在安全FTD上使用Snort 3速率過濾器設定基於速率的攻擊防禦

問題

重點是如何構建規則以覆蓋多個子網、瞭解實施的最佳實踐，以及確定警報或阻止的適當閾值（每秒計數），特別是在防禦SYN泛洪攻擊的情況下。

環境

- 執行FTD 7.4.2.4的Cisco安全防火牆Firepower
- Firepower 2110硬體平台
- 由Firepower管理中心(FMC)7.6.2.1管理
- 已啟用rate_filter檢查器的Snort 3入侵防禦系統
- 多個內部子網需要針對SYN泛洪進行保護
- 不存在活動故障；主動防禦配置指南

解析

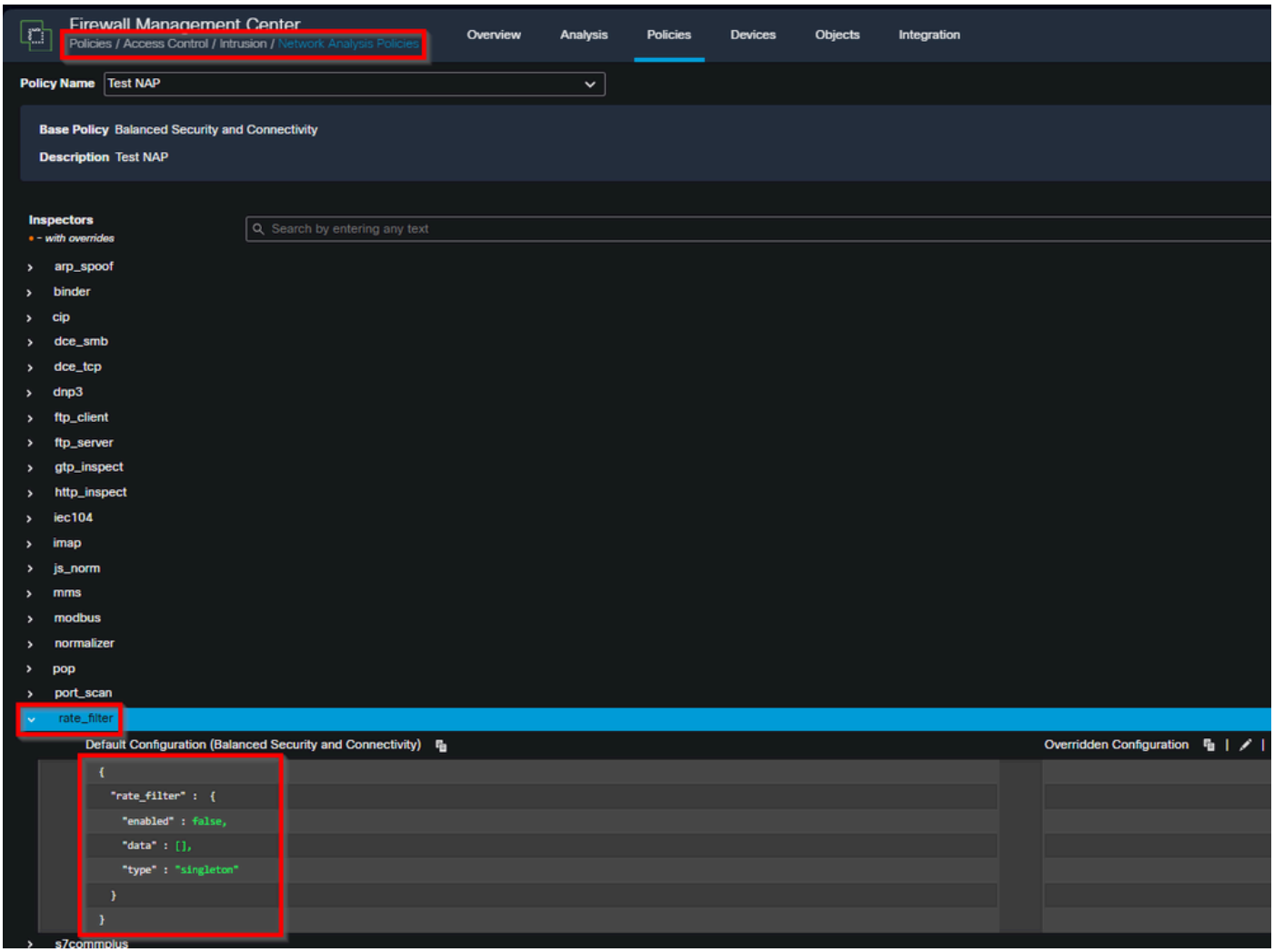
這些步驟詳細說明了如何使用Cisco安全防火牆FTD上的Snort 3 rate_filter檢查器來配置和實施基於速率的攻擊防禦，包括說明多個子網的規則結構和最佳實踐建議。這些操作旨在幫助為正常流量建立基線，並啟用有效檢測或阻止SYN泛洪攻擊。

附註：TAC工作範圍內不建議或建議這些規則過濾器使用的任何特定值。每個環境都不同，需要深入分析流量模式和網路設計，以確定這些過濾器的最佳值。

1：導航至Snort 3 rate_filter

這些過濾器在Policies > Access Control: Intrusion > Network Analysis Policies 下配置，方法是按一

下NAP策略的Snort 3版本，然後按一下左側面板中的rate_filter下拉選單。



inline_image_0.png

2：瞭解Snort 3速率過濾器規則結構

Snort 3中的rate_filter檢查器允許您定義規則，以監視特定型別的流量（如SYN資料包），並在超過定義的閾值時採取操作（警報或丟棄）。這些規則可以針對多個子網。

多個子網的rate_filter配置示例：

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": ["10.1.2.0/24", "10.1.3.0/24"],
        "count": 5,
        "gid": 135,
        "sid": 1,
        "new_action": "alert",
        "seconds": 10,
```

```
        "timeout": 15,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

引數說明：

- apply_to：過濾器應用的IP地址或子網清單（支援多個子網）。
- count + seconds：事件的閾值（例如，10秒內有5個SYN資料包）。
- gid / sid：標識Snort事件（例如ss GID 135,SID 1用於SYN泛洪檢測）。
- new_action:超過閾值時要採取的操作(例如，alert、drop)。
- timeout：觸發相同條件的新警報/操作之前的持續時間。
- track：跟蹤模式(例如，by_src for per-source IP，by_dst for per-destination IP)。

3：閾值調整和策略部署的最佳實踐

- 在警報模式下開始：將new_action設定為alert，然後使用保守的閾值(例如count和seconds)以避免誤報。
- 基線網路流量：監控生成的事件，以瞭解您的環境和子網的「正常」SYN速率是什麼樣的。
- 反複調整引數：根據觀察的流量模式和操作需求調整計數、秒和超時。
- 移至阻止：一旦確信閾值準確反映異常行為，請將new_action從alert更改為drop或等效於主動阻止攻擊。
- 根據需要單獨使用過濾器：如果流量模式不同，請考慮不同網段或角色（例如伺服器與使用者子網）的不同速率限制。
- 持續監控：保持對rate_filter事件的警報和監控，以快速確定調整問題或活動威脅。

原因

無。由於以前的SYN泛洪事件，請求配置是為了實現主動安全並作為指導。

相關內容

- Snort 3檢查器參考：速率過濾器
- 思科安全防火牆管理中心裝置配置指南7.4:基於速率的攻擊防禦
- 思科技術支援與下載

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）。