確定NBAR無法識別的流量

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[瞭解自定義PDLM](#)
[分類「未分類」埠](#)
[使用自定義PDLM阻止Gnutella](#)
[相關資訊](#)

簡介

本文說明如何使用網路型應用程式辨識(NBAR)的自訂封包說明語言模組(PDLM)功能，對非分類流量或非明確支援為match通訊協定語句的流量進行比對。

必要條件

需求

本文檔的讀者應瞭解以下主題：

- 基本QoS方法
- 對NBAR的基本理解

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體版本12.2(2)T
- 思科7206路由器

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

瞭解自定義PDLM

NBAR支援各種靜態和狀態協定。PDLM允許對NBAR提供新的通訊協定支援，且無需IOS版本升級和路由器重新載入。後續的IOS版本包含對這些新協定的支援。

自定義PDLM允許使用match protocol語句將協定對映到NBAR中當前不支援的協定的靜態使用者資料包協定(UDP)和TCP埠。換句話說，它擴展或增強了NBAR識別的協定清單。

以下是將自訂PDLM新增至路由器的步驟。

1. 通過下載**custom.pdlm**檔案，從Software Download頁面(僅限註冊客戶)找到並下載NBAR PDLM。
2. 使用下面的命令將PDLM載入到快閃記憶體裝置，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**驗證對自定義協定的支援 **| 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 ...}命令將埠分配給自定義協**議。例如，要匹配TCP埠8877上的流量，請使用**ip nbar port-map custom-01 tcp 887**命令。

分類「未分類」埠

根據網路流量，您可能需要在NBAR中使用特殊分類機制。對此流量進行分類後，您可以使用自定義PDLM並將UDP和TCP埠號與自定義埠對映進行匹配。

預設情況下，未啟用NBAR未分類機制。**show ip nbar unclassified-port-stats**命令返回以下錯誤消息：

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

在嚴格控制的情況下，使用**debug ip nbar unclassified-port-stats**命令將路由器配置為開始跟蹤資料包到達的埠。然後使用**show ip nbar unclassified-port-stats**命令驗證收集的資訊。現在，輸出會顯示最常用埠的直方圖。

注意：發出**debug命令之前，請參閱**有關Debug命令的重要資訊**。**只有在精心控制的情況下才應啟

用**debug ip nbar**命令。

如果此資訊不夠，您可以啟用捕獲功能，該功能提供了捕獲新協定資料包跟蹤的簡便方法。使用以下**debug**命令，如下所示。

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

第一個命令定義您希望捕獲的資料包。第二個命令將NBAR置於捕獲模式。**capture**命令的引數如下：

- 每個資料包要捕獲的位元組數。
- 要捕獲的起始資料包數，換句話說，在TCP/IP SYN資料包之後要捕獲的資料包數。
- 要捕獲的最終資料包數，換句話說，在流末尾要為其保留空間的資料包數。
- 要捕獲的資料包總數。

注意：指定起始和最終資料包引數只能捕獲長流中的相關資料包。

使用**show ip nbar capture**命令檢視收集的資訊。預設情況下，捕獲模式等待SYN資料包到達，然後開始捕獲該雙向流上的資料包。

使用自定義PDLM阻止Gnutella

讓我們看一下如何使用自定義PDLM的示例。我們使用Gnutella作為要分類的流量，然後應用阻止此流量的QoS策略。

Gnutella使用6個公認的TCP埠 — 6346、6347、6348、6349、6355和5634。當收到Pong時，可能會檢測到其他埠。如果使用者指定其他埠用於Gnutella檔案共用，則可以將這些埠新增到自定義匹配協定語句中。

以下是建立匹配和丟棄Gnutella流量的QoS服務策略的步驟。

1. 如上所述，使用**show ip nbar unclassified-port-stats**命令檢視NBAR「未分類」流量。如果您的網路正在傳輸Gnutella流量，您會看到類似以下的輸出。
   ```
   Port    Proto    # of Packets
   ------- -------- -------
   6346    tcp      347679
   27005   udp      55043
   ```
2. 使用**ip nbar port-map custom**命令定義與Gnutella埠匹配的自定義埠對映。

   ```
   ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355
   ```
   注意：目前，必須使用如custom-xx這樣的名稱。即將發佈的Cisco IOS軟體版本將支援自定義PDLM的使用者定義名稱。
3. 使用**show ip nbar protocol stats**命令確認與自定義語句的匹配。
   ```
   2620# show ip nbar protocol stats byte-count
   FastEthernet0/0
                  Input                Output
   Protocol       Byte Count           Byte Count
   -----------------------------------------------
   custom-02      43880517             52101266
   ```
4. 使用模組化QoS CLI(MQC)命令建立QoS服務策略。
   ```
   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
```

請參閱使用基於網路的應用識別和訪問控制清單阻止「紅色代碼」蠕蟲，瞭解用於阻止Gnutella和其他不需要的流量的其他配置命令。

相關資訊

- QoS支援資源
- 技術支援 - Cisco Systems