含Regex的ASA HTTP URL過濾器功能

目錄

簡介

本檔案介紹在搭載HTTP檢查引擎的調適型安全裝置(ASA)上設定URL過濾器。當HTTP請求的部分內容與使用regex模式清單匹配時，此操作會完成。您可以阻止特定URL或阻止所有URL（少數選擇除外）。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

本節提供用於設定本文件中所述功能的資訊。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

配置步驟

以下是一般組態步驟：

1. 確定應阻止或允許的域的簡短清單
2. 建立匹配所有相關域的regex類對映
3. 建立一個HTTP檢測策略對映，丟棄或允許與這些域匹配的流量
4. 將此HTTP檢測策略對映應用於模組化策略框架中的HTTP檢測

無論您是嘗試阻止某些域並允許所有其他域，還是阻止所有域並僅允許少數域，除建立HTTP檢測策略對映外，步驟都是相同的。

確定應阻止或允許的域的簡短清單

對於此配置示例，這些域被阻止或允許：

- cisco1.com
- cisco2.com
- cisco3.com

為這些域配置regex模式：

```
regex cisco1.com "cisco1.com"regex cisco2.com "cisco2.com"regex cisco3.com "cisco3.com"
```

建立匹配所有相關域的regex類對映

配置與regex模式匹配的regex類：

```
class-map type regex match-any domain-regex-classmatch regex cisco1.commatch regex
cisco2.commatch regex cisco3.com
```

建立一個HTTP檢測策略對映，丟棄或允許與這些域匹配的流量

若要瞭解此組態會是什麼樣子，請選擇最符合此URL過濾器目標的說明。上面構建的regex類將是應該允許的域清單或應該阻止的域清單。

- **允許除列出的域之外的所有域**此配置的關鍵在於建立類對映，其中匹配所列域的HTTP事務被分類為「blocked-domain-class」。 與此類匹配的HTTP事務被重置並關閉。實質上，僅重置與這些域匹配的HTTP事務。
  ```
  class-map type inspect http match-all blocked-domain-class match request header host regex
  class domain-regex-class!policy-map type inspect http regex-filtering-policy parameters
  class blocked-domain-class  reset log
  ```
- **阻止除所列域之外的所有域**此配置的關鍵在於使用關鍵字「match not」建立類對映。 這告訴防火牆，任何與域清單不匹配的域都應與標題為「allowed-domain-class」的類匹配。將重置並關閉與該類匹配的HTTP事務。實際上，除非所有HTTP事務與列出的域匹配，否則它們將被重置。
  ```
  class-map type inspect http match-all allowed-domain-class match not request header host
  ```

```
regex class domain-regex-class!policy-map type inspect http regex-filtering-policy
parameters class allowed-domain-class  reset log
```

將此HTTP檢測策略對映應用於模組化策略框架中的HTTP檢測

現在HTTP檢測策略對映配置為「regex過濾策略」，請將此策略對映應用於模組策略框架中存在的HTTP檢測或新檢測。例如，這會將檢查新增到「global_policy」中配置的「inspection_default」類。

```
policy-map global_policy class inspection_default  inspect http regex-filtering-policy
```

常見問題

當配置了HTTP檢測策略對映和HTTP類對映時，請確保未按照預期目標配置匹配或匹配。這是一個要跳過且會導致意外行為的簡單關鍵字。此外，這種形式的regex處理方式與任何高級資料包處理方式一樣，可能會導致ASA CPU使用率增加以及吞吐量下降。新增越來越多的正規表示式模式時請小心。