네트워크 보안

보안의 개념 과 정의

- 보안
  - ✓ 보안의 한자어 의미는 안전을 지키는 일
  - ✓ 안전은 위험이나 사고의 염려 없이 편안하고 온전한 상태를 가리키는 용어
  - ✓ 보안’ 뜻을 풀이해보면 위험이 생기거나 사고가 날 염려 없이 편안하고 온전한 상태를 지키는 모든 활동 으로 정의할 수 있음
  - ✓ 국어사전에서도 비밀 따위가 누설되지 않도록 보호하거나 사회의 안녕과 질서를 유지하는 일련의 활동으로 정의하고 있음
  - ✓ 전체적인 맥락에서 보안을 이해하지 못하는 가장 큰 이유는 사고 없는 상태를 유지하는 모든 활동으로 정의하기 때문

보안의 개념 과 정의

- 정보 보안
  - ✓ IT에서 다루는 정보 보안은 다양한 위협으로부터 보안을 보호하는 것을 의미
  - ✓ 보안의 정의에 맞추어 확장하면 우리가 생산하거나 유지해야 할 정보에 위험이 발생하거나 사고가 날 염려없이 편안하고 온전한 상태를 유지하는 일련의 활동을 정보 보안이라고 함
  - ✓ 여러 가지 관점에서 정보 보안을 생각할 수 있지만 크게 생산자와 소비자 입장에서 구분해 보았을 때 외부에서 정보가 저장된 시스템을 사용하지 못하게 하거나 유출 시도에 맞서 적절히 보호 및 운영하기 위한 작업과 정보가 내부에서 유출되거나 남용되는 것을 막기 위한 두 가지 분야가 있음

보안의 개념 과 정의

- ❖ 정보 보안
  - ✓ 보안의 필수 요소
    - 기밀성
      - ◆ 인가되지 않은 사용자가 정보를 보지 못하게 하는 모든 작업으로 가장 대표적인 기밀성은 암호화 작업
    - 무결성
      - ◆ 정확하고 완전한 정보 유지에 필요한 모든 작업을 의미
      - ◆ 누군가가 정보를 고의로 훼손하거나 중간에 특정 이유로 변경이 가해졌을 때 그것을 파악해 잘못된 정보가 전달되거나 유지되지 못하게 하는 것이 무결성
      - ◆ 가장 대표적인 무결성 기술은 MD5, SHA와 같은 해시(Hash) 함수를 이용해 변경 여부를 파악하는 것
    - 가용성
      - ◆ 정보가 필요할 때 접근을 허락하는 일련의 작업
      - ◆ 보통 많은 IT 실무자들이 보안을 막거나 통제만 하는 것으로 생각하다 보니 보안에서 가용성 유지가 중요한 이유를 모르는 경우가 있음
      - ◆ 정보에 대해 사고날 염려 없이 온전한 상태를 유지하는 것이 정보 보안이므로 어떤 이유에서라도 그 정보를 사용할 수 없는 상황이라면 정보 보안에 실패한 것

보안의 개념 과 정의

- 정보 보안
  - ✓ 보안의 3대 요소 외에 주가로 진정성(Authenticity), 책임성(Accountability), 부인 방지(Non-Repudiation), 신뢰성(Reliability) 유지를 정보 보안 활동 중 하나로 정의하기도 함
  - ✓ 여러 기관의 정의를 좀 더 이용해 정보 보안을 간단히 정의하면 조직의 지적 자산을 보호하는 절차 , 인가된 사용자만(기밀성) 정확하고 완전한 정보로(무결성) 필요할 때 접근할 수 있도록(가용성) 하는 일련의 작업 임

보안의 개념 과 정의

- 네트워크의 정보 보안
  - ✓ 정보 보안을 IT 종사자의 행동에 맞추어 더 상세히 표현하면 정보를 수집, 가공, 저장, 검색, 송수신하는 도중에 정보의 훼손, 변조 유출을 막기 위한 관리적 기술적 방법을 의미
  - ✓ 네트워크 입장에서의 정보 보안은 수집된 정보를 침해하는 행동을 기술적으로 방어하거나 정보의 송수신 과정에서 생기는 사고를 막기 위한 작업
  - ✓ 정보를 가진 시스템을 공격해 유출하거나 사용하지 못하게 하거나 시스템이 동작하지 못하게 해 정보 서비스를 정상적으로 구동할 수 없게 만드는 행위를 네트워크에서 적절히 막는 것이 네트워크 보안의 1차 목표
  - ✓ 정보는 여러 가지 서비스를 제공하기 위해 한 자리에만 있는 것이 아니라 네트워크를 통해 복제, 이동되므로 그 유출을 막는 것이 2차 목표
  - ✓ 네트워크 보안을 이해하려면 네트워크를 통한 다양한 공격 방식과 그 공격을 네트워크에서 방어하는 장비와 그 구동 방식을 이해해야 함
  - ✓ BOTTOM-UP 형식으로 네트워크 보안이 발전하고 있음

보안의 개념 과 정의

- 네트워크의 정보 보안
  - ✓ 네트워크는 중요한 정보유출 영역
  - ✓ 네트워크가 없다면 정보의 이동이 어려워지므로 정보에 대한 사용도 원활해지지 않는데 이런 자유로움 때문에 적절한 통제가 없을 때 정보가 유출당할 가능성이 매우 큼
  - ✓ 이런 자유로운 이동성을 제공하는 네트워크의 성질 때문에 네트워크에 연결된 정보 시스템을 공격 대상으로 삼는 것이 일반적이지만 외부 공격자가 네트워크 자체를 공격 대상으로 삼는 경우도 많음
  - ✓ 네트워크를 장악하면 많은 시스템에 더 쉽게 접근할 수 있어 침해 범위를 넓히고 외부 침입자가 원하는 정보가 유출될 가능성이 커짐
  - ✓ 네트워크 보안은 외부 공격에 맞서는 중요한 1차 방어선
  - ✓ 대부분의 데이터와 애플리케이션 서비스들이 네트워크에 연결된 상황에서 네트워크 보안을 적절히 제공할 수 있다면 강력한 1차 저지선을 확보한 것
  - ✓ 시스템과 애플리케이션에 결함이 있거나 취약점이 있는 경우에도 네트워크의 다양한 보안 장비를 활용한다면 외부의 공격을 늦추거나 적절히 방어할 수 있음

네트워크 보안

- 네트워크 보안 과 관제 필요성
  - ✓ 2003년 1월 25일 인터넷 대란 이후 대한민국에도 끊임없이 굵직한 정보보안 사고들이 발생하고 있어서 공공 기관 기업들은 정보보안 강화를 위해 정보보안 예산을 늘리는 등 역량 강화에 노력하고 있지만 막상 보안 제품만 도입하고 사후 운영이 제대로 되지 않고 있어 정보보안 사고가 언제든지 발생할 수 있는 위험이 존재
  - ✓ 더욱이 기본적인 보안 시스템조차 없는 중소기업들은 공격을 받고 있는 것은 아닌지 공격을 받았다면 어떤 경로를 통해 유입되었는지 등 그 상황 자체도 파악할 수 없는 경우가 많음
  - ✓ 정보보안 사고를 예방하기 위해서는 보안 시스템을 구축한 이후에도 보안 전담 인력이 보안 관제를 하여 사전에 위협을 탐지할 수 있어야 하고 정보보안 사고를 예방하는 활동과 함께 정보보안 사고 대응 활동을 통해 같은 유형의 공격에 피해를 입지 않도록 대비할 수 있어야 함
  - ✓ 네트워크 보안을 위해 과거에는 단순히 네트워크 보안 시스템들만 구축해서 네트워크의 접근을 통제해도 충분한 시절이 있었지만 현재는 다양한 경로로 네트워크에 연결된 수 많은 단말기로부터 발생하는 다양한 보안 위협을 탐지하고 대응해야 하는 상황에 놓여 있으므로 보안 관제 활동을 지속해야 하는 것이 더욱 중요

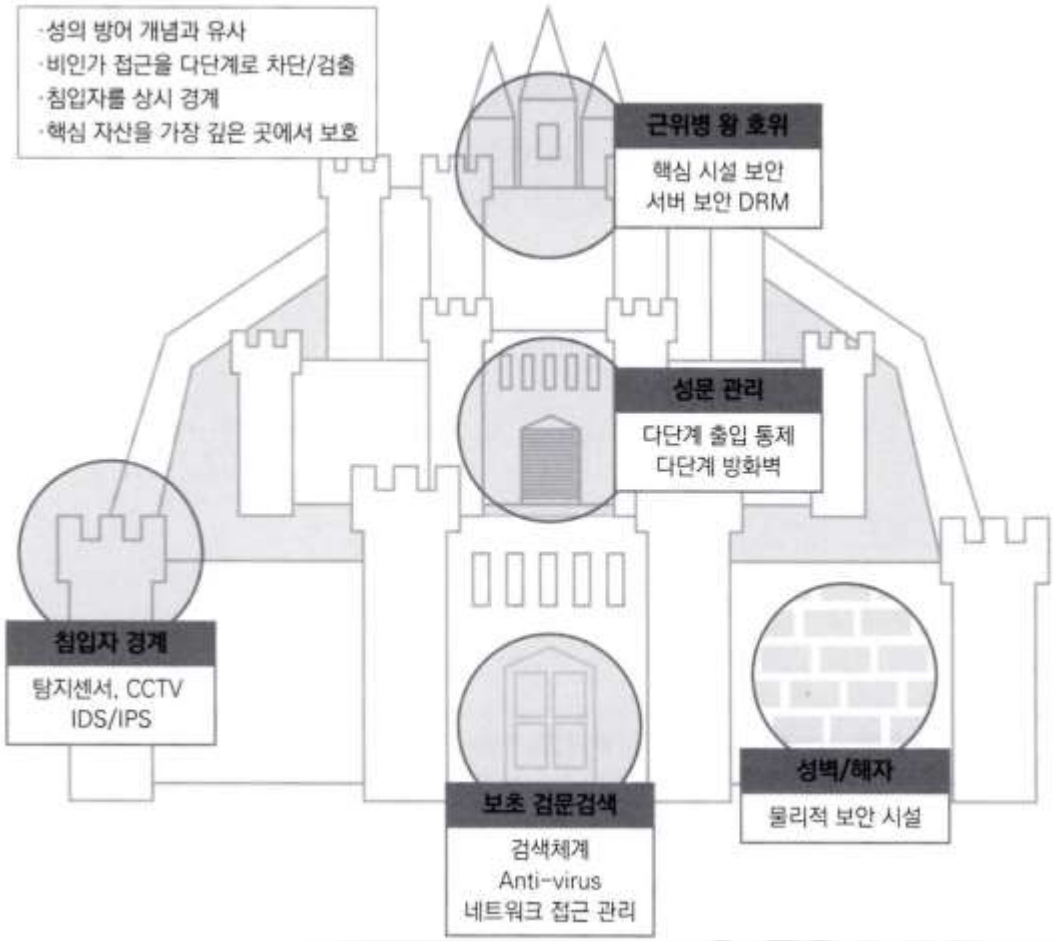
네트워크 보안

- 네트워크 보안 과 관제 필요성
  - ✓ 1980년대로 접어들면서 컴퓨터 기술과 네트워크 기술이 발달하기 시작했고 그와 동시에 컴퓨터 범죄라는 새로운 범죄 형태가 발생하기 시작함
  - ✓ 대표적인 예로 1988년 로버트 모리스가 제작한 모리스 웜 바이러스에 의해 당시 네트워크에 연결된 컴퓨터들이 감염되어 시스템이 마비된 사태 1995년 케빈 미트닉이 미국 주요 국가 기관과 기업체 전산망을 해킹한 사건 등이 있는데 이러한 컴퓨터 범죄들의 공통점은 네트워크로 연결된 곳에서 발생한 사건이라는 문제점을 인지하면서 네트워크 보안의 필요성이 대두되었음
  - ✓ 그 결과 1994년 최초의 상용 네트워크 방화벽 체크포인트 Firewall-1이 등장했으며 1998년 네트워크 침입 탐지 시스템인 Snort가 나오면서 다양한 네트워크 보안 시스템 업체들이 등장했고 복잡한 네트워크 보안을 효과적으로 운용하고 보안 위협을 탐지/대응하는 네트워크 보안 관제 업체들도 등장하기 시작
  - ✓ 국내에도 해커스랩, 코코넛(2007년 안랩으로 인수됨) 등의 보안 관제 업체가 등장하면서 많은 보안 관제 전문 업체가 단순한 보안 관제 서비스뿐만 아니라 전 방위적 보안 관제를 하는 방식으로 발전해 나가고 있음

네트워크 보안

❖ 네트워크 보안 과 관제 필요성

✓ 물리적 보안 관제 와 사이버 보안 관제



네트워크 보안

❖ 네트워크 보안 과 관제 필요성

✓ 보안 관제 현황

- 국내에서 사이버 보안 대응과 관제를 국가 차원에서 다루게 된 계기는 2003년 1월 25일 인터넷 대란을 겪으면서 부터 였는데 1월 25일 인터넷 대란은 슬래머 웜에 감염된 PC들이 국내 최상위 DNS(혜화 전화국 DNS)로 대량의 트래픽을 집중시켜 DNS 장애를 유발했고 그 결과 전국 대부분의 인터넷 망이 불통된 사건 때문인데 이는 우리나라뿐만 아니라 전 세계에서 동시에 벌어진 사건이었는데 이 사건 이후 국가 차원에서 사이버 공격에 대비한 사이버 안전 보장의 필요성이 제기됨
- 공공기관 및 민간 그리고 군 분야 간의 사이버 안전 체계를 수립하고 상호협력하여 유사시 대응할 수 있도록 2003년 7월 24일에 국가 사이버테러 대응체계 구축에 대한 기본 계획을 수립한 후 2004년 2월에 국가정보원 산하에 국가 사이버 안전을 위한 업무를 수행하는 국가 사이버 안전 센터를 설치하여 국가 공공 분야를 담당하게 하고 군 분야는 국방 정보전 대응 센터로 시작하여 현재는 국군 사이버 사령부를 중심으로 임무를 수행
- 민간 분야는 한국인터넷진흥원(KISA)내 인터넷 침해 대응 센터에서 사이버 보안 관제 업무를 수행

네트워크 보안

❖ 네트워크 보안 과 관제 필요성

✓ 보안 관제 유형

유형	설명
자체 보안 관제	자체적으로 보안 전담 조직을 갖추고 관제 시스템을 구축하여 운영하는 관제 방식으로 국가 기관, 통신사, 대기업 등 보안을 중요시하는 곳이나 자체적으로 내부 네트워크망을 구성해서 운영하는 곳에서 주로 실시
원격 보안 관제	보안 관제 전문 업체와 계약된 범위 내에서 보안 시스템을 구축하고 원격에서 보안 관제를 위탁해서 운영하는 방식으로 자체적으로 보안 관제를 하기 힘들거나 보안 인력이 없는 일반 기업에서 주로 실시
파견 보안 관제	자체적으로 관제 시스템을 구축하였으나 보안 관제를 할 수 있는 전담 조직이나 보안 인력이 없는 경우 보안 관제 전문 업체에서 보안 전문 인력을 파견받아 보안 관제를 운영하는 관제 방식

네트워크 보안

- ❖ 네트워크 보안 과 관제 필요성
  - ✓ 기업 기밀 정보 유출 피해
    - 기업에서 어렵게 개발한 핵심 기술이나 영업 노하우 등이 경쟁 업체로 유출되면 피해 기업은 매출 감소 뿐 만 아니라 기업의 존폐가 좌우되는 최악의 상황을 맞이할 수도 있으므로 기업의 기밀 정보가 유출되지 않게 보호하는 일은 중요
    - 기업의 기밀 정보는 주로 퇴직자, 경쟁업체 직원, 협력업체 직원에 의해서 유출되는 경우가 많은데 기술 유출의 경우에는 핵심 인재를 스카우트하는 방식이 가장 많고 중요 자료를 복사하여 유출하는 사례가 그 다음으로 많이 발생하고 있음
    - 기술 유출에 대한 원인으로는 보안 관리와 감독이 허술하거나 임직원의 보안 의식이 부족한 경우가 가장 큰 부분을 차지하는데 안타까운 점은 한번 유출된 정보에 대해서 유출 사실을 입증하기가 쉽지 않다는 것
    - 그러므로 정보 유출을 예방하기 위해 보안 강화에 꾸준히 투자하고 구성원에게 보안 교육을 실시하며 수시로 모니터링하는 것이 중요

네트워크 보안

❖ 네트워크 보안 과 관제 필요성

✓ 개인 정보 유출 피해

- 개인정보는 주로 해킹, 내부 직원 및 협력사 직원을 통해 유출되고 있는데 대표적인 사건으로 2008년 2월에 발생한 옥션에서 1,863만 명의 개인 정보가 해킹으로 인해 유출된 사건이 있고 2011년 싸이월드에서 해킹으로 3,500만 명의 개인정보가 유출되자 많은 사용자가 해당 사이트에서 탈퇴한 사건도 있는데 이 사건은 싸이월드의 기업 매출이 악화된 하나의 원인으로 꼽히게 되었으며 싸이월드의 많은 사용자에게 소송을 당하는 상황까지 발생
- 내부자에 의해 개인정보 유출 피해가 발생한 국민, 롯데, 농협 카드는 영업정지 3개월이라는 처벌을 받은 사례가 있으며 이 결과 기업의 순이익이 감소하는 상황으로 이어짐
- 위와 같은 개인정보 유출 뿐 만 아니라 개인정보보호법 강화로 인해 개인정보 취급 시에도 필요한 범위에서 최소한의 개인정보만 처리하거나 비식별화 처리를 반드시 해야하고 법에 따라 개인정보가 잘 지켜지고 있는지 확인해보도록 해야 함

네트워크 보안

- ❖ 네트워크 보안 과 관제 필요성
  - ✓ 악성 코드로 인한 피해
    - 악성코드 감염은 가장 빈번하게 일어나는 것으로 위험도가 낮은 악성코드는 피해가 작지만 위험도가 높고 지능화된 악성코드는 큰 피해로 이어질 수 있음
    - 2013년 3월 20일 국내 주요 언론(KBS, MBC, YTN) 전산망에서 3만 대 이상의 PC가 악성코드에 감염되어 피해를 입은 사건이 있었는데 사전에 기업 내 일부 PC를 감염시킨 후 필요한 정보를 수집하고 패치 관리 시스템을 장악하여 다수의 PC에 악성코드를 배포한 후 감염시켜 데이터 파일 및 부트 영역을 파괴한 것으로 이로 인해 업무를 원활히 진행할 수 없었으며 복구하는 데 막대한 시간과 비용이 발생함
    - 최근에는 컴퓨터의 문서와 사진 등 중요 파일들을 암호화하여 파일을 인질로 잡고 금전적 이득을 얻고자 하는 랜섬웨어가 기승을 부리고 있음
    - 한국수력원자력공사 해킹 사건은 APT(Advanced 지능형 지속 위협) 공격으로 특정 목표를 대상으로 지속적으로 공격을 수행하여 특정 목표가 위치한 곳까지 악성코드를 침투시키는 방식으로 특정 목표에 위치한 구성원들에게 지속적으로 악성 이메일을 발송하여 누군가 해당 악성 이메일을 확인하면 첨부된 악성코드를 실행시켜 내부까지 침투해서 공격자가 원하는 자료를 유출하는 방식
    - 악성코드 공격은 쉽게 탐지하기 어려우므로 악성 이메일을 확인하는 일이 없도록 기업의 구성원들을 대상으로 지속적으로 보안 교육을 시행하여 정보보안 의식을 강화해야 함

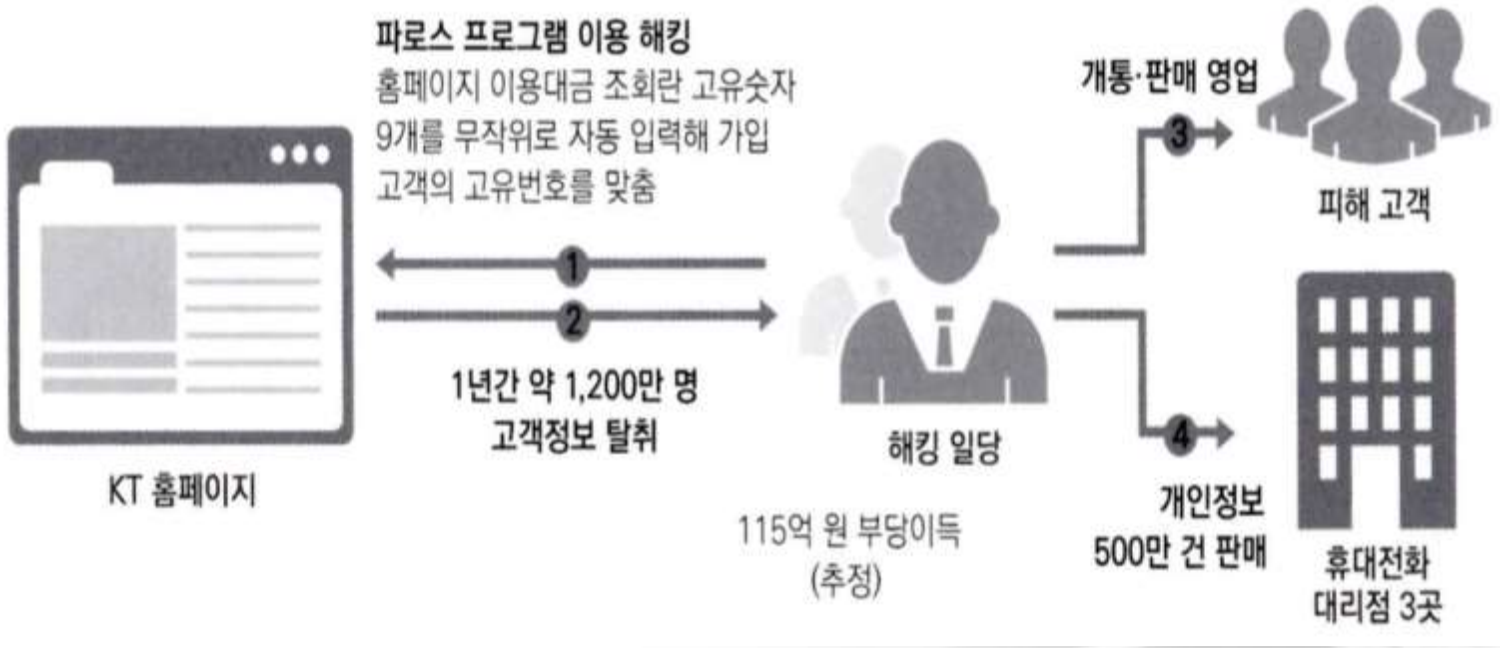
네트워크 보안

- ❖ 네트워크 보안 과 관제 필요성
  - ✓ 악성 코드로 인한 피해
    - 악성코드 감염은 가장 빈번하게 일어나는 것으로 위험도가 낮은 악성코드는 피해가 작지만 위험도가 높고 지능화된 악성코드는 큰 피해로 이어질 수 있음
    - 2013년 3월 20일 국내 주요 언론(KBS, MBC, YTN) 전산망에서 3만 대 이상의 PC가 악성코드에 감염되어 피해를 입은 사건이 있었는데 사전에 기업 내 일부 PC를 감염시킨 후 필요한 정보를 수집하고 패치 관리 시스템을 장악하여 다수의 PC에 악성코드를 배포한 후 감염시켜 데이터 파일 및 부트 영역을 파괴한 것으로 이로 인해 업무를 원활히 진행할 수 없었으며 복구하는 데 막대한 시간과 비용이 발생함
    - 최근에는 컴퓨터의 문서와 사진 등 중요 파일들을 암호화하여 파일을 인질로 잡고 금전적 이득을 얻고자 하는 랜섬웨어가 기승을 부리고 있음
    - 한국수력원자력공사 해킹 사건은 APT(Advanced 지능형 지속 위협) 공격으로 특정 목표를 대상으로 지속적으로 공격을 수행하여 특정 목표가 위치한 곳까지 악성코드를 침투시키는 방식으로 특정 목표에 위치한 구성원들에게 지속적으로 악성 이메일을 발송하여 누군가 해당 악성 이메일을 확인하면 첨부된 악성코드를 실행시켜 내부까지 침투해서 공격자가 원하는 자료를 유출하는 방식
    - 악성코드 공격은 쉽게 탐지하기 어려우므로 악성 이메일을 확인하는 일이 없도록 기업의 구성원들을 대상으로 지속적으로 보안 교육을 시행하여 정보보안 의식을 강화해야 함

네트워크 보안

❖ 네트워크 보안 과 관제 필요성

✓ 보안 취약점으로 인한 피해



네트워크 보안

- ❖ 네트워크 보안 과 관제 필요성
  - ✓ 보안 취약점으로 인한 피해
    - 내부 또는 외부를 대상으로 서비스하는 시스템이나 애플리케이션에 존재하는 취약점을 이용하여 공격자가 시스템 내부에 침투해 해당 데이터베이스에서 원하는 정보의 탈취, 홈페이지 변조, 악성코드 유포지로 활용하는 등의 피해가 발생하고 있음
    - 지난 2014년 3월 6일 KT 1,200만 명 개인정보 유출 사건은 KT 홈페이지의 이용대금 조회 서비스에서 고객 고유번호 9자리를 무작위로 입력할 수 있도록 도와주는 해킹 프로그램을 이용해 1년 동안 1.200만 명의 이름, 집 주소, 은행 계좌 등의 정보를 알아내 텔레마케팅 업체에 팔아 넘긴 사건
    - 해당 사건에 이용된 무작위 대입(Brute Force) 방식은 취약점을 공략하여 원하는 정보를 획득할 때 까지 공격하는 해킹 방식인데 무작위 대입 공격 방식은 횟수 제한이 없는 이상 정상으로 보이기 때문에 공격자가 취약점을 가진 페이지를 집중적으로 공략하여 지속적으로 정보를 획득해가도 해당 공격에 대한 탐지가 어렵지만 지속적으로 접근하거나 비정상으로 접근하는 횟수를 제한하는 방법을 사용했더라면 공격을 방어할 수 있었던 사건
    - KT 사건과 같은 해킹 방법 이외에도 최신 취약점을 이용한 공격들이 계속되고 있으므로 보안을 위해 운영하는 시스템과 서비스에 대해 보안 관제 뿐 만 아니라 최신 보안 패치와 보안성 진단 활동을 병행해야 하며 이 외에도 보유 중인 네트워크 장비와 인터넷 공유기의 보안 취약점들이 갱신되므로 주기적으로 업그레이드를 진행해야 함

네트워크 보안

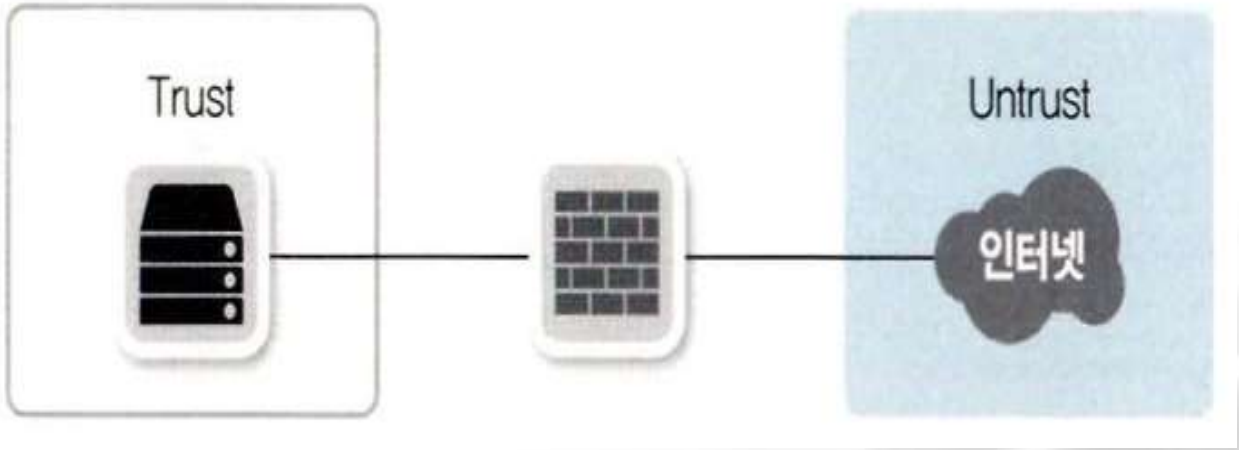
- ❖ 네트워크 보안 과 관제 필요성
  - ✓ 분산 서비스 거부 공격
    - 분산 서비스 거부 공격(DDoS - Distributed Denial of Service)은 악의적인 목적으로 특정 시스템의 자원을 소모하게 하여 정상적으로 서비스할 수 없게 방해하는 공격으로 공격자가 이미 보유한 좀비 PC에 명령을 내려 특정 사이트에 트래픽을 과도하게 보내는 방식과 명령 제어 서버없이 악성코드가 감염된 네트워크에서 특정 사이트나 네트워크에 과도한 트래픽을 유발하는 방식
    - 근래에 발생한 대표적인 서비스 거부 공격 사건으로는 7.7 DDoS, 3.4 DDoS가 있으며 주요 기관 과 은행 사이트를 공격함
    - 이외에도 중소기업이나 인터넷 서비스 업체들을 대상으로 지속적으로 서비스 거부 공격을 시도하여 피해가 발생하는 사건은 여전히 많이 발생하고 있음
    - 피해를 입은 업체 중에는 정상적인 웹 서비스를 할 수 없게 되어 금전적 피해가 발생한 업체들도 있음
    - 이와 같은 피해가 발생하지 않도록 보안 관제 활동을 통해 과도한 트래픽이 발생하고 있는지를 판단하고 별도의 서비스 거부 공격 방어 장비를 이용해 서비스 거부 공격을 방어할 수 있도록 해야 함

네트워크 보안

- ❖ 네트워크 보안 과 관제 필요성
  - ✓ 분산 서비스 거부 공격
    - ● 아이템베이 DDoS 공격 금품 요구 사건

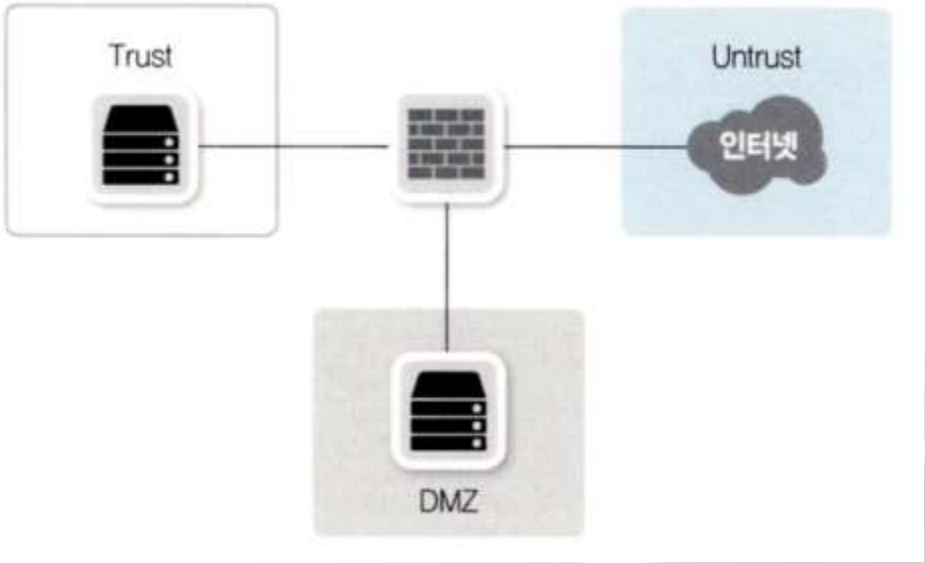
네트워크 보안

- ❖ 주요 개념
  - ✓ 정보 보안 별 네트워크 종류
    - 외부 네트워크로부터 내부 네트워크를 보호하는 것
    - 외부로부터 보호받아야 할 네트워크를 Trust 네트워크 신뢰할 수 없는 외부 네트워크를 untrust 네트워크로 구분



네트워크 보안

- ❖ 주요 개념
  - ✓ 정보 보안 별 네트워크 종류
    - 내부 네트워크이지만 신뢰할 수 없는 외부 사용자에게 개방해야 하는 서비스 네트워크인 경우 DMZ(De Militarized Zone) 네트워크라고 부르며 일반적으로 인터넷에 공개되는 서비스를 이 네트워크에 배치

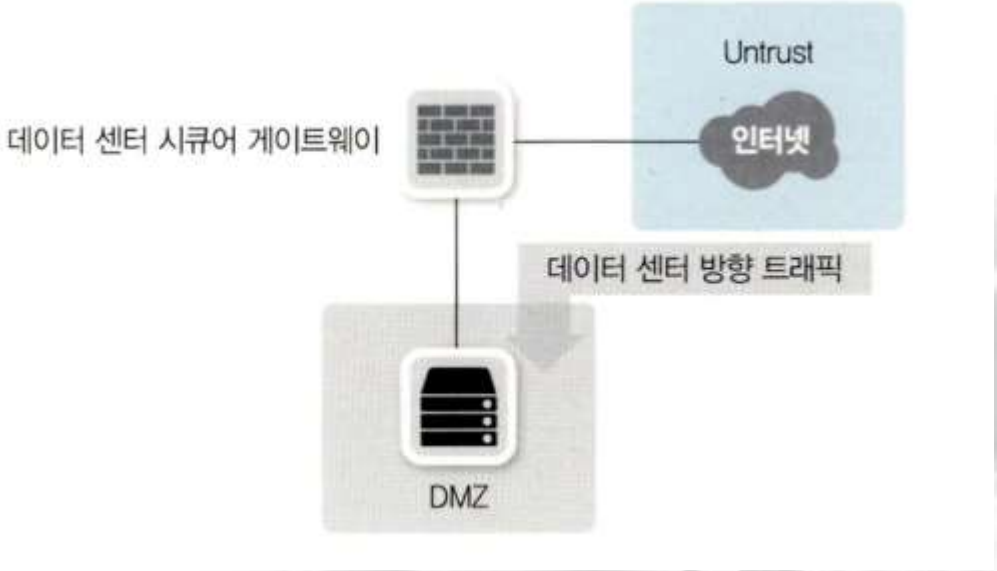


네트워크 보안

- ❖ 주요 개념
  - ✓ 정보 보안 별 네트워크 종류
    - ● 트래픽의 방향과 용도에 따른 네트워크 보안 분야 분류
      - ◆ 인터넷 시큐어 게이트웨이(Internet Secure Gateway)
        - ▪ 트러스트(또는 DMZ) 네트워크에서 언트러스트 네트워크로의 통신을 통제
        - ▪ 인터넷으로 나갈 때는 인터넷에 수많은 서비스가 있으므로 그에 대한 정보와 요청 패킷을 적절히 인식하고 필터링하는 기능이 필요함
        - ▪ 데이터 센터 게이트웨이는 상대적으로 고성능이 필요하고 외부의 직접적인 공격을 막아야 하므로 인터넷 관련 정보보다 공격 관련 정보가 더 중요
        - ▪ 전자의 경우를 인터넷 시큐어 게이트웨이라고 하며 방화벽, SWG(Secure Web Gateway), 웹 필터(Web Filter), 애플리케이션 컨트롤(Application Control), 샌드박스(Sandbox)와 같은 다양한 서비스나 네트워크 장비가 포함되며 보안을 제공, 통제하기 위해 사용되는데 이런 서비스와 보안 장비들은 내부 사용자가 인터넷으로 통신할 때 사용

네트워크 보안

- ❖ 주요 개념
  - ✓ 정보 보안 별 네트워크 종류
    - ● 트래픽의 방향과 용도에 따른 네트워크 보안 분야 분류
      - ◆ 데이터 센터 시큐어 게이트웨이(Data Center Secure Gateway)
        - ▪ 언트러스트 네트워크에서 트러스트(또는 DMZ)로의 통신을 통제
        - ▪ 방화벽, IPS, DCSG(Data Center Secure Gateway), WAF(Web Application Firewall), Anti-DDoS(Distribute Denial of Service) 등의 장비가 이런 용도로 사용



네트워크 보안

- ❖ 주요 개념
  - ✓ 네트워크 보안 정책 수립에 따른 분류
    - White List
      - ◆ 화이트리스트는 방어에 문제가 없다고 명확히 판단되는 통신만 허용하는 방식
      - ◆ 인터넷 전체에 대한 화이트리스트를 만들기 어려우므로 일반적으로 IP와 통신 정보에 대해 명확히 아는 경우에 많이 사용
      - ◆ 일반적으로 회사 내부에서 사용하는 방화벽이 명확한 정책에 의해 필요한 서비스만 허용하는 화이트리스트 방식을 주로 사용
    - Black List
      - ◆ 블랙리스트 방어는 공격이라고 명확히 판단되거나 문제가 있었던 IP 리스트나 패킷 리스트를 기반으로 데이터베이스를 만들고 그 정보를 이용해 방어하는 형태
      - ◆ 각종 패턴으로 공격을 방어하는 네트워크 장비(IPS, 안티바이러스, WAF)들은 일반적으로 블랙리스트 기반의 방어 기법을 제공
      - ◆ 인터넷 어디선가 공격을 당할 때 이것을 분석해 공격 기법을 판단해 탐지하도록 간단히 적어 데이터베이스(시그니처)로 생성

네트워크 보안

- ❖ 주요 개념
  - ✓ 네트워크 보안 정책 수립에 따른 분류
    - 네트워크 보안 장비는 화이트리스트나 블랙리스트 기반 중 하나만 목표로 만들 때도 있음
    - IPS, 안티바이러스처럼 악성 코드나 공격 기법에 대한 시그니처를 만들고 이 데이터베이스들을 업데이트 받아 동작하는 장비가 블랙 리스트 기반 장비
    - 대부분의 장비는 수립 정책에 따라 화이트리스트 기법과 블랙리스트 기법 모두 사용할 수 있음
    - 같은 방화벽이라도 IP 주소 정책을 잘 아는 IP 주소만 정책으로 열어놓고 나머지 주소로 가는 모든 패킷을 방어할 때는 화이트리스트 기반 정책으로 운영할 수 있음
    - 반대로 기존에 해킹을 시도했던 IP 리스트를 작성해 그 IP들만 방어할 때는 블랙리스트 기반으로 운영될 수 있음
    - 최근 보안 위협이 증가하면서 화이트리스트 기반 정책이 많이 사용되고 있는데 화이트리스트 기반 정책을 수립하려면 통신 정보를 상세히 알아야 하고 세부적인 통제가 필요하기 때문에 많은 관리 인력이 필요할 수 있으므로 보안 관리 인력이 부족한 경우 블랙 리스트 기반 방어 정책을 수립하고 공격 데이터베이스를 최신으로 유지하는 것이 안정적인 보안 운영을 위해 바람직

네트워크 보안

- ❖ 주요 개념
  - ✓ 탐지 에러 타입
    - IPS나 안티바이러스와 같은 네트워크 장비에서는 공격 데이터베이스에 따라 공격과 악성 코드를 구분해 방어
    - 공격 데이터베이스를 아무리 정교하게 만들더라도 공격으로 탐지하지 못하거나 공격이 아닌데도 공격으로 감지해 패킷을 드롭시킬 때가 있는데 블랙리스트 기반 데이터베이스를 이용한 방어는 이런 문제점이 있으므로 장비 도입 시 정교한 튜닝이 필요
    - 공격을 탐지할 때 예상과 다른 결과가 나올 수 있는데 이런 경우를 오탐지, 미탐지로 구분하고 정상적으로 탐지한 경우를 정상 탐지로 표현

네트워크 보안

❖ 주요 개념

✓ 탐지 에러 타입

● 공격과 탐지 도표

	공격 상황	정상 상황
공격 인지 (공격 알람)	True Positive (정상 탐지)	False Positive (오 탐지)
정상 인지 (공격 알람 없음)	False Negative (미 탐지)	True Negative (정상 탐지)

◆ 의미

- Yes 라고 추론했는데 정답이 Yes인 경우(공격이라고 추론했는데 실제로 공격인 경우): True Positive(정탐)
- No 라고 추론했는데 정답이 No인 경우(공격이 아니라고 추론했는데 실제로 공격이 아닌 경우): True Negative(정탐)
- Yes라고 추론했는데 정답이 No인 경우(공격이라고 추론해 드롭했는데 공격이 아닌 경우): False Positive(오탐)
- No라고 추론했는데 정답이 Yes인 경우(공격이 아니라고 패킷을 허용했는데 실제로 공격인 경우): False Negative(미탐)

네트워크 보안

- ❖ 주요 개념
  - ✓ 탐지 에러 타입
    - ● 공격과 탐지 도표
      - ◆ 첫번째 와 두번째 경우는 실제 공격과 공격이 아닌 패킷을 잘 분류해냈으므로 정상적인 동작인데 이런 경우를 정탐(정상 탐지)이라고 부름
      - ◆ 세번째 와 네번째 경우는 원래 예상했던 결과와 실제 동작이 다른 경우
      - ◆ 세번째 경우는 공격이라고 생각해 패킷을 드롭했지만 실제로는 공격이 아닌 정상 패킷인 경우인데 이런 경우를 오탐(오 탐지) 이라고 부르는데 공격으로 오인한 탐지이므로 이런 경우가 발생하면 예외로 처리해 오탐을 줄이는 튜닝 작업이 필요
      - ◆ 네번째 경우는 공격이 아니라고 판단했지만 실제로는 공격이었던 경우인데 이런 경우는 공격 패턴에 대한 업데이트가 되지 않았거나 과도한 예외 처리로 공격 패킷 탐지가 정상적으로 되지 않았을 때 발생하는데 공격 데이터베이스가 업데이트되기 전에 발생하는 제로 데이 공격(Zero-Day Attack)이 발생했을 때도 False Positive 오류가 생길 수 있음
      - ◆ 최근 보안 벤더들은 화이트리스트 기반의 공격 방어 기법과 블랙리스트 기반의 공격 방어 기법을 적절히 섞어 사용할 것을 권고하는데 나날이 복잡해지고 악랄해지는 사이버 공격을 쉽게 방어하기는 어려우므로 항상 관심을 가지고 보안을 위해 노력해야 함

네트워크 보안

- ❖ 주요 개념
  - ✓ 네트워크 정보 보안의 발전 추세와 고려사항
    - 네트워크 보안은 중요한 1차 방어선이므로 다양한 공격을 다양한 방법으로 방어하기 위한 노력이 모여 복잡한 양상으로 발전
    - 네트워크 보안 장비와 서비스가 개발되는 이유를 이해하면 장비들의 역할도 쉽게 학습하고 향후 발전 방향도 추측할 수 있음
    - 네트워크 보안 장비는 보안 영역 외부와 내부의 변화로 발전
    - 보안 영역 외부는 인프라스트럭처나 서비스의 대변화로 인해 보안이 따라서 발전해야 하는 경우이고 보안 영역 내부는 해킹 기술의 발전에 대응하다보니 새로운 보안 장비와 서비스가 개발되어 발전하는 경우
    - 네트워크나 서비스의 큰 변화는 보통 필요에 의한 변화이므로 보안이 고려되지 않는 경우가 많은데 이런 경우 보안을 뒤늦게 고려하게 되고 보안 내부적인 변화가 아니어서 쉽게 대응하기 어려움
    - 최근 IT산업 자체에 큰 변화가 있고 보안이 그 변화를 쫓아가는 데 큰 어려움을 겪고 있지만 반대로 이런 변화를 수용해 보안 장비가 발전하기도 함

네트워크 보안

❖ 주요 개념

✓ 네트워크 정보 보안의 발전 추세와 고려사항

- 많이 언급되는 빅데이터(Big Data)와 머신 러닝(Machine Learning) 부분이 특히 그런데 빅데이터가 유행할 때 해당 서비스의 보안 유지를 걱정스럽게 바라보았다면 반대로 빅데이터와 머신 러닝 기법을 보안에 적용해 공격에 더 신속히 대응하는 시스템과 서비스를 개발하려는 움직임이 많아짐
- 최근 악성 코드에 대응하는 많은 업체들이 이 기술들을 활용해 단기간에 새로운 변종 악성 코드를 막도록 내부 시스템을 개발하고 외부에도 서비스를 제공
- 네트워크 보안 장비와 서비스를 이해하려면 인프라스트럭처의 변화와 해킹 기법의 발전을 모두 이해해야 하고 반대로 인프라스트럭처의 발전을 이용해 더 높은 수준의 네트워크 보안을 제공하는 보안업체의 대응도 눈여겨 보아야 함

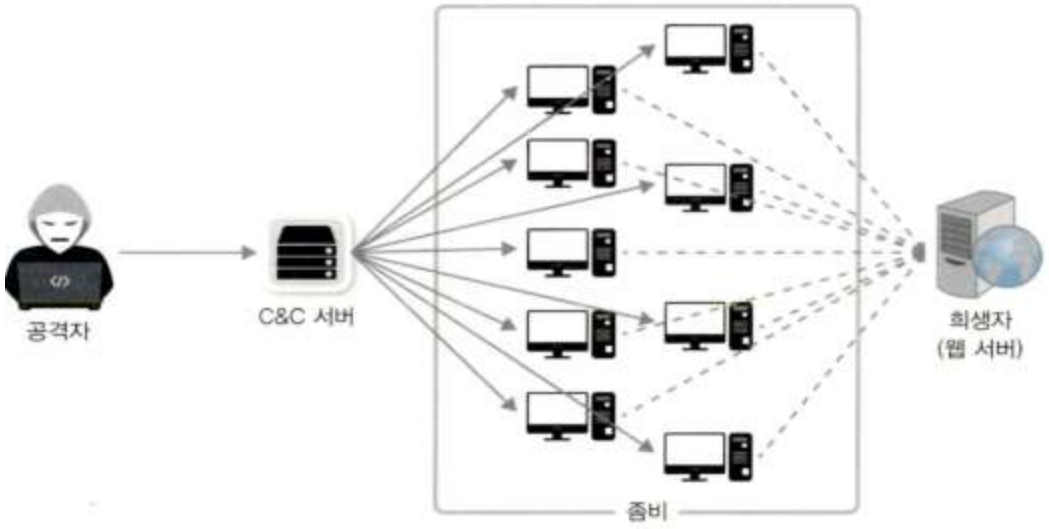
보안 솔루션

❖ 개요

- ✓ 해커들의 공격이 점점 악랄해지고 공격 기법도 나날이 발전해 이런 공격을 막는 보안 진영에서도 방어를 위한 다양한 시도와 새로운 기능의 장비 개발이 진행되고 있음
- ✓ 보안을 위한 다양한 솔루션은 방어 가능한 범위가 다름
- ✓ 새로운 형태의 장비가 출시되었더라도 기존 보안 장비가 필요없는 것이 아니라 기존 보안 장비에 새로운 보안 솔루션이 도움을 주는 형태가 되므로 보안은 타 IT 분야보다 복잡한 형태를 가짐
- ✓ 데이터 센터에서 보안 장비를 디자인할 때 DDoS – 방화벽 - IPS - WAF 형태와 같이 여러 단계로 공격을 막도록 인라인 상에 여러 장비를 배치
- ✓ 한 대로는 방어할 수 없으므로 여러 장비의 기능으로 단계적으로 방어
- ✓ 네트워크 전체 구성

보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ DDoS 공격
    - DoS 공격은 Denial of Service 공격의 약자로 다양한 방법으로 공격 목표에 서비스 부하를 가해 정상적인 서비스를 방해하는 공격 기법
    - DoS 공격은 적이 공격 출발지에서 공격하는 것이 일반적 이었으므로 비교적 탐지가 쉽고 짧은 시간 안에 탐지만 할 수 있다면 IP 주소 기반으로 충분히 방어할 수 있음
    - 이런 탐지를 회피하고 더 짧은 시간 안에 공격 성과를 내기 위해 다수의 봇을 이용해 분산 공격을 수행하는 DDoS 공격 기법이 등장
    - DDoS 공격 형태

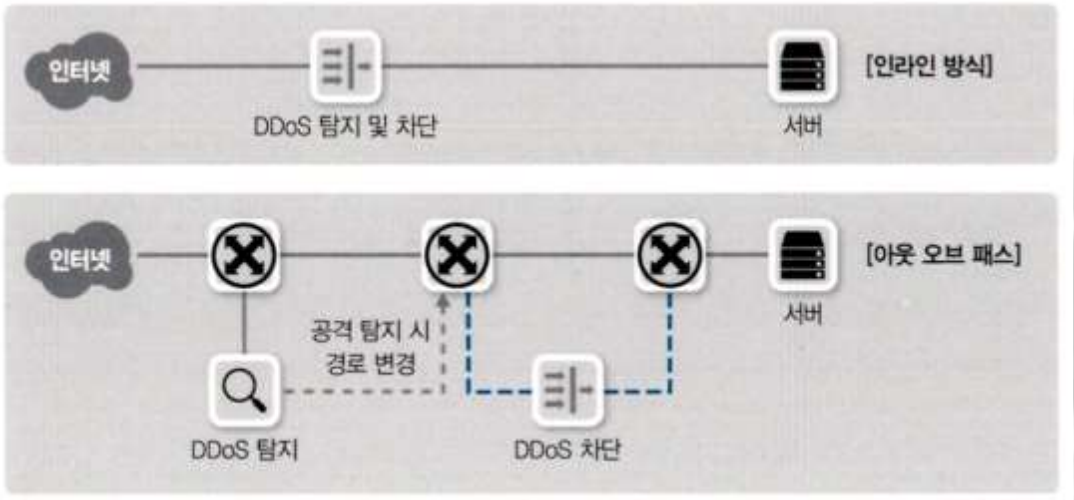


보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ DDoS 방어 장비
    - ● 초기 DDoS 공격은 시스템이나 네트워크 장비의 취약점이 타깃인 경우가 많았는데 단순한 서버 공격에서 네트워크 장비나 DNS 서비스와 같이 인프라 기반 서비스 제공 영역까지 DDoS 공격이 확대됨
    - ● 단순한 DDoS 형태의 공격들도 다양한 기존 장비를 보완하는 기능이 나오고 취약점을 노린 DDoS 공격도 제조업체들의 보안 패치 대응으로 큰 효과를 발휘하지 못하자 다양한 DDoS 공격 형태가 등장함
    - ● 다양한 DDoS 공격을 방어하기 위한 전문적인 장비의 필요성이 대두되었고 DDoS 전용 방어 장비가 나타남
    - ● DDoS 방어 장비는 볼류메트릭 공격을 방어하기 위해 트래픽 프로파일링 기법을 주로 사용하고 인터넷의 다양한 공격 정보를 수집한 데이터베이스를 활용하기도 함

보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ DDoS 방어 장비 동작 방식
    - DDoS 방어 서비스로는 클라우드 서비스, 회선 사업자의 방어 서비스, DDoS 방어 장비를 사내에 설치하는 방법이 있음
    - 회선 사업자와 DDoS 방어 장비를 이원화해 협조하는 서비스도 많이 등장하고 있음
    - DDoS는 워낙 대규모 공격이므로 DDoS 탐지 장비와 방어 장비를 구분하는 경우가 많음
    - DDoS 공격을 탐지해 공격을 수행하는 IP 리스트를 넘겨주면 방어 장비나 ISP 내부에서 이 IP를 버리는 것이 가장 흔한 DDoS 방어 기법



보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ DDoS 방어 장비 동작 방식
    - DDoS 장비가 DDoS 여부를 판별하는 방식은 다양
    - 프로파일링 기법은 평소 데이터 흐름을 습득해 일반적인 대역폭, 초기 접속량, 프로토콜별 사용량 등을 저장한 후 습득한 데이터와 일치하지 않는 과도한 트래픽이 인입되면 알려주고 차단하는 방식으로 습득한 데이터는 다양한 날짜 범위와 다양한 요소를 모니터링
    - 다른 방법으로는 일반적인 보안 장비처럼 보안 데이터베이스 기반으로 방어하는 것으로 ip 평판 데이터베이스를 공유해 DDoS 공격으로 사용된 IP 기반으로 방어 여부를 결정하거나 특정 공격 패턴을 방어하는 방법

보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ DDoS 공격 타입
    - DDoS 공격은 다양한 기법이 있지만 일반적으로 회선 사용량을 가득 채우는 볼류메트릭 공격(Volumetric Attack)과 3, 4계층의 취약점과 리소스 고갈을 노리는 프로토콜 공격(Protocol Attack), 애플리케이션의 취약점을 주로 노리는 애플리케이션 공격(Application Attack.) 3가지

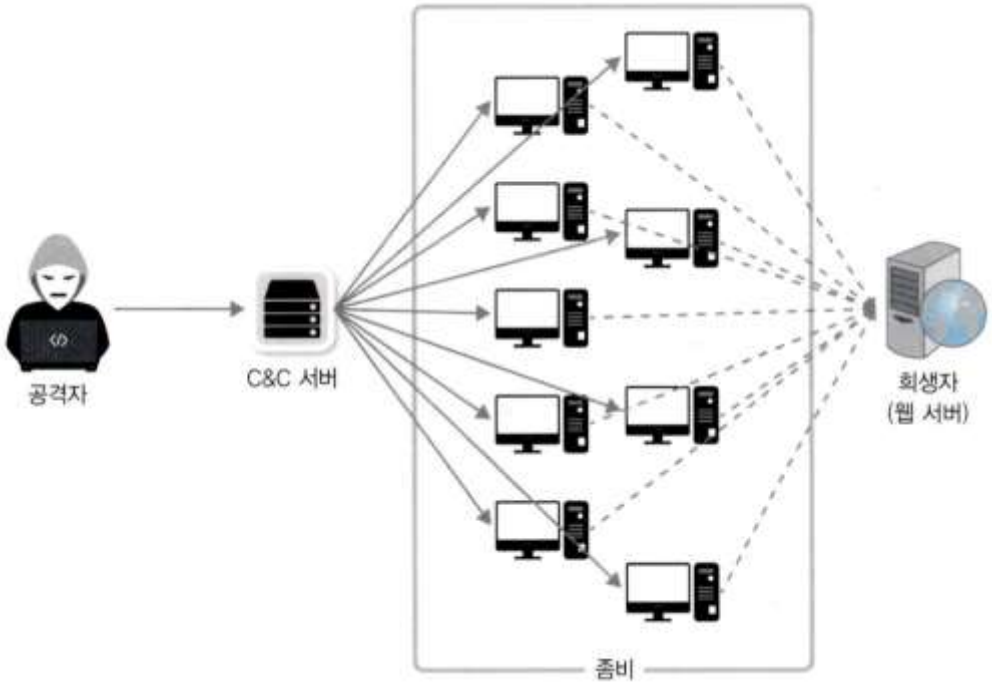
	볼류메트릭 공격	프로토콜 공격	애플리케이션 공격
무엇인가	대용량의 트래픽을 사용해 공격 대상의 대역폭을 포화시키는 공격. 간단한 증폭기술을 사용해 생성하기 쉬움	3, 4계층 프로토콜 스택의 취약점을 악용해 대상을 액세스할 수 있게 만드는 공격	7계층 프로토콜 스택의 약점을 악용하는 공격. 가장 정교한 공격 및 식별, 완화에 가장 까다로운 공격
장애를 어떻게 일으키는가	공격에 의해 생성된 트래픽 양은 최종 자원(웹 사이트 또는 서비스)에 대한 액세스를 완전히 차단할 수 있음. 쓸모없는 패킷이 회선을 모두 차지해 정상적인 서비스 트래픽이 통과할 수 없음.	공격 대상이나 중간 위험 리소스의 처리 용량을 모두 사용해 서비스 중단을 유발함. 일반적인 네트워크 장비나 네트워크 보안 장비를 대상으로 하는 경우가 많음. 공격 대상 장비의 CPU, 메모리 자원을 고갈시켜 정상적인 서비스가 불가능하게 함.	대상과의 연결을 설정한 후 프로세스와 트랜잭션을 독점해 서버 자원을 소모시킴. 애플리케이션 프로토콜 자체의 취약점이나 서비스를 제공하는 플랫폼의 취약점을 악용하는 경우가 많음.
예제	NTP 증폭, DNS 증폭, UDP 플러드(UDP Flood), TCP 플러드	Syn 플러드, Ping of Death	HTTP 플러드, DNS 서비스 공격, Slowloris 등

보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ 볼류 메트릭 공격
    - 볼류메트릭 공격은 회선 사용량이나 그 이상의 트래픽을 과도하게 발생시켜 회선을 사용하지 못하도록 방해하는 공격이므로 회선을 공급해주는 ISP 내부나 사용자 네트워크 최상단에 위치시켜 이 공격을 완화(Mitigation)해야 함
    - DDoS 장비는 주로 볼류메트릭 공격이나 프로토콜 공격을 방어하는 데 사용되는데 혼자 방어할 수 없는 공격도 많으므로 회선을 공급하는 ISP와 공조해 방어할 필요가 있음

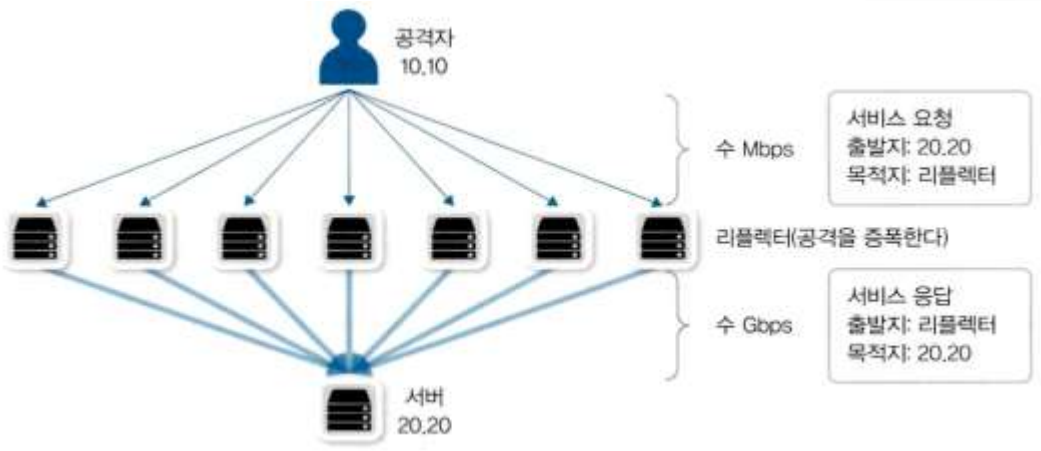
보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ 볼류 메트릭 공격
    - ● 좀비 PC를 이용한 볼류 메트릭 공격
      - ◆ 볼류메트릭 공격은 특정 시간에 특정 타깃을 공격하는 형태로 발생
      - ◆ 이런 공격을 하려면 미리 악성 코드에 감염되어 해커가 컨트롤할 수 있는 좀비 PC를 많이 확보해두어야 함



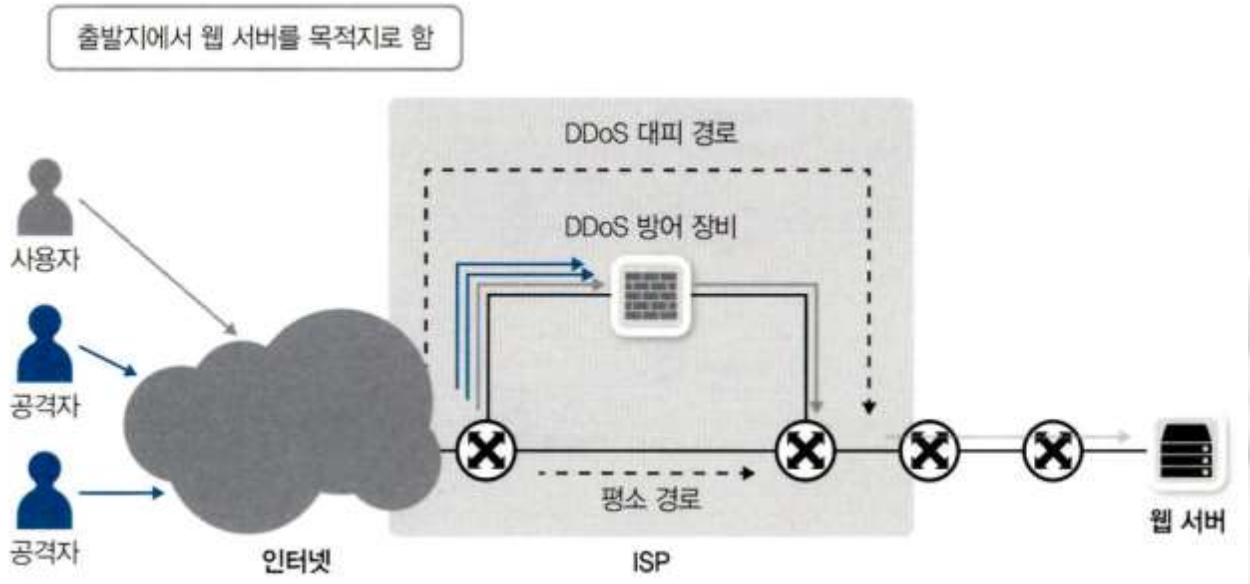
보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ 볼류 메트릭 공격
    - ● 좀비 PC를 이용한 볼류 메트릭 공격
      - ◆ 좀비 PC를 미 리 충분히 확보하지 못하거나 더 강력한 DDoS 공격을 위한 증폭 공격(Amplification Attack)이 증가
      - ◆ 수백 Gbps부터 1Tbps 이상에 이르는 엄청나게 높은 대역폭의 공격은 대부분 증폭 공격으로 수행
      - ◆ 공격자가 상대적으로 적은 대역폭으로 중간 리플렉터에 패킷을 보내면 이 트래픽이 증폭되어 피해자 네트워크에 수십 ~ 수백 배의 공격 트래픽이 발생하는 공격법이 증폭 공격



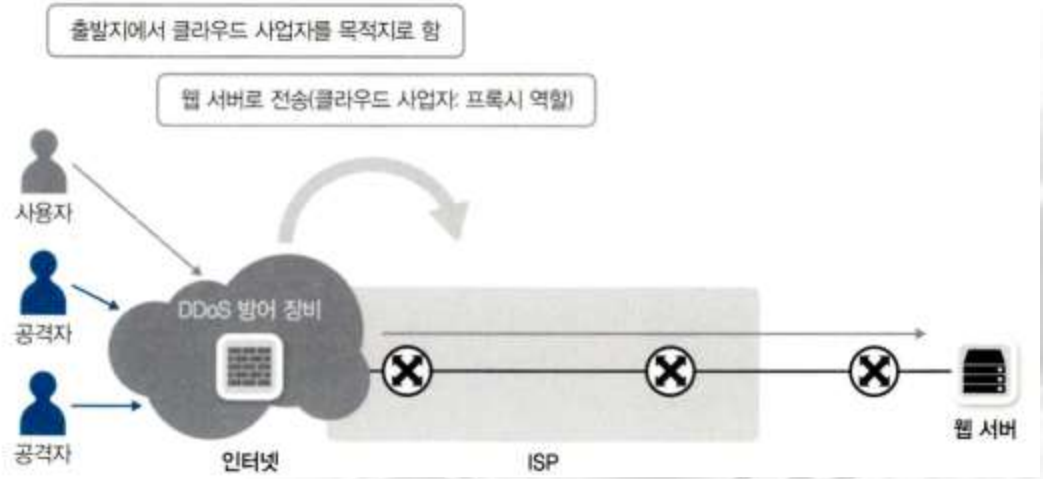
보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ 볼류 메트릭 공격
    - ● 좀비 PC를 이용한 볼류 메트릭 공격
      - ◆ 볼류메트릭 공격을 방어할 수 있는 DDoS 장비를 보유하는 것도 중요하지만 혼자서는 대부분 방어가 불가능하므로 ISP를 통한 방어나 Cloud DDoS 솔루션을 통해 서비스 네트워크로 트래픽이 직접 도달하지 못하도록 조치
      - ◆ ISP에서 제공하는 DDoS 방어 서비스



보안 솔루션

- ❖ DDoS 방어 장비
  - ✓ 볼류 메트릭 공격
    - ● 좀비 PC를 이용한 볼류 메트릭 공격
      - ◆ 볼류메트릭 공격 방어를 위해 클라우드 기반의 DDoS 방어 서비스도 고려해볼 수 있는데 클라우드 기반 서비스는 DDoS, WAF(Web Application Firewall)과 같은 별도의 보안 장비 없이도 다양한 DDoS 공격을 방어할 수 있다는 장점이 있음
      - ◆ 실제 서비스 서버 앞에서 미리 클라이언트의 요청을 받아 처리한 후 문제가 없는 요청만 서버 쪽으로 전달하는 방식
      - ◆ 클라우드 기반 서비스의 최대 장점은 실제 서비스 네트워크가 가려지므로 네트워크 차원이나 대규모 볼류메트릭 공격도 큰 투자 없이 방어할 수 있다는 것



보안 솔루션

- 방화벽
  - ✓ 방화벽은 4 계층에서 동작하는 패킷 필터링 장비
  - ✓ 계층 정보를 기반으로 정책을 세울 수 있고 해당 정책과 매치되는 패킷이 방화벽을 통과하면 그 패킷을 허용(Allow, Permit)하거나 거부(Deny) 할 수 있음
  - ✓ 일반적으로 방화벽은 DDoS 방어 장비 바로 뒤에 놓는 네트워크 보안 장비
  - ✓ 3, 4 계층에서 동작하므로 다른 보안 장비보다 비교적 간단히 동작하고 성능도 우수
  - ✓ 최근 출시되는 고성능 방화벽은 ASIC이나 FPGA와 같은 전용 칩을 이용해 가속하므로 대용량을 요구하는 데이터 센터에서도 문제없이 사용 가능

보안 솔루션

- 방화벽
  - ✓ 방화벽은 4 계층에서 동작하는 패킷 필터링 장비
  - ✓ 계층 정보를 기반으로 정책을 세울 수 있고 해당 정책과 매치되는 패킷이 방화벽을 통과하면 그 패킷을 허용(Allow, Permit)하거나 거부(Deny) 할 수 있음
  - ✓ 일반적으로 방화벽은 DDoS 방어 장비 바로 뒤에 놓는 네트워크 보안 장비
  - ✓ 3, 4 계층에서 동작하므로 다른 보안 장비보다 비교적 간단히 동작하고 성능도 우수
  - ✓ 최근 출시되는 고성능 방화벽은 ASIC이나 FPGA와 같은 전용 칩을 이용해 가속하므로 대용량을 요구하는 데이터 센터에서도 문제없이 사용 가능

보안 솔루션

- IDS, IPS
  - ✓ IDS(Intrusion Detection System - 침입 탐지 시스템)와 IPS(Intrusion Prevention System - 침입 방지 시스템)는 방화벽에서 방어할 수 없는 다양한 애플리케이션 공격을 방어하는 장비
  - ✓ 기존에는 IDS 와 IPS 장비를 구분했지만 최근에는 애플리케이션 공격을 방어하는 장비를 IPS로 통칭
  - ✓ IDS와 IPS는 사전에 공격 데이터베이스(Signature)를 제조사나 위협 인텔리전스'(Threat Intelligence)서비스 업체로부터 받고 이후 IDS와 IPS 장비에 인입된 패킷이 보유한 공격 데이터베이스에 해당하는 공격일 때 차단하거나 모니터링한 후 관리자에게 알람을 보내 공격 시도를 알림
  - ✓ 기존에는 공격인 것만 골라 방어하는 블랙리스트 기반의 방어 방식만 제공했지만 프로파일링 기반의 방어 기법이 IPS 장비에 적용되고 애플리케이션을 골라 방어할 수 있는 애플리케이션 컨트롤(Application Control) 기능이 추가되면서 화이트리스트 기반의 방어 기법도 IPS 장비에 적용할 수 있게 됨
  - ✓ 최근에는 데이터 센터 영역의 보안을 위해 방화벽과 IPS 장비를 통합한 DCSG 장비(Disaggregated Cell Site Gateway의 약자로 5G 이동통신 기지국(Cell Site)에서 발생하는 대량의 데이터를 효율적으로 처리하기 위해 하드웨어와 소프트웨어를 분리한 개방형 네트워크 장비) 시장이 커지고 있음

보안 솔루션

- WAF
  - ✓ WAF(Web Application Firewall)는 웹 서버를 보호하는 전용 보안 장비로 HTTP. HTTPS처럼 웹 서버에서 동작하는 웹 프로토콜의 공격을 방어
  - ✓ IDS/IPS 장비보다 범용성이 떨어지지만 웹 프로토콜에 대해서는 더 세밀히 방어할 수 있음
  - ✓ WAF는 다양한 형태의 장비나 소프트웨어로 제공
    - 전용 네트워크 장비
    - 웹 서버의 플러그인
    - ADC(Application Delivery Controller - 애플리케이션 전송 컨트롤러는 특정 환경 즉 클라우드, 컨테이너, 특정 제조사 장비에 통합하거나 확장하기 위해 사용하는 소프트웨어 모듈) 플러그인
    - 프록시 장비 플러그인
  - ✓ WAF는 IPS에서 방어할 수 없는 IPS 회피 공격(Exasion Attack)을 방어할 수 있는데 IPS는 데이터를 조합하지 않고 처리하지만 WAF는 프록시 서버와 같이 패킷을 데이터 형태로 조합해 처리하기 때문에 회피 공격을 쉽게 만들기 어렵고 데이터의 일부를 수정, 추가하는 기능을 수행할 수 있음
  - ✓ 공격 트래픽을 방어만 하지 않고 공격자에게 통보하거나 민감한 데이터가 유출될 때 그 정보만 제거해 보내줄 수 있음
  - ✓ IPS는 공격을 차단한 후 그에 대한 통보가 어렵고 전체 공격 내용에 대한 차단만 가능

보안 솔루션

- 샌드박스
  - ✓ 기존에는 해커가 원하는 목적지에 직접 공격을 수행했음
  - ✓ 자신을 숨기기 위해 경유지를 통한 공격 외에는 직접적인 공격이 가장 쉬운 방법이었는데 이런 공격을 방어할 수단도 많지 않았고 전문적인 보안 장비가 많이 사용되지 않았기 때문
  - ✓ 보안 장비들이 발전하면서 해커들이 방화벽을 직접 뚫고 원하는 목적지로 공격하는 것이 점점 어려워짐
  - ✓ 해커들은 보안 장비를 우회하기 위해 기존과 다른 방향의 공격을 개발하게 됨
  - ✓ 직접적인 공격 기법 중 기존 보안 장비들을 우회하는 기법들이 많아졌지만 근본적으로 공격 방법이 변함
  - ✓ 직접적인 공격을 원하는 서버에 접근하지 않고 악성 코드를 관리자 PC에 우회적으로 심고 이 악성 코드를 이용해 관리자 PC를 컨트롤하는 방식으로 공격 목표가 변함
  - ✓ 악성 코드가 든 이메일을 관리자에게 직접 보내거나 관리자가 악성 코드를 내려받도록 다양한 방법으로 유도
  - ✓ 유명한 웹 사이트에 악성 코드가 포함된 낚시성 파일을 올려놓고. 영화 파일이나 유틸리티 프로그램을 실행하면 악성 코드가 동작하도록 파일을 변경한 후 사용자가 직접 내려받도록 유도해 PC를 악성 코드에 감염시킴
  - ✓ 이후 이 PC들을 외부에서 컨트롤하도록 C&C(Command & Control) 서버를 만들어놓고 감염 PC들이 이 C&C 서버로 연결하도록 조작하는데 이때 기존 방화벽에서는 내부 사용자가 외부 서버로 통신을 정상적으로 시도한 것으로 보이므로 이 공격을 검출하거나 방어할 수 없음

보안 솔루션

- 샌드박스
  - ✓ 이 공격들이 발전해 현재 APT(Advanced Persistent Threat - 지능형 지속 공격) 와 ATA(Advanced Target Attack - 지능형 표적 공격)가 됨
  - ✓ APT 와 ATA의 공격을 막기 위해 IPS 장비와 C&C 서버와의 통신을 탐지할 수 있는 다양한 형태의 Anti-APT 솔루션들이 개발됨
  - ✓ 샌드박스는 APT의 공격을 방어하는 대표적인 장비로 악성 코드를 샌드박스 시스템 안에서 직접 실행 시킴
  - ✓ 가상 운영체제 안에서 각종 파일을 직접 실행시키고 그 행동을 모니터링해 그 파일들의 악성 코드 여부를 판별하는 방법을 이용
  - ✓ 이 방법은 기존 보안 장비와 보안 솔루션들을 피하는 회피 공격을 탐지하고 기존 보안 솔루션들을 보완
  - ✓ 최근 악성 코드들은 다크웹에서 코드가 공개되거나 사고팔리는 경우가 많아 재사용 됨 짧은 기간에 다양한 변종이 출현해 탐지하기 어렵고 기존 보안 시스템이 공격을 탐지하지 못하도록 암호화 또는 난독화하거나 매우 오랫동안 여러 단계를 거쳐 공격
  - ✓ 파일을 직접 실행한 후 파일의 행동을 모니터링하면 이런 악성 코드를 감싼 많은 트릭을 제거하거나 탐지할 수 있음
  - ✓ APT의 공격을 하나의 장비만으로 방어할 수는 없고 다양한 보안 장비와 솔루션 그리고새로운 공격을 방어해주는 장비 간에 유기적으로 협업해야만 탐지하고 방어 할 수 있음

보안 솔루션

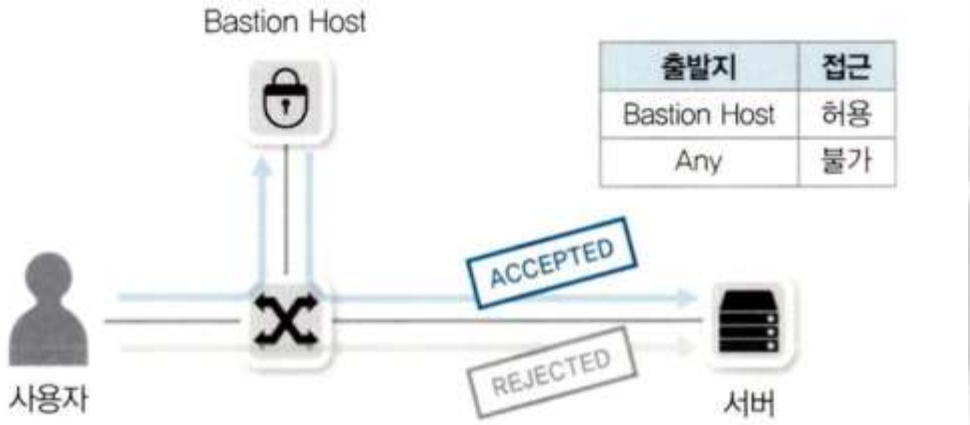
- NAC
  - ✓ NAC(Network Access Control)은 네트워크에 접속하는 장치들을 제어하기 위해 개발
  - ✓ 네트워크에 접속할 때 인가된 사용자만 내부망에 접속할 수 있고 인가받기 전이나 승인에 실패한 사용자는 접속할 수 없도록 제어하는 기술
  - ✓ 내부 PC를 아무리 잘 관리하고 보안 패치를 신속히 수행하더라도 외부 PC가 내부망에 접속해 보안사고를 일으키거나 악성 코드를 전파하는 문제점들이 많이 발생하자 이것을 해결하기 위해 개발

보안 솔루션

- IP 제어
  - ✓ IP 제어 솔루션은 겉으로 보면 NAC 솔루션과 공통적인 기술을 이용하거나 기능이 비슷한 경우도 하지만 IP 제어 솔루션은 국내에서 많이 사용하는 기술로 NAC과 다른 목적으로 개발
  - ✓ 보안사고 추적이 쉽도록 고정 IP 사용 권고 지침이 금융권에 내려오면서 IP를 할당하고 추적하는 솔루션이 필요해졌고 할당된 IP를 관리하고 나아가 정확히 의도된 IP 할당이 아니면 정상적으로 네트워크를 사용하지 못하게 하는 기능이 필요
  - ✓ 이 요구사항들을 구현하기 시작한 것이 IP 제어 솔루션

보안 솔루션

- 접근 통제
  - ✓ 운영자가 서버, 데이터베이스, 네트워크 장비에 직접 접근해 관리하면 각 시스템에서 사용자에 대한 권한을 관리해야 하는데 문제가 발생했을 때 관리자가 작업 내용을 추적하고 감사하기 어려움
  - ✓ 이 문제를 해결하기 위해 서버나 데이터베이스에 대한 직접적인 접근을 막고 작업 추적 및 감사를 할 수 있는 접근 통제 솔루션이 개발됨
  - ✓ 접근 통제 솔루션도 에이전트 기반(Agent Based), 에이전트리스(Agentless) 등 구현 방법에 따라 다양하게 분류할 수 있지만 대부분 배스천 호스트(Bastion Host) 기반으로 구현
  - ✓ 베스천 호스트(Bastion Host)는 보안이 강화된 네트워크 환경에서 외부 네트워크(인터넷)와 내부 네트워크(프라이빗망) 사이를 연결하는 중계 서버 또는 관문(Gateway) 서버를 의미



보안 솔루션

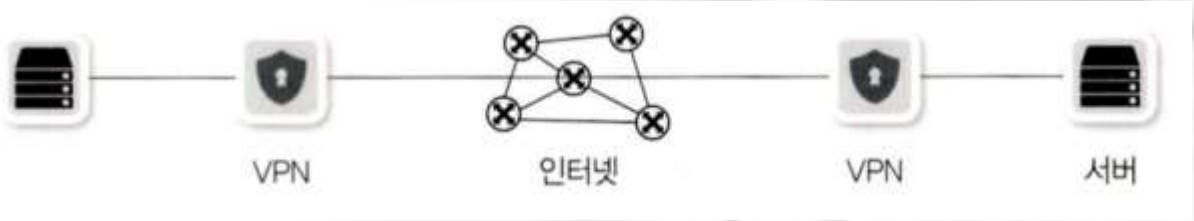
- 접근 통제
  - ✓ 서버 접근을 위한 모든 통신은 배스천 호스트를 통해서만 가능
  - ✓ 서버 호스트의 방화벽에 배스천 호스트에서 출발한 통신만 허용하고 다른 통신은 모두 방어하도록 설정하고 배스천 호스트
  - ✓ 의 보안 감사를 높이면 보안을 강화할 수 있음
  - ✓ 이 기법을 발전시킨 것이 현재의 접근 통제 감사 솔루션입니다
  - ✓ 최근의 접근 통제 솔루션들은 단순한 접근 제어뿐만 아니라 감사 및 보안 이슈 대응 등을 위해 사용자가 작업한 모든 이력을 저장
  - ✓ 윈도의 경우 화면을 레코딩하고 CLI 기반의 솔루션들은 전체 키보드 타이핑을 저장
  - ✓ 사용자가 접근 제어 솔루션을 통과해 서버에 접근하면 그에 대한 감사 로그도 모두 저장
  - ✓ 권한을 제어해 사용 가능한 명령어 수준도 제한할 수 있음

보안 솔루션

❖ VPN

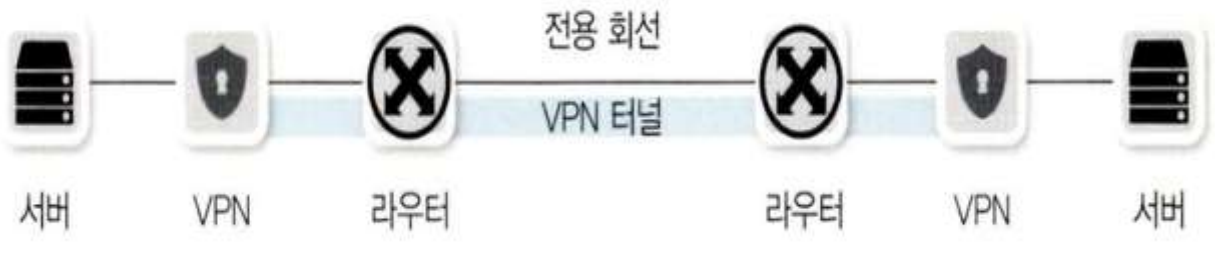
✓ 개요

- VPN은 Virtual Private Network의 약자로 물리적으로 전용선이 아닌 공중망을 이용해 논리적으로 직접 연결한 것처럼 망을 구성하는 기술
- 논리적으로 직접 연결된 것처럼 만들어주는 통로를 터널(Tunnel)이라고 하며 VPN을 이용하면 터널을 이용해 직접 연결한 것처럼 동작
- 터널링 기법만 제공할 수 있다면 VPN이라고 할 수 있지만 터널링만 제공하는 기법은 자주 사용되지 않고 VPN은 주로 인터넷과 같은 공중망을 전용선과 같은 사설망처럼 사용하기 위해도입하므로 강력한 보안을 제공해야 하기 때문에 IPSEC, SSL과 같은 암호화 기법을 제공하는 프로토콜을 VPN에 주로 사용
- IPSEC과 SSL인데 IPSEC은 주로 네트워크 연결용으로 쓰이고 SSLVPN은 사용자가 내부 네트워크에 연결할 때 주로 사용
- 사용자 기반의 VPN 서비스를 제공해주는 장비를 VPN 장비라고 하는데 기존에는 별도의 VPN 서비스를 제공하는 하드웨어가 있었지만 현재는 대부분 방화벽이나 라우터 장비에 VPN 기능이 포함되어 있음
- 일반적인 구성



보안 솔루션

- ❖ VPN
  - ✓ 개요
    - ● 전용 회선 과 VPN
      - ◆ 인터넷 망이 아닌 전용 회선으로 직접 연결할 때도 전용 회선을 통해 VPN을 추가로 구성하는 경우가 있음
      - ◆ 전용 회선은 종단 간에 직접 연결하지만 회선 자체에는 데이터가 그대로 흐르므로 암호화가 되지 않으므로 보안을 더 강화하기 위해 전용 회선에 VPN을 추가로 구성해 데이터를 암호화 하기도 함
      - ◆ 데이터 암호화는 VPN 장비가 아닌 애플리케이션 단에서도 가능
      - ◆ 전용회선을 이용한 VPN 구성

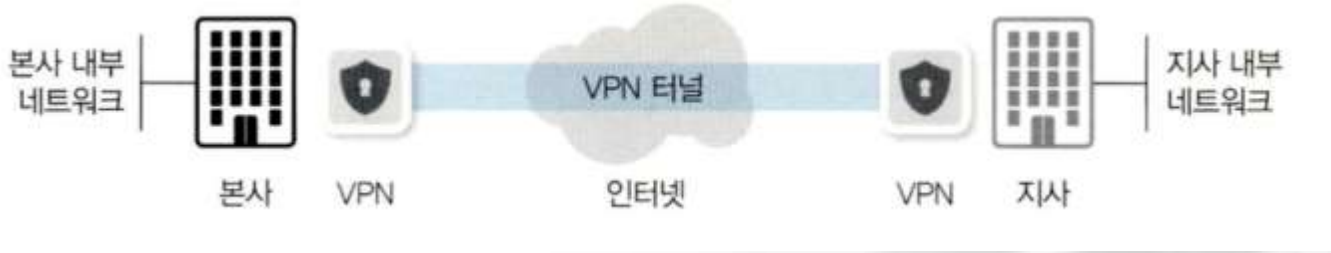


보안 솔루션

❖ VPN

✓ 개요

- 가입자 입장의 VPN 기술에서는 인터넷이라는 공용망을 이용하므로 안전하게 통신할 수 있도록 암호화와 인증과 같은 보안 강화 기술을 적용해야 함
- 과거에는 PPTP, L2TP, GRE와 같이 암호화를 지원하지 않거나 매우 간단한 암호화만 지원하는 기술들이 주로 쓰였지만 최근에는 이런 기술을 사용하더라도 IPSEC의 보안 기술이 추가적으로 함께 사용
- 일반적으로 본사-지사처럼 네트워크 대 네트워크 연결에는 IPSEC VPN 기술을 사용하는데 이 경우 연결되는 본사와 지사 모두 IPSEC VPN 기능을 지원하는 네트워크 장비가 필요

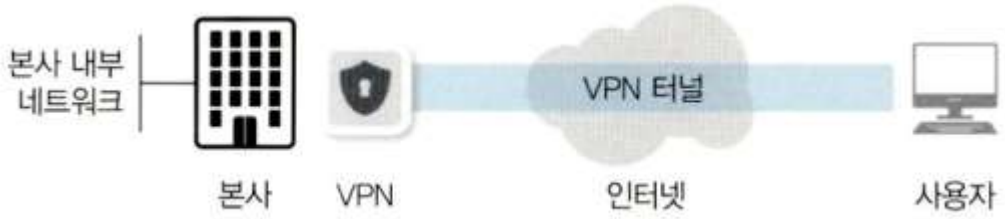


보안 솔루션

❖ VPN

✓ 개요

- 개인 사용자가 본사 네트워크로 접속하는 경우에는 SSLVPN 기술을 사용하는데 SSLVPN 기술은 네트워크 대 네트워크 연결이 아닌 PC 대 네트워크 나 모바일 단말 대 네트워크 접속에 사용하며 이 경우 PC나 모바일 단말과 같은 원격지는 별도의 네트워크 장비 없이 VPN 연결을 사용할 수 있음

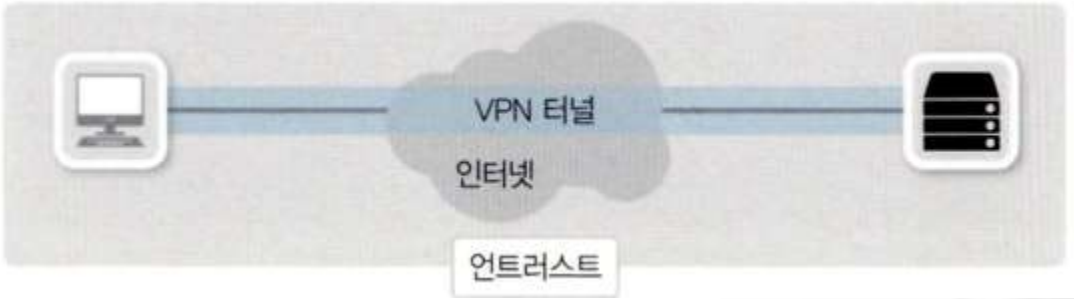


보안 솔루션

- VPN
  - ✓ 동작 방식
    - VPN은 가상 네트워크를 만들어주는 장비로 터널링 기법을 사용하는데 패킷을 터널링 프로토콜로 감싸 통신하는 기법이 터널링 기법
    - 일반적으로 VPN이라고 부르는 프로토콜은 터널링에 보안을 위한 다양한 기술이 포함되어 있음
    - 패킷을 암호화하거나 인증하거나 무결성을 체크하는 보안 기능을 이용해 인터넷에 패킷이 노출되더라도 해커나 기관들이 감청하지 못하도록 보호할 수 있음
    - 현재 가장 많이 사용되는 보안 VPN 프로토콜은 IPSEC과 SSL

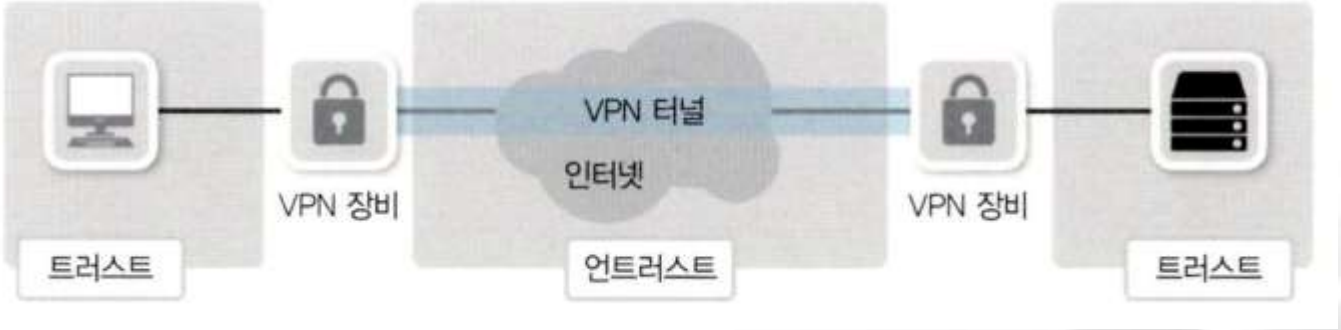
보안 솔루션

- ❖ VPN
  - ✓ 동작 방식
    - ● VPN에서의 통신 보호 구현
      - ◆ Host to Host 통신 보호
        - ▪ Host to Host 통신은 두 호스트 간에 직접 VPN 터널을 연동하는 기법
        - ▪ Host to Host VPN은 VPN 구성으로 잘 사용하지 않음



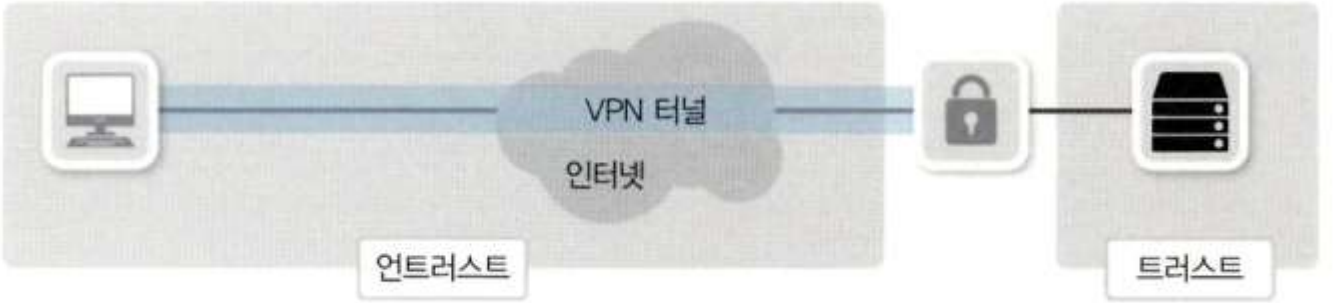
보안 솔루션

- ❖ VPN
  - ✓ 동작 방식
    - ● VPN에서의 통신 보호 구현
      - ◆ Network to Network 통신 보호
        - ▪ Network to Network 통신은 본사 - 지사 같은 특정 네트워크를 가진 두 종단을 연결하는 경우이며 IPSEC 프로토콜 스택을 많이 사용



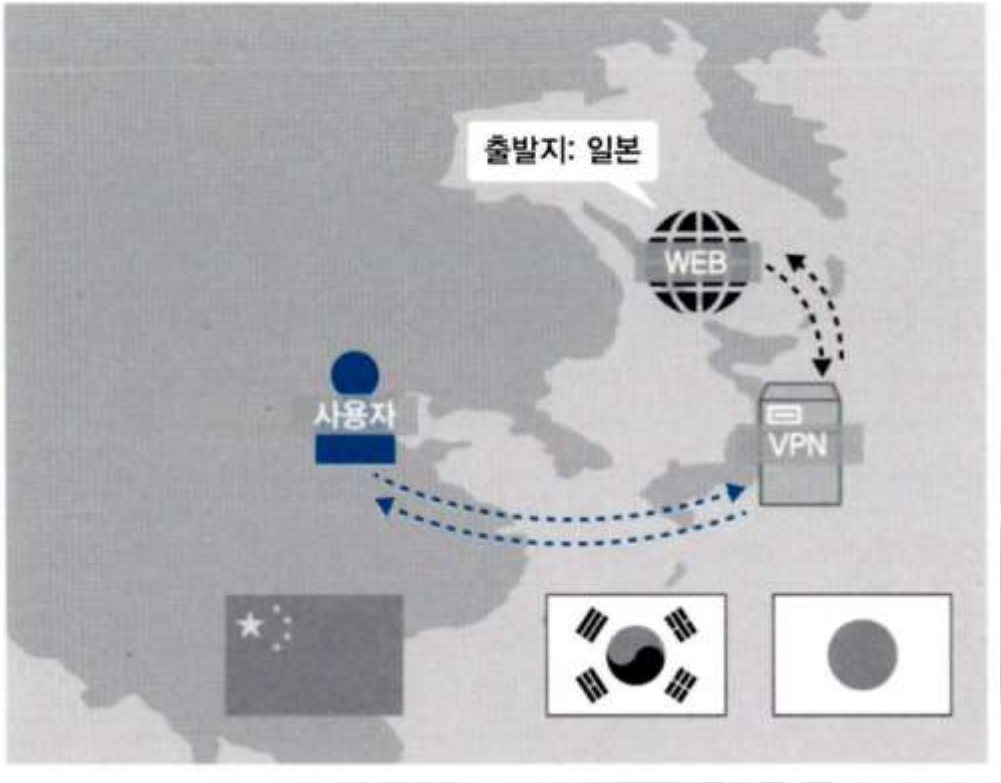
보안 솔루션

- ❖ VPN
  - ✓ 동작 방식
    - ● VPN에서의 통신 보호 구현
      - ◆ Host to Network 통신 보호
        - ▪ 모바일 사용자가 일반 인터넷망을 통해 사내망으로 연결하는 경우이며 IPSEC과 SSL 프로토콜이 범용적으로 사용



보안 솔루션

- VPN
  - ✓ 동작 방식
    - warning.or.kr 사이트를 우회하는 방법이나 특정 국가에서 결제해야 하는 직구 상품 덕분에 다양한 VPN 서비스가 사용되고 있음

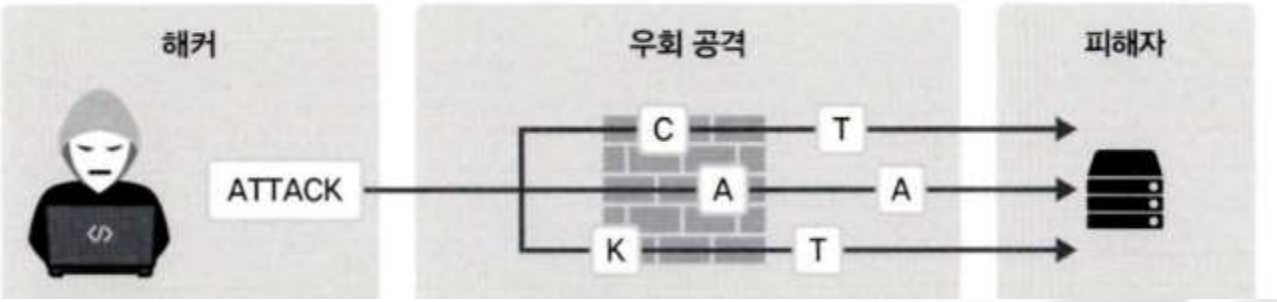


보안 솔루션

- VPN
  - ✓ 동작 방식
    - warning.or.kr 사이트를 우회하는 방법이나 특정 국가에서 결제해야 하는 직구 상품 덕분에 다양한 VPN 서비스가 사용되고 있음
    - 클라우드 방식으로 브라우저 익스텐션과 같은 편리한 방법으로 VPN 서비스를 제공하므로 IP 주소를 매우 쉽게 속이거나 해킹이 쉽지 않도록 패킷을 보호할 수 있음
    - 이런 서비스는 단순히 사이트를 우회하는 기법으로 많이 사용되지만 카페와 같은 공중 무선망을 사용할 때 해커의 공격을 암호화 기법으로 원천 방어할 수 있어 공중 네트워크를 사용하는 경우 이런 VPN을 보안에 활용하는 것이 좋음
    - 클라우드 기반의 VPN은 데이터가 암호화되고 보호되므로 외부에서 그 패킷을 확인할 수 없다는 점을 이용한 것

보안 솔루션

- VPN
  - ✓ 회피 공격
    - 회피 공격은 하나의 공격만 지칭하는 것이 아니라 모든 보안 장비나 보안 프로그램을 우회해 공격하는 방법
    - 우회 기법은 보안 장비의 종류에 따라 달라지고 특정 회사의 특정 보안체계를 회피하기 위한 특별한 공격 일 수도 있음
    - 공격 내용을 분할 전송해 보안 장비를 회피하는 공격



보안 솔루션

- VPN
  - ✓ 회피 공격
    - 공격자가 시도한 공격이 보안 장비에서는 공격으로 판단되지 않고 정상적인 통신으로 확인되지만 실제로 그 공격이 공격 타깃인 피해자(Victim)에게 도착하는 경우 공격으로 동작하는 모든 공격을 회피 공격이라고 함
    - 회피 공격은 피해자가 패킷과 데이터를 처리하는 방법과 보안 장비의 다른 부분을 집중 공격
    - 대부분의 보안 장비가 네트워크 중간에서 공격 여부를 판단하므로 피해자의 입장과 동일한 환경과 상태에서 패킷을 점검하는 것은 불가능
    - 보안 장비를 무력화시키는 회피 공격은 다양한 방법과 타깃이 있지만 우회 공격이 가장 흔하며 집중적인 타깃이 되어온 장비는 IPS
    - ATTACK이라는 단어가 들어간 공격이 있다고 가정하면 IPS에서는 이 공격을 방어하기 위해 공격 데이터베이스(Signature) 중에 ATTACK이라는 단어를 탐지하거나 차단하도록 되어 있는데 공격자는 이 IPS를 우회하기 위해 ATTACK이라는 단어가 한꺼번에 들어가지 않도록 최대한 조절해서 단어 상태로 패킷을 보내는 것이 아니라 알파벳 하나 하나를 쪼개 보냄
    - 쪼개 보낼 때 순서를 바꾸거나 겹쳐 보내면 네트워크 중간에 있는 IPS에서는 ATTACK이라는 단어를 만들어 판단하기 어려워짐
    - 최근 IPS들은 이런 형태의 공격을 방어하는 장치들을 충분히 마련해두고 있지만 복잡한 여러 가지 우회 공격을 섞어 공격하거나 새로운 기법들도 계속 개발 중인 상황이어서 보안 장비 하나만으로는 이런 공격을 더 이상 방어할 수 없음