Firewall configuration using iptables or firewalld

Topics : Centos Server
Written on March 05, 2024

Configuring a firewall is crucial for securing your CentOS system by controlling incoming and outgoing network traffic. There are two main firewall management tools available in CentOS: `iptables` and `firewalld`. Here's an overview of how to configure a firewall using both tools:

1. iptables:

Installation:

- Ensure that `iptables` is installed on your CentOS system. If not, you can install it using the following command:

  ```
  sudo yum install iptables
  ```

Basic Configuration:

- List the current firewall rules:

  ```
  sudo iptables -L
  ```

- By default, the `iptables` ruleset is empty.

Adding Rules:

- Add rules to allow or deny traffic based on specific criteria (e.g., IP addresses, ports, protocols).
- For example, to allow incoming traffic on port 22 (SSH), use the following command:

  ```
  sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
  ```

- Similarly, you can add rules to allow or deny traffic for other services and ports.

Saving Rules:

- To save the `iptables` rules so they persist across reboots, use the following command:

  ```
  sudo service iptables save
  ```

2. firewalld:

Installation:

- `firewalld` is installed by default on CentOS systems. If not, you can install it using the following command:

```
sudo yum install firewalld
```

Basic Configuration:

- Enable and start the `firewalld` service:

```
sudo systemctl enable firewalld
sudo systemctl start firewalld
```

- Check the status of the `firewalld` service:

```
sudo systemctl status firewalld
```

Adding Rules:

- Use the `firewall-cmd` command to add rules to the firewall.
- For example, to allow incoming traffic on port 80 (HTTP), use the following command:

```
sudo firewall-cmd --zone=public --add-port=80/tcp --permanent
```

- Similarly, you can add rules to allow or deny traffic for other services and ports.

Reloading Rules:

- After adding or modifying rules, reload the firewall to apply the changes:

```
sudo firewall-cmd --reload
```

Managing Zones:

- `firewalld` uses zones to group network interfaces and apply firewall rules to them.
- Use the `firewall-cmd` command to manage zones, such as adding or removing interfaces from zones.

Using GUI Tools:

- CentOS also provides GUI tools like `firewall-config` and `firewall-applet` for managing `firewalld` settings.