

瞭解Snort3規則

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[授權](#)

[採用元件](#)

[背景資訊](#)

[Snort3規則](#)

[規則操作](#)

[規則剖析](#)

[規則功能](#)

[範例](#)

[使用http服務標頭和粘滯緩衝區http_uri的示例](#)

[檔案服務標頭的示例](#)

[相關連結](#)

簡介

本檔案介紹思科引擎 Snort3 的規則Secure Firewall Threat Defense (FTD)則。

必要條件

需求

思科建議您瞭解以下主題：

- **CISCO Secure Firewall Threat Defense (FTD)**
- **Intrusion Prevention System (IPS)**
- **Snort2 語法**

授權

沒有特定授權要求，基本授權就足夠了，且提到的功能包含在FTD內的Snort引擎和Snort3開源版本中。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- **CISCO Secure Firewall Threat Defense (FTD)**，思科Secure Firewall Management Center (FMC)版本7.0+，Snort3帶

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。

背景資訊

Snort 思科IPS引擎能夠進行即時流量分析和資料包記錄。

Snort 可以執行協定分析、內容搜尋和檢測攻擊。

Snort3 是Snort2 IPS的更新版本，採用新的軟體架構，可提高效能、檢測、可擴充性和可用性。

Snort3規則

它們使用該LUA格式使規則 Snort3更易於讀取、寫入和驗證。

規則操作

此新版本更改規則操作，新定義如下：

- **Pass**:停止對資料包的後續規則評估
- **Alert**:僅生成事件
- **Block**:丟棄資料包，阻止剩餘會話
- **Drop**:僅丟棄資料包
- **Rewrite**:如果使用**replaces**選項，則此為必需欄位
- **React**:傳送HTML塊響應頁
- **Reject**:插入TCP RST或ICMP無法訪問

規則剖析

其結構如下：



規則報頭包含操作、協定、源和目標網路以及埠。

在中 Snort3中，規則報頭可以是以下選項之一：

- 服務規則標頭

```
<inline" lang="lua">alert http
(
msg:"Alert HTTP rule";
flow:to_client,established;
content:"evil", nocase;
sid:1000001;
)
```

- 檔案規則標題

```
alert file
(
msg: "Alert File example";
file_data;
content:"malicious_stuff";
sid:1000006;
)
```

- 常規規則報頭

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(
msg:"Alert HTTP rule";
flow:to_client,established;
content:"evil", nocase;
sid:1000001;
)
```

規則功能

部分新功能包括：

- 任意空格 (每個選項位於自己的行上)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(
msg:"Alert TCP rule";
flow:to_client,established;
content:"evil", nocase;
sid:1000000;
)
```

- 使用和的一致；

```
content:"evil", offset 5, depth 4, nocase;
```

- 網路和埠是可選的

```
alert http ( Rule body )
```

- 新增更多粘滯緩衝區 (這不是完整清單)

```
http_uri  
http_raw_uri  
http_header  
http_raw_header  
http_trailer  
http_raw_trailer  
http_cookie  
http_raw_cookie  
http_true_ip  
http_client_body  
http_raw_body  
http_method  
http_stat_code  
http_stat_msg  
http_version  
http2_frama_header  
script_data  
raw_data
```

- C樣式註釋

```
alert http  
(  
msg:"Alert HTTP rule"; /* I can write a comment here */  
...  
)
```

- Remark(rem)關鍵字

```
alert http  
(  
msg:"Alert HTTP rule";  
flow:to_client,established;  
rem:"Put comments in the rule anywhere";  
content:"evil", nocase;  
sid:1000001;  
)
```

- appids關鍵字

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any
(
msg:"Alert on apps";
appids:"Google, Google Drive";
content:"evil", nocase;
sid:1000000;
)
```

- 用於敏感資料過濾的sd_pattern
- Regex關鍵字與hyperflex技術的使用
- Service關鍵字替換後設資料

範例

使用http服務標頭和粘滯緩衝區http_uri的示例

工作:編寫檢測HTTP URI中 `malicious`該詞的規則。

解決方案：

```
alert http
(
msg:"Snort 3 http_uri sticky buffer";
flow:to_server,established;
http_uri;
content:"malicious", within 20;
sid:1000010;
)
```

檔案服務標頭的示例

工作:編寫檢測PDF檔案的規則。

解決方案：

```
alert file
(
msg:"PDF File Detected";
file_type: "PDF";
sid:1000008;
)
```

相關連結

[Snort規則和IDS軟體下載](#)

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）。