Firepower資料路徑故障排除第8階段：網路分析策略

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。

本文介紹Firepower資料路徑故障排除的第八階段，即網路分析策略功能。

必要條件

- 本文適用於所有Firepower平台
  trace功能僅在適用於Firepower威脅防禦(FTD)平台的軟體版本6.2.0及更新版本中可用。
- 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/

網路分析策略功能故障排除

網路分析策略(NAP)包含snort前處理器設定，該設定根據確定的應用程式對流量執行檢測。前處理器能夠根據配置丟棄流量。本文介紹如何驗證NAP配置和檢查前處理器丟棄。

> **附註**：前處理器規則具有除「1」或「3」之外的生成器ID(GID)（即129、119、124）。 有關GID到前處理器對映的詳細資訊，請參閱FMC配置指南。

使用「trace」工具尋找前處理器捨棄專案（僅限FTD）

system support trace工具可用於檢測在前處理器級別執行的丟包。

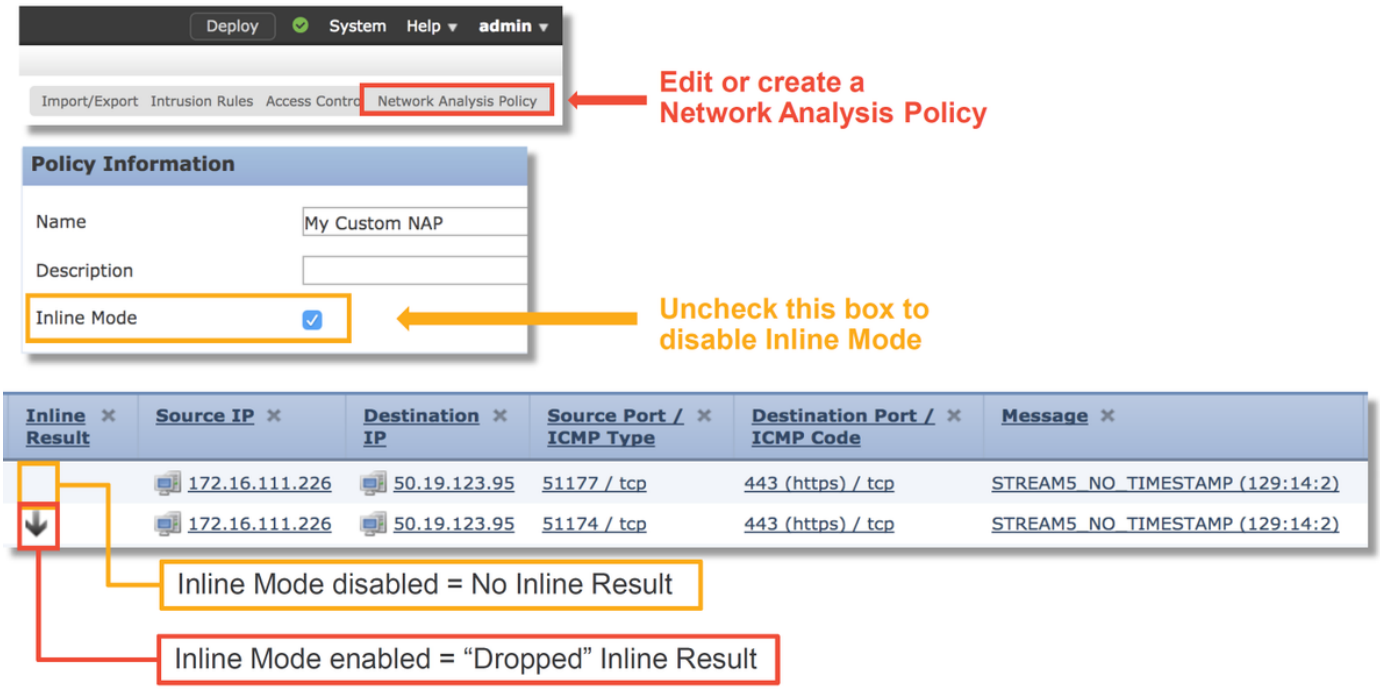
在以下示例中，TCP規範化前處理器檢測到異常。因此，規則**129:14**會捨棄流量，此規則會查詢TCP資料流中遺失的時間戳。

```
> 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
```

> **附註**：雖然**TCP串流組態**前處理器捨棄流量，但由於已啟用內嵌規範化**預處理**器，因此它仍可捨棄流量。有關內嵌規範化的詳細資訊，請閱讀本文。

驗證NAP配置

在Firepower管理中心(FMC)UI上，可以在**Policies > Access Control > Intrusion**下檢視NAP。然後，按一下右上角的**Network Analysis Policy**選項，在此之後，您可以檢視NAP、建立新的和編輯現有的NAP。



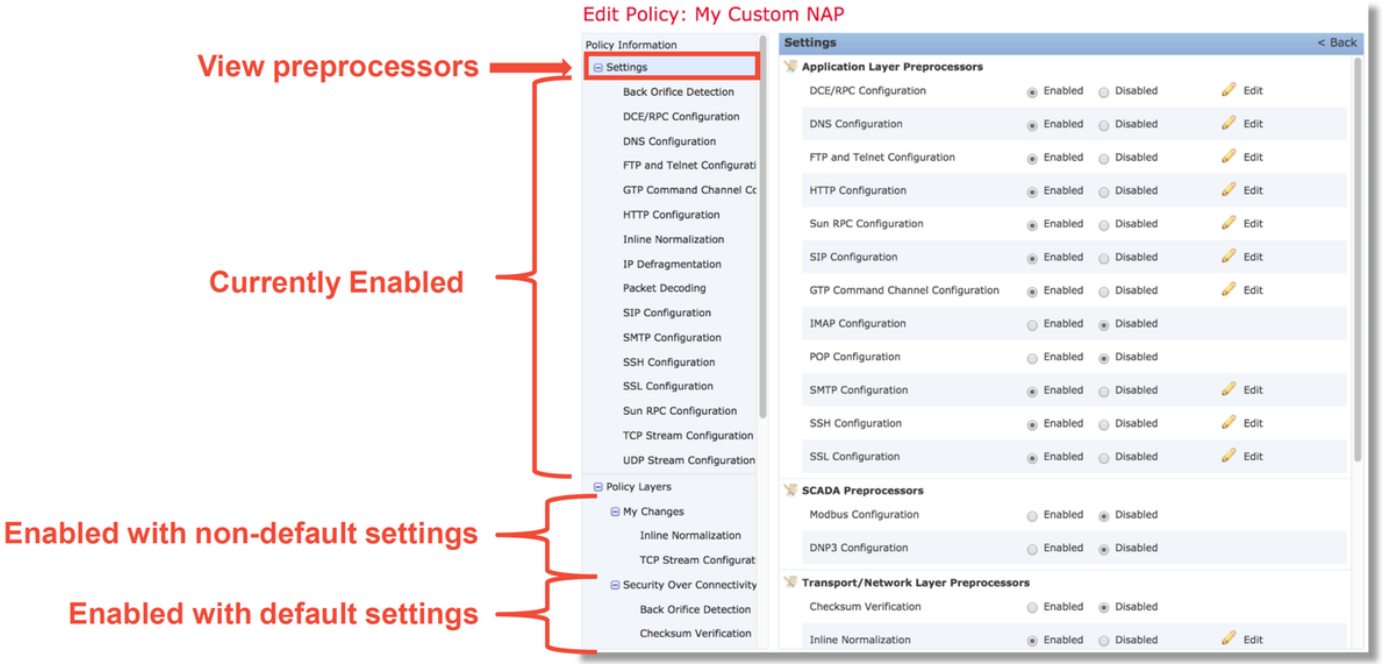
如上圖所示，NAP包含「內聯模式」功能，相當於入侵策略中的「在內聯時丟棄」選項。防止

NAP丟棄流量的快速緩解步驟是取消選中**Inline Mode**。在禁用內聯模式的情況下，NAP生成的入侵事件在**Inline Result**頁籤中不會顯示任何內容。

檢視NAP設定

在NAP中，可以檢視當前設定。這包括已啟用的前處理器總數，緊接著的是

使用非預設設定（手動調整的前處理器）和啟用預設設定的前處理器，如下圖所示。

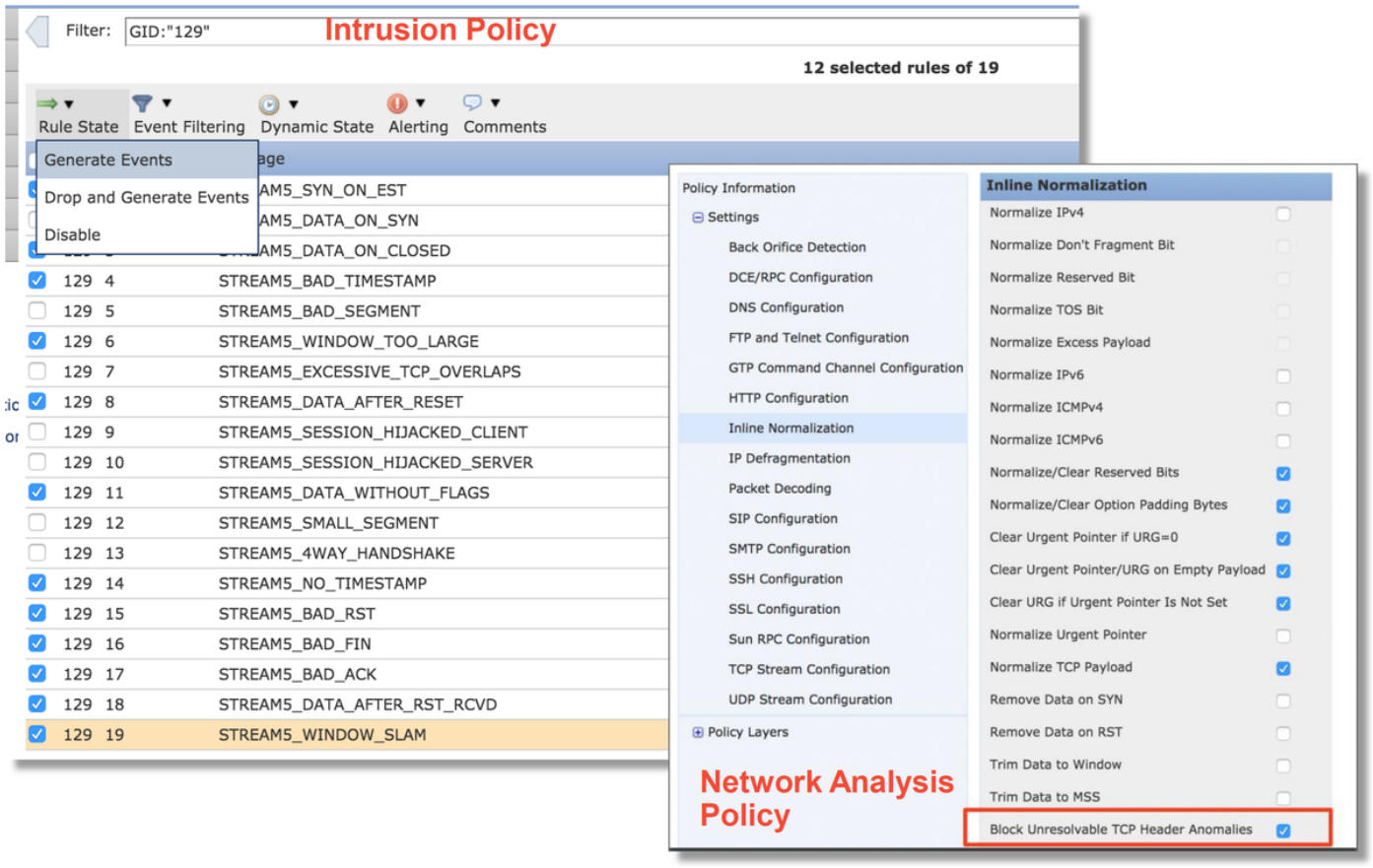


可能導致靜默丟棄的NAP設定

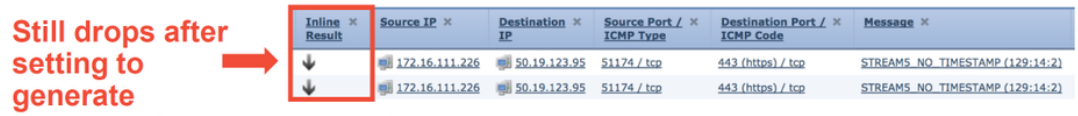
在跟蹤部分中提到的示例中，規則TCP流配置規則**129:14**正在丟棄流量。這通過檢視系統支援**跟蹤輸出**確定。但是，如果上述規則在相應的入侵策略內未啟用，則不會向FMC傳送入侵事件。

之所以會出現這種情況，是因為**內聯規範化**前處理器中有一個名為**Block Unresolvable TCP Header Anomalies**的設定。此選項基本上允許Snort在某些GID 129規則檢測到TCP流中的異常時執行阻止操作。

如果啟用**Block Unresolvable TCP Header Anomalies**，建議按照下圖啟用GID 129規則。



啟用GID 129規則會導致入侵事件在對FMC流量採取行動時傳送到FMC。但是，只要啟用**Block Unresolvable TCP Header Anomalies**，即使將入侵策略中的**Rule State**設定為**Generate Events**，它仍可以丟棄流量。此行為在FMC配置指南中說明。



Check configuration guide for relative protocols/preprocessors:

Block Unresolvable TCP Header Anomalies

When you enable this option, the system blocks anomalous TCP packets that, if normalized, would be invalid and likely would be blocked by the receiving host. For example, the system blocks any SYN packet transmitted subsequent to an established session.

The system also drops any packet that matches any of the following TCP stream preprocessor rules, regardless of whether the rules are enabled:

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 through 129:19

The Total Blocked Packets performance graph tracks the number of packets blocked in inline deployments and, in passive deployments and inline deployments in tap mode, the number that would have been blocked in an inline deployment.

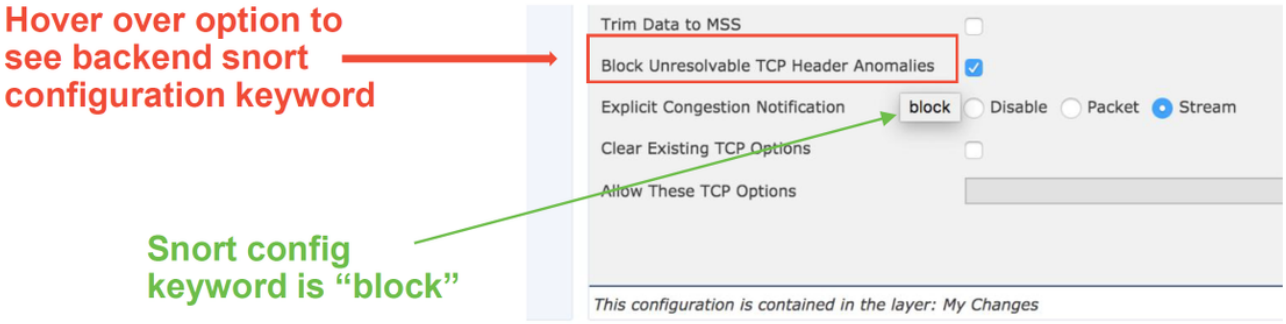
上述文檔可以在本文中找到（對於版本6.4，這是發佈本文時的最新版本）。

驗證後端配置

前處理器的行為增加了另一層複雜性，因為可以在後端啟用某些設定，而不會在FMC中反映出來。以下是一些可能的原因。

- 其他啟用的功能能夠強制啟用前處理器設定（主要功能是檔案策略）
- 某些入侵策略規則需要某些前處理器選項才能執行檢測
- 缺陷可能導致此行為 我們已經看到以下一個例項： CSCuz50295 - 「File policy with Malware block enable TCP normalization with block flag（帶有惡意軟體塊的檔案策略啟用帶有塊標誌的TCP規範化）」

在檢視後端配置之前，請注意，將滑鼠懸停在NAP中的特定設定上即可看到後端Snort配置檔案中使用的Snort關鍵字。請參閱下圖。



NAP頁籤中的Block Unresolvable TCP Header Anomalies選項會轉換為後端上的block關鍵字。記住該資訊後，可從專家外殼檢查後端配置。

```
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

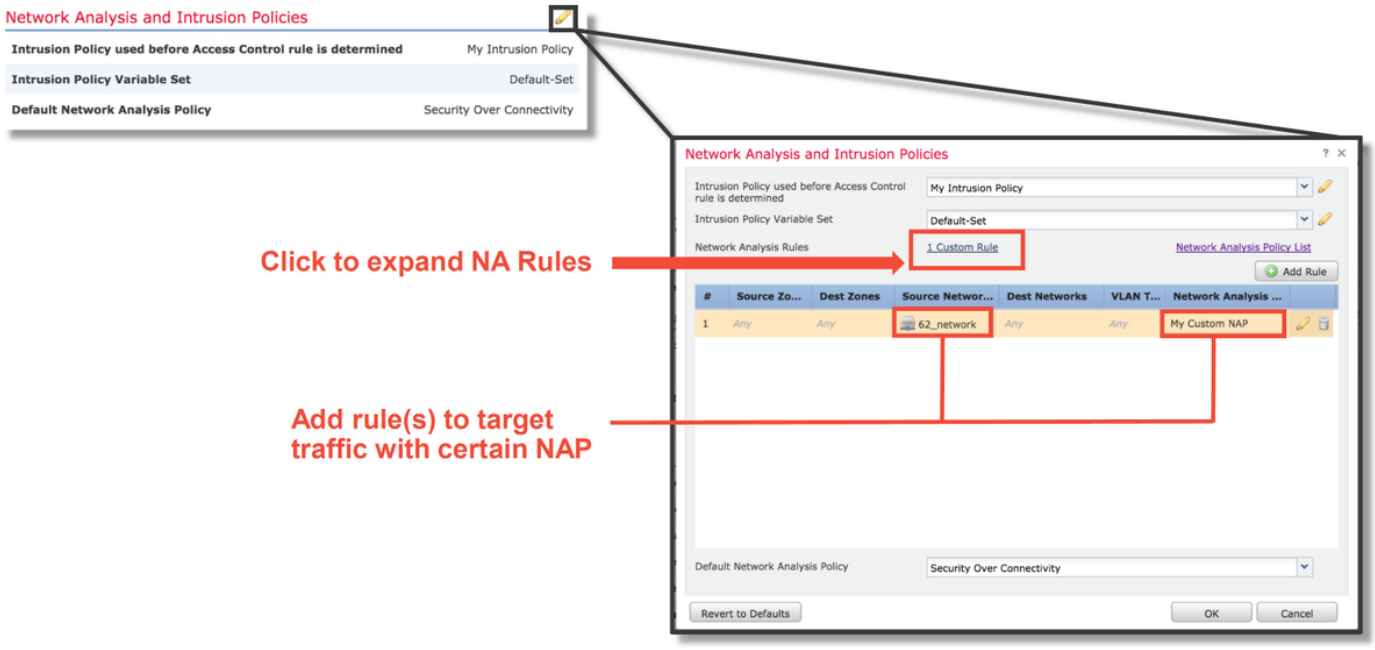
建立目標NAP

如果某些主機正在觸發前處理器事件，可以使用自定義NAP來檢查進出所述主機的流量。在自定義NAP中，可以禁用導致問題的設定。

以下是實施目標國家行動方案的步驟。

1. 按照本文「驗證NAP配置」部分中提到的說明建立NAP。
2. 在訪問控制策略的Advanced頁籤中，導航到Network Analysis and Intrusion Policies部分。按一下Add Rule，使用目標主機建立規則，然後在Network Analysis Policy部分中選擇新建立的

NAP。

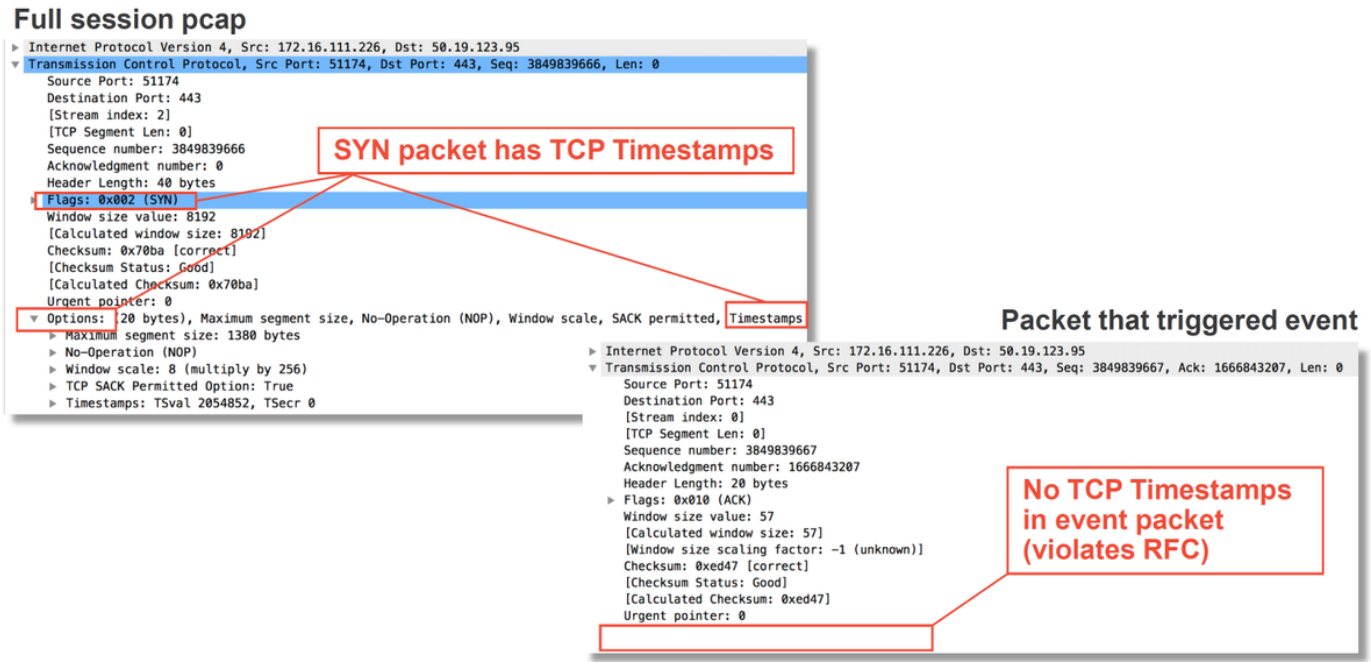


誤報分析

檢查入侵事件中針對前處理器規則的誤報與檢查用於規則評估的Snort規則（包含1和3的GID）完全不同。

為了對前處理器規則事件執行誤報分析，需要完整會話捕獲來查詢TCP資料流中的異常。

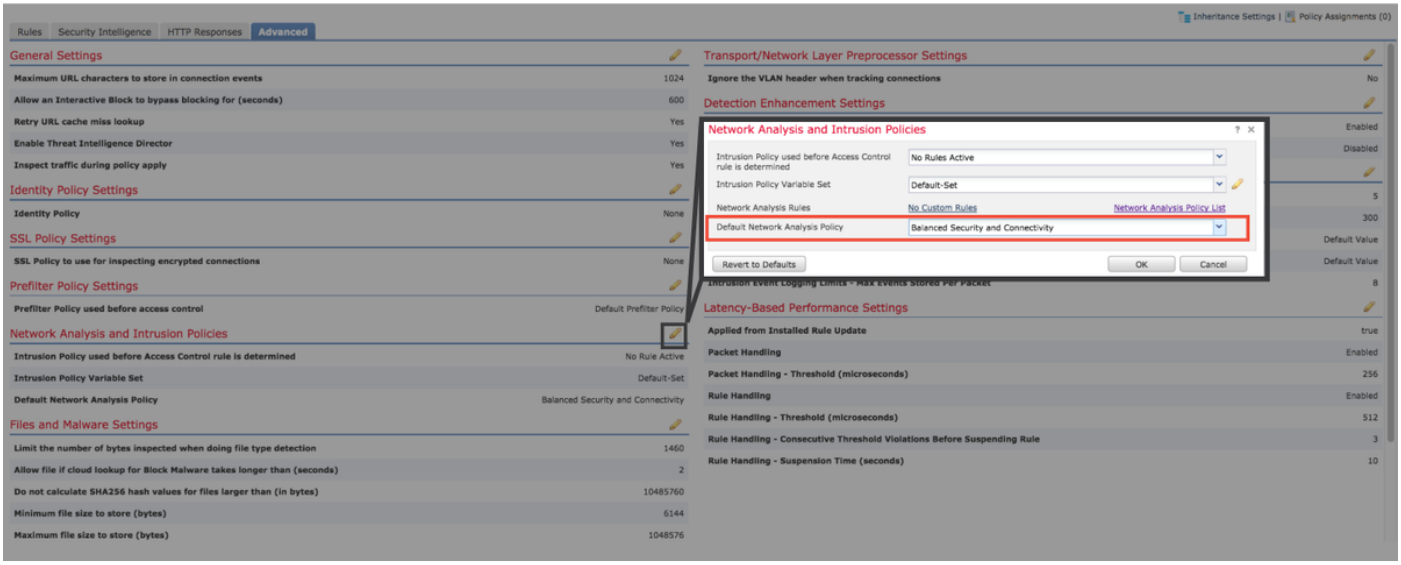
在下面的示例中，對規則129:14執行誤報分析，在上面的示例中，該規則顯示正在丟棄流量。由於129:14正在查詢缺少時間戳的TCP流，因此您可以清楚地看到根據下面所示的資料包捕獲分析觸發規則的原因。



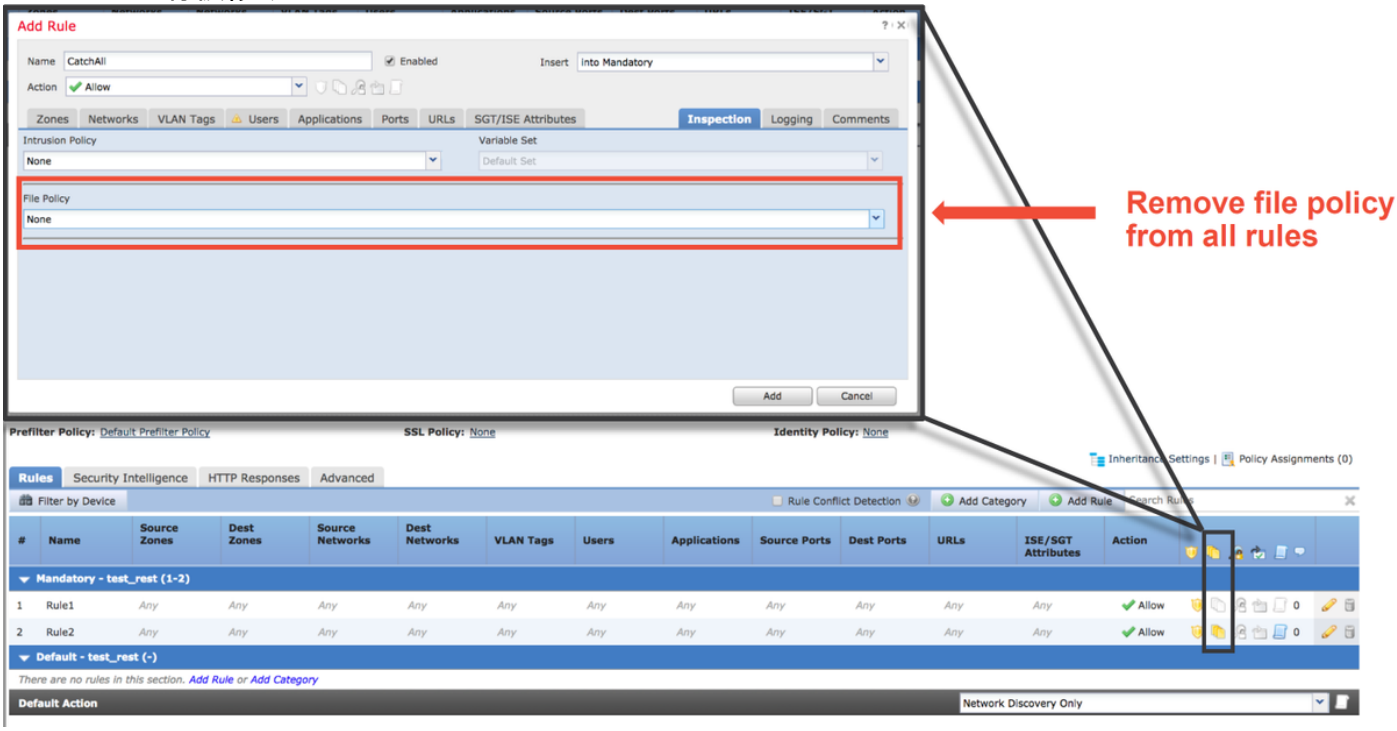
緩解步驟

為快速緩解國家行動方案可能存在的問題，可執行以下步驟。

- 如果使用的是自定義NAP，並且您不確定NAP設定是否正在丟棄流量，但您懷疑可能是丟棄流量，您可以嘗試將其替換為「平衡的安全性和連線」或「通過安全的連線」策略。



- 如果使用任何「自定義規則」，請確保將NAP設定為上述預設值之一
- 如果任何訪問控制規則使用檔案策略，您可能需要嘗試暫時將其刪除，因為檔案策略可以在後端啟用未在FMC中反映的前處理器設定，並且此操作在「全域性」級別執行，這意味著所有NAP都將被修改。



每個協定都有不同的前處理器，故障排除可能非常特定於前處理器。本文未涵蓋每個前處理器的所有設定和故障排除方法。

您可以檢視每個前處理器的文檔，以便更好地瞭解每個選項的作用，這對於排除特定前處理器故障很有幫助。

要提供給TAC的資料

資料	說明
Firepower裝置中的故障排除檔案	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defen

從Firepower裝置捕獲完整會話資料包 http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepo