원리를 알면 IT가 맛있다
IT COOKBOOK

# IT CookBook, 정보 보안 개론(개정판)

## [강의교안 이용 안내]

# 정보 보안 개론 개정판

한 권으로 배우는 보안 이론의 모든 것

## Chapter 10. 보안 시스템 : 시스템을 건강하게 하는 보안 시스템

한빛아카데미

# 목차

1. 인증 시스템
2. 방화벽
3. 침입 탐지 시스템
4. 침입 방지 시스템
5. VPN
6. 출입 통제 및 모니터링 장비
7. 기타 보안 솔루션

# 학습목표

- 인증 수단의 종류와 방법에 대해 이해한다.
- 생채 인식의 종류와 방법을 알아본다.
- 방화벽의 기능과 목적을 이해한다.
- VPN의 기능과 목적을 이해한다.
- 출입 통제 및 모니터링 시스템의 종류와 그 기능을 살펴본다.
- 백신 및 DRM, ESM  등의 보안 솔루션의 기능을 알아본다.
- 보안 솔루션을 이해하고, 이를 구성할 수 있다.

# 01 인증 시스템



## 인증시스템의 정의

- 인증을 하고자 하는 주체(Subject)에 대해 식별(Identification)하고, 이에 대한 인증(Authentication & Authorization) 서비스를 제공하는 시스템

## Something You Know

- 사용자가 알고 있는 정보를 이용해 인증하는 것
- 가장 기본적이고 전통적인 수단
  - » 사용자의 아이디와 패스워드를 이용한 인증이 대표적인 예
- 사용자의 기억에 의존하기 때문에 값싸고 편리하게 사용할 수 있지만, 해킹에 취약함.

## Something You Are

- 생체 조직을 통해 인증하는 방식

### 지문(Fingerprints)

- 가장 흔히 쓰이는 생체인식 수단.
- 지문 인식 시스템은 가격이 싸고 효율성도 좋으며, 사용하는 데 거부감도 거의 없는 편이라 좋음.
- 손에 땀이 많거나 허물이 잘 벗겨지는 사람은 오탐률이 높다는 단점이 있음.
- 인증을 수행하는 데 걸리는 시간은 약 3초.

[그림 10-1] 지문의 모습

## Something You Are

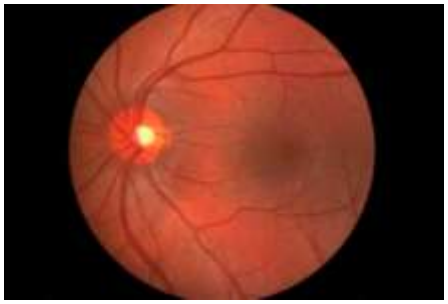
### 손 모양

- 손을 이용한 인증 시스템은 손가락의 길이와 굵기 등을 이용
- 매우 간편하고 인증 데이터의 크기가 작은 편이라 빠른 인증을 수행
- 사람들의 손 모양이 대부분 다르지만 높은 인증 수준을 가질 만큼 완벽하게 다르지는 않다는 것은 단점
- 인증을 수행하는 데 걸리는 시간은 약 3초 미만
- 손을 이용한 인식 시스템 중에는 적외선을 사용해 손 표피 가까이에 있는 정맥의 모양을 이용하는 것도 있음. 손 모양을 이용한 장비보다는 보안 수준이 높으나, 가격이 비싸고 장비가 크다는 단점이 있음.

[그림 10-2] 손 모양을 이용한 인증

## Something You Are

### 망막



[그림 10-3] 망막의 모습

- 망막(Retina) 인증은 눈 뒷부분에 있는 모세혈관의 모습을 이용하여 인증
- 정확도가 매우 높음.
- 인증에 약 10초에서 15초 가량의 시간이 걸림.
- 망막 인식은 망막에 흐르는 모세혈관의 굵기와 흐름을 통해 신분을 확인. 그래서 눈병에 걸리거나 하면 인식률이 떨어짐.
- 심장이 멎거나 죽으면 피의 흐름이 멎어 인식이 불가능해짐.
- 인식 장치에 눈을 대고 특정한 곳에 눈의 초점을 맞춰야만 하기 때문에 인증을 받으려는 의지가 없으면 인증이 불가
- 눈을 기계에 꽤 오래 대고 초점을 맞춰야 하기 때문에 거부감을 불러일으킬 수 있다는 단점이 있음.
- 안경을 쓴 상태에서는 인증을 수행할 수 없음.

## Something You Are

### 홍채

- 홍채(Iris)는 눈의 색깔을 결정하는 부분
- 홍채 인증은 망막 인증보다도 정확도가 높음.

» 인증을 수행하는 장치에 따라 다르지만, 약 50Cm 정도의 거리에서도 인증이 가능

[그림 10-4] 홍채의 모습

# 01 인증 시스템



## Something You Are

### 서명

- 외국에서 서명의 힘은 무척 커 서명을 이용한 인증 장치도 생김.
- 장비를 이용해 서명의 진위를 확인하는 것은 그다지 높은 보안 수준을 가지지 못함.

### 목소리

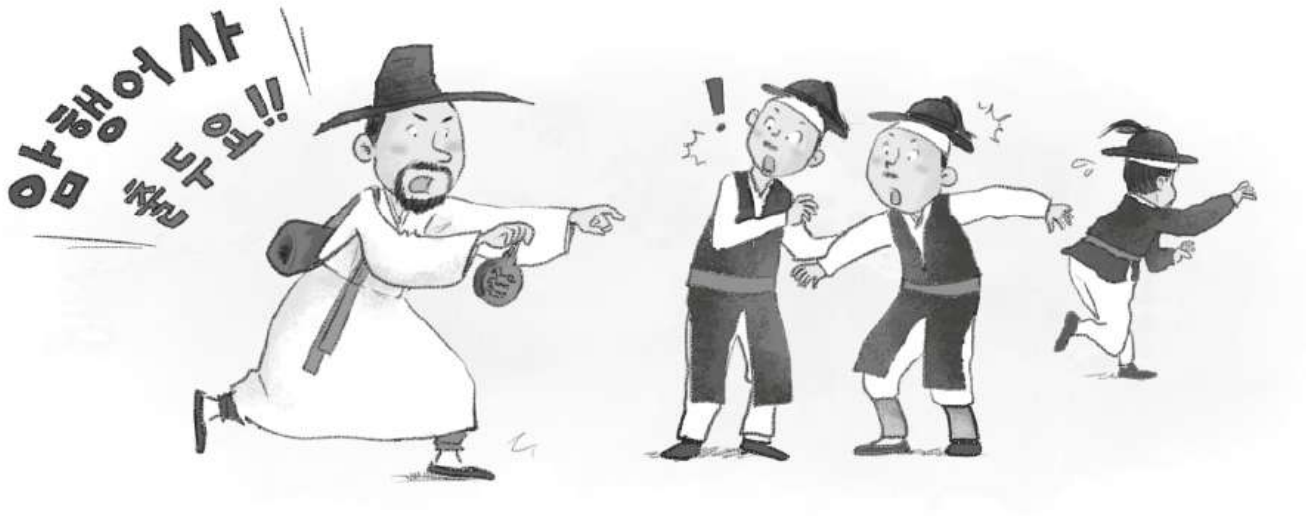
- 고유한 목소리를 이용한 인증 방법
- 원격지에서 전화를 이용할 수도 있고, 사용 방법을 따로 익히지 않아도 되는 편리함이 있음.
- 매우 저렴함.
- 음성은 환경이나 감정에 따라 변할 수 있고, 다른 이가 흉내낼 수도 있어 높은 보안 수준을 가지지는 못함.

### 얼굴

- 얼굴의 윤곽을 통해 인증을 수행.
- 현재의 기술이 다양한 표정의 얼굴을 정확히 인증하기에는 무리가 있음

## Something You Have

- 사용자가 소유한 인증 수단으로 인증하는 방식
- Something You Have 방식은 다른 사람이 쉽게 도용할 수 있기 때문에 단독으로 쓰이지 않고, 일반적으로 Something You Know나 Something You Are 방식과 함께 쓰임.




[그림 10-5] 마패로 자신을 증명하는 암행어사

# 01 인증 시스템



## Something You Have

### 스마트키 or 스마트카드

- 출입자가 카드를 소유해 출입을 허가 받았음을 인증하는 방식
- 대표적인 Something You Have를 통한 인증

### 신분증

- 본인임을 확인하기 위해 얼굴을 대조하므로 신분증은 Something You Have와 Something You Are 둘 다를 인증 수단으로 이용

### OTP

- OTP(One Time Password) 역시 Something You Have를 통한 인증

### 공인인증서

- 공인인증서는 인터넷 뱅킹이나 온라인을 통한 신용카드 거래에서 많이 사용
- 공인인증서는 Something You Have를 통한 인증인 동시에 Something You Know를 이용한 인증

# 01 인증 시스템



## Somewhere You Are

- 사용자의 위치 정보를 이용한 것
- 주로 보조 수단으로 사용됨.

### 사용자 IP

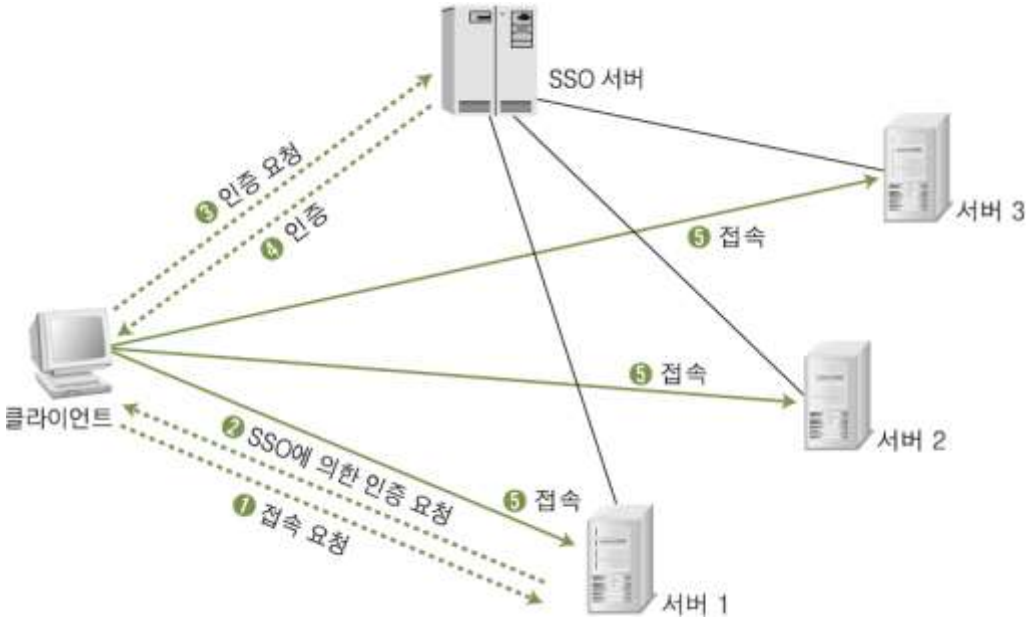
- 인터넷 게임이나 온라인 서비스 이용 시 국가마다 다른 서비스 정책을 갖고 있는 경우가 많음.
- 이때 사용자 IP를 통해 국가 간 접속을 차단하는 것은 Somewhere You Are을 이용한 인증

### 콜백(Call Back)

- 콜백은 발신자가 전화로 서비스를 요청했을 때, 우선 전화를 끊고 걸려온 번호로 전화를 되걸어 최초 발신자의 전화번호가 유효한지 확인하는 방법

## SSO(Single Sign On)

- SSO는 가장 기본적인 인증 시스템
- 모든 인증을 하나의 시스템에서 즉, 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면 다른 시스템에 대한 접근 권한도 모두 얻음.




[그림 10-7] SSO에 의한 인증

# 01 인증 시스템



## SSO(Single Sign On)

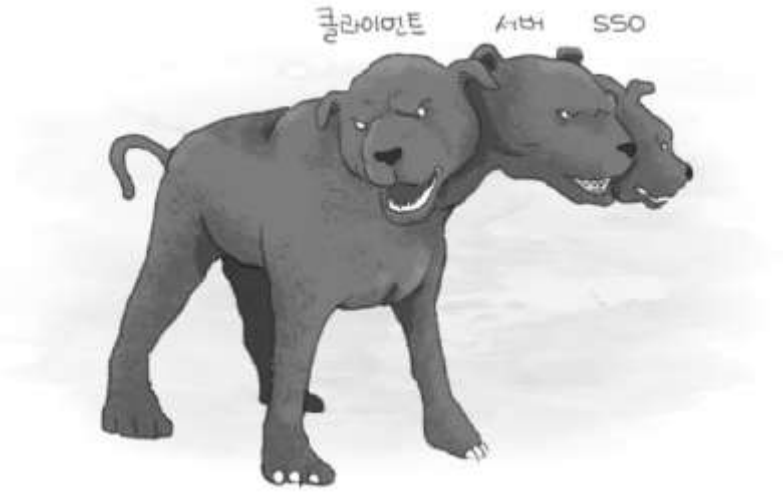
- 처음에 클라이언트가 서버에 연결을 요청하면(❶), 서버는 클라이언트로 하여금 SSO 서버로부터 인증을 받은 후 접속을 요청(❷). 클라이언트가 SSO 서버로부터 인증을 받으면(❸, ❹) SSO 서버와 연결된 서버 1, 2, 3에도 별도의 인증 과정 없이 접속할 수 있음(❺).
- 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스를 이용한 윈도우의 액티브 디렉터리(Active Directory)가 있음.

### SSO의 약점

- 최초 인증 과정을 일단 통과하면 모든 서버나 사이트에 접속이 가능해진다는 점. 이를 Single Point of Failure라 함.
- 이러한 약점을 보완하기 위해 중요 정보에 대한 접근 및 동작 시 지속적인 인증(Continous Authentication)을 하도록 되어 있음.

## SSO(Single Sign On)

- 커버로스(Kerberos)
  - 윈도우 서버에 이용되는 커버로스는 버전 5로, 10여 년 전에 MIT의 Athena 프로젝트 중에 개발됨.
  - 커버로스는 고대 그리스 신화에 나오는 지옥문을 지키는 머리 세 개 달린 개.
  - 여기에서 머리 세 개는 클라이언트와 서버, SSO를 각각 가리킴.




[그림 10-8] 커버로스

# 02 방화벽



## 방화벽의 개념

- 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷을 미리 정한 규칙에 따라 차단하거나 보내주는 기능을 하는 하드웨어나 소프트웨어
- 보안에서 방화벽은 가장 기본적인 솔루션
- 신뢰하지 않는 외부의 무차별적 공격으로부터 내부를 보호한다는 점에서 불길을 막는 방화벽과 비슷한 의미

[그림 10-9] 방화벽의 개념

## 방화벽의 주요 기능

### 접근 제어

- 관리자는 방화벽에 통과시킬 접근과 그렇지 않은 접근을 명시
- 구현 방법에 따라 패킷 필터링(Packet Filtering)방식과 프록시(Proxy) 방식으로 나뉨.
- 방화벽의 가장 기본적인 기능인 접근 제어는 룰셋(Rule Set)을 통해서 수행됨.

» 룰셋은 방화벽을 기준으로 보호하고자 하는 네트워크의 외부와 내부에 존재하는 시스템들의 IP와 포트 단위로 이루어짐.

[표 10-1] 방화벽 룰셋의 예

| 번호 | 외부(From) | | 내부(To) | | 동작 |
|---|---|---|---|---|---|
| | IP 주소 | 포트 | IP 주소 | 포트 | |
| 1 | External | Any | 192.168.100.100 | 80 | Allow |
| 2 | Any | Any | Any | Any | deny |

## 방화벽의 주요 기능

### 접근 제어

- 첫 번째 룰 셋 : 외부(External)에서 접근하는 모든 시스템에게 내부의 192.168.100.100 시스템의 80번 포트에 대한 접근을 허용(Allow)

❶허용할 서비스를 확인

❷제공하고자 하는 서비스가 보안상 문제점이 없는지와 허용이 타당한지를 검토

❸서비스가 이루어지는 형태를 확인하고, 어떤 룰(Rule)을 적용할지 구체적으로 결정

❹방화벽에 실제로 적용하고 적용된 룰을 검사

- 두 번째 룰셋 : '명백히 허용하지 않은 서비스에 대한 거부'를 적용하기 위한 것으로, 룰셋을 통해 명시적으로 허용하지 않으면 모두 차단

# 02 방화벽



## 방화벽의 주요 기능

### 로깅과 감사 추적

- 방화벽은 룰셋 설정과 변경, 관리자의 접근, 네트워크 트래픽의 허용 또는 차단과 관련한 사항을 로그로 남김.

### 인증

- 방화벽은 메시지 인증, 사용자 인증, 클라이언트 인증과 같은 방법을 사용
- 메시지 인증 : VPN(Vitual Private Network)과 같은 신뢰할 수 있는 통신선을 통해 전송되는 메시지의 신뢰성을 보장
- 사용자 인증 : 패스워드를 통한 단순한 인증부터 OTP(One Time Password), 토큰 기반(Token Base) 인증 등 높은 수준의 인증까지 가능
- 클라이언트 인증 : 모바일 사용자처럼 특수한 경우에 접속을 요구하는 호스트 자체를 정당한 접속 호스트인지 확인하는 방법

## 방화벽의 주요 기능

### 데이터의 암호화

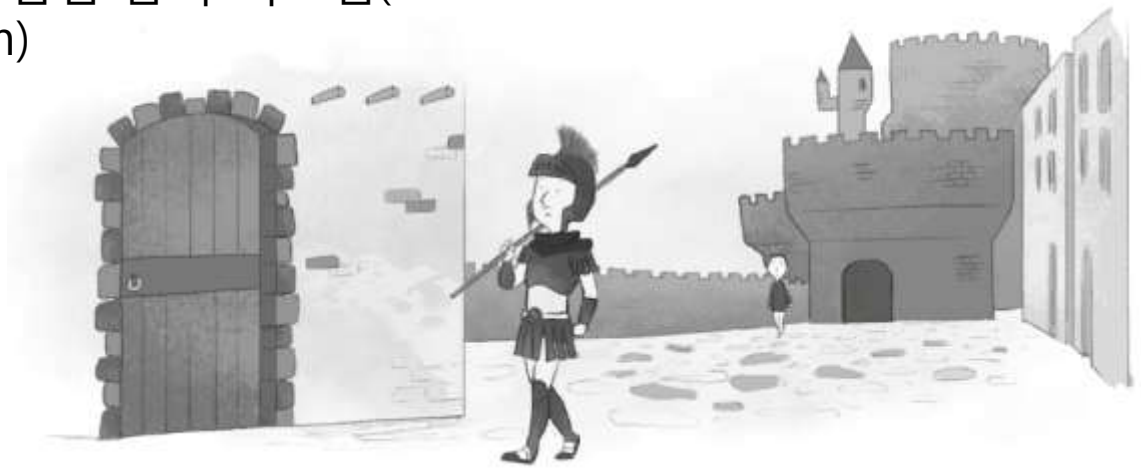
- 한 방화벽에서 다른 방화벽으로 데이터를 암호화해서 보내는 것
- 보통 VPN의 기능을 이용

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 개념

- 침입 탐지 시스템(IDS: Intrusion Detection System)은 네트워크에서 백신과 유사한 역할을 하는 것
- 네트워크를 통한 공격을 탐지하기 위한 장비
- 침입 탐지 시스템은 설치 위치와 목적에 따라 두 가지로 나뉨.
  - 호스트 기반의 침입 탐지 시스템(HIDS: Host-Based Intrusion Detection System)
  - 네트워크 기반의 침입 탐지 시스템(NIDS: Network-Based Intrusion Detection System)



[그림 10-10] 침입 탐지 시스템의 개념

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 주요 기능

### 데이터의 수집

- **HIDS**
  - » 윈도우나 유닉스 등의 운영체제에 부가적으로 설치되어 운용되거나 일반 클라이언트에 설치
  - » 운영체제에 설정된 사용자 계정에 따라 어떤 사용자가 어떤 접근을 시도하고 어떤 작업을 했는지에 대한 기록을 남기고 추적
  - » 네트워크에 대한 침입탐지는 불가능하며 스스로가 공격 대상이 될 때만 침입을 탐지할 수 있음.

- **NIDS**
  - » 네트워크에서 하나의 독립된 시스템으로 운용
  - » 감사와 로깅을 할 때 네트워크 자원이 손실되거나 데이터가 변조되지 않음.
  - » HIDS로는 할 수 없는 네트워크 전반에 대한 감시를 할 수 있으며, 감시 영역이 상대적으로 매우 큼.

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 주요 기능

### 데이터의 필터링과 축약

- "보지 않을 거면 모으지도 말라".
- 매우 방대한 데이터는 감시자를 지치게 하여 효과적인 대응을 막음.
- 따라서 침입탐지 시스템은 데이터의 효과적인 필터링과 축약이 꼭 필요
- 공격 의지를 가졌다고 생각되는 숫자만큼을 Clipping Level로 설정

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 주요 기능

### 침입 탐지

- **오용 탐지 기법(Signature Base나 Knowledge Base)**
  - » 이미 발견되고 정립된 공격 패턴을 미리 입력해두었다가 이에 해당하는 패턴이 탐지되면 알려주는 것
  - » 오판률이 낮고 효율적
  - » 알려진 공격 이외에는 탐지할 수 없고 대량의 데이터를 분석하는 데는 부적합하며 공격을 어떤 순서로 실시했는지에 대한 정보를 얻기가 힘듦.
  - » 전문가 시스템(Expert System)을 이용한 침입탐지 시스템도 이를 기반으로 함.

- **상태 전이(State Transition) 기법**
  - » 각각의 공격 상황에 대한 시나리오를 작성해두고 각각의 상태에 따른 공격을 분석.
  - » 결과가 매우 직관적이나 세밀한 시나리오를 만드는 것이 매우 어려움.
  - » 추론 엔진이 들어가기 때문에 시스템에 부하를 줄 수 있음.

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 주요 기능

### 침입 탐지

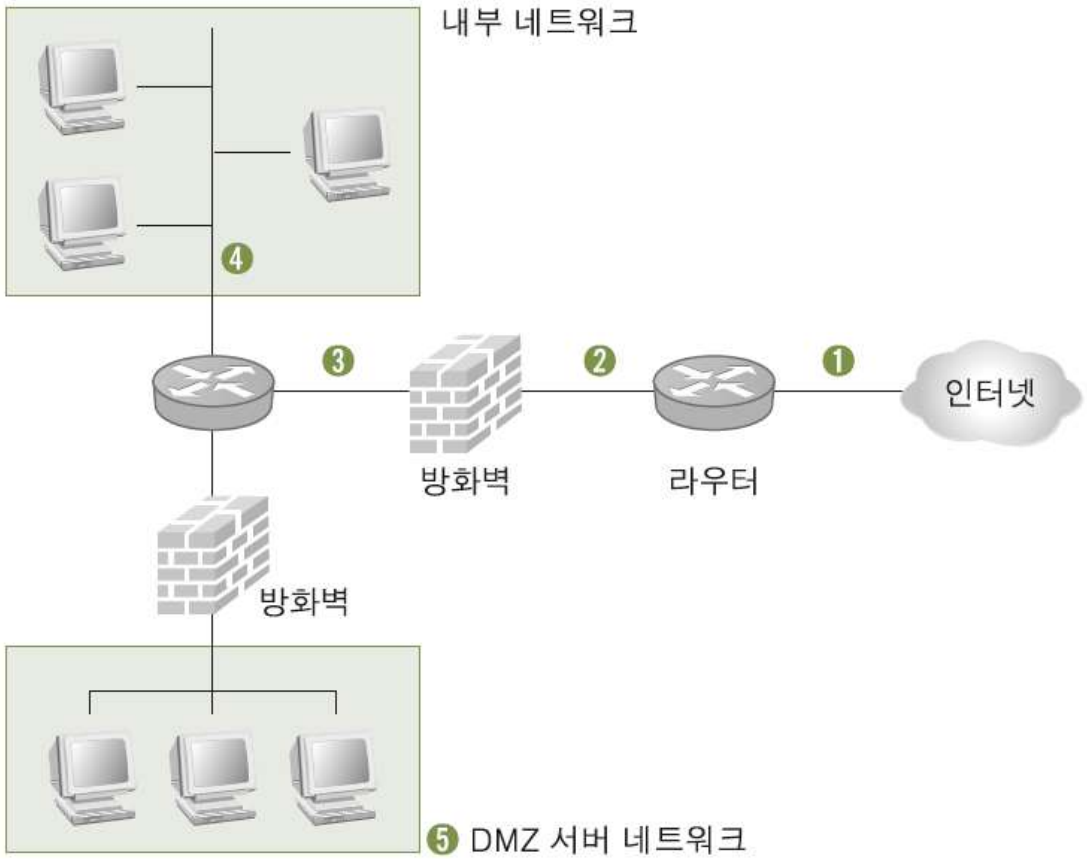
- **이상 탐지 기법 (Behavior Detection 또는 Statistical Detection)**
  - » 정상적이고 평균적인 상태를 기준으로 하여, 이에 상대적으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생하면 침입탐지를 알림.
  - » 이상 탐지 기법: 정량적인 분석, 통계적인 분석, 비특성 통계 분석 등이 있음.
  - » **인공지능 침입탐지 시스템**: 공격에 대해 스스로 판단을 하고 이에 대한 결정을 내려 알려줌. 하지만 그 판단의 근거가 확실하지 않고 오판률 역시 높음.
  - » **면역 시스템**: 새로운 공격을 당하면 그에 대해 스스로 학습해 그 공격이 다시 일어날 때 이에 대응. 재설치를 하면 최초 상태로 돌아가는 큰 단점이 있음.
  - » 인공지능과 면역 시스템은 아직 많은 상품이 개발 중 일부 상품이 나와 있으나 다른 침입탐지 시스템과 공존하는 형태로만 운용되고 있음.

- **책임 추적성과 대응**
  - » 침입탐지 시스템은 공격을 발견하면 관리자에게 알람이나 기타 방법으로 알림.
  - » 능동적인 대응을 하는 시스템은 침입차단시스템이라고 칭함.

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 설치 위치




[그림 10-11] 침입 탐지 시스템의 위치

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 설치 위치

❶ 패킷이 라우터로 들어오기 전

» 네트워크에 실행되는 모든 공격을 탐지할 수 있음. 따라서 공격 의도를 가진 패킷을 미연에 파악할 수 있음.

» 그러나 너무 많은 공격에 대한 데이터를 수집하고, 내부 네트워크로 침입한 공격과 그렇지 못한 공격을 구분하기 어렵기 때문에 공격에 효율적으로 대응하기 어려움.

❷ 라우터 뒤

» 라우터의 패킷 필터링을 거친 뒤의 패킷을 검사

» ❶의 패킷이 라우터로 들어오기 전보다 더 적은 수의 공격을, 더 강력한 의지를 가진 공격자를 탐지할 수 있음.

❸ 방화벽 뒤

» 방화벽 뒤에서 탐지되는 공격은 네트워크에 직접 영향을 주므로 탐지되는 공격에 대한 정책과 방화벽과의 연동성이 가장 중요한 부분

» 내부에서 외부로 향하는 공격도 탐지할 수 있는 곳이므로 내부의 공격자도 어느 정도 탐지할 수 있음.

# 03 침입 탐지 시스템(IDS)



## 침입 탐지 시스템의 설치 위치

❹ 내부 네트워크

» 내부의 클라이언트를 신뢰할 수 없어 이들에 의한 내부 네트워크 해킹을 감시하고자 할 때 설치할 수 있는 곳

❺ DMZ

» DMZ에 침입 탐지 시스템을 설치하는 것은 매우 능력이 뛰어난 외부 공격자와 내부 공격자에 의한 중요 데이터의 손실이나 서비스의 중단을 막기 위함임.

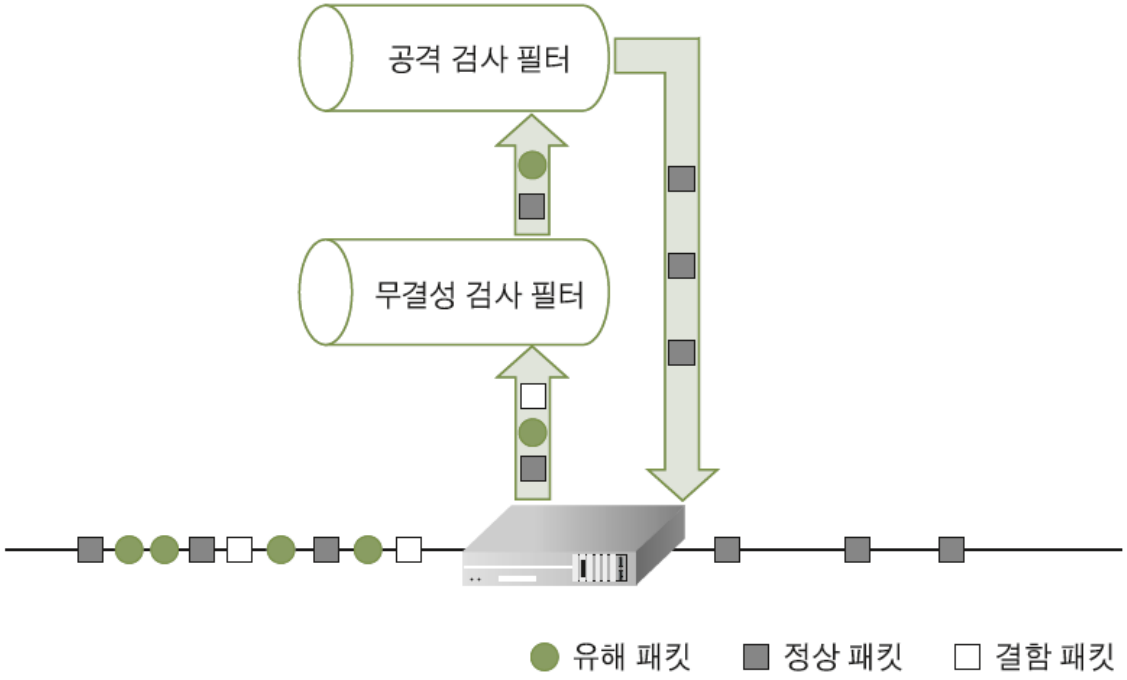
» 중요 데이터와 자원을 보호하기 위해 침입 탐지 시스템을 별도로 운영하기도 함.

# 04 침입 방지 시스템(IPS)



## 침입 방지 시스템의 동작

- 침입탐지 시스템과 방화벽의 조합으로 생각할 수 있음.
- 침입탐지 기능을 수행하는 모듈이 패킷 하나하나를 검사하여 그 패턴을 분석한 뒤, 정상적인 패킷이 아니면 방화벽 기능을 가진 모듈로 이를 차단.



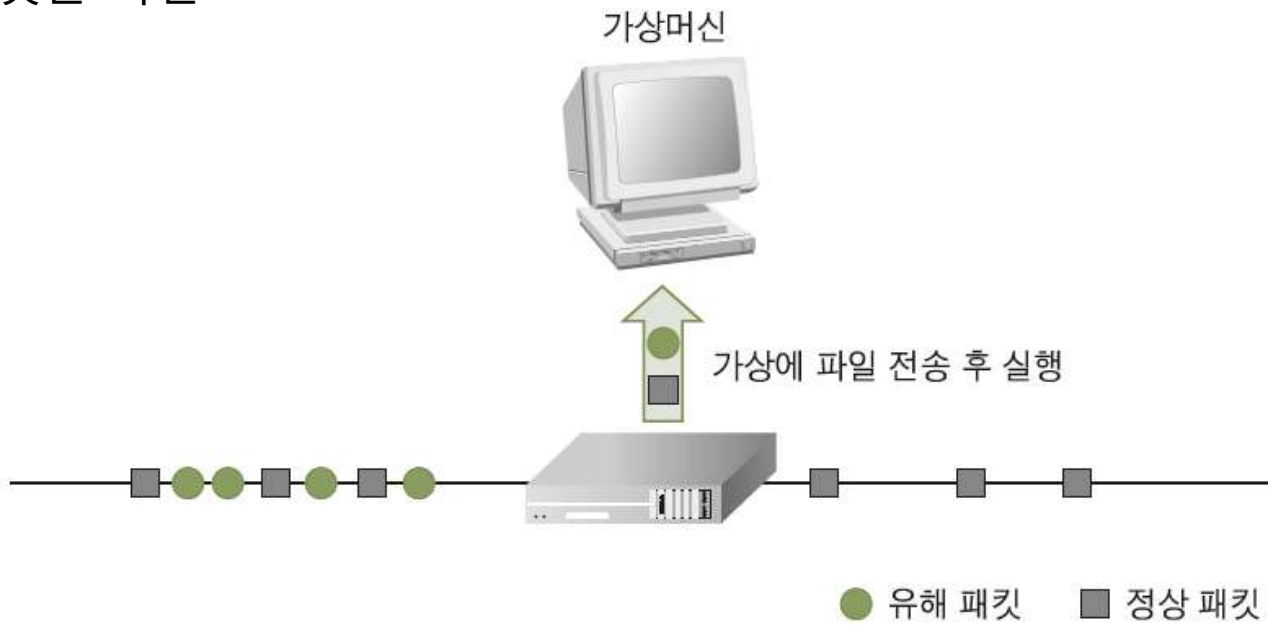

[그림 10-12] 침입 방지 시스템의 동작 원리

# 04 침입 방지 시스템(IPS)



## 침입 방지 시스템의 동작

- 최근에는 침입 방지 시스템에 가상머신(Virtual Machine)을 이용한 악성코드 탐지라는 개념을 도입하여 적용
  - 가상머신에서 실행된 코드나 패킷들이 키보드 해킹이나 무차별 네트워크 트래픽 생성과 같은 악성코드와 유사한 동작을 보이게 되면 해당 패킷을 차단



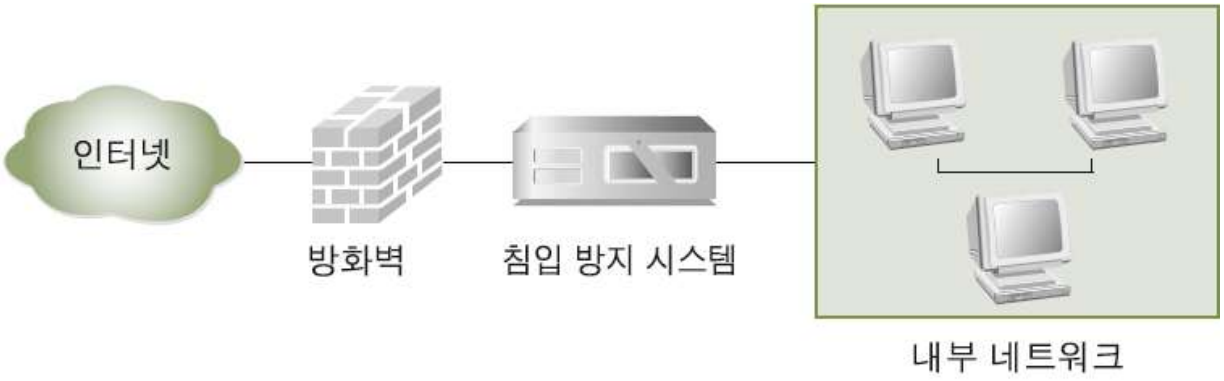

[그림 10-13] 가상머신을 이용한 침입 방지 시스템의 동작 원리

# 04 침입 방지 시스템(IPS)



## 침입 방지 시스템의 설치

- 침입 방지 시스템은 방화벽 다음에 설치
  - 방화벽이 네트워크의 앞부분에서 불필요한 외부 패킷을 한 번 걸러주어 침입 방지 시스템이 더 효율적으로 패킷을 검사할 수 있기 때문



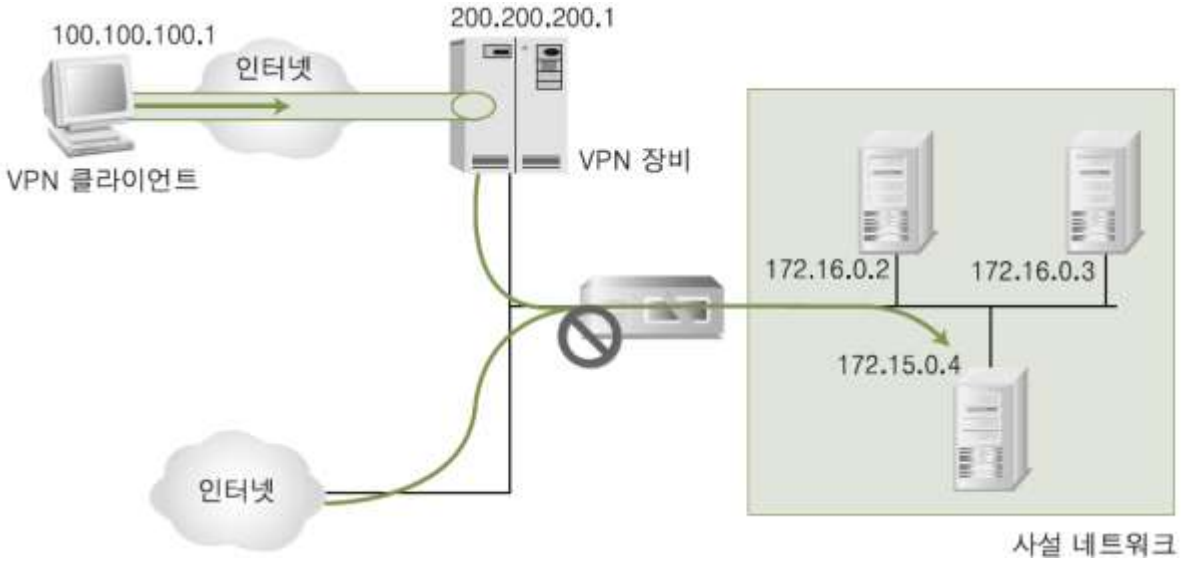

[그림 10-14] 침입 방지 시스템과 방화벽의 구성

# 05 VPN



## VPN(Virtual Private Network)

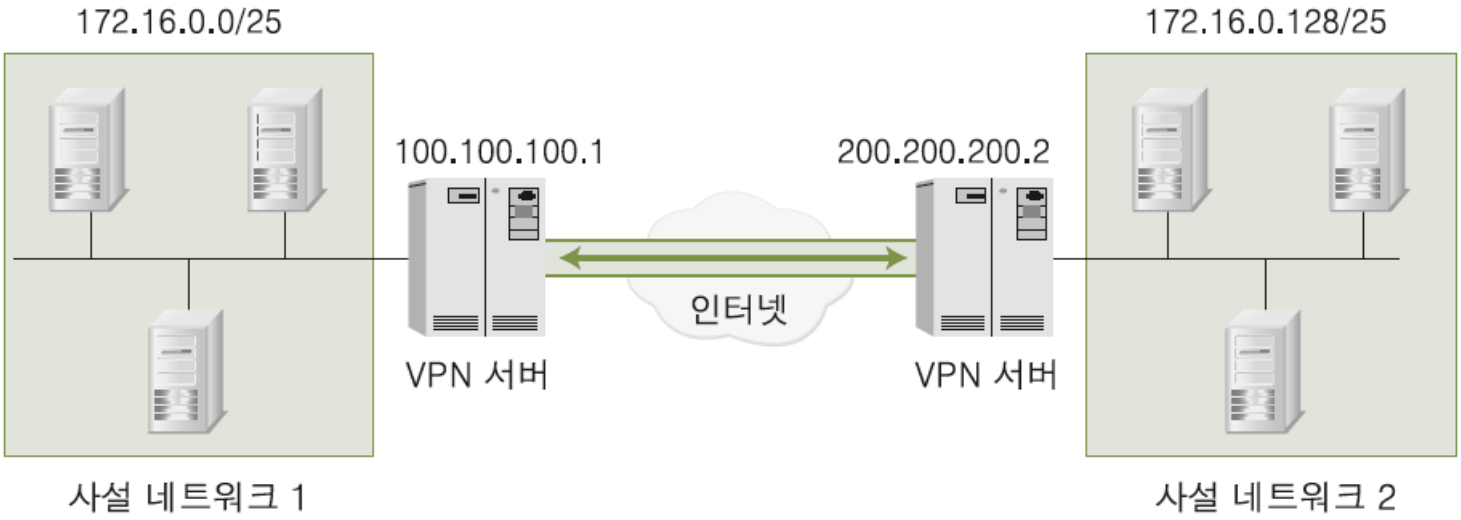
- VPN은 방화벽, 침입 탐지 시스템과 함께 현재 사용되는 가장 일반적인 보안 솔루션 중 하나
- VPN의 사용 예
  - 해외여행을 가서도 국내 온라인 게임을 할 수 있음.
  - 회사내의 서버를 집에서도 보안된 상태로 접근할 수 있음.




[그림 10-15] VPN을 이용한 외부에서의 접근

## VPN(Virtual Private Network)

- VPN의 사용 예
  - 원격의 두 지점 간을 내부 네트워크처럼 이용할 수 있음.




[그림 10-16] VPN을 이용한 터널링

# 06 출입 통제 및 모니터링 장비



## 감시 카메라

- 감시카메라를 설치할 때 확인할 사항
  - 카메라가 포착하지 못하는 사각을 확인
  - 감시 카메라에 찍힌 자료를 보관하는 방법 확인

[그림 10-17] 감시 카메라

# 06 출입 통제 및 모니터링 장비



## 엑스레이 검사기

- 반도체나 LCD와 같은 첨단 산업을 영위하는 회사의 출입구에는 엑스레이 검사기를 쉽게 볼 수 있음.
- 조그만 물건 외에도 큰 트럭이나 화물 컨테이너를 검사하기도 함.

[그림 10-18] 엑스레이 검사 장비

[그림 10-19] 엑스레이 투사 결과

# 06 출입 통제 및 모니터링 장비



## 금속 탐지기

- 출입자가 몸에 전자 장비를 지니고 출입하는 것을 통제하기 위해 많이 사용

[그림 10-20] 금속 탐지기

## 보안 스티커

- 보안 스티커는 한번 붙였다가 떼면 다시 원래 상태로 붙일 수 없게 만든 것
  - 휴대폰 카메라 부분에 붙여서 건물 내부로 들어온 사람이 휴대폰 카메라를 이용해 사진을 찍지 않았음을 확인
  - 노트북의 모니터와 본체 사이에 붙여서 노트북을 내부로 가져가 어떤 작업을 하지 않았다는 확신을 얻기 위해 사용

[그림 10-21] 보안 스티커

# 07 기타 보안 솔루션



## NAC(Network Access Control)

- NAC 시스템은 과거 IP 관리 시스템에서 발전한 솔루션
- 기본적인 개념은 IP 관리 시스템과 거의 같고, IP 관리 시스템에 네트워크에 대한 통제를 강화한 것

[표 6-1] 악성코드의 분류

| 분류 | 주요 기능 |
|---|---|
| 접근 제어/인증 | • 내부 직원 역할 기반의 접근 제어<br>• 네트워크의 모든 IP 기반 장치 접근 제어 |
| PC 및 네트워크 장치 통제(무결성 체크) | • 백신 관리<br>• 패치 관리<br>• 자산 관리 (비인가 시스템 자동 검출) |
| 해킹, 웜, 유해 트래픽 탐지 및 차단 | • 유해 트래픽 탐지 및 차단<br>• 해킹 행위 차단<br>• 완벽한 증거 수집 능력 |

# 07 기타 보안 솔루션



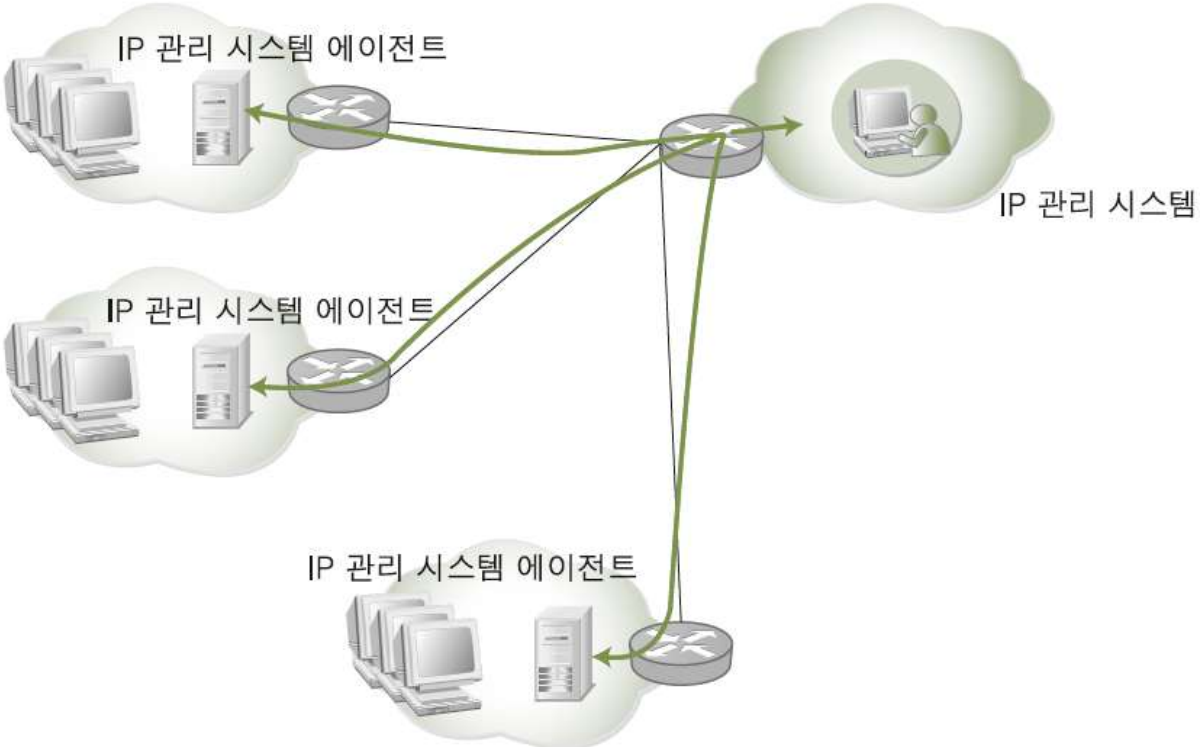
## NAC

- NAC의 접근 제어 및 인증 기능은 일반적으로 MAC 주소를 기반으로 수행됨.
- 네트워크에 접속하려는 사용자는 네트워크 접속에 사용할 시스템의 MAC 주소를 IP 관리시스템의 관리자에게 알려줘야 함.
- 관리자가 해당 MAC 주소를 NAC에 등록하면 사용자는 비로소 해당 네트워크를 사용할 수 있는 권한을 가짐.
- NAC는 등록된 MAC 주소만 네트워크에 접속할 수 있게 허용
  - 라우터로 구분된 서브 네트워크마다 에이전트 시스템이 설치되어 있어야 함.

# 07 기타 보안 솔루션



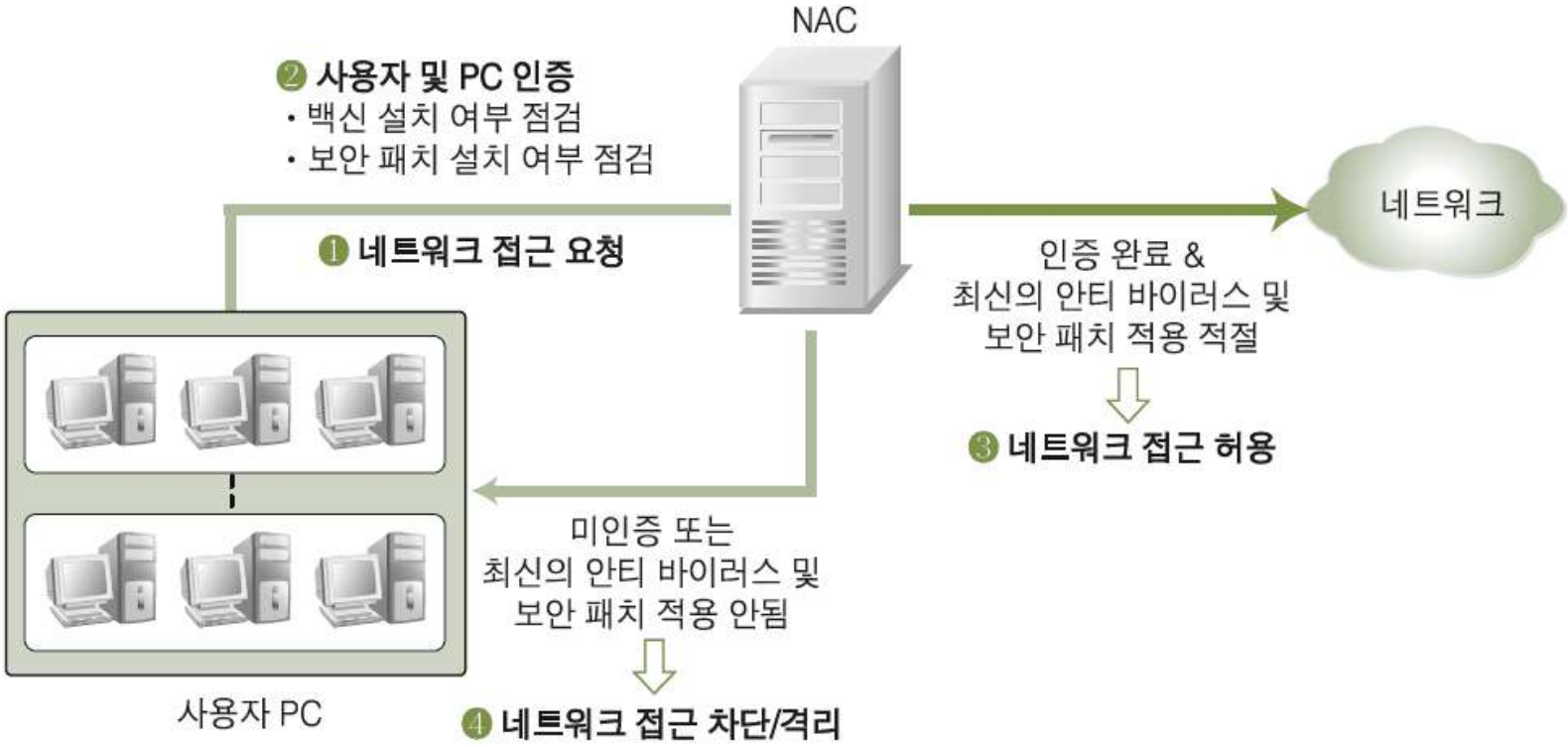
## NAC




[그림 10-22] NAC 구성

## NAC

- NAC를 통한 사용자 인증




[그림 10-23] NAC를 통한 사용자 인증 절차

# 07 기타 보안 솔루션



## NAC

- NAC를 통한 사용자 인증
  1. 네트워크 접근 요청 : 접속하고자 하는 PC 사용자는 최초 네트워크에 대한 접근을 시도
  2. 사용자 및 PC 인증 : NAC에 등록되어 있는 MAC 주소를 통해 사용자 PC를 인증하거나 SSO와 연계하여 네트

     워크에 접근하고자 하는 사용자의 아이디와 패스워드를 추가로 요청하여 인증을 수행. 인증 과정에서 백신이

     나 보안 패치의 적절성 여부를 검토
  3. 네트워크 접근 허용 : 인증이 완료된 경우 네트워크에 대한 접근을 허용
  4. 네트워크 접근 거부 : 보안 정책이 제대로 준수되지 않았거나 바이러스에 감염되어 있는 경우 네트워크 접근

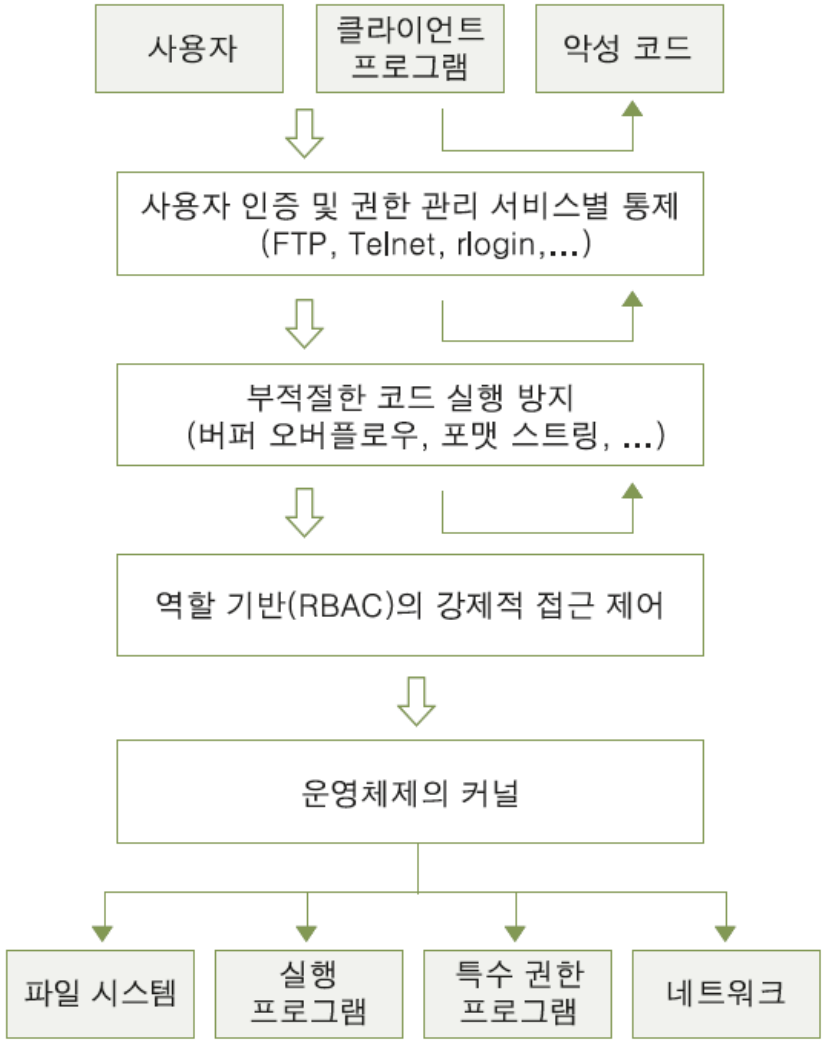
     이 거부되고, 네트워크에서 격리됨. 격리된 PC는 필요한 정책 적용이나 치료 과정을 거쳐 다시 점검

# 07 기타 보안 솔루션



## 보안 운영체제

- 보안 운영체제(Secure OS)는 운영체제에 내재된 결함으로 인해 발생할 수 있는 각종 해킹으로부터 보호하기 위해 보안 기능이 통합된 보안 커널을 추가로 이식한 운영체제.




[그림 10-24] 보안 운영체제의 구성

# 07 기타 보안 솔루션



## 백신

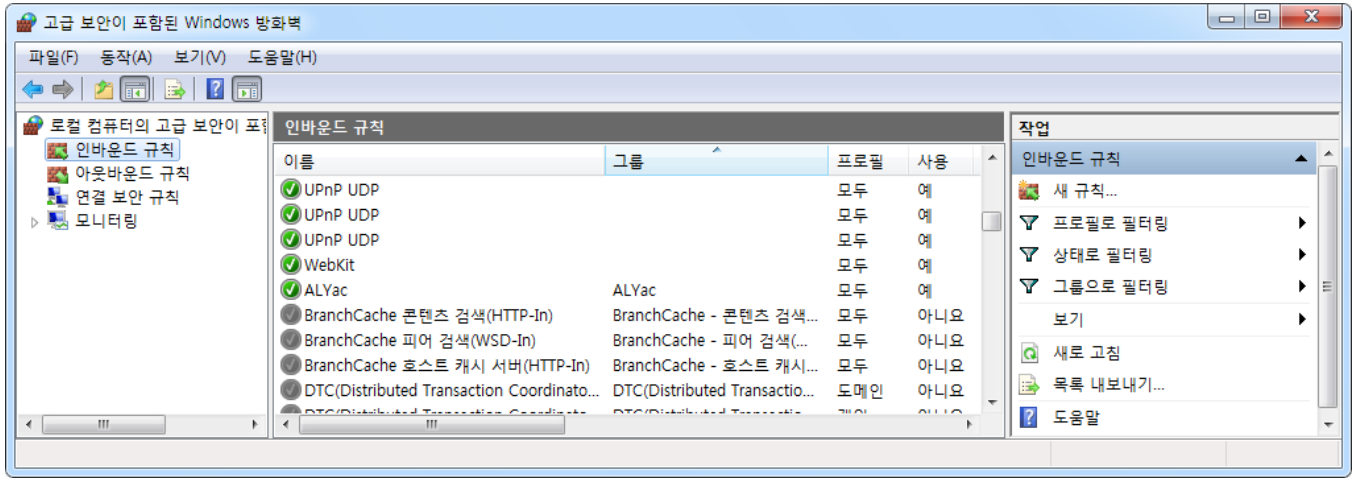
- 백신 프로그램은 시스템에 항상 상주하며 바이러스나 웜이 구동하면 이를 실시간으로 제거하는 형태로 운영
- 바이러스나 웜, 그리고 인터넷으로 유포되는 악성 코드까지 탐지하고 제거할 수 있음.

## PC 방화벽

- PC 방화벽은 네트워크상의 웜이나 공격자로부터 PC를 보호하기 위해서 사용
- PC 방화벽은 PC 내부로 유입되는 패킷뿐만 아니라 나가는 패킷까지 모두 차단하고, 사용자에게 해당 네트워크 패킷의 적절성 여부를 확인한다.
- 윈도우의 파일 공유처럼 취약점에 잘 노출되는 서비스는 기본으로 차단하기도 함.

## PC 방화벽

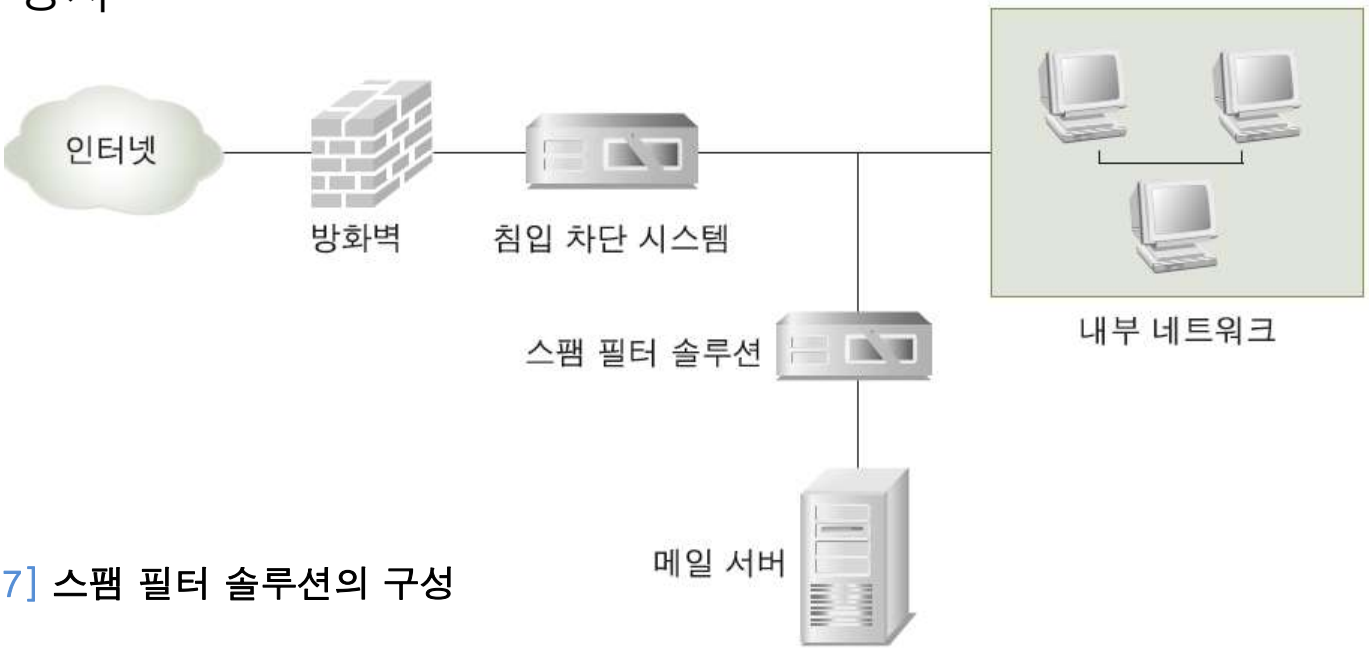
- 윈도우 방화벽에서는 일반적인 방화벽 솔루션과 같은 방식으로 외부에서 내부로 들어오는 패킷에 대한 규칙인 '**인바운드 규칙**'과 내부에서 외부로 나가는 패킷에 대한 규칙인 '**아웃바운드 규칙**'을 별도로 상세하게 통제할 수 있음.




[그림 10-25] 윈도우 방화벽 고급 설정 창[제어판]-[Windows 방화벽]-[고급설정]

## 스팸 필터 솔루션

- 스팸 필터 솔루션은 메일 서버 앞단에 위치하여, 프록시 메일 서버로서 동작
- SMTP 프로토콜을 이용한 DoS 공격이나 폭탄 메일, 스팸 메일을 차단
- 전송되는 메일의 바이러스 체크
- 내부에서 밖으로 전송되는 메일에 대한 본문 검색 기능을 통해 내부 정보 유출 방지




[그림 10-27] 스팸 필터 솔루션의 구성

# 07 기타 보안 솔루션



## 스팸 필터 솔루션

- **메일 헤더 필터링**
  - » 메일 헤더의 기본 구성 : 보내는 사람(From), 받는 사람(To), 참조자(Cc), 숨은 참조자(Bcc)
  - » 메일 헤더의 내용 중에서 ID/보내는 사람의 이름/도메인에 특정 내용이 포함되어 있는지를 검사
  - » 보낸 서버의 IP/도메인/반송 주소(Reply-to)의 유효성과 이상 유무를 검사
  - » 메일 헤더의 받는 사람, 참조자, 숨은 참조자 필드에 너무 많은 수신자가 포함되어 있는지, 존재하지 않은 수신자가 포함되어 있는지도 검사

- **제목 필터링**
  - » 메일 제목의 내용에 '광고', '섹스'와 같은 문자열이 포함되어 있는지를 검사한다.
  - » 메일을 이용한 웜은 제목에 특정 문자열이 있는 경우가 많으며, 일정 수 이상의 공백 문자열을 가지고 있다는 특징이 있어 제목 필터링을 통하면 웜을 차단할 수 있음.

# 07 기타 보안 솔루션



## 스팸 필터 솔루션

- **본문 필터링**
  - » 메일 본문에 특정 단어 혹은 특정 문자가 포함되어 있는지를 검사
  - » 메일 본문 크기와 메일 전체 크기를 비교하여 그 유효성을 검사
- **첨부파일 필터링**
  - » 첨부된 파일의 이름/크기/개수 및 첨부파일 이름의 길이를 기준으로 필터링을 수행
  - » 특정 확장자를 가진 첨부파일만 전송되도록 설정할 수 있음.
  - » 일반적으로 exe, com, dll, bat과 같이 실행이 가능한 확장자를 가진 첨부파일을 필터링함.

# 07 기타 보안 솔루션



## DRM(Digital Right Management)

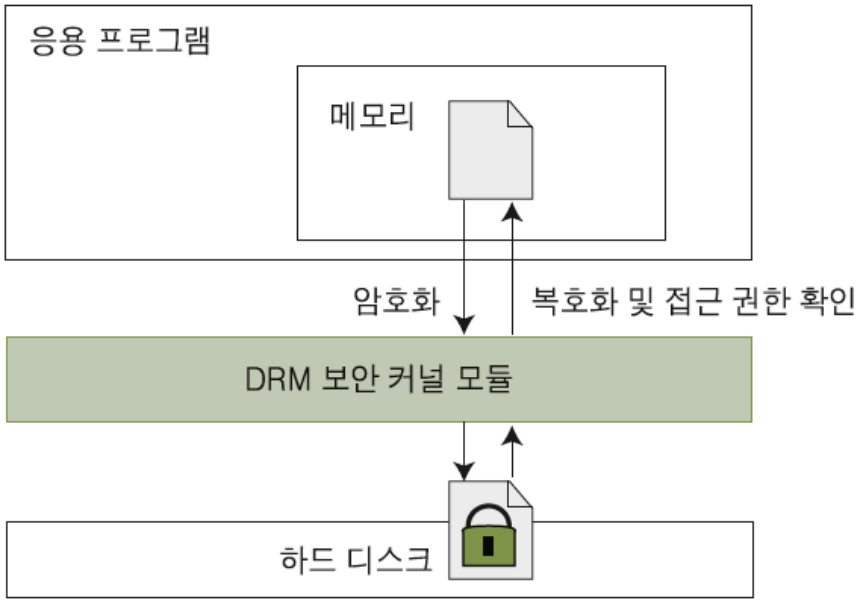
- DRM은 문서 보안에 초점을 맞춘 기술
- 문서 열람/편집/인쇄까지의 접근 권한을 설정하여 통제
- DRM은 특정한 형태의 문서만 통제하는 것이 아니라 MS워드나 HWP, TXT, PDF 파일 등 사무에 사용하는 대부분의 파일을 통제할 수 있음.
  - 사내에서 사용되는 운영체제의 커널에 DRM 모듈을 삽입.

# 07 기타 보안 솔루션



## DRM

- 커널에 삽입된 DRM 모듈은 응용 프로그램이 문서를 작성하여 하드 디스크에 저장할 때 이를 암호화하여 기록
- 응용 프로그램에서 하드 디스크에 암호화되어 저장된 파일을 읽을 때 문서를 읽고자 하는 이가 암호화된 문서를 읽을 자격이 있는지를 확인한 후 이를 복호화하여 응용 프로그램에 전달해줌.




[그림 10-28] 문서 접근 시 DRM 모듈의 역할

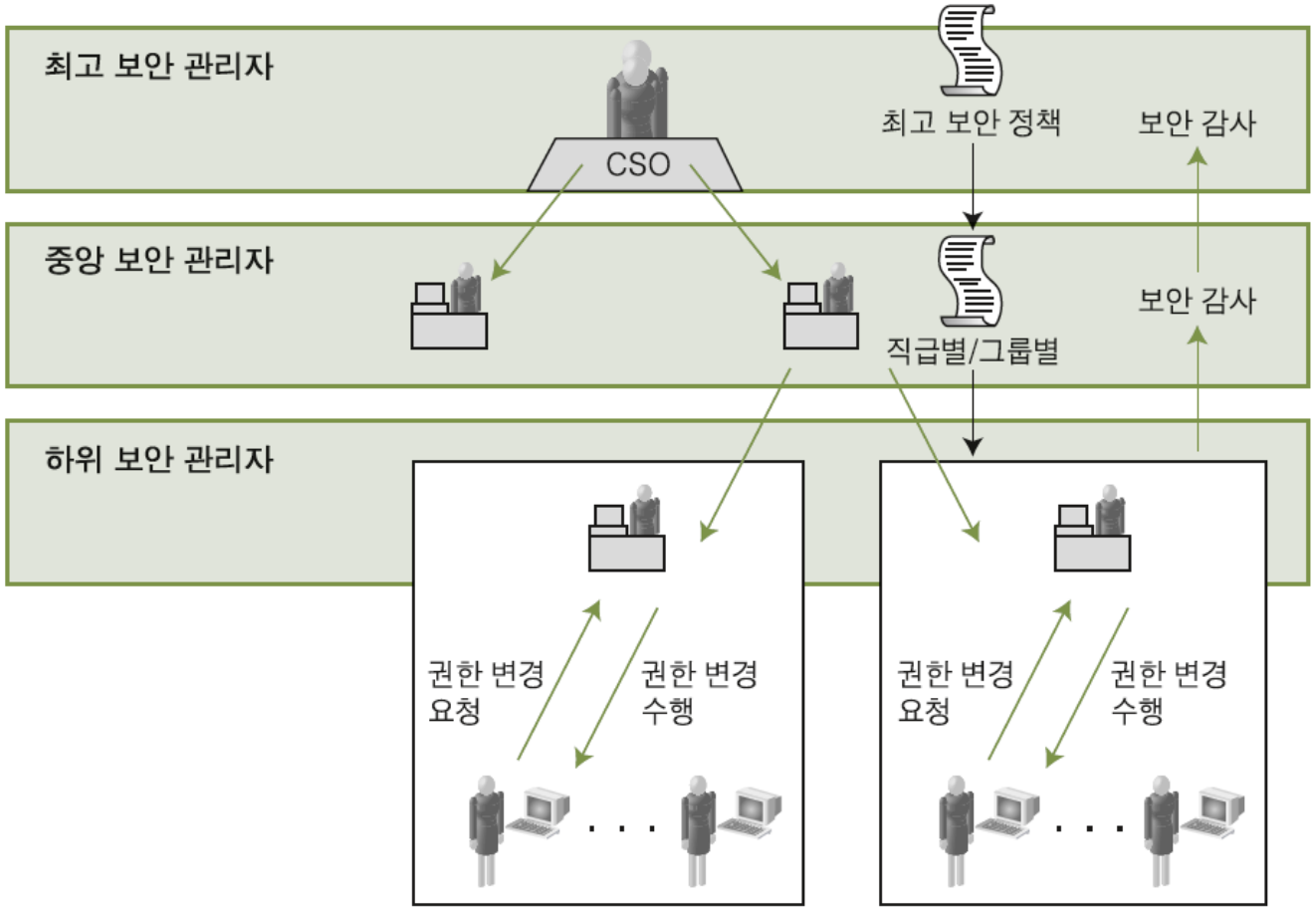
# 07 기타 보안 솔루션



## DRM 인증 체제

- DRM의 인증 체제는 인증서를 이용하는 경우가 많음.
- 각 개인이 인증서를 발급받고, 하나의 문서를 읽거나 편집할 때 그 인증서를 통해 권한을 확인받음.
- 관리자는 각각의 인증서에 대해 권한을 설정함으로써 문서에 대한 접근 권한을 설정할 수 있음.
- DRM 기술은 첨단 지식 관련 산업이나 높은 보안성이 요구되는 정부의 기관에서 사용

## DRM 인증 체제




[그림 10-29] 인증서에 의한 권한 설정 모델

# 정보 보안 개론

개정판

한 권으로 배우는 보안 이론의 모든 것