

발표

# 방화벽(Firewall) 과 IP 스푸핑(Spoofing)



1학년 정보보호학전공 정재성

## 목차

주제 선정 이유

방화벽

방화벽  
보안규칙

IP spoofing  
보호방법

Q&A

방화벽  
필요성

IP spoofing  
발생 이유

IP spoofing

# Firewall



정보가 돈이 되기에 이를 노리는 사람들로부터  
정보를 지키기 위한 가장 좋은 방법

‘방화벽(Fire wall)’이라는 말이 정말 신기하다.

정보보호학개론 수업때 언급이 되었다.

# Firewall



기업이나 조직의 컴퓨터 속 정보 보안을 위해  
외부에서 내부, 내부에서 외부의 정보통신망에  
불법으로 접근 하는 것을 차단하는 시스템

미리 정해진 보안규칙에 따라 들어오고 나가는  
네트워크 트래픽을 모니터링 하고 제어하는  
네트워크 보안 시스템

Traffic : 서버에 전송되는 모든 통신

## 보안 규칙

보안 규칙 : (ACL, Access Control List, 접근 제어 목록)

# Firewall

- 특정 트래픽의 접근을 허용할지 차단할지 결정하는 리스트



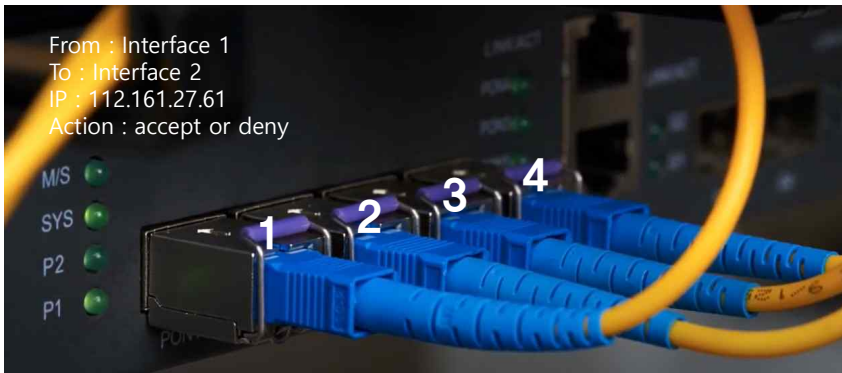
ACL의 IN, OUT



Router : 서로 다른 네트워크를 연결해주는 장치

## 보안 규칙

From : Interface 1  
To : Interface 2  
IP : 112.161.27.61  
Action : accept or deny



# Firewall



## Black List

- 모든 Traffic은 통과
  - 제어할 IP, Port 설정
- ex) 공항 검색대

## white List

- 모든 Traffic를 막음
  - 허용할 IP, Port 설정
- ex) 은행 금고

## 방화벽의 필요성

서비스 거부 공격 (Dos : Denial of Service)

패킷 가로채기 (packet sniffing)

송신측 주소 위조 (IP spoofing)

네트워크 파일 시스템 (NFS : Network File System)노출

네트워크 정보 서비스 (NIS : Network Information Service)노출

등등



## IP spoofing

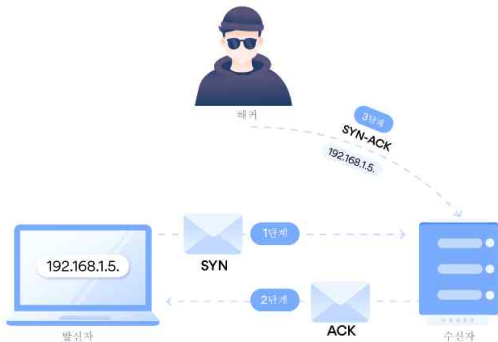
### 스푸핑

승인받은 사용자인 것처럼 시스템에 접근,  
네트워크상에서 허가된 주소로 가장하여  
접근 제어를 우회하는 공격 행위

### IP 스푸핑

특정 인물이 다른 사람의 IP를 모방하거나  
속여서 특정 대상을 공격하는 하나의  
네트워크 공격 기법

## IP spoofing 발생



- 수신자, 발신자 사이에  
신뢰관계 형성

- 후에는 아무런 제약 없이  
접근 가능

## IP spoofing 보호

! 신원이 확실하지 않은 웹사이트, 이메일, 파일 등 안전하지 않은 것들 열람 금지!

### 1. HTTPS, SSH같은 암호화된 네트워크 프로토콜을 이용하여 패킷을 암호화 하기



## IP spoofing 보호

! 신원이 확실하지 않은 웹사이트, 이메일, 파일 등 안전하지 않은 것들 열람 금지!

### 2. IP스푸핑을 감지할 수 있는 소프트웨어 설치 네트워크의 위변조 혹은 이상 감지



## IP spoofing 보호

! 신원이 확실하지 않은 웹사이트, 이메일, 파일 등 안전하지 않은 것들 열람 금지!

3. VPN로 네트워크 트래픽을 암호화하여 해커로부터  
네트워크 트래픽 / IP주소의 노출을 최소화 하기



감사합니다.

Q & A