Firepower資料路徑故障排除第7階段：入侵原則

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。

本文介紹Firepower資料路徑故障排除的第七階段，即入侵策略功能。

必要條件

- 本文適用於運行入侵策略的所有Firepower平台 **trace**功能僅在6.2版及更高版本中可用，僅適用於Firepower威脅防禦(FTD)平台
- 瞭解開源Snort有所幫助，但並非必需 有關開源Snort的資訊，請訪問https://www.snort.org/

入侵策略階段故障排除

使用「trace」工具檢測入侵策略丟棄（僅限FTD）

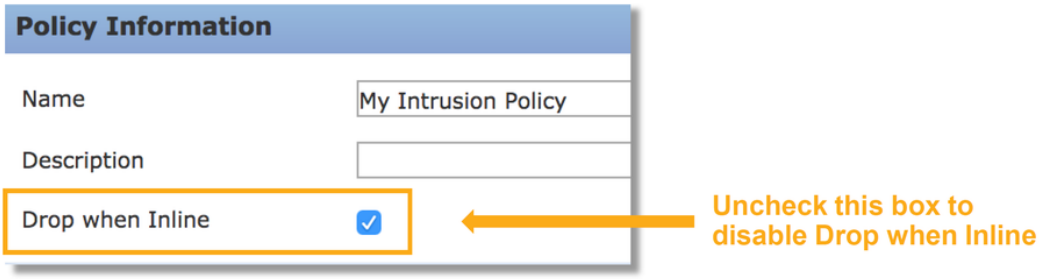
系統支援追蹤工具可從FTD指令行介面(CLI)執行。 這與訪問控制策略階段文章中提到的**firewall-engine-debug**工具類似，不同之處在於它深入瞭解Snort的內部工作方式。這有助於檢視是否有任何入侵策略規則正在觸發相關流量。

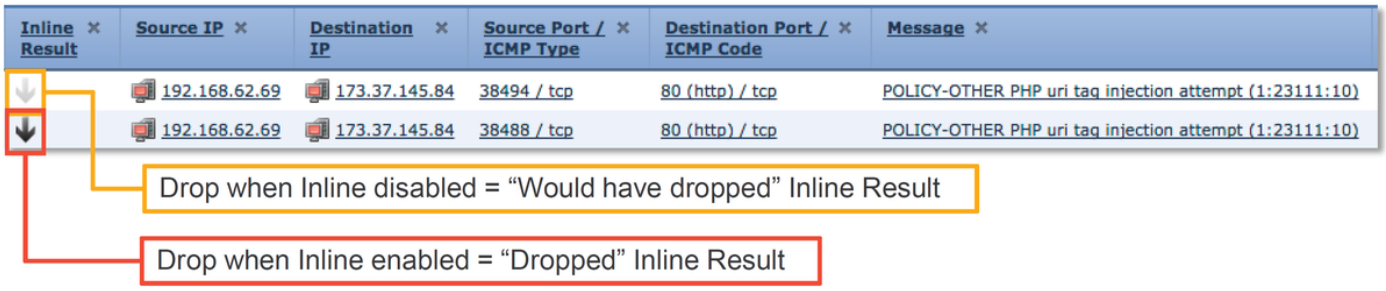
在以下示例中，來自IP地址為192.168.62.6的主機的流量被入侵策略規則阻止(在本例中為**1:2311**)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
…
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

請注意，Snort應用的操作已刪除。當snort檢測到丟棄時，該特定會話會被列入黑名單，以便同時丟棄其他資料包。

snort能夠執行**drop**操作的原因在於，在入侵策略中啟用了「Drop when Inline」選項。這可在入侵策略內的初始登入頁面中驗證。在Firepower管理中心(FMC)中，導航到**Policies > Access Control > Intrusion**，然後按一下相關策略旁邊的編輯圖示。





如果禁用「在內聯時丟棄」，Snort不再丟棄違規資料包，但它仍然會發出警報，在入侵事件中顯示**Inline Result**為「Would Have Dropped」。

停用「Drop When Inline」後，追蹤輸出會顯示有關**流量**作業階段的**would** drop動作。

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

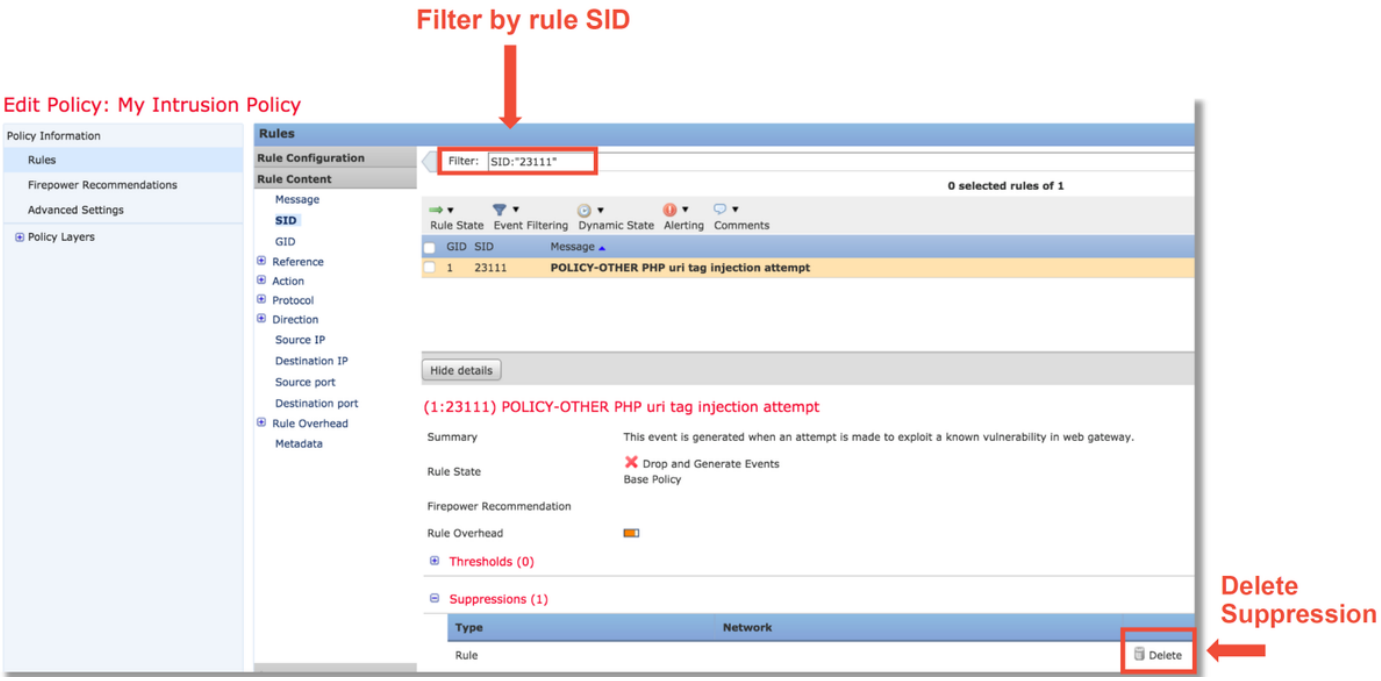
檢查入侵策略中的抑制

snort可能會捨棄流量，而不將入侵事件傳送到FMC（靜默捨棄）。 這是通過配置抑制來**完成的。** 為了驗證入侵策略中是否配置了任何抑制，可以在後端檢查專家外殼，如下圖所示。

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name        : My Intrusion Policy
```

請注意，名為「My Intrusion Policy」的入侵策略包含對1:S規則的23111制。因此，根據此規則，流量可能遭捨棄，而且沒有任何事件。這是跟蹤實用程式可以發揮作用的另一個原因，因為它仍然顯示發生丟包。

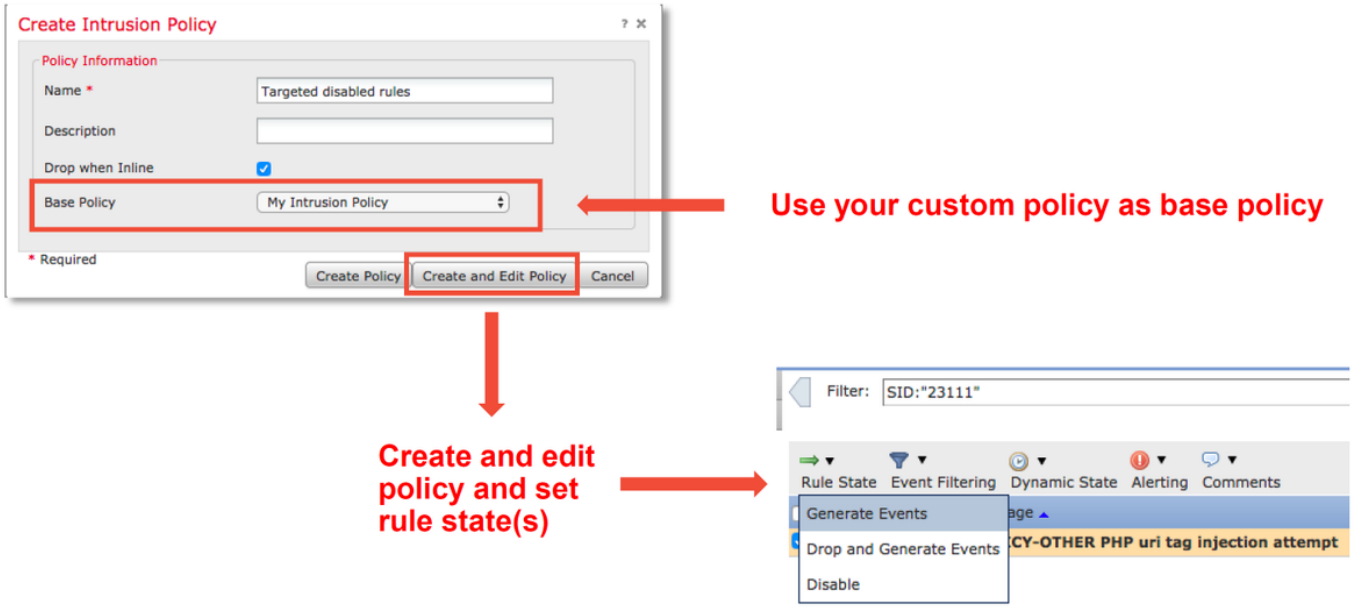
若要刪除抑制，可以在Intrusion Policy **Rules** 檢視內篩選相關規則。此時會出現一個刪除抑制的選項，如下所示。



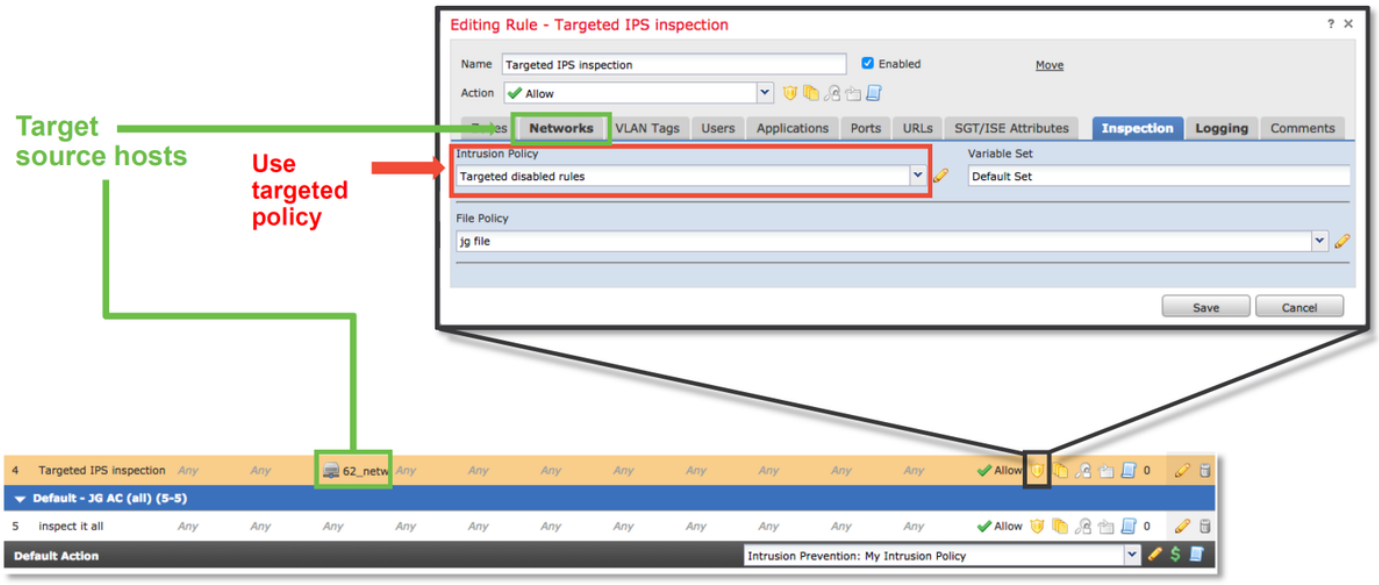
建立目標入侵策略

如果流量被特定入侵策略規則丟棄，您可能不希望相關流量被丟棄，但也可能不希望禁用該規則。解決方案是在禁用違規規則的情況下建立新的入侵策略，然後讓它評估來自目標主機的流量。

以下說明如何建立新的入侵策略(在**Policies > Access Control > Intrusion**下)。



建立新的入侵策略後，可以在新的訪問控制策略規則中使用，該規則以相關主機為目標，這些主機的流量之前已被原始入侵策略丟棄。



誤報故障排除

常見的情況是對入侵事件進行誤報分析。在開啟假陽性病例之前可以檢查以下幾點。

1.在**Table View of Intrusion Events**頁面中，按一下相關事件的覈取方塊

2.按一下**Download Packets**，獲取觸發入侵事件時Snort捕獲的資料包。

3.按一下右鍵**消息**列中的規則名稱，然後按一下**規則文檔**，以檢視規則語法和其他相關資訊。

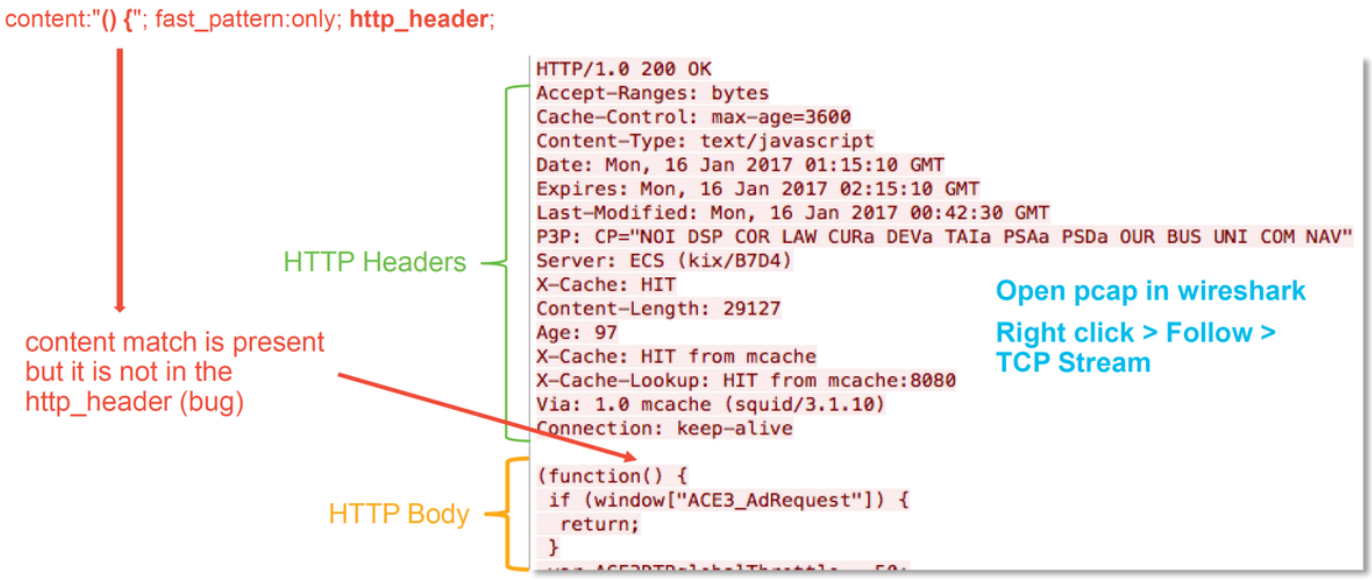
下面是觸發上述示例中事件的規則的規則語法。規則中可針對從FMC下載的此規則的資料包捕獲(PCAP)檔案進行驗證的部分以粗體顯示。

alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg:"OS-OTHER Bash CGI環境變數注入嘗試";\
flow:to_server，established;\
內容："(){";fast_pattern:only;http_header;\
後設資料:policybalanced-ipsdrop、policy max-detect-ipsdrop、policy security-ipsdrop、ruleset community、**service http**;\
參考：cve，2014-6271;參考：cve，2014-6277;參考：cve，2014-6278;參考：cve，2014-7169;\
classtype:attempted-admin;\
sid:31978;rev:5;)

然後，可以按照這些初始步驟執行分析過程，檢視流量是否應該與觸發規則相匹配。

1.檢查流量匹配的訪問控制規則。此資訊作為Intrusion Events頁籤上的列的一部分找到。
2.查詢所述訪問控制規則中使用的變數集。然後可以在**對象>對象管理>變數集**下檢視變數集
3.確保PCAP檔案中的IP地址與變數匹配(在本例中，**$EXTERNAL_NET變數中包含的主機連線到$HOME_NET變數配置中包含的主機**)
4.對於**flow**，可能需要捕獲完整會話/連線。由於效能原因，Snort不會捕獲整個流。但是，在大多數情況下，可以安全假設如果觸發了具有flow:established的規則，則在規則觸發時建立了會話，因此在snort規則中驗證此選項不需要完整的PCAP檔案。但更好的理解觸發它的原因可能是有用的。
5.對於**服務http**，請檢視Wireshark中的PCAP檔案，檢視它是否像HTTP流量。如果為主機啟用了網路發現，並且它以前已看到應用程式「HTTP」，則可能導致會話上的服務匹配。

瞭解此資訊後，您可以進一步在Wireshark中檢視從FMC下載的封包。可以評估PCAP檔案以確定被觸發的事件是否為誤報。



在上圖中，規則檢測到的內容存在於PCAP檔案 — **"(){"中**

但是，規則指定應在資料包的HTTP報頭 — **http**_header中檢測**該內容**

在這種情況下，在HTTP正文中找到了內容。因此，這是一個誤報。但是，從規則編寫錯誤的角度來說，這不是誤報。規則是正確的，在此情況下無法改進。此範例可能會遇到Snort錯誤，該錯誤會導致snort產生緩衝區混亂。這表示Snort未正確識別http_headers。

在這種情況下，您可在裝置執行的版本中檢查snort/IPS引擎是否有任何現有錯誤，如果沒有，則可開啟思科技術協助中心(TAC)的案例。調查此類問題需要完整會話捕獲，因為思科團隊需要審查Snort如何進入該狀態，而單一資料包無法做到這一點。

正數示例

下圖顯示同一入侵事件的資料包分析。這一次，事件為真正，因為內容確實出現在HTTP標頭中。

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-
從FMC下載的封包擷取	有關說明，請參閱本文
收集的任何相關CLI輸出，例如**trace** 輸出	有關說明，請參閱本文

後續步驟

如果確定入侵策略元件不是問題的原因，則下一步是排除網路分析策略功能的故障。

按一下此處繼續閱讀最後一篇文章。