

26. 방화벽 관리

ufw

- 우분투는 자체적으로 방화벽을 관리하는 도구인 ufw를 제공한다.

방화벽 동작 확인

방화벽 서비스의 이름은 ufw

```
[root@itserver ~]# dpkg -l | grep ufw
```

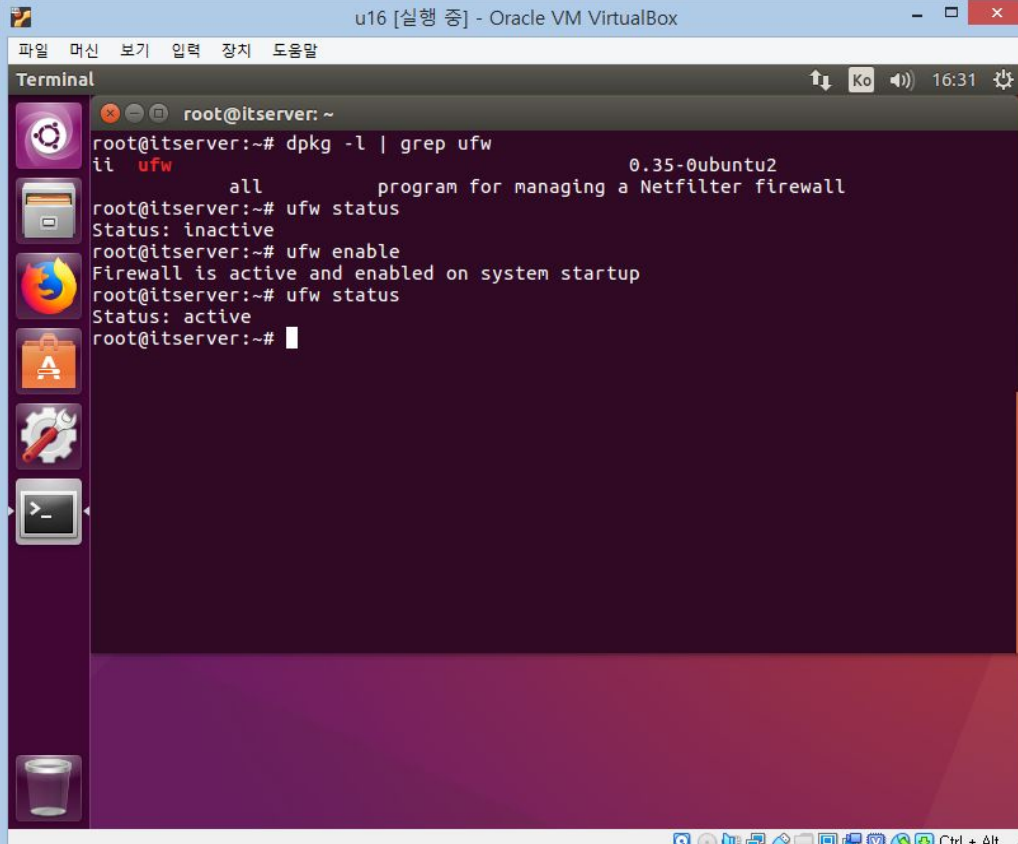
- 방화벽 서비스 설치 여부 확인

방화벽 서비스 동작상태

```
[root@itserver ~]# ufw status
```

방화벽 서비스 활성화/비활성화

```
[root@itserver ~]# ufw {enable | disable}
```



The screenshot shows a terminal window titled "u16 [실행 중] - Oracle VM VirtualBox". The terminal output is as follows:

```
root@itserver: ~  
root@itserver:~# dpkg -l | grep ufw  
ii  ufw          0.35-0ubuntu2  
      all          program for managing a Netfilter firewall  
root@itserver:~# ufw status  
Status: inactive  
root@itserver:~# ufw enable  
Firewall is active and enabled on system startup  
root@itserver:~# ufw status  
Status: active  
root@itserver:~#
```

- ufw 방화벽은 동적으로 방화벽을 관리할 수 있도록 지원한다. 언제든지 방화벽의 설정을 변경할 수 있고, 즉시 적용된다는 의미이다.

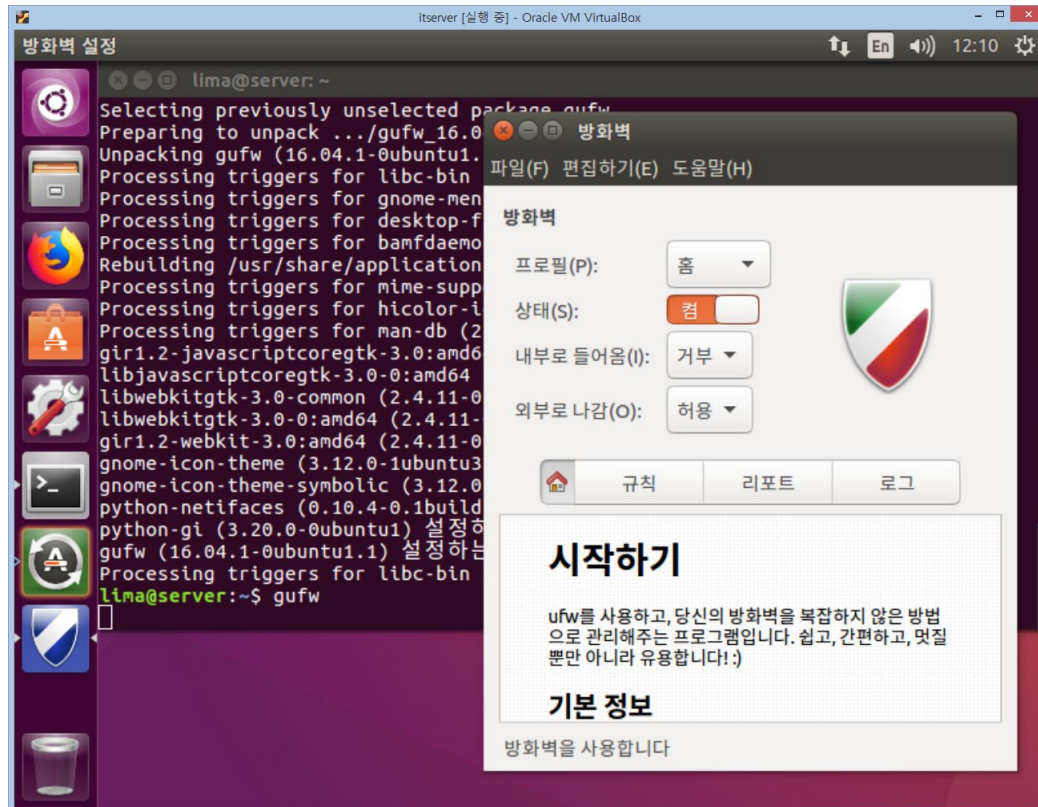
- 방화벽의 변경 내용을 실행하기 위해 별도로 변경 내용을 저장하고 적용하는 과정이 필요없다.

GUI 도구로 방화벽 설정

- 우분투에는 방화벽을 관리하기 위한 GUI 도구로 **gufw**가 있는데 기본적으로 설치되어 있지 않으므로 따로 설치해야 한다.

[root@itserver ~]# apt-get install gufw

gufw 동작 화면



Profile

- 현재 설정하는 내용을 적용할 환경을 설정한다.
- 설정할 수 있는 값은 Home, Office, Public 등 3가지이며 각 환경에 따라 방화벽을 다르게 설정할 수 있다.

Status

- 방화벽 전체를 켜거나 끌 수 있다.

Incoming과 Outgoing

- 시스템으로 들어오는 트래픽과 시스템에서 밖으로 나가는 트래픽을 어떻게 할 것인지 기본값을 설정한다.
- 일반적으로 시스템으로 들어오는 트래픽은 모두 거부하고(deny) 밖으로 나가는 트래픽은 허용하는(allow) 것이 기본값이다.
- 허용과 거부 외에 거절(reject)과 제한(limit)이 있다.
 - 거절은 접속을 거부하고(reject) 거절된 이유를 알려준다.

- 제한은 같은 IP에서 반복적으로 접속을 시도할 때 트래픽이 거부되는 경우이다.

규칙

- 방화벽에서 규칙을 선택하면 현재 적용 중인 규칙을 보여준다.
- 여기서 +를 선택하여 규칙을 추가하거나, -를 선택하여 규칙을 삭제할 수 있다.
- 규칙을 추가하는 3가지 방법
 - 편리하게 모드
 - 방화벽을 적용할 응용분야를 게임, 오디오/비디오, 시스템, 오피스 등으로 구분하고 다시 카테고리를 정해 방화벽 정책을 정할 수 있도록 했다.
 - 간단하게 모드
 - 규칙의 이름을 사용자가 정할 수 있으며, TCP/UDP 선택과 포트 번호나 서비스명을 사용자가 직접 지정하고 정책을 적용할 수 있다.
 - 자세하게 모드
 - 규칙의 이름, 번호, 정책, 방향, 인터페이스 선택, 로그 기록 여부, TCP/UDP 선택뿐만 아니라 출발지와 목적지의 주소, 포트 번호 등을 자세하게 설정할 수 있다.

방화벽 규칙을 추가합니다

편리하게 | 간단하게 | 자세하게

정책: 허용

방향: 내부

카테고리: 모든

하위 카테고리: 모든

프로그램: 0 A.D.

프로그램 필터

닫기(C) | 추가(A)

리포트(열린 포트 보고)

- 현재 열려 있는 포트를 보고한다.
- 프로토콜과 포트 번호, 사용하는 프로그램을 요약해서 보여준다.

로그

- 방화벽과 관련된 로그기록을 보여준다.



방화벽 관리 명령

- 방화벽은 명령으로도 관리할 수 있다.
- ufw 명령으로 방화벽을 켜거나 끌 수 있고, 특정 포트나 서비스를 허용하거나 거부할 수 있다.
- **ufw**

기능	방화벽을 설정한다.
형식	ufw 서브명령
서브 명령	enable:방화벽 활성화 disable: 방화벽 비활성화 default allow deny reject [incoming outgoing]: 방화벽 기본동작 설정 status [verbose]: 방화벽 상태 출력 allow 서비스명 포트/프로토콜: 지정한 서비스나 포트 허용 deny 서비스명 포트/프로토콜: 지정한 서비스나 포트 거부 delete 명령: 명령으로 설정한 규칙을 삭제
사용 예	ufw deny telnet ufw allow 23/tcp ufw status

방화벽 상태 보기

- **ufw status**

규칙 추가

- **ufw allow http**
 - http 서비스 허용

서비스 거부

- **ufw deny telnet**
 - Telnet 서비스 거부

규칙 삭제

- **ufw delete deny telnet**
 - Telnet 서비스 설정 삭제

포트 추가

- 포트를 추가할 때는 tcp나 udp 프로토콜을 지정해야 한다.
- **ufw allow 5000/tcp**
 - 임의로 5000번 포트를 추가

특정 IP 주소의 접속 설정

- **ufw allow from 192.168.18.10 to any port ftp**
 - 192.168.18.10에서 요청하는 ftp 서비스를 허용