**클라우드 #9주차 과제**

21660019 3A김세진

**1. 문서 중앙화**

**2. VPL**

**3. 중복제거 기능**

**4. 보안**

**5. 망분리**

**6. vpn, DoS, DDoS**

**7. DMZ, 웹방화벽**

**8. 인피니밴드**

**9. bandwidth**

**10. SSL, IPsec**

**11. 서버 이중화**

**12. ITSM**

**13. ITAM, ESM**

**1. 문서 중앙화**

1-(1) 문서 중앙화의 개념

문서중앙화란 업무 산출물을 사용자 PC가 아닌 중앙 서버에 통합 저장하여 관리하는 것을 말합니다.

1-(2) 내가 생각하는 문서 중앙화의 개념

기업이나 국가의 데이터가 외부로 빠져나가거나 여러 공격이 가해지는 것을 막기 위해서 만든 시스템같다.   
 이해하기 쉽게 말하면, 일종의 성을 쌓았다고 생각한다. 과거에는 마을을 보호하기 위해서, 비상시에는 모든 자원을 가지고 성으로 들어가 버티는 식으로 보호한 것처럼 생각하면 될 것 같다.   
 군대에서의 경우에 싸지방이 있었는데, 그곳에 USB나 개인 저장장치를 꽂는 행위는 금지되었다. 그 곳에서 데이터가 빠져나가는 것을 방지하기 위해서였다. 같은 경우에서 회사는 산업스파이가 자신의 데이터를 쉽게 빼돌리는 것을 막기 위해, 데이터를 중앙의 서버에 저장하고, 내부망에서는 접근은 가능하지만, 워터마크를 찍어둔다든지, 배포가 불가능하게 처리를 하는 방식으로 내부의 데이터를 지켰을 것이다.   
 또한 모든 데이터가 개인의 PC에서 허술하게 저장되어 있지 않기에, 랜섬감염에 효과성을 보이며, 더욱이 랜섬웨어와 같은 암호화 프로그렘에 암호화 되지않게 하는 솔루션을 사용하기도 한다.  
 따라서 문서 중앙화를 하는 이유는 내부의 정보를 보호하는 역할이 제일 크다고 생각한다.

1-(3) 문서 중앙화의 사례 및 현업에서 어떻게 쓸지

사례 : 현대 중공업의 사례로 2011년에 도입한 문서 중앙화 솔루션이 있다. 구축 제품은 Maxeon S-Work로 문서중앙화의 필요성으로는 산업기밀인 설계도면, 오피스 문서의 저장/유통 통제로 회사의 중요 자산보호 필요, 대내외 업무 협업 시 안전한 문서 공유가능, 개인 PC의 문서를 유통제한 할 수 있는 보안 기준의 필요성을 들었다.   
 솔루션에 들어가는 기능은 도면, 오피스 문서를 보안영역에만 저장 강제화 (대상 Office, AUTOCAD), 필요에 따라 중앙 저장소 서버에 업로드 할 수 있도록 정책 수립, 필요에 따라 중앙 저장소 서버에 업로드 할 수 있도록 정책 수립, 필요에 따라 중앙 저장소 서버에 업로드 할 수 있도록 정책 수립, 필요에 따라 중앙 저장소 서버에 업로드 할 수 있도록 정책 수립 탐색기와 E-FAM 연동을 통해 정책에 따라 E-FAM 에 문서/도면 저장, 탐색기 마우스 메뉴를 통해 협업 시스템으로 문서/도면 공유 (EDAS, E-Room, SecureDisk 등)   
  
이와 같이 문서 중앙화는 협업의 속도를 늘려 생산성을 늘리는 데 도움이 될 것이며, 회사가 자신의 정보를 안전하게 보관하여, 오롯이 자신의 자산으로 만드는데 기여하는 방식으로 쓰일 것이라고 생각한다.

**2. VTL**

2-(1) VTL   
 VTL : (virtual tape library) 가상 테이프 라이브러리란 데이터의 백업 및 복구를 위해 가상화 기술을 이용함으로써 디스크를 마치 테이프처럼 인식하여 데이터를 저장하는 시스템이다.  
  
 2-(2)내가 생각하는 VTL, PTL의 개념  
 예전에 우리가 첩보영화나 드라마를 보면 서버에서 정보를 빼내는 장면을 볼 수 있는데, 그 때 생각나는 것은 어떤 데이터가 들어있는 스토리지를 빼서 넘기는 것이다. 이 때 이 스토리지가 테이프의 형태를 띄었는데, 이렇게 테이프를 이용해 저장해놓는 방식을 PTL이라고 생각하면 될 것이다. 하지만 최근의 트랜드를 보면 데이터의 양이 엄청 많기 때문에 이러한 테이프의 형태로 데이터를 저장하는 방식에는 많은 물리적인 요소가 필요하게 된다. 따라서 우리는 SATA방식의 디스크를 마치 테이프인듯이 사용할 수 있는 방법을 찾게 되었는데 이것을 VTL이라고 한다. 이 VTL방식은 데이터를 저장하는 곳이 물리적인 디스크이지만 컴퓨터는 이 디스크를 테이프라고 인식하게 어떠한 엔진을 단다고 생각하면 된다.   
  
2-(3) 현업에서 어떻게 쓰일지

현업에서 PTL방식은 기존의 백업시스템이라고 보면, 소규모의 데이터를 다루고, 백업을 해야하는 경우에 단순히 테이프 형식의 스토리지를 이용하는 것이 좋아 보인다. 하지만 최근에는 수 많은 데이터가 오가고, 그것을 처리하면 백업해야 되기 때문에 테이프 방식으로 백업을 한다는 것은 수많은 테이프를 물리적으로 보관해야 한다는 것이고, 장애복구 시 일일이 해당하는 테이프를 가져와 복구를 해야 되기에 시간의 소모가 크다. 회사는 이러한 PTL방식을 사용하는 것이 꺼려질 것이다. 그에 비해 VTL방식은 디스크 방식이므로 테이프보다 더 많은 데이터 수용과 물리적으로 작다는 점에서 보관에 용이하다. 따라서 VTL방식은 많은 데이터를 저장하고, 빠른 복구를 지원할 수 있는 곳에 많이 쓰일 것이다. 내 생각에 요즈음의 물리적인 백업은 모두 VTL방식으로 쓰일 것 같다.

실제 사례 : 울산대학교는 유닉스, 리눅스, 윈도우 등 다양한 OS로 운영되는 서버 27개와 여러 종류의 DB를 활용하고 있으며, 닷넷기반으로 개발된 전산환경을 갖추고 있다. 백업을 위해 2002년부터 LTO-1 테이프 장비와 네트워크를 통한 백업 시스템을 구축해 운영하고 있다.

그러나 학교 전체의 백업 데이터량이 폭증하고, 데이터베이스와 익스체인지 서버 파일용량이 커져 백업 윈도우가 지연되며 백업 데이터 저장공간이 부족해졌다. 이에 따라 백업 리사이클 주기가 빨라지고, 미디어 소산작업 주기가 짧아지는 등 어려움이 늘어나고 있었다.  
 울산대는 LTO 드라이브를 증설하는 방안과, 데이터 중복제거 기술을 탑재한 VTL을 설치하는 방안을 다각적으로 검토했다. 검토 끝에 백업의 안정성이나 속도, 향후 데이터 증가를 감안해서 VTL은 가장 효과적인 선택이었다. 이는 VTL이 정보생명주기관리(ILM) 전략에 근거한 효율적인 데이터 관리가 가능했기 때문이다.   
데이터 중복제거 기술을 갖춘 VTL로 결정한 후 울산대는 몇 개의 제품을 실제 환경에서 테스트했다. 그 결과 퀀텀의 ‘DXi’가 15배 정도 용량절감 효과를 기대할 수 있어 성능이 가장 뛰어난 것으로 평가됐다. 일반적으로 중복제거 기능을 가진 VTL이 일반 VTL에 비해 성능이 다소 저하되는 것이 사실이지만, 퀀텀의 DXi는 스토리지 용량을 줄일 수 있다는 장점을 감안하면 훨씬 합리적인 선택이라고 판단했다.  
  
비록 2008년이라는 과거의 기사이지만, PTL방식에서 VTL방식으로의 전환이 시작되는 시점이라 VTL의 장점에 대해서 서술이 잘 되있는 것 같다. 기사를 보면, 점점 데이터 처리와 저장이 늘어가면서 PTL방식의 테이프 라이브러리의 문제점이 대두 되었고, 이에 따라 새롭게 VTL 방식이 나왔으며, 이는 백업의 안정성과 속도, 효율적인 데이터 관리의 장점이 있다는 것을 알 수 있다.   
 울산대가 비록 우리 대학보다는 크지만, 회사나 다른 국가 기관처럼 엄청난 데이터를 처리하는 곳과는 비교하지 못한다. 그럼에도 백업에 테이프를 자주 교체하기 시작했다는 것은 회사는 테이프를 교체하기 위해서 훨씬 더 많은 시간이 든다는 것이며, 이를 대체하는 방식으로 VTL을 많이 도입했을 것이다.

**3. 중복 제거 기능**

3-(1) 중복제거 기능의 개념

중복제거는 서로 다른 데이터(파일)들 간에 중복되는 부분을 검출해내고 백업 파일 저장 시 중복된 부분을 제거한 후 저장하는 기술로, 스토리지 활용의 효율성을 높이는 것을 말하며, 크게 보아 데이터 압축의 일종이라고 볼 수 있다.  
  
 3-(2) 내가 생각하는 중복제거 기능의 개념  
 일단 내가 알고 있는 중복이란 것은 DB시간에 같은 데이터가 여러 테이블에 있는 것을 많이 예시로 들었었다. 이에 대한 문제점은 하나의 데이터가 바꼈을 때 모든 데이터가 바뀌지 않아서 무결성에 문제가 생길 수 있기에, 최대한 데이터의 중복을 피하라고 들었는데, 이것과는 조금 의도는 다르지만, 방식은 비슷하다고 생각한다.   
 데이터를 이곳 저곳에 복사하여 붙이는 방식이 아니라, 참조의 방식으로 이 데이터가 어디에 있다는 것을 알려주는 방식으로 개발한 방식인 것 같다.  
 이런 중복제거를 함으로써 전체 시스템의 부하가 더 적게 걸릴 수도 있고, 백업의 데이터를 줄임으로써 백업, 재해복구 등에 시간을 간소화하기에 유리할 것 같다.  
  
 3-(3) 사례

데이터 중복제거(디듀플리케이션) 솔루션을 도입하는 기업이 속속 등장하고 있다. 데이터 저장 효율을 높여주는 데이터 중복제거 솔루션은 데이터 저장장치 분야 최대 화두이지만 국내서는 도입이 부진했던 게 사실이다. 3일 업계에 따르면 지난 3월부터 현재까지 2개 기업이 데이터중복제거 솔루션을 도입, 사용 중이고 다음달 우리금융이 도입할 예정이다. 퀀텀은 관련 제품군 출시 이후 두 달이 지난 4월에 두산그룹의 기계 부문 계열사 1곳에 중복제거 기능을 갖춘 VTL(가상테이프라이브러리) `DXI3500'을 제공한 것으로 파악됐다. 중복제거는 기업 데이터가 고용량화하는 추세에 따라 백업 데이터 증가, 시간 증가, 관리 비용 증가, 복구시간 단축 요청 등의 수요 변화로 인해 등장한 신기술이다. (2007년 기사)

기사의 내용을 살펴보면, 일단 초기에 중복 제거 기술은 백업 데이터의 증가로 시간이나 관리 비용을 관리하기 위해 중복되는 데이터를 제거함으로써 2차 스토리지의 부담을 덜여주는 식으로 사용을 했던 것 같다. 특히 VTL과 관련된 말들이 자주 나오는 것으로 보아서 처음부터 중복데이터를 제거하는 방식이 아니라 백업하는 방법에서 소모되는 시간을 줄일 때 사용된 것같고, 이러한 한계에서 벗어나 최근에는 백업용 2차 스토리지에 저장할 때 중복을 제거하는 것을 넘어서, 1차 스토리지의 중복도 제거하는 식으로 발전한 것 같다.

**4. 보안**

4-(1) 보안의 개념

관리적 : 인적 자산에 대한 보안

물리적 : 설비 / 시설 자산에 대한 보안

기술적 : 정보자산에 대한 보안

4-(2) 내가 생각하는 보안의 개념

관리적 보안이라는 것은 보안을 하는 인원을 교육시키는 것, 보안하는 인원이 관리태만하는 것을 막기 위해 감사하는 것 등이 여기에 들어간다고 생각한다.

물리적 보안이라는 것은 보안을 처리하는 기업의 중심부를 실제로 지키는 것과 USB와 같은 외부의 저장장치가 바이러스를 침투시키는 것을 방지하는 것, 위험전 백업을 해두는 것 등도 이물리적인 보안에 들어간다.

마지막으로 기술적 보안은 이전에 보안 관련된 말들 즉, 방화벽, 웹 방화벽, DMZ, 암호화, 문서 중앙화, 망 분리 등과 같은 실제적인 보안 방법을 나타내는 말이라고 생각한다.

4-(3) 보안의 기술

관리적 보안에는 Security Risk Management, PMI, Common Criteria, ISO 27001 등의 정책이 있으며, 이는 사용자의 권한, 지위 등에 대한 권한 인증 체계, 보안 위험 관리 프로세스의 감사, 정보보안 경영 시스템의 규격을 제시 하는 등의 관리적 보안의 기술, 매뉴얼, 법 등이 있다.

물리적 보안에는 중요 관리 시설에 들어가기 위한 인증을 해야하는 지문, 홍체, 카드 등의 보안 관리 물품이 있으며, 출입통제하는 인원을 배치할 수도 있고, 백업을 미리 해두어 데이터의 손상에 미리 보호하는 등의 기술이 있다

기술적 보안에는 AAA, XML보안, 암호화, 네트워크 보안(=IPS, VPN 등), 컨텐츠 보안, 개인정보 보안 등의 기술 등이 포함된다.

4-(4) 보안 정책

보안의 아키텍쳐를 설계하고, 관리하기 전에 미리 보안을 어떻게 처리할지 정책을 펼치는데, 주로 보안의 수준을 얼만큼 준수하는 것을 목표로 설정하고, 얼마나 지속적으로 관리할지, 어떤 부분, 장비에 보안을 더 중점으로 둘지 대응은 어떻게 할지 등의 정책을 정해 놓는 것 같다.

**5. 망 분리**

5-(1) 망 분리란?

망분리란 공공기관이나 기업에서 인터넷과 완전히 격리된 환경에서 업무를 볼 수 있도록 망(네트워크)을 분리하는 것이다. 즉, 내부망은 인터넷을 통하지 않고 내부의 망에서 데이터를 주고 받을 수 있으며, 외부망은 인터넷을 통하여 외부와 통신이 가능하다.

5-(2) 내가 생각하는 망 분리의 개념

일단 내부와 외부를 분리한 이유는 보안적인 이유가 강해 보이는데, 헤커나 악성 바이러스의 경우, 주로 인터넷을 통하여 들어오는 경우가 대부분이기에, 중요한 데이터를 인터넷으로는 접근하기 힘들게 내부망에서만 교환이 가능하도록 하는 것이다. 그러기 위해서는 내부망에는 따로 회선을 설치하고 허브등 네트워크 장비를 추가로 필요로 하는 번거러움이 있어보이지만, 외부로 자신의 데이터가 빠져나가는 위험을 감수하는 것보다는 분리해서 확실히 보호하는 것이 좋아보인다.

5-(3) 망 분리의 사례와 현업

우리나라와 관련된 사이버 테러를 보면, 3.20사이버테러, 한수원 사이버 테러, 인터파크 개인정보 유출사고 등이 있는데, 이 3가지 경우를 살펴보면, 3.20사이버 테러는 ActiveX의 취약점이 약점이었으며, 향후 조치사항으로는 금융 기관의 전산 망분리의 의무화가 있었고,

한수원 사이버 테러의 경우 국내가상사설망을 이용해 스피어 피싱을 통하여 내부 자료를 착취하는 방식이었으며, 향후 조치사항으로, 업무망-인터넷 망의 물리적 망분리 구축 운용을 했다. 마지막으로 인터파크 개인정보 유출사건의 경우 외부 인터넷 접속이 가능한 내부망에서 데이터베이스 접근을 통해 일어났고, 이후 내부망과 외부망의 완전 분리가 이루어졌다.

이와 같은 사례들로 정보통신법에는 기업의 데이터가 외부로 빠져나가는 것을 막게, 기업의 전산망을 외부망과 분리하는 것을 의무화하기 시작했고, 기업에서는 자신의 데이터를 보호하기 위해서 더 철저한 내,외부망을 분리하기 시작했다.

그렇다면, 현업에서는 이러한 망분리가 거의 적용되었으니 정보 유출이 안되느냐?   
결코 그렇지 않다. 망을 분리했다고, 모든 보안이 안전한 것은 아니다.   
 실제 사례를 예로 들어보면, 스턱스넷이 이란의 핵시설을 파괴한 것도 내부망에 침투한 것으로 알려졌으며, 방법은 usb에 침투시켜 해당 usb가 내부망에 꽂아졌을 때, 폐쇄망 안에서 망가뜨렸다고 추정된 예시가 있다. 이렇듯, 보안은 어떠한 경우에도 절대라는 것을 믿지 말고 항상 주의를 기울여서 다루는 것이 현업에서 필요하다고 생각한다.

**6.VPN, DoS, DDoS**

6-(1) VPN, DoS, DDoS의 개념

VPN : 가상사설망 또는 VPN(Virtual private network)은 공중 네트워크를 통해 한 회사나 몇몇 단체가 내용을 바깥 사람에게 드러내지 않고 통신할 목적으로 쓰이는 사설 통신망이다.

DoS : (Denial of Service)서비스 거부 공격/ 서비스 방해 공격이라는 뜻으로, 한 사용자가 시스템의 리소스를 독점하거나 모두 사용, 또는 파괴함으로써 다른 사용자들이 이 시스템의 서비스를 올바르게 사용할 수 없도록 만드는 것

DDoS : (Distributed Denial of Service)분산 서비스 거부 공격/ 분산 서비스 방해 공격이라는 뜻으로, DoS의 또 다른 형태이며, 인터넷에 연결된 일련의 시스템들을 이용해 단일 사이트에 대한 플러드 공격을 시도하는 것  
  
  
 6-(2) 내가 생각하는 ) VPN, DoS, DDoS 의 개념

VPN : 회사에서 컴퓨터들을 연결하고 그리고 서버에 연결하는 방식에는 통신망을 이용하여 연결한다. 작은 회사라면 이러한 통신망을 유선으로 연결해도 상관이 없을 것 같다. 하지만 회사가 커지면 수많은 선들이 필요할 것이고, 이러한 선들이 많아지는 것은 결코 좋은 일은 아닐 것이다. 또한, 지점을 여러군데 흩어 놓는다면, 상황은 더 심해지는데 물리적으로 연결할 방법에는 돈이 너무 많이 들것이다. 따라서 가상으로 이러한 연결을 시킬 수 있다면 매우 효과적인 방법이었을 것이며, 이러한 방식으로 개발된 것이 VPN인 것 같다.  
 또한 이 VPN의 데이터의 이동에서 암호화가 이루어지기에 보안에 용이하다는 장점도 있다.

DoS : 서비스를 제공하는 서버의 경우 아무래도 물리적인 한계가 있기 때문에, 처리할 수 있는 량에 한계와 처리 후 데이터를 클라이언트에게 보내는 것에 대한 한계량이 있을 것이다. 이 때, 하나의 클라이언트에서 매크로나 몇몇 방법을 통하여 엄청난 요청을 보내면, 서버에서는 해당 클라이언트의 요청에 응답하느라 다른 클라이언트에게는 응답을 하지못하고, 이는 서비스를 제공하는데 어려움을 겪는다는 것을 의미한다.   
  
 DDoS : 위의 DoS의 방식으로 서버에 공격하는 것은 예전의 작은 규모의 서버를 공격하는데 유용했지만, 요즈음 나오는 서버의 하드웨어 성능은 개인의 공격을 버틸 정도는 되는 것 같으며, 또한 보안이 발달하여, 이상한 트래픽을 감지하면 해당 트래픽을 쓰는 곳의 접근을 차단하는 방법도 생겼기에, DoS의 방식의 한계가 드러났기에, 더 뛰어난 공격 방식으로 DDoS가 나왔다고 생각하면 되겠다. DDoS라는 것은 여러 컴퓨터를 바이러스로 감염시켜서 자신의 것처럼 사용하는데, 이런 수십, 수백의 컴퓨터에서 동시에 요청을 쏟아내면, 접근을 차단하기에 쉽지 않고, 피해도 막심해 진다고 볼 수 있다.

6-(3) 현업에서는 어떻게 쓰일지  
 그렇다면 VPN과 DoS, DDoS에는 어떤 관련이 있을까 검색을 해보았다.   
일단 최근의 VPN의 경우 기업의 원격업무를 위해서 도입이 증가되고 있다고 한다. VPN의 경우에

회사의 내부망을 가상으로 만들었다고 생각하면 되는데, 이때에 가상이라는 말에서 알듯이 실제로 내부망을 구축한 것이 아니라, 인터넷을 통하여 특정 암호화를 거치고, 내부의 사람에게 접근할 수 있는 권한을 부여하여 내부망처럼 사용하는 것이라고 이해했는데, 이렇게 함으로써 사무실 밖 집에서도 업무 시스템에 안전하게 접근할 수 있다는 장점과 주고 받는 트래픽을 보호할 수 있다.   
 위의 사례를 보면 DoS, DDoS의 공격과는 거리가 멀어보이는 개념같다.  
   
VPN의 경우에는 암호화 되어 공격에 아주 완벽할 것 같아보이지만, 사이버보안 교육 기업 SANS 인스티튜트가 운영하는 인터넷 스톰 센터에서 활동하는 강사인 가이 브루노는 지난 15일 VPN을 안전하게 사용하는 방안에 대한 게시물을 게재했다. VPN은 외부에서 접근하기는 힘들지만, VPN의 접근권한을 가진 사용자계정을 탈취하는 방식으로 뚫을 수 있다고 말했다.   
 해결 방안으로는 오픈 VPN, SSL VPN과 연관된 포트들을 면밀히 조사하는 방법이 있다.   
  
  
생각해보니 5번의 망분리에서 나온 것중에 한수원 사이버 공격의 예시가 있었는데,   
이 공격에서 시작은 중국 해양의 어떤 IP로부터 시작하여 국내의가상사설망(VPN)을 통해 공격을 했다는 말이 있었는데, 이것도 VPN의 권한을 탈취해 공격을 한 것으로 봐도 될까 싶다.

**7. DMZ 웹방화벽**

7-(1) DMZ, 웹방화벽의 개념  
DMZ : DMZ는 인프라 네트워크의 구성중에서 외부 인터넷망과 내부 인프라넷망의 사이에 위치하는 중간지대를 지칭한다. 즉, 인프라네트워크의 보안영역의 일부이다.   
Web-Firewall : 웹 서버만을 보호하기 위해 설계된 정보 보호 시스템이다.

웹 해킹 시도로부터 홈페이지 서비스를 전문적으로 방어하기 위해 HTTP 트래픽을 검사해 보호 대상 홈페이지 서버로 유입되는 해킹을 차단하는 정보 보호 시스템 이다.

7-(2) 내가 생각하는 DMZ, 웹방화벽의 개념   
DMZ : 회사를 생각해보면, 내부에 LAN으로 연결된 네트워크가 있고, 외부와의 네트워크는 인터넷을 통해서 연결을 한다. 이때 방화벽이라는 것을 통해서 불법적인 침입을 막는다. 하지만 내부의 데이터를 외부에 제공하는 것이 회사에 필요하다고 했을 때, 모든 방화벽을 해제하는 것은 위험이 꽤나 클 것 이다. 따라서 내부 방화벽과 외부 방화벽 사이에 DMZ라는 중간 지대의 서버를 설정하고, 외부로 들어내야 할 데이터를 DMZ에 저장한다면 외부에서 이 데이터로 접근할 수는 있지만, 내부로는 접속이 힘들기 때문에 보안의 문제에 적절한 방법이 된 것 같다.  
  
Web-Firewall : DMZ의 경우 외부의 네트워크와 내부의 네트워크 사이의 중립지역이라고 한다면, DMZ의 경계지역에는 2개의 방화벽이 있다. 하지만 이름이 비슷한 웹 방화벽은 웹 공격을 막는 방패이며, 방화벽이 내부의 정보가 외부에서 쉽게 접근하지 못하게 막는 역할이라면, 웹방화벽은 일종의 도메인으로 부터의 공격을 막는 것이라고 하면 될 것 같다.   
 쉬운 예시로 내가 naver.com을 검색창에 넣고 수없이 F5를 눌러서 요청을 보내면, 서버는 이를 처리하기가 어렵기 때문에 웹 방화벽의 어떤 기능을 이용해서 이러한 공격적인 트레픽을 막는다고 생각하면 된다.

7-(3) 현업에서 어떻게 쓰일지

웹 애플리케이션 방화벽(Web Application Firewall, 이하 WAF) 시장이 크게 성장하고 있다. 정보보호산업협회(KISIA)는 2017년 정보보호산업 실태조사를 발표하면서 국내 WAF 시장이 전년대비 28% 이상 성장할 것으로 전망했다. 클라우드 환경에 따른 서비스형 WAF로 전환, 암호화폐 거래소와 같은 신규 수요 증가 등으로 인해 WAF 수요가 확대될 것이라는 얘기다. WAF는 웹 애플리케이션에 최적화됐기 때문에 HTTP에 포함된 악의적인 요청 및 의심스러운 응답을 탐지하고 이에 대응할 수 있다. 악의적인 요청은 주로 SQL인젝션(Injection), XSS(Cross Site Scripting), 파일 업로드, 무차별 대입 공격 등이 대표적이다.   
  
사례로는 핀코인의 경우에서 알 수 있는데, 핀코인은 인터넷 쇼핑몰이다. 이 사이트는 웹방화벽을 필수적으로 써야한다고 적혀있는데, 이 사이트는 과거 오픈카트를 기반으로 사이트를 운영하던 시기에 중국으로부터 DDoS공격을 받은적이 있다고 말한다. 당시 사드 외교문제로 중국에서 대대적인 한국의 웹사이트 공격이 시행되던 때인데, 전 세계의 좀비 컴퓨터로부터 무차별적인 로그인 시도를 받았기에 막을 방법이 없었고 서비스를 잠시 중단하기까지 했다는 것이다.

하지만 cloudflare라는 웹방화벽 솔루션을 도입한 이후에 DDoS공격을 완화할 수 있었고, 또한 웹 방화벽 뒤에 실제 서버의 IP를 숨김으로써 실제로 요청이 IP를 타고 바로 들어오지 않는 다는 점에서 효과적인 방어책이라고 말한다.

**8. 인피니밴드**  
 8-(1) 인피니밴드의 개념  
 기존의 PCI의 단점을 보안하는 IO버스의 새로운 표준으로 Infinity Bandwidth의 줄임말이다.   
  
 8-(2) 내가 생각하는 인피니밴드의 개념  
 기존의 PCI라는 것은 메인보드와 주변저장장치 사이의 인터페이스 역할을 하던 선의 규격이라고 생각하면 된다. 예를 들면 CPU가 처리한 데이터를 스토리지에 저장하기 위해서 연결을 해주어야 하는데 이를 연결해주는 선의 규격일 PCI라고 한다.   
 기존의 PCI는 1.064Gbps에서 2.128Gbp의 대역폭을 제공하였고, 단방향의 전송과 대역폭을 공유하는 방식이었기에 매우 많은 데이터를 주고 받는 최근에 와서는 데이터 병목현상을 초래하여 서버를 다운시킬 수 있다는 상화에 이르렀다. 그래서 더 발전시킨 인터페이스 규격이 인피니밴드라고 생각하면 될 것이다.   
 인피니 밴드는 양방향 최저 2.5Gbps에서 최고 30Gbps의 속도를 제공하며, 최대 길이를 100m이상으로 연결할 수 있고, 스위치 구조로 한번에 많은 데이터를 컴퓨터 안팎의 정확한 목적지까지 보내준다.

8-(3) 현업에서 어떻게 쓰일지

최근의 데이터 센터의 경우 가상화로 단일 시스템 안에서 여러 대의 서버가 돌아가게 되었다. 따라서 같은 규모의 서버 클러스터가 이전보다 훨씬 많은 작업을 하게 되었고, 이는 데이터 센터의 구조를 복잡하게 하였다. 이는 수많은 데이터를 주고 받아야 한다는 것이고, 이때, 데이터가 오가는 도로 즉 대역폭이 갖추어 지지 않았다면, 병목현상이 대두 될 것이다. 이에 대한 해결책으로 인피니 밴드가 떠올랐다.  
  
이런 데이터 센터에 적용하는 것 뿐만 아니라 슈퍼컴퓨터에도 적용이 됬는데, 세계 톱500 슈퍼컴퓨터 목록을 보면, 500대의 컴퓨터중 226대에 인피니밴드가 적용되었다고도 한다.

인터넷의 폭발적인 성장과 온라인 상의 정보유지의 필요성으로 대용량 스토리지에 대한 요구가 증가하고 있다. 이에 기존의 서버와 외장형 스토리지를 전용선으로 연결하는 DAS(direct attached storage)에서, LAN을 통해 서버와 스토리지를 접속하는 NAS(network attached storage), 그리고 새로운 엔터프라이즈 환경을 겨냥해 스토리지에 대한 고속 액세스, 일원적인 관리, 그리고 확장성과 내장애성을 높이기 위한 SAN(storage area network)이 스토리지 시스템의 주류로 등장하고 있다.

인피니밴드 서버와 마찬가지로 스토리지 시스템에서도 인피니밴드 기술을 활용한 인피니밴드 스토리지가 점점 증가할 것으로 전망하고 있는데, Yankee Group은 2006년 전세계 스토리지 시스템 시장에서 인피니밴드 스토리지 시스템 시장이 차지하는 비중이 2.47%에 이를 것으로 전망하고 있다.

**9. bandwidth**  
 9-(1) bandwidth의 개념  
대역폭(bandwidth)은 특정한 기능을 수행할 수 있는 주파수의 범위로, 헤르츠 단위로 측정된다. 문맥에 따라 통과대역 대역폭로 부를 수 있다. 대역폭은 정보 이론, 무선 통신, 신호 처리, 분광학 등 여러 분야에서 중요한 개념으로 다룬다.

9-(2)내가 생각하는 bandwidth의 개념

네트워크에서 대역폭은 일종의 데이터가 오가는 통로라고 생각한다. 네트워크에서 대역폭은 도로의 차선에 비유를 많이 하는 것으로 아는데, 컴퓨터가 연산한 결과를 데이터 즉, 차라고 본다면, 이러한 데이터가 지나가는 통로를 도로라고 생각하면 된다. 이때, 컴퓨터 성능이 좋아서 무수히 많은 데이터를 처리할 수 있어도, 도로가 1차선이라면 당연히 데이터의 전송이 느려지고 계속 막히게 되는 일이 벌어질 것이기 때문에, 컴퓨터의 성능만 늘린다고 빨라지는 것이 아니라 그에 대한 통로, 즉 네트워크 장비들의 성능까지 만족을 시켜야 전체적인 시스템이 빨라진다고 생각한다.

9-(3) 현업에서 어떻게 쓰일지  
 대역폭은 네트워크의 많은 부분에서 말이 들리는데, 주로 대역폭 OOGbps을 지원한다 라고 하며, 주로 데이터의 전송 속도를 나타낼 때 쓰인다. 최근에 이동통신에서 5G 시대가 오면서 몇 Gbps가 늘었다고 나오며, 4G의 경우 1기가 영화를 다운 받을 때 10초 이상이 걸리면, 5G의 경우 1초만에 다운이 된다.   
  
  
**10. SSL, IPsec의 관계**

10-(1) SSL, IPsec의 개념  
 VPN 종류에서 암호화 방식에 따라 IPsec방식, SSL방식으로 나뉜다.

IPsec : (Internet Protocol Security)은 통신 세션의 각 IP패킷을 암호화하고 인증하는 안전한 인터넷 프로토콜(IP) 통신을 위한 인터넷 프로토콜 스위트이다.(3 계층 네트워크)

SSL : 웹서버와 클라이언트간의 안전한 통신을 위해 보안을 제공하는 인터넷보안 프로토콜이다. (어느 한 계층에 속하여 동작하는 것이 아니라 응용계층과 전송계층 사이에 독립적인 프로토콜 계층을 만들어서 동작)  
  
10-(2) 내가 생각하는 SSL, IPsec의 개념  
 IPsec은 3계층의 패킷을 암호화하여 통신하는 프로토콜로 인터넷의 경유 구간에 터널링을 형성해주는 방식이며, VPN이 암호화 하는 하나의 방식이라고 생각한다. 일단 패킷은 헤더와 몸통으로 구성되는데, 이때 헤더의 일부분을 암호화 하는 방식이라고 생각한다. 따라서 중간에서 데이터가 변조되거나 위조 되는 것을 방지하며, 중간에 탈취하여 악의적인 트래픽을 막을 수 있다.

SSL은 다른 말로 웹 서버 인증, 서버 인증을 나타내는 것 같다. 웹 브라우저와 서버간의 암호화 통신을 말하며, 내가 생각하기에, 아이디나 패스워드를 통해 로그인을 하면, 이 부분에서 암호화가 처리되어 암호화된 정보를 통해 서버와 클라이언트간의 통신의 보안을 책임진다는 것이다.

10-(3) 현업에서 어떻게 쓰일지

일단 IPsec VPN과 SSL VPN의 차이점을 찾아보았는데, IPsec VPN은 내부망 혹은 외부망 종단에 특정 VPN장비를 연결하여 VPN장비끼리의 암호화로 연결하는 부분이 있으며, SSL VPN은 클라이언트의 접속에서부터 인터넷 망, 내부의 SSL VPN사이를 암호화로 연결한다.   
 각각의 장단점이 있기 때문에 각 회사는 자신에게 가장 적합한 기술을 택하여 적용하는 것이 중요하다.

**11. 서버 이중화**

11-(1) 서버 이중화의 개념  
 서버 이중화는 시스템의 일부에 어떠한 장애가 발생했을 경우에 대비하여, 장애 발생시 시스템 전체의 기능을 계속 유지하도록 예비 장치를 평상시부터 백업으로 배치해 운용하는 일이다.

11-(2) 내가 생각하는 서버 이중화의 개념  
 저번에 작성한 HA(고가용성)을 보장하기 위해서 필요한 방법이 이중화인 것 같다. 서버의 경우 트레픽이 과부화 걸려 첫 번째 서버가 터졌을 때, 자연스럽게 두 번째 서버가 동작하면서 사용자들이 서버가 터진 것을 느끼지 않게 하는 방식으로 구현을 한다고 생각한다.   
 우리가 부산에서 서울을 가야한다고 생각하면, 비행기, 기차, 버스, 자가용 등의 여러 방법이 있다. 만약 비행기가 다 매진이라면 기차를 기차가 매진이라면 버스를 이용하듯이, 어떤 방식에 문제가 생겼을 때, 다른 방식을 사용하여 결국에 서울로 가는 목적을 이룰 수 있게 해주는 방식이라고 생각한다.

11-(3) 서버 이중화의 방식 (A-A, A-S)  
 A-A : Active- Active방식은 다중화 장비가 두 대 모두 활성화 되어 동작하는 구성이다.   
두 대의 장비가 모두 처리를 하기에 처리률이 높지만, 하나의 장비에 장애가 생기면, 다른 서버가 2배 이상의 처리를 해야 하기 때문에, 이후 리소스에 대한 계획도 세워 놓아야 한다.

내 의견으로 이 방식은 서버 컴퓨터를 몇대 연결하여 슈퍼 컴퓨터를 만드는 방식에 많이 쓰일 것 같다.

A-S : Active- Stand\_by방식은 기본적인 HA 방법이며 두 대 중 하나는 활성화 되어 동작하고 하나는 장애 등 의 경우를 대비하여 대기 시키는 구성이다. Active 상태의 서버가 어떤한 일로 인해 장애가 발생하면, stand상태의 서버가 이 서버를 대체하여 서비스를 이어가는 방식이다.

이 방식의 경우에는 내 서버가 특정 서비스를 클라이언트에게 제공하고 있을 때, 제해발생시에 서비스가 문제 없이 돌아가게 할 때 많이 사용하는 방식일 것 같다.

**12. ITSM**

12-(1) ITSM의 개념  
 IT 서비스 관리(IT service management, ITSM)는 고객에게 제공하는 정보기술(IT) 서비스들을 계획, 설계, 전달, 운영하기 위해 단체에 의해 수행되는 활동 전반을 가리킨다.

SLA : 어떤 서비스가 제공될 것인지를 측정이 가능한 지표로 명시한 문서이며, 서비스 공급자와 사용자간에 서비스에 대한 측정지표와 목표 등에 대한 협약서이다.

SLM : SLA가 잘 적용되고 있는지 확인, 검토, 모니터링 하는 일이며, SLA에서 정의한 바에 대해 실제 서비스 수준을 측정/평가하고 개선 방안을 마련하는 과정이다.

12-(2) 내가 생각하는 ITSM의 개념  
 ITIL과 여러 방면에서 헷깔리는 개념이었는데, ITIL은 ITSM의 가장 많이 채택되어 사용된 실천모델, 표준 같은 느낌이다. 따라서 ITSM이라는 것은 IT서비스를 구축하고 그 서비스를 고객에게 효과적으로 사용하게 끔 설계하는 일종의 IT서비스 설계도라고 볼 수 있다.  
 앞에 설명했지만, 이러한 설계도의 존재 차이는 서비스의 품질에 영향을 줄 수도 있다고 생각한다.  
 이런 설계도로 IT서비스를 만들었으면, 이 서비스가 잘 돌아 갈 것이라고 보증하는 것이 SLA, 그리고 이러한 보증인 SLA가 잘 이루어지고 있는 것을 감독 관리하는 과정이 SLM이라고 생각한다

12-(3) 현업에서 어떻게 쓸지

ITSM은 크게 두가지 프로세스로 구성되어 있는데, 서비스 제공과 서비스 지원의 프로세스이다.

이런 프로세스는 현업에서 IT서비스 구축할 때에 어떻게 하면 효율적으로 만들지와 얼마나

서비스를 문제없이 사용자에게 줄지를 생각하여 더 좋은 프로그램을 만드는데 이바지를 할

것이다.   
 예를 들면 서비스 제공의 측면에서 서비스가 얼만큼의 자원을 필요할지, 얼만큼의 서비스를

제공할지, 재난복구나 자원 스캐줄링에 대해서 생각하게 하는 프로세스이며, 서비스 지원

측면에서, 사용자들이 이 서비스를 이용하는데 더 편리한 방식이나 에로사항을 문의하는

방식등의 지침을 제공함으로써 서비스를 제공하는데 이바지를 할 것이다.

**13. ITAM, ESM**  
 13-(1) ITAM, ESM 개념  
 ITAM : IT자산관리 솔루션(ITAM)이란 소프트웨어와 하드웨어와 같은 IT자산의 물리적 정보, 재무정보, 계약 정보 등을 관리하는 솔루션이다.  
 ESM : 기업보안관리(ESM)이란 방화벽, 침입 탐지 시스템, 가상 사설망 등의 보안 솔루션을 하나로 모은 통합 보안 관리 시스템이다.

13-(2) 내가 생각하는ITAM, ESM 이란?

IT자산이라는 것은 쉽게 말하면, 서버, 스토리지, 네트워크 장비 등과 같은 하드웨어와 관리용 소프트웨어, 플랫폼 등 시스템을 동작시키고 관리하는 데에 필요한 소프트웨어가 여기에 들어가며, 수업시간에 나왔던 감가상각비의 개념도 여기에 들어간다고 생각한다.

이런 IT자원은 감가상각비에 나왔듯이 수명이 있기에 이러한 자원의 도입, 유지, 폐기를 잘 조절하여 경제적으로 관리하는 것이 꼭 필요하다고 생각한다.

ESM은 이전까지 배웠던 보안기술의 방법을 모두 한데 묶어 관리하는 시스템이라고 생각한다. DBMS를 생각하면, 우리가 DB에 직접 접근하여 데이터를 뽑아오는 것보다 편리하며, 데이터를 손상시키지 않는 방법을 제공한다면, ESM은 보안에 관련된 모든 것들을 효율적, 안정적으로 관리하고 사용할 수 있게 서비스를 제공해주는 시스템이라고 생각한다.

13-(3) 현업에서 어떻게 사용할지, 사례  
한국CA가 기업 내 각종 IT자산을 구매에서 폐기에 이르는 전 라이프사이클에 걸쳐 관리하는 ITAM(IT 자산관리) 시스템 사례를 국내 처음으로 확보해 눈길을 끌고 있다. 대한생명은 이번 프로젝트에서 유무형 자산의 수명주기 관리 및 조회가 가능하도록 관리 방안을 수립하는 데 초점을 맞추고, 하드웨어, 소프트웨어, 애플리케이션 등 IT자산 정보의 라이프사이클 관리를 위한 시스템을 구축했다. 또한 ERP, IPS 등 기존 시스템과의 연계를 통해 데이터 처리를 실시간화해 업무 효율성을 높였다. 이번 프로젝트에서 기술지원을 담당한 정광훈 한국CA 부장은 "IT 자산은 효율적인 IT관리를 위해 가장 기본이 되는 단위이며, 대한생명의 IT자산관리 시스템 도입은 기업의 업무 효율을 높이고 IT 투자의 ROI를 극대화하기 위한 핵심요소가 되어 IT거버넌스의 시발점이 될 것"이라고 밝혔다.

이 기사의 말처럼, 기업이 IT자산의 라이프사이클을 계산하여, 자신이 가지고 있는 IT자산을 잘 계산하여, 이후의 투자에 미리 대비할 수 있다는 장점이 있다.