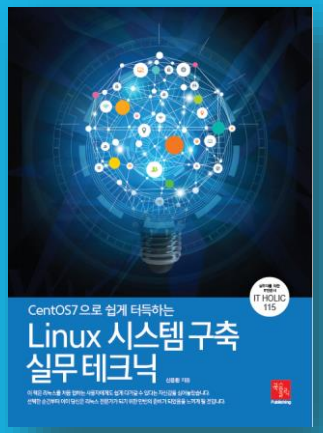
CHAPTER 15

리눅스 방화벽 관리



Section 01 | 정보보안 입문

Section 02 | 방화벽 관리

SECTION 01

정보보안 입문

- 정보보안에 대해 이해하기익히기

1. 리눅스 시스템에서 취약한 보안유형에 대해 살펴봅니다.
2. 취약한 보안유형에 따른 대처방안을 제시합니다.

리눅스 시스템에서 취약한 보안유형

오픈형 소스는 라이선스 등의 규제로부터 제약받지 않는다는 장점이 있는 반면 응용 프로그램의 모든 소스가 공개되어 있기 때문에 보안에 취약할 수밖에 없습니다. 리눅스에서의 보안 위협의 유형을 살펴보면 비 인가된 물리적 접근, 계정 도용, 파일시스템의 비밀성 및 무결성 침해, 비 인가된 네트워크의 접근 등을 들 수 있습니다. 이와 같이 취약한 보안유형에 대해 관리자는 적절히 대응해야 하지만 쉽지 않은 것이 현실입니다. 그렇지만 어느 정도 취약한 보안에 대처할 수 있는 방안을 충분히 검토하여 대응전략을 수립하는 것이 현명한 처사입니다.

취약한 보안유형 대처방안

주기적인 시스템 점검

시스템은 언제 어떠한 상황으로 인해 정상적으로 구동되지 않을 위험에 노출되어 있습니다. 그렇기 때문에 주기적으로 시스템을 점검할 수 있도록 대응방안을 수립해야 합니다. 가장 바람직한 자세는 매월 또는 매주 특정한 주기를 정해놓고 시스템을 점검하는 습관을 길러야 합니다. 그리고 보안 관리를 위한 시스템과 네트워크 점검 등의 솔루션을 적극 활용하는 방법도 권장합니다.

소프트웨어 최신버전 유지관리

현재 사용 중인 리눅스 시스템은 배포판이므로 현재 버전에서 발생할 수 있는 결함들을 수렴하여 출시되는 새로운 버전을 신속히 설치해야 합니다. 소프트웨어 패치버전은 가장 최신버전으로 유지관리해 주는 것이 바람직한 보안관리 대처방안이기도 합니다.

불필요한 서비스 통제

리눅스 시스템은 동시에 여러 사람이 네트워크를 통해 사용되고 있는 시스템으로 언제든지 보안에 노출되어 있습니다. 그렇기 때문에 불필요한 서비스에 대한 통제가 필요합니다. 이와 같이 불필요한 서비스를 통제하기 위해서는 불필요한 서비스 자체를 제거하거나 방화벽에서 패킷을 필터링하는 방법 등을 사용하는 것이 좋습니다.

정기적인 백업관리

주기적인 시스템 점검과 소프트웨어 패치 및 불필요한 서비스를 통제한다고 해도 시스템 자체는 예기치 못한 상황과 문제가 발생할 소지는 다분히 존재합니다. 그렇기 때문에 정기적으로 시스템의 주요 환경설정과 소프트웨어 및 사용자 데이터 등은 백업하는 습관을 갖는 것이 바람직한 자세입니다.

물리적 보안요소 점검

컴퓨터 열쇠, CMOS 암호, Boot loader 암호, xlock, vlock 등 물리적으로 보안에 취약한 요소를 점검하여 대응전략을 수립해야 합니다. linux single 부팅 시 root 권한을 획득할 수도 있기 때문에 물리적으로 취약한 보안요소에 대한 주기적인 점검이 반드시 필요합니다.

관리자의 보안의식 고취

무엇보다 중요한 것은 시스템 관리자가 갖고 있는 보안의식에 대한 고취입니다. 해커들의 해킹능력은 나날이 진보되어 향상된 실력을 과시하고 있는 것이 지금의 현실입니다. 이와 같은 현실에서 시스템 관리자의 보안관련 전문지식 또한 향상되어야 합니다. 그래야만 새로운 해킹방법에 대한 대응전략과 보안관리 지침 등을 수립하여 추진함으로써 보안 위협 요인으로부터 어느 정도 대비할 수 있습니다.

SECTION 02

방화벽 관리

- 리눅스 시스템 방화벽 관리 이해하기

1. gedit 사용방법에 대해서 이해합니다.
2. 에디터를 사용하여 파일을 편집하는 실습을 진행합니다.

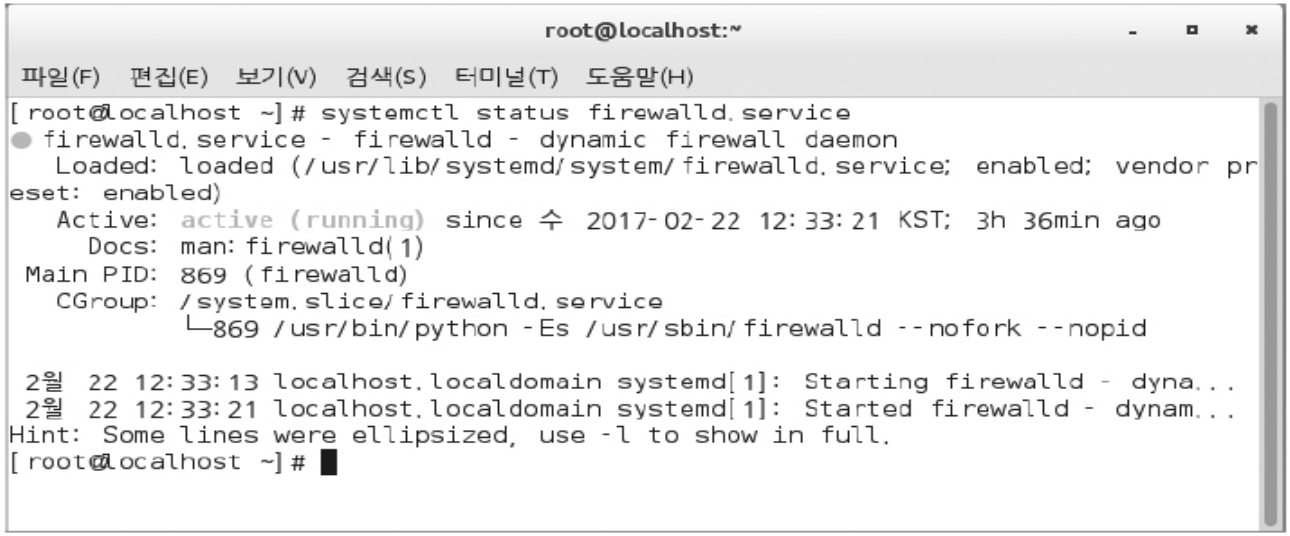
방화벽 동작 확인

방화벽과 관련된 서비스를 제공하는 firewalld.service로 현재 방화벽의 동작 상태를 먼저 확인합니다. 만일 방화벽이 설치되어 있지 않을 경우에는 설치하고 설치되어 있지만 동작하고 있지 않다면 방화벽을 동작시켜야 합니다. 다음 예제를 통해 자세히 살펴보도록 하겠습니다.

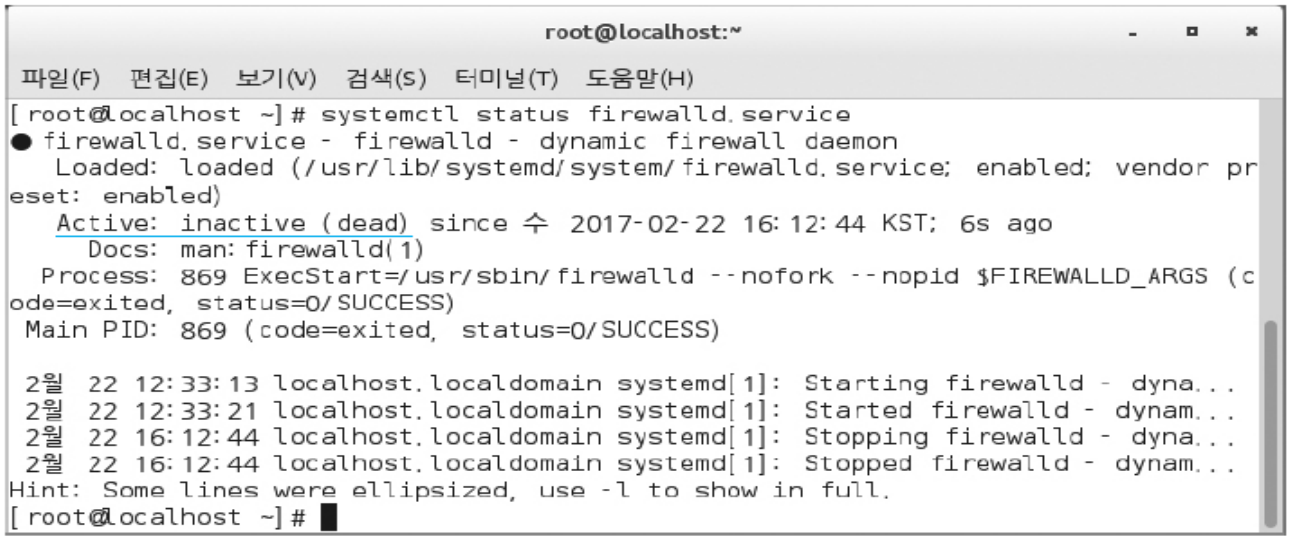
예제 15-1

- **Step 01** | 터미널 창에서 방화벽이 동작 중인지를 확인하기 위해 다음과 같이 명령을 수행합니다. Active: inactive(dead)와 같이 나타나면 방화벽이 동작하고 있지 않은 상태이고 Active: inactive(rinning)과 같이 나타나면 방화벽이 정상적으로 동작하고 있음을 의미합니다.

```
# systemctl status firewalld.service
```



(a) 방화벽이 정상적으로 동작 중인 상태

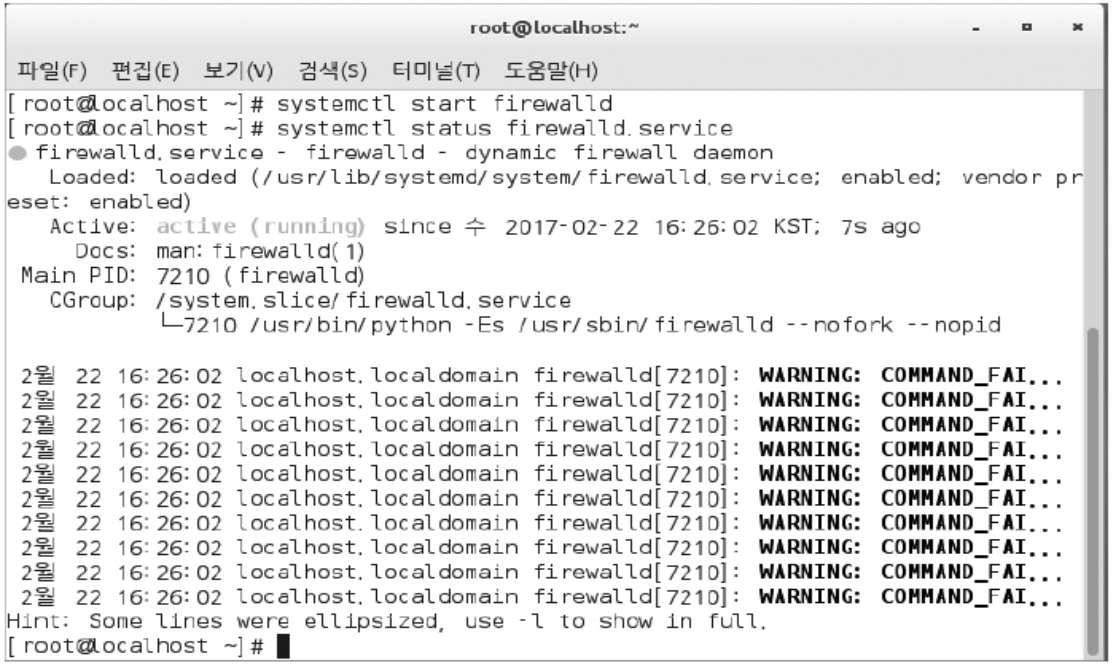


(b) 방화벽이 동작하고 있지 않은 상태

Section 02 방화벽 관리

- **Step 02** | 만약 [그림 15-1]의 (b)와 같이 방화벽 동작상태가 Active: inactive(dead)와 같이 나타났다면 방화벽을 동작시키기 위해 다음과 같이 명령을 수행합니다.

```
# systemctl start firewalld
# systemctl status firewalld.service
```



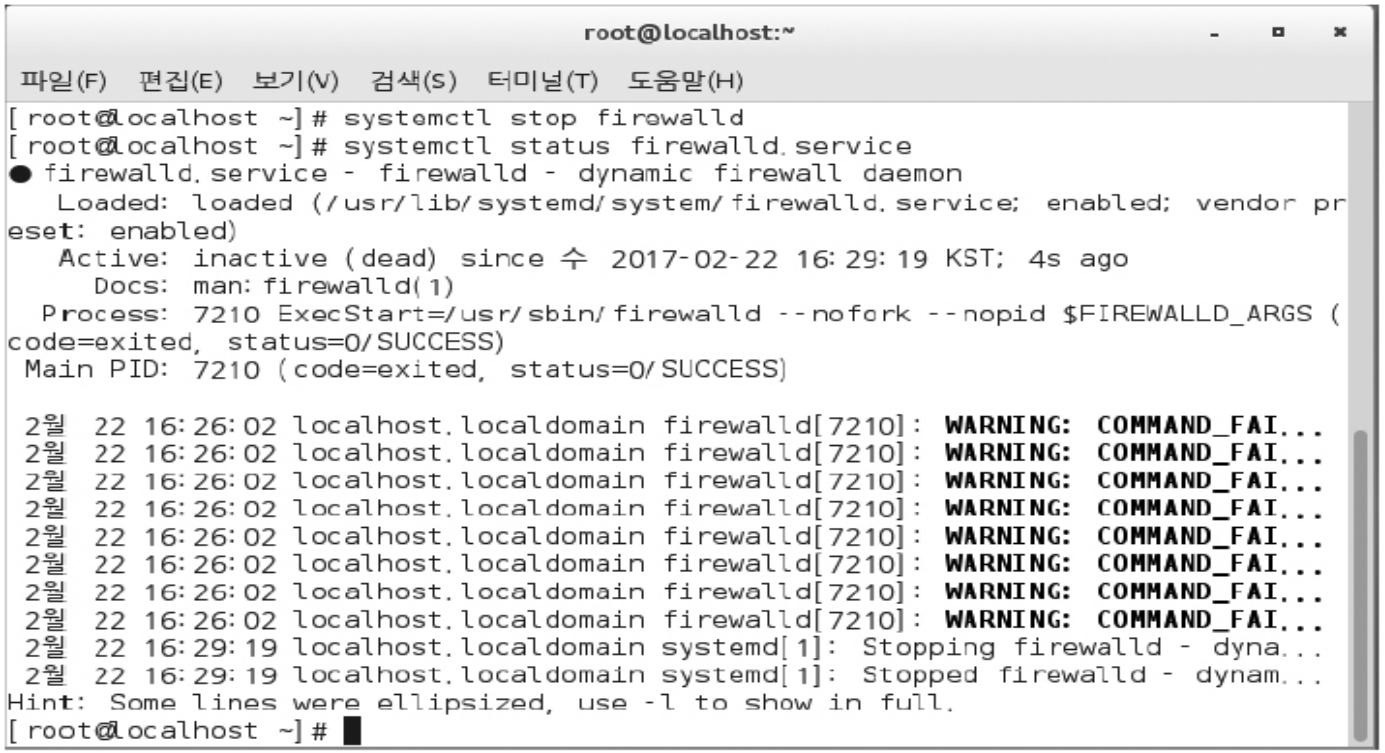
```
[root@localhost ~]# systemctl start firewalld
[root@localhost ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor pr
eset: enabled)
   Active: active (running) since 수 2017-02-22 16:26:02 KST; 7s ago
     Docs: man:firewalld(1)
 Main PID: 7210 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─7210 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost ~]# █
```

[그림 15-2] 방화벽 동작 시작과 동작 상태 확인

- **Step 03** | 동작 중인 방화벽을 강제로 종료하려면 다음과 같이 명령을 수행합니다.

```
# systemctl stop firewalld
# systemctl status firewalld.service
# systemctl start firewalld
```



```
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor pr
eset: enabled)
   Active: inactive (dead) since 수 2017-02-22 16:29:19 KST; 4s ago
     Docs: man:firewalld(1)
  Process: 7210 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (
code=exited, status=0/SUCCESS)
 Main PID: 7210 (code=exited, status=0/SUCCESS)

 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:26:02 localhost.localdomain firewalld[7210]: WARNING: COMMAND_FAI...
 2월 22 16:29:19 localhost.localdomain systemd[1]: Stopping firewalld - dyna...
 2월 22 16:29:19 localhost.localdomain systemd[1]: Stopped firewalld - dynam...
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost ~]#
```

[그림 15-3] 방화벽 강제 종료와 동작 상태 확인

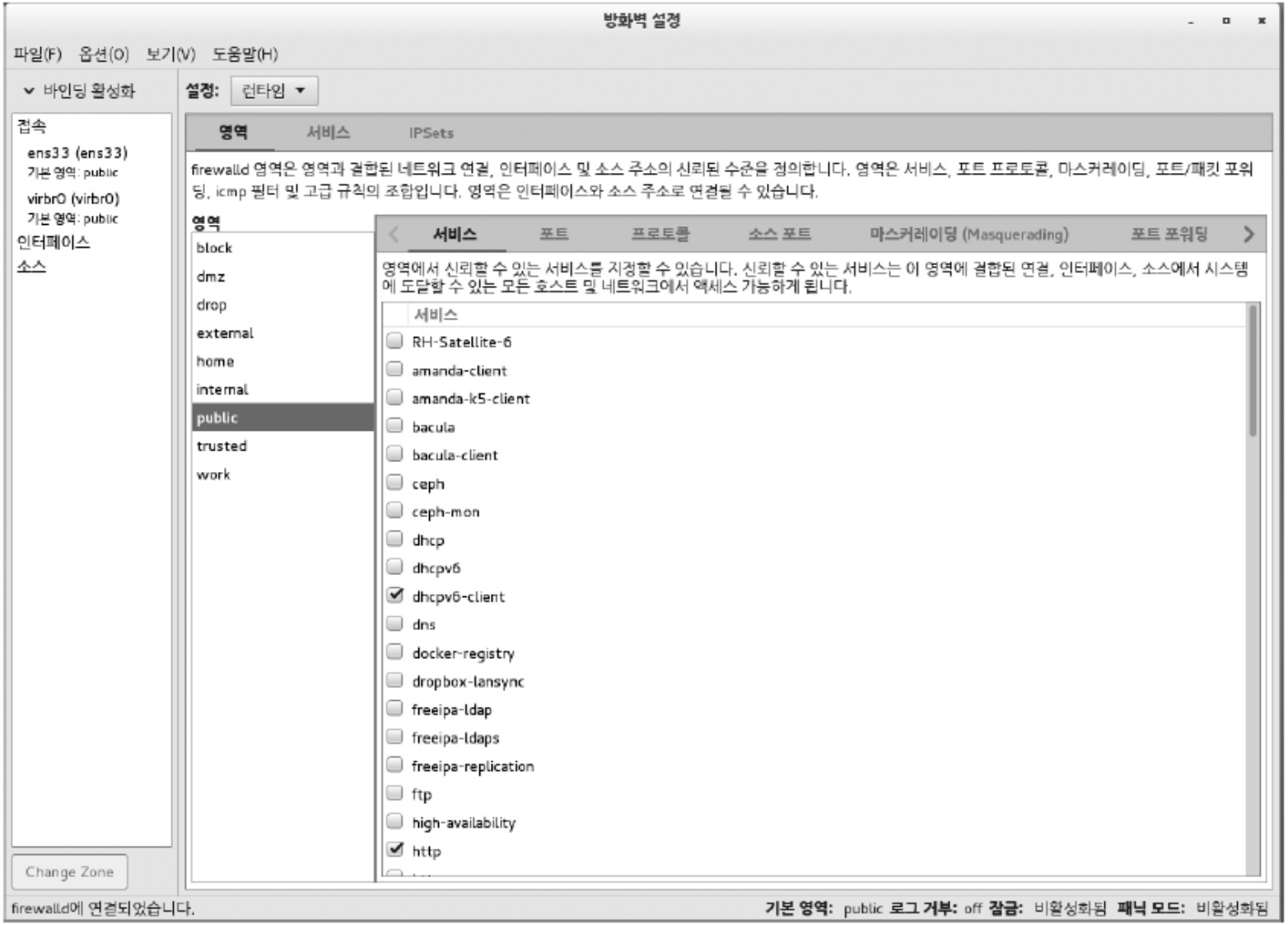
방화벽 설정

방화벽 설정은 터미널 창에서 설정하는 방법과 GUI 도구로 설정하는 두 가지 방법이 존재합니다. 이 두 가지 방법을 [예제 14-3]에서 이미 살펴보았습니다. 여기서는 GUI 도구로 방화벽을 설정하는 방법에서의 항목들에 대해서만 다음 예제를 통해 살펴보도록 하겠습니다.

예제 15-2

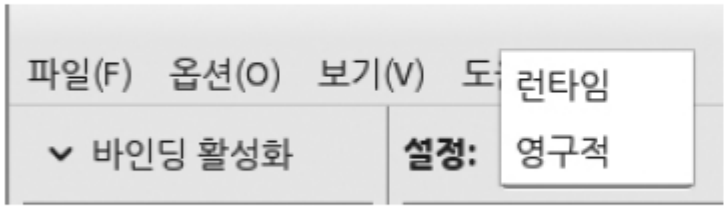
GUI 도구로 방화벽을 설정하기 위해 터미널 창에서 다음과 같이 명령을 수행합니다.

```
# firewall-config
```



[그림 15-4] 방화벽 설정 화면

설정 뷰



[그림 15-5] 설정 뷰

설정 뷰는 방화벽 설정내용을 즉시 적용할 것인지를 결정합니다. [런타임]으로 설정할 경우 그 즉시 적용됩니다.

영역

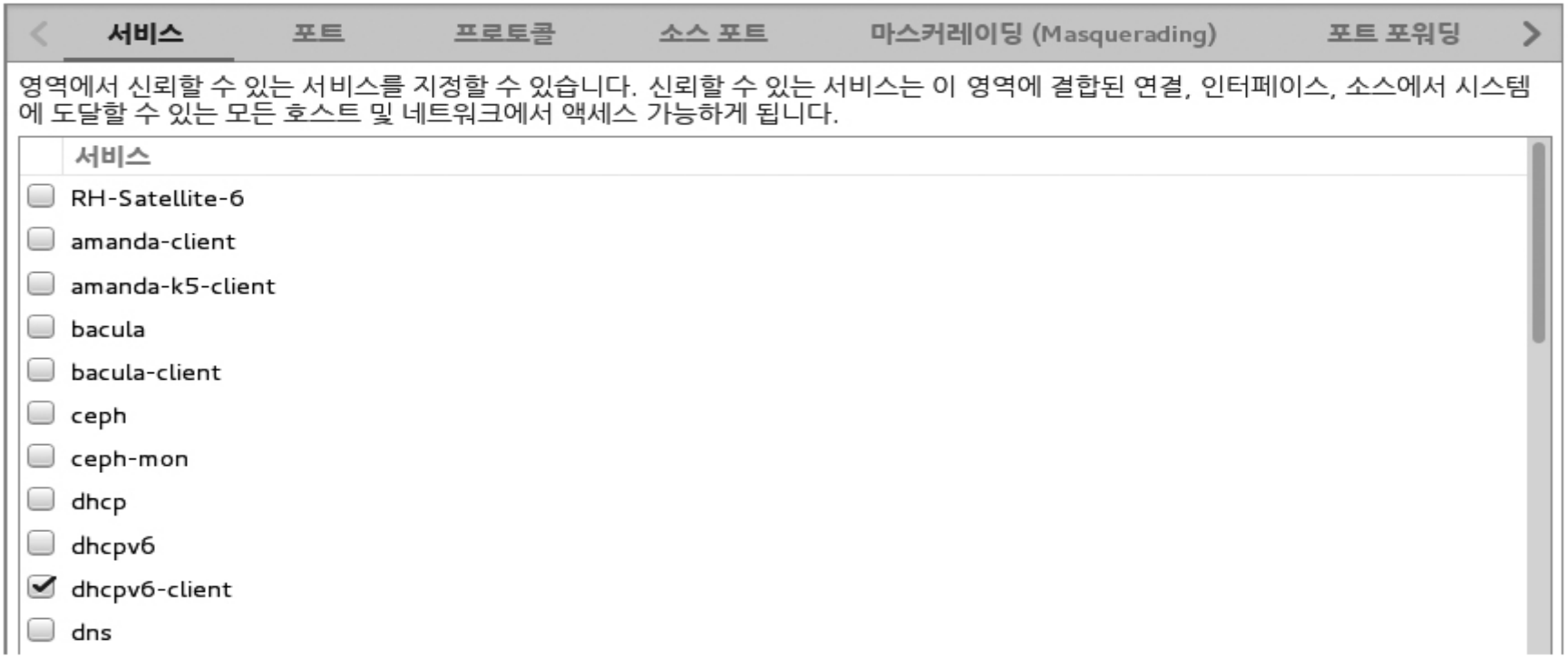
[그림 15-6] 영역 설정

영역은 네트워크를 신뢰도 수준에 따라 구분하여 방화벽을 설정할 수 있도록 제공하고 있습니다. 이 영역 중에서 하나를 기본 영역으로 지정할 수 있으며 현재 설정된 기본영역은 public 입니다.

- block : 모든 네트워크 접속요청 거부
- dmz : dmz으로 구분된 영역에 있는 컴퓨터만 접근가능
- drop : 내부에서 외부로 접속하는 것만 허용
- external : 외부 네트워크를 위해 선택된 서비스만 접속
- home : 홈 영역으로 선택된 서비스만 접속 허용
- internal : 내부 네트워크를 위한 것으로 선택된 서비스만 접속 허용
- public : 공개 영역으로 선택된 서비스만 접속 허용
- trusted : 이 영역에 있는 컴퓨터의 모든 네트워크 연결
- work : 작업영역으로 선택된 서비스만 접속 허용

방화벽 설정하기

방화벽에서는 서비스, 포트, 프로토콜, 소스포트, 마스커레이딩, 포트 포워딩, ICMP 필터, 고급 규칙, 인터페이스, 소스 등을 설정할 수 있습니다. 서비스 항목 중에서 신뢰할 수 있는 서비스를 지정하려면 체크박스에 체크하면 됩니다.



[그림 15-7] 신뢰할 수 있는 서비스 선택

Chapter 15

최상의 노력에 따른 인고의 가치는 반드시 증명될 수 있습니다!

Thank You