Determining the Traffic Not Recognized by NBAR

Contents

Introduction

Este documento mostra como usar o recurso PDLM (Módulo de Idiomas para Descrição de Pacotes) do NBAR (Reconhecimento de Aplicativo Baseado em Rede) para fazer a correspondência em tráfego não classificado ou sem suporte específico como uma declaração de protocolo de correspondência.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

- Metodologias básicas de QoS
- Compreensão básica do NBAR

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco IOS® versão 12.2(2)T
- Cisco 7206 Router

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Entendendo o PDLM personalizado

O NBAR suporta uma variedade de protocolos estáticos e stateful. Os PDLMs permitem o suporte a novos protocolos para o NBAR, sem o requisito de uma atualização de versão do IOS e recarga do roteador. Versões subseqüentes do IOS incorporam suporte para esses novos protocolos.

O PDLM Personalizado permite mapear protocolos para o User Datagram Protocol (UDP) estático e portas TCP para protocolos que não são atualmente suportados em NBAR com uma instrução de protocolo correspondente. Em outras palavras, ele estende ou aprimora a lista de protocolos reconhecidos pelo NBAR.

Aqui estão as etapas para adicionar o PDLM personalizado ao roteador.

1. Localize e baixe o NBAR PDLM na página Download de software (somente clientes registrados) fazendo o download do **arquivo custom.pdlm**.
2. Carregue o PDLM em um dispositivo de memória flash, como placa PCMCIA nos slots 0 ou 1, usando o comando abaixo.
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. Verifique o suporte para protocolos personalizados usando o **show ip nbar port-map | inclua o** comando **personalizado** (mostrado abaixo) ou o comando **show ip nbar pdlm**.
   ```
   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. Atribua portas aos protocolos personalizados usando o comando **ip nbar port-map custom-XY {tcp|udp} {port1 port2 ...}**. Por exemplo, para corresponder no tráfego na porta TCP 8877, use o comando **ip nbar port-map custom-01 tcp 8877**.

Classificando portas "não classificadas"

Dependendo do tráfego de rede, talvez seja necessário usar mecanismos de classificação especiais no NBAR. Assim que você classificar esse tráfego, poderá usar o PDLM personalizado e comparar os números de porta UDP e TCP com um mapa de portas personalizado.

Por padrão, os mecanismos não classificados do NBAR não estão ativados. O comando show ip nbar unclassified-port-stats retorna a seguinte mensagem de erro:

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

Sob circunstâncias cuidadosamente controladas, utilize o comando debug ip nbar unclassified-port-stats para configurar o roteador para iniciar o rastreamento nas portas nas quais os pacotes devem chegar. Em seguida, use o comando **show ip nbar unsegmentado-port-stats** para verificar as informações coletadas. A saída agora exibe um histograma das portas usadas com mais freqüência.

Observação: antes de inserir o comando **debug**, consulte Informações importantes sobre os comandos debug. Os comandos debug ip nbar apenas devem ser habilitados em circunstâncias cuidadosamente controladas.

Se essas informações não forem suficientes, você poderá ativar o recurso de captura, que fornece uma maneira fácil de capturar rastreamentos de pacotes de novos protocolos. Use os seguintes comandos de depuração, conforme mostrado abaixo.

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

O primeiro comando define os pacotes nos quais você está interessado na captura. O segundo comando coloca o NBAR no modo de captura. Os argumentos do comando capture são os seguintes:

- Número de bytes a capturar por pacote.
- Número de pacotes iniciais para capturar, em outras palavras, quantos pacotes capturar após o pacote SYN TCP/IP.
- Número de pacotes finais para capturar, em outras palavras, quantos pacotes no final do fluxo para o qual o espaço deve ser reservado.
- Número total de pacotes a capturar.

Observação: a especificação dos parâmetros de pacote inicial e final captura somente os pacotes relevantes em um fluxo longo.

Use o comando **show ip nbar capture** para exibir as informações coletadas. Por padrão, o modo de captura espera que um pacote SYN chegue e começa a capturar os pacotes nesse fluxo bidirecional.

Bloqueando Gnutella com o PDLM personalizado

Vamos ver um exemplo de como usar o PDLM personalizado. Usamos Gnutella como o tráfego que desejamos classificar e, então, aplicamos uma política de QoS que bloqueia esse tráfego.

Gnutella usa seis portas TCP conhecidas - 6346, 6347, 6348, 6349, 6355 e 5634. Outras portas podem ser detectadas quando os pinos são recebidos. Se os usuários especificarem outras portas para uso no compartilhamento de arquivos Gnutella, você poderá adicionar essas portas à sua instrução de protocolo de correspondência personalizada.

Aqui estão as etapas para criar uma política de serviço de QoS que corresponda e descarte o tráfego Gnutella.

1. Como observado acima, use o comando **show ip nbar unclassification-port-stats** para exibir o tráfego "não classificado" do NBAR. Se sua rede estiver transportando tráfego Gnutella, você verá uma saída semelhante à seguinte.

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

2. Utilize o comando ip nbar port-map custom para definir um mapa de portas personalizado, compatível com as portas do Gnutella.

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

   Observação: atualmente, você deve usar um nome como custom-xx. Os nomes definidos pelo usuário para PDLMs personalizados serão suportados em uma próxima versão do Cisco IOS Software.

3. Use o comando show ip nbar protocol stats para confirmar correspondências na instrução personalizada.

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

4. Crie uma política de serviço de QoS usando os comandos do CLI de QoS modular (MQC).

```
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
```

   Consulte Utilização de Listas de Controle de Acesso e Reconhecimento de Aplicativos Baseados em Rede para Bloquear o Worm "Código Vermelho" para obter outros comandos de configuração para bloquear o Gnutella e outros tráfegos indesejados.

Informações Relacionadas

- Recursos de suporte de QoS
- Suporte Técnico - Cisco Systems