

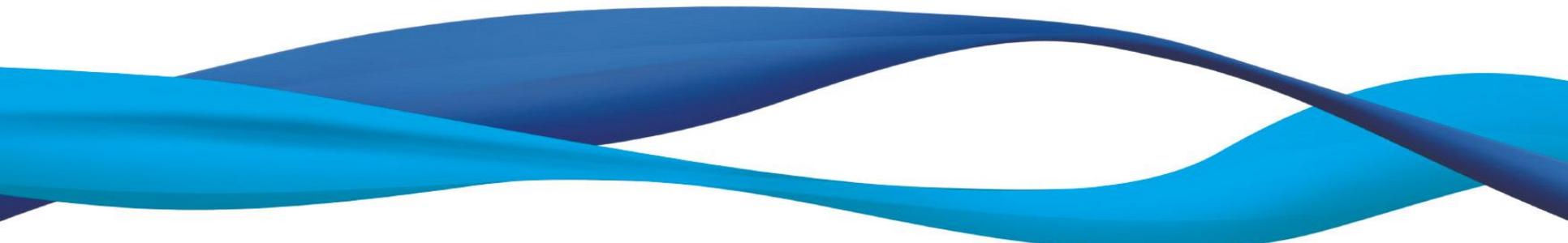
6장 네트워크보안(2)

Network Security

박종현

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr



[관련영상] 네트워크 보안 통합 솔루션

- UTM장비의 다양한 기능 (방화벽, 침입차단, 안티바이러스, VPN, 앱차단, 웹 차단, ISP백업)

<https://www.youtube.com/watch?v=Y3Q6EOQPqml>

- 안랩NW보안 - TrusGuard

<https://www.youtube.com/watch?v=8qg5dKG4A70>

- 통합된 보안 패브릭으로 더 강력하고 효율적인 플랫폼 - 포티넷

<https://www.youtube.com/watch?v=ZunZWPpAcr0>

- 한드림넷 IP통합관리 솔루션 - VIPM

<https://www.youtube.com/watch?v=fwqnuvL8N6A>

7. 기타 보안 시스템

- VPN
- UTM
- NGFW
- NAC
- 보안OS
- 블루투스

본 교재

양대일, 정보보안개론(개정4판),
한빛아카데미, 2021

6-7 기타 보안 시스템

• VPN

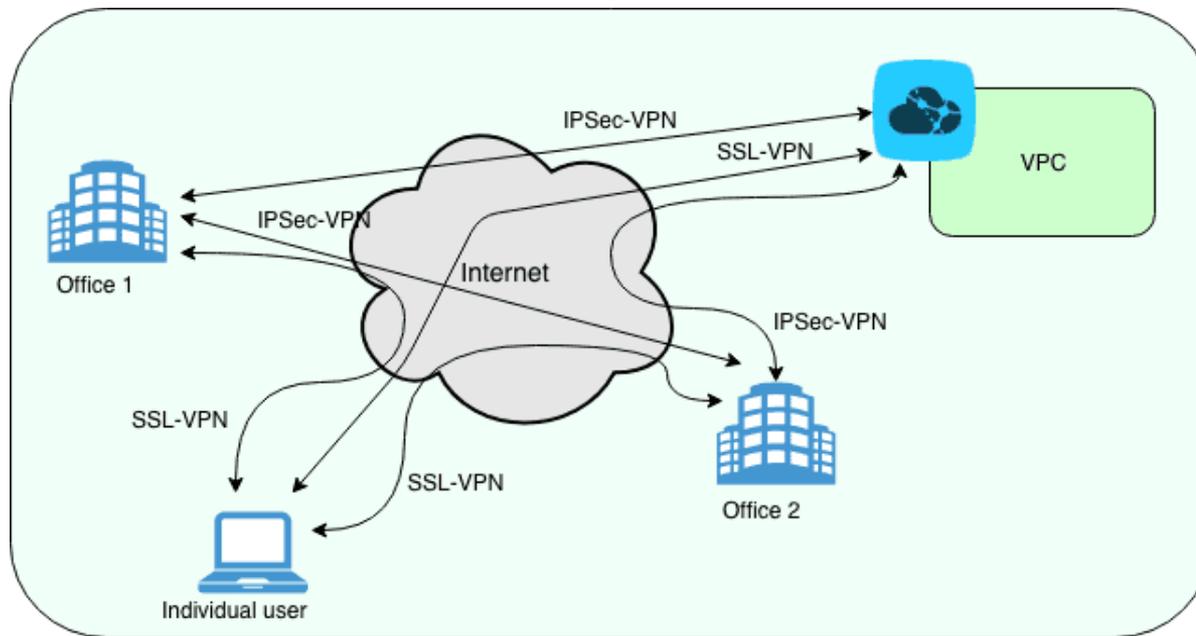
- VPN(Virtual Private Network): 가상사설망
- 방화벽, 침입 탐지 시스템과 함께 사용되는 가장 일반적인 보안 솔루션
- 기존의 인터넷 서비스를 통해 하나의 사설 네트워크처럼 사용하는 가상 사설망
- 터널링 프로토콜과 보안 과정을 거쳐 내부 기밀을 유지
- 기업 내부의 네트워크에서 주고받는 데이터는 외부로 유출되면 안 되는 경우가 많음
 - . 기업 내의 데이터 통신에는 인터넷과 구분된 별도의 임대 회선(leased line)을 사용

• VPN 터널을 위한 프로토콜

- 2계층: PPTP(Point to Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol), L2F(Layer 2 Forwarding Protocol)
- 3계층: SSL(Secure Sockets Layer)

• VPN의 용도

- ✓집에서도 회사 내의 서버에 보안 상태로 접근하는 경우
- ✓원격의 두 지점을 내부 네트워크처럼 이용하는 경우
- ✓해외여행 중 국내 온라인 게임에 접속하는 경우



• VPN 기능

- ✓ 보안 강화: 인터넷 연결을 암호화하여 해킹과 도청을 방지
- ✓ 개인 정보 보호: IP 주소를 숨겨 온라인 활동의 익명성 확보
- ✓ 지역 제한 우회: 특정 국가에서만 접속 가능한 콘텐츠나 서비스에 접근 가능
- ✓ 업무용 원격 접속: 외부에서 안전하게 기업 내부 네트워크 접근
- ✓ 속도 최적화: ISP 속도 제한 우회로 스트리밍 및 다운로드 최적화
- ✓ 안전한 파일 공유: 토렌트 사용 시 IP 보호 및 개인정보 보호

• VLAN (Virtual Local Area Network)

- VLAN을 이용할 때 네트워크 관리자는 네트워크를 작은 네트워크로 나눔
- VLAN은 ACL(Access Control List)을 통해 접근 통제 가능, 악성 코드 발생시 범위 제한 가능
- VLAN은 스위치에서 설정하며 포트별로 구분
- 통신을 위한 절차

① 패킷 전송

- 클라이언트가 스위치에 프레임을 전달하면 스위치는 클라이언트가 속한 VLAN을 표시하기 위해 전송받은 프레임에 VLAN 정보 붙임

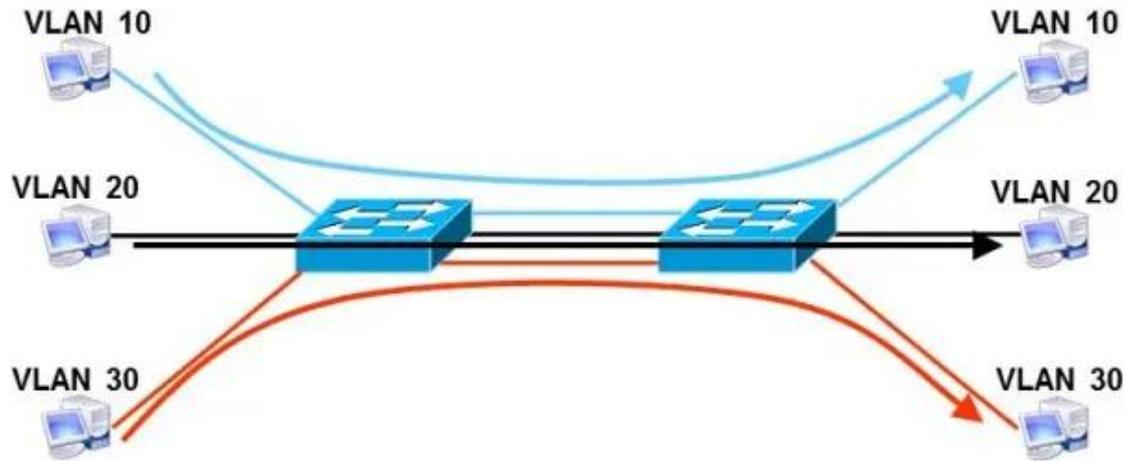
② 패킷 수신

- 프레임을 스위치 밖으로 보내기 전에 프레임의 VLAN 정보와 스위치 포트의 VLAN 정보 비교
- 두 정보가 같으면 프레임에 붙어 있는 VLAN 정보를 떼어내고 프레임만 전송
- 다른 VLAN으로 프레임을 보낼 때는 해당 포트의 VLAN과 프레임에 추가된 VLAN이 다르므로 프레임 차단

③ 스위치 간의 VLAN 통신

- 2개 이상의 스위치에서 VLAN 간 통신을 하려면 여러 개의 VLAN 프레임을 전송할 수 있는 트렁크(trunk) 포트 이용

■ VLAN 구성 예시

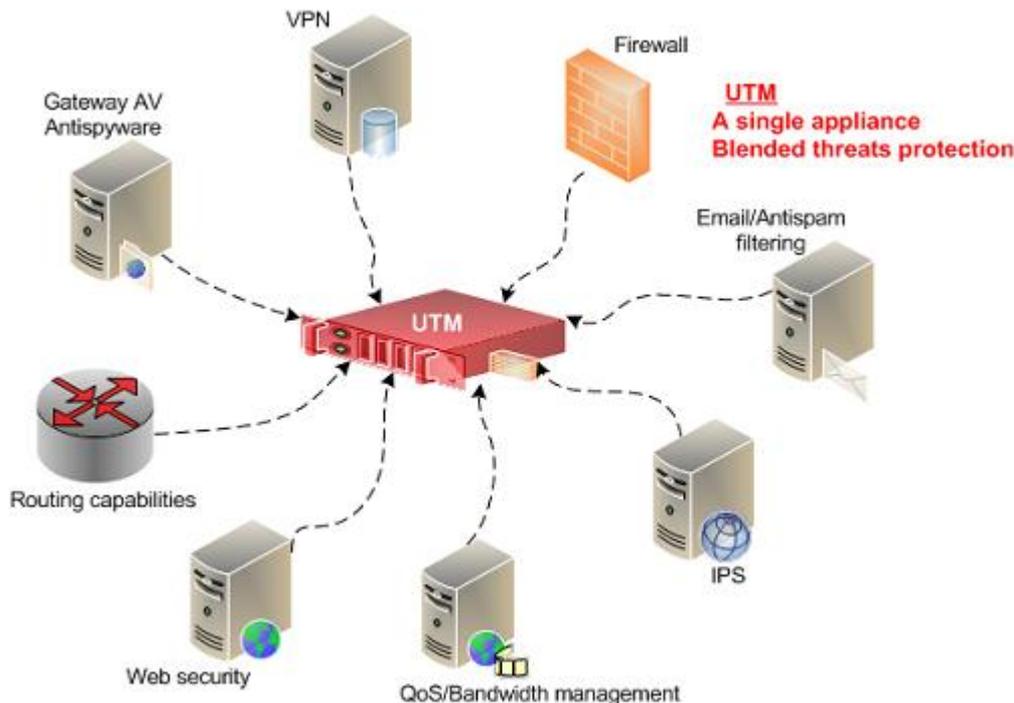


• VLAN의 스위치 구현 방법 예

- Port 기반 - 스위치 포트별 VLAN 고정 (가장 단순한 방식)
- MAC address 기반 - MAC 주소로 VLAN 구분, 이동해도 동일 VLAN 유지
- Network layer protocol 기반 - IP/프로토콜 종류에 따라 VLAN 분리
- IP multicast 기반 - 멀티캐스트 그룹 기준 VLAN 구성
- Policy 기반 - 정책(사용자, 시간 등)에 따라 VLAN 동적 할당
- 사용자 정의 기반 - 관리자가 임의 기준으로 직접 VLAN 구성

통합보안시스템(UTM)

- UTM (Unified Threat Management) / 통합위협관리: 방화벽 기반의 VPN, IPS, 웹 필터링, 안티바이러스, 트래픽 관리 등 다양한 기능을 통합해 지원하는 통합 위협 보안 관리 시스템



- 장점
 - 유연성 및 적응성
 - 중앙 집중식 통합 및 관리 - 장점: 업데이트 / 점검, 단점: 네트워크구조가 중앙 집중형이 아닌 경우 다중모듈공격 방지의 어려움
 - 비용 효율성
- 차세대 방화벽과 비교 필요

차세대 방화벽 (NGFW: Next Generation Firewall)

• 차세대 방화벽 기능

- 애플리케이션 인식
 - ✓ 포트 + 어플리케이션 기반으로 트래픽을 필터링하고 복잡한 규칙 적용 → NGFW의 핵심기능
: 특정 애플리케이션의 트래픽 차단 및 개별 애플리케이션 제어
- 심층 패킷 검사
 - ✓ 패킷에 포함된 데이터 검사
 - ✓ 패킷의 IP 헤더만을 검사하여 소스와 대상을 확인하는 기존의 방화벽 기술보다 개선
- 침입 방지 시스템(IPS)
 - ✓ 네트워크의 악성 활동을 모니터링하여 이러한 활동이 발생하는 위치에서 차단
 - ✓ 시그니처 기반, 정책 기반, 또는 이상 행위 기반 운영
- 고성능
 - ✓ 속도 저하 없이 막대한 양의 네트워크 트래픽을 모니터링
- 외부 위협 인텔리전스
 - ✓ 네트워크와 통신하여 위협에 대한 정보를 최신 상태로 유지하고 악성 행위자를 파악

UTM과 NGFW의 차이

	UTM (Unified Threat Management)	NGFW (Next Generation Firewall)
구성요소	<ul style="list-style-type: none"> FW + IPS/Anti-DDoS+AV/AS+IPSecVPN +WebFilter 	<ul style="list-style-type: none"> UTM +애플리케이션제어+사용자 기반제어+DLP + SSL Inspection + SSL VPN + Anti-APT+Etc.
트래픽 제어	<ul style="list-style-type: none"> 정적 정보인 IP, Port 기반의 제어 Layer-4까지 제어 	<ul style="list-style-type: none"> 동적 정보인 애플리케이션, 사용자 기반의 제어 Layer-7 까지 제어
주요 특징	<ul style="list-style-type: none"> 암호화 트래픽 제어 불가 고도화된 위협에 대한 탐지/제어 불가 	<ul style="list-style-type: none"> 암호화 트래픽 제어 가능(w/SSL Inspection) 고도화된 위협에 대한 탐지/제어 가능 <ul style="list-style-type: none"> - 외부 기능과의 연동을 통해 제공
정보 가시성 (Visibility)	<ul style="list-style-type: none"> 단순/나열식 형태의 모니터링 정보 정보의 판단/분석은 100% 관리자의 몫 	<ul style="list-style-type: none"> 상관 분석, Drill-Down 형태 등의 모니터링 정보 정보의 판단/분석을 일정 부분 장비 자체적으로 수행하여 관리자 판단이 용이한 형태로 제공
관리 편의성 (Manageability)	<ul style="list-style-type: none"> 설정 추가/수정 등의 기본적인 편의성 	<ul style="list-style-type: none"> 정책/객체에 대한 고도화된 편의성 제공 다양한 부가 기능 제공 <ul style="list-style-type: none"> - 미사용/미참조 정책 검색, 중복 정책 검색 등

(출처: 안랩)

기타 통합보안 솔루션 개념

솔루션	목적	기능
SIEM (Security Information & Event Management)	보안 이벤트 및 경고 관리	<ul style="list-style-type: none"> - 실시간 로그 수집 및 분석 - 이상 징후 탐지 - 조기 보안 사고 발견
EDR (Endpoint Detection and Response)	엔드포인트 보안 강화	<ul style="list-style-type: none"> - 실시간 악성 코드 탐지 - 비정상 활동 모니터링 - 포렌식 데이터 수집 및 자동 대응
SOAR (Security Orchestration, Automation, and Response)	보안 도구 통합 및 자동화	<ul style="list-style-type: none"> - 사건 발생 시 신속 대응 - 보안 팀의 효율성 증대 - 인시던트 대응 시간 단축

- SOA SOAR (Security Orchestration, Automation, and Response)

- 보안 오케스트레이션(Orchestration) + 자동화(Automation) + 대응(Response)
- 대규모 조직의 보안 운영센터(SOC)에서는 수많은 경고(alerts)와 여러 보안 도구가 존재하며, 수작업 조사에 많은 시간이 소요
- 여러 보안 도구를 통합하고 반복적인 작업을 자동화하며, 경고 대응 워크플로우를 중앙에서 관리 ==> 평균 탐지 시간(MTTD) 및 평균 대응 시간(MTTR) 을 단축하고 전체 보안 태세(Security Posture)를 개선
- 더 많은 경고를 더 짧은 시간에 처리 가능
 - 경고 피로(Alert Fatigue) 감소
- 일관성 있는 대응 프로세스 수립 가능
 - 사례별 대응이 아닌 표준화된 플레이북 활용
- SOC 의사결정역량 강화
 - 중복·오탈(誤脫) 경고 감소, 우선순위화 강화
- 분석가 및 관련 부서(HR, 법률, 집행기관 등)와의 협업 체계 개선

• SOA 참고 사례

- 차세대 위협대응을 위한 스마트의료 보안 세미나] 보안 운영 자동화 플랫폼 SOAR 소개 및 데모
- <https://www.youtube.com/watch?v=i0F59helEBw&t=476s>
[13:32~26:17]

- **NAC**

- NAC(Network Access Control) : 네트워크에 접근하는 접속단말의 보안성을 강화할 수 있는 보안 인프라 (하드웨어 및 소프트웨어)
- IP 관리 시스템에서 발전한 솔루션

- **도입 배경**

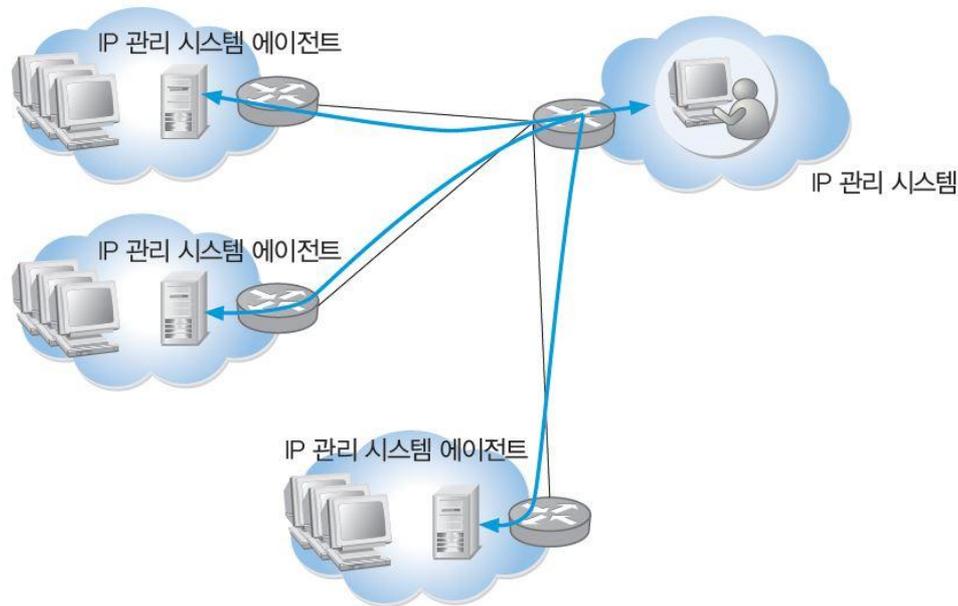
- 모바일 환경의 일반화
- 접속단말의 다양화
- 내부 보안관리의 필요성 증가

- NAC 주요 기능

구분	기능
접근 제어 및 인증	<ul style="list-style-type: none"> • 내부 직원 역할 기반의 접근 제어 • 네트워크의 모든 IP 기반 장치 접근 제어
PC 및 네트워크 장치 통제(무결성 확인)	<ul style="list-style-type: none"> • 백신 관리 • 패치 관리 • 자산 관리(비인가 시스템 자동 검출)
해킹, 웜, 유해 트래픽 탐지 및 차단	<ul style="list-style-type: none"> • 유해 트래픽 탐지 및 차단 • 해킹 행위 차단 • 완벽한 증거 수집

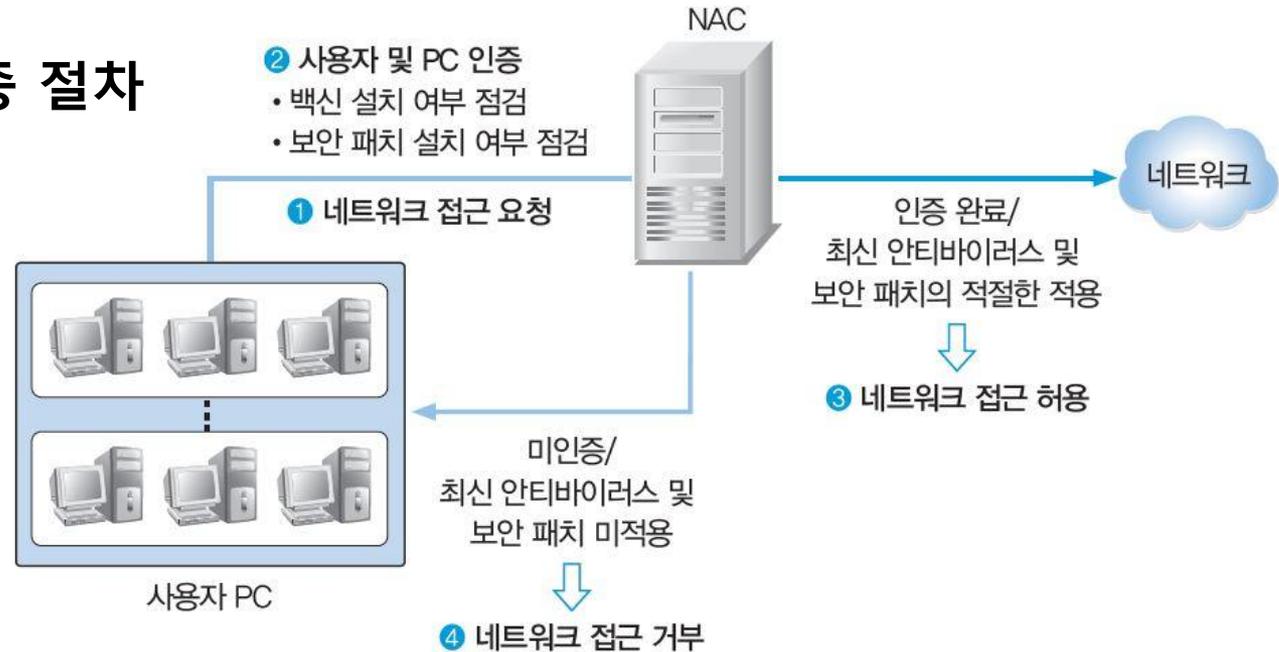
[NAC의 주요 기능]

- 접근 제어 및 인증 기능은 **MAC 주소를 기반으로** 수행
- NAC는 등록된 MAC 주소만 네트워크에 접속할 수 있게 허용
- 라우터로 구분된 서브 네트워크마다 에이전트 시스템이 설치되어야 함



[NAC의 구성]

• NAC 사용자 인증 절차



- ① 네트워크 접근 요청: 접속하려는 PC 사용자가 네트워크에 대한 접근을 처음 시도
- ② 사용자 및 PC 인증
 - NAC에 등록되어 있는 MAC 주소로 사용자 PC 인증
 - SSO와 연계하여 네트워크에 접근하는 사용자의 아이디와 패스워드를 추가로 요청하여 인증 수행
 - . 인증 과정 중 백신, 보안 패치의 적절성 여부 검토
- ③ 네트워크 접근 허용: 인증이 완료되면 네트워크 접근 허용
- ④ 네트워크 접근 거부
 - 보안 정책을 제대로 준수하지 않거나 바이러스에 감염되었을 때는 네트워크 접근이 거부되고 네트워크에서 격리됨
 - 격리된 PC는 필요한 정책 적용이나 치료 과정을 거친 후 다시 점검

• NAC 구현 방식

- 인라인 방식

- ✓ NAC를 이용하여 방화벽과 같은 방식으로 접근 차단
- ✓ 게이트웨이 형태로 일부 물리적 네트워크에 NAC를 추가하는 것으로, 기존 네트워크 변경을 최소화하여 적용 가능

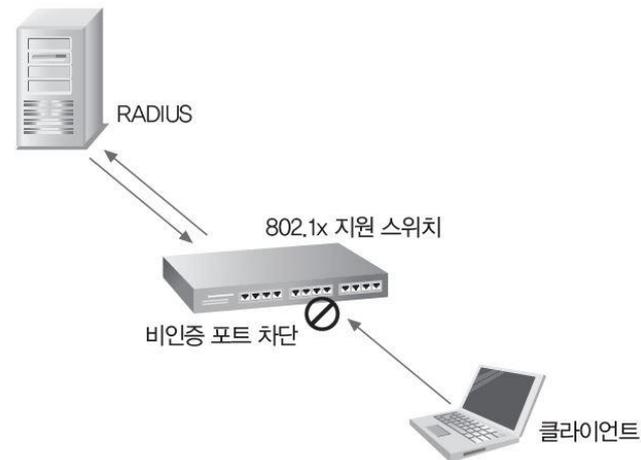


[인라인 방식을 이용한 NAC 구현]

• NAC 구현 방식

- 802.1x 방식 (스위치 이용)

- ✓ 802.1x 프로토콜과 RADIUS 서버를 이용하는 것
- ✓ 실질적인 접근 허용이나 차단은 **스위치**에서 수행
- ✓ 신규 클라이언트에 대한 인증 요청은 실제로 **인증을 수행하는 RADIUS 서버로 전달**
- ✓ RADIUS 서버에서 스위치로 반환되는 결과에 따라 스위치는 네트워크에 대한 클라이언트 접근을 허용하거나 거부



[802.1x 방식을 이용한 NAC 구현]

• NAC 구현 방식

- VLAN 방식

- ✓ 인가받지 않은 사용자는 VLAN으로 미리 분리된 망 중에서 통신이 되지 않는 VLAN 망에 신규 클라이언트 할당
- ✓ 인가받은 사용자라면 통신이 가능한 VLAN 망에 할당

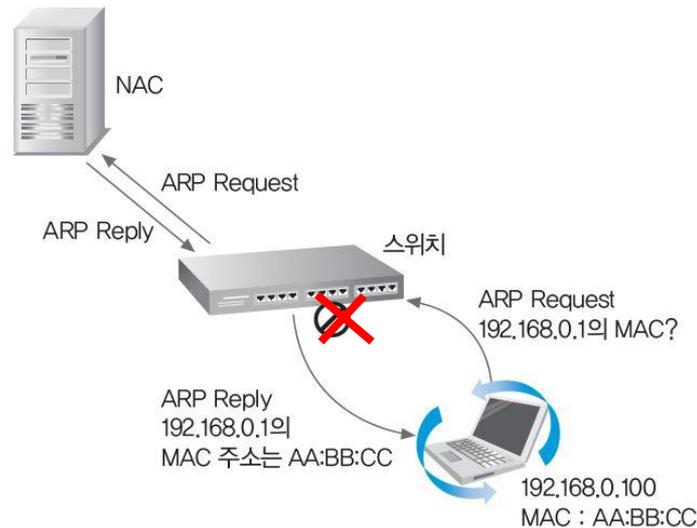


[VLAN 방식을 이용한 NAC 구현]

• NAC 구현 방식

- ARP 방식

- ✓ 신규 클라이언트가 적법한 사용자라면 NAC가 게이트웨이의 정상적인 MAC 주소를 알려줌
- ✓ 적법하지 않은 사용자라면 비정상적인 MAC 주소를 전송하여 네트워크에 대한 접근을 막음

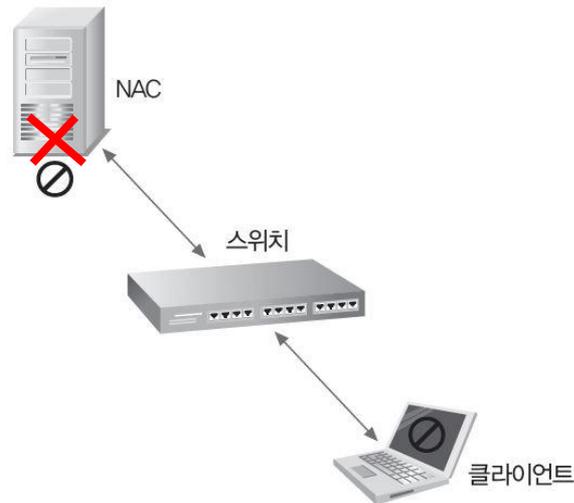


[ARP 방식을 이용한 NAC 구현]

• NAC 구현 방식

- 소프트웨어 에이전트 설치 방식

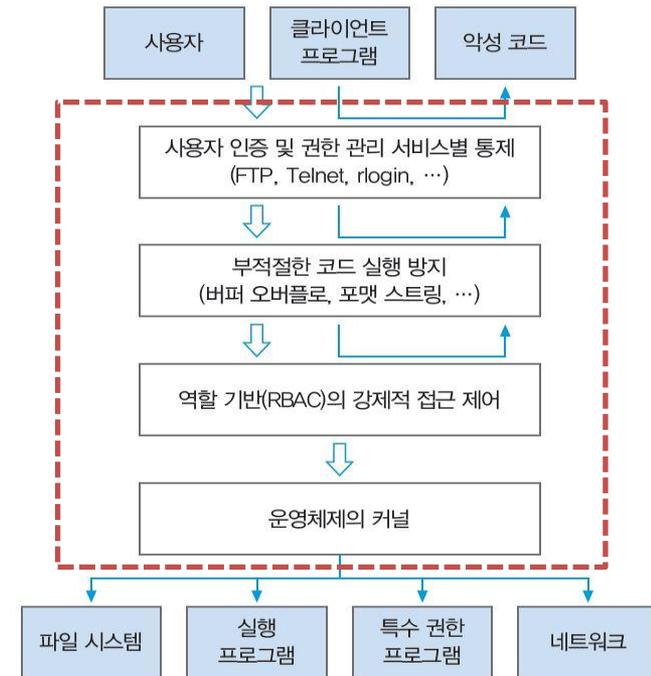
- ✓ 네트워크에 접속하려는 모든 클라이언트에 에이전트를 설치하는 것 (관리부담 증가)
- ✓ 서버에서 **차단 정책을 설정**하여 설치된 에이전트로 네트워크를 차단
 - . 정책에 따라 보안 요건을 충족하지 않는 단말은 네트워크 접속을 차단



[소프트웨어 에이전트 설치 방식을 이용한 NAC 구현]

• 보안 운영체제

- 운영체제에 내재된 결함으로 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위해 보안 기능이 통합된 보안 커널을 추가로 이식한 운영체제
- 일반적인 서버용 시스템은 보안성보다 **가용성**이 우선이지만
- 보안 운영체제는 기본으로 열려 있는 취약 서비스를 모두 차단하여 더 나은 보안 체계로 운영되도록 함



[보안 운영체제의 구성]

- ✓ 보안 운영체제는 일정 수준의 CPU를 점유하므로 성능이 중요할 때는 신중하게 도입해야 함
- ✓ 보안상의 이유로 구매했다가 성능 때문에 다시 제거하는 경우가 많음

• 보안운영체제 주요기능

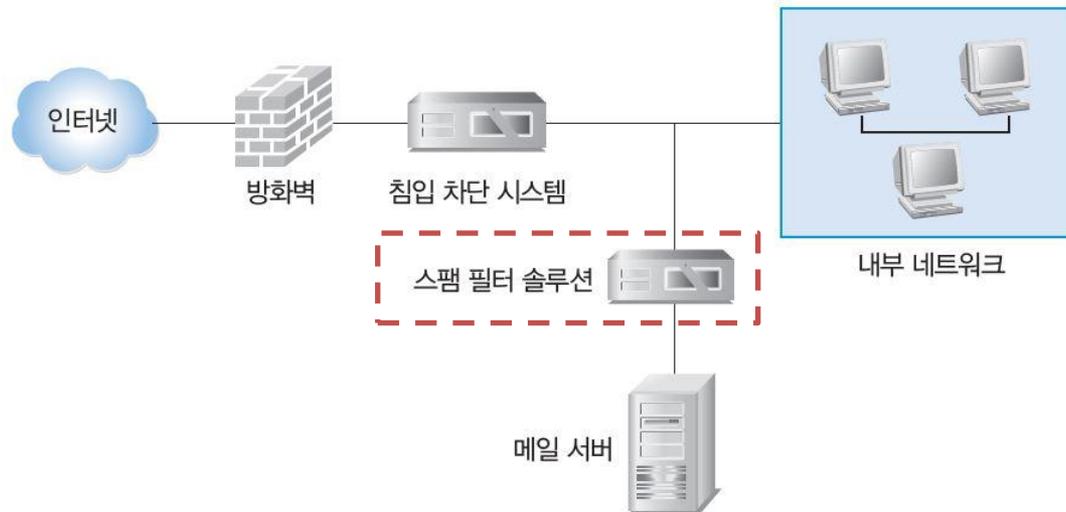
- 보안 커널(Security Kernel) 내장
 - ✓ OS 핵심부(커널)에 보안 기능이 통합됨
 - ✓ 사용자 인증, 접근통제, 코드 실행 통제 등 보안 정책을 운영체제 레벨에서 강제 적용
- 취약 서비스 차단
 - ✓ FTP, Telnet 등 보안에 취약한 프로토콜이나 서비스를 기본적으로 차단
- 역할 기반 접근제어(RBAC) 적용
 - ✓ 사용자 권한을 역할(Role) 단위로 설정
- 악성 코드 실행 방지
 - ✓ 버퍼 오버플로우, 포맷 스트링 공격 등 취약점 공격을 탐지 및 차단
 - ✓ 실행 전 코드 무결성 검사 수행 가능

[보안 운영체제의 구성]

• 스팸 필터 솔루션

- 메일 헤더 필터링

- ✓ 메일 헤더의 내용 중에서 ID/보내는 사람 이름/도메인에 특정 내용이 포함되어 있는지 검사 후
- ✓ 보낸 서버에서 IP/도메인/반송 주소(Reply-to)의 **유효성과 이상 유무 검사**
- ✓ 메일 헤더의 받는 사람, 참조자, 숨은 참조자 필드에 너무 많은 수신자가 포함되어 있는지, 존재하지 않은 수신자가 포함되어 있는지 검사



[스팸 필터 솔루션의 구성]

- 제목 필터링

✓ 메일을 이용한 웹 공격은 제목에 **특정 문자열**이 있거나 **일정 수 이상의 공백 문자열**이 있는 것이 특징

✓ 메일 제목에 '광고' 등의 특정 문자열이 포함되어 있는지 검사하여 웹 차단 가능

- 본문 필터링

✓ 메일 본문에 **특정 단어나 문자**가 포함되어 있는지 검사

✓ 메일 본문과 메일 전체의 크기를 비교하여 유효성 확인

- 첨부 파일 필터링

✓ 첨부된 파일의 이름, 크기, 개수 및 첨부 파일 이름의 길이를 기준으로 필터링 수행

✓ 특정 확장자를 가진 첨부 파일만 전송되도록 설정

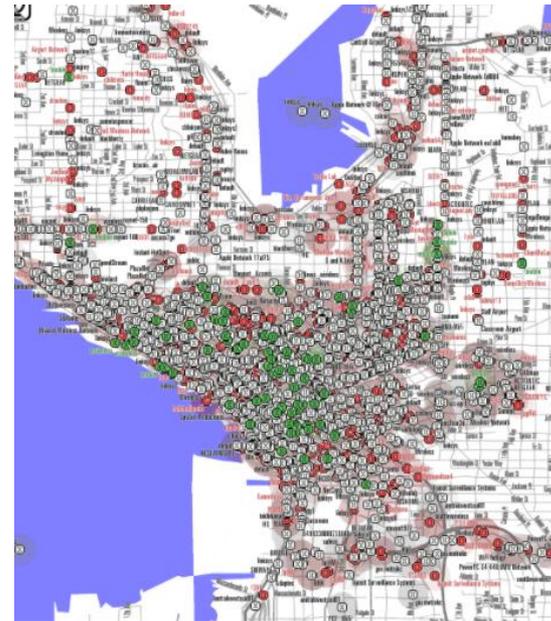
- exe, com, dll, bat처럼 실행이 가능한 확장자를 가진 첨부 파일을 **필터링**

• 모바일 보안 – 이동성 문제

- 모바일 기기는 이동성이 뛰어나므로 공격을 받을 때보다 공격에 사용될 때 더 위험
- **워드라이빙 (wardriving)** : 노트북에 수신율 좋은 안테나 연결하고 차에 탄 채 보안이 취약한 무선 랜을 탐색하며 해킹 시도하는 것
 - ✓ 워워킹 (War walking): 걸어 다니면서 하는 행위



[워드라이빙]



[어느 학생이 제작한 시애틀의 무선랜 노드 맵, Wikipedia]

• 블루투스

- 선을 사용하지 않고 휴대전화, 휴대용 단말기, 주변 장치 등을 연결하는 기술
- 여러 가지 장치가 작은 규격과 적은 전력으로 접근하기 때문에 높은 수준의 암호화와 인증을 구현하기가 어려워 다양한 위험에 노출될 수 있음
- 블루투스와 관련된 다양한 해킹 기술은 네트워크 해킹과 개념이 유사

- 블루프린팅

- 블루프린팅(blueprinting)은 블루투스 **공격 장치의 검색** 활동을 의미
- 블루투스 장치의 종류(전화 통화, 키보드 입력, 마우스 입력 등)를 식별하기 위해 사용하는 서비스 발견 프로토콜 (Service Discovery Protocol, SDP)을 이용해 공격이 가능한 블루투스 장치 검색 및 모델 확인 가능

- 블루스나프

- 블루스나프(bluesnarf)는 블루투스 취약점을 이용하여 **장비의 임의 파일에 접근하는 공격**
- 블루투스 장치끼리 인증 없이 정보를 교환하도록 개발된 **OPP(Obex Push Profile) 기능을 사용**
- 특정 내용을 요청 및 열람하거나 취약한 장치의 파일에 접근함

- 블루버그

- 블루버그(bluebug)는 블루투스 장비 간의 **취약한 연결 관리를 악용한 공격**
- 한 번 연결되면 다시 연결하지 않아도 서로 연결되는 인증 취약점을 이용

- 비교

구분	공격 목적	이용 취약점	공격 결과
블루프린팅	공격 가능한 장치 검색	SDP	대상 장치 탐색
블루스나프	장비 내 파일 탈취	OBEX/OPP	개인정보 유출
블루버그	장치 제어 권한 탈취	인증 관리 취약점	원격 조작, 통화 제어

참고문헌

- 양대일, 정보보안개론(개정4판), 한빛아카데미, 2021
- 양대일, 네트워크 보안과 해킹, 한빛아카데미, 2016
- 박영호, 문상재 (1995) OSI 참조모델의 네트워크 계층 보호 프로토콜 정보보호학회지, 5(2), 64-73
- 장성렬, 이영경, and 이경현 "보안성을 개선한 WEP 프로토콜 제안 " 한국멀티미디어학회 학술발표논문집 (2002): 271-274
- 강유성, et al "무선 LAN 보안 취약점과 단계적 해결 방안 " 한국통신학회지 (정보와통신) 20 7 (2003): 117-128
- Kavitha, T , and D Sridharan "Security vulnerabilities in wireless sensor networks: A survey " Journal of information Assurance and Security 5 1 (2010): 31-44
- 진화하는 국내 UTM 시장, 2017. 11, <http://www.comworld.co.kr/news/articleView.html?idxno=49330>
- How the DNS works, <http://www.centri.org>
- DNS 캐시 중독이란 무엇입니까? | DNS 스푸핑, Cloudflare, <https://www.cloudflare.com/ko-kr>
- DNSSEC소개, 한국인터넷정보센터,
[한국인터넷정보센터/jsp/resources/dns/dnssecInfo/dnssecInfo.jsp](http://www.kisa.or.kr/jsp/resources/dns/dnssecInfo/dnssecInfo.jsp)
- 차세대 무선통신 네트워크 기술 동향 및 보안 이슈 분석, 주소영 외 2인, 한국정보보호학회지, 제31권 제3호, 2021
- 차세대 방화벽, vmware, 2021, <https://www.vmware.com/kr.html>
- VPN이란 무엇인가요?, Alibaba Cloud, 2021, <https://www.alibabacloud.com/ko/knowledge/what-is-vpn>
- Switch VLAN configuration basis and examples, OPTCORE, 2021, <https://www.optcore.net/switch-vlan-configuration-basis-and-examples/>
- UTM(통합 위협 관리)이란 무엇입니까?, Fortinet
- SOAR(보안 오케스트레이션, 자동화 및 대응)이란 무엇인가요?, IBM, <https://www.ibm.com/kr-ko/think/topics/security-orchestration-automation-response>

