통신 보안

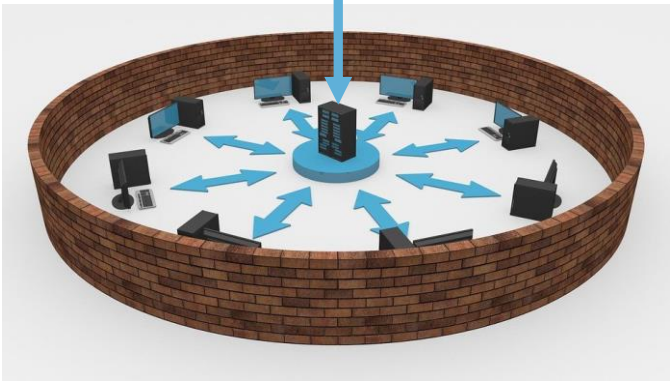
컴퓨터정보공학과
이 종 찬

방화벽의 목적

- 네트워크에서 방화벽은 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷을 미리 정해놓은 **패킷 필터링 규칙**에 따라 차단하거나 보내주는 기능을 하는 하드웨어나 소프트웨어
- 인터넷 세계로부터 서버를 보호하기 위하여 네트워크 출입구에 배치하는 기기
  - IP 주소 또는 포트번호를 기준으로 패킷의 입출력 제어
- 인터넷에 공개하는 서버는 방화벽으로 보호

비신뢰
외부 네트워크

- 외부 네트워크와 내부 네트워크의 구성을 위한 별개의 네트워크를 갖음
- 외부 네트워크 사용자가 내부 네트워크에서 제공하는 서비스를 사용하려면 반드시 방화벽 시스템을 통과해야 함

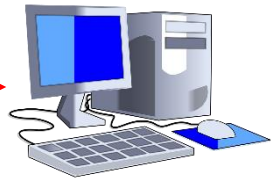


신뢰하는 내부 네트워크

방화벽의 기능

- 접근 제어(Access Control)
  - 통과시킬 접근과 그렇지 않은 접근을 결정하여 허용과 차단
- 외부 네트워크를 통한의 불법적인 침입을 감지
  - DDos, 해킹, 바이러스 등의 차단
- 로깅(Logging)과 감사 추적(Auditing)
  - 허용 또는 거부된 접근에 대한 기록을 유지
- 인증(Authentication)
  - 메시지 인증, 사용자 인증, 클라이언트 인증
- 데이터 암호화
  - 방화벽에서 다른 방화벽까지 전송되는 데이터를 암호화해서 보내는 것으로, 보통 VPN의 기능을 이용
- NAT(Network Address Translation)
  - 내부(사설 주조)와 외부(공인 주소)의 주소 변환(Mapping)

프로토콜과 방화벽



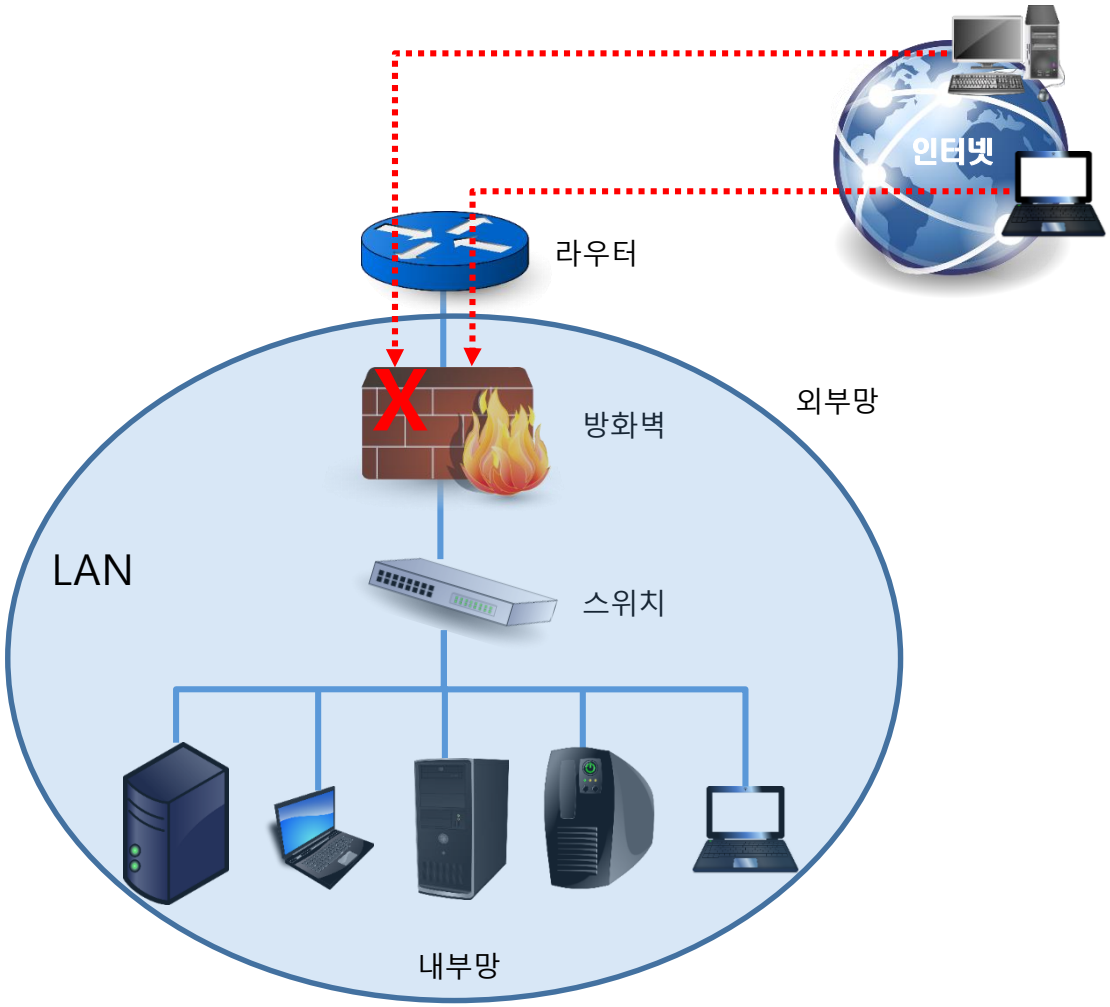
응용계층(Application Layer)	사용자로부터 데이터를 입력/출력	L7
표현계층(Presentation Layer)	데이터 형식 규정	WAF
세션계층(Session Layer)	어플리케이션 및 통신 장치 제어	
전송계층(Transport Layer)	데이터를 패킷, 패킷을 데이터로	L4
네트워크계층(Network Layer)	패킷 송신 및 수신	IDS/IPS
데이터링크계층(Data link Layer)	물리적 링크 제어	FireWall
물리계층(Physical Layer)	물리적 링크 장치	

데이터

방화벽의 분류

분류	특징	선택
기본 방화벽	IP 주소와 포트 번호로 제어	단순 사이버 공격의 대응 필요 시
UTM	방화벽+보안기능	보안 관리를 쉽고 편하게 하고 싶다면
NGF	통신 제어를 애플리케이션 레벨에서 수행	사용자 단위로 웹 애플리케이션 제어가 필요 시에
WAF	웹 서버에 대한 제어를 애플리케이션 레벨에서 수행	공개된 웹 서버의 보안 강화 시에

기본 방화벽

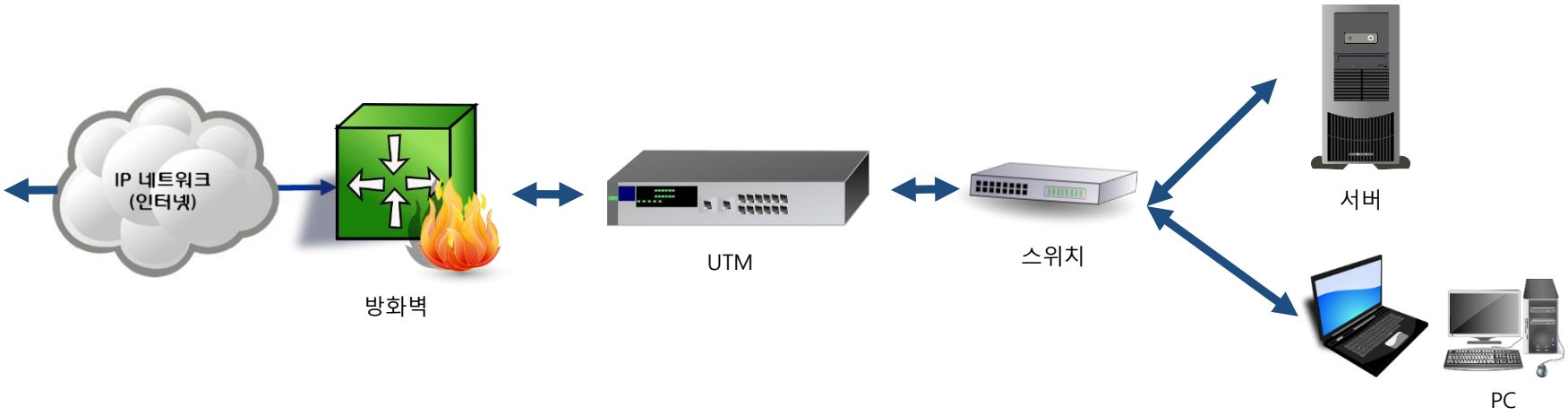


기본 방화벽

- **한계**
  - 기본 방화벽은 패킷의 IP 주소와 포트 번호로 접근 제어
    - 패킷 내용 검사 불가로 e-mail 등 바이러스 대처 불가
  - 기본 방화벽은 자신을 통과하지 않은 통신에 대한 제어가 불가능
    - 내부 사용자가 방화벽을 통과하는 통신 선로가 아닌 무선이나 사설 통신 선로를 이용해 통신을 한다면, 공격자는 방화벽을 우회하여 내부 네트워크로 접속할 수 있음
    - 내부 사용자 역시 방화벽을 우회하여 외부로 허용되지 않은 접속을 시도할 수 있음
  - 백도어 문제
    - Convert Channel을 통한 백도어 생성 및 침입 방어 문제

UTM

- UTM(Unified Threat Management)의 특징
  - 각종 보안 기능을 하나로 모은 방화벽
  - 서로 다른 기기에서 수행하던 보안 기능을 한 대의 기기에서 모두 지원
    - 기기 비용의 대폭 감소 및 효율적인 운용 관리
  - 많은 기능을 한 기기에서 작동하므로 기기의 성능 저하에 주의 필요
    - 대규모 환경에서는 기능에 따라서는 전용 어플라이언스에 전담 필요
  - 확장성 부족
    - 한 기능이 병목현상이 발생해도 그 기능만을 업그레이드 할 수 없음- 전부 교체 필요



UTM

UTM 기능 및 주요 제품

- **다수의 보안 기능을 하나로 모은 방화벽**
  - Anti-Virus : 바이러스 체크
  - Anti-Spam : 스팸 메일을 체크
  - Content/Web Filter : 웹 사이트 및 웹 컨텐츠의 허용 및 차단
  - VPN : 거점 간 또는 원격 연결을 제어
  - IDS/IPS: 서버에 대한 부정 침입을 방지

SonicWall 시리즈

Fortigate 시리즈

Junifer SSG 시리즈

NGFW

- NGFW(Next Generation FireWall)
  - UTM의 방화벽에 기능 추가

우선 모든 직원들의 SNS 통신을 차단해주세요.
아! 홍보팀, 인사팀은 제외해주시는데 저희는 기업을 홍보할 때 트위터랑 페이스북만 쓰니까
홍보팀, 인사팀 직원들만 트위터, 페이스북에 한해 허용이 필요한데,
굳이 chat기능은 필요없으니까 인사팀 김OO대리만 제외하고 chat기능은 차단바랍니다.
그리고 지금 토렌트 차단정책 올라가 있는걸로 아는데, 송OO대표님은 제외해주시고,
중국, 러시아 대역 통신 모두 차단추가해주시고요.
이번 자바 업데이트 버전에서 취약점나왔던데 전사 직원 자바업데이트 막아주세요.

애플리케이션 식별

애플리케이션 제어 및 차단

IP주소가 아닌 사용자(ID) 자체 인식

통신 상황의 가시화

참고: https://m.blog.naver.com/PostList.nhn?blogId=s2kiess

NGFW

- NGFW의 기능 및 주요 제품

- **UTM 기능에 추가 기능 부여**
  - 방화벽 : IP, PORT 를 기반으로 차단
  - Application 제어 : 애플리케이션(트위터, 페이스북, G마켓, 쿠팡 등) 기반으로 차단
  - 사용자 ID 기반 정책 : 기업 고유 정보인 User-ID 기반으로 세분화된 보안 정책 적용
  - DLP(Data Loss Prevention) : 데이터 흐름을 감시하여 기업 내부의 중요 정보의 외부 유출방지

PALOALTO 시리즈

NGFW

- 웹 어플리케이션의 공격에 취약함
  - SQL 주입
    - 데이터베이스 서버와의 연계에 사용하는 SQL 문을 이용하여 공격
  - 사이트 간 스크립팅(Cross-Site Scripting)
    - 웹 브라우저의 표시 처리를 이용하여 공격
  - CSRF(Cross Site Request Forgery)
    - 가짜 웹 사이트로부터 의도하지 않는 HTTP 요청을 보내 공격
  - 쿠키, 세션 또는 매개 변수 변조 공격을 감지할 수 없음

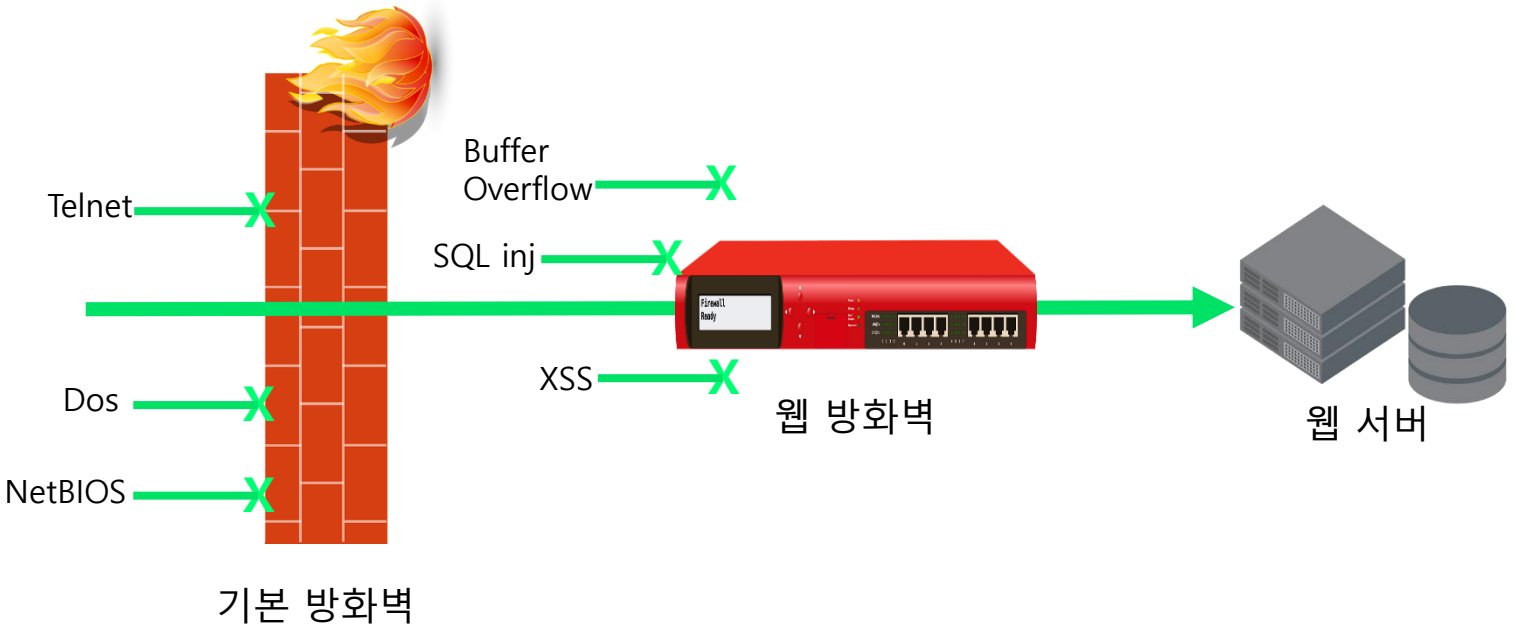
기존 방화벽의 한계

기업에서는 해커들의 침입을 막기 위해 방화벽과 침입방지시스템(IPS)을 배포했으나 웹 어플리케이션에 대한 접근을 허용한 경우 해커들은 인코딩 및 주석 등을 사용하여 기존 방화벽과 IPS를 신속하게 우회하여 쉽게 데이터를 유출하였다.

몇 년 후 개발된 차세대 방화벽은 HTTP 또는 인스턴트 메시징과 같은 어플리케이션 트래픽 유형을 식별할 수 있게 되었다. 이로 인해 액세스를 차단할 수는 있지만, 차세대 방화벽은 SQL 주입, 사이트 간 스크립팅 또는 웹 어플리케이션 취약점을 악용하는 기타 공격들은 차단할 수 없으며 쿠키, 세션 또는 매개 변수 변조 공격을 감지할 수 없다는 한계를 여전히 가지고 있다.

WAF

- 웹 방화벽(Web Application FireWall)의 특징
  - 웹 어플리케이션 공격을 보호하도록 특별히 설계된 솔루션
    - 서버의 소프트웨어로서 도입하는 호스트형
    - 어플라이언스 서버를 도입하는 어플라이언스 서버형
    - 클라우드의 SaaS로서 제공되는 SaaS형



WAF

- 웹 어플리케이션 보호 방법
  - HTTP 및 HTTPS 요청 네트워크 패킷 차단
  - 네트워크 패킷의 데이터 컨텐츠를 검사
    - 헤더, 세션 세부 정보, 쿠키, 매개 변수, 파일 업로드, 형식, 프로토콜 등
  - 데이터 분석
    - 시스니처 분석: 알려진 취약점을 패턴 매칭으로 즉시 차단
    - 논리 분석 탐지: 신종 공격의 특성을 파악하여 지능적 차단
  - 검사 결과에 따라 클라이언트가 웹 어플리케이션에 액세스하도록 허용
    - 합법적인 클라이언트가 아닌 경우, 요청, 세션, IP 주소, 사용자 또는 파일 업로드/다운로드를 차단

WAF

WAF의 기능 및 주요 제품

- HTTP 및 HTTPS 요청 네트워크 패킷 차단
- 네트워크 패킷의 데이터 컨텐츠를 검사
  - 헤더, 세션 세부 정보, 쿠키, 매개 변수, 파일 업로드, 형식, 프로토콜 등
- 데이터 분석
  - 시스니처 분석: 알려진 취약점을 패턴 매칭으로 즉시 차단
  - 논리 분석 탐지: 신종 공격의 특성을 파악하여 지능적 차단
- 검사 결과에 따라 클라이언트가 웹 어플리케이션에 액세스하도록 허용
  - 불법 클라이언트인 경우, 요청, 세션, IP 주소, 사용자 또는 파일 업로드/다운로드를 차단

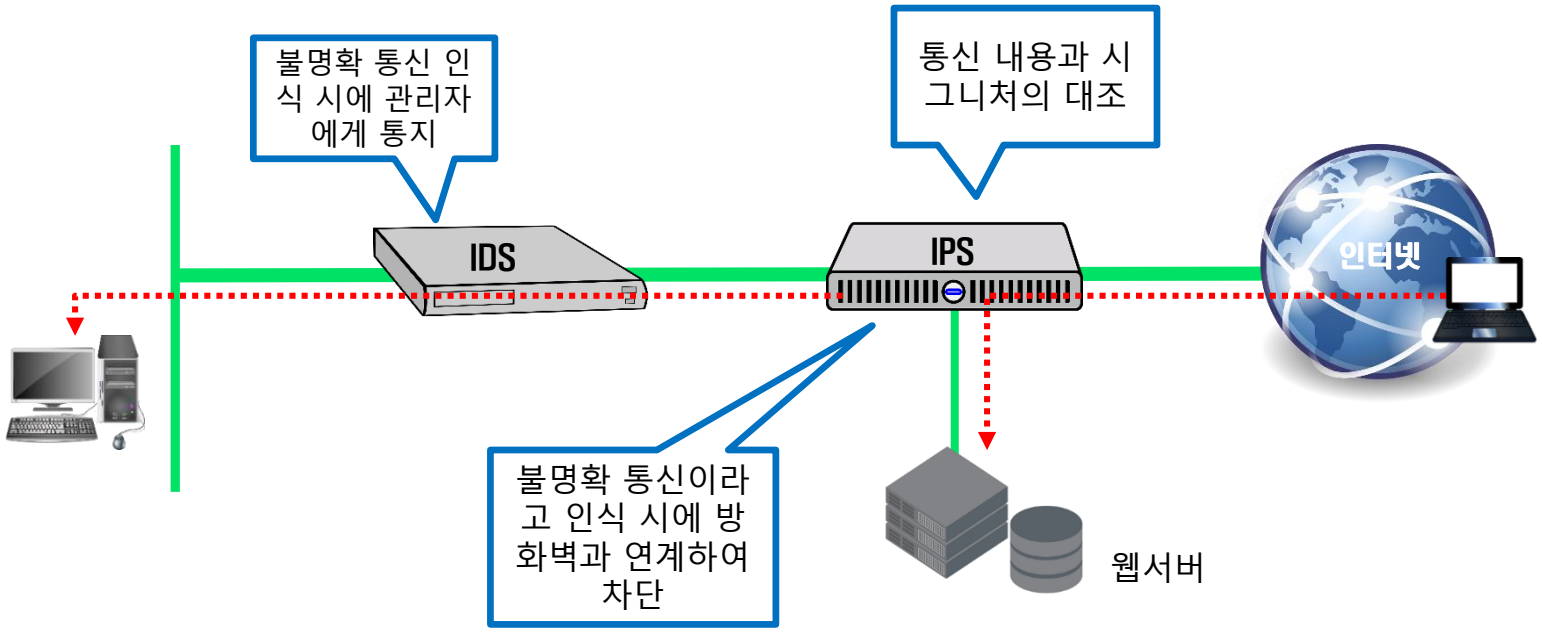
펜타시큐리티시스템의 웹방화벽

IDS/IPS

- 네트워크에 흐르는 비정상적인 통신을 식별하여 관리자에게 통지하거나 차단하는 기능
- 최근에는 방화벽이나 UTM의 기능 중 하나로 탑재되고 있음
- IDS(IDS, Intrusion Detection System)
  - 통신의 움직임으로부터 침입을 감지하는 기능
  - 경고를 받은 관리자는 액세스 로그 점검 또는 필터를 변경 등의 조치
  - 오용 탐지(Misuse Detection)
    - 사전 정립된 공격 패턴(시그니처, Signature)을 미리 입력해 두고, 해당 패턴을 탐지
    - 탐지 오판 확률이 낮고 비교적 효율적이지만 알려진 공격 외에는 탐지 불가능
  - 이상 탐지(Anomaly Detection)
    - 정상적이고 평균적인 상태를 기준으로, 상대적으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생할 경우 침입 탐지
    - 인공지능 IDS는 공격에 대해 스스로 판단하고 결정을 내리지만 판단의 근거가 확실하지 않고 오판 확률도 높음

IDS/IPS

- IPS(IDS, Intrusion Protection System)
  - 통신의 움직임으로부터 공격이나 부정 침입을 방어하는 기능
  - 침입 탐지 시스템에 방화벽의 차단 기능을 부가한 시스템
  - IDS로는 감지만 수행하고 서버의 상태를 확인 후에 IPS로 차단

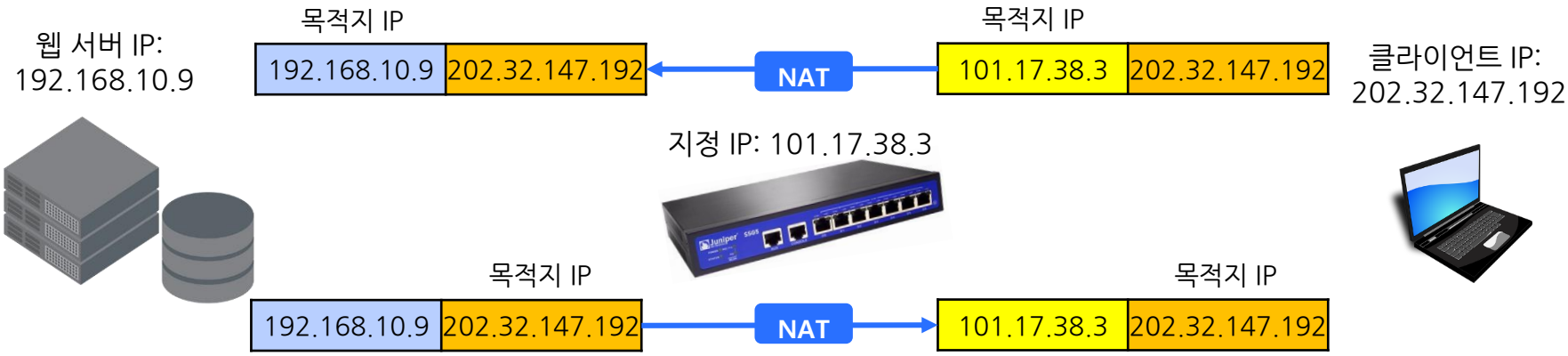


NAT

- 웹 서버 등은 내부 네트워크에서 사설IP(Private Address)를 소유
  - 인터넷으로 연결 시 라우팅이 가능한 공인IP(Public Address)로 변환
- 연결 방법
  - 사설IP와 공인IP를 1:1로 연결
  - IP 주소의 변환 정보를 기억하여 재변환
- 작동 방법
  1. 클라이언트는 공인IP 주소를 출발지 주소로, 방화벽 지정 외부IP를 목적지 주소로 하는 패킷을 생성하여 방화벽 전송
  2. 방화벽은 패킷의 목적지 주소를 미리 설정되어 있는 내부(사설) IP 주소로 바꾸어 내부 서버에 전송
  3. 내부 서버는 이에 대한 응답을 방화벽으로 전송
  4. 방화벽은 내부(사설) IP 주소로 되어 있는 출발지 IP 주소를 방화벽 지정 외부 IP 주소로 바꾸어 클라이언트에 전송

NAT

- 사설 주소와 공인 주소
  - 웹 서버 IP: 사설IP
  - 방화벽(또는 라우터) 지정 IP: 공인IP



NAPT

- 연결 방법
  - 사설IP와 공인IP를 n:1로 연결
  - 사설IP와 포트 번호를 동시에 변환
  - IP 주소와 포토 번호의 변환 정보를 기억하여 재 변환
- 작동 방법

1. 클라이언트는 사설IP 주소를 출발지 주소로, 외부 공인IP를 목적지 주소로 하는 패킷을 생성하여 방화벽에 전송
2. 방화벽은 클라이언트의 사설IP 주소를 방화벽 지정 공인 IP로 변환하고 포트 번호도 변경하여 목적지 클라이언트에 전송
3. 내부 서버는 이에 대한 응답을 방화벽으로 전송
4. 방화벽은 수신된 패킷의 목적지 IP주소와 목적지 포트 번호를 클라이언트의 사설IP와 포트 번호로 변환하고 클라이언트에 전송

NAPT

클라이언트 IP/Port:
192.168.10.9/200

목적지 IP			
200	443	192.168.10.9	202.32.147.192

NAPT

목적지 IP			
1200	443	101.17.38.3	202.32.147.192

서버 IP/Port:
202.32.147.192/443

지정 IP/Port:
101.17.38.3/1200, 1300

192.168.10.7/300

목적지 IP			
300	443	192.168.10.9	202.32.147.192

NAPT

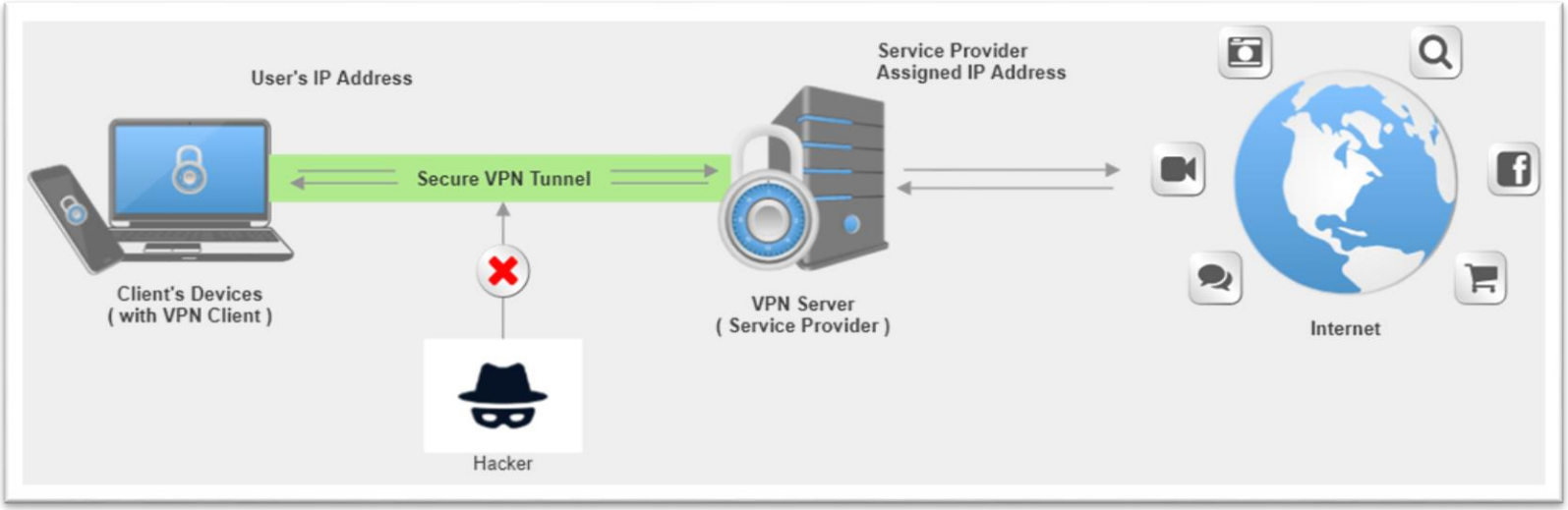
목적지 IP			
1300	443	101.17.38.3	202.32.147.192

VPN

- 공중망(인터넷)에 연결되어 있는 네트워크 사이의 연결을 마치 사설망처럼 이용 할 수 있도록 하는 보안 네트워크 기술.
- 공중망을 기반으로 가상의 전용망을 구축
  - 인터넷 회선을 임대 회선과 유사하게 사용할 수 있게 해주는 솔루션
  - 기업의 본사와 지사 간에 전용회선대신 공용 네트워크를 사용함으로서 비용 절감 효과를 가짐
  - VPN 클라이언트는 터널링 프로토콜이라는 특별한 TCP/IP 기반 프로토콜을 사용하여 VPN 서버의 가상 포트에 대해 가상 호출 수행
- VPN 상에서 전송되는 데이터는 기밀성을 위해 암호화
  - VPN이 임대 회선과 비슷한 수준의 기밀성을 제공하기 위해서는 암호화가 필요. VPN에 사용되는 프로토콜에는 PPTP, L2TF, IPSec, SSL 등이 있음
  - 암호화 키가 없으면 공유 또는 공용 네트워크에서 패킷을 가로채도 해독할 수 없음.

VPN

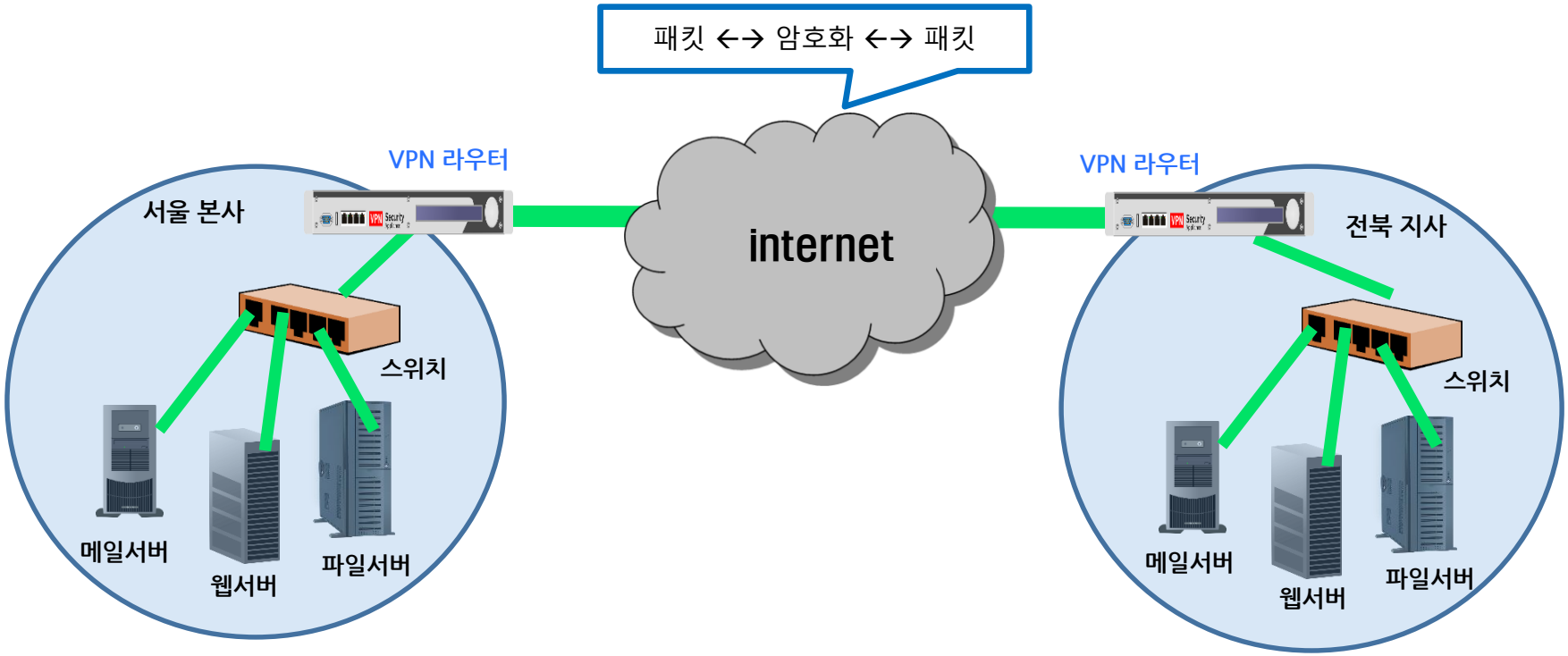
- 물리적인 목적
  - 본사 내부에 있는 전산망에 원격지의 PC를 마치 내부의 망에 연결된 것 처럼 만듦
    - 물리적으로는 공중망 상에서의 연결
  - 일단 연결되면 원격 작업자는 마치 사무실에 있는 것처럼 다른 장치, 웹 서버, 데이터베이스 서버 및 프린터 등에 안전하게 액세스
  - 방화벽은 VPN 서버 대상으로 들어오는 보안 연결을 허용하도록 구성
  - 이제 작업자는 사실상 내부 리소스에 액세스 할 수 있는 사설 네트워크의 일부



참고: https://www.hkcert.org/mobile_url/en/blog/20081801

VPN

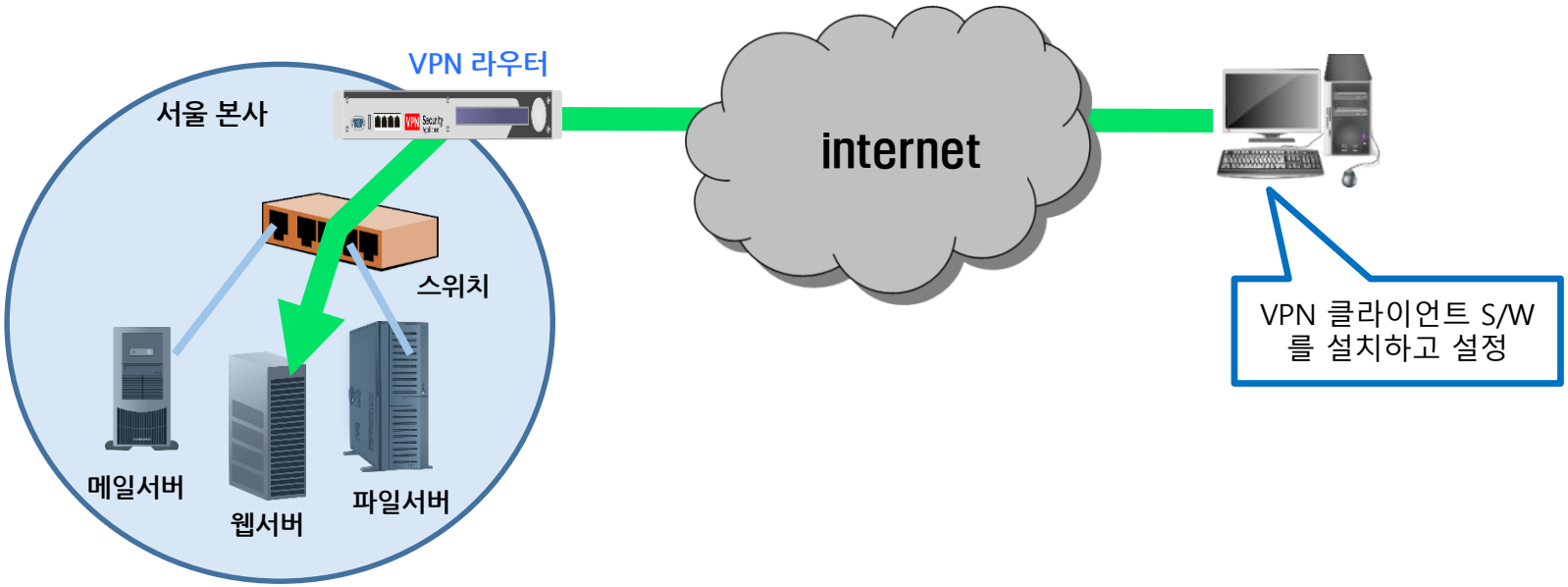
- **거점(장비; 라우터)간 VPN**
  - 방화벽, 라우터, UTM 등의 VPN 기능을 사용
  - 사이트 간 VPN 연결은 사설망의 두 부분을 연결
    - 라우터는 VPN 연결을 통해 패킷을 다른 라우터로 전달
    - 라우터에서 VPN 연결은 데이터 링크 계층 링크로 작동
  - 암호화를 위하여 IPSec(IP security protocol) 적용



VPN

원격 액세스 VPN

- 재택 근무자나 이동 중인 사용자가 인터넷과 같은 공용 네트워크에서 제공하는 인프라를 사용하여 사설망의 서버에 액세스할 수 있음
  - 가상의 회선을 (소프트웨어적으로)설치하는 과정 필요
- 사용자 관점에서 VPN은 컴퓨터(VPN 클라이언트)와 조직 서버 간의 지점 간 연결
- 논리적으로 데이터가 전용 개인 링크를 통해 전송되는 것처럼 나타남
- 암호화를 위하여 IPSec 또는 SSL (Secure Socket Layer) 적용



VPN

- VPN 설정 방법

① VPN 클라이언트 설치

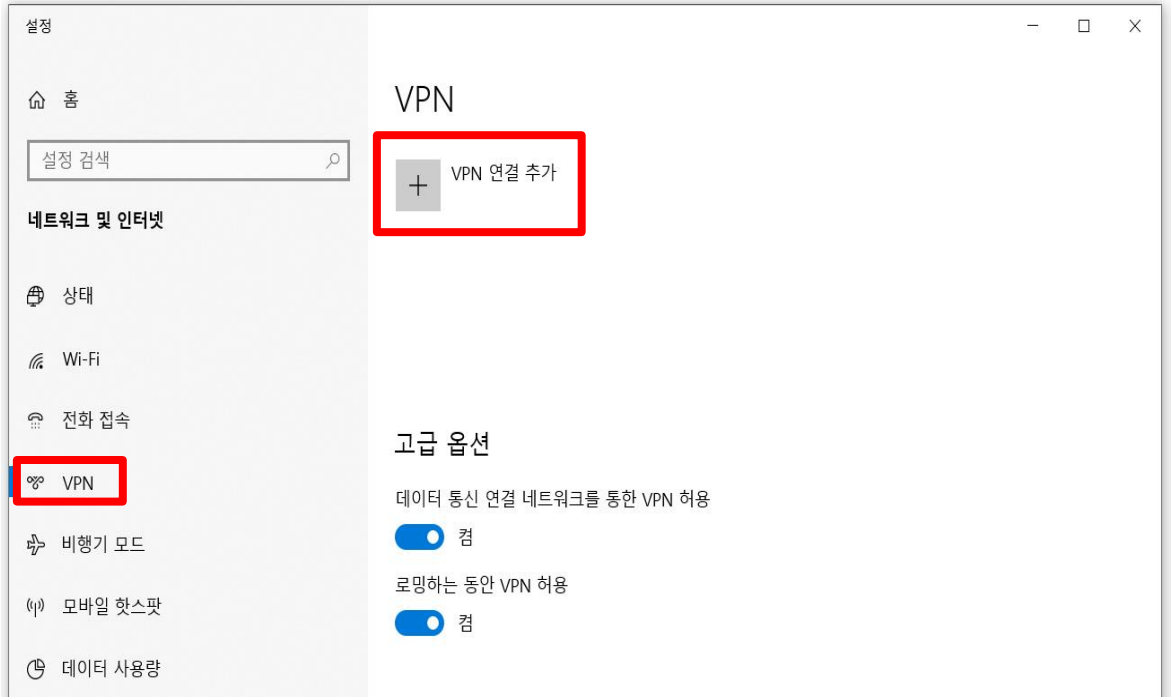
- 클라이언트에서 VPN 접속을 위하여 지정된 VPN클라이언트를 설치

VPN

VPN 설정 방법

② VPN 연결 추가

- 윈도우 시작 → 설정 → 네트워크 및 인터넷 → VPN → VPN 연결 추가

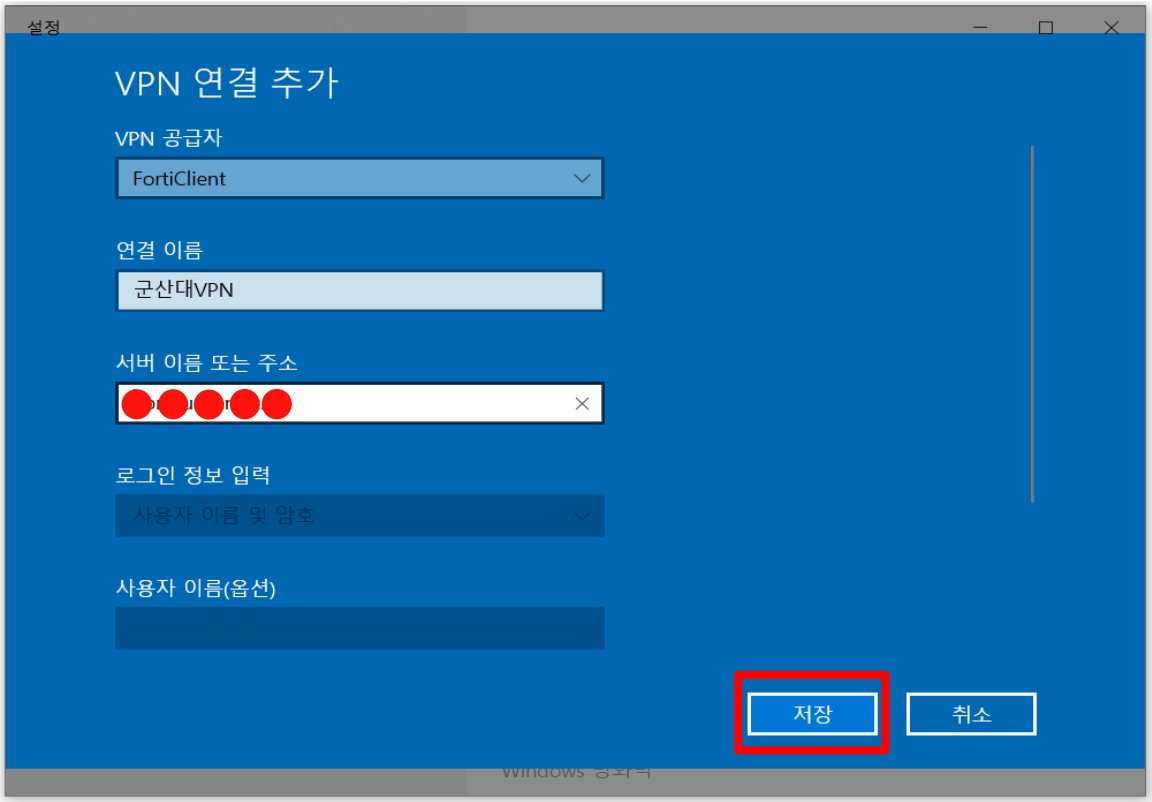


VPN

VPN 설정 방법

③ VPN 연결 추가 항목 입력 후, 저장

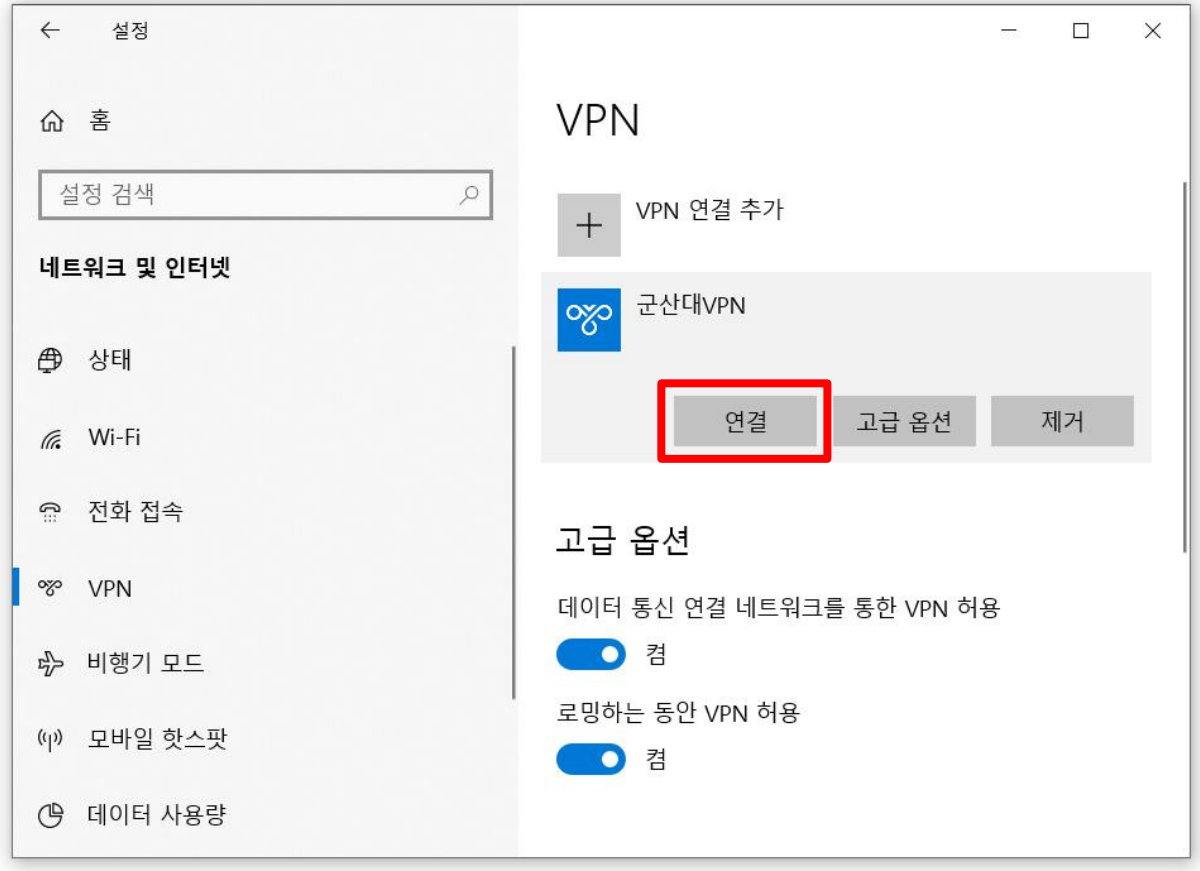
- VPN 공급자 : 설치한 VPN클라이언트 선택
- 연결 이름 : 임의 입력
- 서버 이름 또는 주소 : 지정한 VPN서버 이름



VPN

VPN 설정 방법

④ 생성한 VPN 클릭 후, 연결

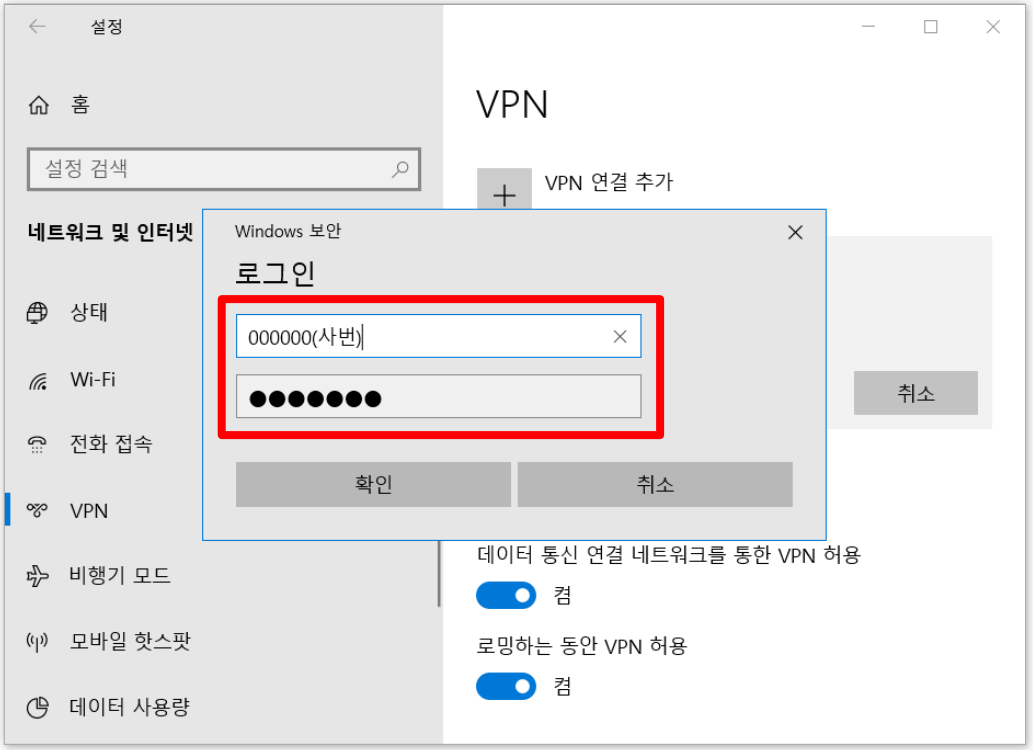


VPN

VPN 설정 방법

⑤ 로그인 정보 입력 후 확인

- 사용자 이름 : 사번(사용자 계정)
- 암호 : 사용자 암호



VPN

VPN 설정 방법

⑥ 연결 확인