NBAR에서 인식되지 않는 트래픽 확인

목차

소개

이 문서에서는 NBAR(Network-Based Application Recognition)의 PDLM(Custom Packet Description Language Module) 기능을 사용하여 미분류 트래픽 또는 매치 프로토콜 문으로 특별히 지원되지 않는 트래픽에서 매칭하는 방법을 보여 줍니다.

사전 요구 사항

요구 사항

이 문서의 독자는 다음 주제에 대해 알고 있어야 합니다.

- 기본 QoS 방법론
- NBAR에 대한 기본적인 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.2(2)T
- Cisco 7206 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

맞춤형 PDLM 이해

NBAR는 다양한 정적 및 스테이트풀 프로토콜을 지원합니다.PDLM은 IOS 릴리스 업그레이드 및 라우터 다시 로드 없이 NBAR에 대한 새 프로토콜 지원을 허용합니다.후속 IOS 릴리스에는 이러한 새로운 프로토콜에 대한 지원이 통합되어 있습니다.

Custom PDLM에서는 프로토콜을 match protocol 문을 사용하여 NBAR에서 현재 지원되지 않는 프로토콜의 UDP(Static User Datagram Protocol) 및 TCP 포트에 매핑할 수 있습니다.즉, NBAR에서 인식하는 프로토콜 목록을 확장하거나 강화합니다.

다음은 라우터에 사용자 지정 PDLM을 추가하는 단계입니다.

1. custom.pdlm **파일**을 다운로드하여 소프트웨어 다운로드 페이지(등록된 고객만 해당)에서 NBAR PDLM을 찾아 **다운로드합니다**.
2. 아래 명령을 사용하여 PDLM을 슬롯 0 또는 1의 PCMCIA 카드와 같은 플래시 메모리 장치에 로드합니다.
   ```
   7206-15(config)# ip nbar pdlm slot0:custom.pdlm
   ```
3. **show ip nbar port-map**을 사용하여 맞춤형 프로토콜 지원 확인 | **사용자 지정** 명령(아래 표시) 또는 **show ip nbar pdlm** 명령 포함
   ```
   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 ...}** 명령을 사용하여 사용자 지정 프로토콜**에 포트를** 할당합니다.예를 들어, TCP 포트 8877의 트래픽에서 매칭하려면 **ip nbar port-map custom-01 tcp 8877** 명령을 사용합니다.

"미분류" 포트 분류

네트워크 트래픽에 따라 NBAR에서 특수 분류 메커니즘을 사용해야 할 수 있습니다.이 트래픽을 분류한 다음 사용자 지정 PDLM을 사용하고 UDP 및 TCP 포트 번호를 사용자 지정 포트 맵에 일치시킬 수 있습니다.

기본적으로 NBAR 미분류 메커니즘은 활성화되지 않습니다.show ip **nbar unclassified-port-stats** 명령은 다음 오류 메시지를 반환합니다.

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

신중하게 제어된 환경에서 debug **ip nbar unclassified-port-stats** 명령을 사용하여 패킷이 도착하는 포트를 추적하도록 라우터를 구성합니다.그런 다음 **show ip nbar unclassified-port-stats** 명령을 사용하여 수집된 정보를 확인합니다.이제 출력에 가장 일반적으로 사용되는 포트의 히스토그램이 표시됩니다.

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.debug **ip nbar** 명령은 신중하게 제어된 상황에서만 활성화해야 합니다.

이 정보가 충분하지 않으면 새 프로토콜의 패킷 추적을 쉽게 캡처할 수 있는 캡처 기능을 활성화할 수 있습니다.아래와 같이 다음 **debug** 명령을 사용합니다.

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

첫 번째 명령은 캡처하려는 패킷을 정의합니다.두 번째 명령은 NBAR를 캡처 모드로 전환합니다 .**capture** 명령의 인수는 다음과 같습니다.

- 패킷당 캡처할 바이트 수입니다.
- 캡처할 시작 패킷 수, 즉 TCP/IP SYN 패킷 이후 캡처할 패킷 수입니다.
- 캡처할 최종 패킷의 수(즉, 플로우의 끝에 공간이 예약되어야 하는 패킷의 수)입니다.
- 캡처할 총 패킷 수입니다.

참고: 시작 및 최종 패킷 매개변수를 지정하면 긴 흐름에서 관련 패킷만 캡처됩니다.

수집된 정보를 보려면 **show ip nbar capture** 명령을 사용합니다.기본적으로 캡처 모드는 SYN 패킷이 도착할 때까지 기다린 다음 해당 양방향 흐름에서 패킷을 캡처하기 시작합니다.

사용자 지정 PDLM으로 Gnutella 차단

사용자 지정 PDLM을 사용하는 방법의 예를 살펴보겠습니다.분류하려는 트래픽으로 Gnutella를 사용한 다음 이 트래픽을 차단하는 QoS 정책을 적용합니다.

Gnutella는 6346, 6347, 6348, 6349, 6355 및 5634 등 6개의 잘 알려진 TCP 포트를 사용합니다 .Pongs를 수신하면 다른 포트가 탐지될 수 있습니다.사용자가 Gnutella 파일 공유에서 사용할 다른 포트를 지정하는 경우 이러한 포트를 사용자 지정 일치 프로토콜 문에 추가할 수 있습니다.

다음은 Gnutella 트래픽과 매칭하고 삭제하는 QoS 서비스 정책을 생성하는 단계입니다.

1. 위에서 설명한 대로 **show ip nbar unclassified-port-stats** 명령을 사용하여 NBAR "unclassified" 트래픽을 확인합니다.네트워크에서 Gnutella 트래픽을 전송하는 경우 다음과 유사한 출력이 표시됩니다.
   ```
   Port    Proto    # of Packets
   ------- -------- -------
   6346    tcp      347679
   27005   udp      55043
   ```
2. ip nbar **port-map custom** 명령을 사용하여 Gnutella 포트와 일치하는 사용자 지정 포트 맵을 정의합니다.

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

참고: 현재 custom-xx와 같은 이름을 사용해야 합니다.맞춤형 PDLM에 대한 사용자 정의 이름은 Cisco IOS Software의 다음 릴리스에서 지원됩니다.

3. show ip **nbar protocol stats** 명령을 사용하여 사용자 지정 문에 대한 일치를 확인합니다.

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

4. 모듈형 MQC(QoS CLI)의 명령을 사용하여 QoS 서비스 정책을 생성합니다.

```
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
```

Gnutella와 기타 원치 않는 트래픽을 차단하기 위한 다른 컨피그레이션 명령은 네트워크 기반 애플리케이션 인식 및 액세스 제어 목록을 사용하여 "코드 레드" WORM 차단을 참조하십시오 .

관련 정보

- QoS 지원 리소스
- Technical Support - Cisco Systems