了解Snort3规则

目录

简介

本文档介绍适用于 **Snort3** 思科引擎 **Secure Firewall Threat Defense (FTD).**

先决条件

要求

Cisco 建议您了解以下主题：

- 思科 **Secure Firewall Threat Defense (FTD)**
- **Intrusion Prevention System (IPS)**
- **Snort2** 语法

许可

无特定许可证要求，基本许可证已足够，并且提到的功能包含在FTD内的**Snort引擎**和**Snort3开源版本**中。

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Snort 是能够进行实时流量分析和数据包记录的Cisco IPS引擎。

Snort 可以执行协议分析、内容搜索和检测攻击。

Snort3 是Snort2 IPS的更新版本，采用可提高性能、检测、可扩展性和可用性的新软件架构。

Snort3规则

它们使用该LUA格式来将 **Snort3** 规则更易于读取、写入和验证。

规则操作

此新版本更改规则操作，新定义如下：

- **Pass**：停止对数据包的后续规则评估
- **Alert**：仅生成事件
- **Block**：丢弃数据包，阻止剩余会话
- **Drop**：仅丢弃数据包
- **Rewrite**：如果使用replaces选项，则为必需
- **React**：发送HTML块响应页面
- **Reject**：插入TCP RST或ICMP不可达

规则剖析

剖析如下：

规则报头包含操作、协议、源和目标网络以及端口。

在 **Snort3**规则报头可以是以下选项之一：

- 服务规则报头

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

- 文件规则报头

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

- 常规规则报头

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

规则功能

其中一些新功能包括：

- 任意空格（每个选项位于自己的行上）

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

- 始终如一地用和；

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

- 网络和端口是可选的

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

- 添加更多粘滞缓冲区（这不是完整列表）

```
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样式注释

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

- Remark(rem)关键字

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

- appids关键字

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

- sd_pattern用于敏感数据过滤
- Regex关键字与Hyperflex技术的用法
- Service关键字替换元数据

Examples

http服务报头和粘滞缓冲区http_uri的示例

任务：编写检测该词的规则 **malicious** 在HTTP URI中。

解决方案：

```
alert http ( msg:"Snort 3 http_uri sticky buffer"; flow:to_server,established; http_uri;
```

```
content:"malicious", within 20; sid:1000010; )
```

文件服务标题示例

任务：编写检测PDF文件的规则。

解决方案：

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

相关链接

Snort规则和IDS软件下载

Github

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。