28. CentOS7 방화벽

Chapter 28 CentOS7 Firewall

Server 방화벽 기능 설정

Firewalld

- 서버 보안을 확보하려면 방화벽을 설치해야 한다.
- CentOS 7은 이전 버전까지 사용하던 iptables 대신 **firewalld**를 통해 방화벽 기능을 제공한다.
- firewalld는 명령을 실행해서 설정하거나 GUI 설정 도구를 사용해서 설정할 수 있다.

Zone(영역)

- 사전에 CentOS 사용 용도에 맞춰 방화벽을 설정할 수 있는 템플릿을 말한다.
- 서버의 용도나 상황, 네트워크 인터페이스에 따라 적절한 영역을 설정한다.
- 특정 IP 주소에 대해서는 영역을 따로 설정할 수도 있다.

Zone 설정

CentOS에서 설정할 수 있는 Zone

영역	설명
external	외부 네트워크 접근 시 사용하는 영역. 설정한 서비스에 대한 접속만 허용
dmz	외부 네트워크 접속은 허가하지만, 내부 네트워크 접속은 제한
work	업무 목적으로 사용하는 영역으로, 설정한 서비스에 대한 접속만 허가
home	가정에서 사용하는 영역으로, 설정한 서비스에 대한 접속만 허가
internal	내부 네트워크 영역으로, 설정한 서비스에 대한 접속만 허가
trusted	모든 접속을 허가
drop	모든 접속을 거부
public	공개 서버를 설치할 때. 접속을 허가할 서비스나 포트를 추가하여 사용

네트워크 인터페이스에 적용된 영역 확인

- **firewall-cmd --get-active-zones**

모든 영역 확인

- **firewall-cmd --list-all-zones**
    - active: 활성화 영역

- default: 기본 영역

네트워크 인터페이스에 적용 중인 영역 변경

- **firewall-cmd --zone=영역 --change-interface=enp0s3**

접속 거부 설정

- **특정 주소**
  - **firewall-cmd --zone=drop --add-source=주소/32**
- **특정 네트워크**
  - **firewall-cmd --zone=drop --add-source=네트워크/서브넷비트**
- **접속 거부 설정 삭제(다시 접속 가능)**
  - **firewall-cmd --zone-drop --remove-source=네트워크/서브넷비트**

방화벽 설정 적용 및 지속적 활성화

방화벽 설정 적용

- **firewall-cmd --reload**

방화벽 설정 지속적 활성화

- **firewall-cmd --permanent …**
  - 방화벽 설정을 지속적으로 활성화하려면 --permanent 옵션을 붙여야 한다.

서비스 확인 및 서비스 허가

특정 영역만의 서비스 허가 상황을 확인

- **firewall-cmd --zone=public --list-service(s)**

특정 영역에서의 서비스 허가 추가

- **firewall-cmd --zone=public --add-service=서비스명**

특정 영역에서의 서비스 허가 거부

- **firewall-cmd --zone=public --remove-service=서비스명**

설정 가능한 서비스 목록

- **firewall-cmd --get-services**

포트 접속 허가 및 거부

포트 접속 허가

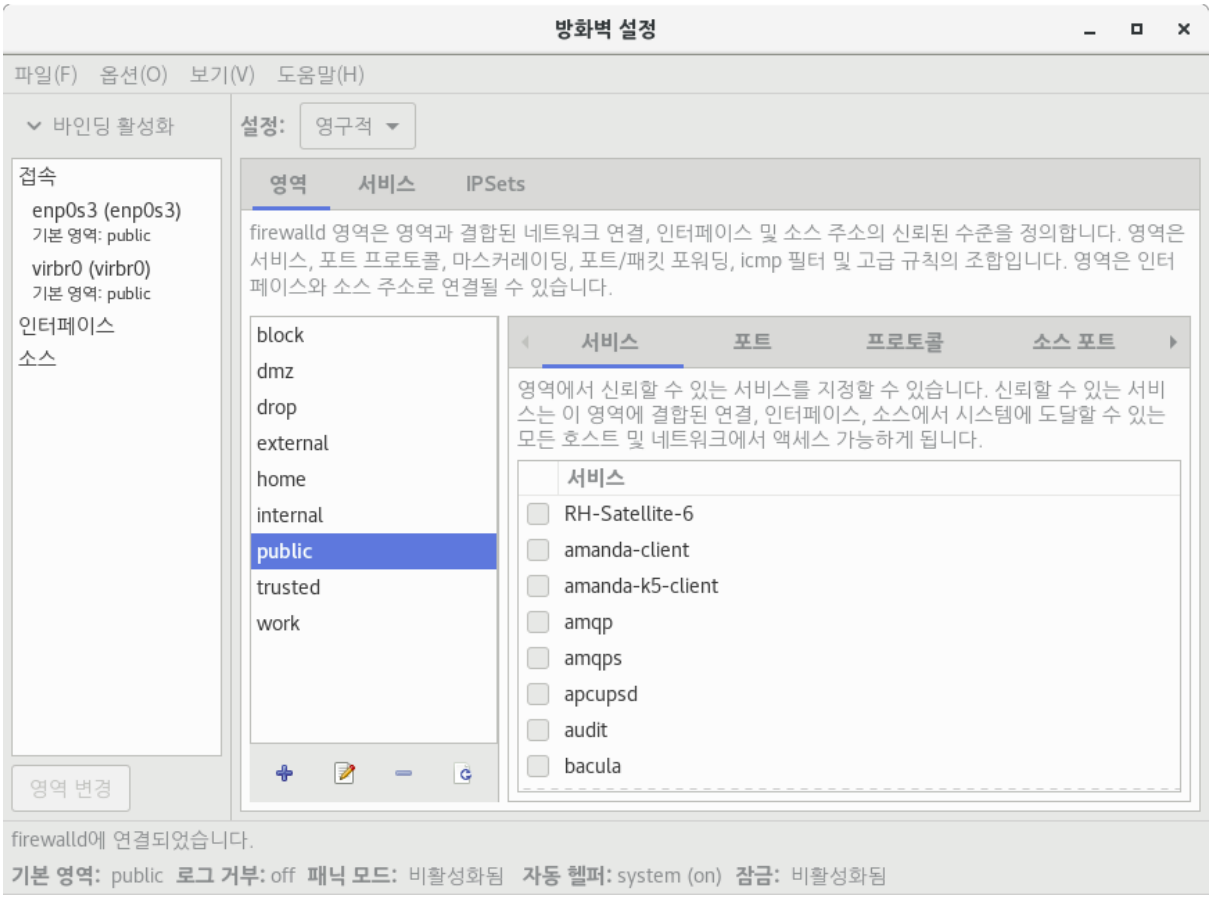
- **firewall-cmd --permanent --zone=public --add-port=포트번호/tcp(or udp)**

포트 접속 거부

- **firewall-cmd --permanent --zone=public --remove-port=포트번호/tcp(or udp)**

GUI 방화벽 설정 도구에서 방화벽 설정

프로그램 메뉴에서 잡다 > 방화벽을 선택하면 설정


방화벽 설정
파일(F) 옵션(O) 보기(V) 도움말(H)
바인딩 활성화
설정: 영구적
접속
enp0s3 (enp0s3)
기본 영역: public
virbr0 (virbr0)
기본 영역: public
인터페이스
소스
영역 변경
영역 서비스 IPSets
firewalld 영역은 영역과 결합된 네트워크 연결, 인터페이스 및 소스 주소의 신뢰된 수준을 정의합니다. 영역은 서비스, 포트 프로토콜, 마스커레이딩, 포트/패킷 포워딩, icmp 필터 및 고급 규칙의 조합입니다. 영역은 인터페이스와 소스 주소로 연결될 수 있습니다.
block
dmz
drop
external
home
internal
public
trusted
work
서비스 포트 프로토콜 소스 포트
영역에서 신뢰할 수 있는 서비스를 지정할 수 있습니다. 신뢰할 수 있는 서비스는 이 영역에 결합된 연결, 인터페이스, 소스에서 시스템에 도달할 수 있는 모든 호스트 및 네트워크에서 액세스 가능하게 됩니다.
서비스
RH-Satellite-6
amanda-client
amanda-k5-client
amqp
amqps
apcupsd
audit
bacula
firewalld에 연결되었습니다.
기본 영역: public 로그 거부: off 패닉 모드: 비활성화됨 자동 헬퍼: system (on) 잠금: 비활성화됨