Firepower資料路徑故障排除第3階段：安全情報

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三階段，即安全情報功能。

必要條件

- 本文涉及當前支援的所有的Firepower平台
- URL和DNS的安全情報是在6.0.0版中引入的

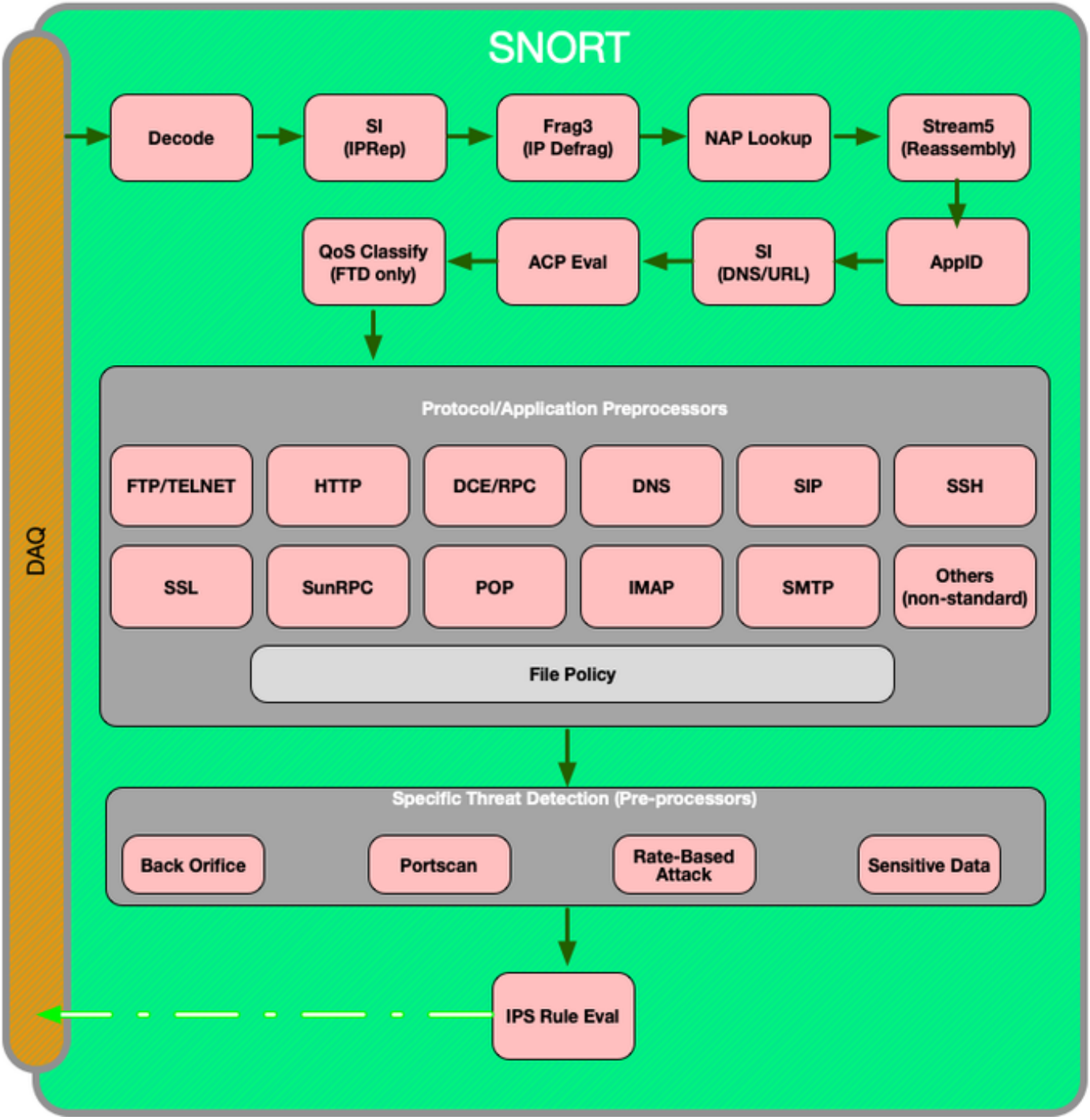
Firepower安全情報階段故障排除

安全情報是一項功能，可針對以下專案對黑名單和白名單執行檢查：

- IP地址（在UI的某些部分也稱為「網路」）
- 統一資源定位器(URL)
- 網域名稱系統(DNS)查詢

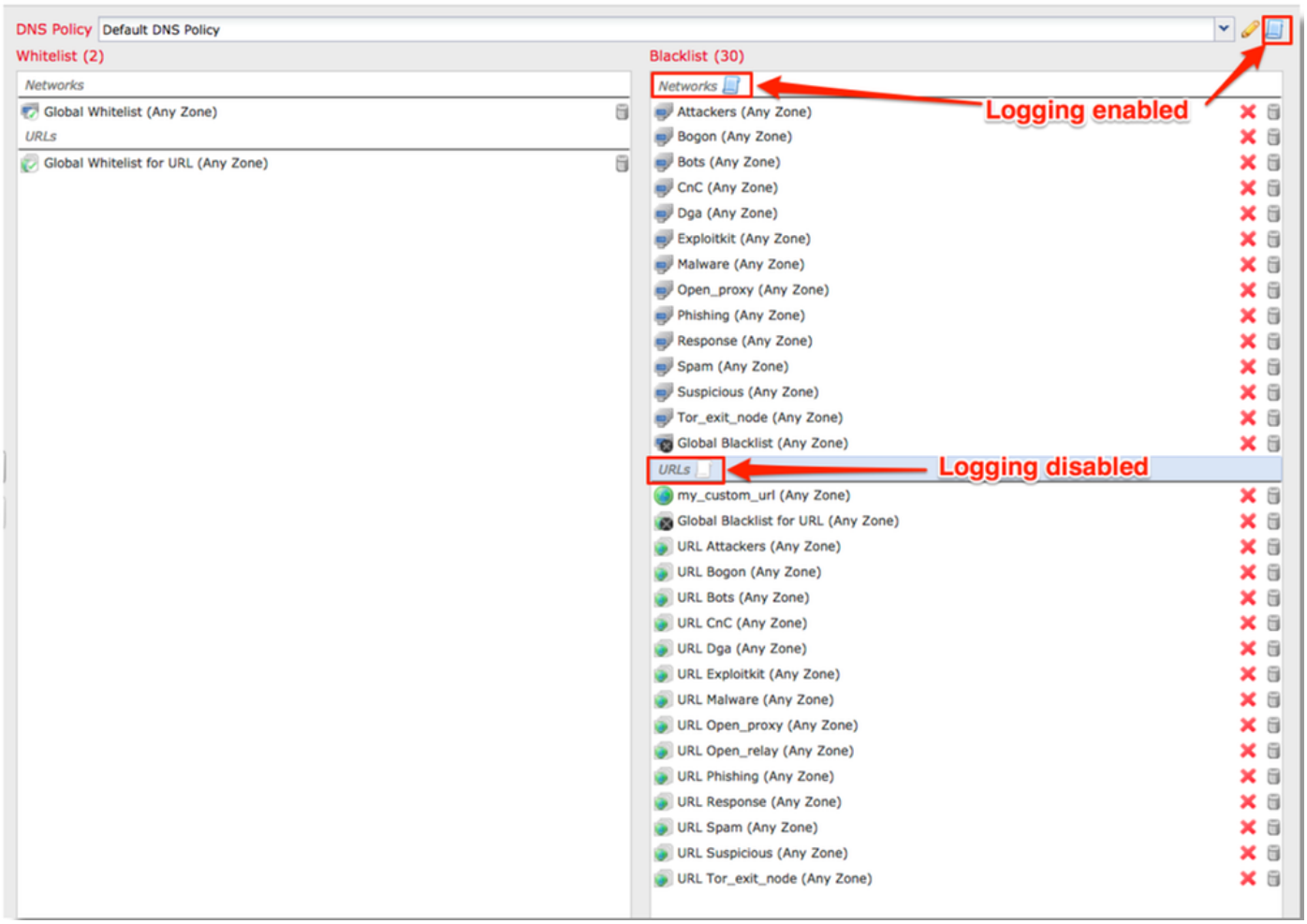
安全情報中的清單可以由思科提供的源和/或使用者配置的清單和源填充。

基於IP地址的安全情報信譽是Firepower中第一個檢查流量的元件。一旦發現相關應用協定，就會立即執行URL和DNS安全情報。下面是概述Firepower軟體檢查工作流程的圖表。



確定已啟用安全情報事件記錄

只要啟用了日誌記錄，就很容易確定安全情報級別的塊。這可在Firepower管理中心(FMC)使用者介面(UI)上通過導航到**策略>訪問控制>訪問控制策略**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。

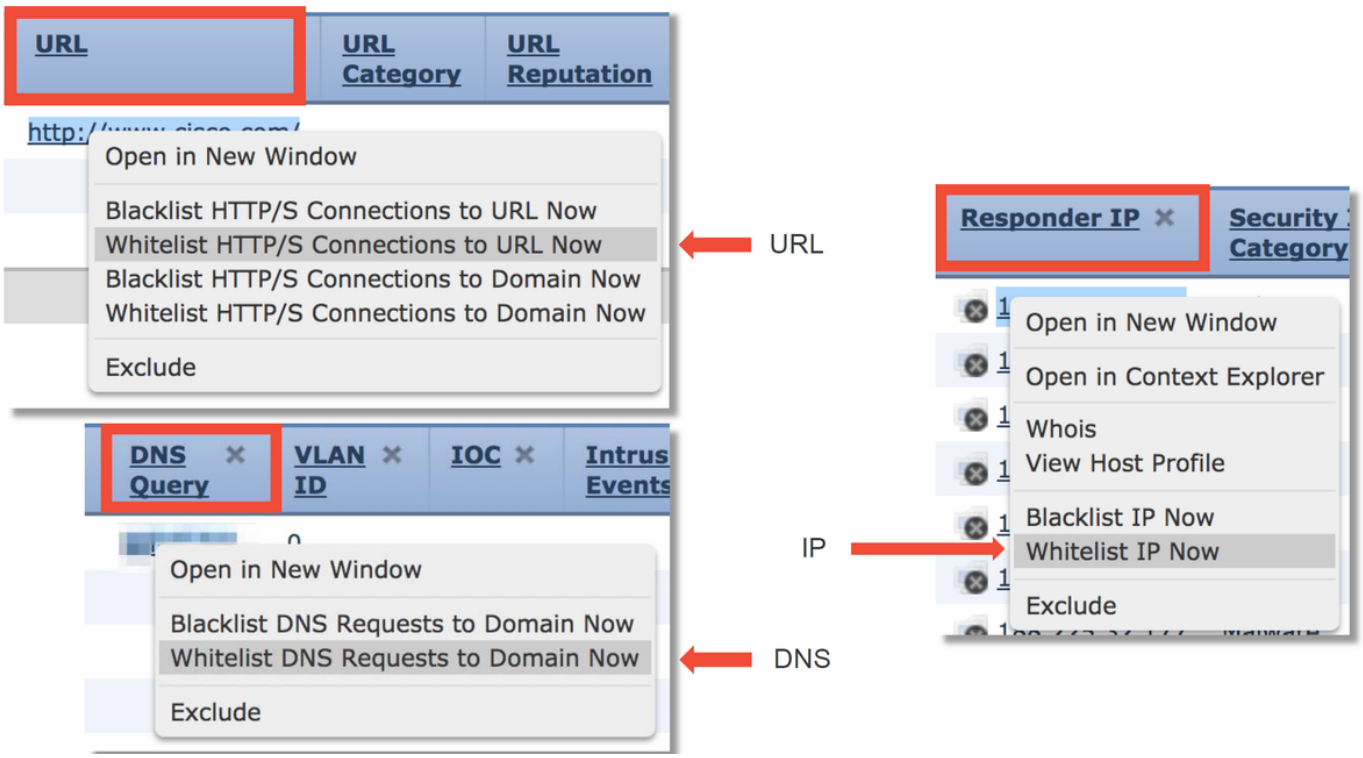


檢視安全情報事件

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

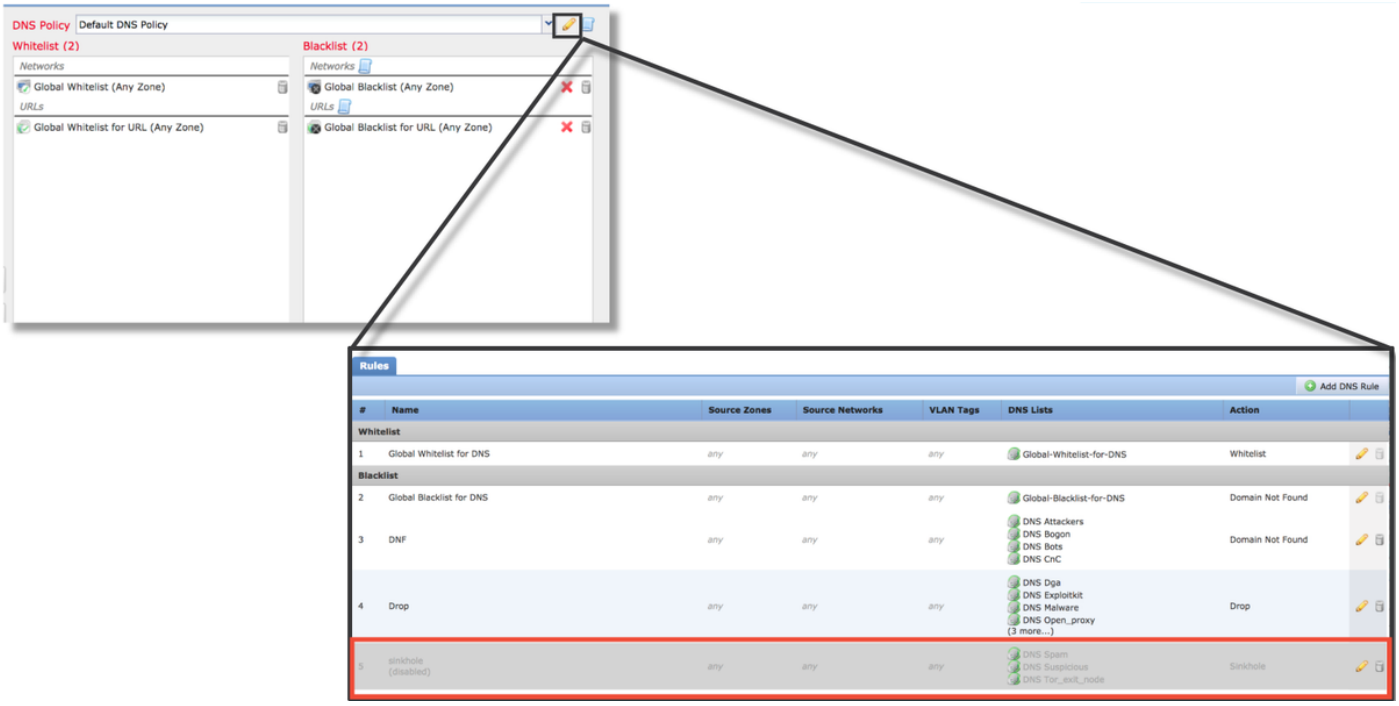
您還可以將資料提供給思科技術協助中心(TAC)，以調查是否應將這些專案從黑名單中刪除。

> **附註**：新增到白名單只會向相關安全情報白名單新增一個條目，這意味著允許對象通過安全情報檢查。但是，所有其他Firepower元件仍可以檢查流量。

如何刪除安全情報配置

要刪除安全情報配置，請導航到**安全情報**頁籤（如上所述）。共有三部分；一個用於網路、URL以及DNS策略。

從這裡可以點選垃圾桶符號刪除清單和源。



請注意，在上面的螢幕截圖中，除全域性黑名單和白名單外，所有IP和URL安全情報清單都已刪除。

在DNS策略（儲存DNS安全情報配置的位置）中，禁用其中一個規則。

> **附註**：要檢視全域性黑名單和白名單的內容，請導航到**對象>對象管理>安全情報**。然後，按一下感興趣的部分（網路、URL、DNS）。 然後，編輯清單將顯示內容，儘管配置必須在訪問控制策略中執行。

驗證後端上的設定

可通過**> show access-control-config** 命令在CLI上驗證安全智慧配置，該命令顯示Firepower裝置上運行的活動訪問控制策略的內容。

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action           : Allow
Default Policy           : SOC
Logging Configuration
   DC                  : Enabled
   Beginning           : Disabled
   End                 : Enabled
Rule Hits                : 0
Variable Set             : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                : Global-Whitelist (List)
   IP Count            : 0
   Zone                : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration    : Enabled
   DC                  : Enabled


--------------------[ Block ]---------------------
   Name                : Attackers (Feed)
   Zone                : any

   Name                : Bogon (Feed)
   Zone                : any
...[omitted for brevity]
```

請注意，在上面的示例中，為網路黑名單配置了日誌記錄，並且黑名單中至少包含兩個源（Attackers和Bogon）。

可以在專家模式下確定單個專案是否位於安全情報清單中。請參閱以下步驟：

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware
```

IP SI lists are in /var/sf/iprep_download/

```
$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url
```

URL SI lists are in /var/sf/siurl_download/

```
$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

DNS SI lists are in /var/sf/sidns_download/

每個具有唯一UUID的安全情報清單都有一個檔案。上例顯示如何使用**head -n1** 命令識別清單的名稱。

要提供給TAC的資料

資料	說明
檢查流量的FMC和Firepower裝置的檔案故障排除	http://www.cisco.com/c/en/us/support/docs/
事件的螢幕截圖（包括時間戳）	有關說明，請參閱本文
CLI會話的文本輸出	有關說明，請參閱本文
如果提交誤報案例，請提供要爭議的專案（IP、URL、域）。	提供執行爭議的原因和證據。

下一步

如果確定安全情報元件不是問題的原因，則下一步是排除訪問控制策略規則的故障。

按一下here繼續下一篇文章。