IP 주소에 처리율 제한 적용하기.araboja

(주의!) 여러 상황을 고려하지 않고 단편적으로만 araboja

Contents

정보처리기사 단골 주제 아인교..?

"물데네전세표응"의 주인공, OSI 7 Layer

- "물데네전세표응" 이라고 외워보자
- 그래서 뭐가 있었지?

L7 ("응", Application) - HTTP, FTP, SMTP

L6 ("표", Presentation) - 암호화, 인코딩

L5 ("세", Session) - 세션 관린

L4 ("전", Transport) - TCP, UDP

L3 ("네", Network) - IP, 라우팅

L2 ("데", Data Link) - 이더넷

L1 ("물", Physical) - 물리적 전송

문제 인식

IP 주소로 처리율 제한기를 두면 L7까지 갈 필요 없는거 아니야?

- L7까지 올라가면 발생하는 오버헤드
  - TCP 핸드셰이크
  - HTTP 요청 수신
  - HTTP 헤더 파싱
  - 애플리케이션 서버 처리

- L7까지 올라가면 발생하는 오버헤드(feat. 제프 딘의 Numbers Everyone Should Know)
  - TCP 핸드셰이크 - **750,000**ns
  - HTTP 요청 수신 - **250,100**ns
  - HTTP 헤더 파싱 - **1,500**ns
  - 애플리케이션 서버 처리 - **X**ns
- 750,000 + 250,100 + 1,500 + X = **1,001,600 + X**ns

- L4으로 내리면 발생하는 오버헤드(출처. 갓GPT)
  - 패킷 수신 - **250,000**ns
  - IP/TCP 헤더 읽기 - **100**ns
  - 룰 매칭 - **100**ns
  - 카운터 업데이트 - **100**ns
- 250,000 + 100 + 100 + 100 = **250,400**ns

그러니까 L3/L4에서 해결해 보자...

Iptables 가져와

Iptables가 뭘까?

- 리눅스 시스템에서 네트워크 트래픽을 제어하는 방화벽 툴
- L3/L4 수준에서 패킷을 효율적으로 필터링

방법

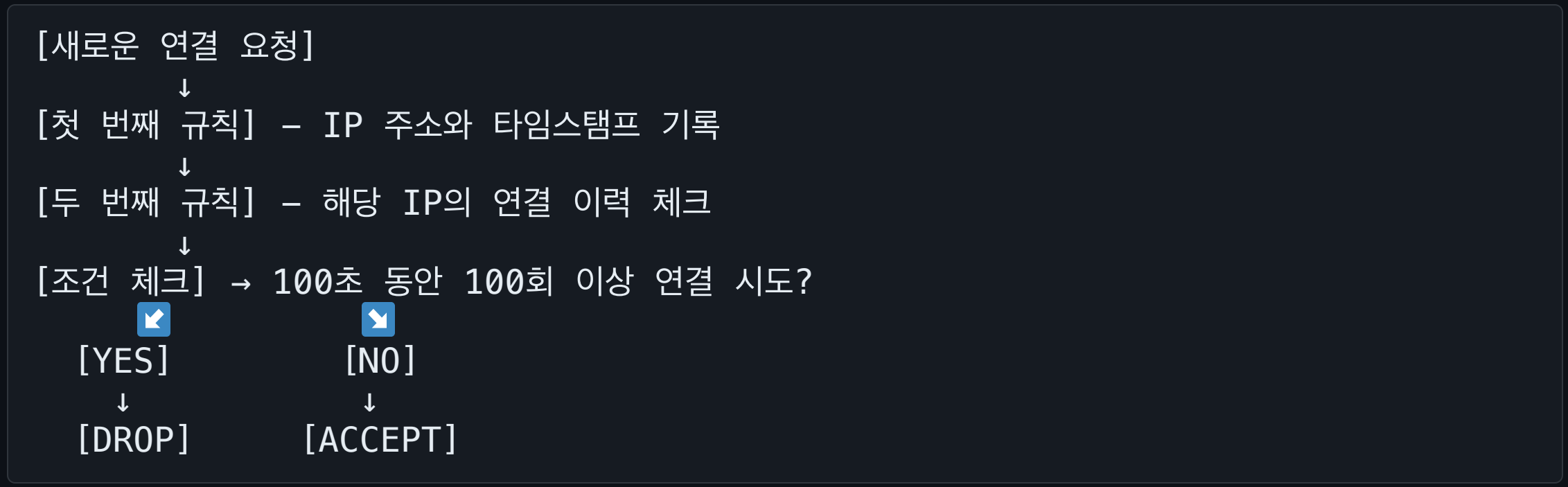
- https://blog.programster.org/rate-limit-requests-with-iptables

"제가요.. 서버 보안을 위해서 IP 기반 연결 제한 방법을 적용했는데요. 특정 IP당 일정 시간 내 최대 연결 수를 제한했답니다.. 🥹 뭐, DoS 공격 정도는 막을 듯요~"

```
[클라이언트 요청] → [iptables 규칙 체크] → [허용/차단]
                          ↓
                  [연결 수 카운팅]
                  [시간 체크]
```

- TIME_PERIOD = 100 **(100초 동안)**
- BLOCKCOUNT = 100 **(100회 이상 연결시)**
- DACTION = "DROP" **(조건 넘기면 버려)**

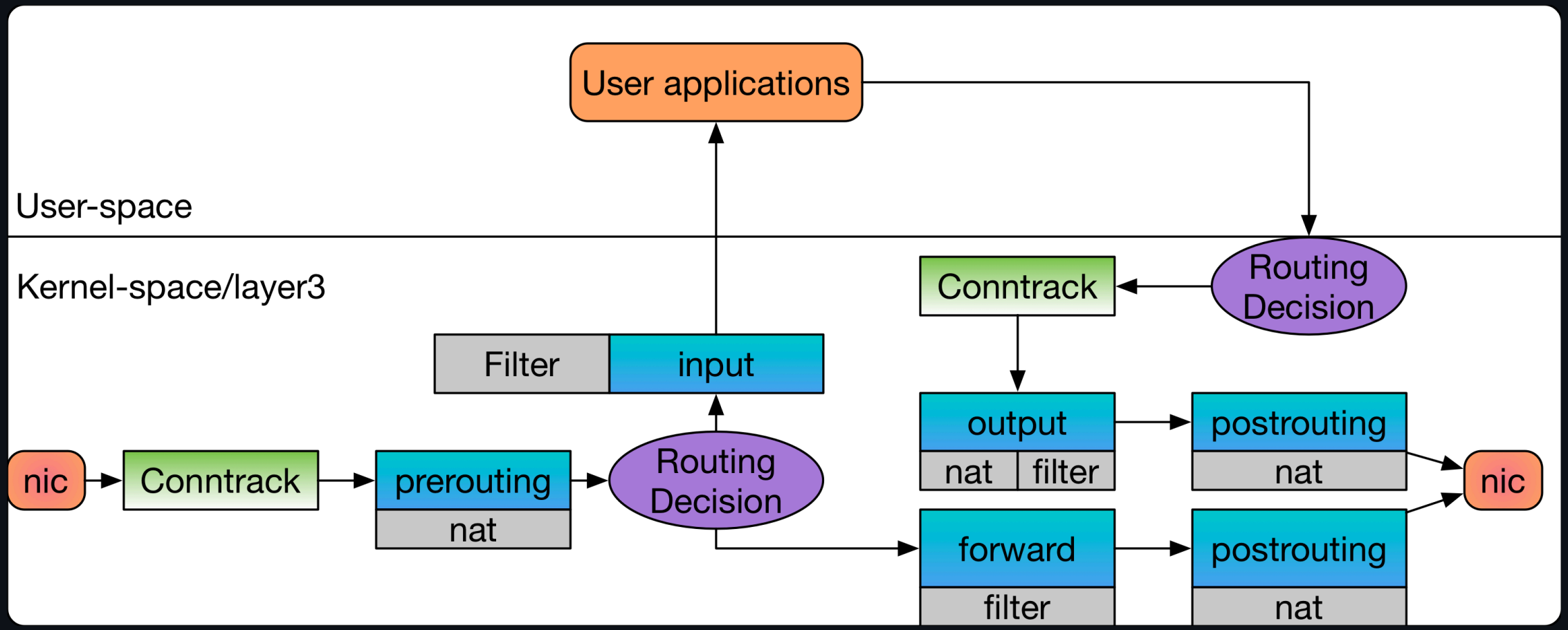
```
# HTTP(80) 포트 규칙
$IPT -A INPUT -p tcp --dport 80 -i eth0 -m state --state NEW -m recent --set
$IPT -A INPUT -p tcp --dport 80 -i eth0 -m state --state NEW -m recent \
    --update --seconds $TIME_PERIOD --hitcount $BLOCKCOUNT -j $DACTION

# HTTPS(443) 포트 규칙
$IPT -A INPUT -p tcp --dport 443 -i eth0 -m state --state NEW -m recent --set
$IPT -A INPUT -p tcp --dport 443 -i eth0 -m state --state NEW -m recent \
    --update --seconds $TIME_PERIOD --hitcount $BLOCKCOUNT -j $DACTION
```



아! **고정 윈도 카운터 알고리즘** 을 사용했구나 🤔

새로운 문제

근데 iptables이 툴이면 애플리케이션 아니야? 그러면 L7 아니야? 라는 단순한 생각 ㅋㅋ



- `netfilter` 라고 하는 커널의 패킷 필터링 훅(Layer3)과 연계함 **(패킷 제어)**
- `iptables` 는 `netfilter` 를 제어하는 네트워크 스택 인터페이스 **(패킷 제어 룰)**

끗.