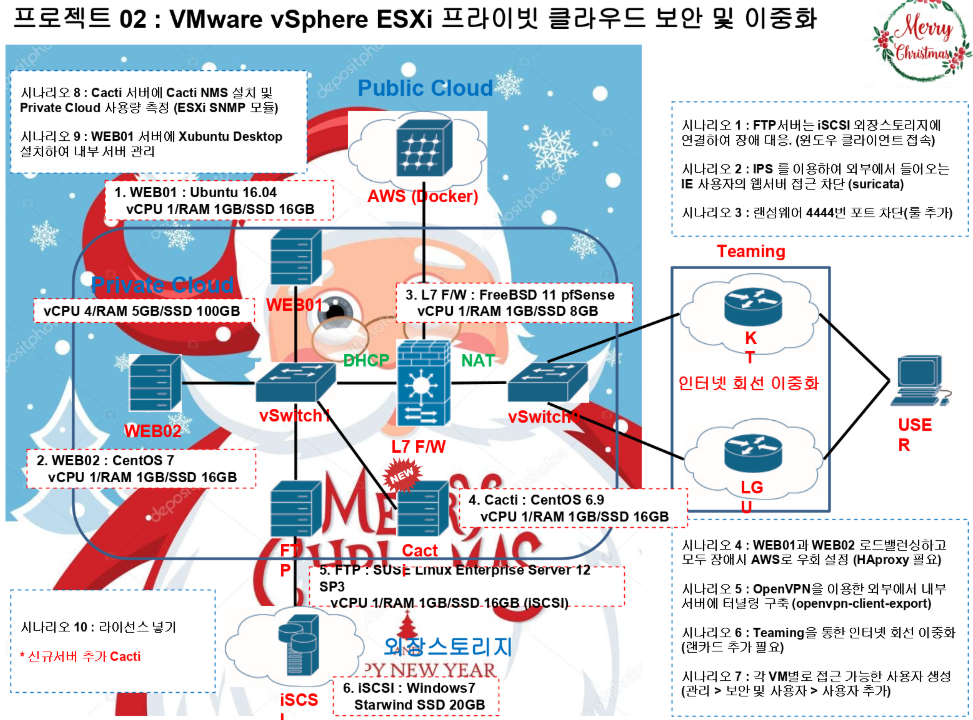
**프로젝트 02**

**-VMware vSphere ESXi private cloud security and LoadBalancing**

**(프라이빗 클라우드 보안 및 이중화)**

****

**[환경설정]**

1. VMware에 ESXi6.7 설치하기 ☞ 가상화 VM을 올리기 위한 하이퍼바이저 설치
2. 호스트PC 웹에서 ESXi 접속 및 VM 설치 전 가상 스위치 vSwitch1, 네트워크 VM Network1 추가
3. WAN과 LAN을 연결해 줄 L7 F/W 설치(pfSense) ☞ vSwitch0과 vSwitch1을 연결해줌.
4. WEB01(Xubuntu), WB02(CentOS7)
5. AWS Docker EC2(혹은 확인용 google연결) 만들고 WEB01, WEB02 로드밸런싱 확인하기
6. iSCSi, FTP 설치
7. Cacti 설치 및 그래프 사용확인하기

**[시나리오]**

1. FTP서버는 iSCSI 외장 스토리지에 연결하여 보안 및 장애 대응(윈도우 클라이언트 접속)
2. 랜섬웨어 4444번 포트 차단(firewall rule 추가)
3. WEB01과 WEB02 로드밸런싱하고 모두 장애시 AWS로 우회설정(HAproxy 필요)
4. OpenVPN을 이용한 외부에서 내부서버에 터널링 구축(openvpn-client-export)
5. Teaming을 통한 인터넷 회선 이중화(ESXi에 랜카드 추가 필요)
6. 각 VM별로 접근 가능한 사용자 생성(관리 > 보안 및 사용자 > 사용자 추가)
7. Cacti 서버에 Cacti NMS 설치 및 Pricate Cloud 사용량 측정 (ESXi SNMP 모듈)
8. WEB01 서버에 Xubuntu Desktop 설치하여 내부 서버 관리
9. 라이선스 넣기

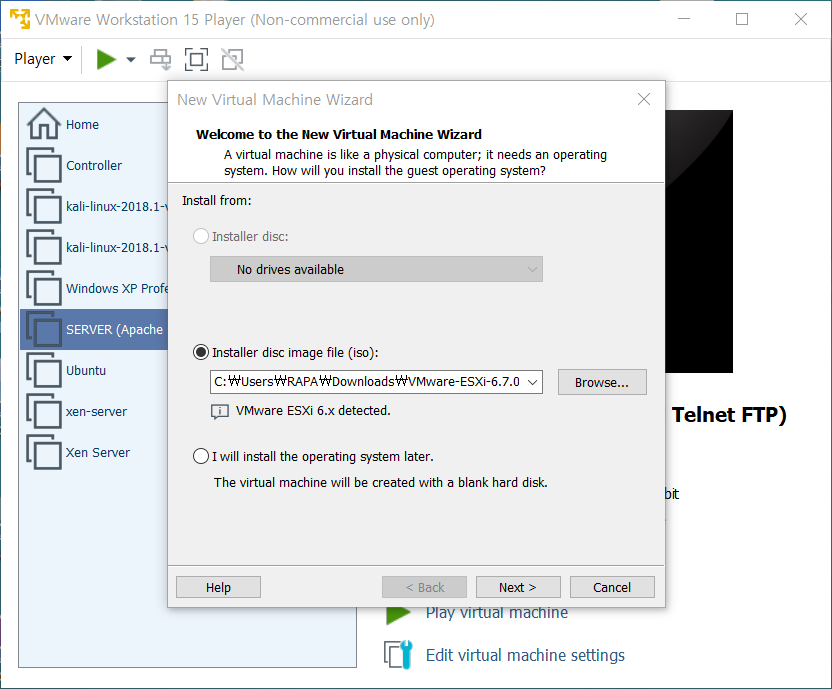
**환경설정**

**1. ESXi 설치**

- VMware Workstation 15 Player에서 설치한다.

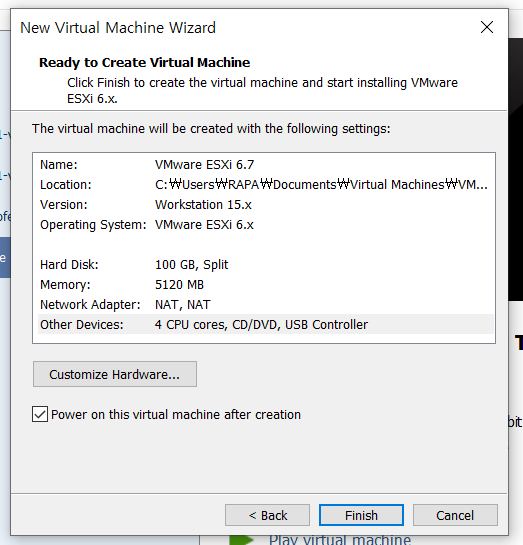
☞ Player>file>new virtual machine

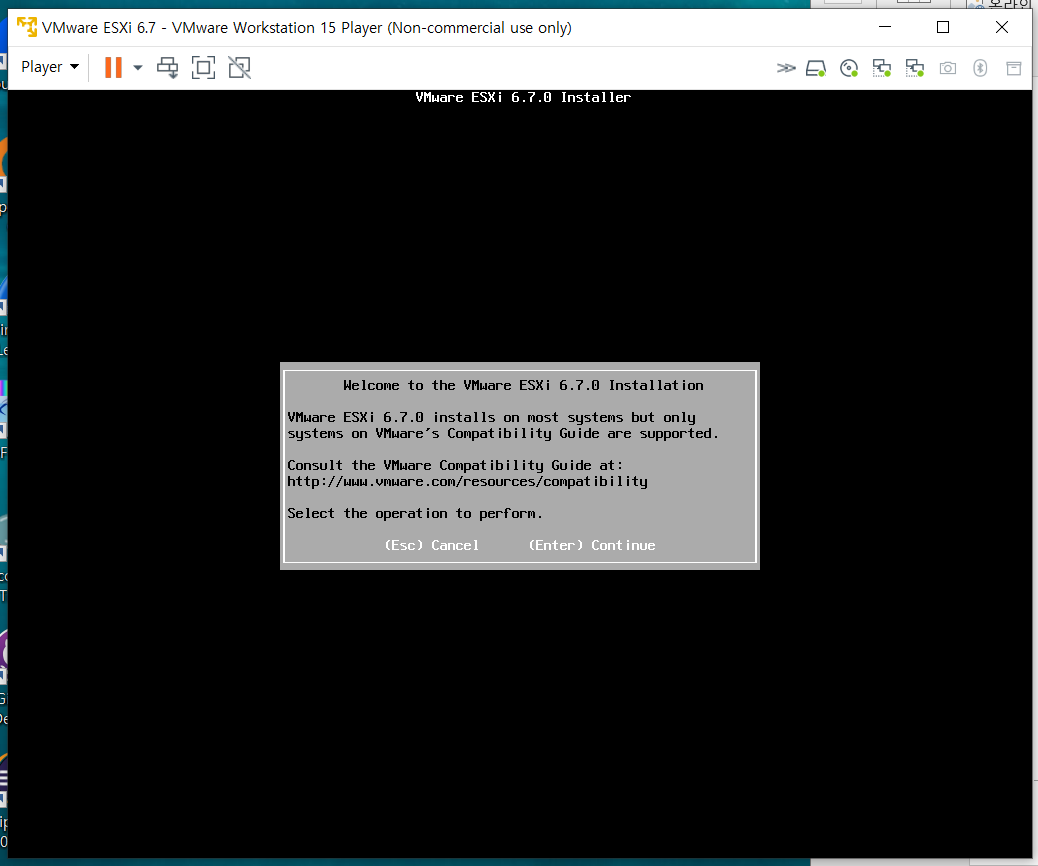
-미리 준비해둔 VMware-ESXi-6.7.0 iso파일을 찾아서 넣는다. (없다면 VMware 홈페이지 가서 로그인 후 다운가능)



-추가 설정 : 용량 100GB / split (꼭 split으로 쓰지 않아도 됌)

-Customize Hardware>Processors 4, Memory 5120MB, Add Network Adapter2(NAT)

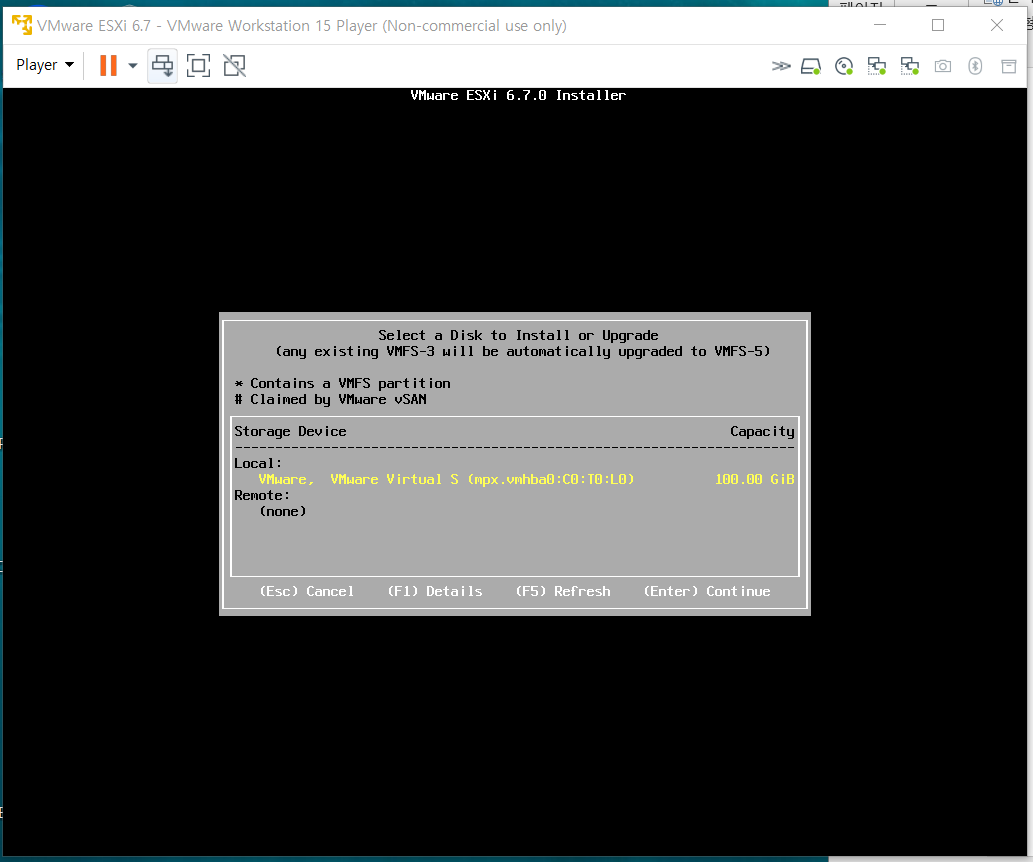


-이 뒤에 Finish를 누르면 ESXi 설치 시작.

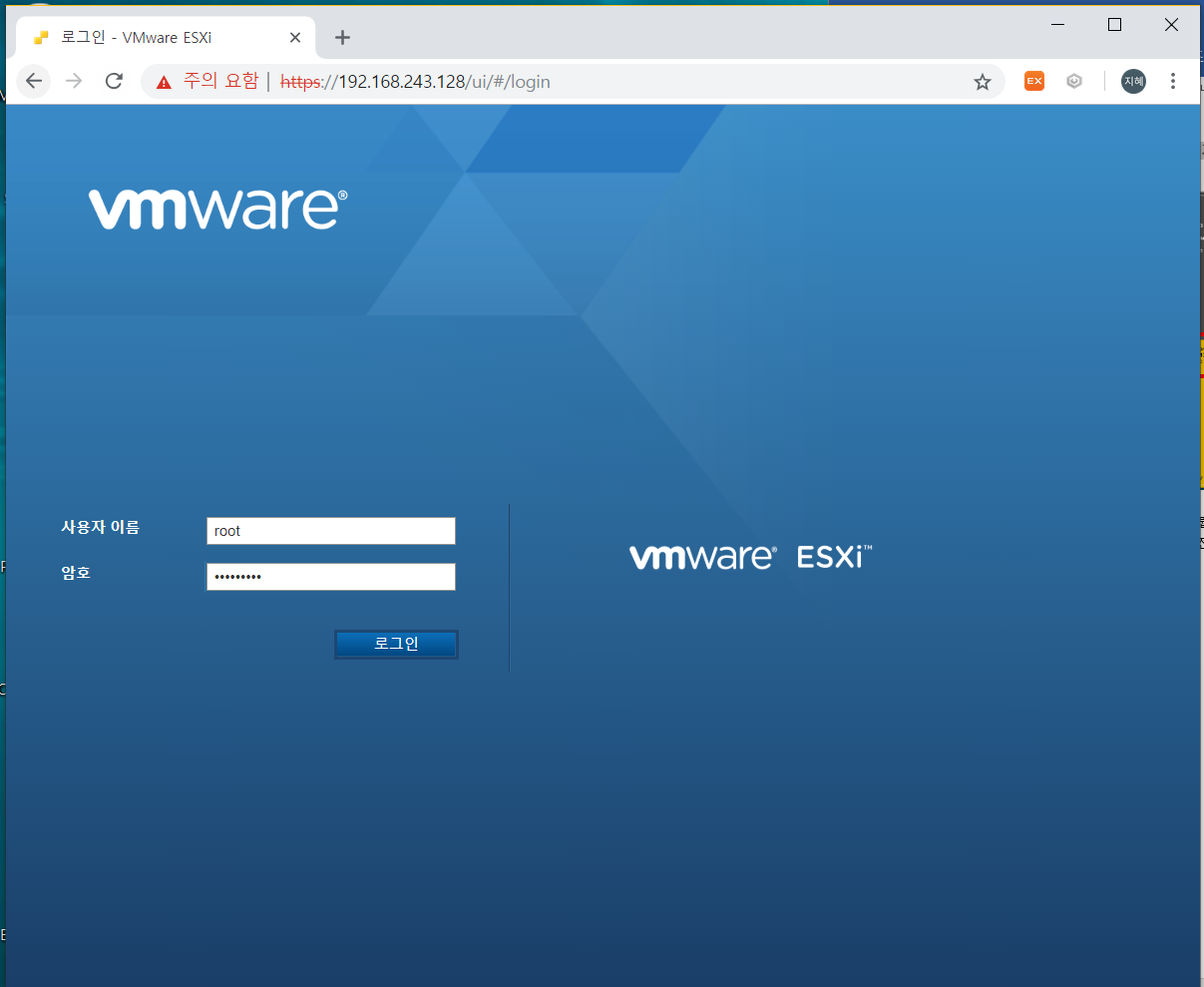
* Continue



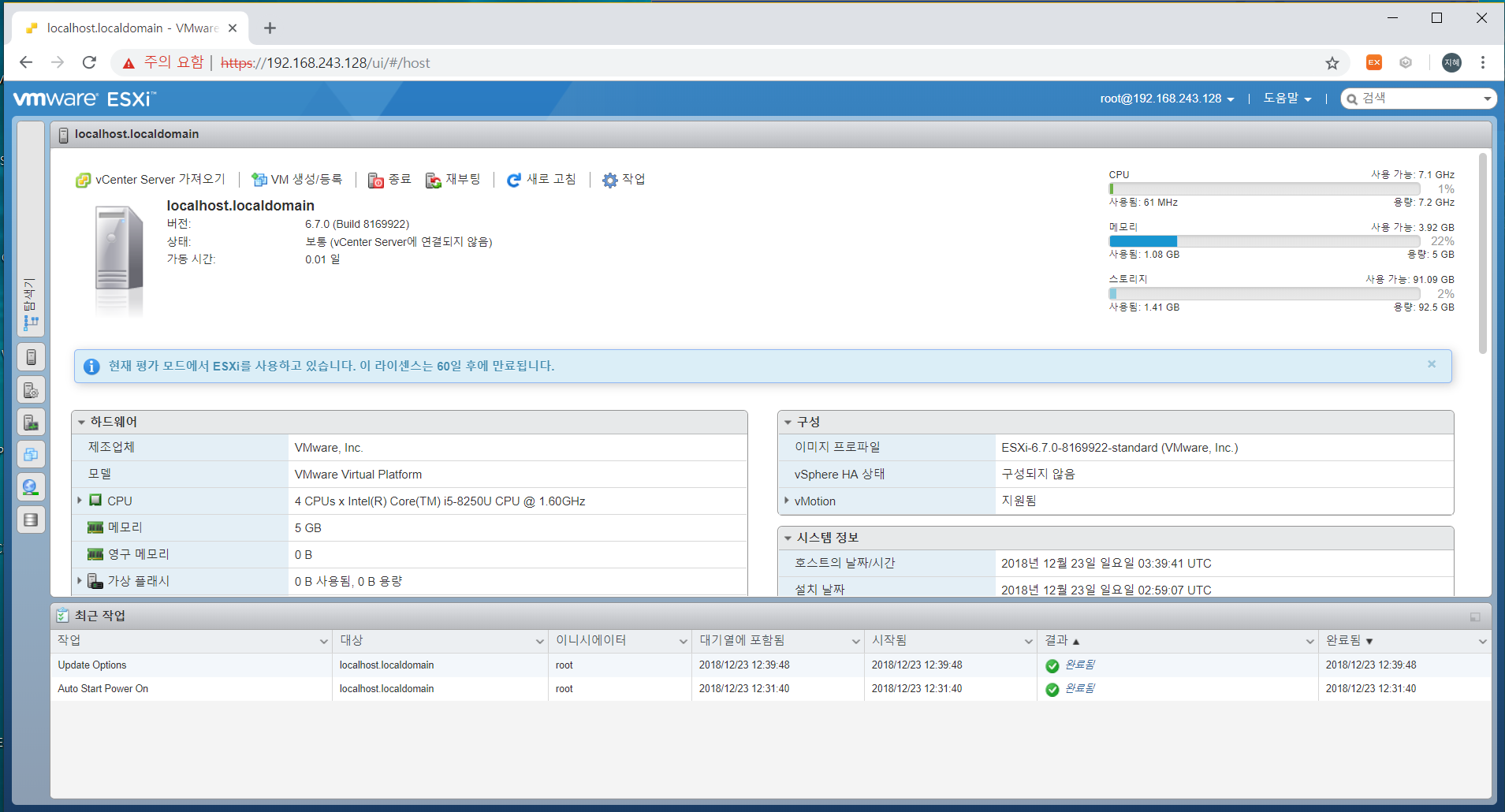
* F11 (Accept and Continue)



* Enter (Continue) 이 뒤에 나올 Language : US Default로 두기
* Root password는 보안 규칙에 따라 대소문자+특수문자 해서 8문자이상으로.
* 그 다음 F11눌러서 설치한 뒤에 Reboot 하고 화면에 뜬 Management ip를 호스트PC 웹페이지로 들어가서 확인하면 바로 ESXi Management 화면이 나온다.
* Management IP : <http://192.168.243.128> / Root password : Mode1752!

-위의 IP로 host PC의 웹페이지 접속 시, 연결이 비공개로 설정되어 있지 않다고 경고 화면이 뜨는데, [고급]을 눌러 [안전하지 않음]으로 이동을 클릭하면 제대로 나온다.

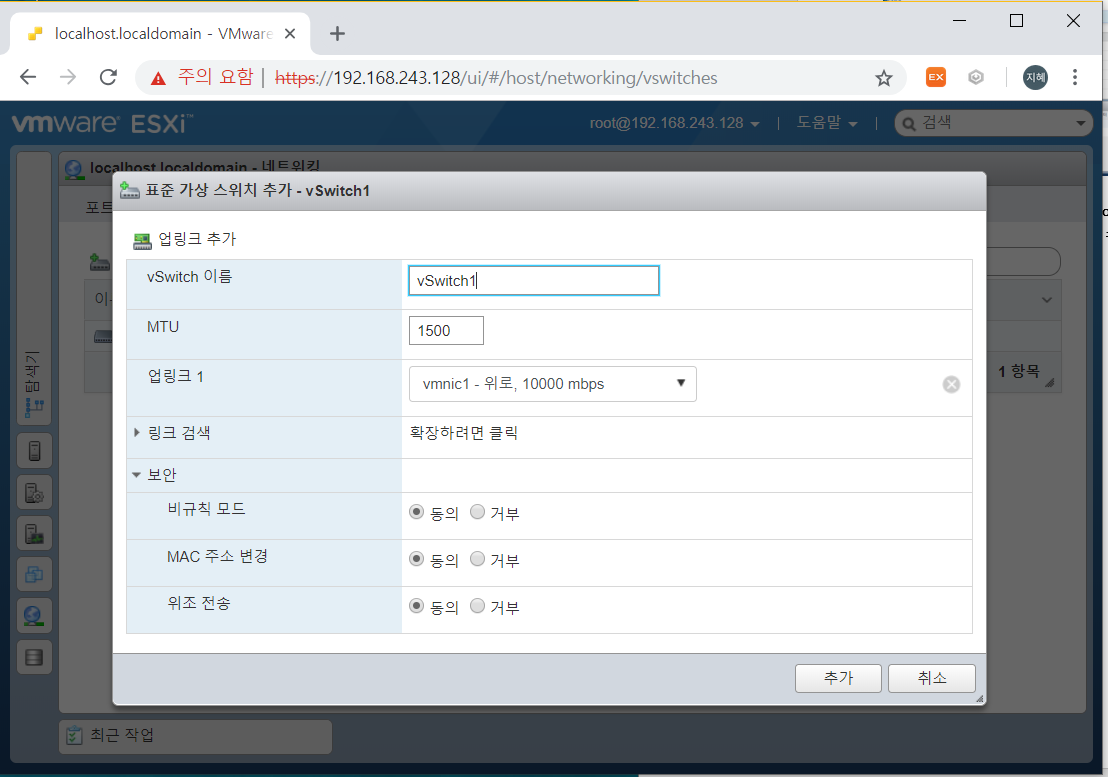
-접속 시 아래와 같은 ESXi Management 화면이 나온다.

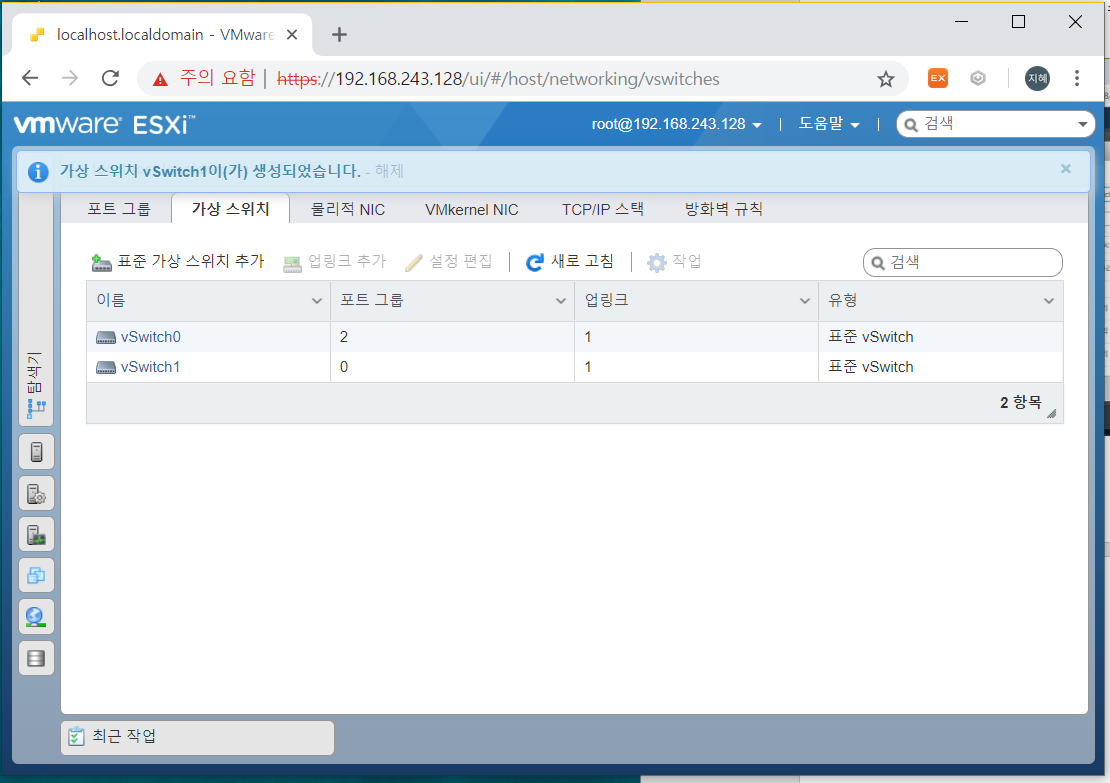


**2. ESXi 에 vSwitch1와 VM network1 추가하기**

> 네트워킹 > 가상스위치 > 표준 가상 스위치 추가

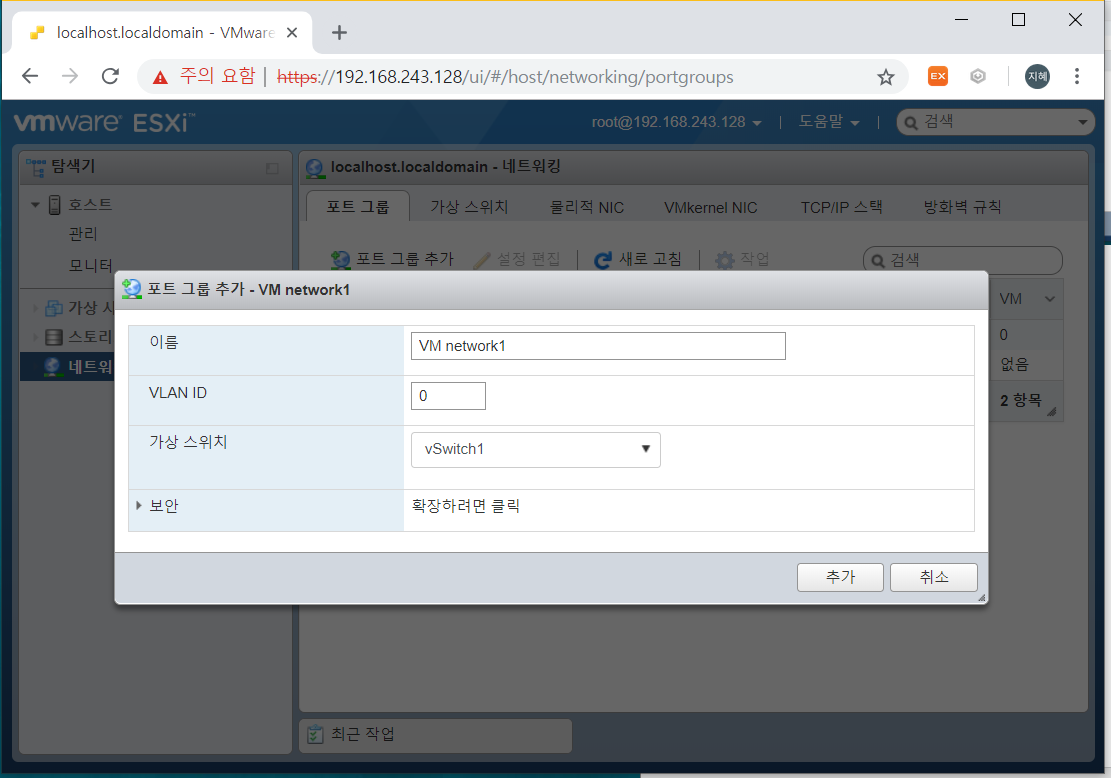
> 이름 : vSwitch1 / 보안 : 비규칙 모드, MAC 주소 변경, 위조 전송 모두 [동의]로 바꾸기





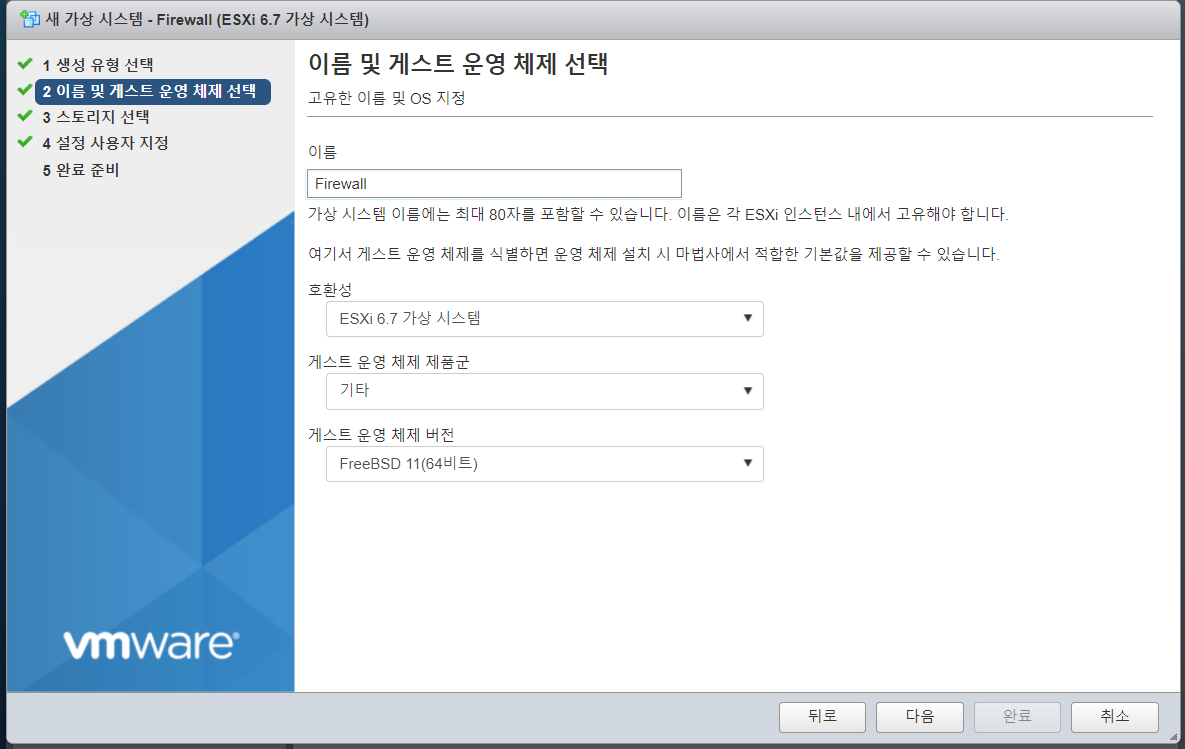
> 포트 그룹 > 포트 그룹 추가

> 이름 : VM network1 / 가상 스위치 : vSwitch1

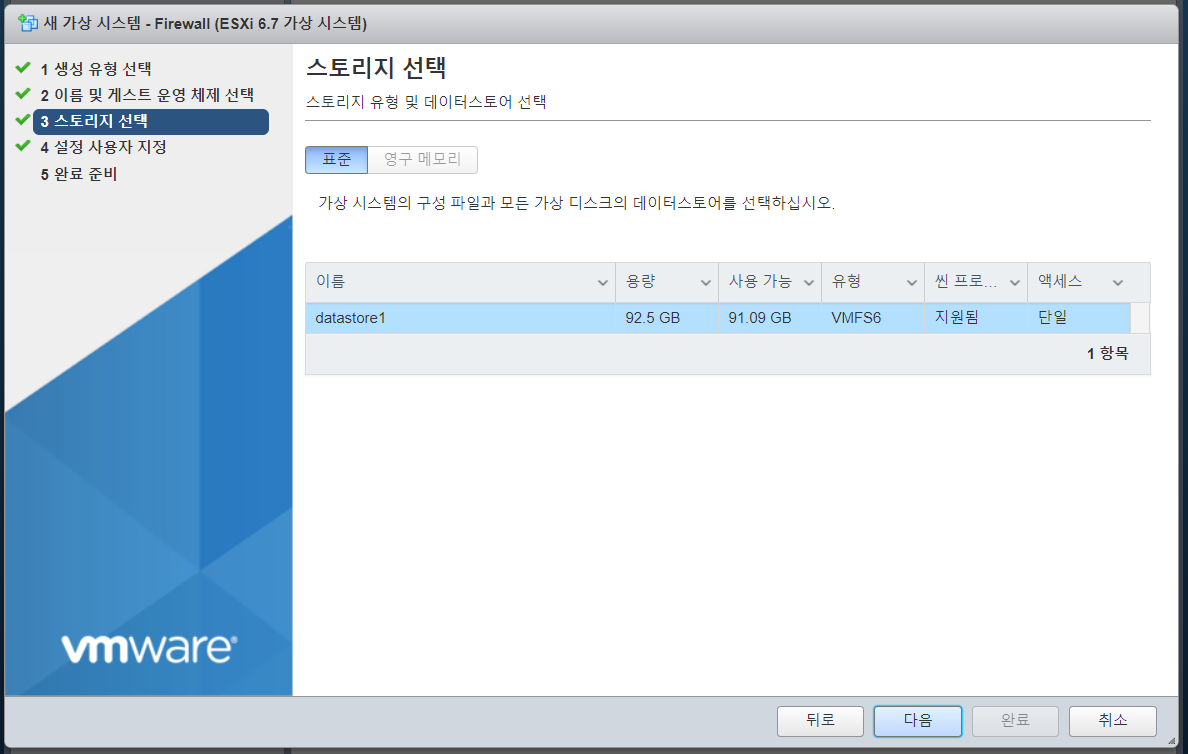


**3. F/W(방화벽) 설치**

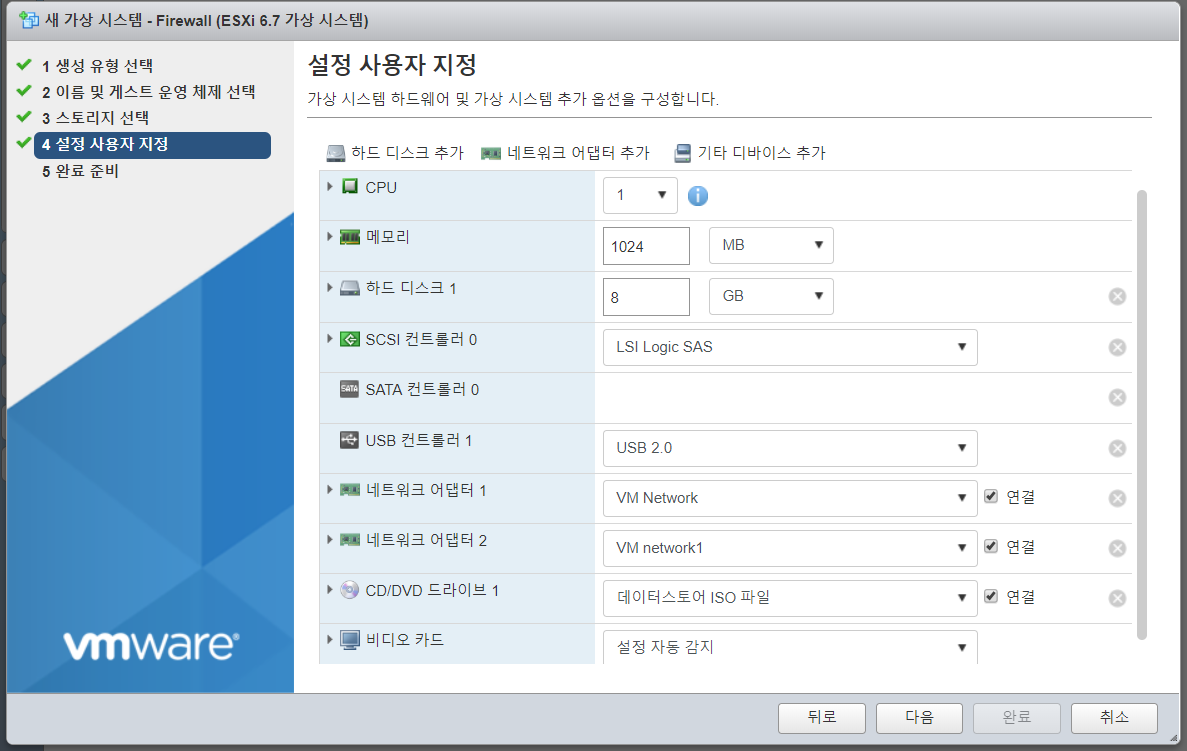
> 가상 시스템 > VM생성/등록



* pfSense는 운영체제 버전이 FreeBSD 11(64bit) 이다.

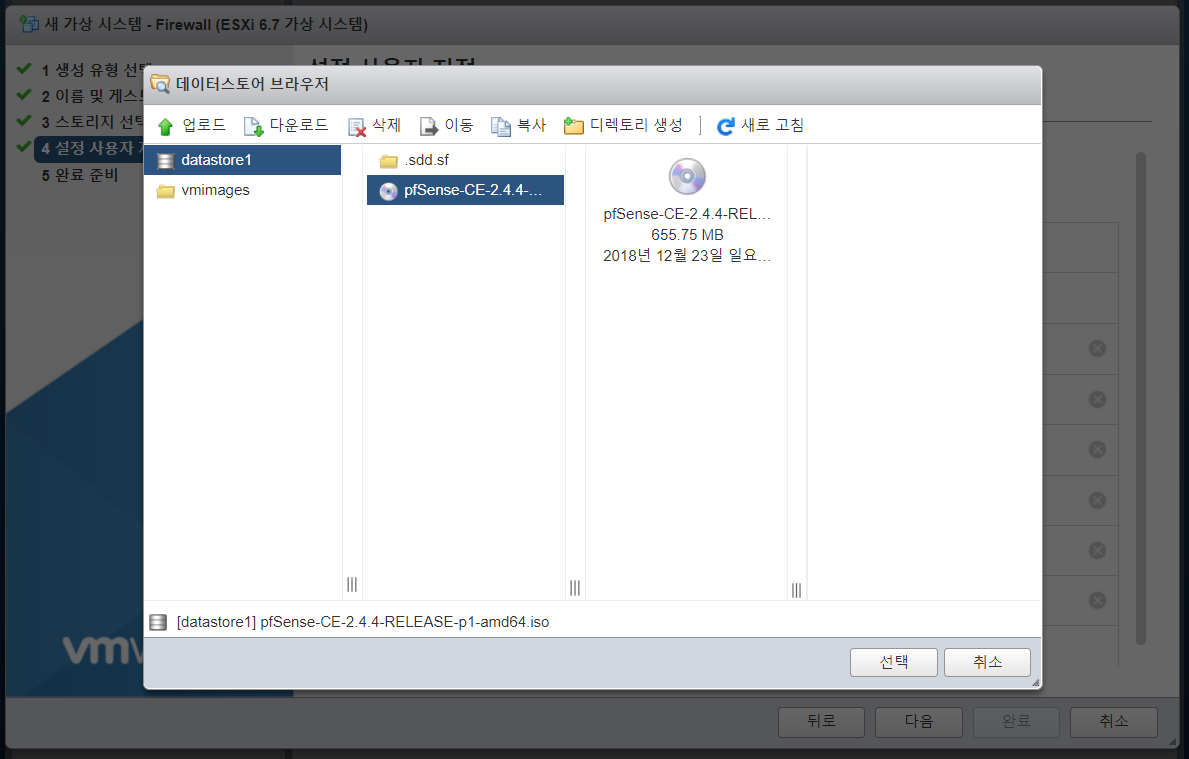


* 외장 스토리지 iSCSI가 아직 설치되지 않았으므로 기본 스토리지인 datastore1 밖에 없음.

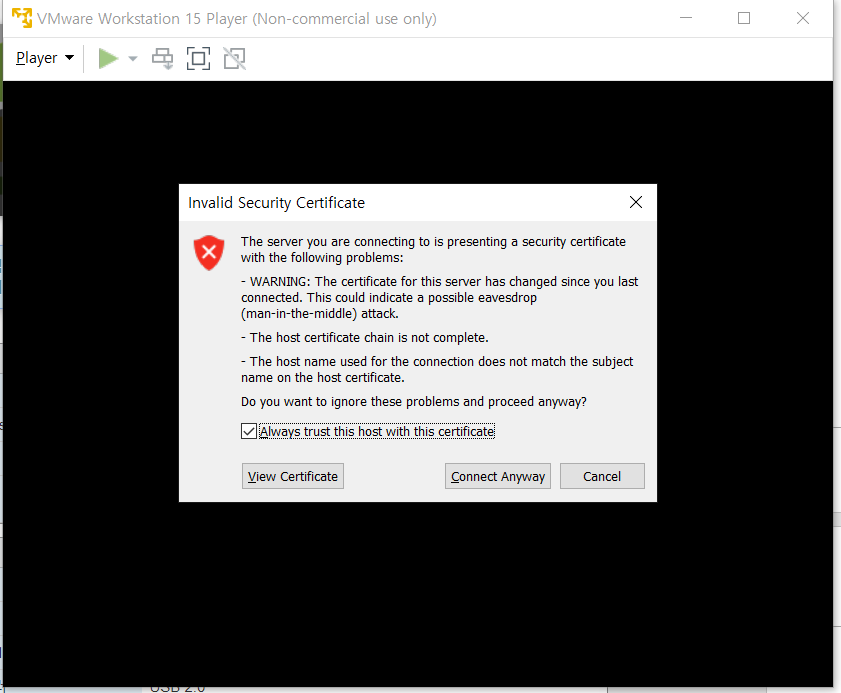


* 하드 디스크1 세부설정 : 1024MB. 8GB, 씬 프로비저닝됨.
* 네트워크 어댑터1 : VM network1 (아까 새로 만든 가상 네트워크)
* 네트워크 어댑터2 : VM Network (기존의 WAN과 연결되는 네트워크)
* CD/DVD 드라이브1 : pfSense iso 파일
* 그래픽 : 설정 자동 감지

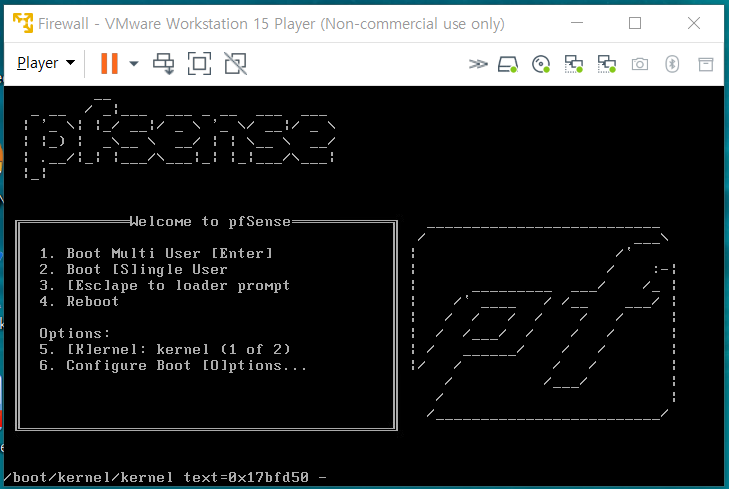
-만약 iso 파일이 없다면 datastore1에 pfsense파일을 업로드해서 선택하기.



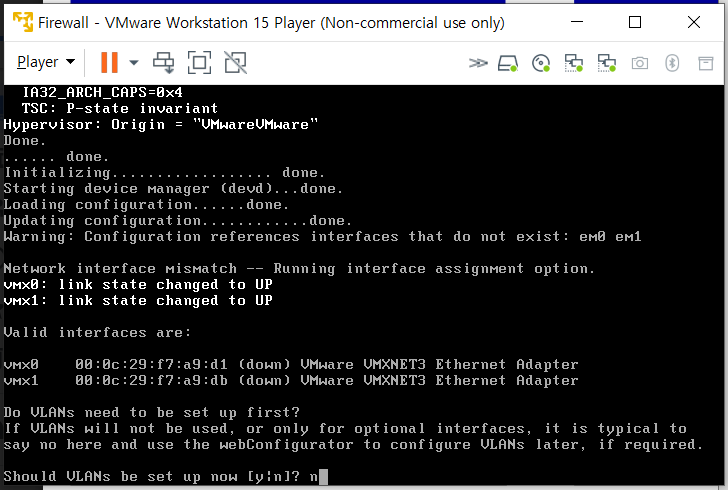
-생성 완료 시, 해당 VM에 오른쪽 마우스 클릭, 원격 콘솔 조종 시작.



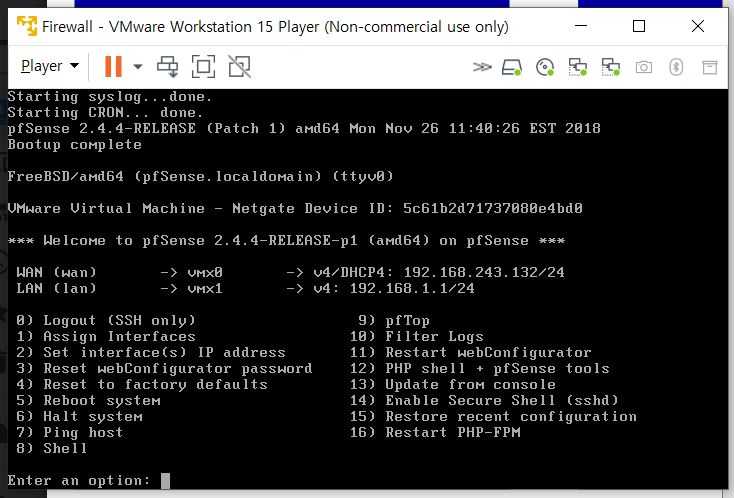
-Connect Anyway 클릭.



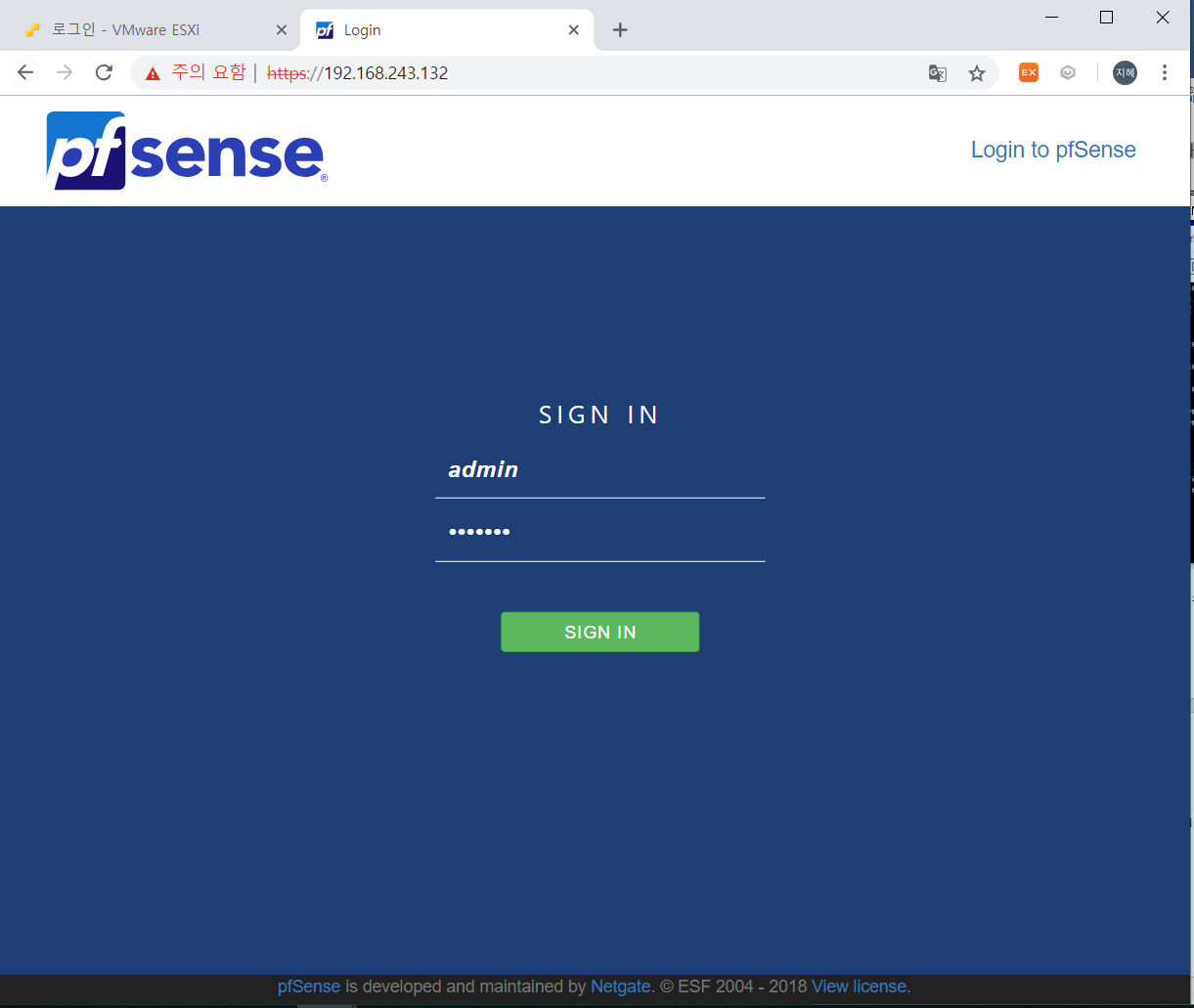
* 부팅이 다 될 시 Accept 후, 계속 Enter 후, fault 설정에서 바뀌는 것 없음)



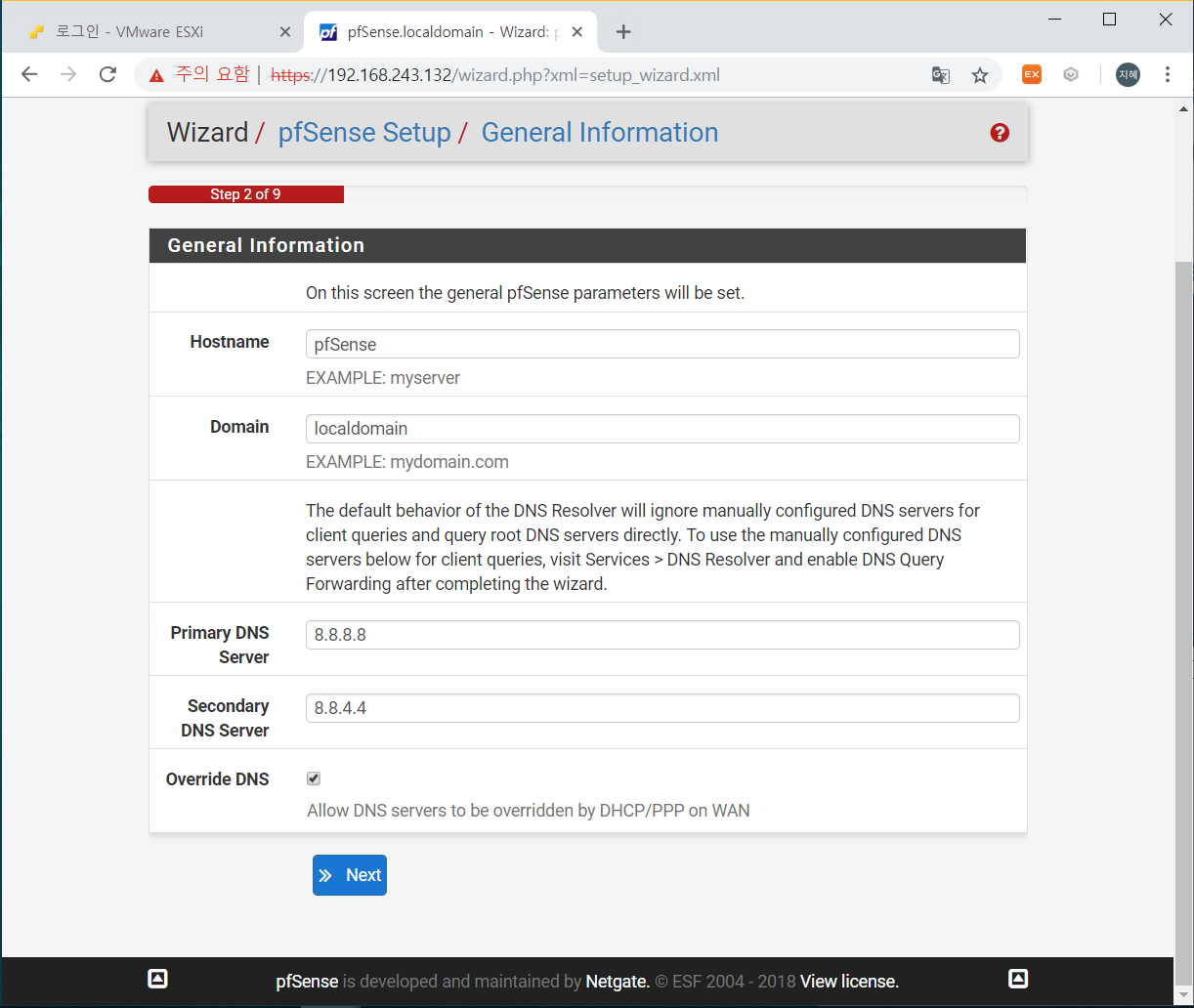
* 부팅 로딩 후, VLAN을 설정하겠냐는 질문이 나오는데, 우리는 VLAN 설정을 하지 않을 것이기 때문에 n을 눌러준다.
* WAN : vmx0 / LAN : vmx1



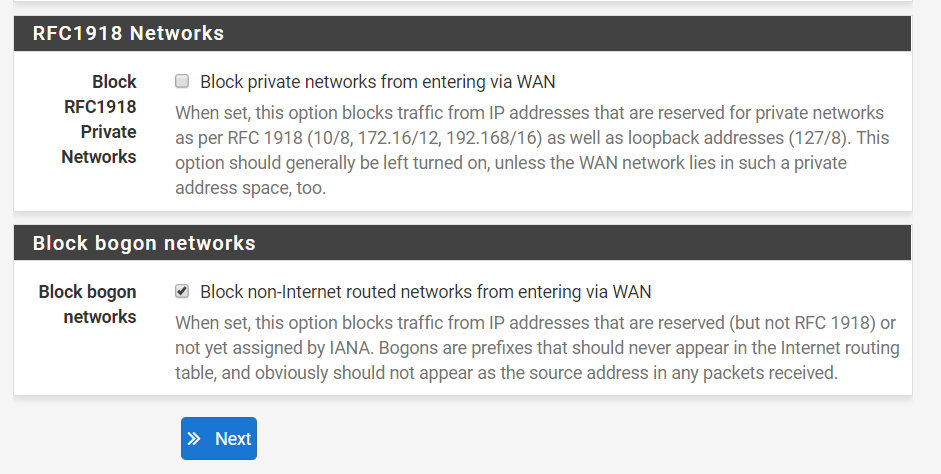
* 8 > pfctl -d
* 방화벽 기본 설정을 위해 방화벽 열어주기
* 위에 할당 받은 192.168.243.132(pfsense management ip)로 호스트 pc들어가서 환경설정해주기 (초기 id : admin / 초기 pw : pfsense)



* 로그인 되면 바로 wizard>pfSense Setup 이 자동적으로 시작됨
* 앞의 두 설명문은 next로 넘기고 information 작성하기 (8.8.8.8 -> 구글네임서버)



* Step3 : Timezone만 Aisa/Seoul로 바꿔주기
* Step4 : RFC1918 Networks 만 체크 없애기(우리는 개인 네트워크를 설정하므로 개인 네트워크가 WAN 통해 들어오는 걸 다 차단할 필요가 없음)

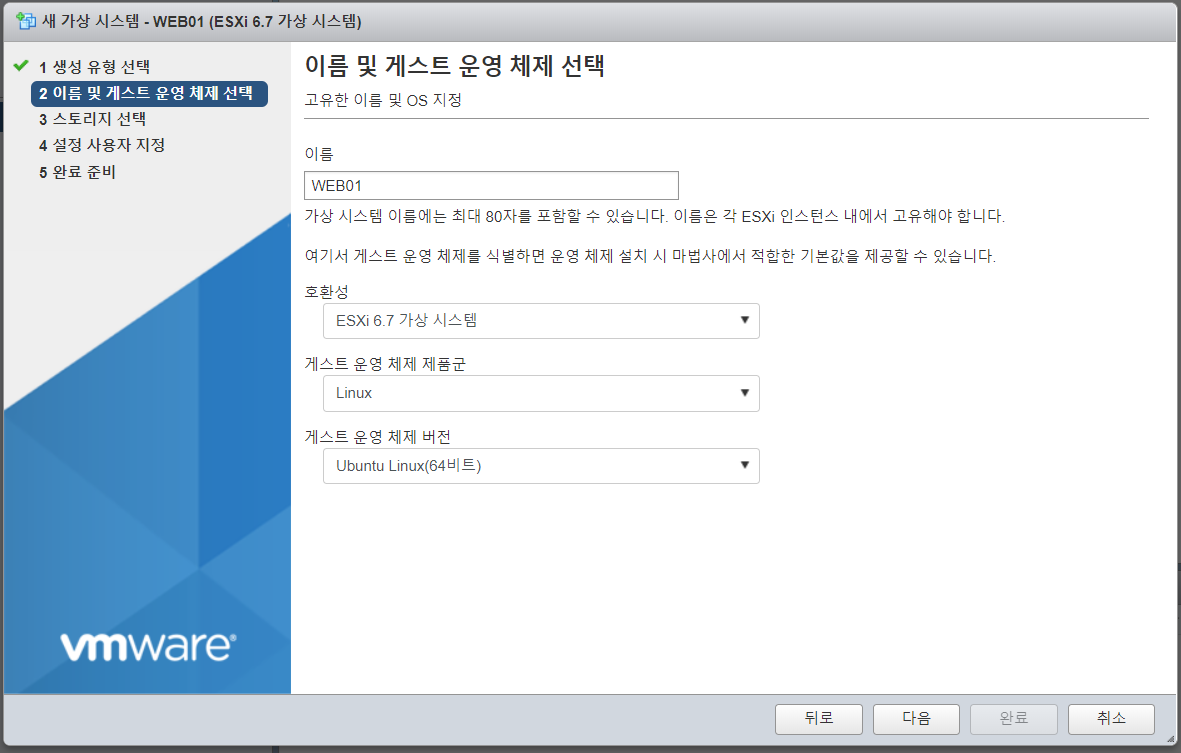


* Step5 : LAN IP Address는 기본으로 감
* Step6 : Admin PW 바꾸기 (원래 pfsense였던 걸 자기 임의설정으로 바꾸는 것)
* 그 뒤로는 reload하고 complete페이지가 나오면 finish하면 방화벽 설정 끝.

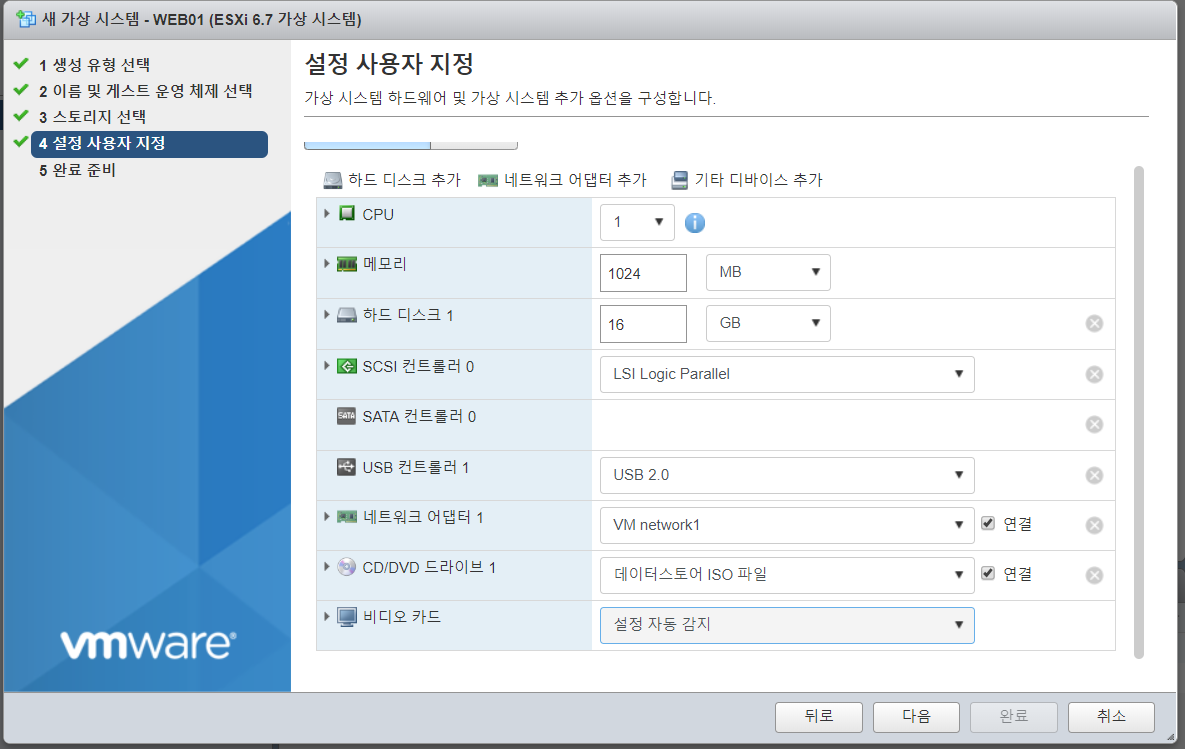
(나중에 WEB01 의 Xubuntu 설치 후 구글에서 192.168.1.1로 들어가면 방화벽 관리페이지 나타남.)

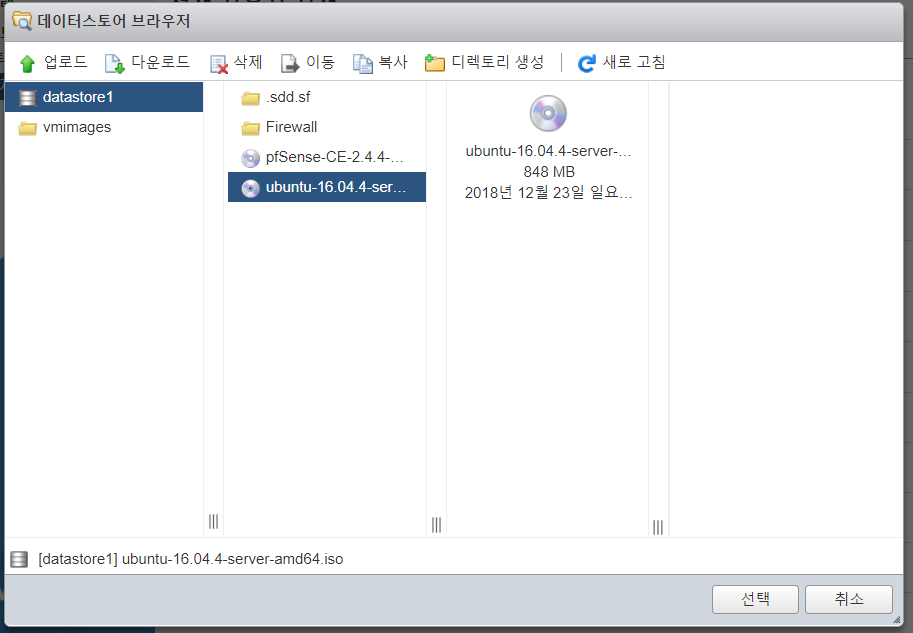
**3. WEB01(XUbuntu) 설치**

> 가상 시스템 > VM생성/등록

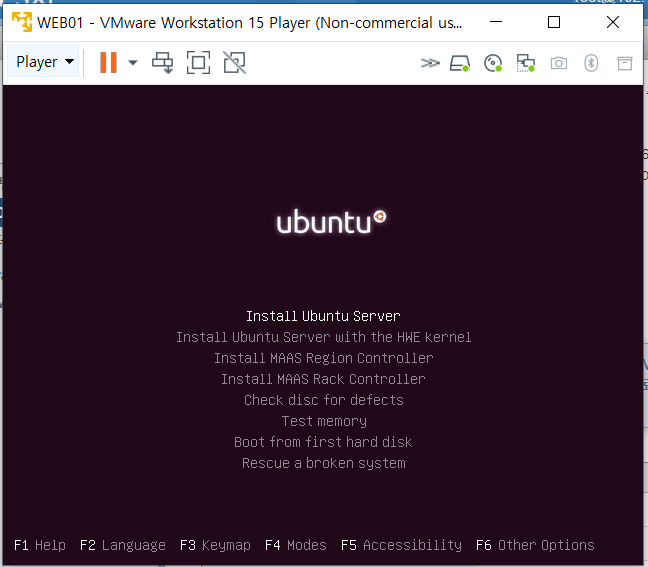


* WEB01은 먼저 Ubuntu부터 설치해야 함. (ubuntu 64bit)
* datastore1을 스토리지 선택함
* 메모리 : 1024MB, 하드디스크1 : 16GB, 씬프로비져닝, 네트워크 어댑터 : VM network1





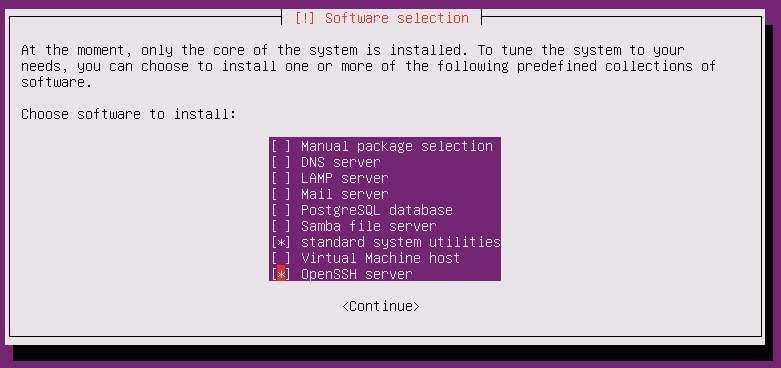
* 이후 VM 전원 켜서 Ubuntu 설치로 들어가면 된다.



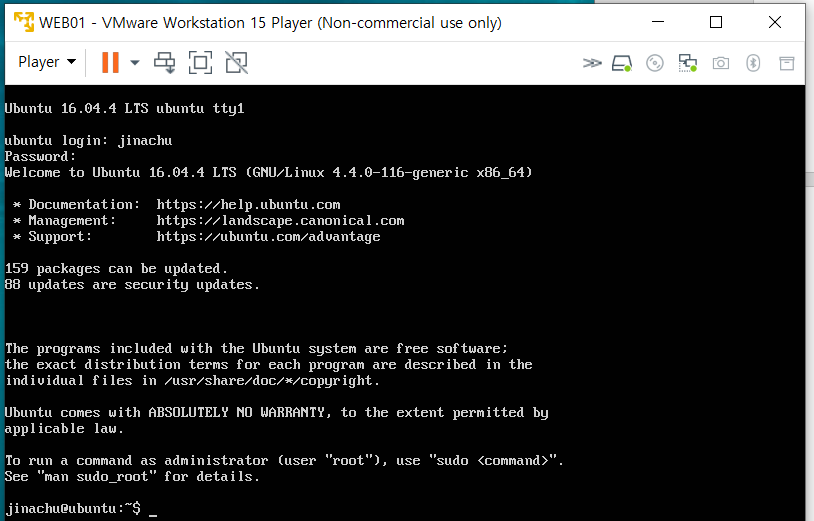
* 기본 Language는 키보드 설정은 영어로 하되, 지역은 Korea Republic of 으로 하기.
* Hostname은 기본 ubuntu로 놔두기. New user나 pw는 자기임의로. 그 뒤로는 디폴트설정.

Ex) New user : jinachu / pw : mode1752

* 파티션은 전체 디스크를 다 쓰는 것으로 하기 -> 파티션 디스크 change yes
* 프록시 설정은 하지 않음(프록시 사용 안함), 자동 업데이트도 하지 않기



* OpenSSH Server 꼭 열어주기, 이 후 Grub boot loader 설치하기
* 다 설치하면 console 화면이 나오는데 이 때 아까 설정했던 user/pw로 로그인해주기



-XFCE 데스크톱을 만들기 위해 아래의 명령어 그대로 입력해서 깔기

1) 레포지토리 다음카카오로 설정

sudo cp /etc/apt/sources.list ~/sources.list.old

sudo sed -i 's/kr.archive.ubuntu.com/ftp.daumkakao.com/g' /etc/apt/sources.list

sudo diff ~/sources.list.old /etc/apt/sources.list | wc -l

38

2) 주분투 데스크톱 설치

sudo apt update && sudo apt-get install --no-install-recommends xubuntu-desktop -y

3) 구글 설치

sudo wget https://dl.google.com/linux/direct/google-chrome-stable\_current\_amd64.deb

sudo apt-get install libxss1 libgconf2-4 libappindicator1 libindicator7 fonts-liberation libnspr4 libnss3 -y

sudo dpkg -i google-chrome-stable\_current\_amd64.deb

4) 특정사용자에게 관리자 권한 사용시 비밀번호 묻지 않기

echo "jinachu ALL = (root) NOPASSWD:ALL" | sudo tee /etc/sudoers.d/jinachu

sudo chmod 0440 /etc/sudoers.d/jinachu

5) 휴지통 설치

sudo apt install trash-cli -y

6) 그놈 터미널 설치

sudo apt install gnome-terminal -y

7) 자동 해상도 설정 프로그램 설치

sudo apt install open-vm-tools-desktop -y

8) 네트워크 인터페이스 설정

sudo vi /etc/network/interfaces

auto eth0

iface eth0 inet dhcp

9) NIC 이름 바꾸기

sudo vi /etc/default/grub

#GRUB\_CMDLINE\_LINUX=""

#to

GRUB\_CMDLINE\_LINUX="net.ifnames=0 biosdevname=0"

#and, finally:

sudo update-grub

10) 저장소 업데이트 및 프로그램 업그레이드

sudo apt update && sudo apt upgrade -y

sudo reboot

* Reboot 후에 다시 VM켜서 로그인 하면 데스크톱 화면이 나온다. 거기서 pfSense 들어가서 세팅해주기
* 그리고 terminal에서 apache2 설치해주기

**[ubuntu apache2 설치방법]**

#업데이트

> apt-get update

#아파치2 설치

> apt-get install apache2

#firewall 풀어주기

firewall-cmd --permanent –add-service=http

firewall-cmd --reload

#아파치2 상태 확인

> systemctl status apache2

#아파치2 구동

> systemctl start apache2

#아파치2 부팅시 실행

> systemctl enabled apache2

* 그리고 해당 WEB01의 <http://ip>로 접속하면 apache2 화면이 떠야함.

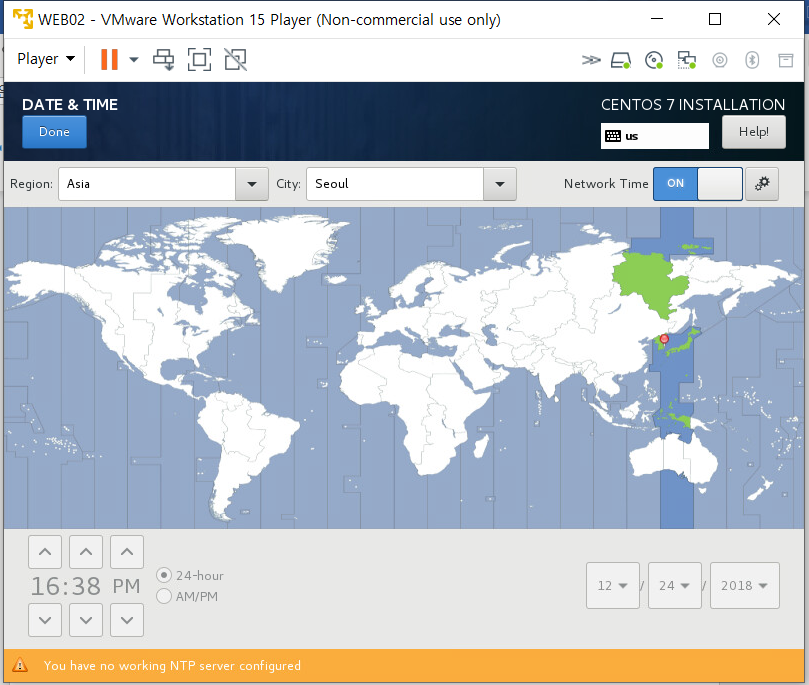
**3. WEB02(CentOS7) 설치**

> 가상 시스템 > VM생성/등록

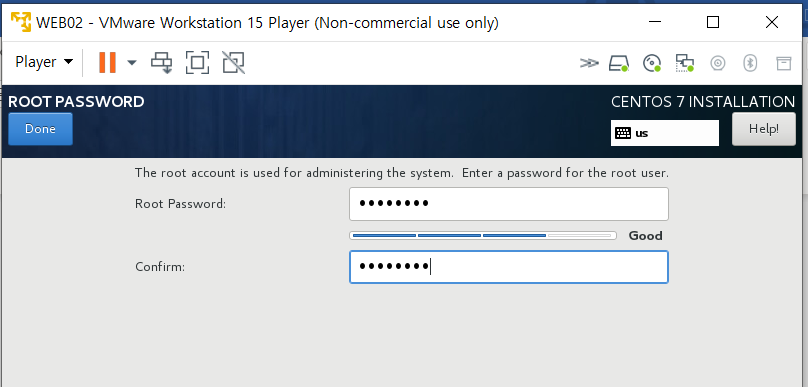




* 위와 같은 설정으로 ubuntu를 설치할 때처럼 과정을 넘어가면 된다.
* 아래는 VM 전원 후에 설치 특이사항으로 시간과 나라, 메모리 할당, 네트워크 통신 열기 등등의 기타사항을 가리킨다.



* 시간과 국가 설정



* 로그인 PW 정하기(로그인 시 필요)



* 가상 디스크 용량 정하기
* 이 위의 과정을 거치면 설치가 되고, reboot 후에 apache2를 설치해주면 된다.

**[CentOS7 apache2 설치방법]**

#apache2 설치되어 있는지 확인

yum list installed | grep httpd

#apache2 없을 시 설치하기

yum install -y httpd

#firewall 풀어주기

firewall-cmd --permanent –add-service=http

firewall-cmd --reload

#apache2 부팅시 실행

systemctl enable httpd

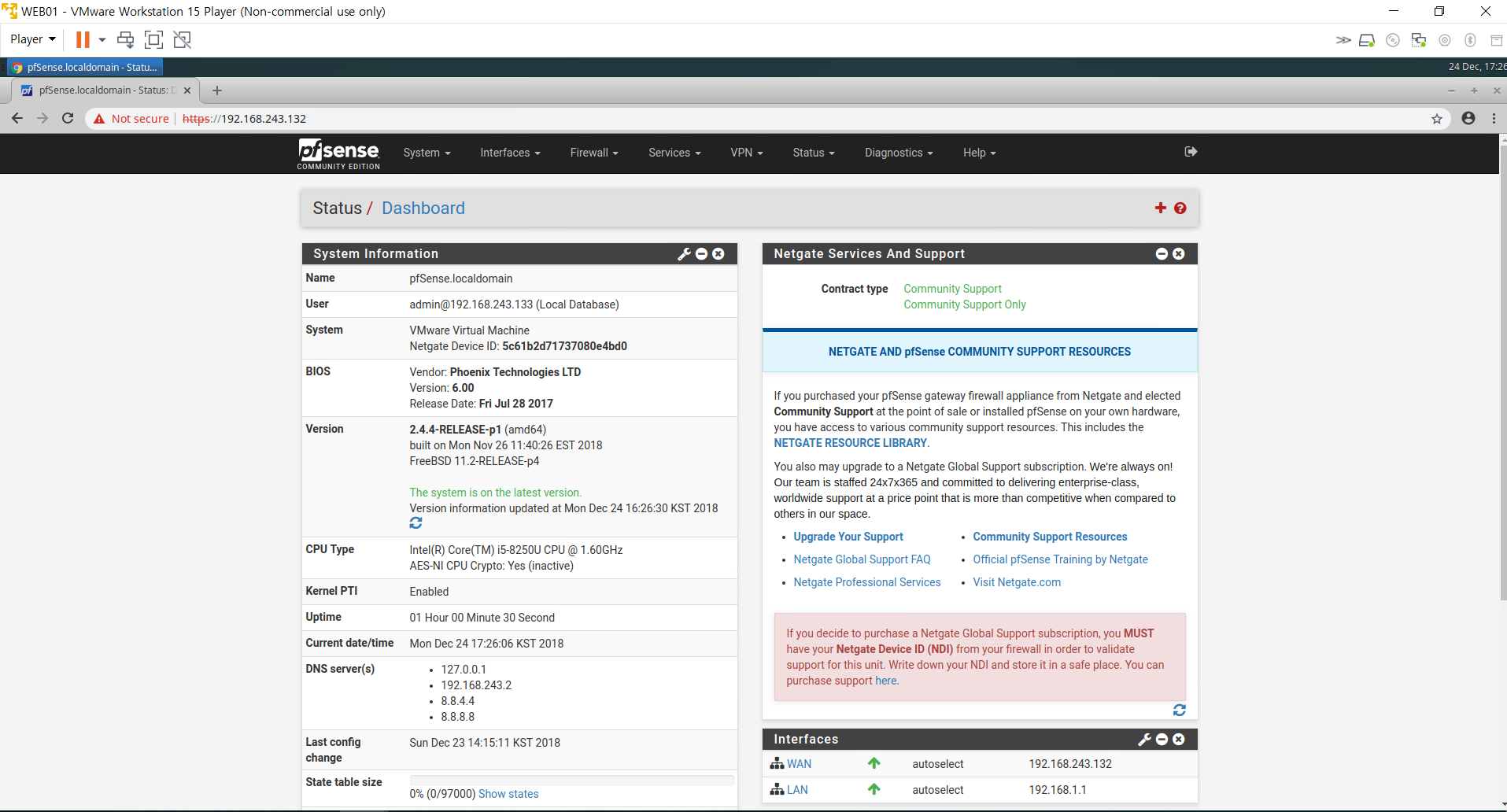
#apache2 서비스 시작

systemctl start httpd

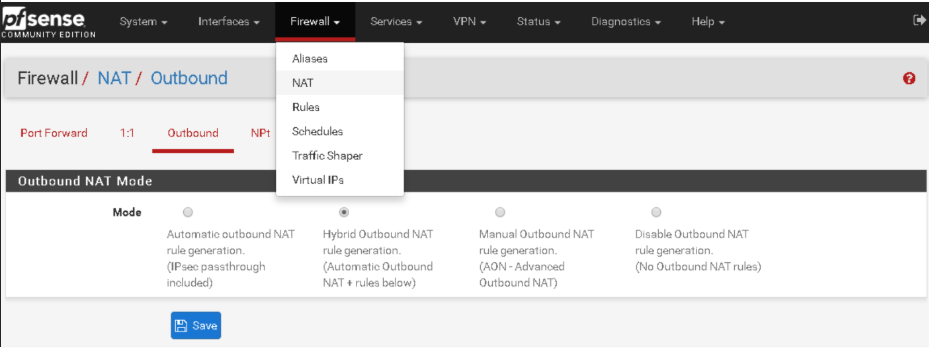
* 그리고 해당 WEB02의 <http://ip>로 접속하면 apache2 화면이 떠야함.

**4. WEB01에서 pfSense NAT 재설정**

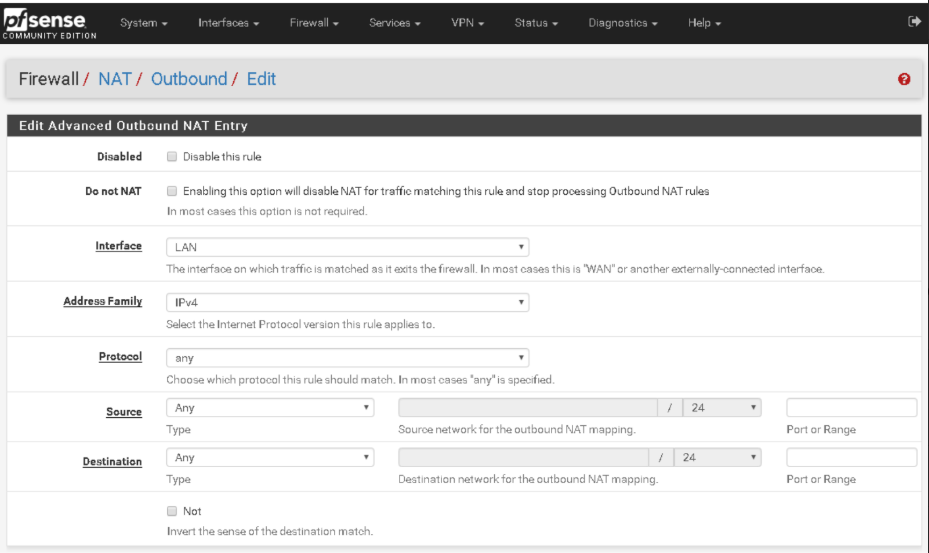
> WEB01에서 인터넷(구글)을 들어가서 pfSense의 ip를 친다. (admin/mode1752)



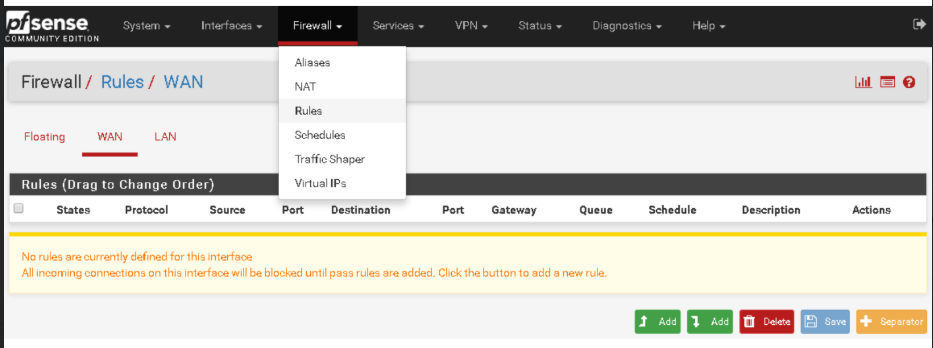
* 로그인 시 메인 화면의 모습



* Firewall > NAT > OutBound > NAT Mode를 Hybrid Outbound NAT로.



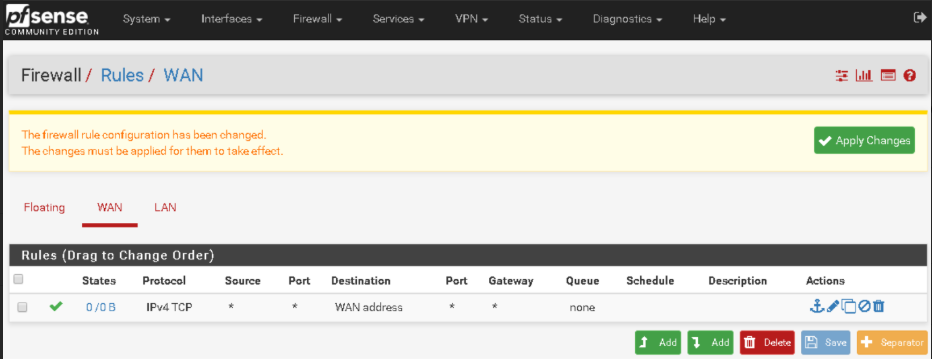
* Edit로 통신 들어올 수 있는 LAN추가해주기



* Firewall > rules > edit



* WAN으로 바깥통신 들어올 수 있는 연결통로 만들어주기

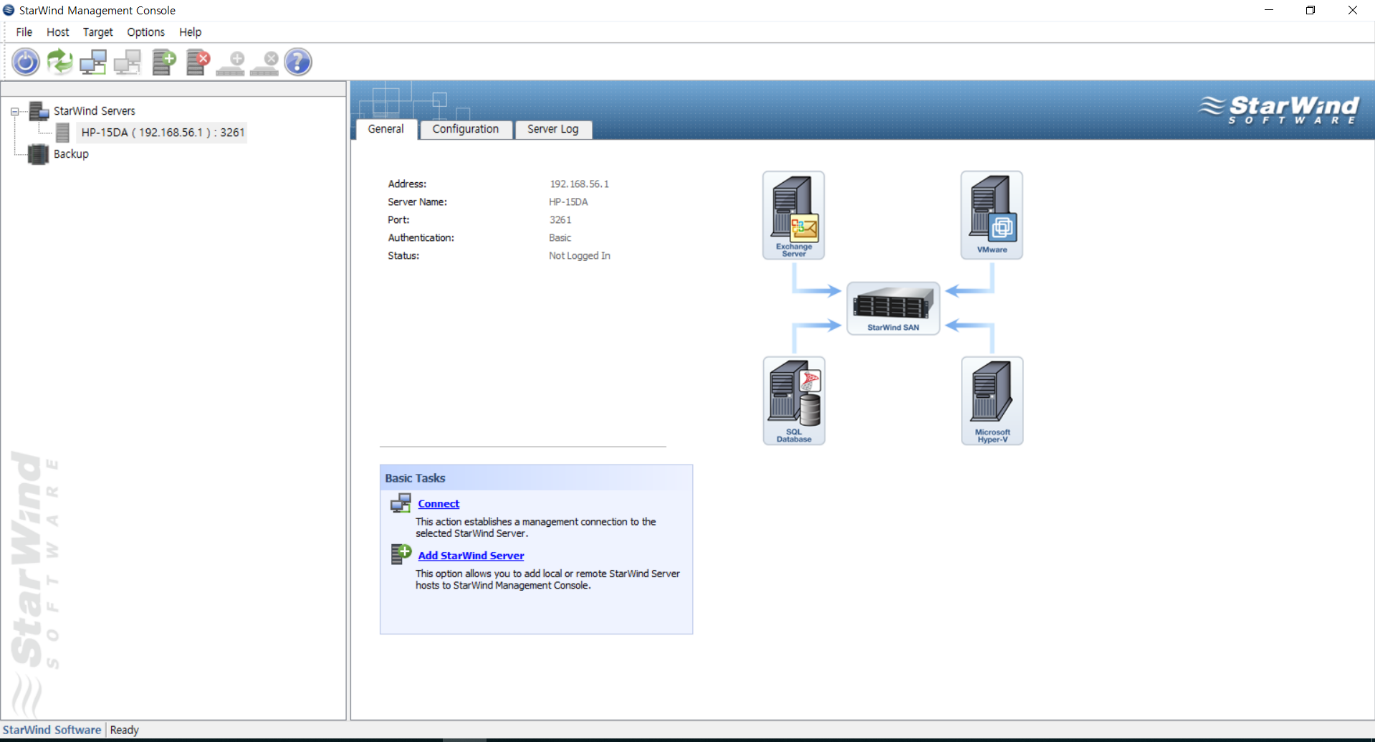


* 완성 시 , 꼭 위에 apply Changes를 눌러서 적용시켜주기

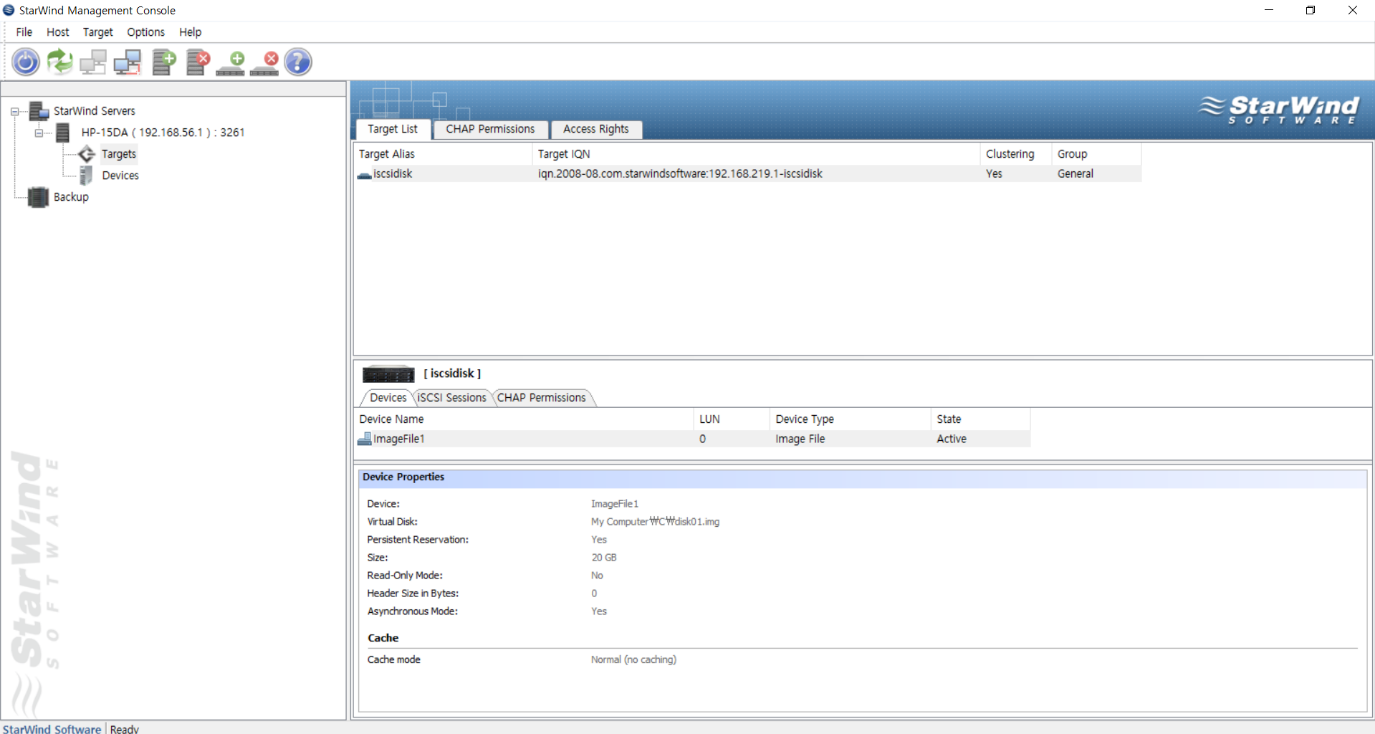
**5. iSCSI StarWind 설치 (시나리오1 실행)**

> StarWind iSCSI SAN 프로그램 설치하기

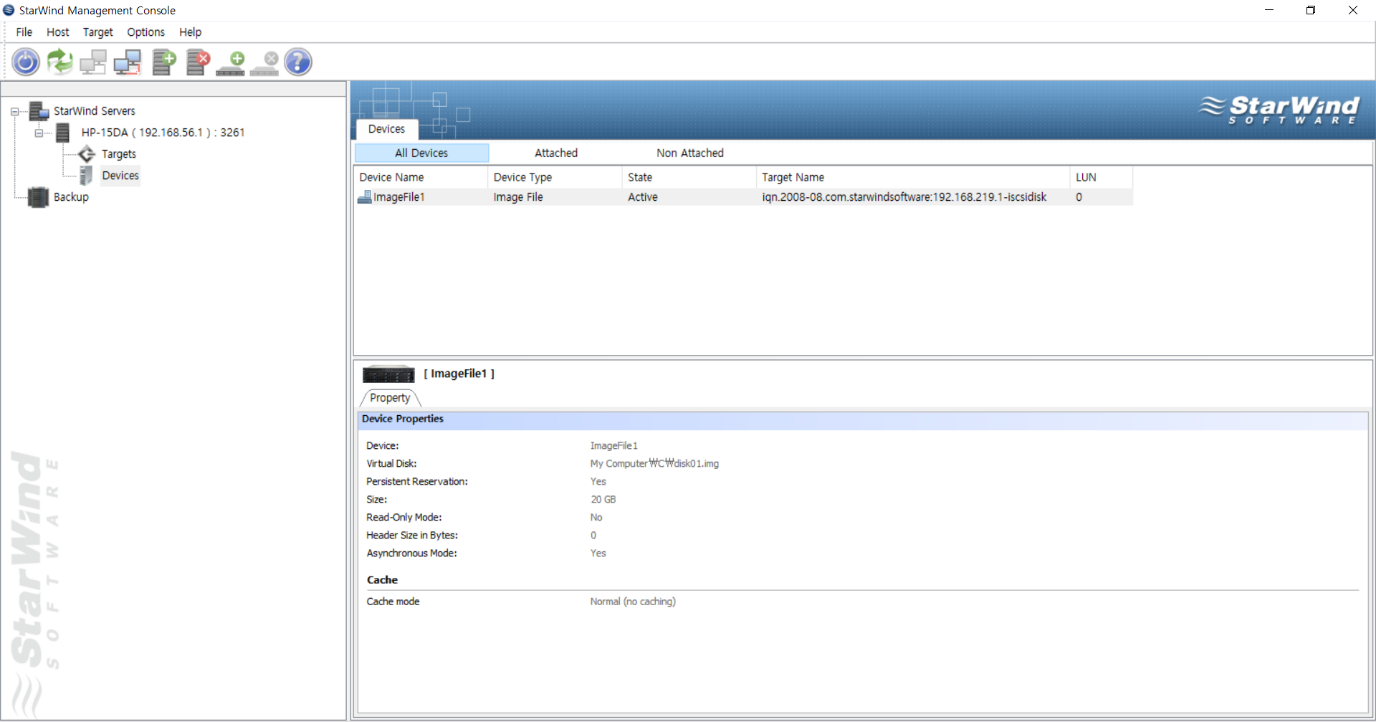
> 기존 iSCSI SERVER 호스트를 삭제하고 VMware Workstation의 NAT 네트워크에 연결될 수 있도록 호스트를 재추가해주기



* 새로 추가한 호스트는 HP-15DA (192.168.56.1) : 3261
* 이후 나오는 라이선스 키는 미리 준비해둔 키파일로 등록해두기.



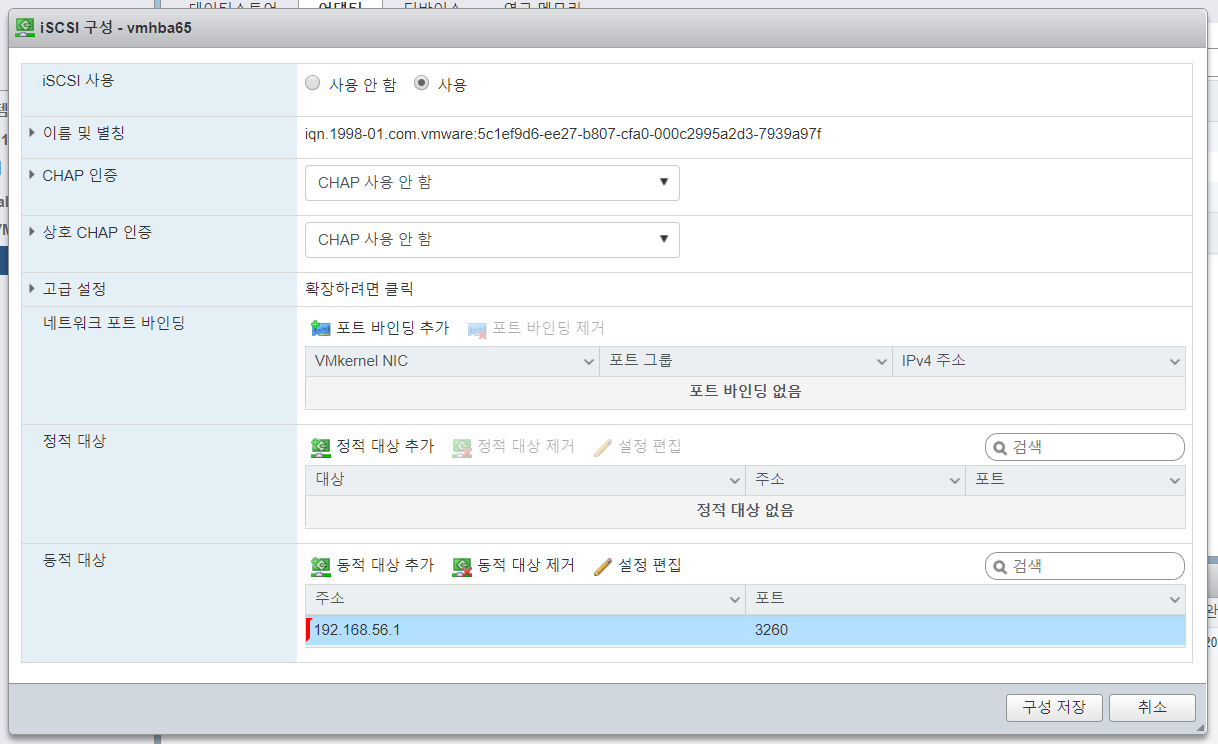
* 추가된 호스트에 target을 iscsidisk01을 만들어서 추가



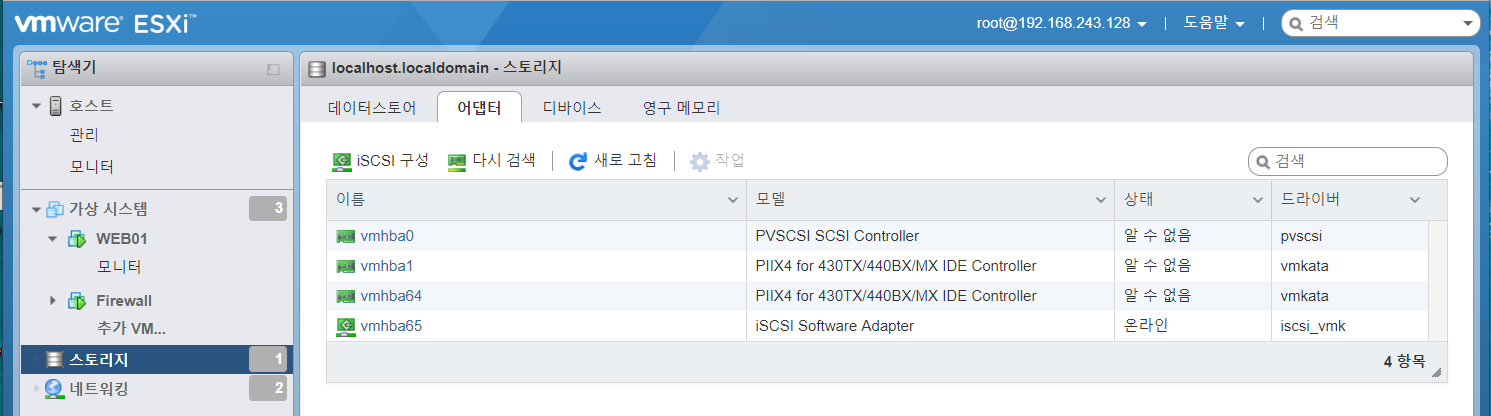
* 추가된 호스트에 새로운 imageFile01을 만들어서 test라는 디스크 서버를 만들기.
* 주의! 이 뒤에 ESXi에 iSCSI 외장 스토리지를 추가해줘야 FTP 설치 시 연동 가능!

**[ESXi에서 연동하기]**

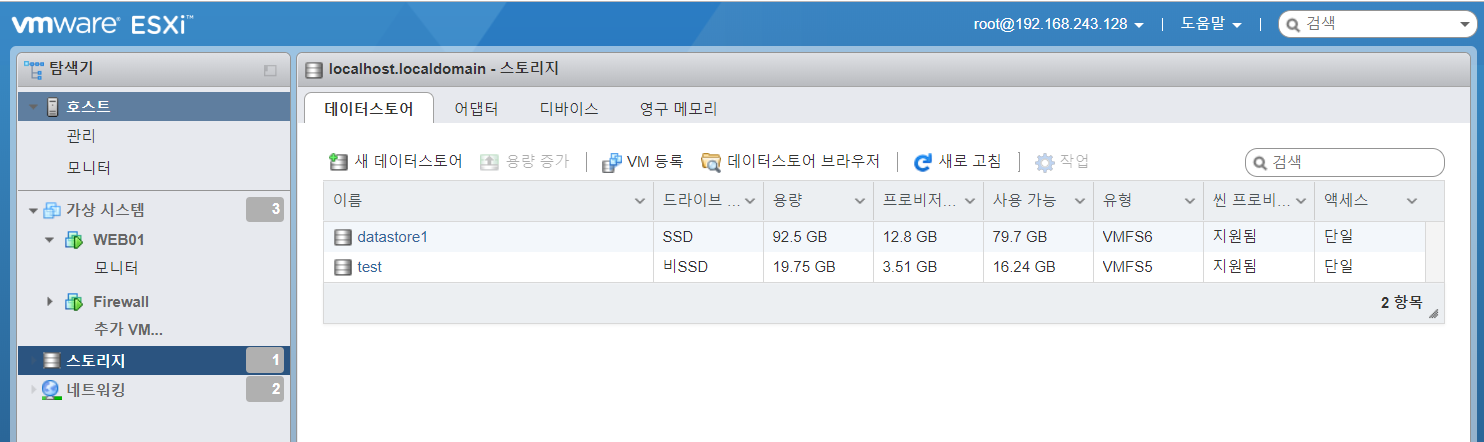
1) ESXi 환경설정을 위한 ip로 들어가서 스토리지> 어댑터> iSCSI구성



* 동적대상에 방금만든 iSCSI의 호스트ip를 넣어준다. (정적은 자동으로 만들어짐)



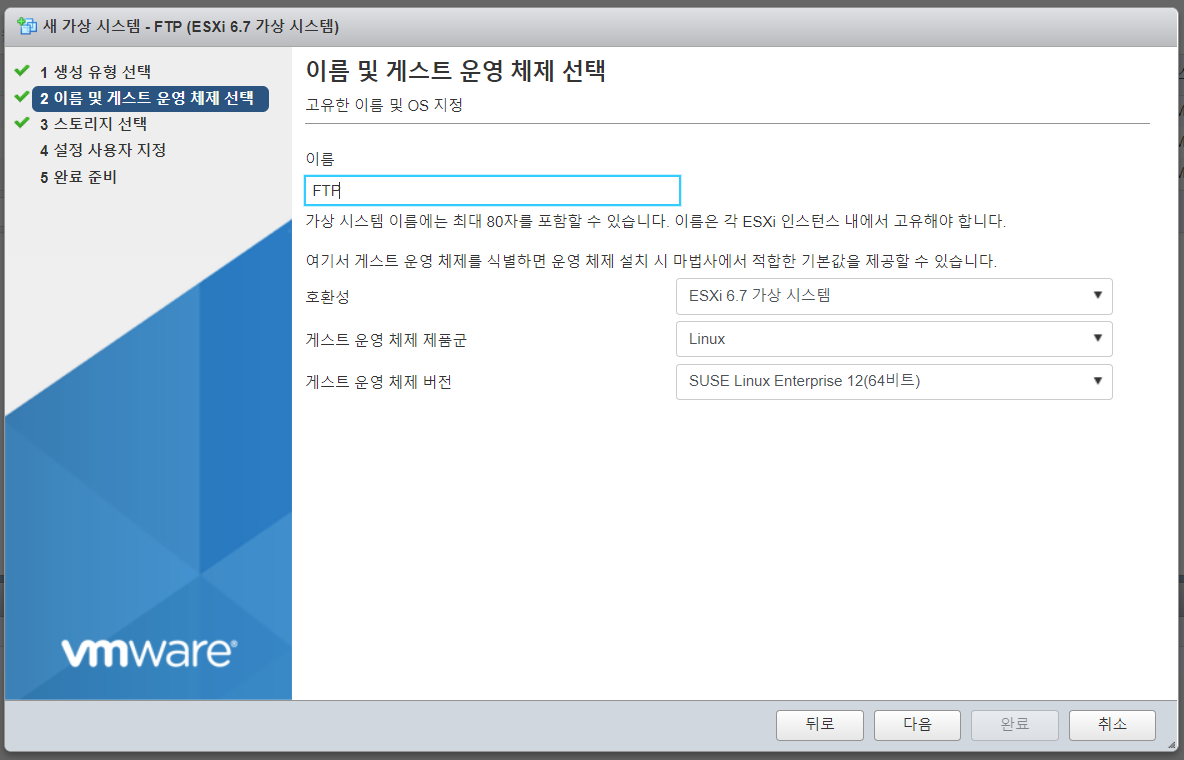
* 결과, vmhba65라는 새로운 어댑터가 추가됨(iSCSI용)



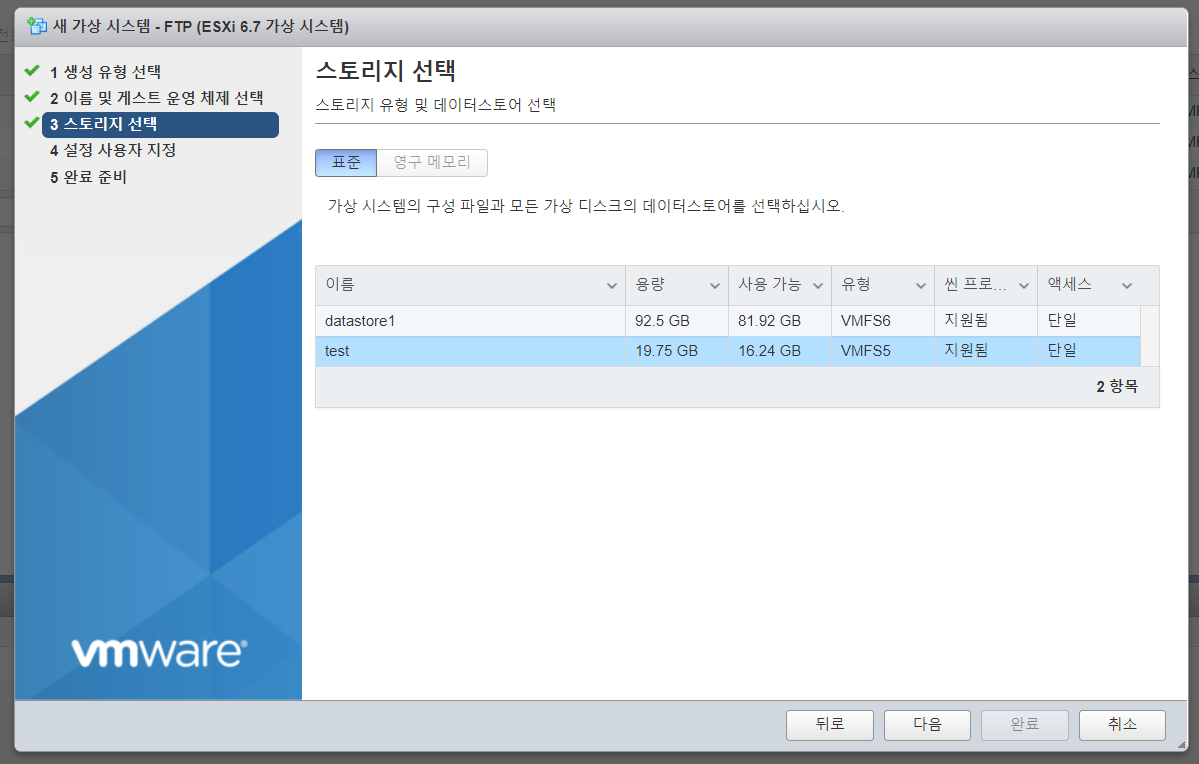
* 데이터스토어 탭으로 들어가서 확인하면 앞서 만든 test 스토리지가 포함됨.

**6. FTP OpenSUSE로 설치하기**

> 가상 시스템 > VM생성/등록

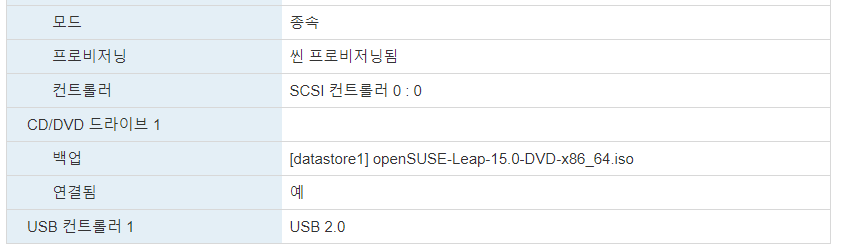


* 이름은 FTP로, openSUSE LEAP로 깔지만, openSUSE enterprise server12로 진행

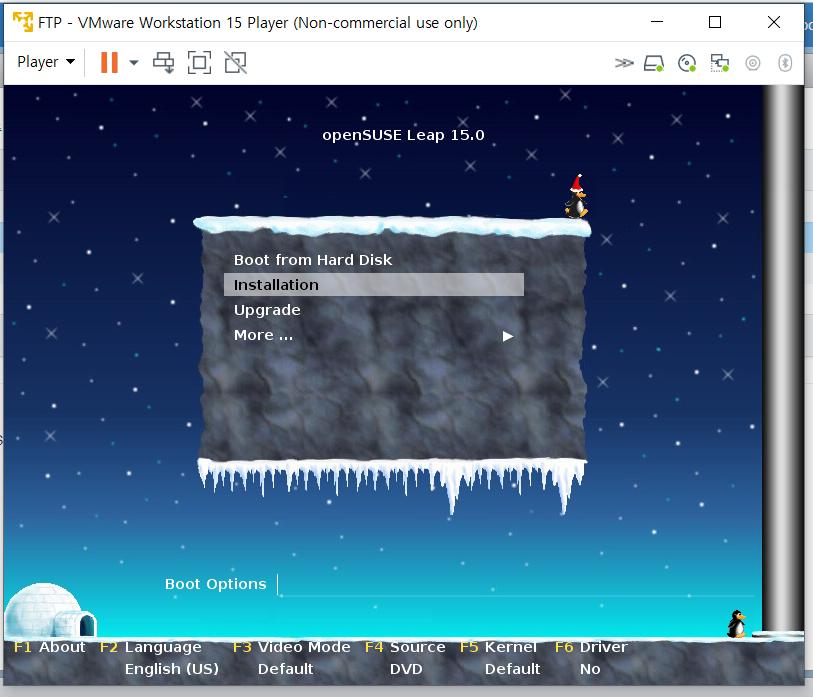


* 반드시!!! 외장 스토리지인 iSCSI 데이터스토어 이용(test)

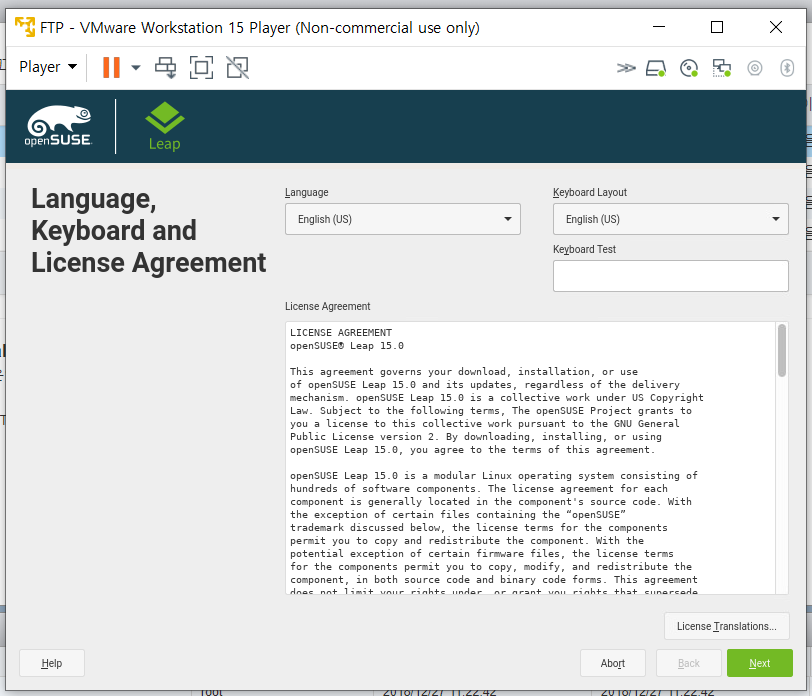




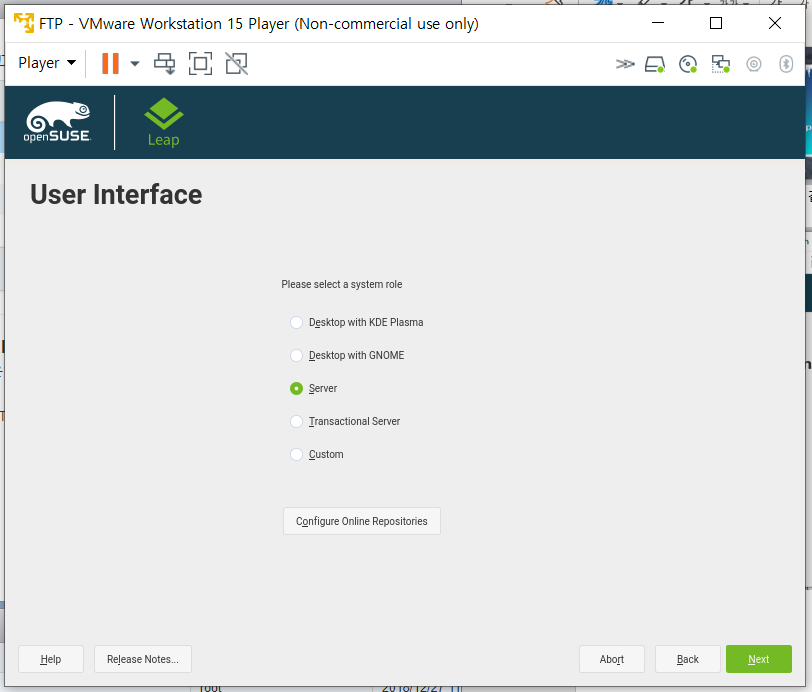
* 위와 같은 환경설정을 완료 후에 설치를 VM생성 후 전원을 켜주면 설치 시작.



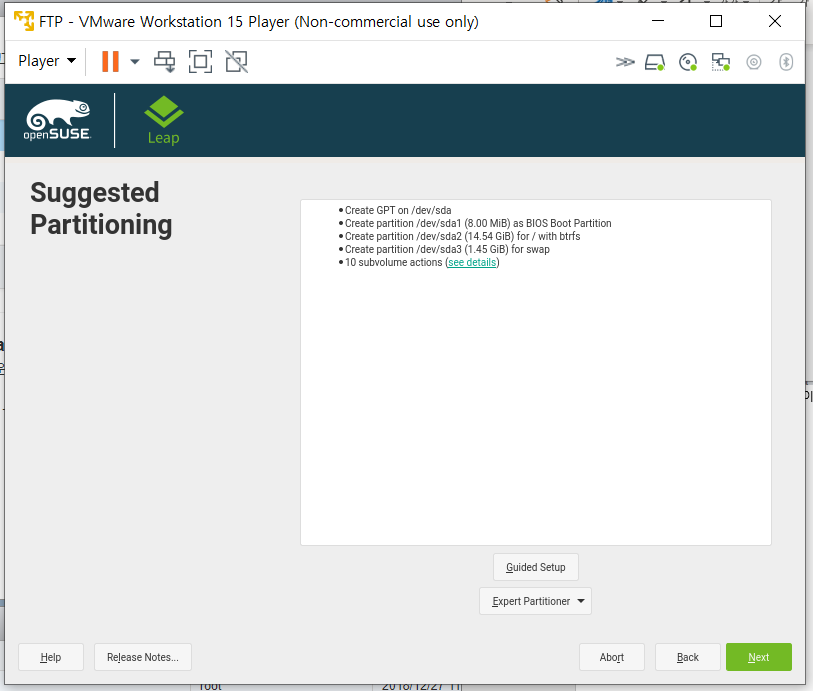
* 전원을 켜면 위와 같은 화면이 나오는데 installation을 통해 설치해준다.



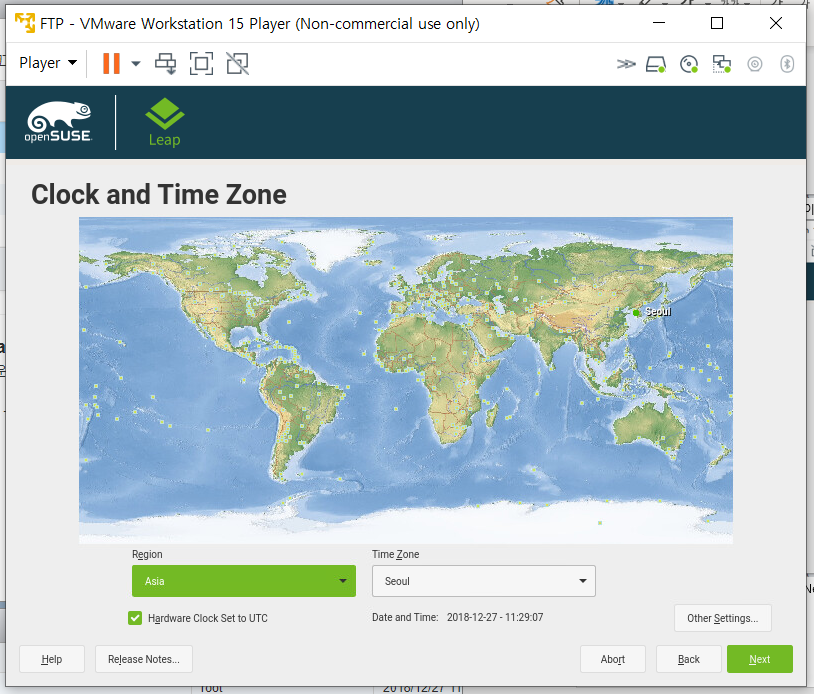
* Next를 누른다.



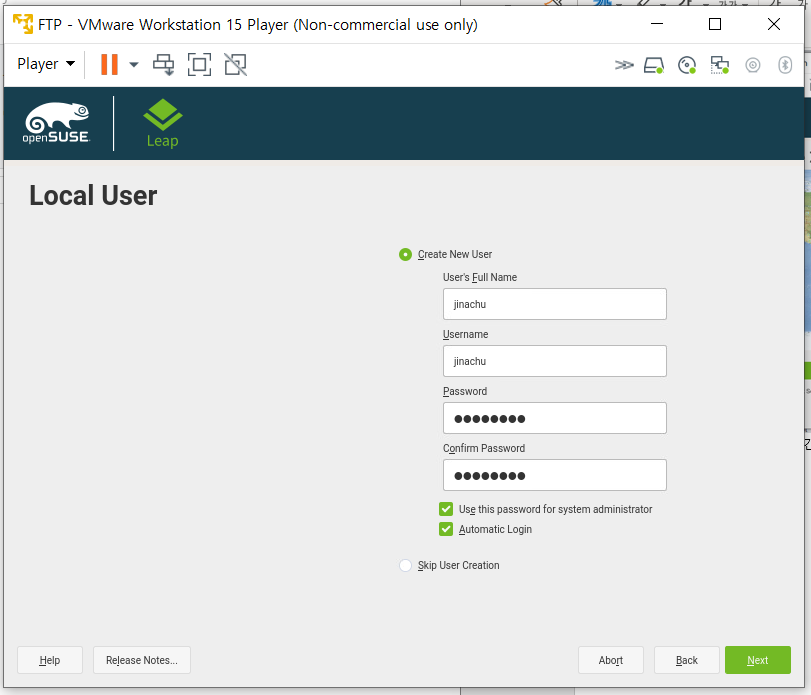
* 서버로 설치할 것이기에 Server를 선택한다.



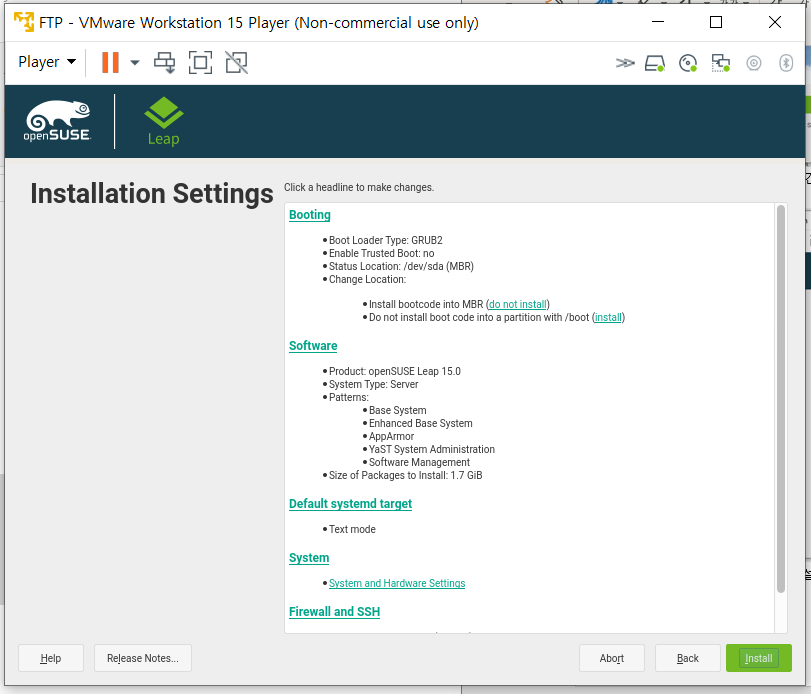
* 파티션 기본으로 Next 선택한다.



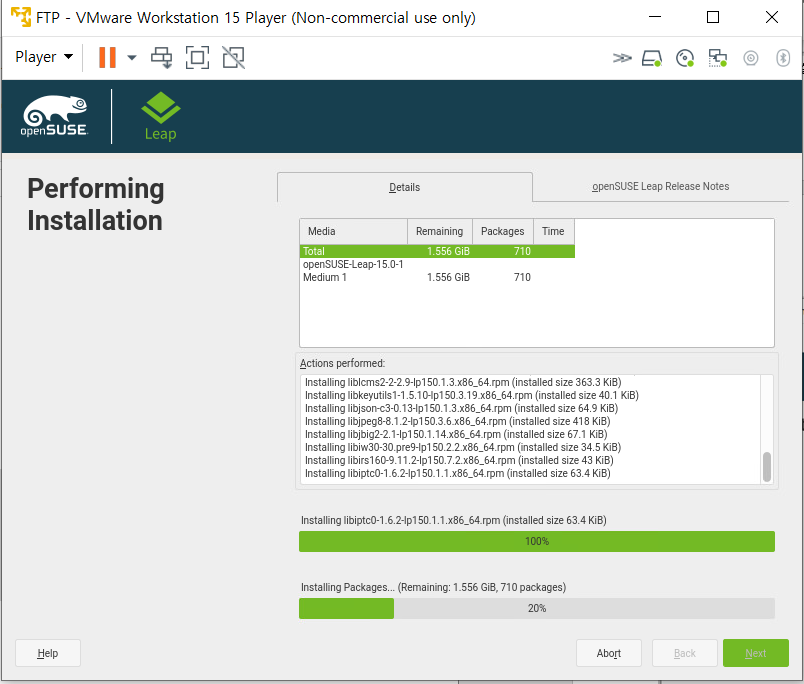
* 아시아, 서울로 시간 지역 설정해주기



* User랑 패스워드 설정 후, Next를 누른다.



* 이 뒤에 잘린 내용으로 방화벽은 켜져 있고, ssh는 사용하지 않는 상태, ssh포트도 닫혀 있는 상태이다.



* 이후 install을 누르면 바로 설치가 진행된다.

[설치 후, Console 창 설치 명령어]

--vsftpd 설치

#zypper install vsftpd -y

-- vsftpd 서비스 시작 및 등록

#systemctl start vsftpd

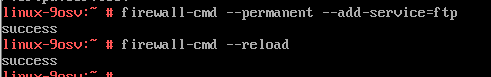
#systemctl enable vsftpd



-- 방화벽 FTP 21 포트 열기

firewall-cmd --permanent --add-service=ftp

firewall-cmd –reload

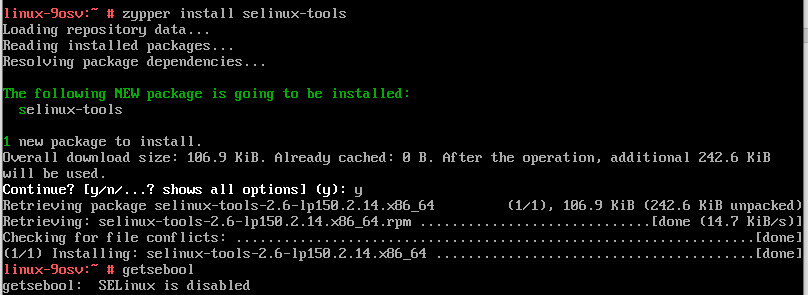


-- selinux 비활성하기

Zypper install selinux-tools

Getsebool

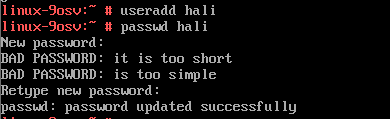
* SELINUX=disabled



-- FTP 사용자 추가 및 암호 설정

useradd hali

passwd hali



* 이 후 reboot(시스템 재시작) 해주기

-- Anonymous 비활성하기 및 패시브모드로 바꿔주기(사용자 내가 설정한 것만 사용하도록, 방화벽 뒤에 있는 FTP에 접근할 수 있도록)

#vi /etc/vsftpd/vsftpd.conf

anonymous\_enable=NO

pasv\_enable=Yes

pasv\_min\_port=30000(임의의 포트)

pasv\_max\_port=30100(임의의 포트)

#systemctl restart vsftpd

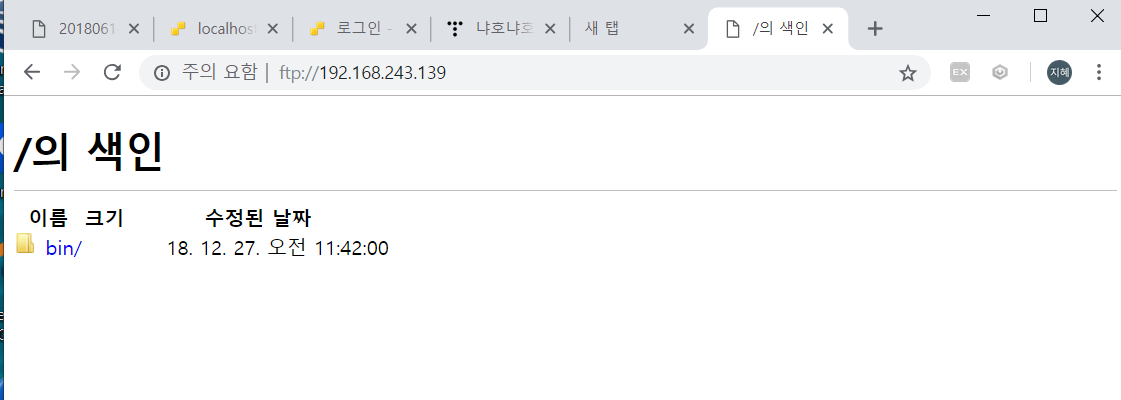
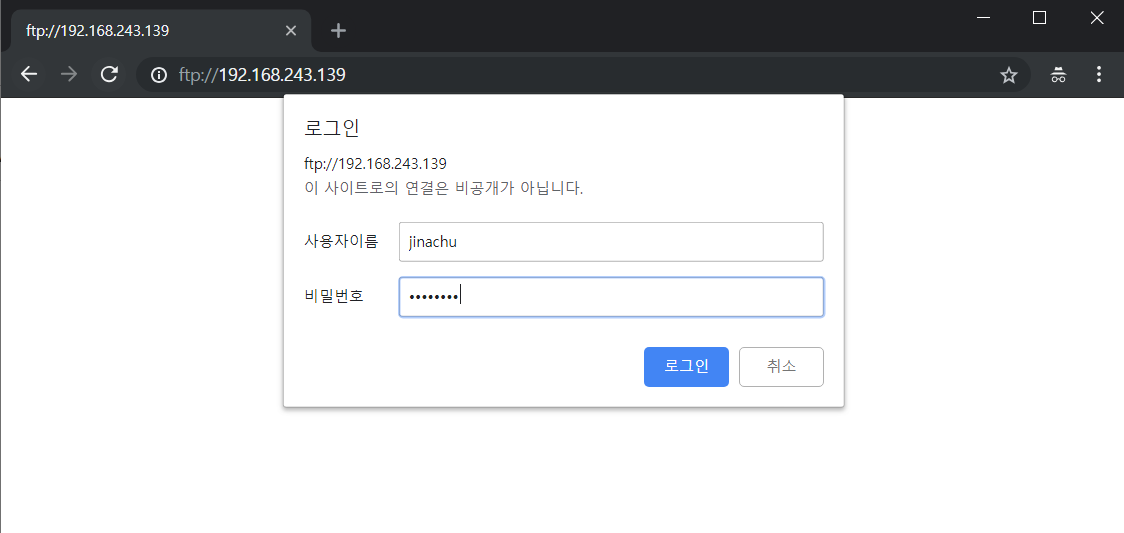
\*iptables로 할 시에는

#vi /etc/sysconfig/iptables

-A INPUT -m state –state NEW -m tcp –dport 50000 50005 -j ACCEPT

를 추가하여 위의 포트가 허용되도록 추가를 해주기.

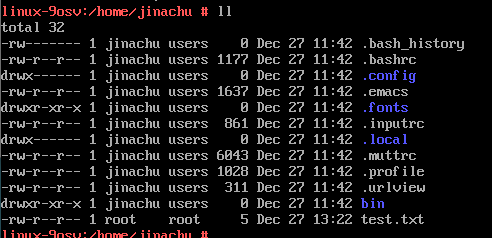
* 다 설정 후에 밖의 host PC의 웹에서 해당 ftp ip로 접속되는지 확인하자.



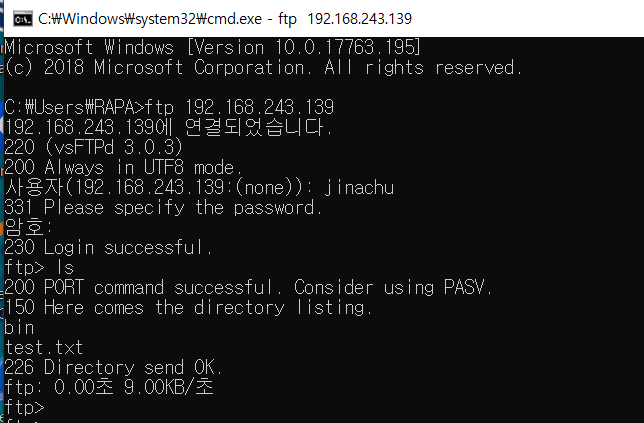
* 맨 처음 suse의 아이디/pw로 로그인한다.

[WEB01 console 창에서 들어갈 시]

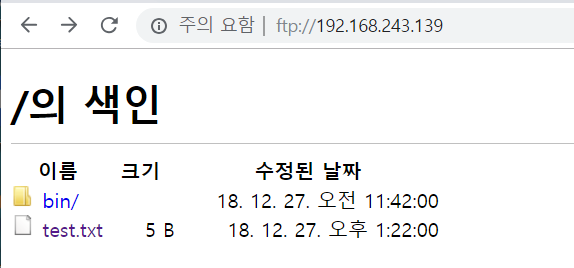
1) 먼저 ftp console에서 jinachu의 홈디렉토리로 들어가, 시험용 다운로드 파일 test.txt를 만든다.



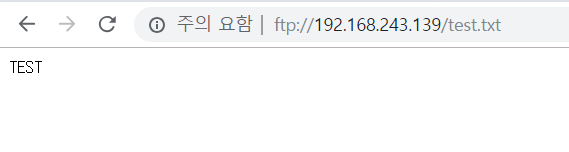
2) HostPC cmd에서 ftp 접속하여 파일이 있는지 확인한다.



3) HostPC의 웹으로 들어가서 파일이 생겼는지 확인한다.

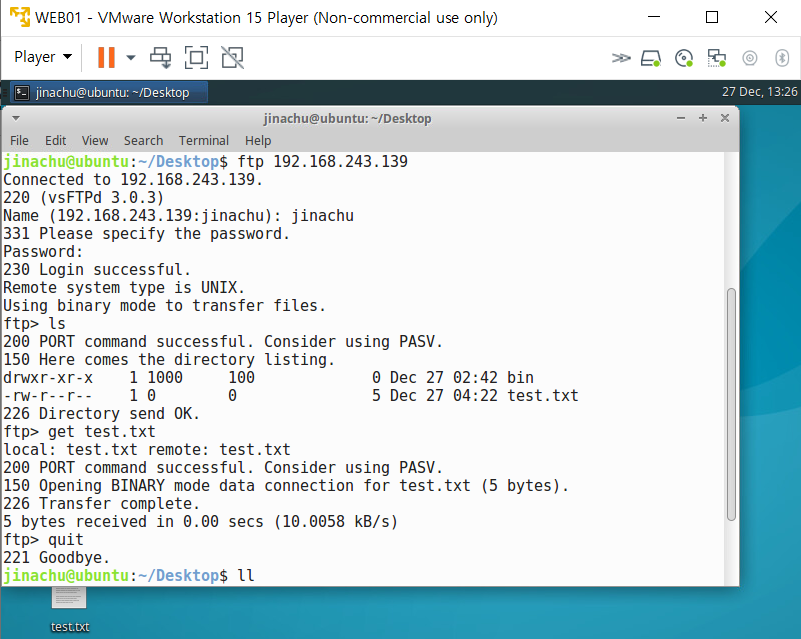


* 새로 생긴 test.txt 파일이 보인다.



* Test.txt로 들어가면 그 내용을 볼 수 있다.

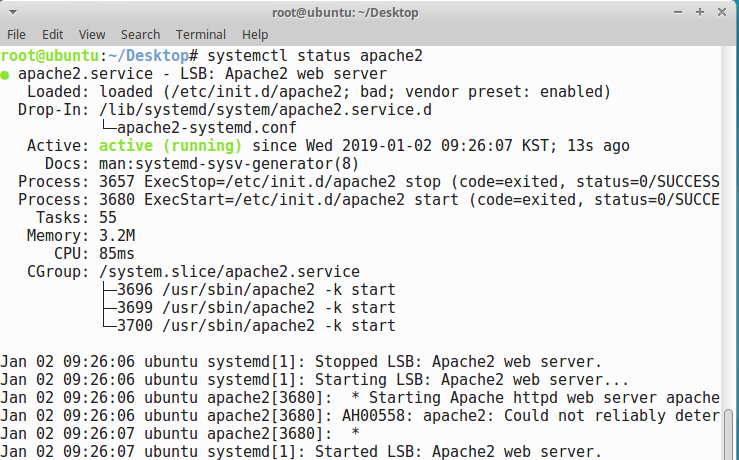
4) web01의 console에서도 접속 및 다운 가능한지 확인한다.

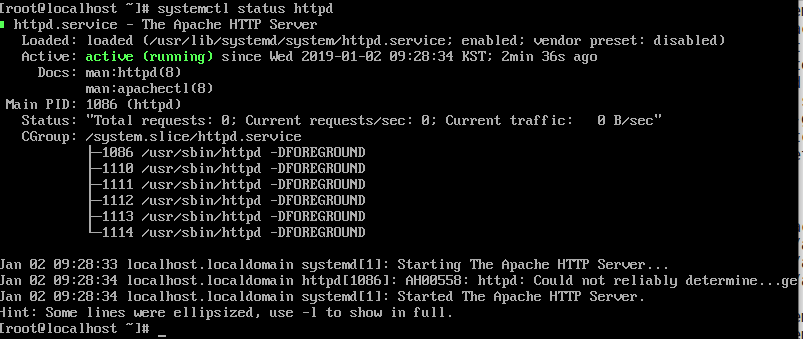


* 접속 가능 및 get 명령어로 다운로드도 가능하다.

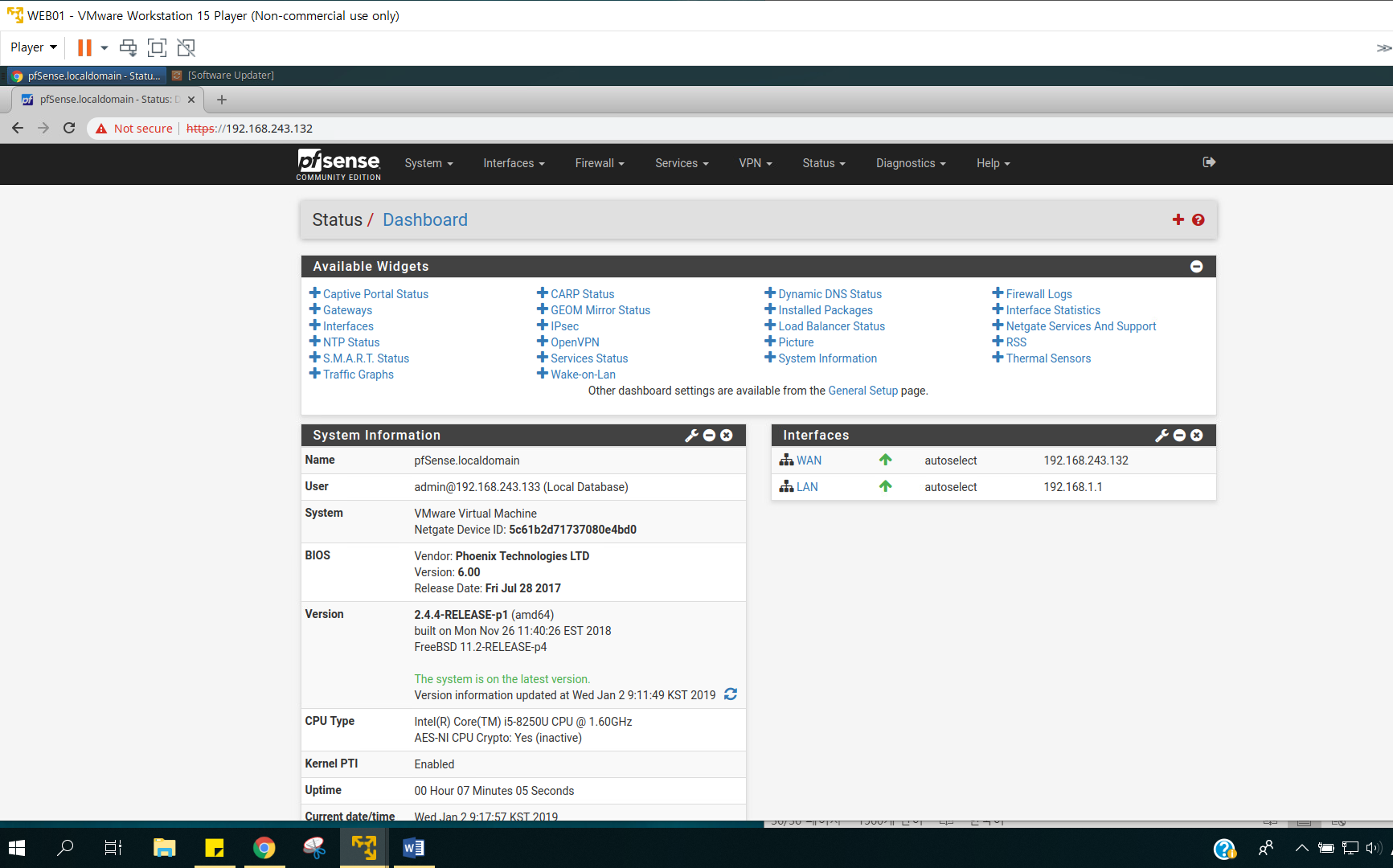
**7. Haproxy 설치해서 WEB01과 WEB02 로드밸런싱하기**

> 미리 web01과 web02에 apache2 서버를 설치해둔다.

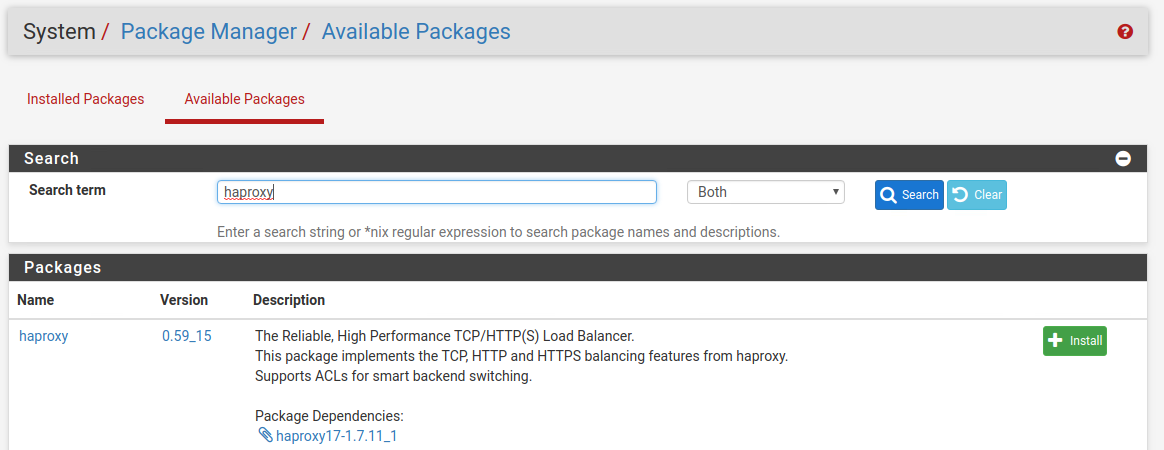




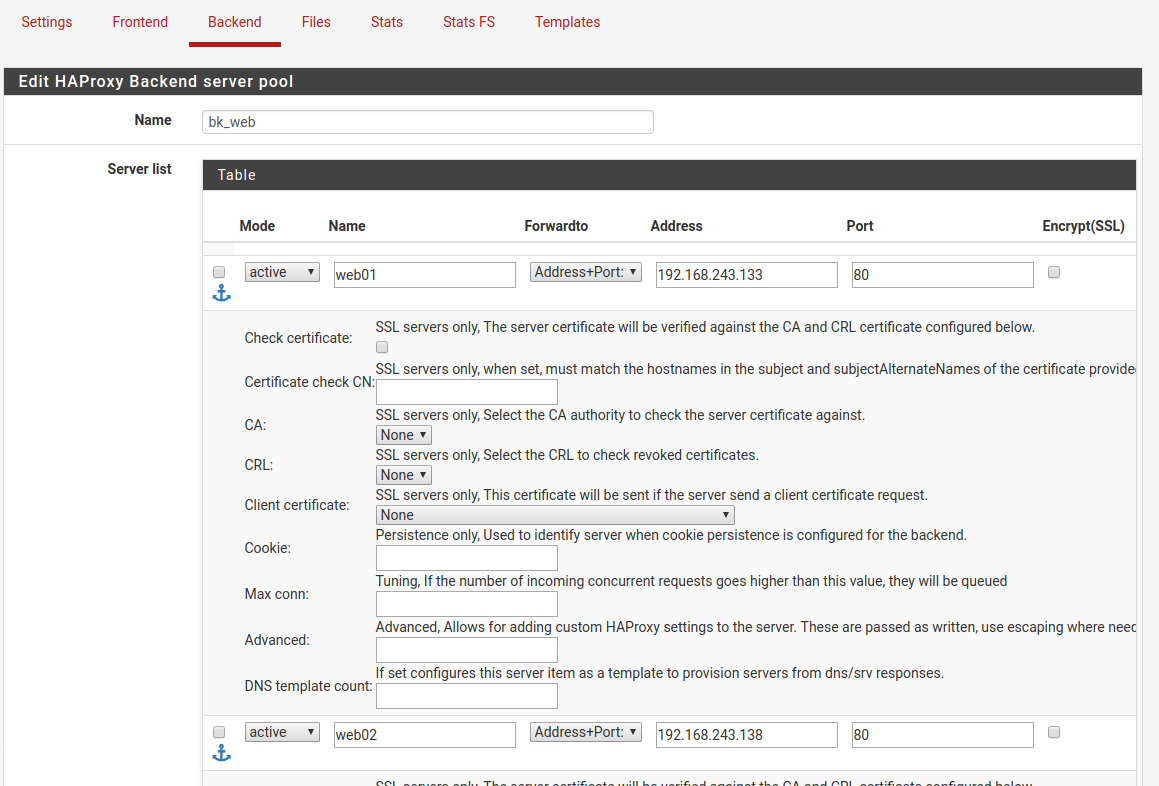
* web01에 들어가서 pfsense management ip(192.168.243.132)로 접속하기



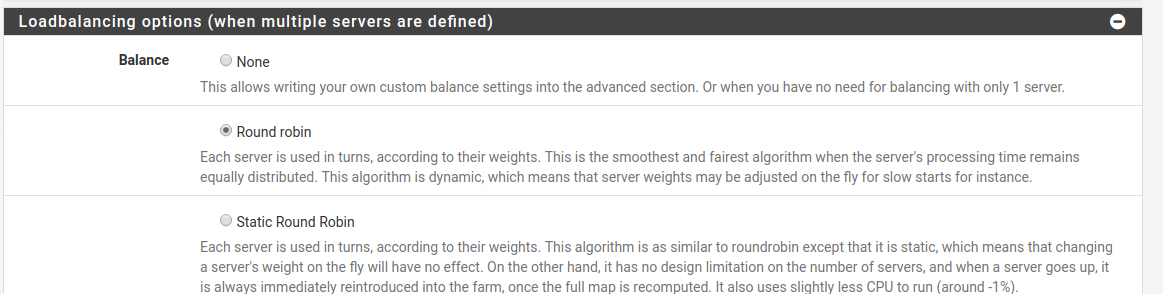
* System > package manager > available packages 에서 HAproxy 설치



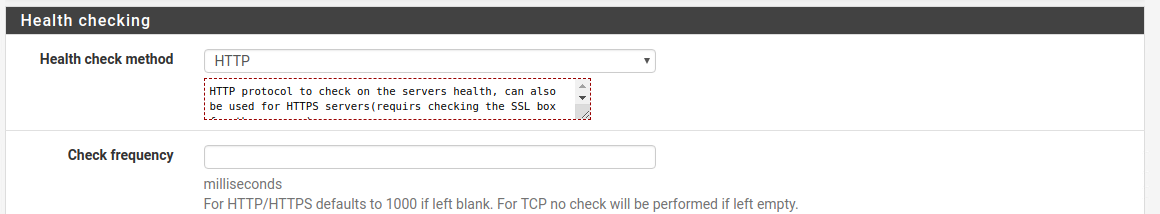
* 설치 후에 Services > HAProxy > Backend > edit 로 간다. (backend 추가하기)



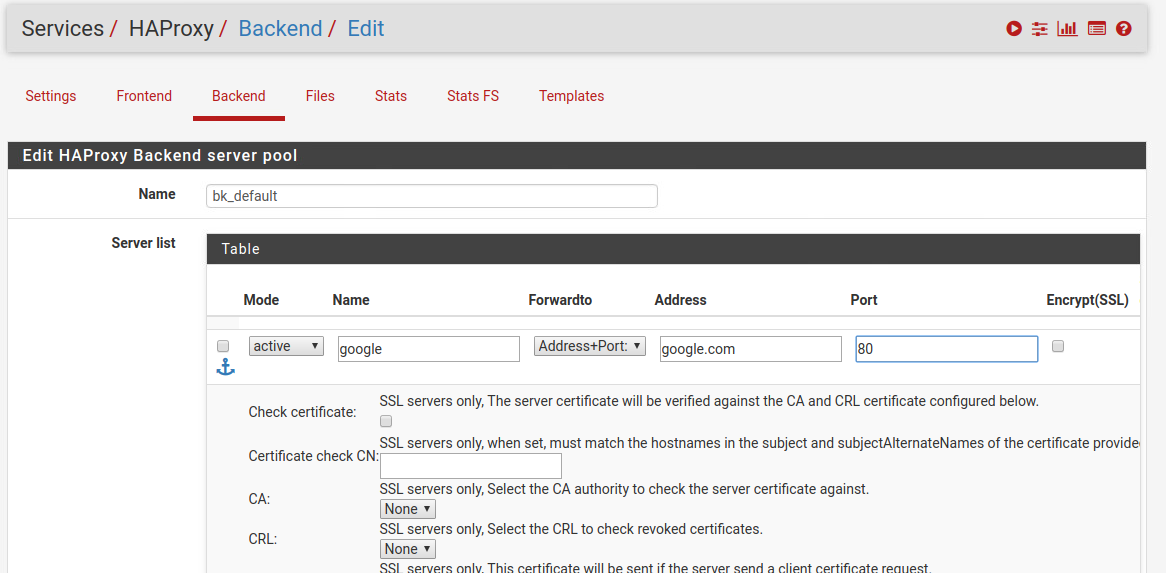
* 백엔드에 서버리스트를 web01, web02로 지정해준다.



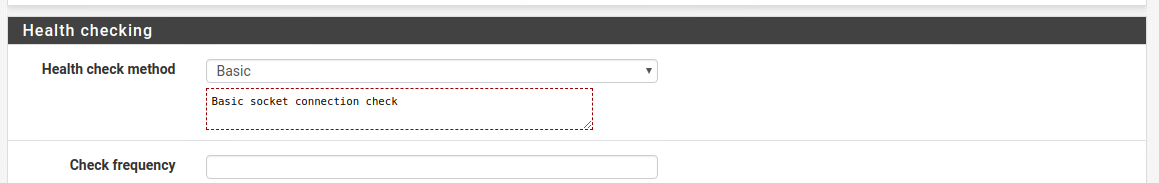
* Round Robin으로 Loadbalancing options을 지정해준다.



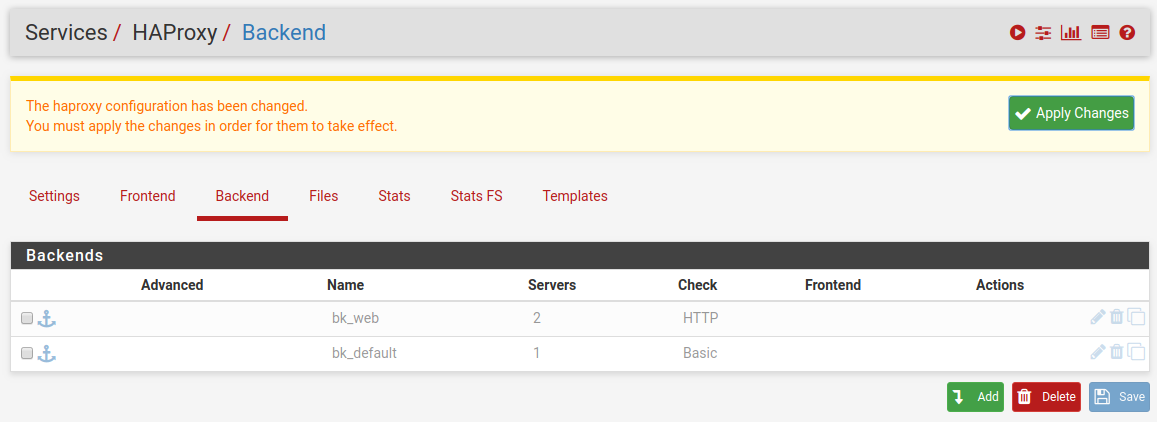
* Health Checking은 http로 설정해준다.



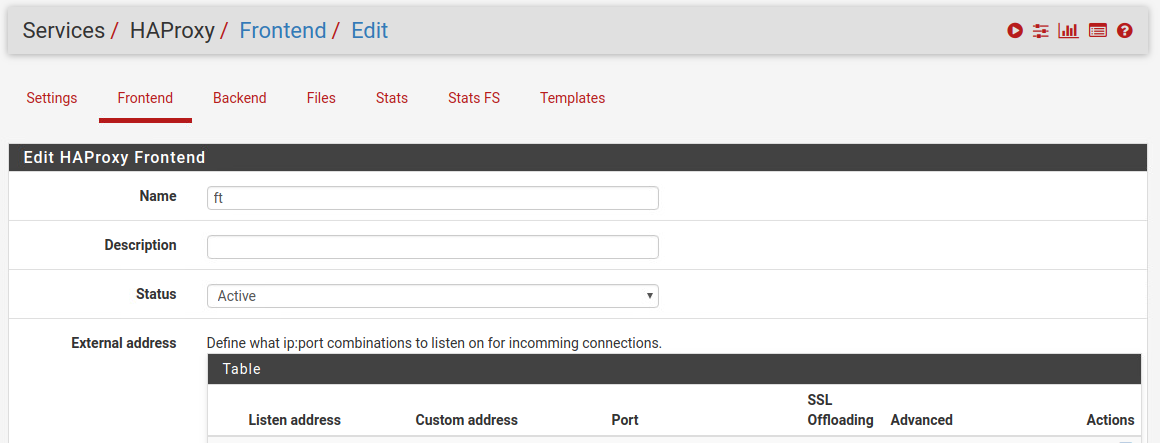
* 위에 세팅해둔 것처럼 google.com으로 연결시켜준다(원래는 AWS EC2연결 – test 용이를 위해 google.com으로 바꿈.)



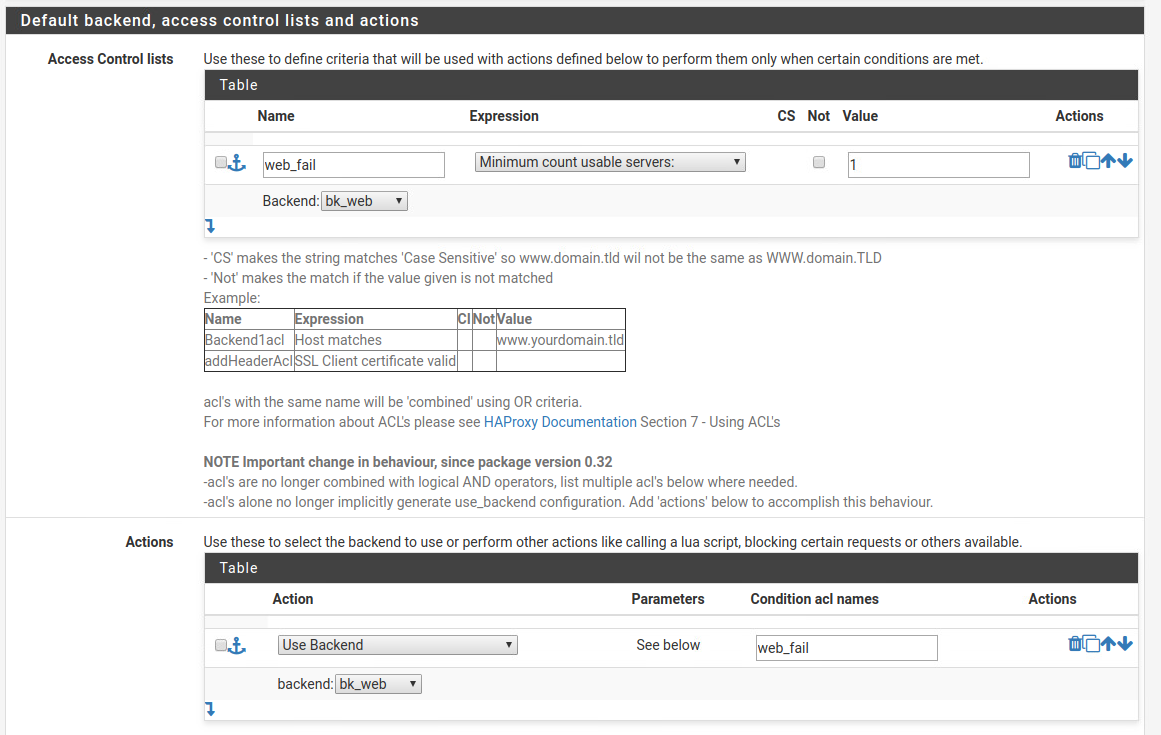
* 단, 여기서는 google.com에서 들어오는 것이기에 http가 아닌 basic으로 지정해준다. (꼭 http에서 들어온다는 보장이 없다. 에러방지)



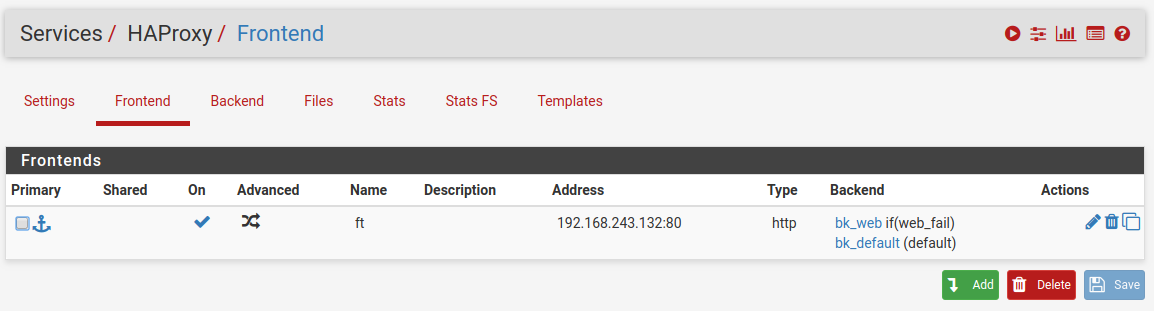
* Apply changes 꼭 해주기, 그 다음에 frontend로 간다.



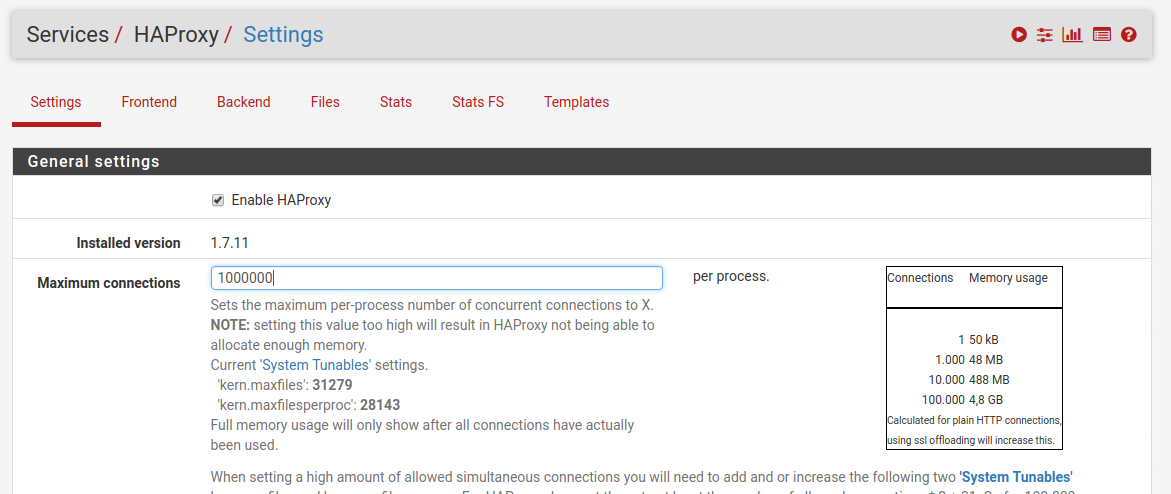
* Ft로 이름 설정



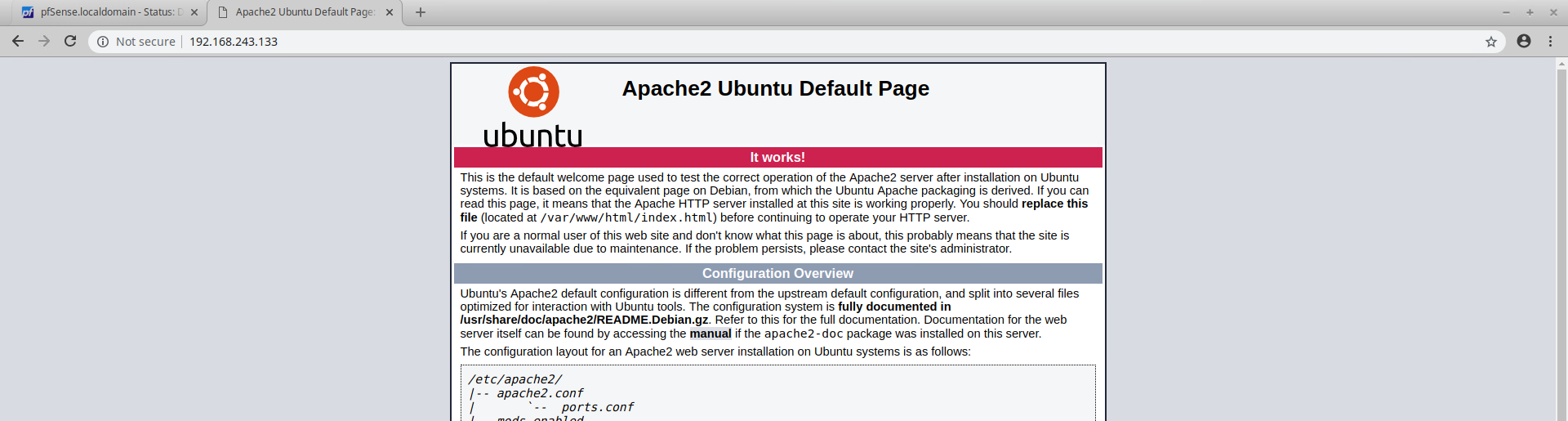
* Web loadbalancing하는 backend들 연결해주기(acl작성)
* 만약 해당 연결된 web들 중 살아있는 것이 1개이하일 경우, bk\_web의 로드밸런싱이 작동하도록! 만약 두 web이 실패할 때 bk\_default인 google.com으로 연결되도록.



* 다 만든 후의 결과. 이제 시험해보도록하자.



* 그 전에 꼭 HAproxy를 enable로 만들어준다. (사용을 해야 위에 규칙들 확인가능) 그리고 maximum connections는 임의로 지정해주기



* 192.168.243.133으로 들어가면 확인가능.