Содержание

Введение

Этот документ показывает, как использовать функцию Custom Packet Description Language Module (PDLM) Network-Based Application Recognition (NBAR) для сопоставления неклассифицированного трафика или трафика, не поддерживаемого специально в качестве совпадающего протокольного утверждения.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам:

- Основные методы QoS
- Основное понимание NBAR

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Релиз 12.2 программного обеспечения Cisco IOS (2) T
- Маршрутизатор Cisco 7206

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Основные сведения о пользовательском PDLM

NBAR поддерживает множество помех и протоколов с хранением адресов. PDLM обеспечивают поддержку новым протоколам для NBAR без необходимости обновления версии IOS и перезагрузки маршрутизатора. В последующие версии IOS была включена поддержка этих новых протоколов.

Пользовательский PDLM позволяет сопоставлять протоколы со статическими портами протоколов UDP и TCP для протоколов, которые на данный момент не поддерживаются в NBAR, с сообщением о сопоставлении протоколов. Другими словами, это расширяет или улучшает список протоколов, распознанных NBAR.

Вот шаги в добавление Пользовательского PDLM к вашему маршрутизатору.

1. Найдите и загрузите PDLM NBAR от Страницы загрузки программного обеспечения (только зарегистрированные клиенты) путем загрузки **custom.pdlm файла**.
2. Загрузите PDLM на устройство с флэш-памятью, такое как карта PCMCIA в слотах 0 или 1, с помощью команды ниже.`7206-15(config)# ip nbar pdlm slot0:custom.pdlm`
3. Проверьте поддержку настраиваемых протоколов с помощью **команды show ip nbar port-map | include custom** (показанный ниже) или **команды 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. Назначьте порты на настраиваемые протоколы с помощью **Ip nbar port-map custom-XY {tcp|udp} {port1 port2... Команда.** Например, для соответствия на трафике в порту TCP 8877 используйте **команду ip nbar port-map custom-01 tcp 8877**.

Классифицирование "неклассифицированных" портов

В зависимости от вашего сетевого трафика вы, возможно, должны использовать механизмы особой классификации в NBAR. Классификация данного трафика позволяет применять пользовательский PDLM и сопоставлять номера портов UDP и TCP пользовательской карте портов.

По умолчанию NBAR несекретные механизмы не включен. **Команда show ip nbar unclassified-port-stats используется для возврата следующего сообщения об ошибках:**

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

Под жестким контролем используйте команду debug ip nbar unclassified-port-stats, чтобы настроить маршрутизатор для начала отслеживания, на какие порты поступают эти пакеты. Затем используйте **команду show ip nbar unclassified-port-stats** для проверки собранной информации. Теперь выходные данные отображают гистограмму наиболее часто используемых портов.

Примечание: Поддержку команд debug ip nbar следует включать только в строго

контролируемой среде.

Если эта информация не достаточна, можно включить возможность перехвата, которая предоставляет простой способ для получения трассировок пакетов новых протоколов. **Используйте следующие команды debug, как показано ниже.**

`debug ip nbar filter destination_port tcp XXXX debug ip nbar capture 200 10 10 10`
Первая команда определяет пакеты, которыми вы интересуетесь для перехвата. Вторая команда помещает NBAR в режим перехвата. **Аргументы команды записи:**

- Количество байтов для получения на пакет.
- Количество стартовых пакетов для получения, другими словами, сколько пакетов для получения после SYN - пакета TCP/IP.
- Количество финальных пакетов для получения, другими словами, сколько пакетов в конце потока, для которого должно быть зарезервировано пространство.
- Количество общих пакетов для получения.

Примечание: Определение начальных и конечных параметров пакетов позволяет перехватывать в длинном потоке только соответствующие пакеты.

Используйте **команду show ip nbar capture** для просмотра собранной информации. По умолчанию режим перехвата ждет SYN - пакета для поступления и затем начинает перехватывать пакеты на том двунаправленном потоке.

Блокировка сети Gnutella настраиваемыми пакетами PDLM

Давайте посмотрим на пример того, как использовать Пользовательский PDLM. Мы отметим данные из сети Gnutella как трафик, который хотим классифицировать, а затем применим политику QoS, которая блокирует этот класс трафика.

Gnutella использует шесть известных портов TCP - 6346, 6347, 6348, 6349, 6355, и 5634. Другие порты могут быть обнаружены, поскольку получена Вонь. Если пользователи задают другие порты для использования в общем файле Gnutella, можно добавить эти порты к настраиваемому выражению соответствия протокола.

Вот шаги в создание политики обслуживания QoS, которая совпадает на и отбрасывает Трафик сети Gnutella.

1. Как обращено внимание выше, используйте **команду show ip nbar unclassified-port-stats** для просмотра NBAR "несекретный" трафик. Если ваша сеть транспортирует Трафик сети Gnutella, то вы будете видеть выходные данные, подобные следующему.**`debug ip nbar filter destination_port tcp XXXX debug ip nbar capture 200 10 10 10`**
2. **Для задания настроек переадресации портов, соответствующих портам Gnutella, пользуйтесь произвольной командой ip nbar port-map.**`ip nbar port-map custom-02 tcp 5634 6346 6347 6348 6349 6355` **Примечание:** В настоящее время необходимо использовать название, такое как пользовательский xx. Определяемые пользователем названия для пользовательских PDLM будут поддерживаться в программном обеспечении планируемого релиза Cisco IOS.
3. **Воспользуйтесь командой show ip nbar protocol stats, чтобы подтвердить совпадения настраиваемой инструкции.**`2620# show ip nbar protocol stats byte-count FastEthernet0/0 Input Output Protocol Byte Count Byte Count ----------`

```
------------------------------ custom-02      43880517           52101266
```

4. Создайте политику обслуживания QoS с помощью команд командной строки Modular QoS CLI (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`**См. Использование Сетевого распознавания приложений и Списков контроля доступа для Блокирования Червя "Code Red" для других команд настройки для блокирования Gnutella и другого нежелательного трафика.

Дополнительные сведения

- Ресурсы поддержки QoS
- Техническая поддержка - Cisco Systems