



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

- 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。它通过加密通道传输数据，防止窃听和篡改。SSH 通常用于远程登录和管理服务器。SSH 协议支持多种加密算法和认证方式，确保通信的安全性和完整性。SSH 还可以用于文件传输（SFTP）和端口转发等功能。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 默认端口是 22。ftp 21, http/https 80/443 都是 IANA (Internet Assigned Numbers Authority) 定义的 TCP/UDP 端口 (Well-known port)。Linux 默认使用 22 端口，而 Windows 默认使用 22 端口。ssh 默认使用 22 端口，而 Windows 默认使用 22 端口。

SSH 配置

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

SSH 端口

sshd\_config 中的 Port 配置项指定了 SSH 服务的默认端口。默认情况下，SSH 服务使用 22 端口。如果希望更改端口，可以将 Port 配置项的值修改为所需的端口号。

```
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，也可以部署在服务器前面。它可以根据IP地址、端口号、协议类型等信息进行过滤。
 配置防火墙时，需要明确要保护的资源和要允许访问的资源。通常，我们会配置默认拒绝策略，只允许必要的流量通过。

📄



1. 📄 📄 📄 📄 📄

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

2. 📄 📄

iptables

📄 :

- 📄 📄 📄 📄 📄
- 📄 📄 📄 📄 📄
- 📄 📄 📄 📄 📄 📄 📄

📄 :

- 📄 📄 📄 📄 📄
- 📄 📄 📄 , 📄 📄 📄 📄 📄 📄 📄

nftables

📄 :

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

- `iptables -F` : 所有规则清除

注意 :

- `iptables` 命令使用 `iptables` 包, 安装 `iptables` 包

## firewalld

简介 :

- `iptables` 和 `nftables` 是 Linux 内核自带的防火墙工具
- `firewalld` (Zone) 是 Linux 系统自带的防火墙管理工具, 它使用 `iptables` 或 `nftables` 作为后端
- `firewalld` 是 `iptables` 的封装

安装 :

- `iptables` 和 `nftables` 是 Linux 内核自带的, 无需安装
- `firewalld` 是 Linux 系统自带的, 安装 `firewalld` 包

## ufw

简介 :

- `ufw` 是 `iptables` 的封装, 使用 `iptables` 作为后端
- `ufw` 是 `iptables` 的封装 ( `ufw allow 22/tcp` )
- Ubuntu 16.04 及以后版本默认安装 `ufw`

安装 :

- `ufw` 是 `iptables` 的封装, 安装 `ufw` 包
- `iptables` 和 `nftables` 是 Linux 内核自带的, 无需安装

--	--	--

# firewalld

firewalld (firewall) + (daemon) , RHEL1 . firewalld .

- **GPIO** **Pin** : **GPIO** **Pin** **Pin** **Pin** **Pin** **Pin**
- **(Zone)** **Pin** : **GPIO** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin**
- **GPIO** **Pin** **Pin** **Pin** : **GPIO** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin**
- **D-Bus API** **Pin** : **GUI** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin** **Pin**

1. 在 CentOS 7 中，默认使用 `iptables` 作为防火墙工具。  
 2. 在 RHEL 7 中，默认使用 `firewalld` 作为防火墙工具。  
 3. 在 CentOS 7 中，默认使用 `iptables` 作为防火墙工具。

# Zone( $\square$ ) $\square$ ?

```
firewalld# Zone( ) # firewalld zone configuration file
# Firewall rules are organized by zones. Zones are defined in
# /etc/firewalld/zones.conf. The default zone is dmz.
# Zones can be added or removed from the system. See
# firewalld --help for more information.
# Zones can be added or removed from the system. See
# firewalld --help for more information.
```

項目	概要	詳細
drop	許可	許可されたパケットは、宛先に送られる。許可されたパケットは、宛先に送られる。
block	許可	許可されたパケットは、宛先に送られる。許可されたパケットは、宛先に送られる。
public	許可	許可されたパケットは、宛先に送られる。許可されたパケットは、宛先に送られる。
external	許可	許可されたパケットは、宛先に送られる。許可されたパケットは、宛先に送られる。
dmz	許可	DMZ 許可されたパケットは、宛先に送られる。許可されたパケットは、宛先に送られる。
work	許可	許可されたパケットは、宛先に送られる。許可されたパケットは、宛先に送られる。



区域	IP地址	说明
home	192.168.1.0/24	家庭网络，包括所有连接到路由器的设备。
internal	10.0.0.0/8	内部网络，包括所有连接到内部网络的设备。
trusted	0.0.0.0/0	信任网络，包括所有连接到信任网络的设备。

在配置防火墙规则时，需要指定规则适用的区域。默认情况下，防火墙规则适用于所有区域。可以通过指定区域来限制规则的适用范围。例如，可以指定规则只适用于家庭网络或内部网络。

# firewalld 配置

## firewalld 配置

在配置 firewalld 之前，需要先安装 firewalld 包。

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

firewalld 默认配置为使用 nftables 作为后端。可以通过以下命令查看当前配置：

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

# firewalld 配置

## firewalld 配置

在配置 firewalld 之前，需要先安装 firewalld 包。

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

firewalld 默认配置为使用 nftables 作为后端。可以通过以下命令查看当前配置：

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

firewalld 默认配置为使用 nftables 作为后端。

root@localhost ~ #

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

root@localhost ~ #

root@localhost ~ # firewall-cmd --zone=public --list-all

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

root@localhost ~ #

root@localhost ~ #

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

root@localhost ~ #

root@localhost ~ #

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

root@localhost ~ #

root@localhost ~ # firewall-cmd --zone=internal --change-interface=eth1 --permanent

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

1. RHEL 7 安装 .