹配，而連線事件顯示由於入侵策略規則導致的**阻止**操作(由於「原因」列顯示**入侵阻止**而確定)。

發生這種情況的原因是**在訪問控制規則被確定**在ACP上**Advanced**頁籤中的Setting之前使用的入侵策略。在根據規則操作對流量進行信任之前，相關入侵策略會識別模式匹配並丟棄流量。但是，由於IP地址與「信任伺服器備份」規則的條件匹配，因此ACP規則評估的結果與信任規則匹配。

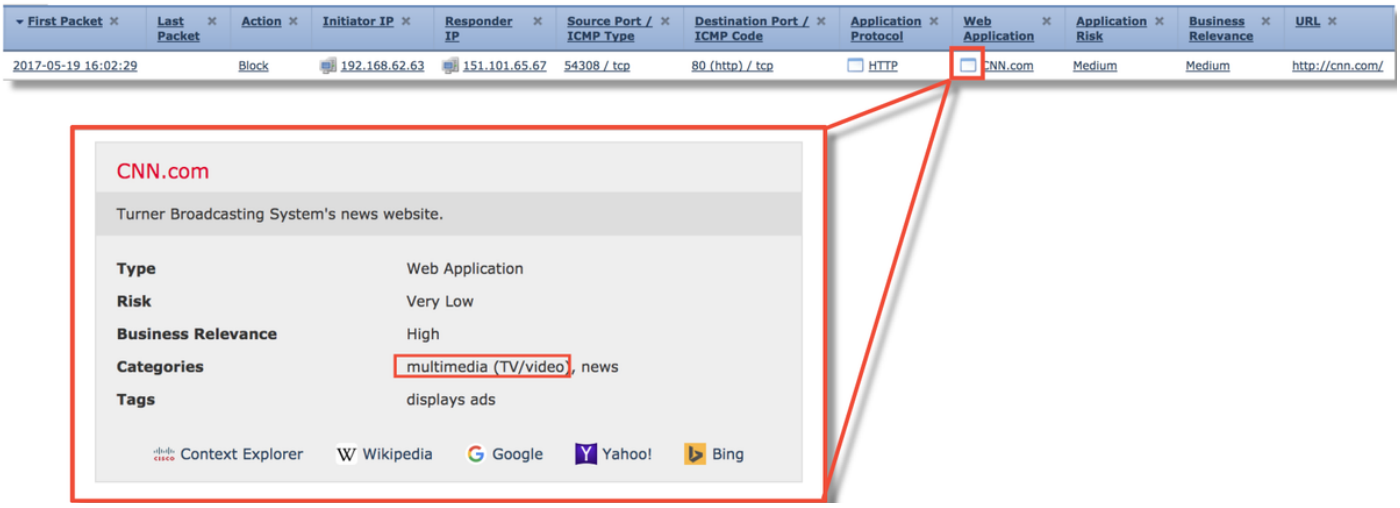
為了使流量不經過入侵策略檢測，可以將信任規則置於「inspect」規則之上，這是兩種情況下的最佳實踐。由於應用程式標識對於「檢查」規則的匹配和不匹配是必需的，因此確定訪問控制規則之

前使用的入侵策略(**Intrusion Policy)將用於該規則評估的流**量。將「trust server backup」規則置於「inspect」規則之上會導致在發現第一個資料包時流量與規則匹配，因為該規則基於IP地址，而第一個資料包中可以確定該IP地址。因**此,確定訪問控制規則之前使用的**入侵策略不需要使用。

案例 3:流量被應用標籤阻止

在此案例中，使用者報告正在阻止cnn.com。不過，並沒有什麼具體的規定會阻止CNN的播出。連線事件以及**firewall-engine-debug**輸出會顯示阻止的原因。

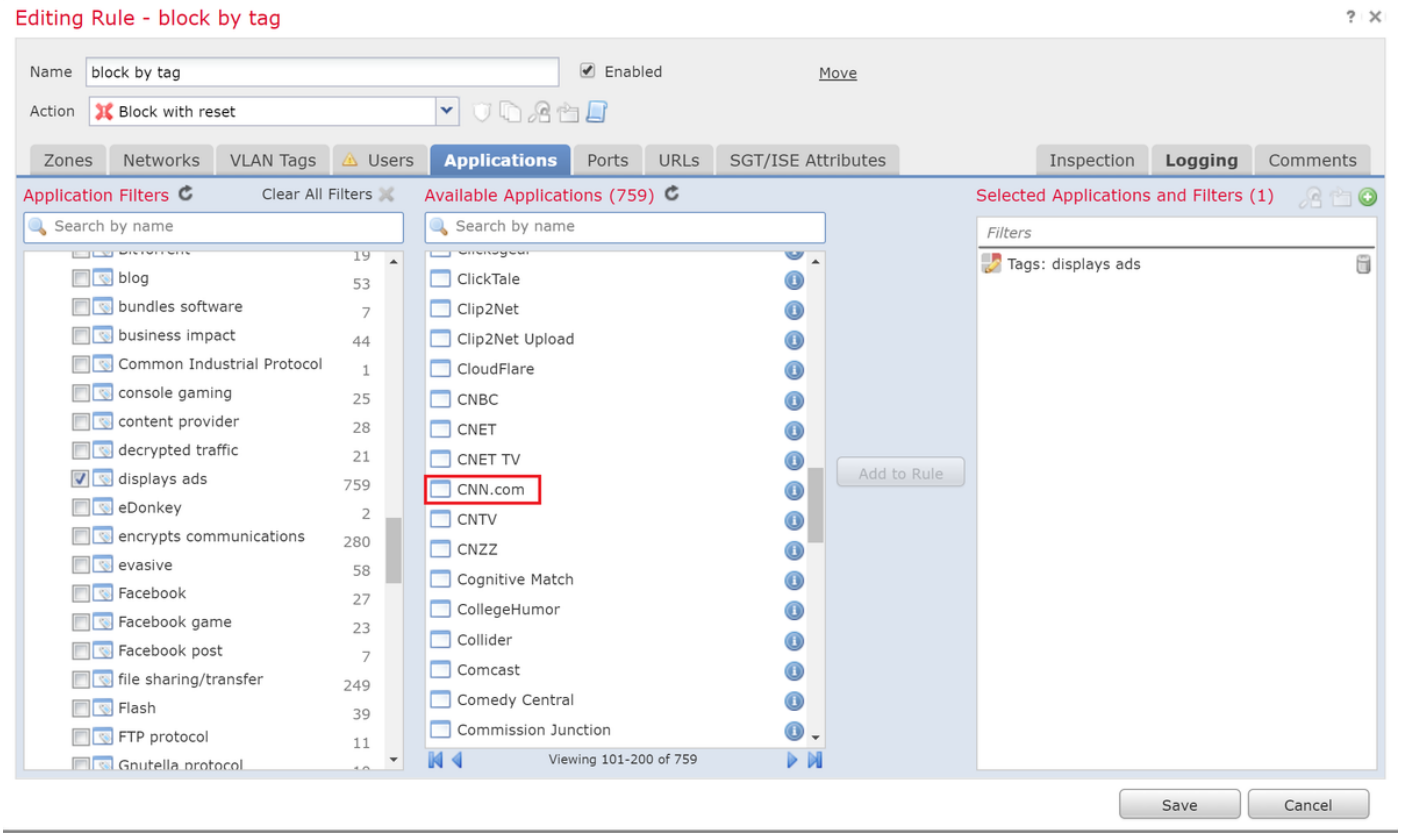
首先，「連線事件」在應用程式欄位旁邊有一個資訊框，其中顯示有關應用程式的資訊以及Firepower對此應用程式的分類方式。



記住此資訊後，會執行**firewall-engine-debug**。在調試輸出中，根據應用標籤阻止流量。

```
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
```

即使沒有明確阻止http://cnn.com的規則，ACP規則的**Applications**頁籤中仍會阻止已標籤的廣告。



要提供給TAC的資料

資料	說明
檢查流量的Firepower裝置的故障排除檔案	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-
system support firewall-engine-debug和**system-support-trace**輸出	有關說明，請參閱本文
訪問控制策略匯出	導航到**System > Tools > Import/Export**，選擇Access Control P

注意：如果ACP包含SSL策略，請在匯出之前從ACP中刪除SSL策略，以避免洩露敏感的PKI資訊

下一步：SSL策略層故障排除

如果正在使用SSL策略，並且訪問控制策略故障排除未發現問題，則下一步是對SSL策略進行故障排除。

按一下here繼續下一篇文章。