

firewalld

firewalld는 방화벽 (firewall) + 데몬 (daemon)으로 구성되며, 현재 RHEL1에서는 기본으로 설치되어 있습니다. firewalld는 iptables보다 더 강력하고 사용하기 쉽습니다.

- 방화벽을 구성하는 데 필요한 모든 설정을 단일 인터페이스로 관리할 수 있습니다.
- **Zone (지역)** 개념을 도입하여 네트워크 인터페이스에 따라 다른 수준의 보안 정책을 적용할 수 있습니다.
- 다양한 서비스와 포트에 대한 접근을 쉽게 허용하거나 거부할 수 있습니다.
- **D-Bus API**를 통해 GUI나 다른 프로그램과 통합하여 방화벽을 관리할 수 있습니다.

이전에는 iptables를 사용하여 방화벽을 구성해야 했지만, RHEL에서는 firewalld를 사용하여 더 간단하고 강력하게 방화벽을 관리할 수 있습니다.

Zone(지역)이란 무엇인가?

firewalld는 Zone(지역)을 사용하여 네트워크 인터페이스에 따라 다른 수준의 보안 정책을 적용할 수 있습니다. Zone은 방화벽의 구성을 정의하는 데 사용되며, 각 Zone은 특정 수준의 보안 정책을 나타냅니다. 예를 들어, public Zone은 외부 네트워크에 노출된 인터페이스에 적용되며, drop Zone은 모든 트래픽을 차단합니다. firewalld는 이러한 Zone을 사용하여 방화벽을 쉽게 구성하고 관리할 수 있습니다.

Zone 이름	기본 정책	설명
drop	모든 트래픽 차단	모든 트래픽을 차단하는 가장 엄격한 Zone입니다.
block	모든 트래픽 차단	모든 트래픽을 차단하는 Zone입니다. public Zone과 유사합니다.
public	기본 정책	외부 네트워크에 노출된 인터페이스에 적용되는 기본 Zone입니다.
external	기본 정책	외부 네트워크에 노출된 인터페이스에 적용되는 Zone입니다. public Zone과 유사합니다.
dmz	기본 정책	DMZ (Demilitarized Zone)에 노출된 인터페이스에 적용되는 Zone입니다.
work	기본 정책	작업용 네트워크에 적용되는 Zone입니다.
home	기본 정책	가정용 네트워크에 적용되는 Zone입니다.


```
# firewall-cmd --get-default-zone
```






 (









):

```
# firewall-cmd --zone=public --list-all
```

```
# firewall-cmd --get-zone-of-interface=eth0
```

```
# firewall-cmd --set-default-zone=internal
```

. --permanent

```
# firewall-cmd --zone=internal --change-interface=eth1 --permanent
```

1. RHEL 7

Revision #5

Created 12 March 2025 00:45:09 by yjj8353

Updated 22 April 2025 08:12:09 by yjj8353