네트워크 보안 시스템

부제: 방화벽

202321594
최익진

네트워크 보안 시스템

네트워크 보안 시스템이란?

What is Network Security System

환경구축

Ubuntu와 GNS3을 사용한 환경구축

Creating an enviroments using Ubuntu and GNS3

방화벽

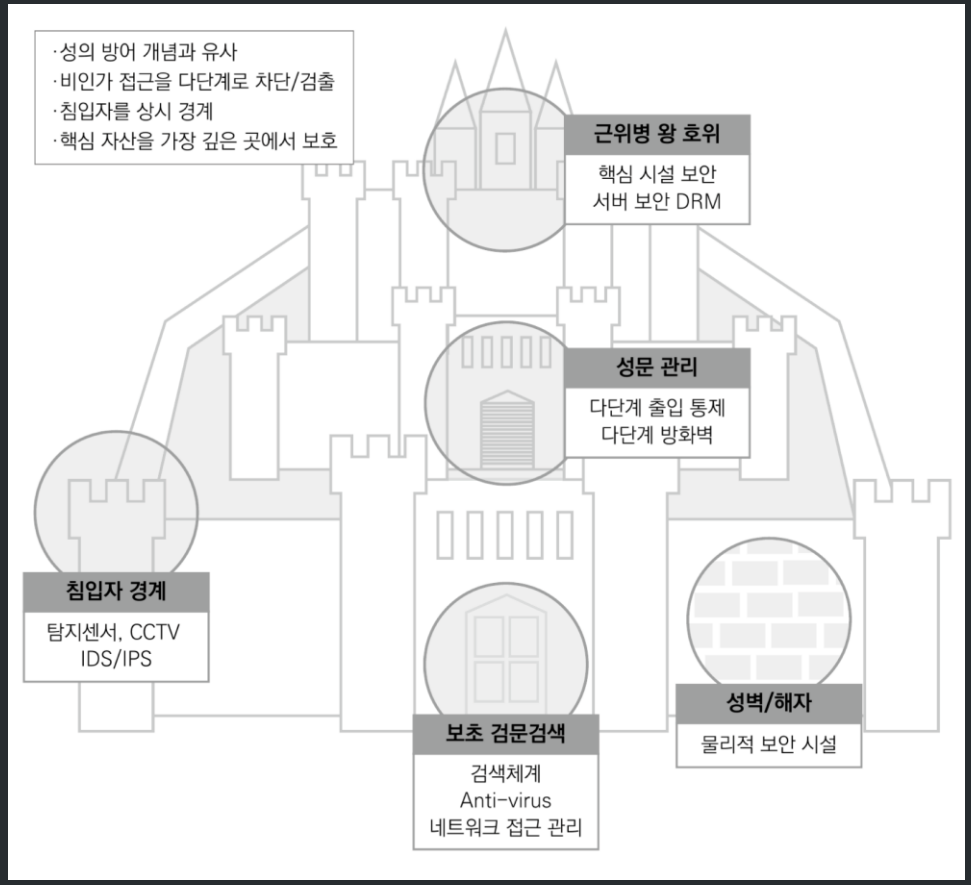
방화벽이란?

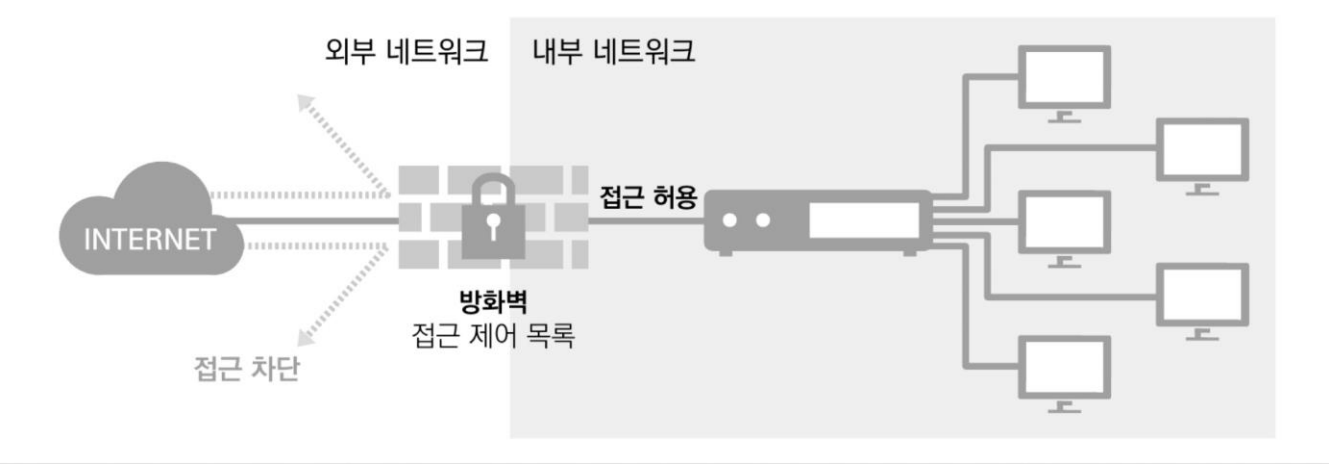
What is FIrewall

네트워크는 하나의 보안 시스템으로
모든 위험을 방어 할 수 없다,
그렇기에 다양한 시스템을 통하여
보안 체계를 구축해야 한다.

시스템의 구성으로는
옆의 사진과 같이 현실 세계의 성과도
같은 구성을 지닌다.

1. 검색체계, 백신, 네트워크 접근관리
2. 물리적 보안 시설, 탐지센서, CCTV
IDS / IPS
4. 다단계 방화벽
5. 서버 보안 DRM





방화벽은 외부로부터의 불법적인 접근이나 공격을 방어하기 위해 내부 네트워크와 외부 네트워크가 연결되는 접점에 구축되는 보안시스템이자.

보안 정책에 따라 비인가 통신은 차단하고 인가된 통신은 허용하는 방식으로 내부 네트워크를 외부 네트워크로부터 보호한다

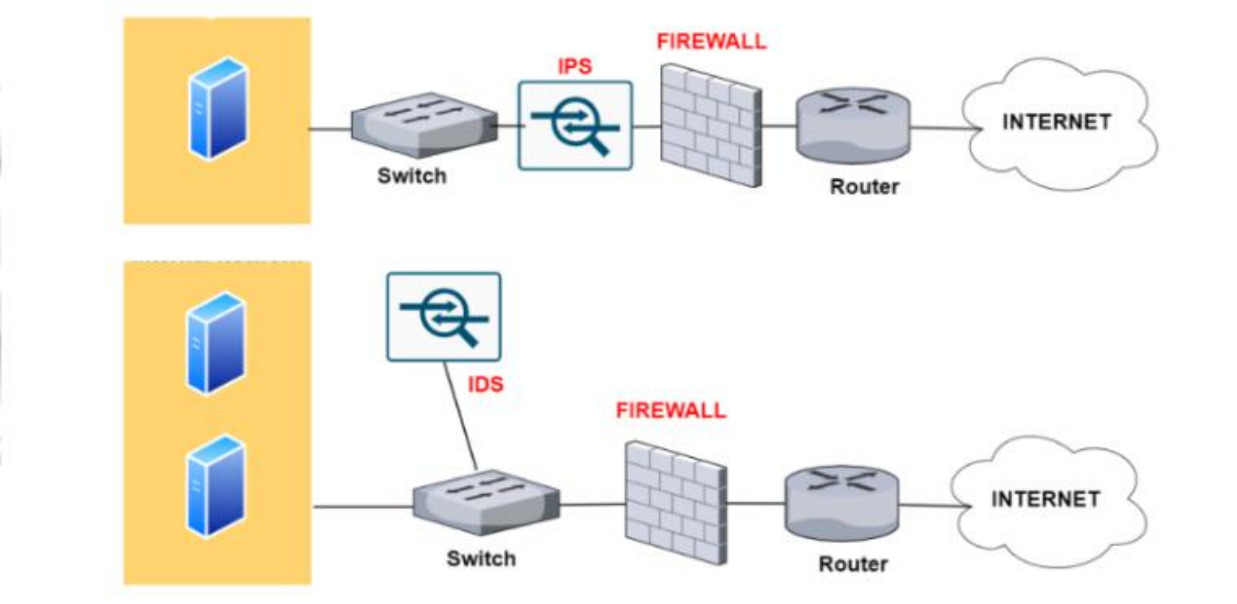
처음의 방화벽은 IP 주소, 포트 번호를 기준으로 접근을 제어하는 Packet Filtering 방식을 적용하고 있었다, 추가 기능으로는 Network Address Translation 그리고 Virtual Private Network만 지원했다.

그후 발전된 2세대의 방화 벽은 Stateful Inspection 방식으로서 1세대의 방어벽의 공격 탐지 기능을 강화하였다.

마지막으로 현재의 차세대 방화벽은 Application Package를 분석하고 상세히 제어할수 있다.

네트워크 침입 탐지/차단(방어) 시스템은 네트워크 패킷 데이터를 분석하여 악성코드, 취약점 공격코드, 권한 상승, 비정상 접근 등의 공격을 탐지한다.

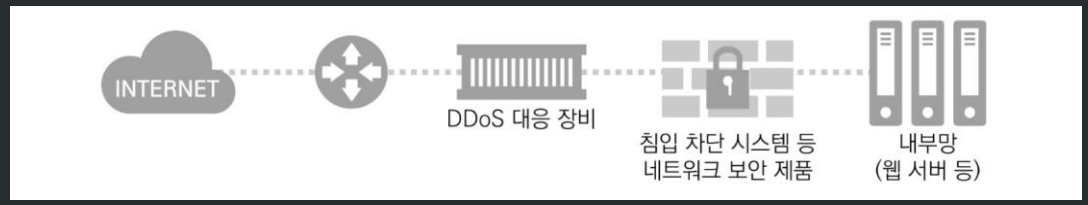
시스템 운영 절차로는 정보 수집, 정보 가공, 정보 분석, 보고 및 대응 순으로 이루어져 있다.

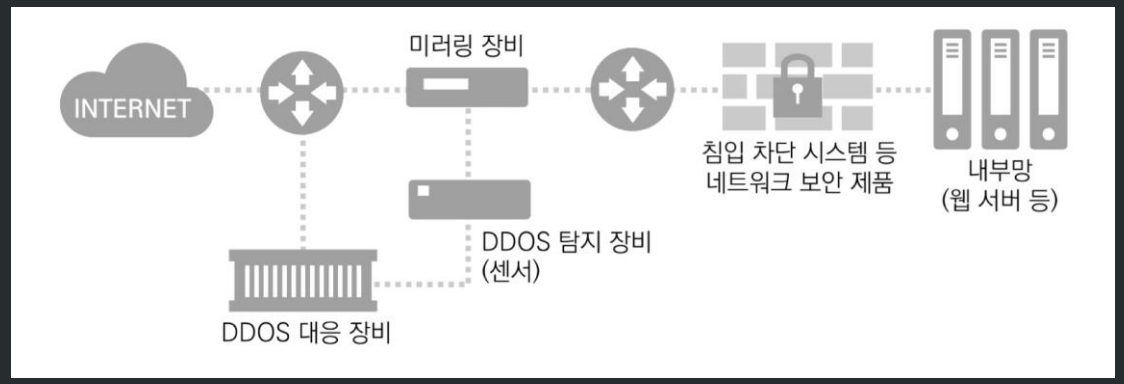


Intrusion Detection System은 위에 서술 한데로 탐지하고,
Intrusion Detection and Preventation System은 이름에서 알 수 있다시피, 능동적인 대응 기능이 추가되어 있다

Distributed Denial of Serviced는 그 이름에서도 알 수 있다시피, 공격 대상 사이트에 대량의 트래픽을 보내 네트워크 대역폭을 소비하게 하거나, 용량을 과다하게 발생시켜 서비스 가용성을 떨어트리는 공격 방식이다.

In-Line 구성은 기존 물리적 회선 가운데 DDoS 대응장비가 설치되는 방식으로, DDoS 대응장비로 유입되는 트래픽을 모니터링 하여 DDoS공격을 직접 탐지하고 차단하는 방식이며, 대부분의 환경에서 구현되는 일반적 구성방식이다.



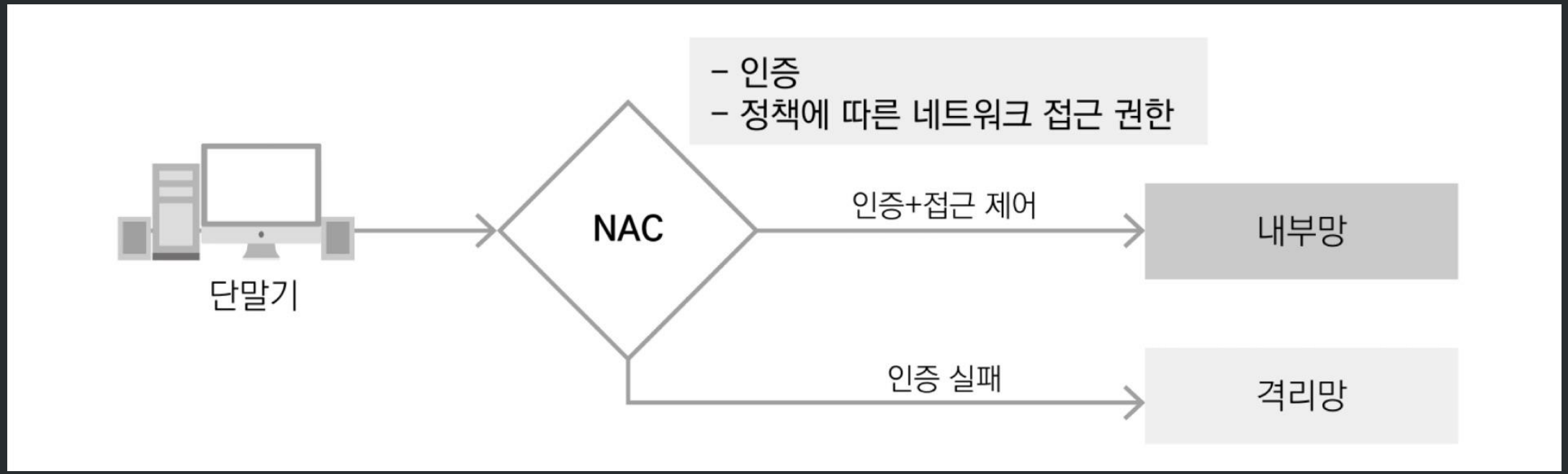


Out-of-Path 구성은 물리적 회선 구성 바깥에 DDoS 탐지장비 및 차단장비가 설치되는 방식으로, 미러링 장비를 통해 유입된 트래픽을 DDoS탐지장비(센서)에서 분석하고, DDoS 차단장비에서 해당 DDoS공격을 차단하는 방식이다.

일반적으로 백본급 네트워크 장비와의 연동을 통해 차단기능을 제공하기 때문에 In-Line 방식에 비해 구성상 복잡하며 상대적으로 고비용이 요구되므로 ISP 및 대형 서비스 망에서 주로 구성되는 방식이다

NAC는 말 그대로 네트워크 접근 제어를 뜻하는 것으로 엔드 포인트 (PC, 스마트폰 등과 같은 네트워크에 접속하는 모든 유무선 기기)가 네트워크에 접근하기 전 보안 정책 준수 여부를 검사하여 네트워크 사용을 제어하는 것을 말한다.

또한, NAC 시스템은 네트워크에 연결된 엔드 포인트들의 여러 정보를 수집하여 엔드 포인들을 분류하고 분류한 그룹의 보안 위협 정도에 따른 제어를 수행하기도 한다.

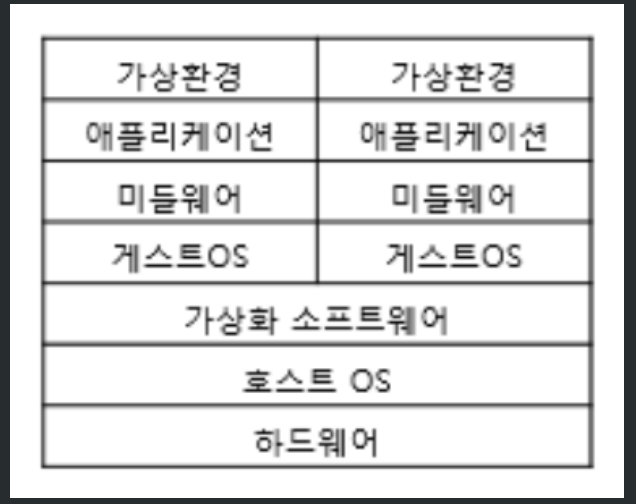


환경구축은 현제 상황에서의 리스크가 크고 리턴이 적당한 실제환경이 아닌 리스크는 작고 리턴도 그럭저럭 인 가상환경으로 구축 했다.

가상화는 3가지의 종류로 나누어 볼 수 있다. 그 중 첫번째는 호스트 가상화이다

호스트 가상화 :

호스트가상화는 Base가 되는 Host OS위에 Guest OS가 구동되는 방식이다. 종류로는 VM Workstation, VMware Server, VMware Player, MS Virtual Sever, Virtual PC, Virtual Box, Paralles Workstation 등이 있다.



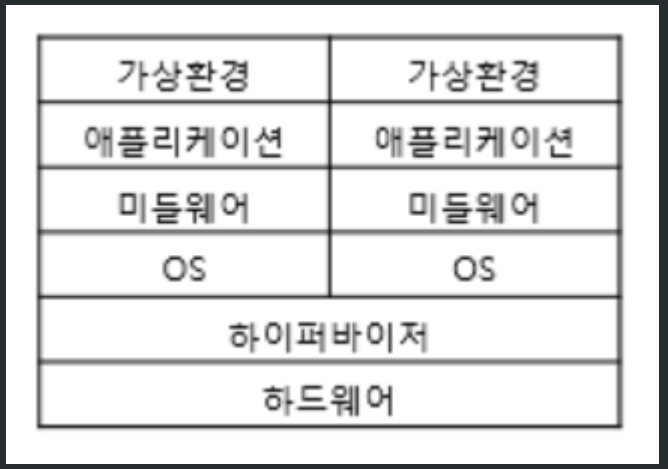
장점 : 가상의 하드웨어를 에뮬레이팅 하기 때문에 호스트 운영체제에 크게 제약사항이 없음

단점 : OS위에 OS가 얹히는 방식이기 때문에 오버헤드가 클 수 있음

두번째는 하이퍼 가상화이다

하이퍼 바이저 가상화 :

하이퍼 가상화는 Host OS없이 하드웨어에 하이퍼 바이저를 설치하여 사용하는 방식이다. 종류로는 Xen, MS hyper-V, citrix, KVM 등이 있다.



장점 : 별도의 Host OS가 없기 때문에 오버헤드가 적고, 하드웨어를 직접 제어하기 때문에 효율적으로 리소스를 사용할 수 있음

단점 : 자체적으로 머신에 대한 관리 기능이 없기 때문에 관리를 위한 컴퓨터나 콘솔이 필요함

하이퍼 바이저 가상화는 또 두개의 분류로 나누어 지는 데

전가상화(Full-Virtualization or Hardware Virtual Machine)와 반가상화(Para-Virtualization)로 나누어진다.

전가상화(Full-Virtualization)

전가상화는 하드웨어를 완전히 가상화 하는 방식으로 Hardware Virtual Machine 이라고도 불린다.
하이퍼 바이저를 구동하면 DOM0라고 하는 관리용 가상 머신이 실행되며, 모든 가상머신들의 하드웨어 접근이 DOM0을 통해서 이루어진다.
즉, 모든 명령에 대해서 DOM0가 개입을 하게 되는 형태이다.

쉽게 말해 하이퍼 바이저는 가상화 된 OS가 가리지 않고 각 OS들이 내리는 명령어를 실행할 수 있다.
또한 가상화 된 OS들에게 자원을 할당해주는 역할도 담당한다.

장점 : 하드웨어를 완전히 가상화 하기 때문에 Guest OS 운영체제의 별다른 수정이 필요 없음

단점 : 하이퍼 바이저가 모든 명령을 중재하기 때문에 성능이 비교적 느림

반가상화(Para-Virtualization)

반가상화는 전가상화와 달리 하드웨어를 완전히 가상화 하지 않는 다.

전가상화의 가장 큰 단점인 성능저하의 문제를 해결하기 위해 하이퍼 콜(Hyper Call)이라는 인터페이스를 통해 하이퍼 바이저에게 직접 요청을 날릴 수 있다.

쉽게 말하면 가상화된 각 OS들이 각각 다른 번역기를 갖고 있는 것입니다. 그 번역기는 각각 다른 OS에서 내리는 각각 다른 명령어를 "더해라" 라고 번역해주게 되는 것이다.

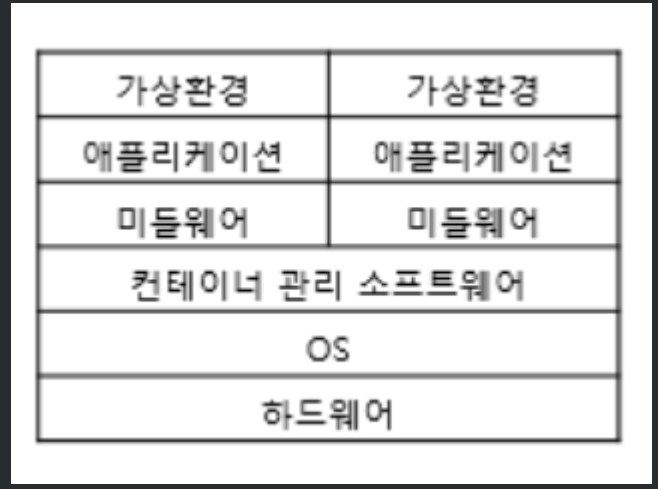
장점 : 모든 명령을 DOM0를 통해 하이퍼 바이저에게 요청하는 전가상화에 비해 성능이 빠름

단점 : 하이퍼 바이저에게 Hyper Call 요청을 할 수 있도록 각 OS의 커널을 수정해야 하며 오픈소스 OS가 아니면 반가상화를 이용하기가 쉽지 않음

마지막으로는 컨테이너 가상화이다

컨테이너 가상화 :

호스트 OS위에 컨테이너관리 소프트웨어를 설치하여, 논리적으로 컨테이너를 나누어 사용한다.
컨테이너는 어플리케이션 동작을 위한 라이브러리와 어플리케이션 등으로 구성되기때문에 이를 각각 개별 서버처럼 사용 가능하다.



장점 : 컨테이너 가상화는 오버헤드가 적어 가볍고 빠른 장점이 있음

그중 실습에 사용할 가상화는 호스트 가상화이다, 가상머신으로는 VirtualBox을 OS는 Linux의 Ubuntu를 사용 했고 가상 네트워크 시뮬레이터로는 GNS3을 사용 할 것이다.

그 외의 사용할 프로그램으로는 방화벽을 위한 오픈소스 프로그램인 Untangle 방화벽을 사용할 것이지만 현제는 ARISTA로 개명 한 이후 유료 프로그램으로 전환 되며 실습에 어려움을 주고있다.

감사합니다

1p mix ▼

이후에는 십습들과 심화 적인 이론들을 공부 해보고
느껴 보겠습니다.