Chapter 03. 시스템 모니터링

보안 및 방화벽

보안 기능 및 방화벽(iptables)

- 보안 기능 개요
  - SELinux
- 방화벽
  - iptables
- 접근 차단 유틸리티
  - fail2ban, brute-force ssh 접속 차단

보안 기능 개요 - SELinux 소개

- 접근통제 (ACL) 기능을 통한 디렉토리, 파일, 네트워크 소켓 등에 대한 자원에 접근 권한을 설정

- 접근 통제 모델
  - 임의적 접근 통제 : DAC (Discretionary Access Control)
    - 사용자의 신분 (및 그룹) 을 통해 제한 (uid, gid, setuid 등)
    - 객체(objects)의 사용자(user)에게 소유권(ownership)이 결정 됨
  - 강제적 접근 통제 : MAC (Mandatory Access Control)
    - 미리 정해진 정책과 보안 등급에 의거하여 주체(subjects - 사용자, 프로세스, 프로그램)와 객체(파일, 디바이스 등)에게 허용된 접근 권한 부여
    - 불필요한 부분을 제거하고, 오직 필요한 기능만에 대한 권한을 안전하게 부여

- DAC 은 리눅스 계정 권한으로 기본 탑재
- MAC 은 SELinux 를 통해 구현

- SELinux (Security-Enhanced Linux)
  - sudo apt install selinux (초보자는 비추천)

방화벽 - 개요

네트워크 트래픽 접근제어 설정

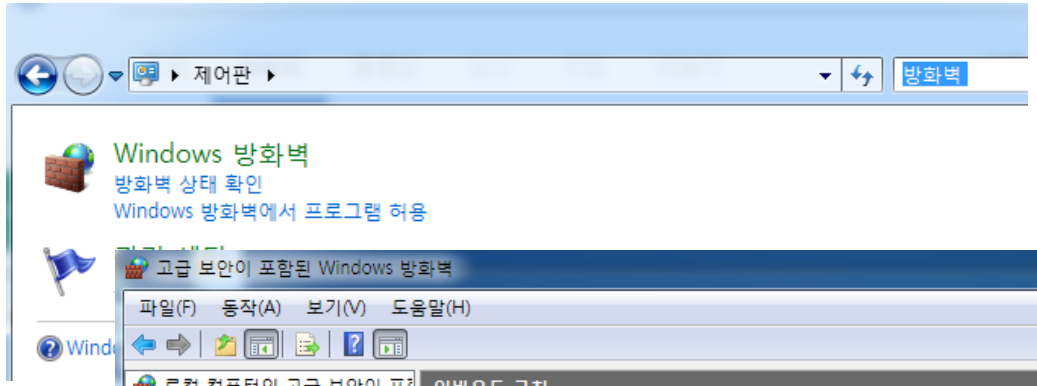
- 방화벽?
  - 기본 차단 (Default Deny Rule)
  - 5-Tuple based (SIP / DIP / PROTO / SPORT / DPORT)

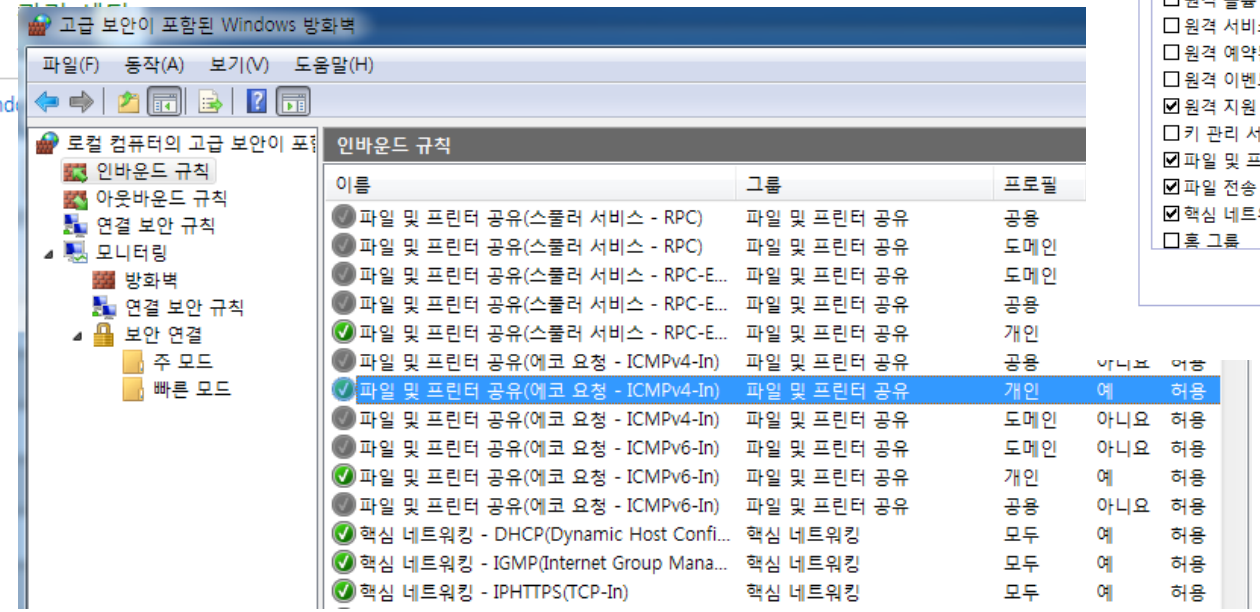
Priority	Action	Src	Dst	Proto	Sport	Dport
1	ALLOW	ANY	8.8.8.8	TCP, UDP	ANY	53
2	ALLOW	192.168.0.0/24	172.16.0.0/16	TCP	ANY	22
3	ALLOW	ANY	10.0.2.15	TCP	ANY	80
4	DENY	ANY	ANY	ANY	ANY	ANY

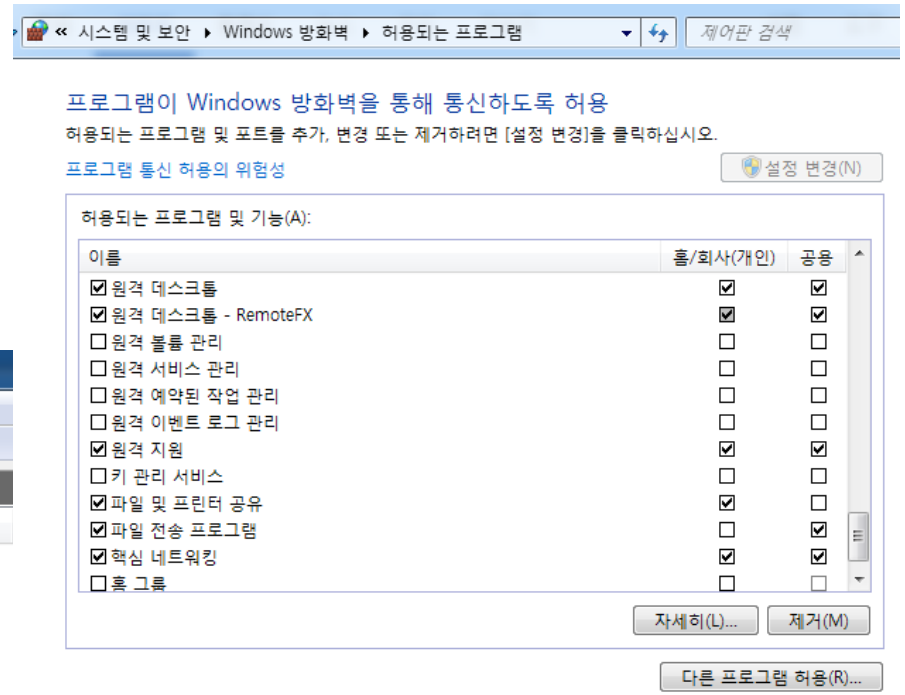
방화벽 - 개요 (윈도우즈)

네트워크 트래픽 접근제어 설정

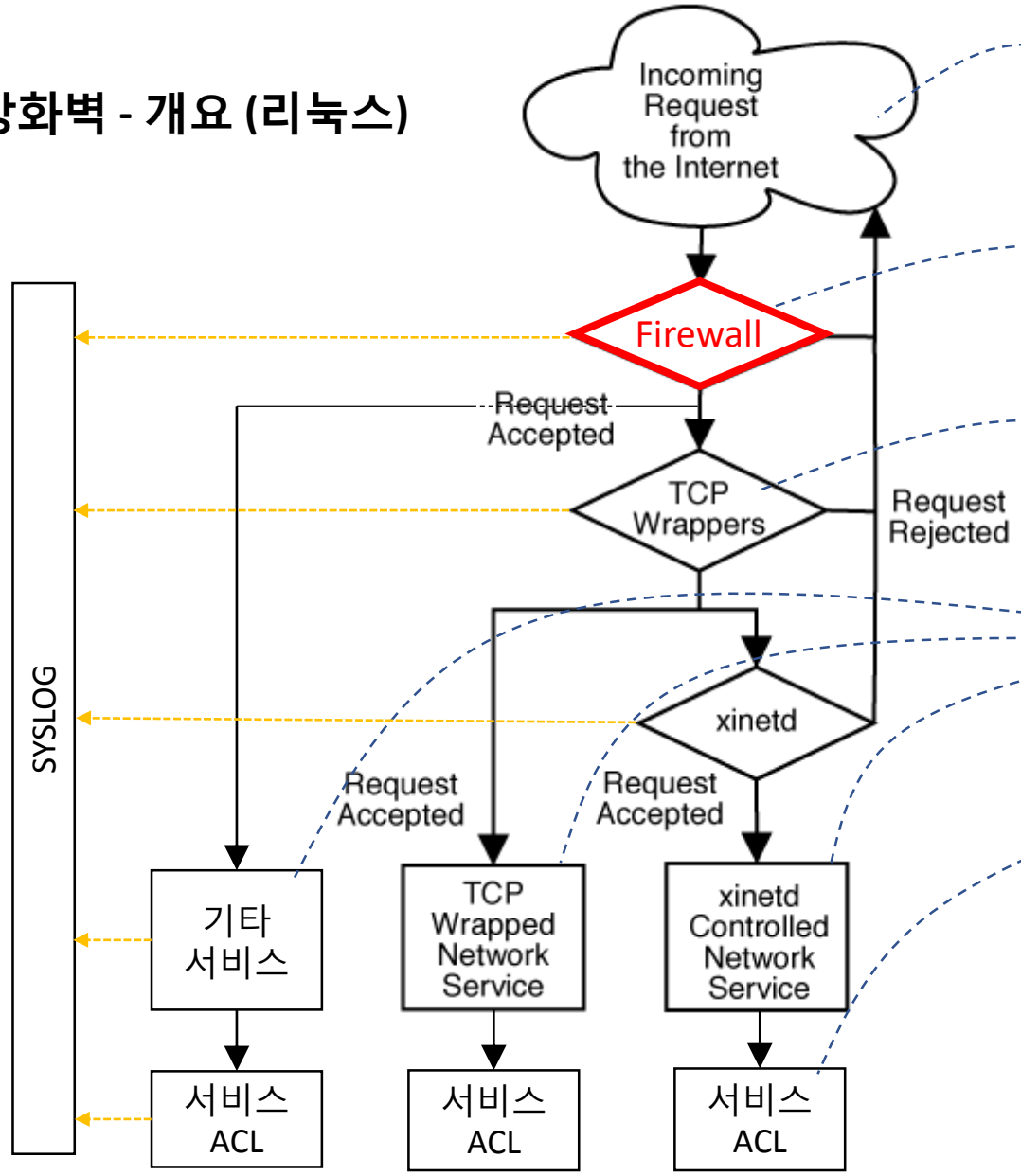
- 운영체제마다 다양하게 구현







방화벽 - 개요 (리눅스)



리눅스 시스템의 네트워크 서비스 접근 제어 모델

사용자 접근 / 서비스 요청

(커널 레벨) 방화벽 – L2/L3/L4
- netfilter / ebtables / iptables

어플리케이션 방화벽 – L3/L4
- tcpwrapper

응용 소프트웨어

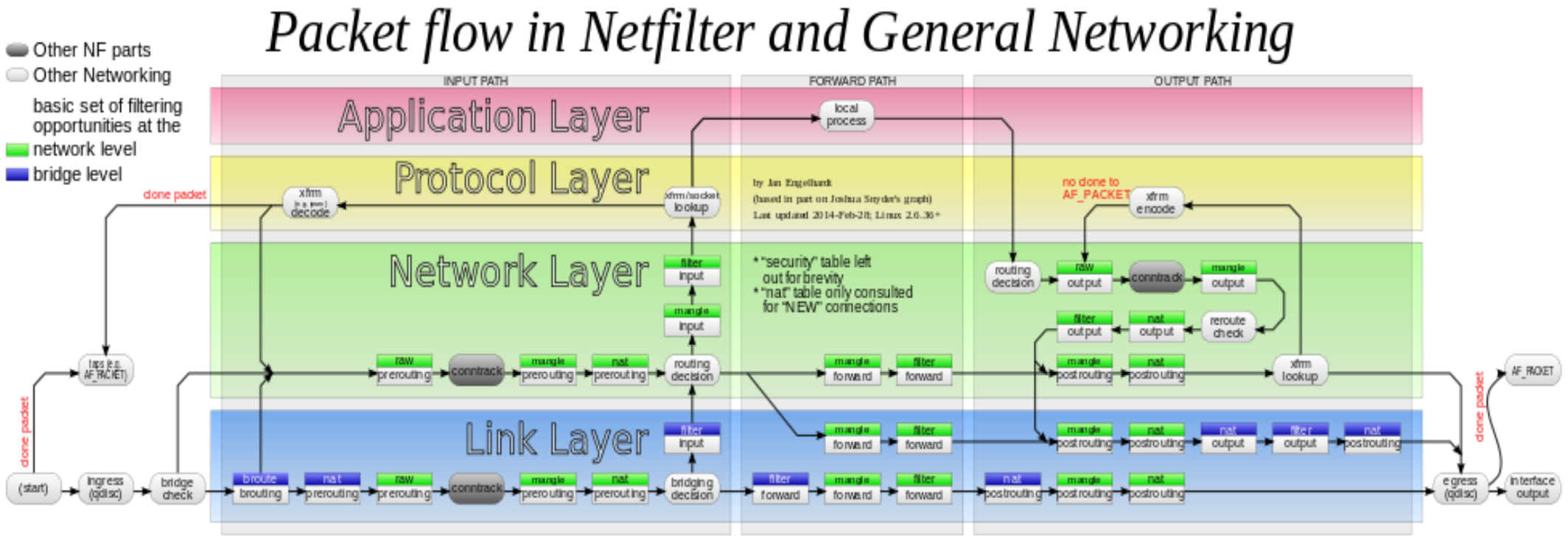
응용 소프트웨어 보안모듈 / 접근제어 – L7
- Auth / PAM (Pluggable Authentication Module)
- LDAP / Radius / …

참고자료
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Reference_Guide/ch-tcpwrappers.html

방화벽 - 리눅스 넷필터 아키텍처

네트워크 트래픽 접근제어 프레임워크

- 리눅스에서의 네트워크 필터링

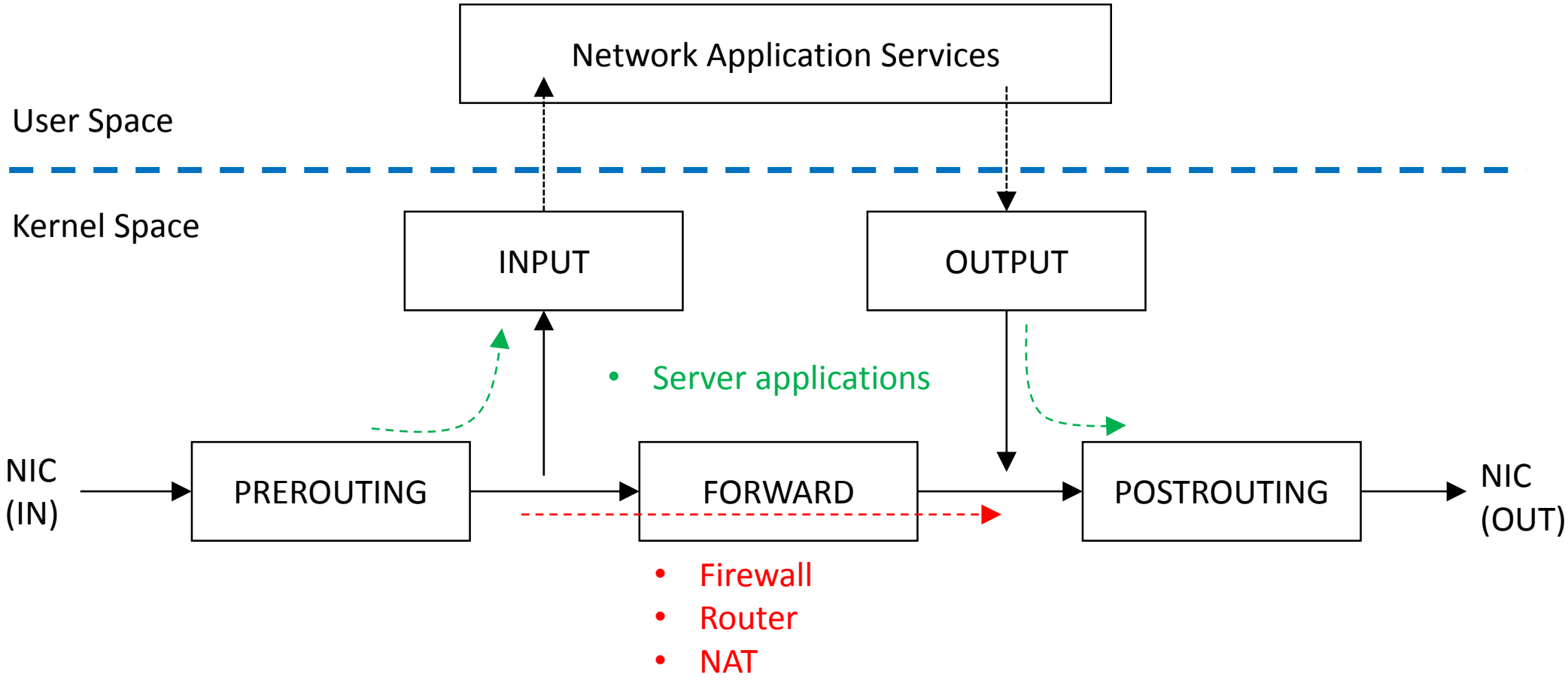


출처 : https://en.wikipedia.org/wiki/Netfilter

방화벽 - 리눅스 넷필터 아키텍처 정책 설정도구, iptables

네트워크 트래픽 접근제어 프레임워크 - 단순화

- 리눅스에서의 iptables 체인을 사용한 네트워크 패킷 필터링



방화벽 - 리눅스 넷필터 아키텍처 정책 설정도구, iptables

네트워크 트래픽 접근제어 설정

- iptables 명령어

```
user1@user1-VirtualBox:~ $ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- 참고:
  docker 가 설치된 경우 docker0 인터페이스로
  주고받는 패킷으로 인해 상당히 많은 룰이 있음

Direction	Stage	Table	Chain
remote-to-local	before routing	raw	PREROUTING
		mangle	PREROUTING
		nat	PREROUTING
	after routing	mangle	INPUT
		filter	INPUT
remote-to-remote	before routing	raw	PREROUTING
		mangle	PREROUTING
		nat	PREROUTING
	after routing	mangle	FORWARD
		filter	FORWARD
		mangle	POSTROUTING
		nat	POSTROUTING
local-to-remote	before routing	raw	OUTPUT
		mangle	OUTPUT
		nat	OUTPUT
		filter	OUTPUT
	after routing	mangle	POSTROUTING
		nat	POSTROUTING

방화벽 - 리눅스 넷필터 아키텍처 정책 설정도구, iptables

네트워크 트래픽 접근제어 설정 - iptables 기본 문법

- iptables <옵션> <상세명령> <정책>
  - 옵션
    - -L : 목록 출력
    - -A <Chain> : 새로 정책 추가 (--append)
    - -I <Chain> <Prio> : 특정 위치에 정책 추가 (--insert)
    - -D <Chain> : 정책 삭제 (--delete)
    - -N <Chain> : 새로운 체인 추가(생성)
    - -F <Chain> : 체인 내 규칙 삭제 (--flush)
    - -X <Chain> : 체인 삭제 (--delete-chain)
    - -P <Chain> <Action> : 체인의 기본 정책 설정 (--policy)
  - 상세명령
    - -s <IP> : 패킷의 출발지
    - -d <IP> : 패킷의 목적지
    - -p <proto> : 패킷의 프로토콜
    - --sport <port> : 패킷의 출발지 port
    - --dport <port> : 패킷의 목적지 port
  - 정책
    - -j DROP : 패킷 차단
    - -j ACCEPT : 패킷 허용
    - -j LOG : 패킷 로깅

방화벽 - 리눅스 넷필터 아키텍처 정책 설정도구, iptables

네트워크 트래픽 접근제어 설정 - iptables 활용 예시

- iptables 사용 예
  - 외부 입력 차단
    - iptables -A INPUT -p tcp --dport 80 -j DROP
    - iptables -I INPUT 1 -p tcp --dport 21 -j ACCEPT
    - iptables -D INPUT -p tcp --dport 80 -j DROP
  - 내부 송신 차단 또는 허용/로깅
    - iptables -A OUTPUT -p icmp -d 8.8.8.8 -j DROP
    - iptables -A OUTPUT -p icmp -d 8.8.8.8 -j LOG --log-level 4 --log-prefix “MyLog: ”
  - 새로운 로깅과 차단 체인 생성
    - iptables -N LOG_DROP
    - iptables -A LOG_DROP -j LOG --log-prefix “INPUT:DROP: “ --log-level 6
    - iptables -A LOG_DROP -j DROP
    - iptables -A INPUT -p tcp --dport 5555 -j LOG_DROP
  - 기존 룰 삭제
    - iptables –F INPUT
  - 로그 예시, tail –F /var/log/kern.log
    Jun 23 12:59:22 user1-VirtualBox kernel: [37274.981486] MyLog: IN= OUT=enp0s3 SRC=10.0.2.15 DST=8.8.8.8 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=3530 DF PROTO=ICMP TYPE=8 CODE=0 ID=10292 SEQ=1

방화벽 - 리눅스 넷필터 아키텍처 정책 설정도구, iptables

네트워크 트래픽 접근제어 설정 - iptables 활용한 다양한 응용 실 사례

- iptables 사용 예
  - slow down SSH brute-force attack (연속해서 4번 접속 실패(시도) 시 60초동안 차단)
    - iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --set
    - iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --update --seconds 60 --hitcount 4 -j DROP
  - PING 요청 차단 (DDoS 공격 방지를 위한...)
    - iptables -A OUTPUT -p ICMP --ICMP-type echo-request -j DROP
  - HTTP/HTTPS 패킷의 conntrack 관리
    - iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
    - iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
    - iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
    - iptables -A OUTPUT -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
    - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
    - iptables -A INPUT -i lo -j ACCEPT

무작위 SSH 접속 차단 유틸리티 - fail2ban

특정 시간 내 반복 로그인 실패 시 정해진 시간만큼 해당 호스트의 접속을 차단

- 설치방법
  - apt install fail2ban
- 확인/활성화
  - systemctl status fail2ban
  - systemctl enable fail2ban
  - systemctl restart fail2ban
- 설정파일
  - /etc/fail2ban/jail.conf
  - /etc/fail2ban/jail.local (생성)
- 로그파일
  - /var/log/fail2ban.log

```
user1@user1-VirtualBox:~$ systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset:
   Active: active (running) since 화 2020-06-23 13:29:49 KST; 3min 37s ago
     Docs: man:fail2ban(1)
 Main PID: 11309 (fail2ban-server)
    Tasks: 3
   Memory: 11.6M
      CPU: 891ms
   CGroup: /system.slice/fail2ban.service
           └─11309 /usr/bin/python3 /usr/bin/fail2ban-server -s /var/run/fail2ba

 6월 23 13:29:48 user1-VirtualBox systemd[1]: Starting Fail2Ban Service...
 6월 23 13:29:48 user1-VirtualBox fail2ban-client[11287]: 2020-06-23 13:29:48,98
 6월 23 13:29:48 user1-VirtualBox fail2ban-client[11287]: 2020-06-23 13:29:48,99
 6월 23 13:29:49 user1-VirtualBox systemd[1]: Started Fail2Ban Service.
lines 1-15/15 (END)
```

무작위 SSH 접속 차단 유틸리티 - fail2ban #2

fail2ban 의 각종 설정 및 내부 동작

- 설정파일
  - /etc/fail2ban/jail.conf

```
[DEFAULT]
ignoreip = 127.0.0.1/8      # 차단 하지 않을 대역
bantime = 600               # 차단 시간
findtime = 600              # 접속 시도 체크 범위
maxretry = 5                # 실패 횟수
```

=> 600초(10분) 동안에 5회 실패 시 600초(10분) 간 차단

- 주의:
  차단 시 SSH 접속 시도만이 아닌,
  해당 IP주소의 모든 패킷 차단됨

auth.log

```
tail -F /var/log/auth.log
tualBox sshd[11750]: Failed password for user1 from 10.0.2.2 port 51450 ssh2
tualBox sshd[11750]: message repeated 2 times: [ Failed password for user1 fro
```

fail2ban-server, fail2ban.log

```
2020-06-23 13:58:51,761 fail2ban.filter         [11309]: INFO    [sshd] Found 10.0.2.2
2020-06-23 13:58:53,466 fail2ban.filter         [11309]: INFO    [sshd] Found 10.0.2.2
2020-06-23 13:59:15,923 fail2ban.filter         [11309]: INFO    [sshd] Found 10.0.2.2
2020-06-23 13:59:17,921 fail2ban.filter         [11309]: INFO    [sshd] Found 10.0.2.2
2020-06-23 13:59:33,211 fail2ban.filter         [11309]: INFO    [sshd] Found 10.0.2.2
2020-06-23 13:59:33,312 fail2ban.actions        [11309]: NOTICE  [sshd] Ban 10.0.2.2
2020-06-23 13:59:35,015 fail2ban.filter         [11309]: INFO    [sshd] Found 10.0.2.2
```

fail2ban-server, iptables

```
user1@user1-VirtualBox:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 f2b-sshd   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            multiport
 dports 22

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain f2b-sshd (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
user1@user1-VirtualBox:~$
```

```
Chain f2b-sshd (1 references)
 pkts bytes target     prot opt in     out     source               destination
   21  2360 REJECT     all  --  *      *       10.0.2.2             0.0.0.0/0            reject-wi
th icmp-port-unreachable
  270 26848 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```