



□□□    □□□□□    □□□    □□□    □□□    □□    □

- SSH

- □□    □□
- root □□    □□    □□

- □□□

- □□□□    □□□□    □□□
- firewalld

# SSH

**SSH(Secure Shell)** 是一个安全的网络协议，用于在计算机之间进行安全通信。它通过加密数据来防止窃听和攻击。SSH 通常用于远程登录和管理服务器。SSH 使用公钥加密技术来验证身份，确保通信的安全性。SSH 还可以用于文件传输（SFTP）和端口转发。SSH 是 Linux 和 Unix 系统上的标准工具，广泛应用于网络管理和系统维护。

SSH



ssh 的默认端口是 22。ftp 21, http/https 80/443 都是 IANA (Internet Assigned Numbers Authority) 定义的 TCP/UDP 的知名端口 (Well-known port)。在 Linux 上，ssh 默认监听 22 端口。如果 22 端口被占用，可以修改 sshd\_config 文件中的 Port 配置项，将 ssh 的默认端口修改为其他端口。例如，将 Port 22 修改为 10022。

SSH 配置

```
# vi /etc/ssh/sshd_config
```

SSH 端口

sshd\_config 中的 Port 配置项用于指定 sshd 监听的端口。默认情况下，Port 配置项的值为 22。如果希望使用其他端口，可以修改该配置项的值。例如，将 Port 22 修改为 10022。

```
Port 10022
```

SSH 安装

Debian

```
# systemctl restart ssh
```

RHEL

```
# systemctl restart sshd
```

SSH

root  

!!! root    
  ,  

SSH  

# vi /etc/ssh/sshd\_config

PermitRootLogin  

sshd\_config  PermitRootLogin  no  .  
  ,  

PermitRootLogin no

SSH  

Debian  

# systemctl restart ssh

RHEL  

# systemctl restart sshd



防火墙 (Firewall) 用于防止未经授权的访问，保护网络资源。它通过配置规则来允许或拒绝流量。
 防火墙可以部署在网络边界，也可以部署在内部网络中。它可以根据IP地址、端口号、协议类型等信息进行过滤。
 常见的防火墙类型有包过滤防火墙、状态检测防火墙、应用层网关等。

📄



1. 📄 📄 📄 📄 📄

📄 📄	📄 📄
iptables	📄 📄 📄 📄 📄 📄 📄 📄 📄
nftables	iptables📄 📄 📄 📄 📄 📄 📄 📄 ,📄 📄 📄 📄 📄 📄
firewalld	iptables/nftables📄 📄 📄 , Zone📄 📄 📄 📄 . 📄 RHEL📄 📄 📄 📄 📄 . (RHEL 7 📄 )
ufw	iptables📄 📄 📄 ,📄 📄 📄 📄 📄 📄 📄 . 📄 📄 📄 📄 📄 📄 📄 .

2. 📄 📄

iptables

📄 :

- 📄 📄 📄 📄 📄
- 📄 📄 📄 📄 📄
- 📄 📄 📄 📄 📄 📄

📄 :

- 📄 📄 📄 📄 📄
- 📄 📄 📄 ,📄 📄 📄 📄 📄 📄 📄

nftables

📄 :

- iptables📄 📄 📄 📄 📄 📄 📄
- 📄 📄 IPv4, IPv6, ARP, 📄 📄 📄

- 在 系统 中 安装

命令 :

- 使用 命令 `iptables` 来 配置

## firewalld

命令 :

- `iptables` 和 `nftables` 是 两个 不同的 防火墙 引擎
- 在 (Zone) 中 可以 设置 不同的 防火墙 策略 和 规则
- 在 系统 中 安装

命令 :

- `iptables` 和 `nftables` 是 两个 不同的 防火墙 引擎
- 在 系统 中 安装

## ufw

命令 :

- 在 系统 中 安装
- 使用 命令 `ufw allow 22/tcp` 来 配置
- Ubuntu 系统 中 安装

命令 :

- 在 系统 中 安装
- `iptables` 和 `nftables` 是 两个 不同的 防火墙 引擎

# firewalld

## 1. firewalld ?

firewalld는 firewall + daemon의 합성어이며, RHEL1부터 도입된 서비스이다. firewalld는 iptables를 대체한다.

- firewalld는 firewalld.conf로 설정된다.
- Zone (Zone)은 네트워크 인터페이스에 할당되는 보안 영역이다.
- firewalld는 firewalld.conf로 설정된다.
- D-Bus API : GUI 프로그램에서 firewalld를 제어할 수 있다.

firewalld는 iptables를 대체한다. RHEL1부터 도입된 서비스이다. firewalld는 iptables를 대체한다.

## 2. Zone(네트워크 인터페이스)은 무엇인가 ?

firewalld는 Zone(네트워크 인터페이스)을 기반으로 보안 정책을 적용한다. Zone은 네트워크 인터페이스에 할당되는 보안 영역이다. Zone은 firewalld.conf로 설정된다. Zone은 firewalld.conf로 설정된다.

Zone 이름	기본 정책	설명
drop	모든 트래픽을 차단한다.	모든 트래픽을 차단한다. (보안 수준이 높음)
block	모든 트래픽을 차단한다.	모든 트래픽을 차단한다. (보안 수준이 높음)
public	기본적인 보안 정책을 적용한다.	기본적인 보안 정책을 적용한다. (보안 수준이 낮음)
external	외부 네트워크에 대한 보안 정책을 적용한다.	외부 네트워크에 대한 보안 정책을 적용한다. (보안 수준이 낮음)



구분	주요 특징	비고
dmz	외부에서 접근 가능	DMZ 설정 시 내부 IP를 지정하여 외부에서 접근 가능하게 함
work	내부에서 접근 가능	내부 네트워크에서 접근 가능하게 함
home	내부에서 접근 가능	내부 네트워크에서 접근 가능하게 함
internal	내부에서 접근 가능	내부 네트워크에서 접근 가능하게 함
trusted	내부에서 접근 가능	내부 네트워크에서 접근 가능하게 함

이러한 설정을 통해 외부에서 내부 네트워크로 접근할 수 있도록 하며, 내부 네트워크에서 외부로 접근할 수 있도록 함. (EX. 웹 서버)

### 3. firewalld

#### 3-1. 기본 설정

firewalld

firewalld가 설치되어 있는지 확인 :

```
# firewall-cmd --state
```

firewalld가 설치되어 있는 경우, firewall-cmd 명령어를 사용하여 설정을 변경할 수 있음.

```
# firewall-cmd --reload
```

#### 3-2. 기본 설정

firewalld가 설치되어 있는 경우, firewall-cmd 명령어를 사용하여 설정을 변경할 수 있음.

firewalld가 설치되어 있는 경우, firewall-cmd 명령어를 사용하여 설정을 변경할 수 있음.

```
# firewall-cmd --get-zones
```

firewalld가 설치되어 있는 경우, firewall-cmd 명령어를 사용하여 설정을 변경할 수 있음.



```
# firewall-cmd --add-port=80/tcp --permanent
# firewall-cmd --zone=public --add-port=443/tcp --permanent
# firewall-cmd --zone=public --add-port=443/udp --permanent
```

□□ □□

```
--zone= □□ □□ □□ □□ □□□□ □□ □□□□ . --zone= □□ □□□□ □□ □□ ,
default-zone □□ □□ □□□□ . --permanent □□ □□ □□□□ □□□□ .
```

```
# firewall-cmd --remove-port=80/tcp --permanent
# firewall-cmd --zone=public --remove-port=443/tcp --permanent
# firewall-cmd --zone=public --remove-port=443/udp --permanent
```

### 3-4. □□ □□ □□ /□□ □□

□□ □□

```
--zone= □□ □□ □□ □□ □□□□ □□ . --zone= □□ □□□□ □□ □□ , default-zone
□□ □□ □□ . --permanent □□ □□ □□□□ □□□□ .
```

```
# firewall-cmd --add-service=http --permanent
# firewall-cmd --zone=public --add-service=https --permanent
```

□□ □□

```
--zone= □□ □□ □□ □□ □□□□ □□□□ . --zone= □□ □□□□ □□ □□ , default-
zone □□ □□□□ □□□□ . --permanent □□ □□ □□□□ □□□□ .
```

```
# firewall-cmd --remove-service=http --permanent
# firewall-cmd --zone=public --remove-service=https --permanent
```

#### 1. RHEL 7 □□ □□□□ .