Firepower資料路徑故障排除：概觀

目錄

簡介

本指南旨在幫助快速確定具備FirePOWER服務的Firepower威脅防禦(FTD)裝置或自適應安全裝置(ASA)是否導致網路流量問題。此外，它還有助於縮小調查哪些Firepower元件以及應在聯絡思科技術支援中心(TAC)之前收集哪些資料的範圍。

所有Firepower資料路徑故障排除系列文章的清單。

Firepower資料路徑故障排除第1階段：封包輸入

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

Firepower資料路徑故障排除第2階段：DAQ層
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Firepower資料路徑故障排除第3階段：安全情報
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Firepower資料路徑故障排除第4階段：訪問控制策略

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Firepower資料路徑故障排除第5階段：SSL策略
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Firepower資料路徑故障排除第6階段：主動驗證
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Firepower資料路徑故障排除第7階段：入侵原則
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Firepower資料路徑故障排除第8階段：網路分析策略

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

必要條件

- 本文假設您對FTD和ASA平台有基本瞭解。
- 建議具備開源snort知識，但不需要。

有關Firepower文檔的完整清單（包括安裝及設定指南），請訪問文檔路線圖頁。

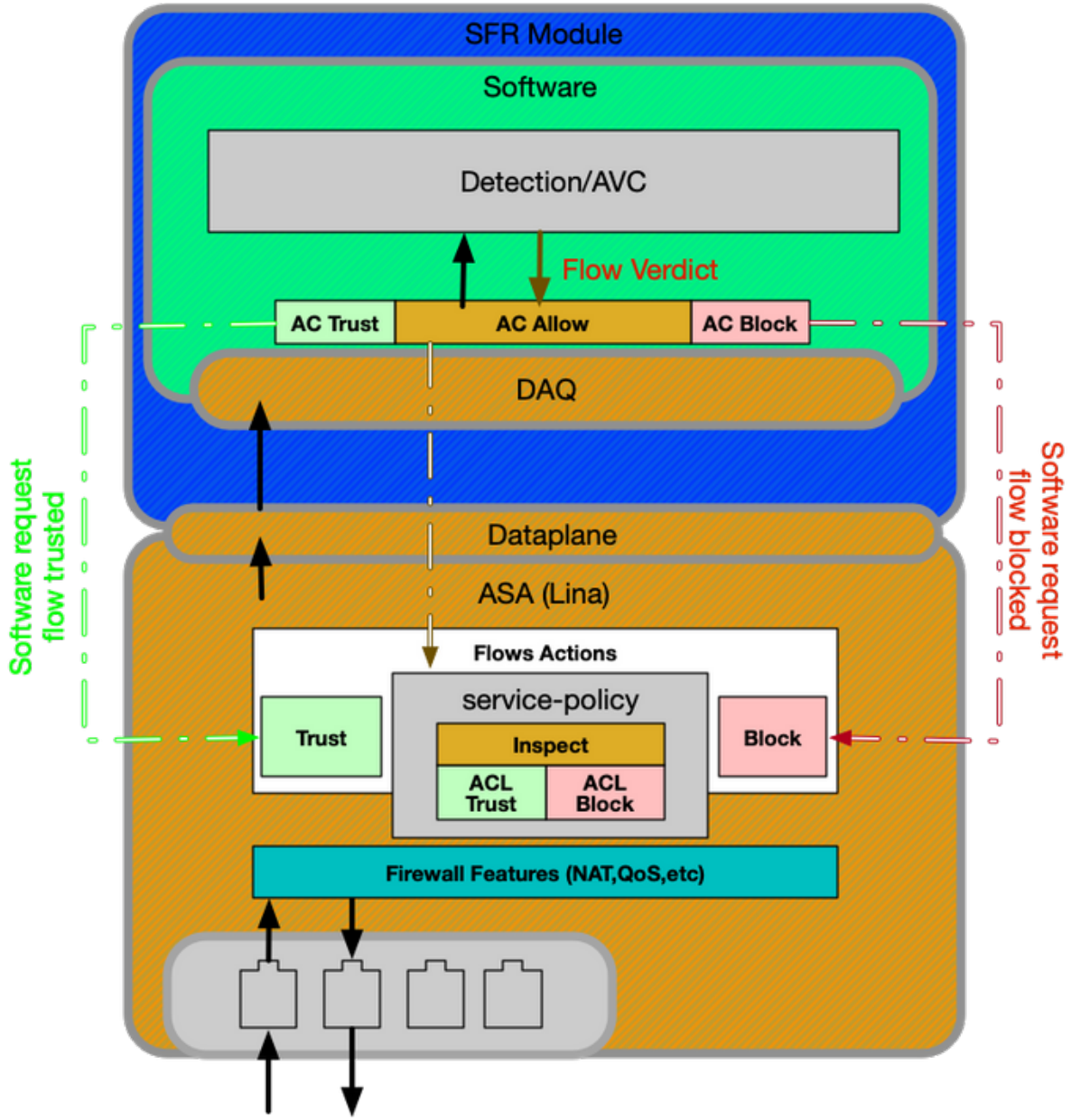
資料路徑的架構概覽

下一節介紹各種Firepower平台的架構資料路徑。在瞭解該架構後，我們接下來將介紹如何快速確定Firepower裝置是否正在阻止流量。

> **附註**：本文不包括舊版Firepower 7000和8000系列裝置，也不包括NGIPS（非FTD）虛擬平台。有關對這些平台進行故障排除的資訊，請訪問我們的TechNotes頁面。

具備FirePOWER服務（SFR模組）平台的ASA

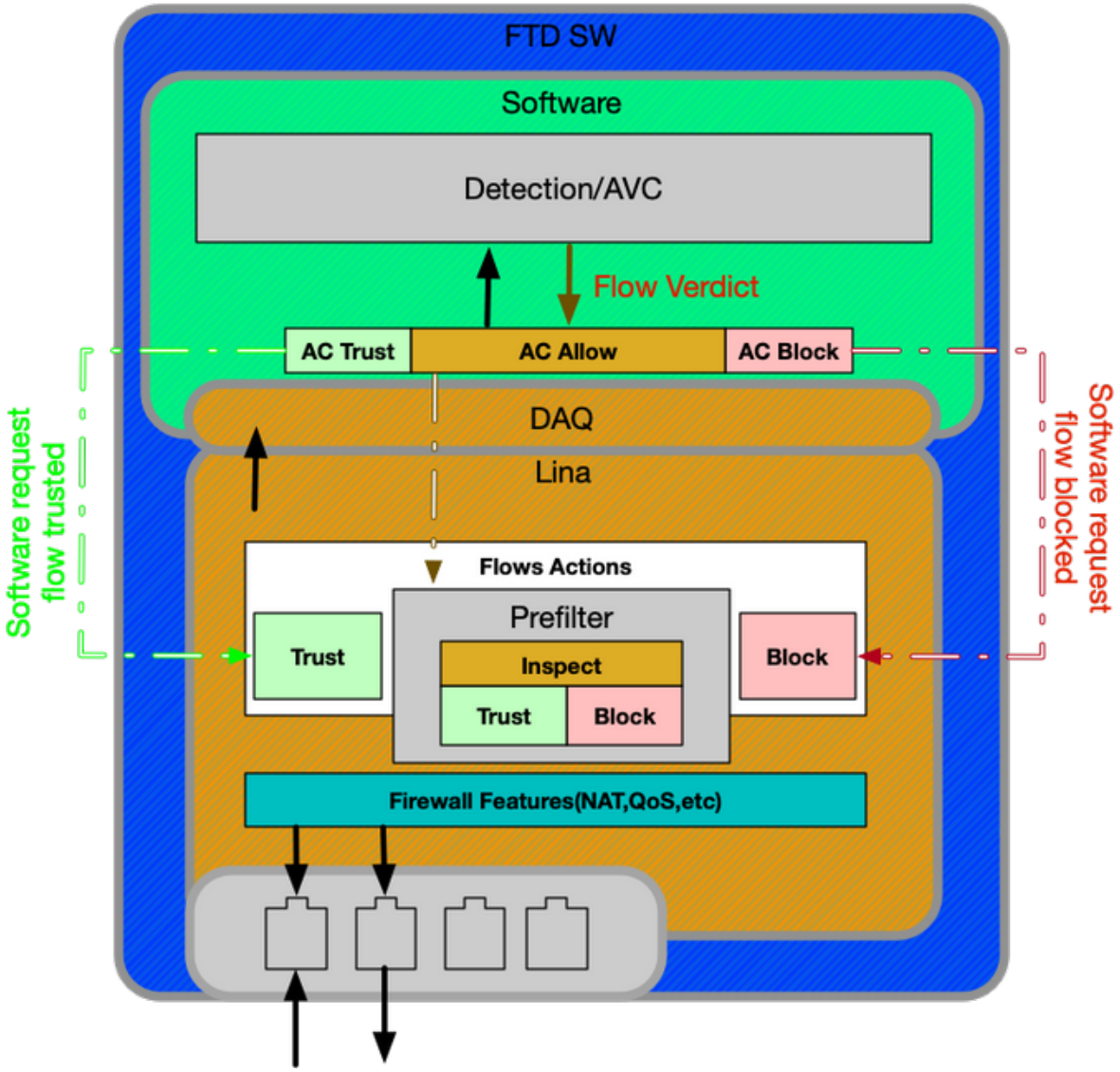
FirePOWER服務平台也稱為SFR模組。這基本上是運行在5500-X ASA平台上的虛擬機器。



ASA上的服務策略確定將哪些流量傳送到SFR模組。有一個資料平面層用於與Firepower資料採集(DAQ)引擎通訊，後者用於以snort能夠理解的方式轉換資料包。

ASA500-X和虛擬FTD平台上的Firepower威脅防禦

FTD平台由單一映像組成，其中包含Lina(ASA)和Firepower代碼。此平台與具有SFR模組平台的ASA之間的一個主要區別在於Lina和snort之間的通訊更為有效。

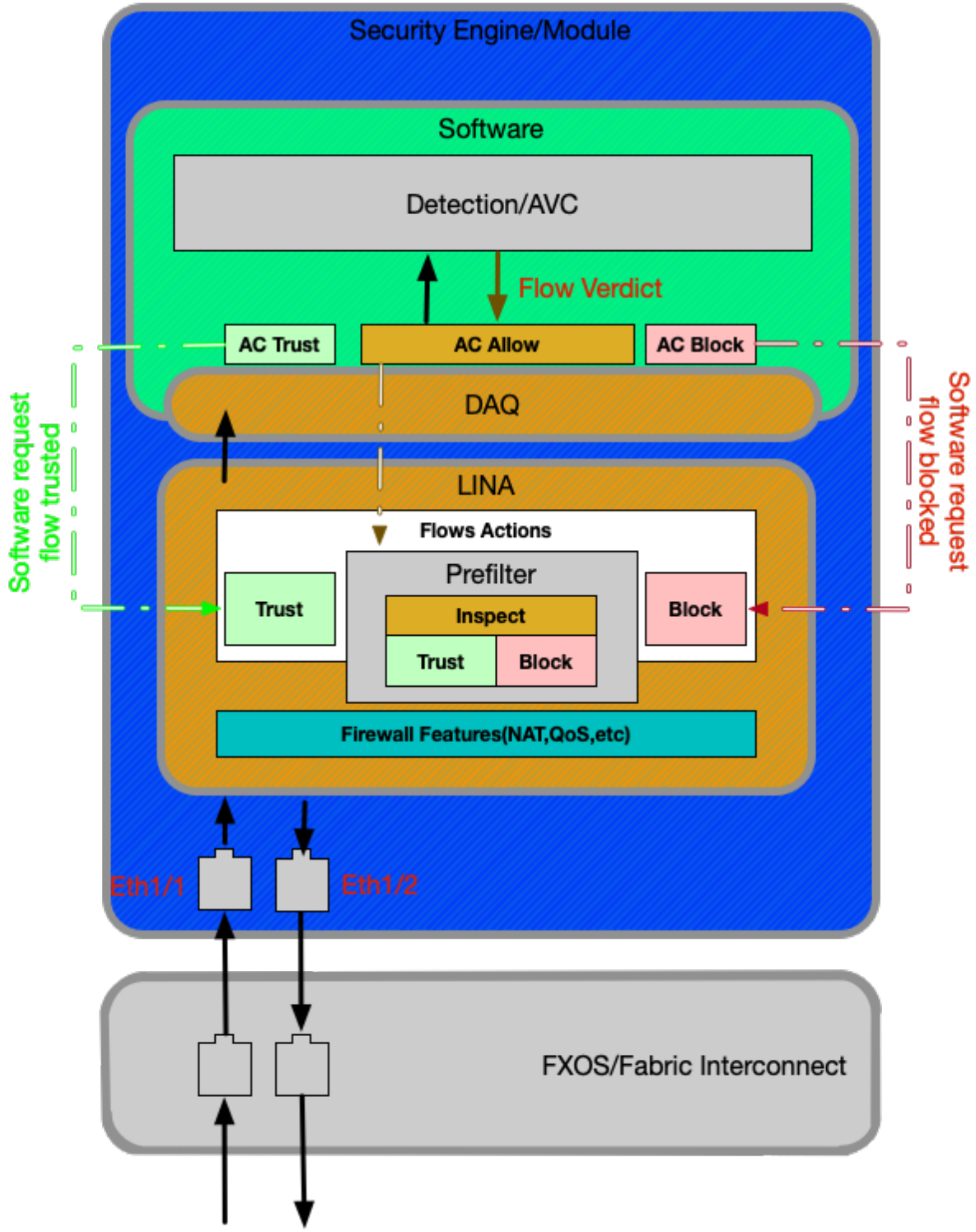


SSP平台上的FTD

在安全服務平台(SSP)型號上，FTD軟體運行在Firepower可擴展作業系統(FXOS)平台之上，該平台是底層作業系統(OS)，用於管理機箱硬體和託管各種應用程式（稱為邏輯裝置）。

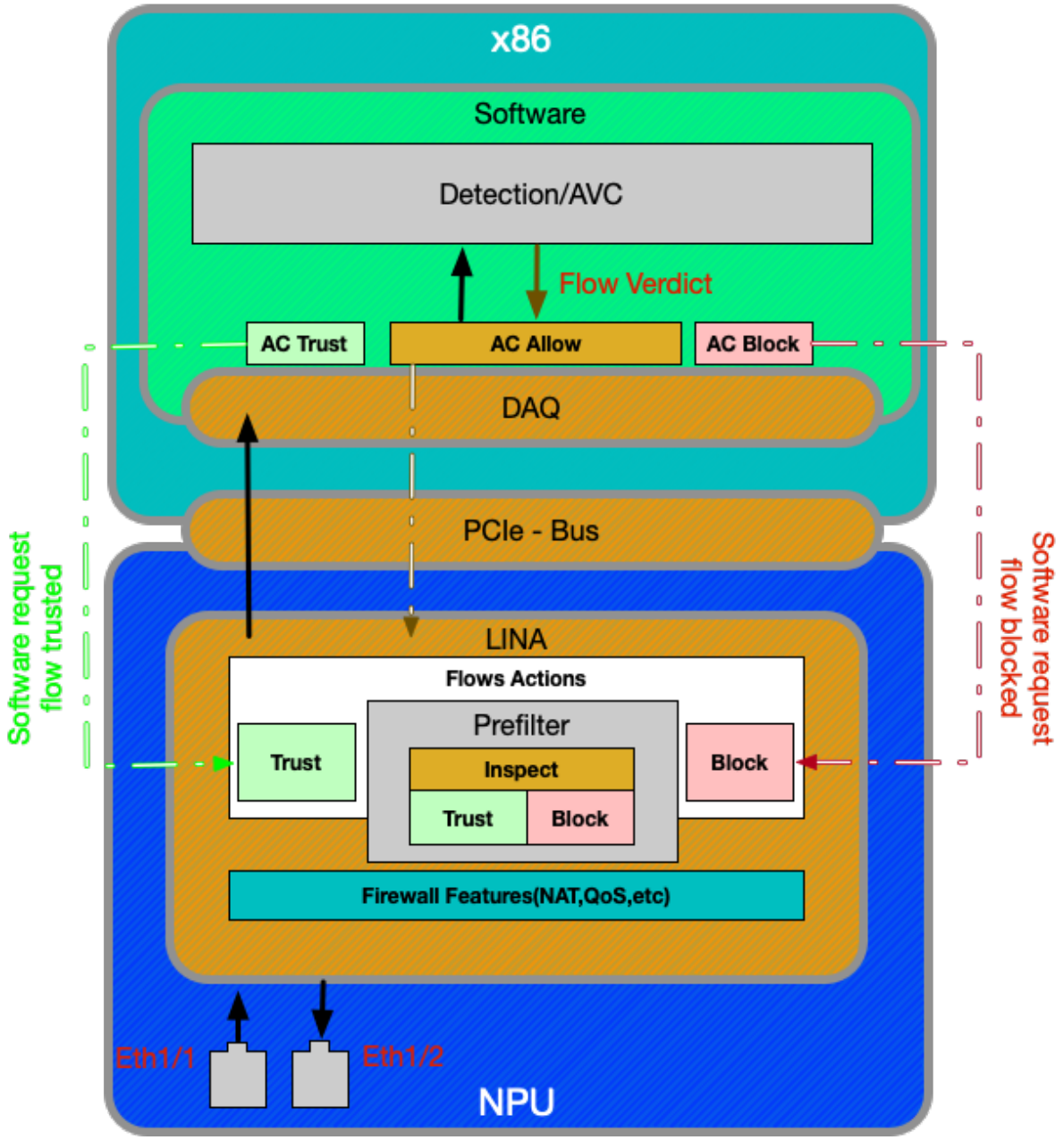
在SSP平台中，不同型號之間有一些差異，如下面的圖表和說明所示。

Firepower 9300和4100裝置



在Firepower 9300和4100平台上，入口和出口資料包由由FXOS韌體（交換矩陣互聯）供電的交換機處理。 然後將封包傳送到指派給邏輯裝置的介面（在本案例中為FTD）。 之後，封包處理與非SSP FTD平台上的處理相同。

Firepower 2100裝置



Firepower 2100裝置的功能與非SSP FTD平台非常相似。它不包含9300和4100型號上存在的交換矩陣互聯層。但是，2100系列裝置與其他裝置相比有一個重大差異，那就是存在專用積體電路(ASIC)。 所有傳統ASA功能(Lina)均在ASIC上運行，而所有下一代防火牆(NGFW)功能（snort、URL過濾等）均在傳統x86架構上運行。在此平台上Lina和Snort的通訊方式是透過封包佇列的外圍元件互連高速(PCIe)進行，而不是使用直接記憶體存取(DMA)將封包佇列為snort的其他平台。

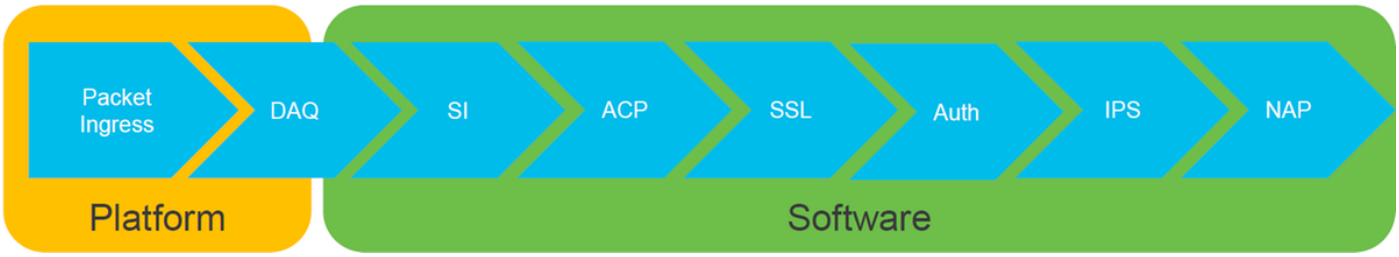
附註：在FPR-2100平台上，將採用與FTD非SSP平台相同的故障排除方法。

Firepower資料路徑故障排除的建議過程

現在，我們已經討論了如何在Firepower平台中識別唯一流量以及基本資料路徑體系結構，現在我們來瞭解資料包可以丟棄的特定位置。資料路徑文章中介紹了八個基本元件，它們可以系統地進行故障排除以確定可能的資料包丟棄。其中包括：

1. 封包輸入
2. Firepower DAQ層
3. 安全情報

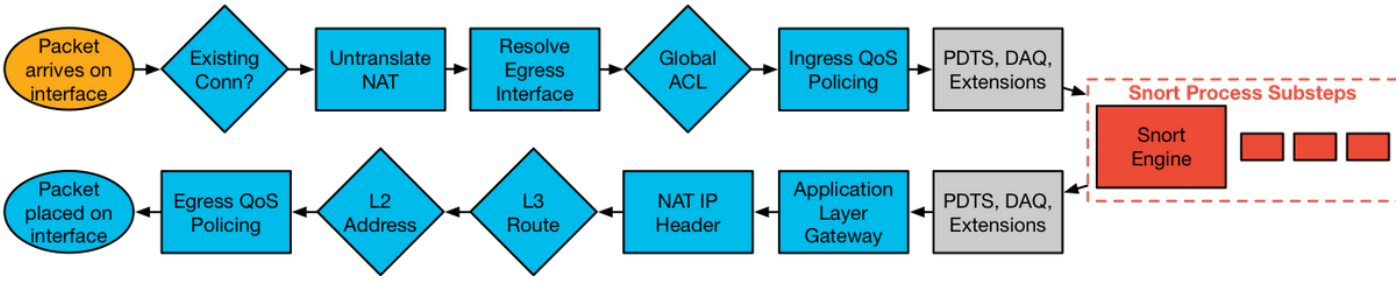
4. 訪問控制策略
5. SSL策略
6. 主動驗證功能
7. 入侵策略（IPS規則）
8. 網路分析策略（snort前處理器設定）



附註：在Firepower處理中，這些元件沒有按確切的操作順序列出，而是按照我們建議的故障排除工作流程進行訂購。有關資料包圖的實際路徑，請參閱下圖。

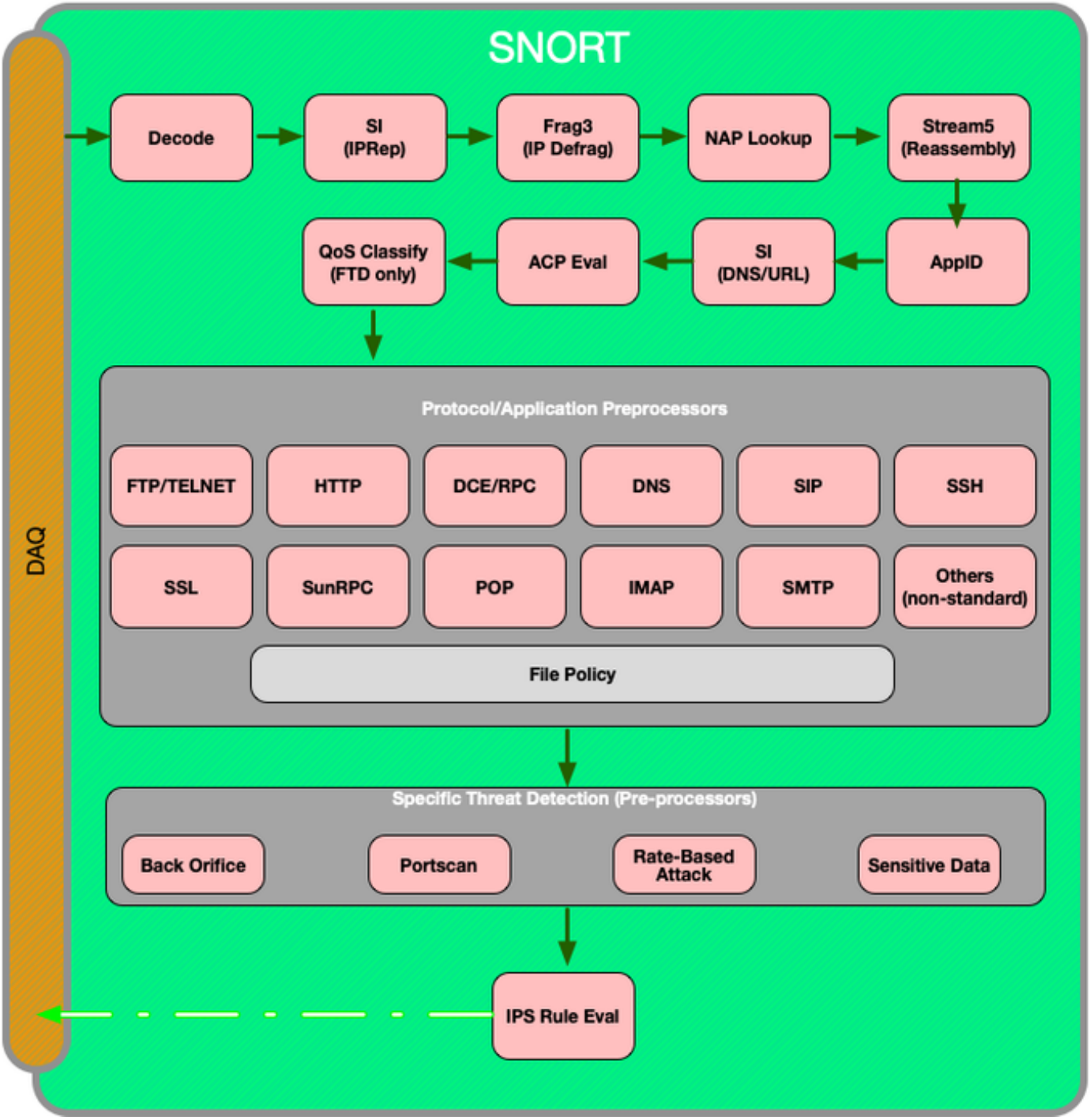
封包通過FTD的實際路徑

下圖顯示封包通過FTD時的實際路徑。



Snort封包路徑

下圖顯示資料包通過Snort引擎的路徑。



封包輸入和輸出

第一個資料路徑故障排除步驟是確保資料包處理的入口或出口階段不會發生丟包。如果資料包正在進入，但未進入，則您可以確定資料包正被裝置在資料路徑中的某個位置丟棄。

本文將介紹如何對Firepower系統上的資料包入口和出口進行故障排除。

Firepower DAQ層

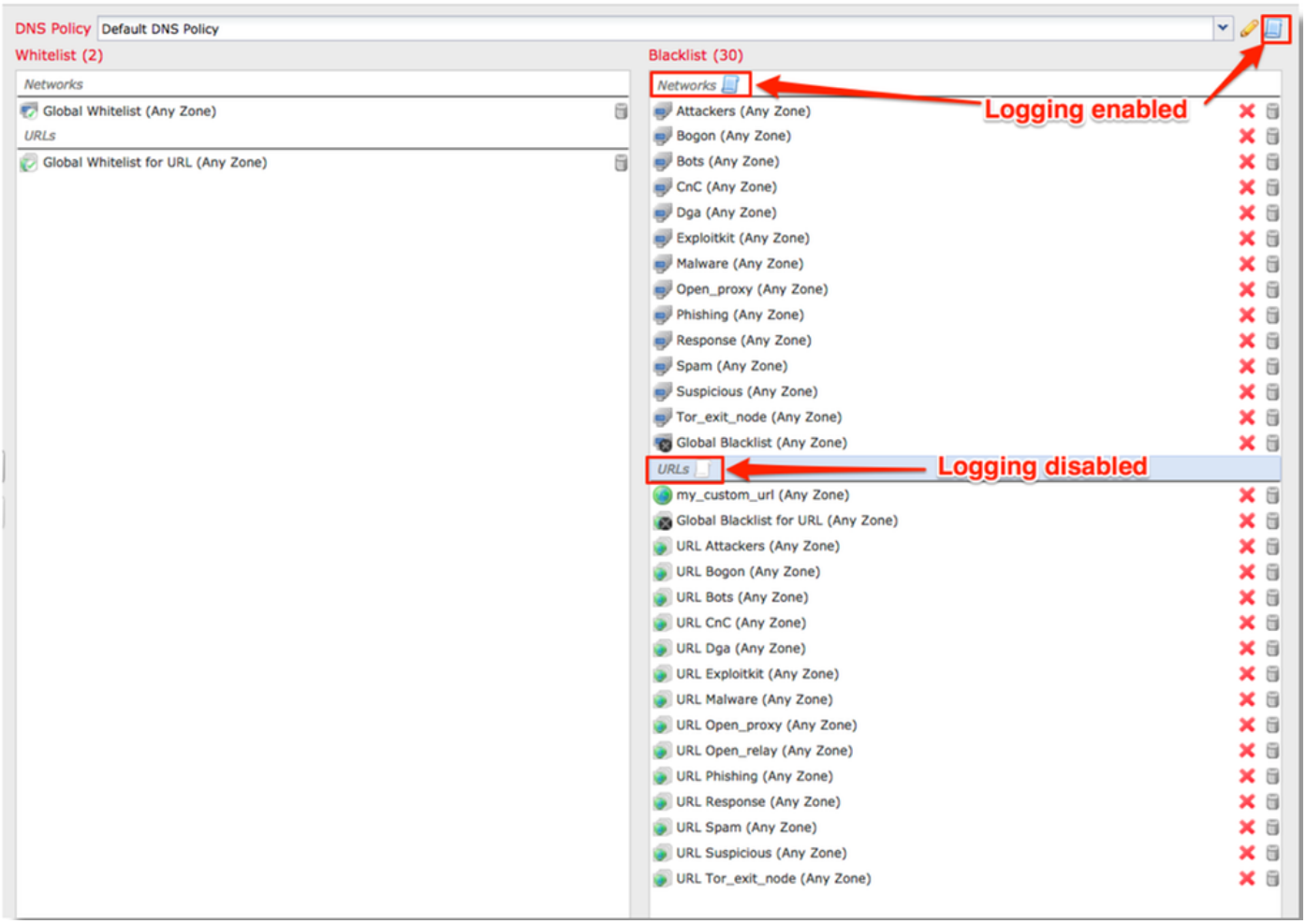
如果確定資料包正在進入，但並未進入，則資料路徑故障排除的下一個步驟應該是Firepower DAQ（資料採集）層，以確保相關流量被傳送到Firepower進行檢測，如果是，則進行丟棄或修改。

這篇文章介紹如何排除Firepower對流量的初始處理以及在整個裝置中採用的路徑故障。

它還介紹了如何完全繞過Firepower裝置，以確定Firepower元件是否負責流量問題。

安全情報

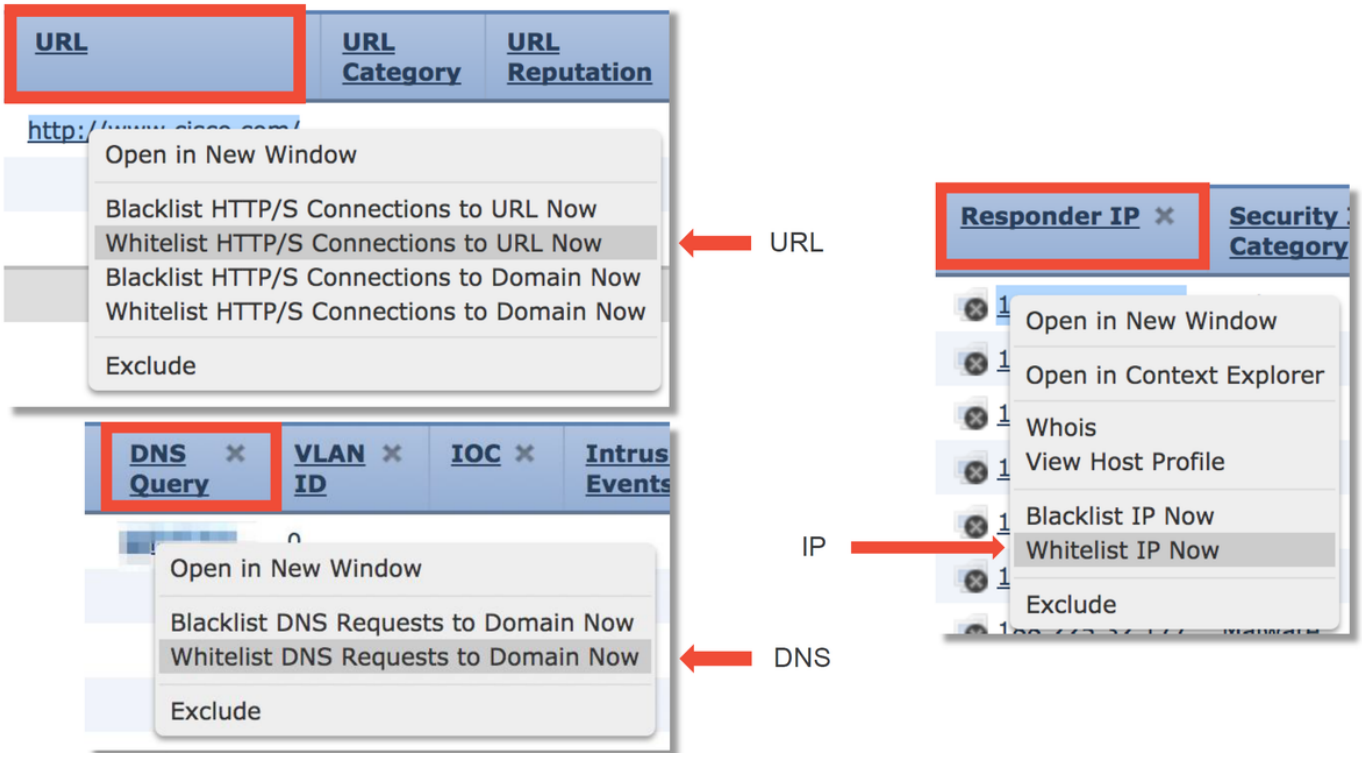
安全情報是Firepower中第一個檢查流量的元件。只要啟用了日誌記錄，此級別的塊很容易確定。這可在FMC GUI上透過導覽至**Policies > Access Control > Access Control Policy**來確定。按一下相關策略旁邊的編輯圖示後，導航到**Security Intelligence**頁籤。



啟用日誌記錄後，您可以在**分析>連線>安全情報事件**下檢視安全情報事件。應該清楚說明流量被阻塞的原因。

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

作為快速緩解步驟，您可以按一下右鍵被安全情報功能阻止的IP、URL或DNS查詢，並選擇白名單選項。



如果您懷疑某些內容被錯誤地列入黑名單，或者您想請求更改信譽，您可以在以下連結直接與Cisco Talos開啟票證：

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

您還可以將資料提供給TAC，以報告被阻止的內容，並可能將條目從黑名單中刪除。

有關安全情報元件的深入故障排除，請檢視相關的資料路徑故障排除文章。

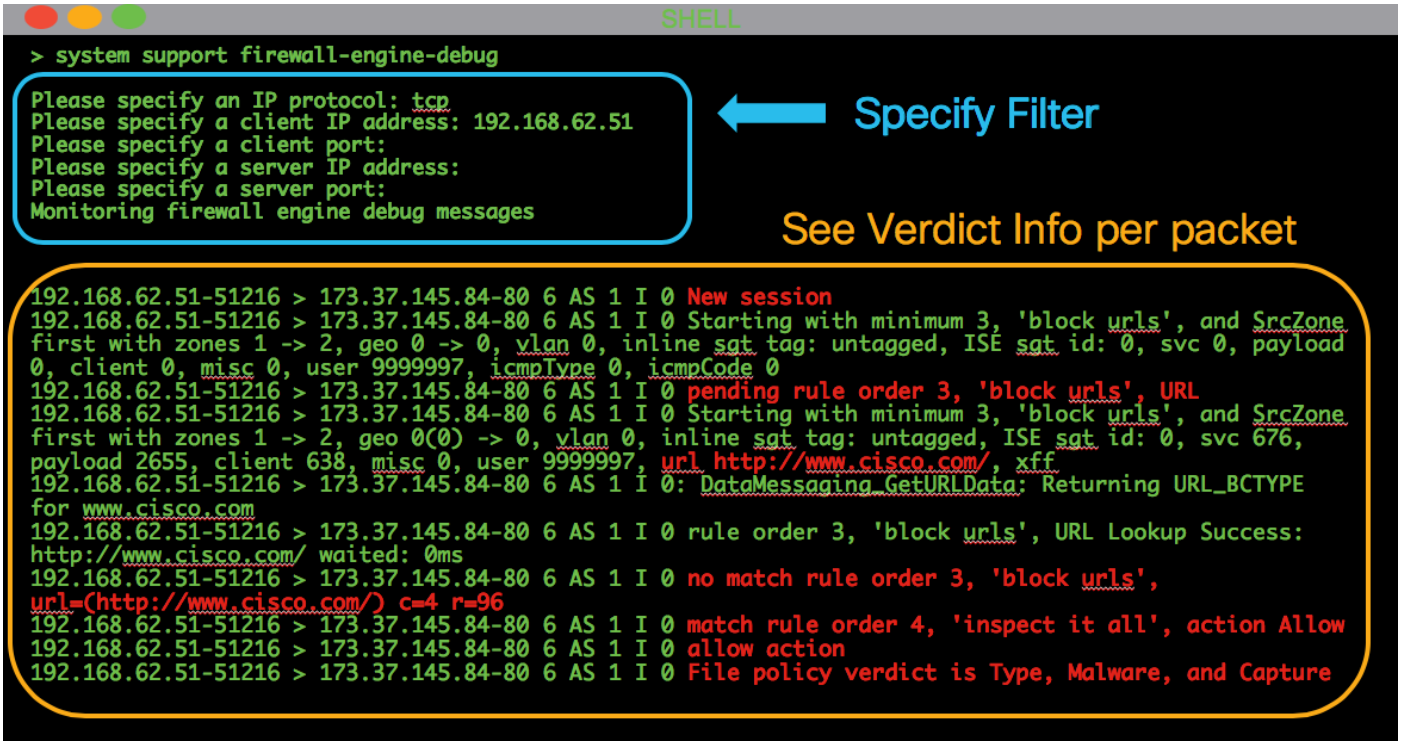
訪問控制策略

如果確定安全情報功能未阻止流量，則下一個建議步驟是排除訪問控制策略規則故障，檢視具有「阻止」操作的規則是否正在丟棄流量。

建議開始使用「firewall-engine-debug」命令或使用trace進行捕獲。通常，這些工具可以立即給出答案，並告訴您流量所遵循的規則，以及出於什麼原因。

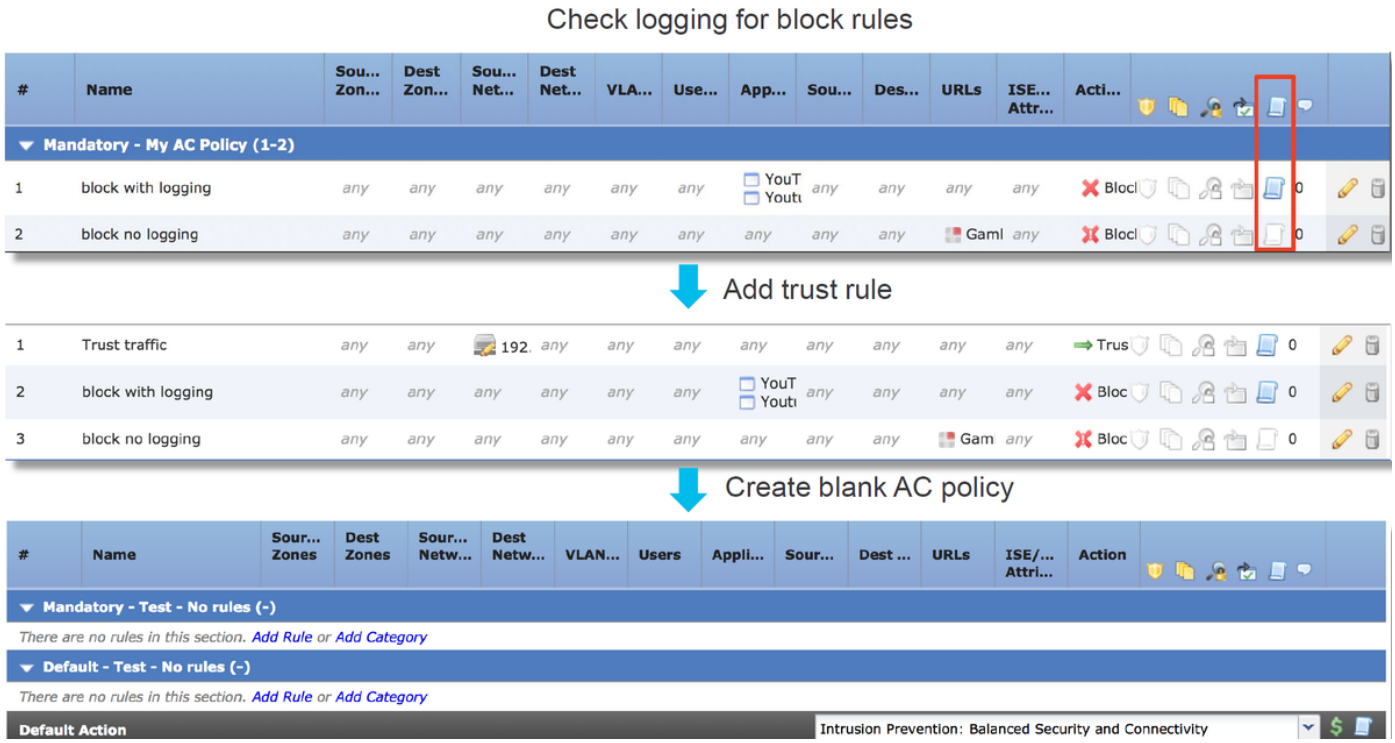
- 通過以下命令在Firepower CLI上運行調試，檢視哪個規則正在阻止流量（確保輸入儘可能多的引數）：**>系統支援firewall-engine-debug**
- 偵錯輸出可提供給TAC進行分析

以下是一些示例輸出，其中描述了使用「允許」操作匹配訪問控制規則的流量的規則評估：



如果您無法確定匹配的是哪條訪問控制(AC)規則，或者您無法使用上述工具確定AC策略是否出現問題，則下面是排除訪問控制策略故障的一些基本步驟（請注意，這些選項不是第一個選項，因為它們需要策略更改/部署）：

- 使用「阻止」操作為任何規則啟用日誌記錄
- 如果您仍然沒有看到流量的連線事件，並且它正被阻止，則接下來為相關流量建立信任規則作為緩解步驟
- 如果流量的信任規則仍不能解決此問題，但您仍懷疑AC策略存在故障，接下來，如果可能，使用除「阻止所有流量」之外的預設操作建立新的空白訪問控制策略

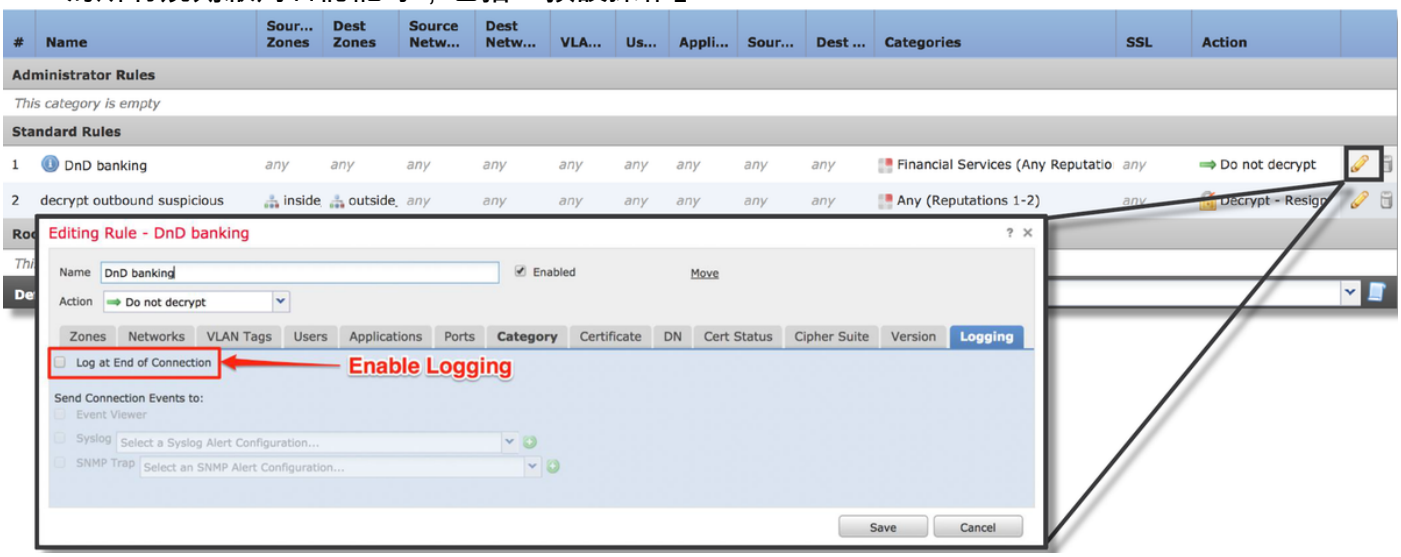


有關訪問控制策略的深入故障排除，請檢視相關資料路徑故障排除文章。

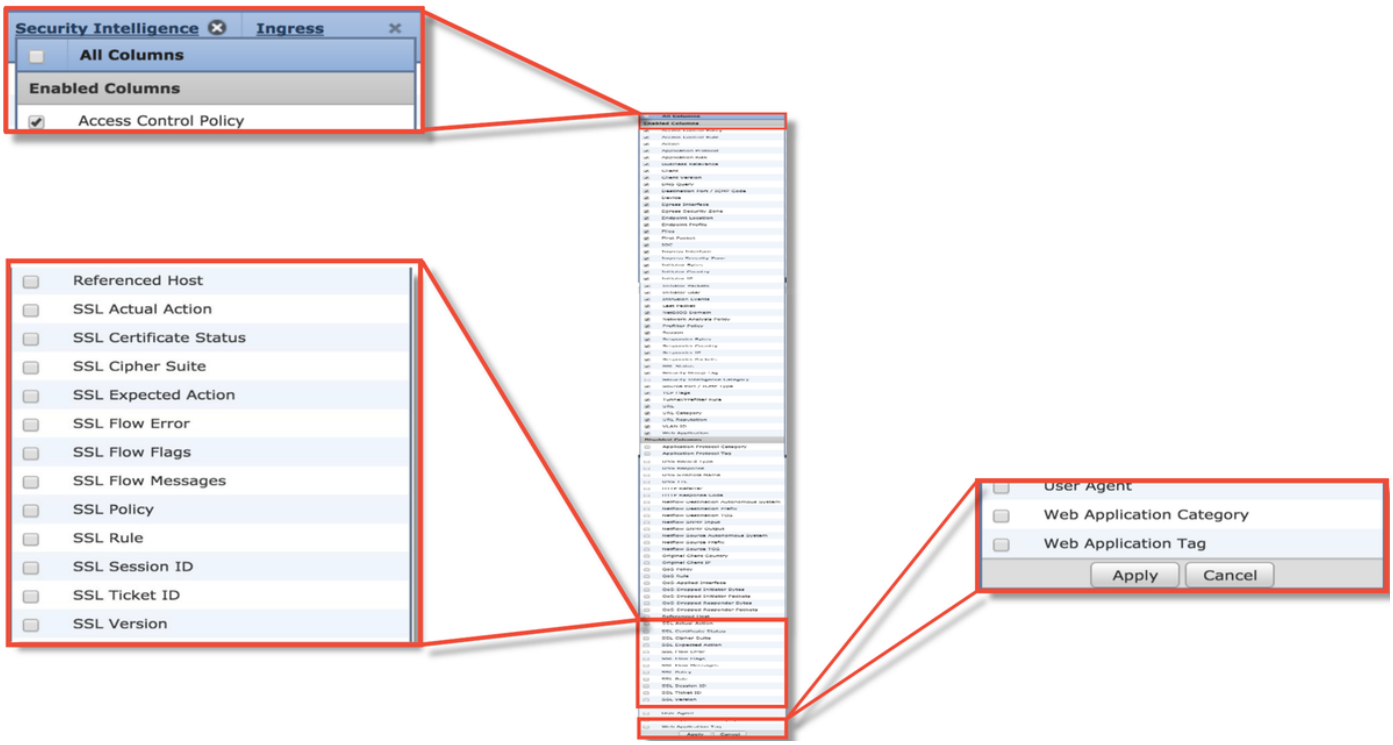
SSL策略

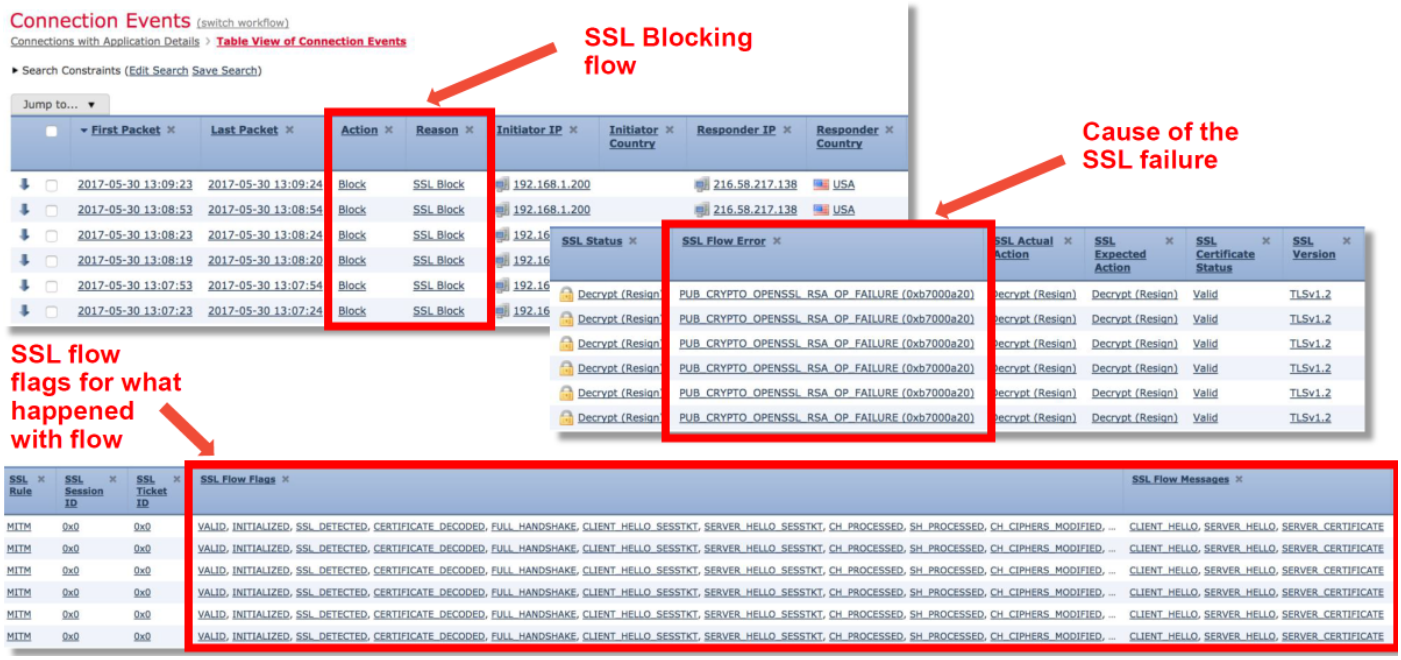
如果使用SSL策略，則可能阻塞了流量。以下是排除SSL策略故障的一些基本步驟：

- 為所有規則啟用日誌記錄，包括「預設操作」



- 檢查Undecryptable Actions頁籤，檢視是否將選項設定為阻止流量
- 在Connection events部分，檢查名稱中帶有「SSL」的所有欄位
  預設情況下禁用大多數功能，需要通過按一下任何列名稱旁邊的交叉點在「連線事件」檢視器中啟用這些功能





- 建立空白SSL策略，並將Do not Decrypt作為預設操作作為緩解步驟
- 作為緩解步驟，從訪問控制策略中刪除SSL策略
  在「高級」頁籤中設定此項

懷疑是SSL策略丟棄流量，可將連線事件以及策略配置傳送到TAC。

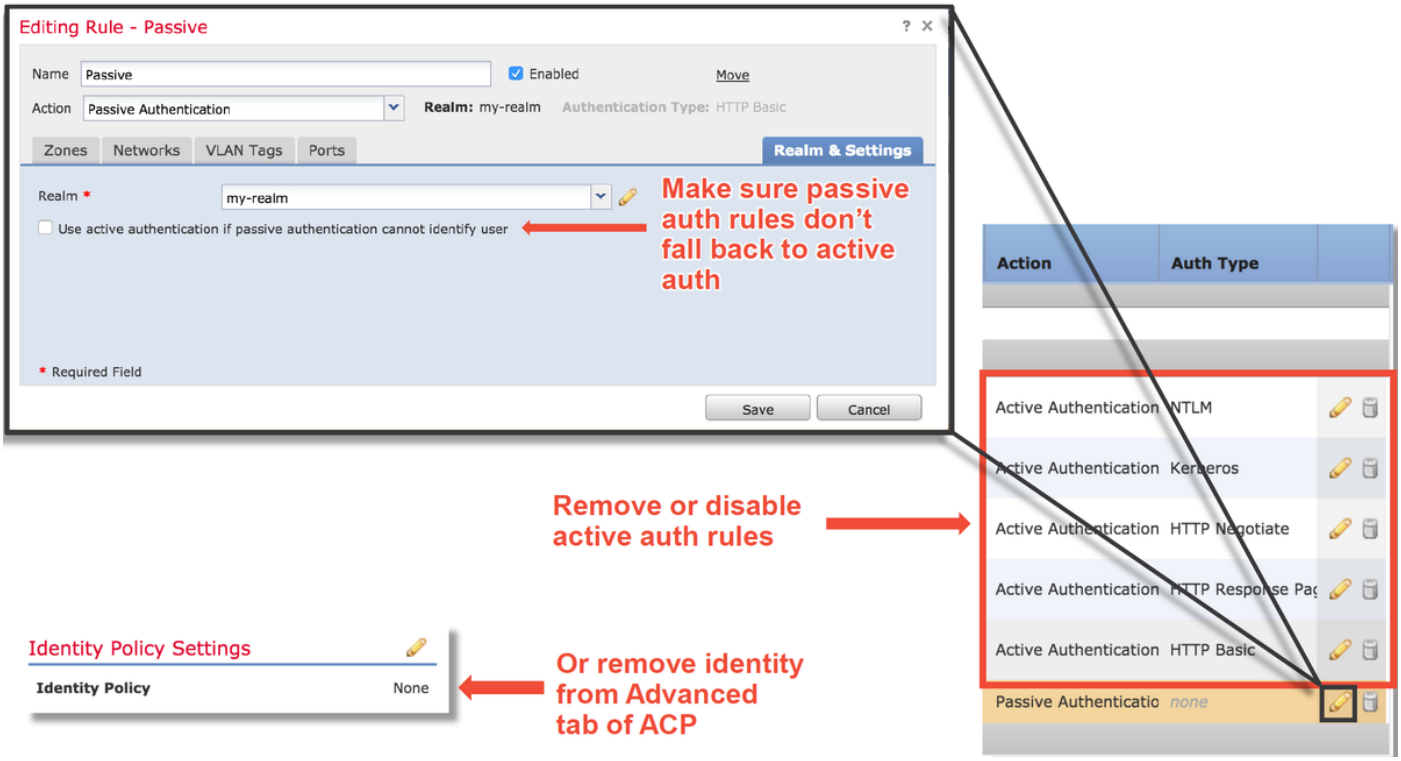
有關SSL策略的更深入故障排除，請參閱相關資料路徑故障排除文章。

主動驗證

在身份策略中使用時，主動身份驗證能夠丟棄流量，在出現故障時應允許丟棄流量。主動驗證功能本身可以直接影響所有HTTP/HTTPS流量，因為如果確定我們需要驗證使用者，則所有這些僅通過HTTP協定發生。這表示主動驗證不應影響其他網路服務（例如DNS、ICMP等），除非您具有根據使用者封鎖的特定存取控制規則，且使用者無法透過FTD上的主動驗證服務進行驗證。但是，這不是主動身份驗證功能的直接問題，而是使用者無法進行身份驗證以及擁有阻止未經身份驗證的使用者的策略的結果。

快速緩解步驟是使用「活動身份驗證」操作禁用身份策略中的任何規則。

此外，請確保具有「被動身份驗證」操作的任何規則均未選中「如果被動身份驗證無法識別使用者，則使用主動身份驗證」選項。



有關主動身份驗證的更多深入故障排除資訊，請檢視相關資料路徑故障排除文章。

入侵原則

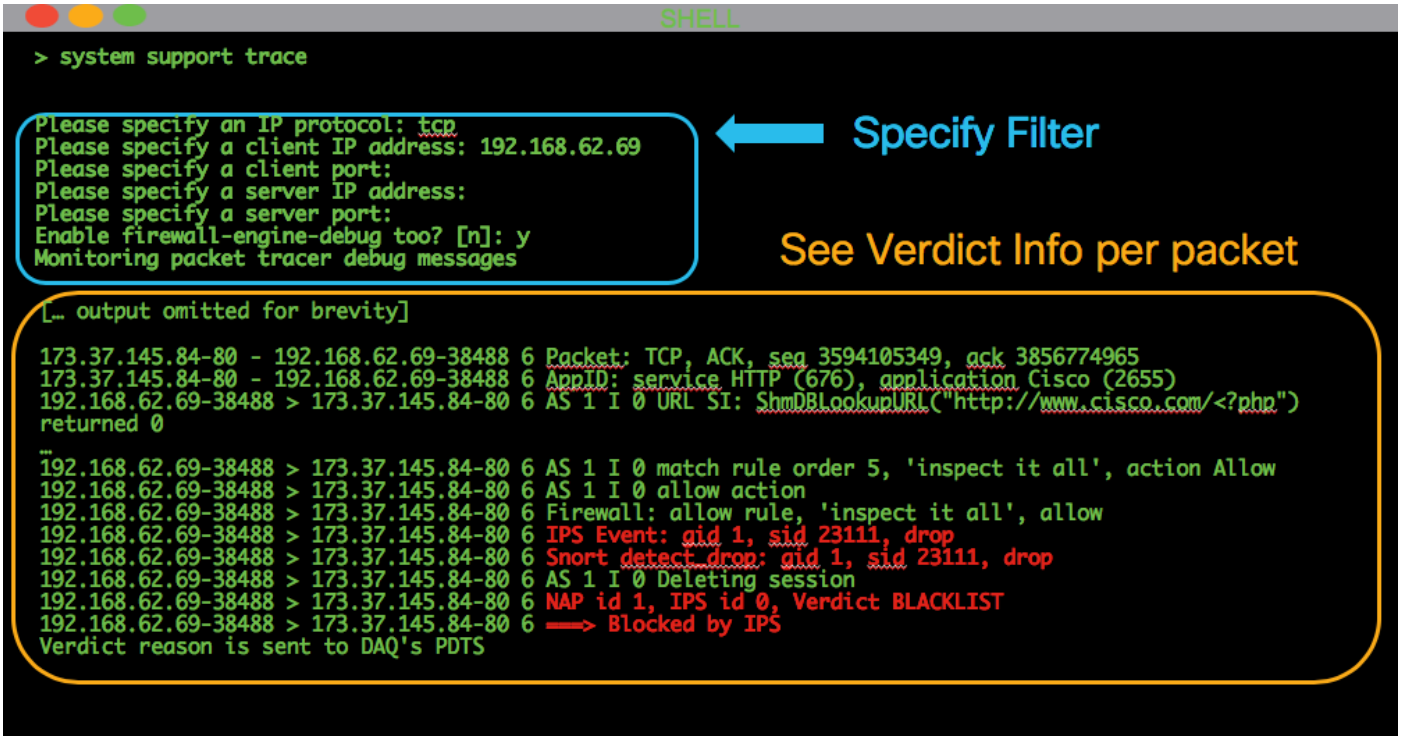
入侵策略可能正在丟棄流量或導致網路延遲。入侵策略可以在訪問控制策略的以下三個位置之一中使用：

- 在訪問控制規則中的「檢查」頁籤中
- 在預設操作中
- 在「高級」頁籤中，在**確定訪問控制規則之前使用的網路分析和入侵策略 > 入侵策略**部分

要檢視入侵策略規則是否阻止流量，請導航到FMC中的**分析>入侵>事件**頁面。Table View of Intrusion Events檢視提供有關事件中涉及的主機的資訊。有關事件分析的資訊，請參閱相關資料路徑故障排除文章。

判斷入侵原則簽章(IPS)是否封鎖流量的第一個建議步驟是使用FTD的CLI中的**>系統支援追蹤功**能。此debug命令的工作方式與firewall-engine-debug類似，它還提供在跟蹤的同時啟用firewall-engine-debug的選項。

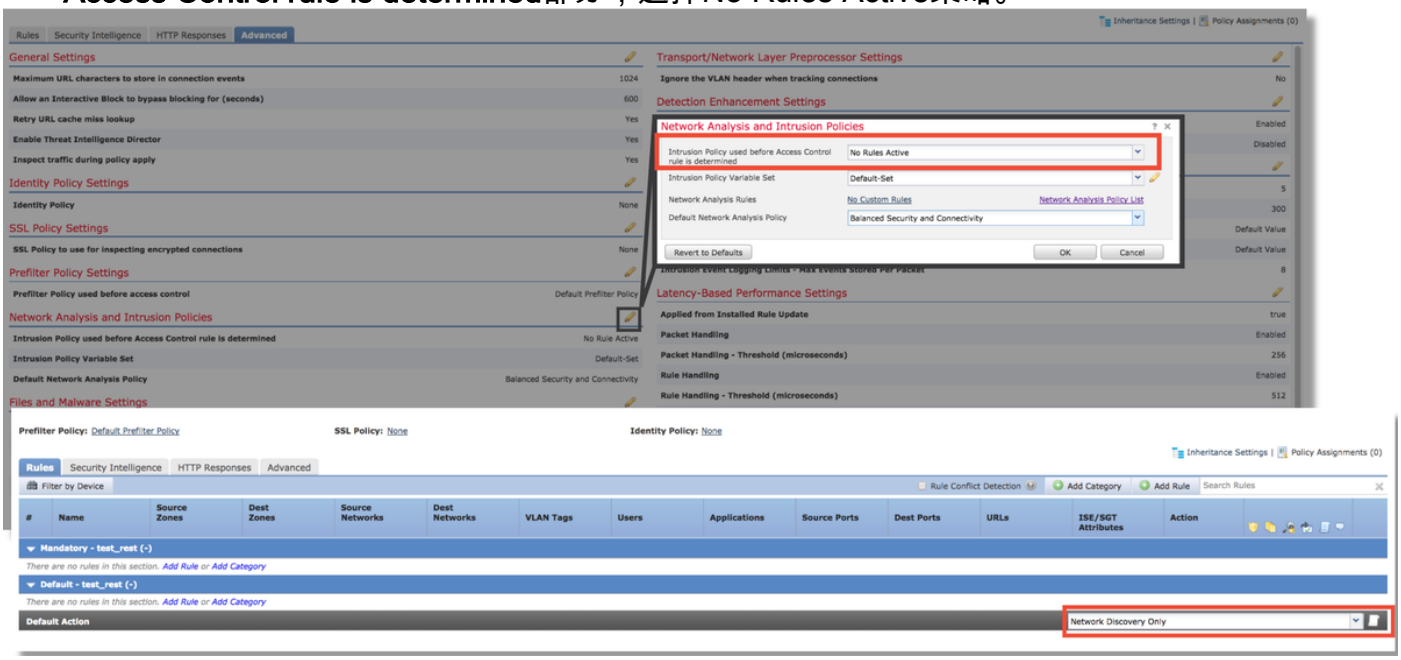
下圖顯示使用系統支援跟蹤工具的示例，該示例的結果顯示由於入侵規則導致資料包被阻止。這樣，您就可以獲得所有詳細資訊，例如GID（組識別符號）、SID（簽名識別符號）、NAP（網路分析策略）ID和IPS ID，因此您可以確切地看到哪些策略/規則正在阻止此流量。



如果您無法確定IPS正在阻止跟蹤輸出，但是您懷疑它是由於自定義入侵策略而丟棄的IPS，則可以用「平衡安全性和連線」策略或「通過安全的連線」策略替換入侵策略。這些是思科提供的入侵策略。如果進行更改，則解決此問題，則之前使用的自定義入侵策略可以由TAC進行故障排除。如果使用預設思科策略，您可以嘗試將預設策略更改為較不安全的策略，因為這些策略的規則較少，這樣有助於縮小範圍。例如，如果流量被阻止，而您使用的是平衡策略，則您會切換至通過安全策略的連線，問題消失，平衡策略中很可能有一個規則丟棄未設定為通過安全策略進行連線的流量。

可以在訪問控制策略中進行以下更改，以消除所有入侵策略檢查阻止的可能性（建議儘可能減少更改以不改變安全效力，因此建議針對相關流量設定目標AC規則，而不是在整個策略中禁用IPS）：

- 在所有訪問控制規則（或僅是特定流量匹配且受影響的規則）中，從Inspection頁籤中刪除Intrusion Policy
- 在Advanced頁籤的**Network Analysis and Intrusion Policies > Intrusion Policy used before Access Control rule is determined**部分，選擇No Rules Active策略。



如果仍然不能解決問題，請繼續排除網路分析策略故障。

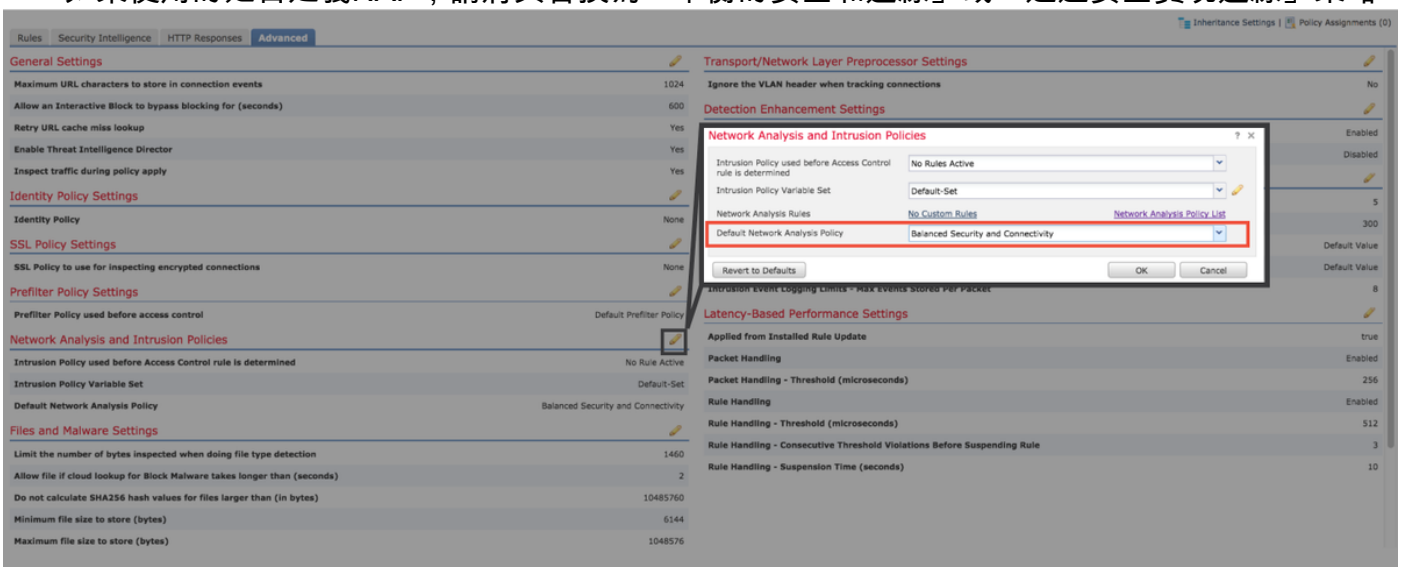
有關入侵策略功能的更多深入故障排除，請檢視相關的資料路徑故障排除文章。

網路分析策略

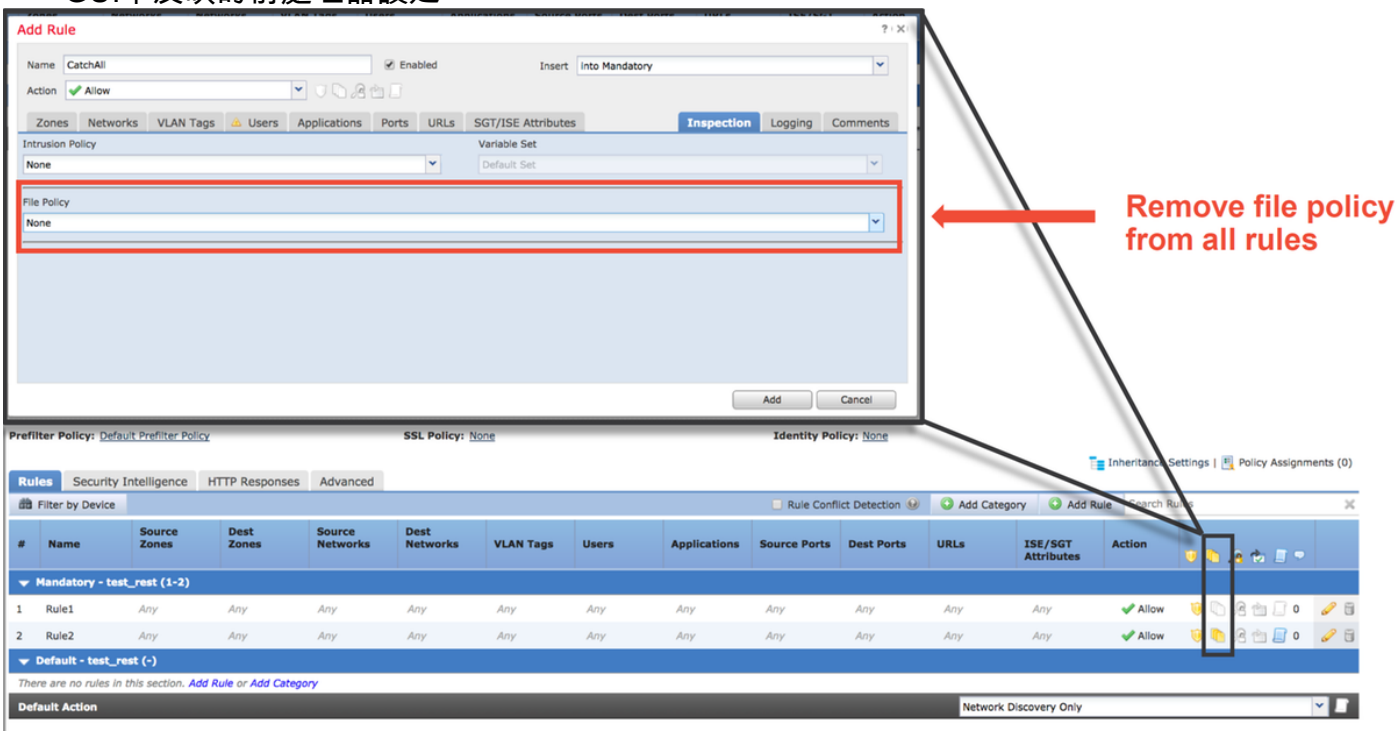
網路分析策略(NAP)包含Firepower前處理器設定，其中一些設定可以丟棄流量。進行此故障排除的第一個建議步驟與IPS故障排除相同，即使用**>系統支援跟蹤**工具嘗試查詢snort中阻塞流量的內容。請參閱上面的「入侵策略」部分，瞭解有關此工具和示例用法的更多資訊。

為快速緩解NAP可能存在的問題，可執行以下步驟：

- 如果使用的是自定義NAP，請將其替換為「平衡的安全和連線」或「通過安全實現連線」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，請暫時將其刪除，因為檔案策略可以在後端啟用不會在GUI中反映的前處理器設定



有關網路分析策略功能的更深入故障排除，請參見本文中。

相關資訊

指向Firepower文檔的連結

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