Determinación del tráfico no reconocido por NBAR

Contenido

Introducción

Este documento muestra cómo utilizar la función Custom Packet Description Language Module (PDLM) de Network-Based Application Recognition (NBAR) para hacer coincidir el tráfico no clasificado o el tráfico que no se admite específicamente como una instrucción match protocol.

Prerequisites

Requirements

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Metodologías básicas de calidad del servicio
- Comprensión básica de NBAR

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 12.2(2)T del software del IOS® de Cisco
- 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.

Convenciones

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

Información sobre el PDLM personalizado

NBAR admite una variedad de protocolos estáticos y stateful. Los PDLM permiten un nuevo soporte de protocolo para NBAR sin el requerimiento de una actualización de la versión del IOS ni de una recarga de router. Las versiones siguientes del IOS incorporan el soporte para estos nuevos protocolos.

El PDLM personalizado le permite mapear los protocolos a los puertos estáticos de Protocolo de datagrama de usuarios (UDP) y TCP para protocolos que no sean admitidos actualmente en NBAR con un enunciado de protocolo de coincidencia. En otras palabras, amplía o mejora la lista de protocolos reconocidos por NBAR.

Estos son los pasos para agregar el PDLM personalizado al router.

1. Localice y descargue el NBAR PDLM desde la página de descarga de software (sólo clientes registrados) descargando el **archivo custom.pdlm**.
2. Cargue el PDLM en un dispositivo de memoria flash, como la tarjeta PCMCIA en las ranuras 0 o 1, usando el siguiente comando.
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. Verifique el soporte para los protocolos personalizados usando **show ip nbar port-map | incluye** el comando **personalizado** (que se muestra a continuación) o el 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. Asigne puertos a los protocolos personalizados mediante el **comando ip nbar port-map custom-XY {tcp|udp} {port1 port2 ...}**. Por ejemplo, para hacer coincidir el tráfico en el puerto TCP 8877, utilice el **comando ip nbar port-map custom-01 tcp 8877**.

Clasificación de los puertos "sin clasificar

En función del tráfico de red, es posible que deba utilizar mecanismos de clasificación especiales

en NBAR. Una vez que clasifique este tráfico, puede utilizar el PDLM personalizado y corresponder los números del UDP y del puerto TCP con un mapa de puerto personalizado.

De forma predeterminada, los mecanismos NBAR no clasificados no están habilitados. El comando show ip nbar unclassified-port-stats vuelve a dar el siguiente mensaje de error:

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

Bajo circunstancias controladas cuidadosamente, utilice el comando debug ip nbar unclassified-port-stats para configurar el router para comenzar a rastrear a qué puertos llegan los paquetes. A continuación, utilice el comando **show ip nbar unclassi-port-stats** para verificar la información recolectada. La salida ahora muestra el histograma de los puertos más utilizados.

Nota: Antes de ejecutar un comando **debug**, consulte Información Importante sobre Comandos Debug. Sólo se deben habilitar los comandos debug ip nbar bajo circunstancias controladas cuidadosamente.

Si esta información no es suficiente, puede habilitar la capacidad de captura, que proporciona una manera fácil de capturar rastros de paquetes de nuevos protocolos. Use los siguientes comandos de depuración, como se muestra a continuación.

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

El primer comando define los paquetes en los que está interesado para la captura. El segundo comando coloca NBAR en el modo de captura. Los argumentos del comando capture son los siguientes:

- Número de bytes para capturar por paquete.
- Número de paquetes iniciales para capturar, en otras palabras, cuántos paquetes capturar después del paquete SYN TCP/IP.
- Número de paquetes finales que se capturarán, en otras palabras, cuántos paquetes al final del flujo para los que se debe reservar espacio.
- Número de paquetes totales para capturar.

Nota: La especificación de los parámetros de inicio y final del paquete captura solamente los paquetes relevantes en un flujo largo.

Utilice el comando **show ip nbar capture** para ver la información recolectada. De forma predeterminada, el modo de captura espera a que llegue un paquete SYN y luego comienza a capturar los paquetes en ese flujo bidireccional.

Bloqueo de Gnutella con PDLM personalizado

Veamos un ejemplo de cómo utilizar el PDLM personalizado. Usamos Gnutella como el tráfico que queremos clasificar y luego aplicamos una política QoS que bloquea este tráfico.

Gnutella utiliza seis puertos TCP conocidos: 6346, 6347, 6348, 6349, 6355 y 5634. Se pueden detectar otros puertos cuando se reciben los Pongs. Si los usuarios especifican otros puertos para usarlos en el uso compartido de archivos de Gnutella, puede agregar estos puertos a la

instrucción de protocolo de coincidencia personalizada.

Estos son los pasos para crear una política de servicio de QoS que coincida con el tráfico Gnutella y lo descarte.

1. Como se indicó anteriormente, utilice el comando **show ip nbar unclassi-port-stats** para ver el tráfico "no clasificado" de NBAR. Si su red está transportando tráfico Gnutella, verá una salida similar a la siguiente.
```
Port    Proto    # of Packets
------- -------- -------
6346    tcp      347679
27005   udp      55043
```
2. Use el comando ip nbar port-map custom para definir custom port-map que coincida con los puertos Gnutella.

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

   Nota: Actualmente, debe utilizar un nombre como custom-xx. Los nombres definidos por el usuario para los PDLM personalizados se admitirán en una próxima versión de Cisco IOS Software.
3. Utilice el comando show ip nbar protocol stats para confirmar las coincidencias con la sentencia personalizada.
```
2620# show ip nbar protocol stats byte-count
FastEthernet0/0
               Input               Output
Protocol       Byte Count          Byte Count
-----------------------------------------------
custom-02      43880517            52101266
```
4. Cree una política de servicio de QoS mediante los comandos de la 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
```

   Refiérase a Uso del Reconocimiento de Aplicaciones Basadas en Red y Listas de Control de Acceso para Bloquear el gusano "Código Rojo" para otros comandos de configuración para bloquear Gnutella y otro tráfico no deseado.

Información Relacionada

- Recursos de soporte de QoS
- Soporte Técnico - Cisco Systems