Linux

iptables?
iptables는 Linux 시스템에서 방화벽을 구성하고 관리하는 도구

iptables를 사용하여 시스템의 네트워크 트래픽을 제어하고 보안을 강화할 수 있다.

중요: iptables를 구성할 때 주의해야 한다.
잘못된 설정은 서버에 액세스하는 데 문제가 되기도 한다.

[iptables 설치 및 활성화]
iptables 패키지가 설치되어 있는지 확인하고 없으면 설치.
대부분의 Linux 배포판에는 이미 설치되어 있다.
sudo yum install iptables

[iptables 서비스 시작]
sudo systemctl start iptables

[기본 정책 설정하기]

iptables는 입력(Input), 출력(Output), 전달(Forward) 체인에 대한 기본 정책을 설정할 수 있다.
기본적으로 모든 트래픽을 Drop 하여 거부하도록 설정하고 하나씩 필요한 규칙을 추가하여 완성하는 것이 안전합니다.

sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT DROP
sudo iptables -P FORWARD DROP

[규칙 추가 하기]
허용하려는 트래픽에 따라 규칙을 추가합니다.
[포트 추가]
sudo iptables -A INPUT -p tcp --dport 22 –j ACCEPT
SSH 포트를 예로 들었지만, 이메일, 웹, FTP 등 다른 서비스의 포트 추가도 이같이 하면 됩니다.

[규칙 저장 및 적용]
규칙을 추가한 후에는 변경 사항을 저장하고 적용해야 합니다.
sudo service iptables save # CentOS 6 이하 버전에서 사용
sudo systemctl restart iptables # CentOS 7 이상

[저장 및 적용된 규칙 확인]

sudo iptables –L -n

필요에 따라 iptables 설정을 보다 세부적으로 구성할 수 있다.
NAT(Network Address Translation)를 구성하여 내부 서버의 트래픽을 외부로 전달하거나, 특정 IP 주소 또는 대역의 트래픽을 제한하는 규칙 등을 추가할 수 있다.

iptables를 사용하여 네트워크 트래픽을 제어하면 시스템의 보안을 높일 수 있지만, 잘못된 규칙 설정으로 서버에 액세스하는 데 문제가 될 수 있기에 주의 깊게 설정해야 한다.