在安全防火牆威脅防禦7.4中配置AppID早期資料包檢測

目錄

簡介

本文檔介紹如何在Cisco Secure Firewall 7.4中配置AppID早期資料包檢測。

背景-問題（客戶要求）

- 透過深度資料包檢測的應用檢測可能需要多個資料包來辨識流量。
- 有時，在已知應用伺服器的IP和/或埠的情況下，您可以避免檢查其他資料包。

最新消息

- 基於Snort的新Lua AppID API已經建立，它允許我們將IP地址、埠和協定對映到以下各項：
  - 應用協定(service appid)、
  - 客戶端應用（客戶端appid）和
  - Web應用程式（有效負載appid）。
- 可以使用此API在FMC上建立自定義應用檢測器，以進行應用檢測。
- 一旦啟用此檢測器，我們便可使用此新的API來辨識會話中第一個資料包上的應用。

功能概述

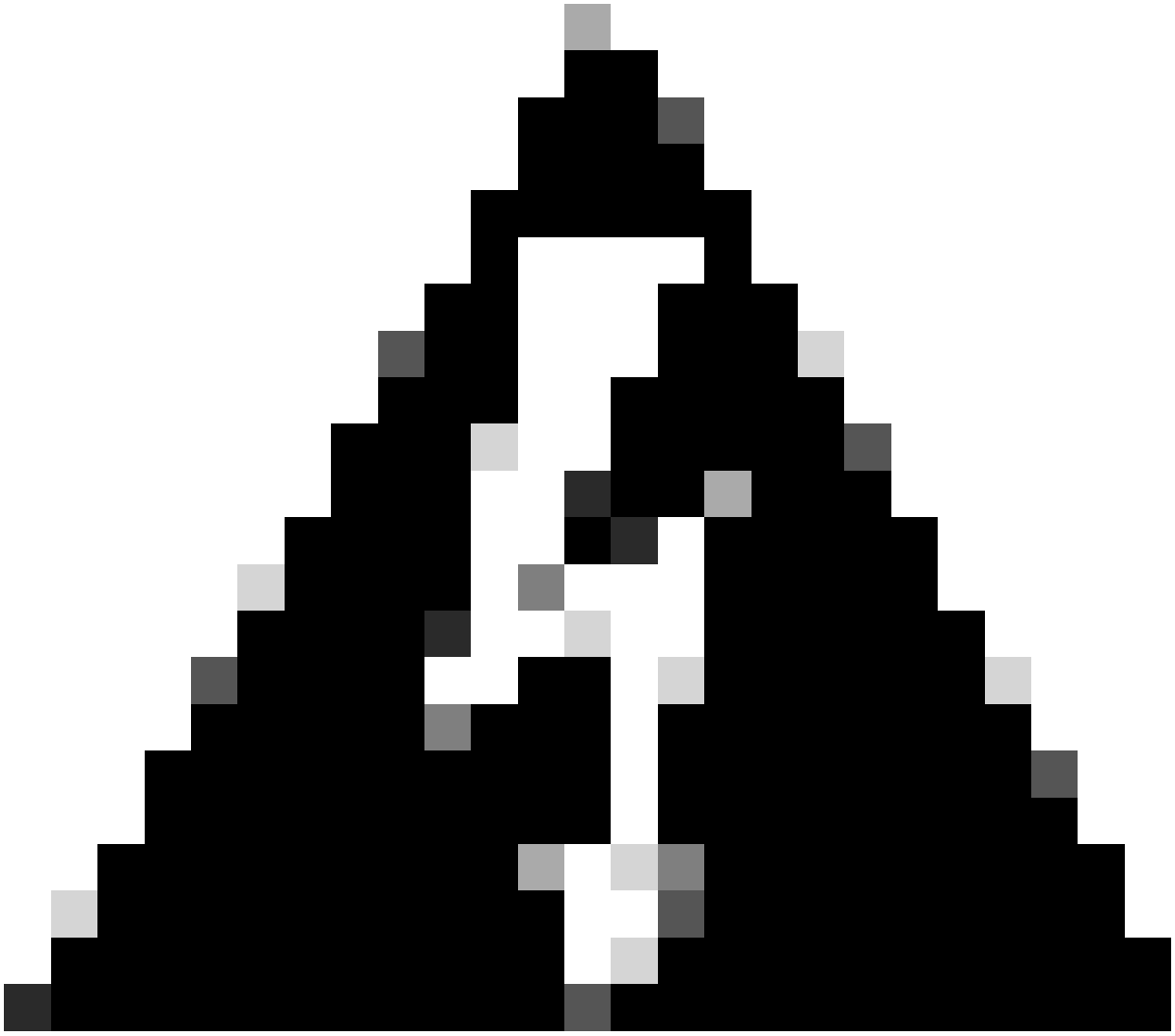
- API標識為：
  - **addHostFirstPktApp** （protocol_appId、client_appId、payload_appId、IP地址、埠、協定、恢復）

- 在自訂應用程式偵測器中建立的每個對應都會建立快取專案。
- 檢查所有傳入會話的第一個資料包，檢視在快取中是否找到匹配項。
- 找到匹配項後，我們將為該會話分配相應的appid，應用發現過程將停止。
- 即使在API找到匹配項後，使用者仍可以選擇重新檢測流量。
- reinspection引數是一個布林值，指明是否需要重新檢測在第一個資料包中找到的應用程式。
- 當重新檢查為true時，即使API找到匹配項，應用發現也會繼續。
- 在這種情況下，第一個資料包上分配的appid可能會發生變化。

必要條件、支援的平台、授權

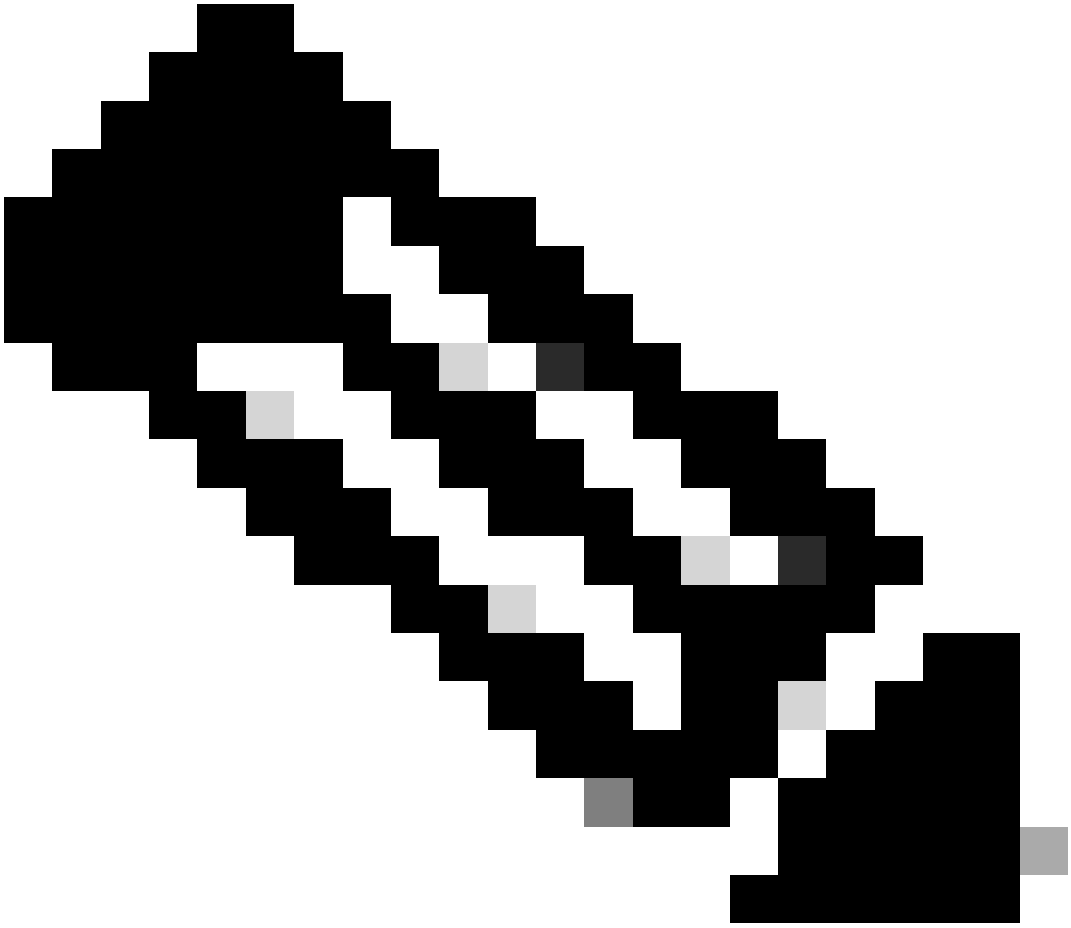
最低軟體和硬體平台

應用程式與最低版本	支援的託管平台和版本	管理員	備註
安全防火牆7.4 使用Snort3	所有支援FTD 7.4的平台	FMC內建+ FTD	這是裝置端功能；FTD必須在7.4上



警告： Snort 2不支援此API。

Snort 3、多例項和HA/群集支援



註：要求Snort 3成為檢測引擎。

FTD	
是否支援多例項？	是
支援高可用性裝置	是
群集裝置是否支援？	是

採用元件

本文中的資訊係根據以下軟體和硬體版本：
· 運行7.4或更高版本的Cisco Firepower威脅防禦。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

功能詳細資料

功能功能說明

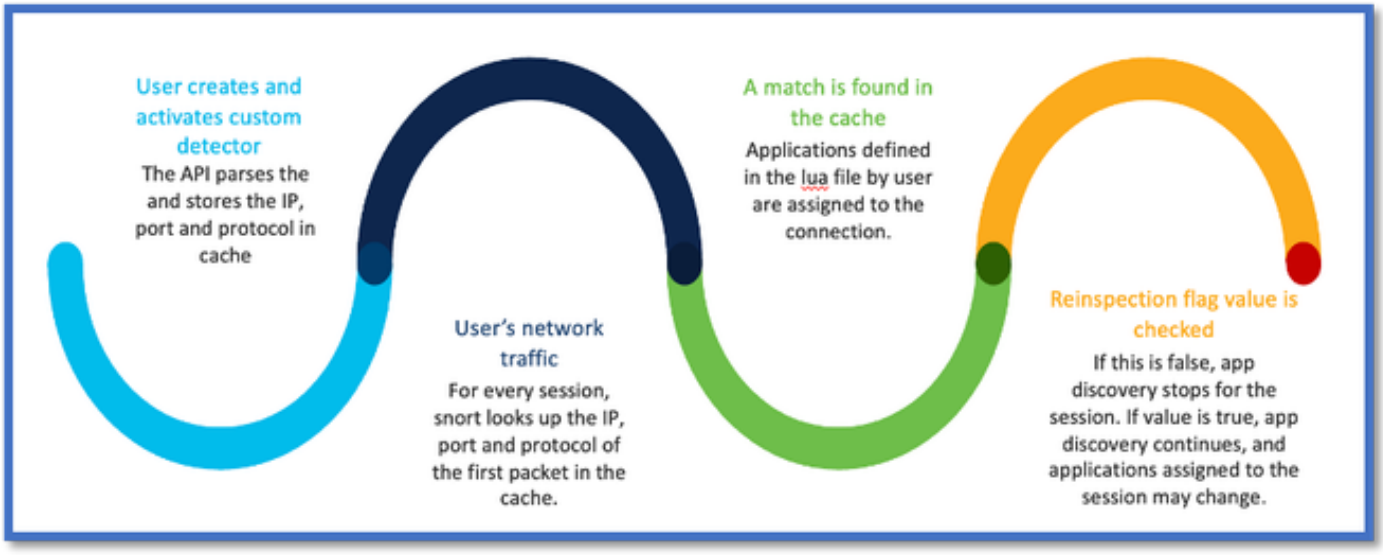
與此發行版本之前的版本比較

在安全防火牆7.3及更低版本中	安全防火牆7.4新功能
· 用於已知IP/埠/協定組合的應用檢測僅在用盡所有其他應用檢測機制後可用作後退選項。 · 基本上，不支援對會話中第一個資料包進行檢測。	· 新的LUA檢測器API在任何其它應用檢測機制之前進行評估， · 因此，在7.4中，我們支援檢測會話中的第一個資料包。

運作方式

- 建立lua檔案：確定檔案位於lua範本中（沒有語法錯誤）。此外，請確認檔案中指定給API的引數是否正確。
- 建立新的自定義檢測器：在FMC上建立新的自定義檢測器，並在其中上傳lua檔案。啟動探測器。
- 運行流量：將匹配自定義應用檢測器中定義的IP/埠/協定組合的流量傳送到裝置。
- 檢查連線事件：在FMC上，檢查按IP和埠過濾的連線事件。將辨識使用者定義的應用。

AppID早期資料包檢測API工作流



來自自定義檢測器的API欄位說明示例

gDetector:addHostFirstPktApp

(gAppIdProto、gAppIdClient、gAppId、0, "192.0.2.1", 443, DC.ipproto.tcp)；

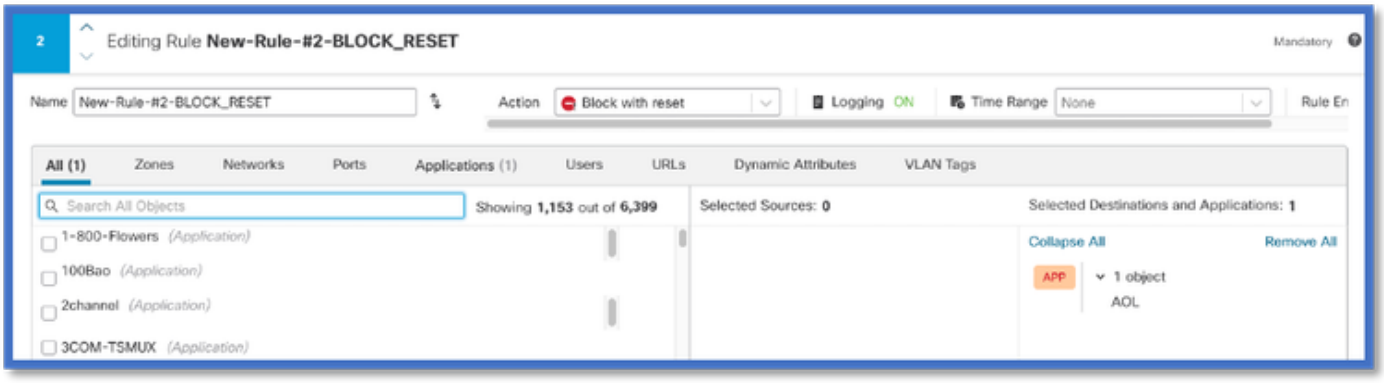
- 反白的引數是使用者定義的復原旗標、IP位址、連線埠和通訊協定值。
- 0表示萬用字元。

引數	說明	預期值
復原旗標	如果使用者偏好檢查流量，而不是根據IP/連線埠/通訊協定採取防火牆動作，則可以將重新檢查旗標值啟用為1。	0 =停用復原或 1 =已啟用復原
IP 位址	伺服器的目標IP（子網路中的單一或一組IP）。會話中第1個資料包的目標IP。	192.168.4.198或 192.168.4.198/24或 2a03:2880：f103:83：face：b00c：0:25de或 2a03:2880：f103:83：face：b00c：0:25de/32
連接埠	作業階段中第1個封包的目的地連線埠。	0到65535

通訊協定	網路協定	TCP/UDP/ICMP

使用案例：如何更快地阻止流量

- 策略檢視：應用程式「AOL」的阻止規則。



- 使用curl測試流量：curl https://www.example.com v/s curl https://192.0.2.1/（TEST的IP地址之一）

<#root>

> curl https://www.example.com/

curl: (35) OpenSSL SSL_connect: SSL_ERROR_SYSCALL in connection to www.example.com:443

> curl https://192.0.2.1/

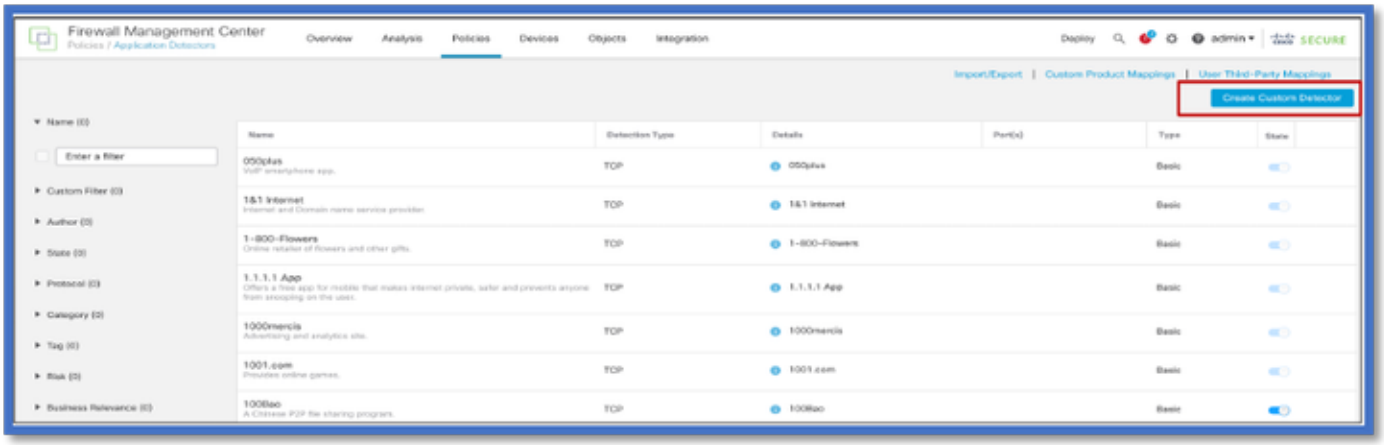
curl: (7) Failed to connect to 192.0.2.1 port 443: Connection refused

防火牆管理中心逐步解說

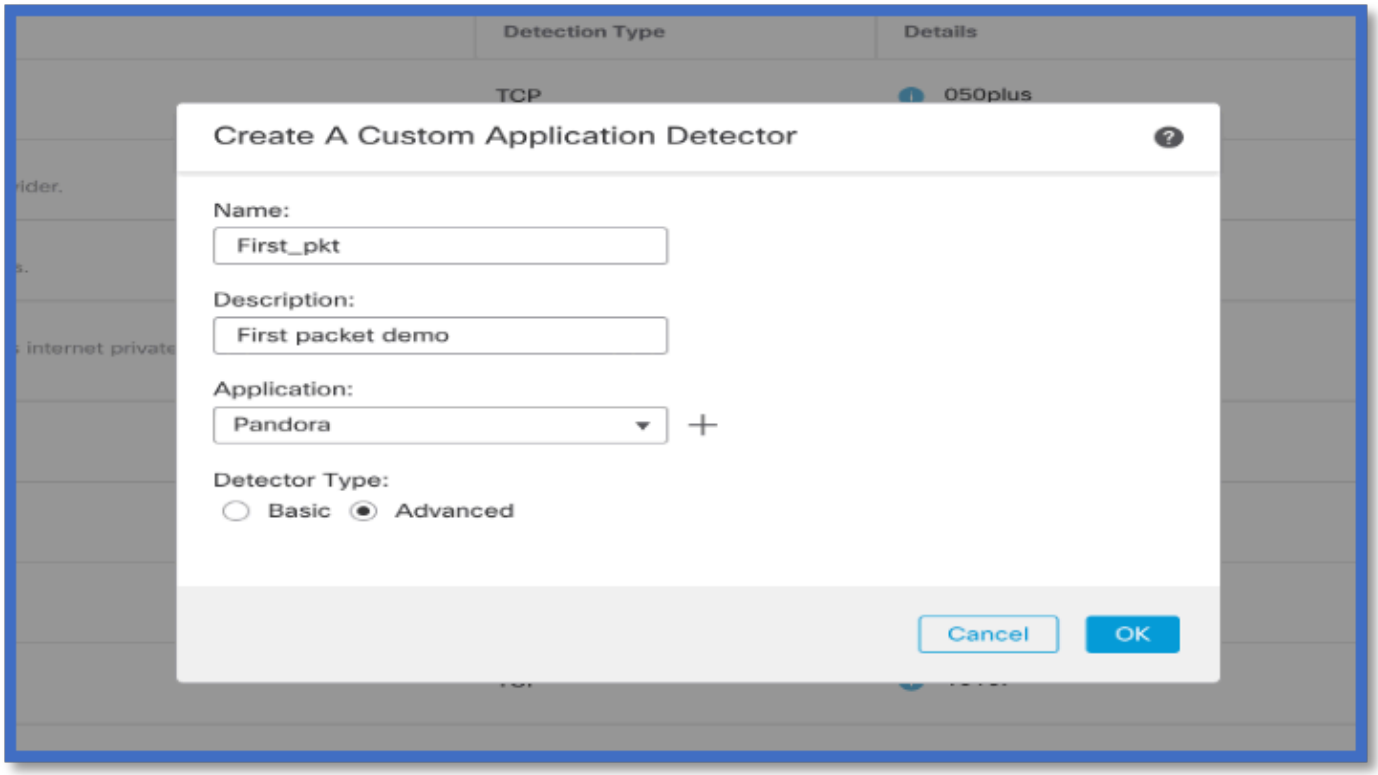
使用API建立自定義檢測器的步驟

從FMC建立新的自訂偵測器：

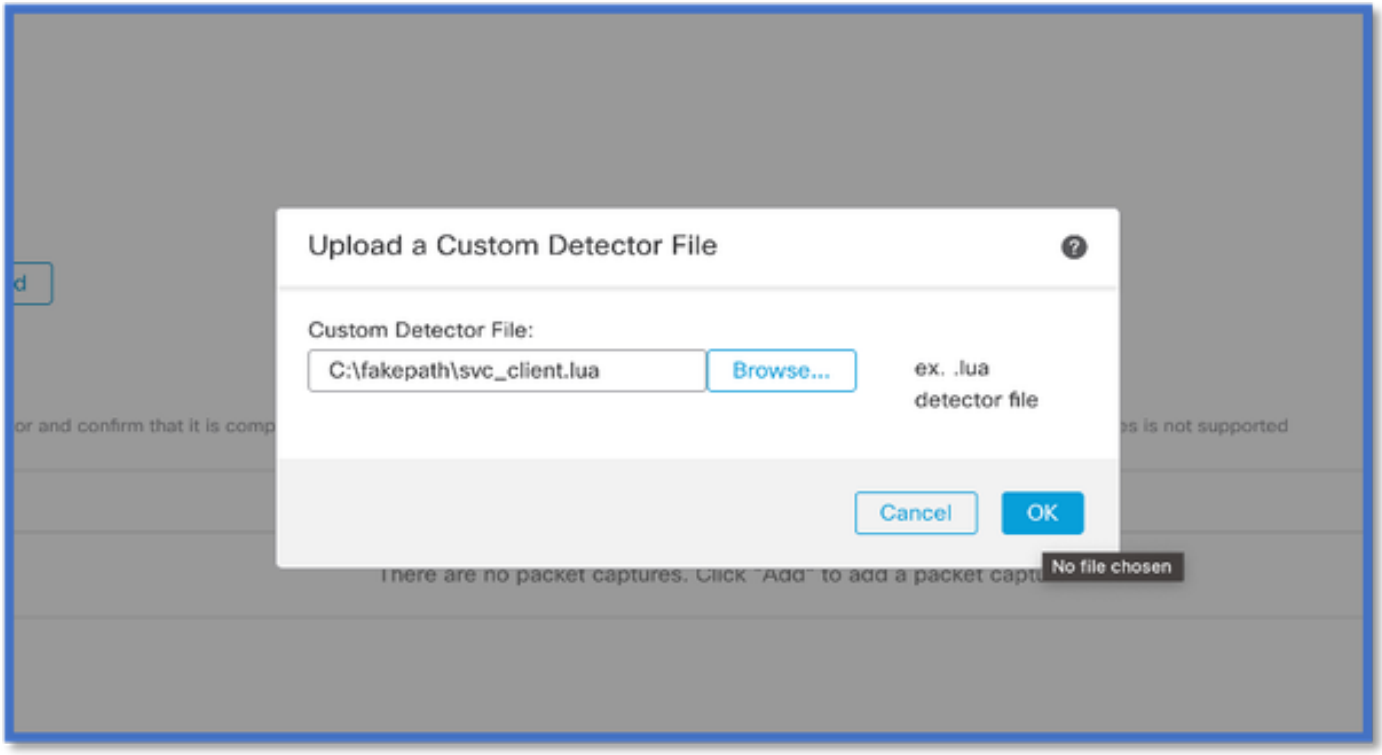
- Policies > Application Detectors > Create Custom Detector .



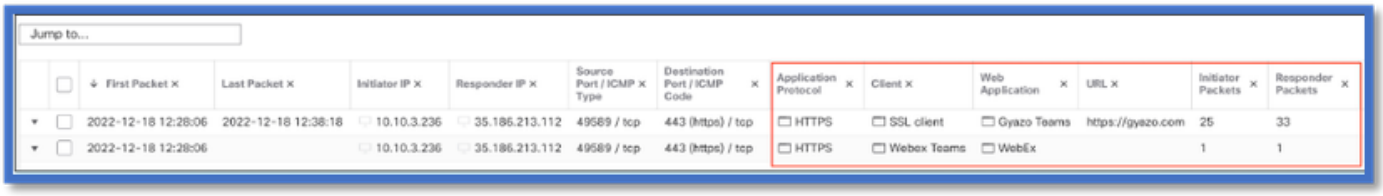
- 定義名稱和說明。
  - 從下拉式功能表中選擇應用程式。
  - 選擇Advanced Detector Type。



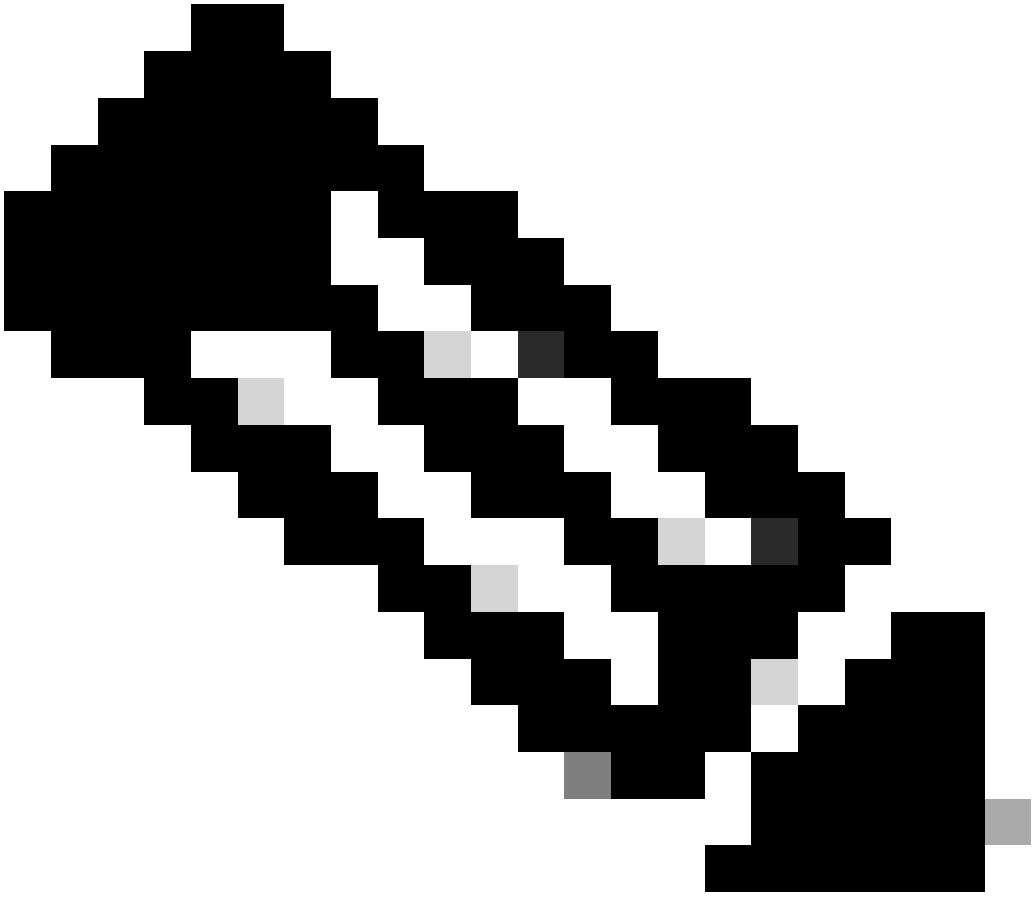
- 上傳「檢測標準」下的Lua檔案。儲存並啟用檢測器。



Respect已啟用v/s已停用



- 這兩個事件顯示連線的開始v/s和啟用重新檢查時的連線的結束。



附註：需注意的事項：

1. 在連線開始時，API會標識「HTTPS、Webex和Webex團隊」。由於重新檢查為真，應用發現繼續進行，並且appId更新為「HTTPS、SSL客戶端和Gyazo團隊」。

2. 注意發起方和響應方資料包的數量。常規應用檢測方法需要的資料包比API多得多。

疑難排解/診斷

診斷概要

- 系統支援應用程式標識調試中增加新日誌，以指示第1個資料包檢測API是否找到任何應用程式。
- 這些日誌還顯示使用者是否選擇重新檢查流量。
- 在FTD的/var/sf/appid/custom/lua/<UUID>下可以找到使用者上傳的lua檢測器檔案的內容。
- 在啟用檢測器時，lua檔案中的任何錯誤都會轉儲到/var/log/messages檔案中的FTD上。

CLI：系統支援應用程式標識-調試

<#root>

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 New AppId session

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first packet, service: HTTPS(1

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 app event with client changed, service changed, payload
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 New firewall session
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-Rule-#1-MONITOR', and Src
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-MONITOR', action Audit
```

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-BLOCK_RESET', action Re
```

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 MidRecovery data sent for rule id: 268437504, rule_acti
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Generating an SOF event with rule_id = 268437504 ruleAc
```

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 reset action
```

```
192.0.2.1 443 > 192.168.1.16 51251 6 AS-4 ID=0 New AppId session
192.0.2.1 443 > 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first
packet, service:
HTTPS (1122), client: AOL(1419), payload: AOL (1419), reinspect: False
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 app event with client changed,
service changed, payload changed, referred no change, miss no change, Mad no
change, fas host no change, bits 0x1D 192.168.1.16 51251 > 192.0.2.1 443 6 AS=4
ID=0 New firewall session
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-
Rule-#1-MONITOR', and Saclone first with zones 1 →> 1, geo 0(xff0) →> 0, yan 0,
sae, sgt; 0, sag sat, type: unknown, det sat: 0, det sat type: unknown, sve 1122,
payload 1419, client 1419, mise 0, user 9999997, no Mad or host, no xff
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-
MONITOR', action Audit
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-
BLOCK_
_RESET', action
Reset
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID=0 MidRecovery, data sent for rule id:
268437504, rule_action:5, rev id:3558448739, Eule_match flag:0x1
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID-0 Generating an SOF event with
zuleid - 268437504
ruleAction = 5 ruleReason = 0
```

AppID Lua檢測器內容的位置

要確認具有此新API的Lua檢測器是否存在於裝置/FTD上，您可以檢視addHostFirstPktApp API是否正用於2個應用檢測器資料夾：

1. VDB AppID檢測器-/var/sf/appid/odp/lua

2. 自定義檢測器-/var/sf/appid/custom/lua

例如：grep addHostFirstPktApp * 在每個資料夾中。

問題示例：

- 問題：未在FMC上啟用自定義Lua檢測器。

要檢查的位置： /var/sf/appid/custom/lua/

預期結果：在FMC上啟用的每個自訂應用程式偵測器都必須有一個檔案存在。驗證內容是否與上載的lua檔案匹配。

- 問題：上載的lua檢測器檔案有錯誤。

要檢查的檔案： /var/log/messages on FTD

錯誤記錄：

<#root>

Dec 18 14:17:49 intel-x86-64 SF-IMS[15741]:

Error - appid: can not set env of Lua detector /ngfw/var/sf/appid/custom/lua/6698fbd6-7ede-11ed-972c-d12

疑難排解步驟

問題：對於流向使用者定義IP地址和埠的流量，應用程式辨識不正確。

故障排除的步驟：

- 驗證是否已在FTD上正確定義並啟動lua檢測器。
  - 確認FTD上lua檔案的內容，並檢查啟動時是否看不到錯誤。
- 檢查流量會話中第一個資料包的目的IP、埠和協定。
  - 它可以與lua檢測器中定義的值匹配。
- 檢查system-support-application-identification-debug。
  - 查詢行Host cache match found on first packet. 如果缺少該行，則表示API未找到任何匹配。

限制詳細資訊、常見問題和解決方法

在7.4中，沒有UI可以使用API。未來版本中將增加UI支援。

修訂記錄

修訂	發佈日期	意見
1.0	2024年7月18日	初始版本

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）。