确定 NBAR 不能识别的数据流

目录

简介

本文档说明如何使用 Network-Based Application Recognition (NBAR) 的自定义数据包描述语言模块 (PDLM) 功能，以在未分类的流量上或未作为 match protocol 语句而特别受到支持的流量上进行匹配。

先决条件

要求

本文档的读者应掌握以下这些主题的相关知识：

- 基本 QoS 方法
- 基本了解 NBAR

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS® 软件版本 12.2(2)T
- Cisco 7206 路由器

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。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

了解自定义 PDLM

NBAR 支持各种静态和状态协议。通过 PDLM，可为 NBAR 提供新协议支持，而无需 IOS 版本升级和路由器重新加载。后续 IOS 版本包含这些新协议支持。

通过自定义 PDLM，您可使用一个 match protocol 语句，将协议映射到 NBAR 中目前不支持的协议的静态 User Datagram Protocol (UDP) 和 TCP 端口。换句话说，自定义 PDLM 会扩展或增强由 NBAR 识别的协议的列表。

下面是向路由器添加自定义 PDLM 的步骤。

1. 通过下载 **custom.pdlm 文件，从**软件下载页（仅限注册用户）找到并下载 NBAR PDLM。
2. 使用下面的命令，将 PDLM 加载到闪存设备（如插槽 0 或 1 中的 PCMCIA 卡）。
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. 使用 **show ip nbar port-map | include custom**命令（如下所示）或**show ip nbar pdlm命**令。
   ```
   7206-16# show ip nbar port-map | include custom
   port-map custom-01            udp 0
   port-map custom-01            tcp 0
   port-map custom-02            udp 0
   port-map custom-02            tcp 0
   port-map custom-03            udp 0
   port-map custom-03            tcp 0
   port-map custom-04            udp 0
   port-map custom-04            tcp 0
   port-map custom-05            udp 0
   port-map custom-05            tcp 0
   port-map custom-06            udp 0
   port-map custom-06            tcp 0
   port-map custom-07            udp 0
   port-map custom-07            tcp 0
   port-map custom-08            udp 0
   port-map custom-08            tcp 0
   port-map custom-09            udp 0
   port-map custom-09            tcp 0
   port-map custom-10            udp 0
   port-map custom-10            tcp 0
   ```
4. 使用ip nbar port-map custom-XY {tcp|udp} {port1 port2 ...}命**令将端口分配给自定义协**议。例如，若要在 TCP 端口 8877 的流量上进行匹配，请使用 **ip nbar port-map custom-01 tcp 8877 命令。**

“未分类”端口分类

根据具体网络流量，您可能需要在 NBAR 中使用特殊分类机制。对此流量分类后，您就可以使用自定义 PDLM，将 UDP 和 TCP 端口号匹配到自定义端口映射。

默认情况下，没有启用 NBAR 未分类机制。**show ip nbar unclassified-port-stats 命令返回以下错误消息：**

```
d11-5-7206-16# show ip nbar unclassified-port-stats
Port Statistics for unclassified packets is not turned on.
```

在严格控制情况下，可使用 **debug ip nbar unclassified-port-stats 命令配置路由器，使其在数据包到达的端口上开始跟踪。**然后，使用 **show ip nbar unclassified-port-stats 命令验证收集的信息。**输

出此时会显示最常用端口的柱状图。

注意：在发出debug命令之前，请参阅有关Debug命令的重要信息。**debug ip nbar 命令只能在严格控制情况下启用。**

如果这些信息不充分，您可以启用捕获功能，此功能可以方便地捕获新协议的数据包踪迹。请使用下面所示的 **debug 命令。**

```
debug ip nbar filter destination_port tcp XXXX
debug ip nbar capture 200 10 10 10
```

第一个命令定义要在其中进行捕获的数据包。第二个命令将 NBAR 置于捕获模式。**capture 命令的参数如下：**

- 每个数据包要捕获的字节数。
- 要捕获的起始数据包数，换句话说，就是要在 TCP/IP SYN 数据包之后捕获的数据包数。
- 要捕获的结束数据包数，换句话说，就是应为其保留空间的流结束处的数据包数。
- 要捕获的数据包总数。

注意：指定起始和最终数据包参数仅捕获长流中的相关数据包。

使用 **show ip nbar capture 命令可查看收集的信息。**默认情况下，捕获模式会等待 SYN 数据包到达，然后在该双向数据流上开始捕获数据包。

用自定义 PDLM 阻塞 Gnutella

请看一个示例，了解如何使用自定义 PDLM。我们使用 Gnutella 作为要分类的流量，然后应用一个阻止此流量 QoS 策略。

Gnutella 使用六个我们熟知的 TCP 端口 - 6346、6347、6348、6349、6355 和 5634。接收到 Pong 时，可能会检测到其他端口。如果用户指定在 Gnutella 文件共享中使用其他端口，则可以将这些端口添加到自定义 match protocol 语句中。

下面是创建在 Gnutella 流量上进行匹配并丢弃的 QoS 服务策略的步骤。

1. 如上所述，使用 **show ip nbar unclassified-port-stats 命令可查看 NBAR“未分类”流量。**如果您的网络正在传输 Gnutella 流量，则会看到与下面类似的输出。
   ```
   Port     Proto    # of Packets
   ------- -------- -------
   6346     tcp      347679
   27005    udp      55043
   ```
2. 使用 **ip nbar port-map custom 命令可自定义一个在 Gnutella 端口上匹配的端口映射。**

   ```
   ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355
   ```
   注意：目前，您必须使用诸如custom-xx之类的名称。Cisco IOS 软件的将来版本将支持自定义 PDLM 的用户定义名称。
3. 使用 **show ip nbar protocol stats 命令可确认与自定义语句的匹配。**
   ```
   2620# show ip nbar protocol stats byte-count
   FastEthernet0/0
                  Input                Output
   Protocol       Byte Count           Byte Count
   -----------------------------------------------
   ```

```
custom-02      43880517            52101266
```

4. 使用模块化 QoS CLI (MQC) 创建 QoS 服务策略。

```
d11-5-7206-16(config)# class-map gnutella
d11-5-7206-16(config-cmap)# match protocol custom-02
d11-5-7206-16(config-cmap)# exit
d11-5-7206-16(config)# policy-map sample
d11-5-7206-16(config-pmap)# class gnutella
d11-5-7206-16(config-pmap-c)# police 1000000 31250 31250 conform-action
            drop exceed-action drop violate-action drop
```

有关用于阻止 Gnutella 以及其他不需要的流量的其他配置命令，请参阅使用 Network-Based Application Recognition 和访问控制列表拦截“红色代码”蠕虫。

相关信息

- QoS 支持资源
- 技术支持 - Cisco Systems