ASA HTTP URL过滤器功能（带Regex）

目录

简介

本文档介绍在具有HTTP检测引擎的自适应安全设备(ASA)上配置URL过滤器。当部分HTTP请求与正则表达式模式列表的使用匹配时，此操作即完成。您可以阻止特定URL或阻止除少数URL外的所有URL。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置步骤

以下是一般配置步骤：

1. 确定应阻止或允许的域的简短列表
2. 创建匹配所有相关域的正则表达式类映射
3. 构建丢弃或允许与这些域匹配的流量的HTTP检测策略映射
4. 将此HTTP检测策略映射应用于模块化策略框架中的HTTP检测

无论您是尝试阻止某些域并允许所有其他域，还是阻止所有域并仅允许少数域，除了创建HTTP检测策略映射外，这些步骤都是相同的。

确定应阻止或允许的域的简短列表

对于此配置示例，这些域被阻止或允许：

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

配置这些域的正则表达式模式：

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

创建匹配所有相关域的正则表达式类映射

配置与regex模式匹配的regex类：

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

构建丢弃或允许与这些域匹配的流量的HTTP检测策略映射

要了解此配置的外观，请选择最符合此URL过滤器目标的描述。上面构建的正则表达式类可以是应允许的域列表或应阻止的域列表。

- **允许除列出的域外的所有域**此配置的关键是创建类映射，其中匹配所列域的HTTP事务被分类为“blocked-domain-class”。 匹配此类的HTTP事务将重置并关闭。实际上，仅重置与这些域匹配的HTTP事务。
  ```
  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
  ```
- **阻止除所列域外的所有域**此配置的关键是使用关键字“match not”创建类映射。 这告诉防火墙，任何与域列表不匹配的域都应与标题为“允许域类”的类匹配。匹配该类的HTTP事务将重置并关闭。实际上，除非所有HTTP事务与列出的域匹配，否则将重置这些事务。
  ```
  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
```

将此HTTP检测策略映射应用于模块化策略框架中的HTTP检测

现在，HTTP检测策略映射已配置为“regex-filtering-policy”，请将此策略映射应用于模块化策略框架中存在的HTTP检测或新检测。例如，这会将检测添加到在“global_policy”中配置的“inspection_default”类。

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

常见问题

配置HTTP检测策略映射和HTTP类映射后，请确保匹配或不匹配的配置与预期目标相符。这是一个简单的关键字，可跳过并导致意外行为。此外，与任何高级数据包处理一样，这种形式的正则表达式处理可能会导致ASA CPU利用率增加以及吞吐量下降。添加越来越多的正则表达式模式时，请小心。