■ FreeBSD 에서 ipfw 를 이용한 방화벽 설정

- 커널 설정 파일에 옵션을 주고 컴파일 해야 사용가능
- 아래 처럼 간단히 커널 컴파일을 하기 위해 기본설정 파일인 GENERIC 을 복사하여 옵션을 추가.
  - ✓ [root@rootous ~]# mkdir Kernel ; cd Kernel
  - ✓ [root@rootous ~]# cp /usr/src/sys/i386/conf/GENERIC ~/Kernel/rootous
  - ✓ [root@rootous ~]# vi ~/Kernel/rootous
  - ✓ ident rootous
  - ✓ options IPFIREWALL
  - ✓ options IPFIREWALL_VERBOSE
  - ✓ options IPFIREWALL_VERBOSE_LIMIT=5
  - ✓ options IPFIREWALL_DEFAULT_TO_ACCEPT
  - ✓ options IPDIVERT

- 커널 설정 파일을 심볼링크로 걸고 컴파일을 시작.
  - ✓ [root@rootous ~] /usr/src
  - ✓ [root@rootous ~]# ln -s ~/Kernel/rootous /usr/src/sys/i386/conf/rootous
  - ✓ [root@rootous ~]# make buildkernel KERNEL=rootous ; make installkernel KERNEL=rootous

- CPU 스펙에 따라 시간이 걸림
  - ✓ /etc/sysctl.conf 파일에 아래와 같이 추가 해준다.
  - ✓ [root@rootous ~]# echo 'net.inet.ip.fw.verbose=1' >> /etc/sysctl.conf
  - ✓ [root@rootous ~]# echo 'net.inet.ip.fw.verbose_limit=5' >> /etc/sysctl.conf

- ipfw 활성화, 로깅, 방화벽 설정파일을 지정.
  - ✓ [root@rootous ~]# echo 'firewall_enable="YES"' >> /etc/rc.conf
  - ✓ [root@rootous ~]# echo 'firewall_logging="YES"' >> /etc/rc.conf
  - ✓ [root@rootous ~]# echo 'firewall_type="/etc/firewall.conf"' >> /etc/rc.conf

- 방화벽 룰을 저장할 /etc/firewall.conf 를 생성하고 그 안에 원하는 해당 룰을 첨가.
  - ✓ [root@rootous ~]# vi /etc/firewall.conf

■ ### IP 차단 ###

- ✓ 192.168.100.0/24 대역에서 오는 TCP, UDP 패킷들 차단
- ✓ add 10 deny tcp from 192.168.100.0/24 to any
- ✓ add 10 deny udp from 192.168.100.0/24 to any

■ ### Port 허용 ###

- 서비스 포트 허용
  - ✓ (FTP, SSH, Mail, DNS, HTTP)
  - ✓ add 20 allow tcp from any to any 21 in
  - ✓ add 20 allow tcp from any to any 21 out
  - ✓ add 20 allow tcp from any to any 22 in
  - ✓ add 20 allow tcp from any to any 22 out
  - ✓ add 20 allow tcp from any to any 25 in
  - ✓ add 20 allow tcp from any to any 25 out
  - ✓ add 20 allow udp from any to any 53 in
  - ✓ add 20 allow udp from any to any 53 out
  - ✓ add 20 allow tcp from any to any 80 in
  - ✓ add 20 allow tcp from any to any 80 out

■ ### Port 차단 ###

- 외부 포트 6667 에서 들어오고 나가는 모든 TCP 패킷 차단
  - ✓ add 30 deny tcp from any to any src-port 6667 in
  - ✓ add 30 deny tcp from any to any src-port 6667 out
  - ✓ 내부 포트 6667 에서 들어오고 나가는 모든 TCP 패킷 차단
  - ✓ add 30 deny tcp from any to any dst-port 6667 in
  - ✓ add 30 deny tcp from any to any dst-port 6667 out

■ ### ICMP 차단 ###

- ICMP 를 차단하고 로깅을 활성화
  - ✓ add 40 deny icmp from any to any via fxp0
  - ✓ add 40 deny log icmp from any to any via fxp0

■ ### 모든 접속 차단 ###

- 외부에서 오는 모든 접속을 차단하며 룰셋순위가 아래에 있어야 한다.
  - ✓ add 65534 deny ip from any to any

- 적용후 리부팅
  - ✓ [root@rootous ~]# reboot

■ 룰셋이 정상적으로 적용 됬는지 ipfw 목록을 확인.

- [root@rootous ~]# ipfw list
  - ✓ 00010 deny tcp from 192.168.100.0/24 to any
  - ✓ 00010 deny udp from 192.168.100.0/24 to any
  - ✓ 00020 allow tcp from any to any dst-port 21 in
  - ✓ 00020 allow tcp from any to any dst-port 21 out
  - ✓ 00020 allow tcp from any to any dst-port 22 in
  - ✓ 00020 allow tcp from any to any dst-port 22 out
  - ✓ 00020 allow tcp from any to any dst-port 25 in
  - ✓ 00020 allow tcp from any to any dst-port 25 out
  - ✓ 00020 allow udp from any to any dst-port 53 in
  - ✓ 00020 allow udp from any to any dst-port 53 out
  - ✓ 00020 allow tcp from any to any dst-port 80 in
  - ✓ 00020 allow tcp from any to any dst-port 80 out
  - ✓ 00030 deny tcp from any 6667 to any in
  - ✓ 00030 deny tcp from any 6667 to any out
  - ✓ 00030 deny tcp from any to any dst-port 6667 in
  - ✓ 00030 deny tcp from any to any dst-port 6667 out
  - ✓ 00040 deny icmp from any to any via fxp0
  - ✓ 00040 deny log logamount 5 icmp from any to any via fxp0
  - ✓ 00100 allow ip from any to any via lo0
  - ✓ 00200 deny ip from any to 127.0.0.0/8
  - ✓ 00300 deny ip from 127.0.0.0/8 to any
  - ✓ 65534 deny ip from any to any
  - ✓ 65535 allow ip from any to any