정보보안론 11주차 강의

! 시험 - 어떤 인증 수단이 가장 강력한 인증 수단 일까? !

! 시험 !

인쇄된 서명(오프라인 서명)은 위조가 가능하다.

전자 서명은 위조가 불가능하다. -> 사람마다 사인을 하는 속도와 각도가 다르다.

! 시험 – OTP의 약자 !

OTP : 1분마다 다른 패스워드를 생성하는 단말 장치

! 시험 – SSO, 커메로스 !

SSO : 가장 기본적인 인증 시스템

'모든 인증을 하나의 시스템에서'라는 목적으로 개발

시스템이 몇 대라도 한 시스템의 인증에 성공하면 다른 시스템의 접근 권한을 모두 얻는 것

커메로스 : SSO 접속 형태의 대표적인 인증 방법으로는 커베로스를 이용한 윈도우 액티브 디렉터

! 시험 !

KerBeros의 핵심 개념

1. 중앙 집중식 인증 시스템

    사용자는 한 번 로그인하면, 이후 여러 서비스에 별도 로그인 없이 접근 가능

    (Single Sign-On, SSO)

2. 비밀 키 기반 대칭 암호화 사용

    사용자와 서버 간의 통신은 암호화된 "티켓"을 통해 이루어짐

3. 티켓 기반 인증

사용자는 인증 서버로부터 "TGT"를 받고, 이를 통해 서비스 접근용 티켓을 발급 받음

4. 세 가지 주요 구성 요소

Client : 인증을 요청하는 사용자

KDC : 인증 서버 + 티켓 발급 서버

Service Server : 사용자가 접근하려는 실제 서비스

! 시험 - 방화벽의 기능 !

접근 제어 : 구현 방법에 따라 패킷 필터링 방식, 프록시 방식으로 나뉨

로깅과 감사 추적

인증

데이터 암호화

방화벽의 한계

! 시험 - 침입 탐지 시스템 설치 위치 !

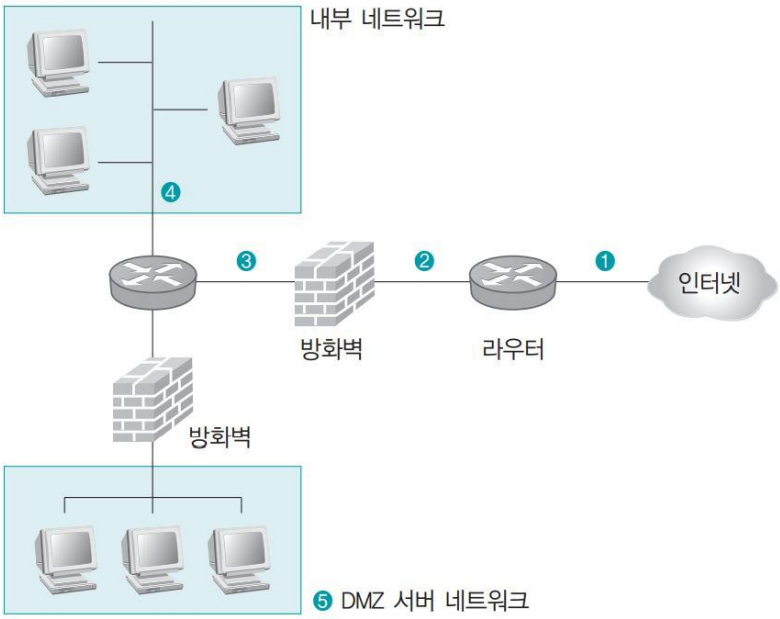

그림 9-6 침입 탐지 시스템의 위치

1번. 패킷이 라우터로 들어오기 전

- 네트워크에 실행되는 모든 공격 탐지 가능

2번. 라우터 뒤

- 라우터의 패킷 필터링을 거친 패킷 검사

3번. 방화벽 뒤 (침입탐지시스템은 3번이 제일 좋은 위치!)

- 방화벽 뒤에서 탐지되는 공격은 네트워크에 직접 영향을 주므로 공격에 대한 정책과 방화벽 연동성이 가장 중요

4번. 내부 네트워크

- 내부의 클라이언트를 신뢰할 수 없어 내부 네트워크 해킹을 감시하려 할 때 설치

5번. DMZ (침입탐지시스템은 5번이 그 다음 좋은 위치!)

- DMZ에 침입 탐지 시스템을 설치하는 이유는 능력이 매우 뛰어난 외부 및 내부 공격자에 의한 중요 데이터의 손실이나 서비스 중단을 막기 위함

침입 탐지 시스템의 설치 우선순위는 ❸ → ❺ → ❹ → ❷ → ❶

! 시험 !

VPN : 방화벽, 침입 탐지 시스템과 함께 사용되는 가장 일반적인 보안 솔루션

! 시험 - NAC (네트워크 접근 제어), NAC를 통한 사용자 인증 절차, NAC 구현 방식 !

표 9-2 NAC의 주요 기능

구분	기능
접근 제어 및 인증	• 내부 직원 역할 기반의 접근 제어 • 네트워크의 모든 IP 기반 장치 접근 제어
PC 및 네트워크 장치 통제(무결성 확인)	• 백신 관리 • 패치 관리 • 자산 관리(비인가 시스템 자동 검출)
해킹, 웜, 유해 트래픽 탐지 및 차단	• 유해 트래픽 탐지 및 차단 • 해킹 행위 차단 • 완벽한 증거 수집

NAC를 통한 사용자 인증 절차

1. 네트워크 접근 요청

2. 사용자 및 PC 인증

3. 인증 과정 중 백신, 보안 패치의 적절성 여부 검토

4. 네트워크 접근 거부

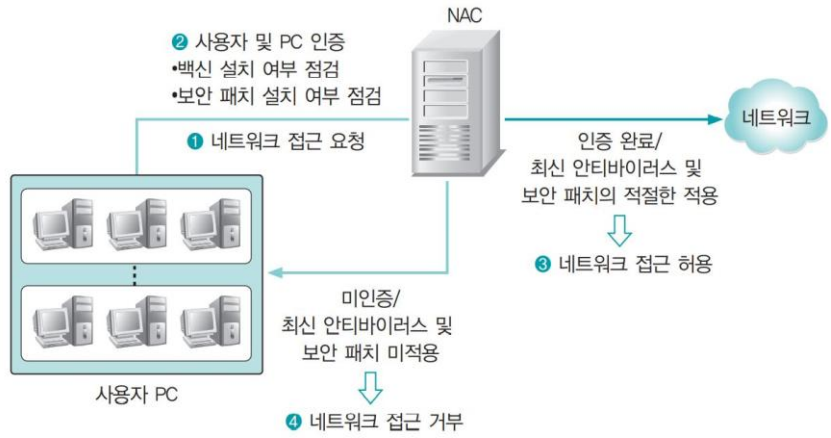

그림 9-19 NAC를 통한 사용자 인증 절차

NAC 구현 방식

인라인 방식 : NAC를 이용하여 방화벽과 같은 방식으로 접근 차단

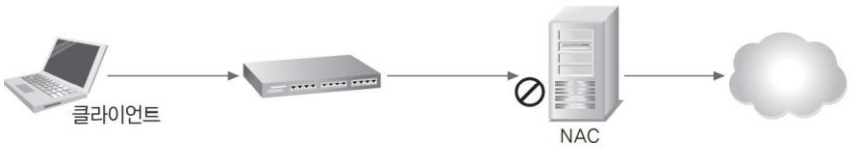

그림 9-20 인라인 방식을 이용한 NAC 구현

802.1x 방식 : 802.1x 프로토콜과 RADIUS 서버를 이용하는 것 (일반적으로 많이 사용)

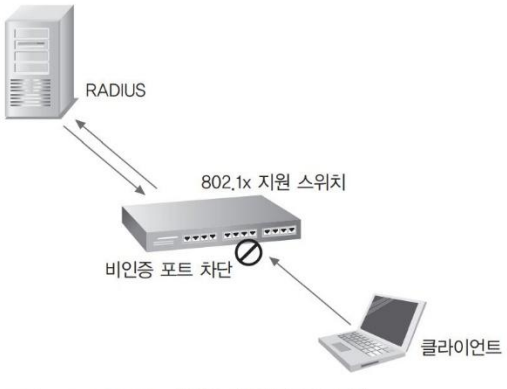

그림 9-21 802.1x 방식을 이용한 NAC 구현

VLAN 방식 : 인가받지 않은 사용자라면 VLAN으로 미리 분리된 망 중에서 통신이 되지 않는 VLAN 망에 신규 클라이언트를 할당

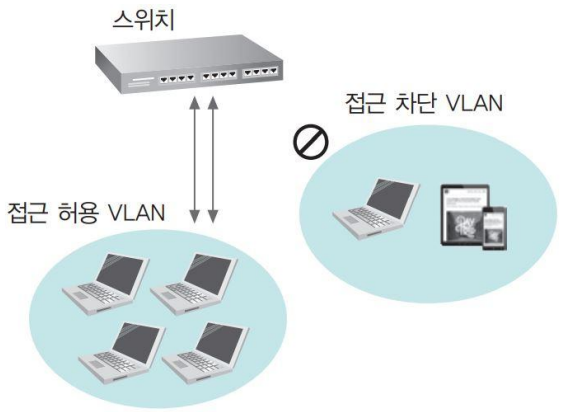

그림 9-22 VLAN 방식을 이용한 NAC 구현

ARP 방식 : 신규 클라이언트가 적법한 사용자라면 NAC가 게이트웨이의 정상적인 MAC 주소를 알림

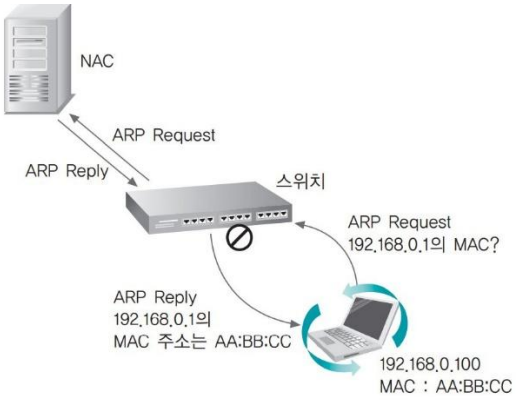

그림 9-23 ARP 방식을 이용한 NAC 구현

! 시험 !

DRM (디지털 저작권 관리) : 모든 파일, 문서 등에 디지털 워터마킹을 심어놓는 것

문서 보안에 초점을 둔 기술로 문서의 열람, 편집, 인쇄에 접근 권한을 설정하여 통제

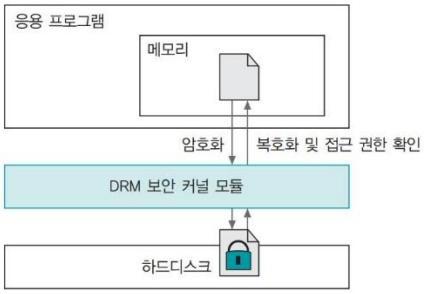

그림 9-30 문서 접근 시 DRM 모듈의 역할

! 시험 !

DLP의 핵심 목적

기밀 정보 보호 : 개인정보, 금융정보, 기업 기밀 등 민감한 데이터를 식별하고 보호

유출 방지 : 이메일, USB, 클라우드 등 다양한 경로를 통한 데이터 반출 차단

규정 준수 지원 : GDPR, HIPAA, ISO27001 등 보안 규정에 따른 데이터 보호

DLP의 적용 위치

위치	설명
네트워크 DLP	네트워크 트래픽을 분석해 외부 유출 차단
엔드포인트 DLP	PC, 노트북 등 사용자 장치에서 데이터 이동 감시
클라우드 DLP	SaaS, 이메일, 클라우드 저장소에서 데이터 보호

활용 예시

직원이 이메일로 고객 정보를 외부에 전송하려 할 때 자동 차단

USB 저장장치에 민감한 파일 복사 시 경고 또는 차단

클라우드에 기밀 문서 업로드 시 관리자 승인 필요