Cấu hình Firewalld

Gv: Nguyễn Thế Đức
Học viện CNTT Bkacad

Firewalld là một công cụ quản lý tường lửa cho các hệ điều hành Linux. Nó cung cấp các tính năng tường lửa bằng cách đóng vai trò là giao diện người dùng cho khung bộ lọc mạng của nhân Linux thông qua tiện ích không gian người dùng nftables, hoạt động như một giải pháp thay thế cho chương trình dòng lệnh nft.

Firewalld chứa các zones và các services – xác định mức độ tin cậy và các dịch vụ liên quan, đây cũng là điều khác biệt cơn bản với những phiên bản tường lửa khác trước đây trên centos: block dmz drop external home internal public trusted work

- Liệt kê tất cả các zone trong hệ thống:

firewall-cmd --get-zones

- Kiểm tra zone mặc định

firewall-cmd --get-default-zone

- Kiểm tra zone active

firewall-cmd --get-active-zones

- Thay đổi zone mặc định:

firewall-cmd --set-default-zone=home

- Liệt kê toàn bộ các quy tắc của các zones:

firewall-cmd --list-all-zones

firewall-cmd --list-all

- Liệt kê toàn bộ các quy tắc trong một zone cụ thể

firewall-cmd --zone=home --list-all

- Liệt kê danh sách services/port được cho phép trong zone cụ thể:

firewall-cmd --zone=public --list-services

firewall-cmd --zone=public --list-ports

- Thiết lập các service trên zones của Firewalld:
    - Xác định các services trên hệ thống:

firewall-cmd --get-services

- Thông tin của services:

/usr/lib/firewalld/services/

- Thiết lập cho phép services trên FirewallD

firewall-cmd --zone=public --add-service=http

firewall-cmd --zone=public --add-service=http –permanent

- Kiểm tra: firewall-cmd --zone=public --list-services
    - Xóa services trên FirewallD

firewall-cmd --zone=public --remove-service=http

firewall-cmd --zone=public --remove-service=http --permanent

- Thiết lập cho Port
    - Mở Port:

firewall-cmd --zone=public --add-port=9999/tcp

firewall-cmd --zone=public --add-port=9999/tcp --permanent

firewall-cmd --zone=public --add-port=4990-5000/tcp

firewall-cmd --zone=public --add-port=4990-5000/tcp –permanent

- Remove Port:

firewall-cmd --zone=public --remove-port=9999/tcp

firewall-cmd --zone=public --remove-port=9999/tcp –permanent

- Tạo thêm zone:
  firewall-cmd --permanent --new-zone=<tên zone>
  firewall-cmd –reload
- Định nghĩa Services:
  - Copy file định nghĩa riêng từ file chuẩn ban đầu:

cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/<tên-service>.xml

/etc/firewalld/services//<tên-service>.xml

firewall-cmd –reload

firewall-cmd --get-services

- Thiết lập:

firewall-cmd --zone=public --add-service=<tên-service>

firewall-cmd --zone=public --add-service=<tên-service> --permanent