iTEASY

리눅스 방화벽 등록 매뉴얼

아이티이지

서비스 운영팀

1. Linux 방화벽 사용 방법

: 리눅스에서 기본적으로 사용하는 방화벽은 iptable 입니다.

- 현재 방화벽 설정을 확인합니다.

root@ksidc# iptables -nL

```
[root@ksidc ~]# iptables -nL
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
```

: 방화벽을 사용하지 않으실 경우 위와 같은 화면이 나오십니다.

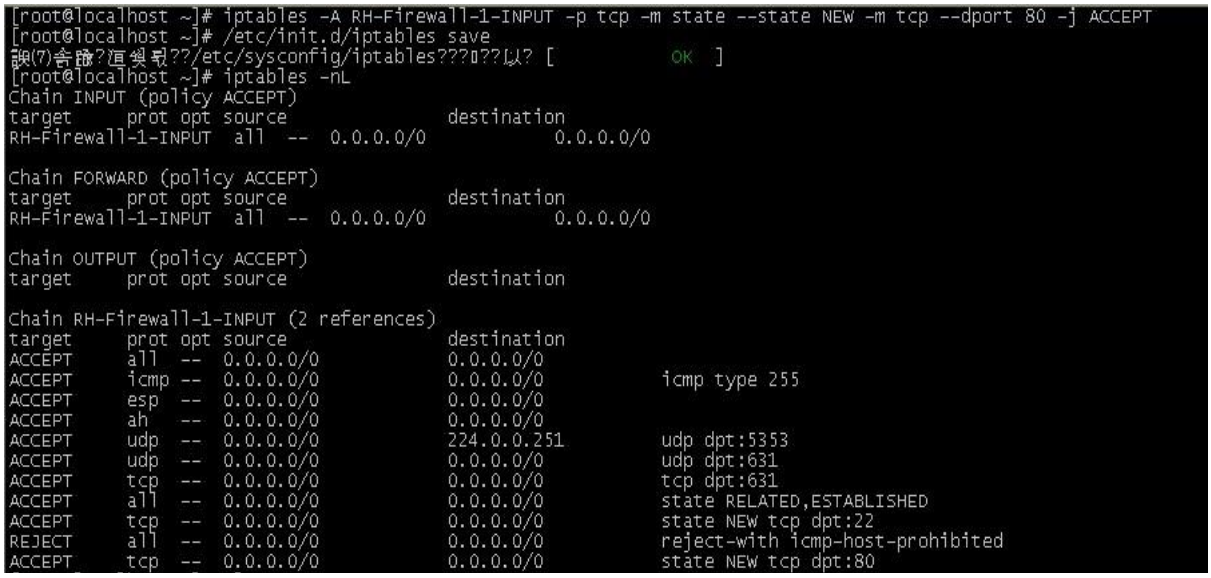
```
[root@localhost ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

: 방화벽에 등록된 포트를 확인할 수 있습니다.

: 이 경우, 등록된 포트로만 네트워크를 사용하실 수 있습니다.

- 사용할 포트 등록

root@ksidc# iptables -A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
root@ksidc# /etc/init.d/iptables save



: 명령어로 사용하시는 포트 등록 후 저장하시면 자동적으로 적용되십니다.

[iptable 룰 설정]

① -A : 체인 추가 설정 (ex. INPUT : 입력 , OUTPUT : 출력, FORWARD : 전달)
② -D : 체인 삭제 설정
③ -s : 출발지 주소
④ -d : 목적지 주소
⑤-m, -p : 사용할 프로토콜 선택 (ex. Tcp, udp)
⑥ --sport : 출발지 포트 지정
⑦ --dport : 목적지 포트 지정
⑧ -j : 규칙 설정 (ex. ACCEPT : 허용, DROP : 차단)

2. 공유형 방화벽 사용 방법

- www.ksidc.net 에 로그인 후 KS Panel에 접속

- 시스템 관리 설정 → 방화벽 관리

- 정책 적용 전 기본 정책 생성을 클릭하시면 기본적으로 사용하시는 포트가 등록되십니다. (HTTP, POP3, DOMAIN, SMTP, FTP, RED, ECHO)
- 등록된 정책 허용하기 클릭
  : 등록된 정책 허용하기를 클릭하셔야 사용하시는 포트를 등록하실 수 있습니다.
- 등록 클릭 후 사용하시는 포트 등록

: 사용하는 포트 지정 후 등록해 주시기 바랍니다.