瞭解Snort 3：狀態簽名評估Byte_Jump

目錄

簡介

本檔案將說明Snort 3自7.4之後新增的技術。

背景資訊

- Snort 3檢測模組在塊模式下工作。雖然這種方法具有效能優勢和實作簡便性（相對而言），但在檢測跨越多個資料塊的特徵碼方面存在一些限制。
- 為了方便使用者體驗，Snort中已經進行了一些改進，即：
  1. Flowbits允許規則編寫器使用使用者定義的屬性標籤網路流；該屬性可以在流中的任何資料包上設定、清除和測試（它提供了一種在資料包上得出某些較大簽名的方法）。
- 流模組將有線資料包累積為重建資料包，該資料包比原始資料包更大、更有意義；針對重建資料包評估IPS規則可提供更多機會來檢視整體情況並匹配更大的模式（簽名）。
- 在一些情況下，重建的資料包不僅呈現新資料，而且包括檢測已處理的先前資料的某些部分；同樣地，該累積資料塊允許檢測向後跨越流（在某種程度上）的簽名。
- 資料流拆分器將資料流分成多個塊，但切點可能是攻擊者用來避免模式檢測的薄弱點；因此Snort採用了一種抖動機制，使得拆分更加不可預測。這使對攻擊者的分析更加複雜。

最新消息

狀態簽名評估是一種可以增加到清單的新技術。它透過在多個塊上啟用IPS規則評估來擴展檢測能力。因此，如果當前塊缺少資料，規則不會立即不匹配，而是等待更多資料到達。

支援的平台

最低軟體和硬體平台

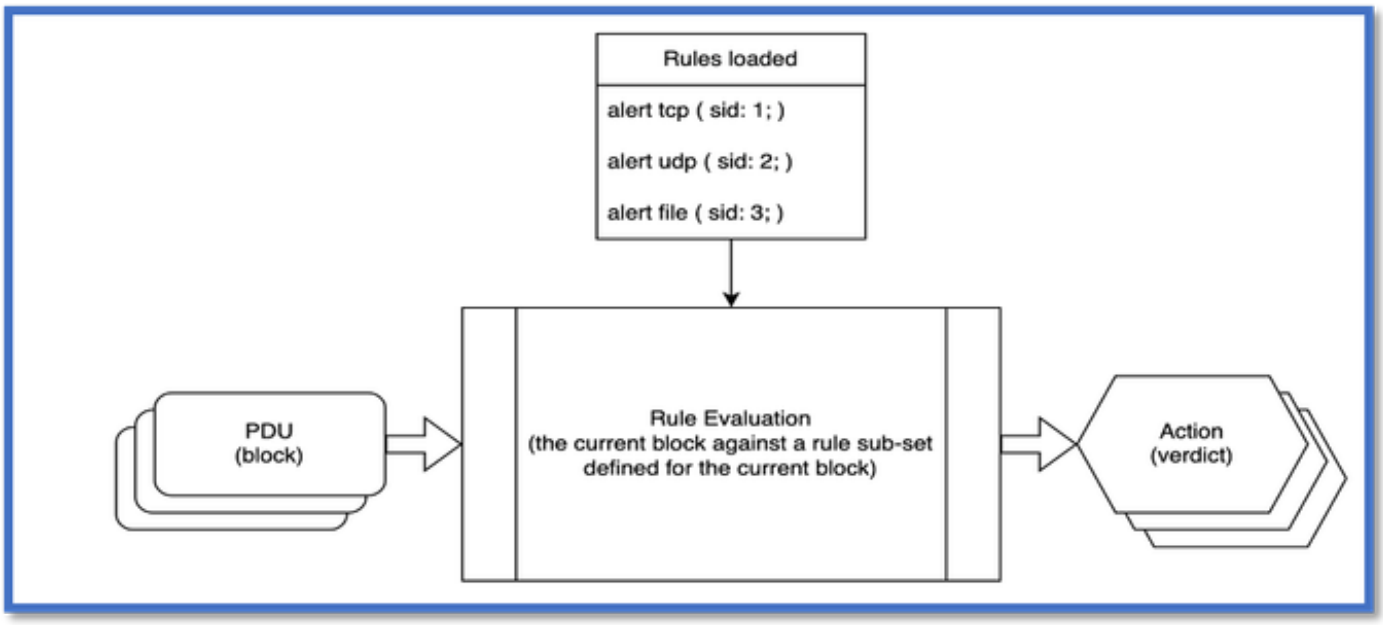
支援的管理員最低版本	受管裝置	需要支援的最低受管裝置版本	備註
管理中心7.4.0	FTD	7.4.0	僅Snort 3
裝置管理員7.4.0	支援FDM管理的任何FTD	7.4.0	僅Snort 3

功能詳細資料

功能功能說明

如何運作？

檢測模組工作流程如圖所示。在流量處理階段，模組已載入了所有規則，並且它以逐個方式接受資料塊、評估規則並定義要為進程狀態簽名評估塊執行的操作。



有關方案的附註：

1. 為當前資料塊定義規則子集後，將獨立於其他規則評估其中的每個規則。

2. 每個資料塊的計算與其他塊無關。
3. 資料塊是為當前資料包評估的一組IPS緩衝區的抽象。
4. Action是為當前資料包評估的操作的清單；最終判定將在稍後確定。

要瞭解狀態簽名評估的工作方式，請檢視如何評估常用的IPS規則，以及資料塊如何形成流。

通用規則評估

IPS規則可以以下列形式表示：

```
action protocol source → destination ( option_1: parameters; option_2: parameters;
option_3: parameters; gid: 1; sid: 1; meta_option_1; meta_option_2; meta_option_3; )
```

其中：

action -如果規則觸發，則對資料包執行IPS操作

protocol -匹配的協定

源、目標- IP地址和埠

option_1、option_2、option_3 -作為規則評估一部分的IPS選項

gid、sid -標識規則的唯一對（類似於後設資料選項）

meta_option_1、meta_option_2、meta_option3 -如消息、類型別或引用等規則後設資料，這些選項不參與規則計算。

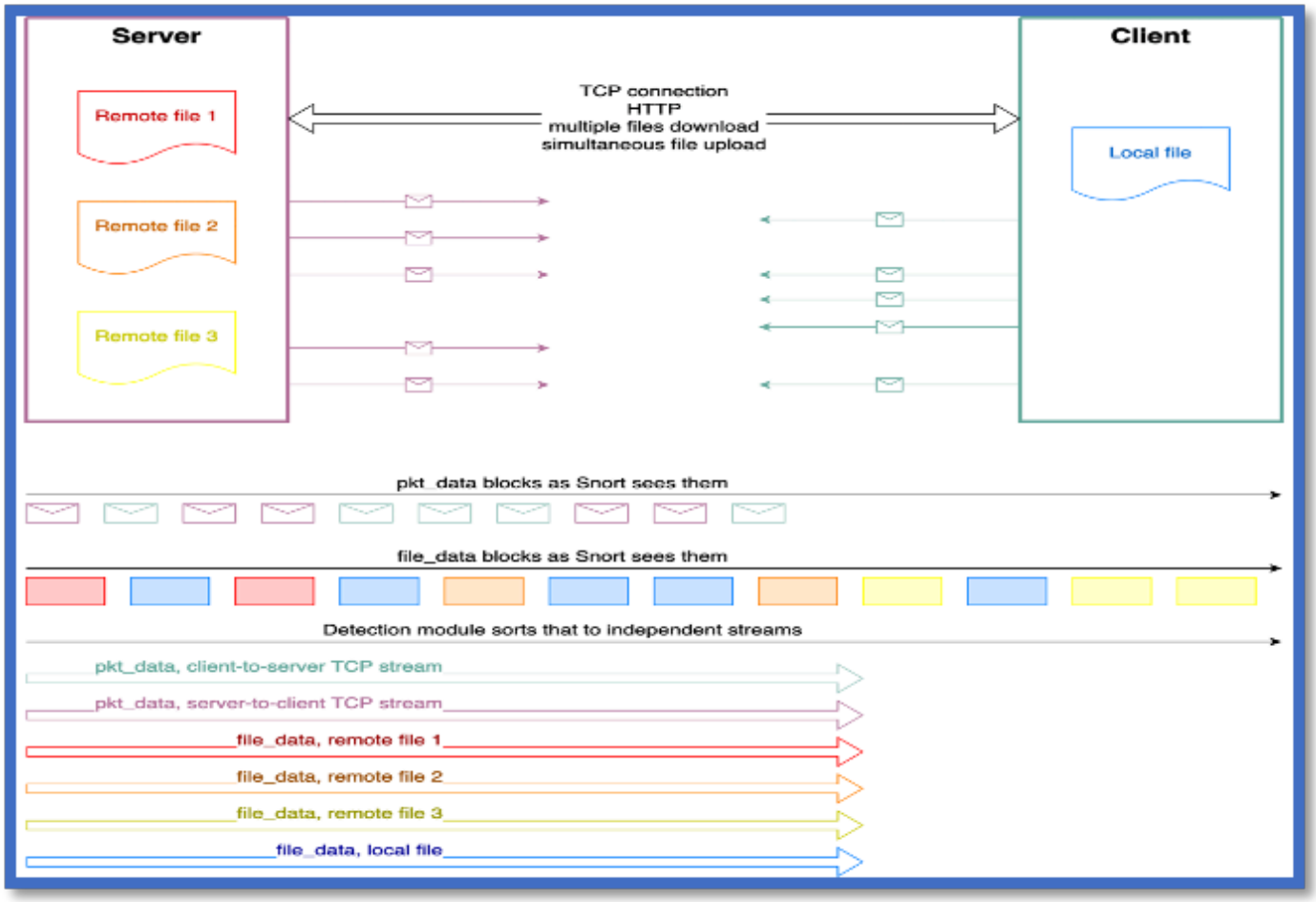
- 協定、源和目標構成一個規則報頭。它充當網路流的過濾器（接受該流進行評估）。括弧中的所有內容都是規則主體。來自規則主體的IPS選項（規則後設資料除外）是為資料塊評估的選項。它們符合以下宣告：
- 選項嚴格按照從左到右的順序進行計算。
    1. 可以是兩種主要型別之一。
    2. buffer setter時，該選項會為當前資料包選擇IPS緩衝區。
- 其他（模式搜尋、數學操作、游標操作、flowbit操作）
- 游標用於跟蹤選定IPS緩衝區中的位置。

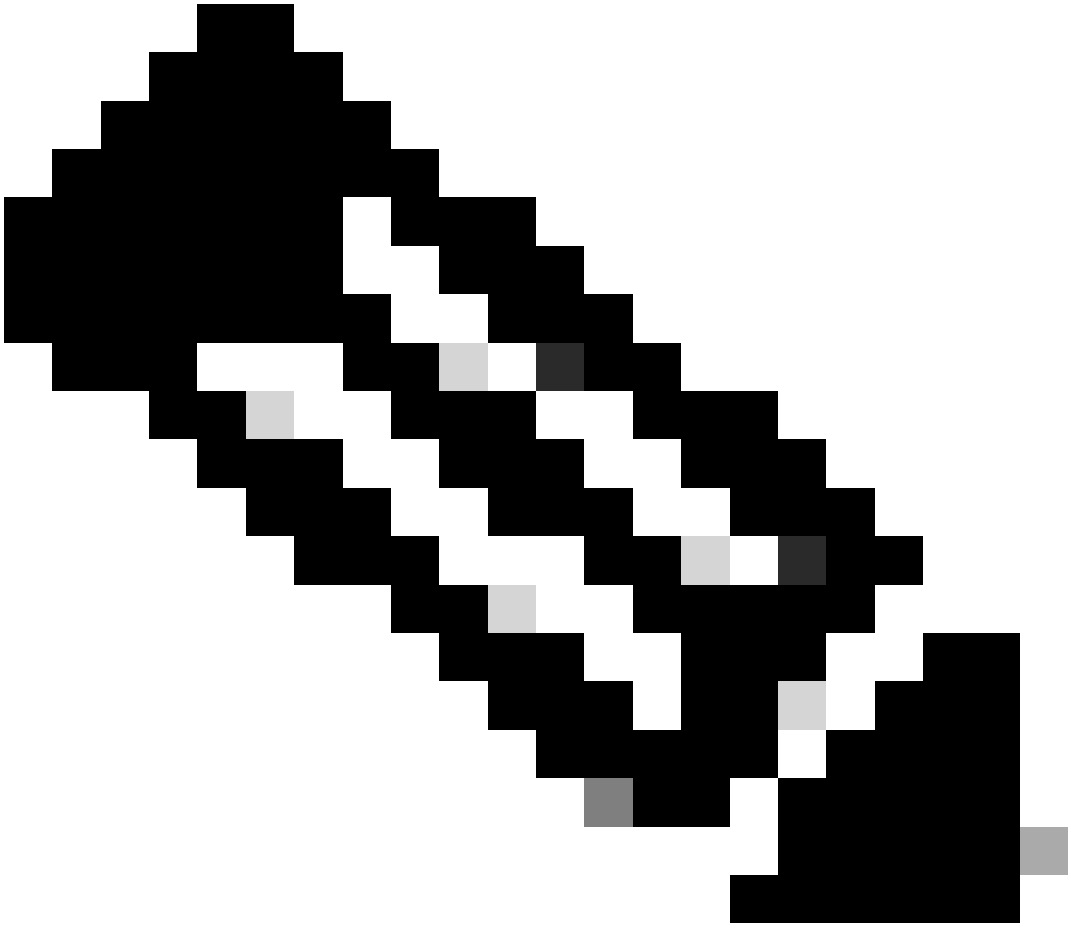
- 選項可以是：
    1. 「absolute」，表示不依賴於游標位置
    2. 「相對」，表示從游標位置開始計算
- 如果某個選項嘗試將游標從選定的IPS緩衝區中設定，則該選項會失敗，並且整個規則不匹配（由於缺少資料）
- 最後一點是檢測模組的限制。如果Snort可以擁有無限的資源，則當資料可用時（有更多有線資料包到達），它會快取所有被視為評估規則的資料。

資料流和IPS緩衝區

- 資料流是來自同一源的連續形式的位元組流。它是一種支援狀態評估的新概念。塊之間的規則評估必須在同一邏輯資料（無論是檔案、純TCP資料流還是JavaScript文本）內完成。

- 通常，檢測模組接收的資料塊可以：
  - 來自不同的IPS緩衝區（例如，pkt_data和file_data不相同）
  - 屬於另一個流
  - 不形成流（從原始資料包生成的緩衝區）
  - 不形成連續串流(ICMP、UDP)
  - 不按順序（HTTP部分響應）
  - 包含重複的資料（累積區塊，如http_inspect.script_detection或HTTP區塊回應）
- 該檢測模組可以僅對來自同一流的塊進行排序以串聯，否則，該評估過程將看到來自交織塊的不需要的干擾。





注意：此處的示例顯示一個HTTP客戶端同時上載和下載多個檔案的情況。

- 目前，只有兩個IPS緩衝區可以表示一個流：pkt_data和file_data，其中：
  1. pkt_data形成TCP協定的兩個資料流（客戶端到伺服器和伺服器到客戶端方向）
  2. file_data必須為檔案、MIME附件和其他協定資料（如HTTP HTML頁面和/或其他Content-Type）建立流
- 有狀態評估僅在資料流內進行。

規則延續

- 前面部分以說明IPS選項在游標位於當前IPS緩衝區之外時不匹配。但是，當IPS緩衝區形成資料流時，狀態簽名評估功能會逐步進入，並將規則評估上下文儲存在Snort流對象中。儲存的評估內容（狀態）稱為規則延續。狀態簽名評估會將規則的最終判定延後，直到有更多資料可用。
- 規則延續有三個主要部分：IPS緩衝區名稱、緩衝區來源和目標游標位置（緩衝區來源是資料流的唯一辨識碼）。
- 當資料塊由檢測模組處理時，後續操作發生：-

    - 狀態簽名評估會建立規則連續性，並在以下情況下將其附加到流：
        - IPS選項（byte_jump、content、pcre或任何更新游標位置的其他內容）將游標設定在當前IPS緩衝區之後
        - 當前IPS緩衝區支援資料流。
        - 當前IPS緩衝區會形成資料流。
- 有狀態簽名評估會撤銷剛剛建立的規則連續性，並在以下情況下將其從流中刪除：
    - IPS規則已在當前資料塊上觸發（該規則與塊的其他位置匹配）
- 有狀態簽名評估拒絕待處理的規則繼續，並在以下情況下將其從流中刪除：
    - IPS緩衝區不會形成連續的資料流(例如，資料塊中有重複的資料，或者存在間隙（資料丟失的一部分或資料塊順序錯誤）。
- 有狀態簽名評估會在下列情況下使用新的可用資料更新目標游標位置：
    - 規則延續的緩衝區來源與選取的緩衝區來源相同
    - IPS緩衝區形成連續流
- 有狀態簽名評估會在以下情況將規則繼續傳送回IPS規則引擎：
    1. 目標游標將點定位在選定IPS緩衝區內（這意味著它最終收到了完成規則評估所需的所有資料）。

使用者組態

- 由於規則持續佔用記憶體，因此Snort無法儲存無限數量的記憶體。有一個組態選項可控制限制：
    1. Detection.max_continuations_per_flow = 1024：同時儲存在流中的最大連續數{0：65535 }
- 當有狀態簽名評估達到限制時，它將用新規則替換最舊的規則延續。
- 駐留在該流上的最舊規則延續時間太長，這意味著它仍然不符合恢復規則評估的條件。
- 此外，還有大量掛接計數可用於微調IPS規則（這必須是主要焦點）和限制（如果需要）：
    1. detection.cont_creations：建立的連續總數（總和）
    2. detection.cont_recalls：已召回的繼續總數（總和）
    3. detection.cont_flows：使用連續流的流總數（總和）
    4. detection.cont_evals：符合條件的連續總數（總和）
    5. detection.cont_matches：符合的連續作業總數（總和）
    6. detection.cont_mismatches：不符合的連續作業總數（總和）
    7. detection.cont_max_num：每個流同時繼續的峰值數（最大）
    8. detection.cont_match_distance：匹配連續數跳過的位元組總數（總和）
    9. detection.cont_mismatch_distance：不匹配連續數跳過的位元組總數（總和）

疑難排解

此功能是對現有檢測過程的增強，因此無法顯式進行故障排除。如果任何檢測失敗，則必須檢查規則、配置或流量。

問題示例

問題：描述

- 讓我們假設簽名必須同時檢查檔案的開頭及其尾部。
- 例如，在此結構的目標檔案（標頭、主體、中繼資料）中，我們需要檢視其中繼資料是否有0值。

- 檔案位元組：e1 f3 22 03 7f ff xx xx ... xx 01 00 02 00 ，其中

    - e1 f3 22 03 – 4個位元組，用於標識檔案型別的幻數
    - 7f ff - 2位元組代表主體大小
    - xx xx ... xx - 32kb的部分資料
    - 01 00 02 00 – 4位元組後設資料，採用標籤值格式（每個1位元組）
- IPS規則將如下所示：alert file (file_data； content：「|e1f32203|」，fast_pattern；byte_jump：2,0，relative； content：「00」，within：4， relative； sid： 1；)

    - 其中

        - 檔案協定確保規則僅接受重建的資料包（原始資料包不參與狀態簽名評估）
        - 'file_data選項選擇可以形成流的檔案資料緩衝區
        - 第1個內容選項是一個快速模式，它會檢查幻數（如果這是預期的檔案型別）
        - byte_jump選項會讀取檔案主體大小並跳至檔案主體
        - 第二個內容選項會在引數限制搜尋深度內執行中繼資料值的最終檢查，並使該選項成為相對選項。

問題：解決方案

將以下列方式評估規則：

第1個封包（大小為8kB），其中含有檔案標頭及內文的一部分：

1. 已選擇IPS buffer file_data。游標指向第0位元組e1。
2. 快速圖樣選項會比對並設定游標在幻數之後的位置，指向位元組7f。
3. byte_jump選項讀取兩個位元組的檔案主體大小。游標會以這兩個位元組更新。然後byte_jump計算超過32768個位元組的跳躍。
4. 狀態簽名評估會建立規則延續，在該規則中它需要多24578位元組(32768 -（8kB - 4位元組報頭- 2位元組正文大小））。
5. 整個規則不匹配，因為byte_jump選項無法將游標位置設定得那麼遠。

第二個封包（大小為16kB）攜帶檔案主體部分：

1. 狀態簽名評估發現掛起規則延續。
2. 它會依名稱選取緩衝區，並看到file_data可用且新資料大小為16384。
3. 更新的游標顯示仍需要8194位元組(24578 - 16384)
4. 規則未恢復。

第3個資料包（大小為8198個）攜帶檔案正文部分和後設資料：

1. 狀態簽名評估發現掛起規則延續。
2. 它會依名稱選取緩衝區，並看到file_data可用，而新的資料大小為8198。
3. 更新的游標顯示緩衝區有足夠的資料，游標位置是8194。
4. 狀態簽名評估會刪除規則連續性。

5. 狀態簽名評估從第2個內容選項恢復規則評估，游標指向位元組01。
6. 內容選項會在搜尋到的第二個位元組上尋找相符專案。
7. 整個規則終於觸動了。

限制詳細資訊和常見問題

限制和其他注意事項

- 由於狀態簽名評估實現，Snort在重新載入其配置時丟棄所有待處理的規則繼續。請注意，儘管規則被丟棄，但繼續操作仍會佔用Snort記憶體，直到下一個資料塊傳送到檢測模組為止。
- 狀態評估中IPS規則的規則延遲功能的作用與普通規則評估相同。總結了不同資料塊上規則部分的評估時間。如果時間超過限制，則規則評估會執行短路，提前退出。
- Flowbits操作保留了它們的意義，儘管它們仍然像「靜態」選項一樣運行。
  在當前已知環境中執行flowbit設定/清除/測試操作。因此，如果在規則繼續中評估flowbit選項，它將考慮當前環境（flowbits集），而不是規則開始評估時的環境。

此外，規則編寫者必須注意快速模式位置。

即使它可位於規則的任何部分，也會在整個規則之前評估fast-pattern選項。它觸發規則評估。對於基於狀態簽名評估的規則，這意味著規則接續點必須位於fast-pattern選項之後。
此外，IPS規則的評估可以有多個規則連續性（一個接一個，而不是同時）。由於規則主體中的任何選項都可以繼續，因此規則編寫器可以使用相同的IPS規則在資料流中的不同位置執行額外檢查。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。