NBAR が認識しないトラフィックの判別

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[カスタムPDLM について](#)
[「Unclassified」ポートの分類](#)
[カスタム PDLM で Gnutella をブロックする方法](#)
[関連情報](#)

概要

このドキュメントでは、Network-Based Application Recognition(NBAR)のCustom Packet Description Language Module(PDLM)機能を使用して、未分類トラフィックまたはmatch protocol文として特にサポートされていないトラフィックを照合する方法について説明します。

前提条件

要件

このドキュメントの読者は次のトピックについての専門知識を有している必要があります。

- 基本的な QoS の方法論
- NBAR に関する基本知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS® ソフトウェア リリース 12.2(2)T
- Cisco 7206 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

カスタムPDLM について

NBAR では、スタティックおよびステートフルのさまざまなプロトコルをサポートしています。PDLM により、IOS のリリースのアップグレードやルータのリロードを行わずに、新しいプロトコルで NBAR をサポートできるようになります。これに続く IOS リリースには、これらの新しいプロトコルのサポートが組み込まれています。

カスタム PDLM を使用すると、現在は NBAR において match protocol 文でサポートされていないプロトコルに対して、スタティックな User Datagram Protocol（UDP）ポートや TCP ポートを割り当てることができます。つまり、NBAR によって認識されるプロトコルのリストが拡張されることになります。

ルータにカスタム PDLM を追加する手順は次のとおりです。

1. ソフトウェアのダウンロード ページ（登録ユーザ専用）から NBAR PDLM の検索とダウンロードを行います。つまり、**custom.pdlm ファイルをダウンロードします。**
2. 次のコマンドを使用して、PDLM をフラッシュ メモリ デバイス（スロット 0 または 1 の PCMCIA カードなど）に読み込みます。
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. カスタム プロトコルのサポートを確認します。これには、**show ip nbar port-map | include custom**コマンド（以下を参照）または**show ip nbar pdlmコマンド**です。
   ```
   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. **ip nbar port-map custom-XY {tcp|udp} {port1 port2 ...}コマンドを使用して、ポートをカスタムプロトコルに割り当てます。**たとえば、TCP ポート 8877 でトラフィックを照合するには、**ip nbar port-map custom-01 tcp 8877 コマンドを使用します。**

「Unclassified」ポートの分類

ネットワーク トラフィックによっては、NBAR で特別な分類メカニズムを使用する必要があります。このトラフィックを分類すると、カスタム PDLM を使用して、UDP および TCP ポートの番号をカスタム ポートマップと照合できます。

デフォルトでは、NBAR の unclassified のメカニズムは有効になっていません。**show ip nbar**

unclassified-port-stats コマンドからは、次のエラー メッセージが返されます。

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

慎重に管理された環境で、**debug ip nbar unclassified-port-stats コマンドを使用して、どのポートにパケットが着信するかについてのトラッキングをルータが開始するよう設定します。**次に **show ip nbar unclassified-port-stats コマンドを使用して、収集された情報を確認します。**この出力には、最も一般的に使用されるポートのヒストグラムが表示されます。

注：debugコマンドを発行する前に、『debugコマンドの重要な情報』を参照してください。**debug ip nbar コマンドは、慎重に制御されている環境でだけイネーブルにするようにしてください。**

この情報が十分でない場合は、キャプチャ機能を有効にできます。これは、新しいプロトコルのパケットのトレースをキャプチャする簡単な方法です。次の **debug コマンドを下記のように使用します。**

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

最初のコマンドでは、キャプチャの対象とするパケットを定義します。2 番目のコマンドでは、NBAR をキャプチャ モードにします。**capture コマンドの引数は次のとおりです。**

- パケットごとのキャプチャするバイト数。
- キャプチャする最初のパケット数。つまり、TCP/IP SYN パケットの後でキャプチャするパケットの数。
- キャプチャする最後のパケット数。つまり、スペースを予約しておく必要がある、フローの最後の部分のパケット数。
- キャプチャする総パケット数。

注：開始および最終パケットパラメータを指定すると、関連するパケットだけが長いフローでキャプチャされます。

収集した情報を表示するには **show ip nbar capture コマンドを使用します。**デフォルトでは、キャプチャ モードは SYN パケットが到着するのを待機し、次に双方向のフローでパケットのキャプチャを開始します。

カスタム PDLM で Gnutella をブロックする方法

カスタム PDLM の使用方法の例を見てみましょう。分類するトラフィックとして Gnutella を使用し、次にこのトラフィックをブロックする QoS ポリシーを適用します。

Gnutella では、よく知られている 6 個の TCP ポート（6346、6347、6348、6349、6355、5634）を使用します。他のポートは ping の受信で検出されます。ユーザが他のポートを Gnutella ファイル共有で使用するよう指定した場合は、カスタム化した match protocol 文にこれらのポートを追加できます。

Gnutella トラフィックを照合して、ドロップする QoS サービス ポリシーの作成手順は次のとおりです。

1. 上記のように、**show ip nbar unclassified-port-stats コマンドを使用して、NBAR の「unclassified」トラフィックを表示します。**ネットワークで Gnutella トラフィックを伝送している場合は、次のような出力が表示されます。

```
Port     Proto     # of Packets
-------  --------  -------
6346     tcp       347679
27005    udp       55043
```

2. **ip nbar port-map custom コマンドを使用して、Gnutella ポートと対応するカスタム ポート マップを定義します。**

```
ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355
```

注：現在は、custom-xxなどの名前を使用する必要があります。カスタム PDLM の名前のユーザ定義は、Cisco IOS ソフトウェアの今後のリリースでサポートされる予定です。

3. **show ip nbar protocol stats コマンドを使用して、カスタム文に一致することを確認します。**

```
2620# show ip nbar protocol stats byte-count
FastEthernet0/0
                Input                Output
Protocol        Byte Count           Byte Count
-------------------------------------------------
custom-02       43880517             52101266
```

4. モジュラ QoS CLI (MQC) のコマンドを使用して、QoS サービス ポリシーを作成します。

```
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
```

Gnutella および他の不要なトラフィックをブロックするための他のコンフィギュレーション コマンドについては、『ネットワークの入口で「Code Red」ワームをブロックするための Network-Based Application Recognition およびアクセス コントロール リストの使用方法』を参照してください。

関連情報

- QoS に関するサポート リソース
- テクニカルサポート - Cisco Systems