# Thiết lập tường lửa FirewallD trên CentOS 7

1. Các khái niệm cơ bản trong FirewallD

Trước khi thực sự dùng đến FirewallD để quản lý tường lửa, hãy cùng làm quen với các khái niệm cơ bản: Zone và thời gian hiệu lực của quy tắc.

1.1. Zone

Trong FirewallD, zone là một nhóm các quy tắc nhằm chỉ ra những luồng dữ liệu được cho phép, dựa trên mức độ tin tưởng của điểm xuất phát luồng dữ liệu đó trong hệ thống mạng. Để sử dụng, bạn có thể lựa chọn zone mặc đinh, thiết lập các quy tắc trong zone hay chỉ định giao diện mạng(Network Interface) để quy định hành vi được cho phép

Các zone được xác định trước theo mức độ tin cậy, theo thứ tự từ “ít-tin-cậy-nhất” đến “đáng-tin-cậy-nhất”:

* **drop**: ít tin cậy nhất – toàn bộ các kết nối đến sẽ bị từ chối mà không phản hồi, chỉ cho phép duy nhất kết nối đi ra.
* **block**: tương tự như drop nhưng các kết nối đến bị từ chối và phản hồi bằng tin nhắn từ icmp-host-prohibited (hoặc icmp6-adm-prohibited).
* **public**: đại diện cho mạng công cộng, không đáng tin cậy. Các máy tính/services khác không được tin tưởng trong hệ thống nhưng vẫn cho phép các kết nối đến trên cơ sở chọn từng trường hợp cụ thể.
* **external**: hệ thống mạng bên ngoài trong trường hợp bạn sử dụng tường lửa làm gateway, được cấu hình giả lập NAT để giữ bảo mật mạng nội bộ mà vẫn có thể truy cập.
* **internal**: đối lập với external zone, sử dụng cho phần nội bộ của gateway. Các máy tính/services thuộc zone này thì khá đáng tin cậy.
* **dmz**: sử dụng cho các máy tính/service trong khu vực DMZ(Demilitarized) – cách ly không cho phép truy cập vào phần còn lại của hệ thống mạng, chỉ cho phép một số kết nối đến nhất định.
* **work**: sử dụng trong công việc, tin tưởng hầu hết các máy tính và một vài services được cho phép hoạt động.
* **home**: môi trường gia đình – tin tưởng hầu hết các máy tính khác và thêm một vài services được cho phép hoạt động.
* **trusted**: đáng tin cậy nhất – tin tưởng toàn bộ thiết bị trong hệ thống.

1.2. Hiệu lực của các quy tắc Runtime/Permanent

Trong FirewallD, các quy tắc được cấu hình thời gian hiệu lực Runtime hoặc Permanent.

* **Runtime**(mặc định): có tác dụng ngay lập tức, mất hiệu lực khi reboot hệ thống.
* **Permanent**: không áp dụng cho hệ thống đang chạy, cần reload mới có hiệu lực, tác dụng vĩnh viễn cả khi reboot hệ thống.

Ví dụ, thêm quy tắc cho cả thiết lập Runtime và Permanent:

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

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

# firewall-cmd --reload

Việc Restart/Reload sẽ hủy bộ các thiết lập Runtime đồng thời áp dụng thiết lập Permanent mà không hề phá vỡ các kết nối và session hiện tại. Điều này giúp kiểm tra hoạt động của các quy tắc trên tường lửa và dễ dàng khởi động lại nếu có vấn đề xảy ra.

**Lưu ý**: Các ví dụ thiết lập trong bài sử dụng cả Runtime và Permanent.

2. Cài đặt FirewallD

– FirewallD được cài đặt mặc định trên CentOS 7. Cài đặt nếu chưa có:

# yum install firewalld

– Khởi động FirewallD:

# systemctl start firewalld

– Kiểm tra tình trạng hoạt động

# systemctl status firewalld

● firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)

Active: active (running) since Wed 2017-12-13 16:43:20 +07; 30s ago

Docs: man:firewalld(1)

Main PID: 12696 (firewalld)

CGroup: /system.slice/firewalld.service

└─12696 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

# systemctl is-active firewalld

active

# firewall-cmd --state

running

– Thiết lập FirewallD khởi động cùng hệ thống

# systemctl enable firewalld

Kiểm tra lại :

# systemctl is-enabled firewalld

enabled

Ban đầu, bạn không nên cho phép FirewallD khởi động cùng hệ thống cũng như thiết lập Permanent, tránh bị khóa khỏi hệ thống nếu thiết lập sai. Chỉ thiết lập như vậy khi bạn đã hoàn thành các quy tắc tường lửa cũng như test cẩn thận.  
– Khởi động lại

# systemctl restart firewalld

# firewall-cmd --reload

– Dừng và vô hiệu hóa FirewallD

# systemctl stop firewalld

# systemctl disable firewalld

3. Cấu hình FirewallD

3.1. Thiết lập các Zone

– Liệt kê tất cả các zone trong hệ thống

# firewall-cmd --get-zones

block dmz drop external home internal public trusted work

– Kiểm tra zone mặc định

# firewall-cmd --get-default-zone

public

– Kiểm tra zone active (được sử dụng bởi giao diện mạng)  
Vì FirewallD chưa được thiết lập bất kỳ quy tắc nào nên zone mặc định cũng đồng thời là zone duy nhất được kích hoạt, điều khiển mọi luồng dữ liệu.

# firewall-cmd --get-active-zones

public

interfaces: eth0

– HocVPS sẽ hướng dẫn sử dụng duy nhất **public** zone – cho phép những services/port được thiết lập và từ chối mọi thứ khác

– Thay đổi zone mặc định, ví dụ thành home:

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

success

3.2. Thiết lập các quy tắc

Trước khi thiết lập các quy tắc mới, hãy cùng HocVPS kiểm tra các quy tắc hiện tại:  
– Liệt kê toàn bộ các quy tắc của các zones:

# firewall-cmd --list-all-zones

– Liệt kê toàn bộ các quy tắc trong zone mặc định và zone active

# firewall-cmd --list-all

public (active)

target: default

icmp-block-inversion: no

interfaces: eth0

sources:

services: ssh dhcpv6-client

ports:

protocols:

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules:

Kết quả cho thấy public là zone mặc định đang được kích hoạt, liên kết với card mạng eth0 và cho phép DHCP cùng SSH.  
– Liệt kê toàn bộ các quy tắc trong một zone cụ thể, ví dụ home

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

home

target: default

icmp-block-inversion: no

interfaces:

sources:

services: ssh mdns samba-client dhcpv6-client

ports:

protocols:

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules:

– 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

a. Thiết lập cho Service

Đây chính là điểm khác biệt của FirewallD so với Iptables – quản lý thông qua các services. Việc thiết lập tường lửa đã trở nên dễ dàng hơn bao giờ hết – chỉ việc thêm các services vào zone đang sử dụng.  
– Đầu tiên, xác định các services trên hệ thống:

# firewall-cmd --get-services

RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-client dns docker-registry dropbox-lansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client ganglia-master high-availability http https imap imaps ipp ipp-client ipsec iscsi-target kadmin kerberos kibana klogin kpasswd kshell ldap ldaps libvirt libvirt-tls managesieve mdns mosh mountd ms-wbt mssql mysql nfs nrpe ntp openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius rpc-bind rsh rsyncd samba samba-client sane sip sips smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh synergy syslog syslog-tls telnet tftp tftp-client tinc tor-socks transmission-client vdsm vnc-server wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server

Lưu ý: Biết thêm thông tin về service qua thông tin lưu tại /usr/lib/firewalld/services/.

Hệ thống thông thường cần cho phép các services sau: ssh(22/TCP), http(80/TCP), https(443/TCP), smtp(25/TCP), smtps(465/TCP) và smtp-submission(587/TCP)

– Thiết lập cho phép services trên FirewallD, sử dụng --add-service:

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

success

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

success

Ngay lập tức, zone “public” cho phép kết nối HTTP trên cổng 80. Kiểm tra lại

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

ssh dhcpv6-client http

– Vô hiệu hóa services trên FirewallD, sử dụng --remove-service:

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

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

b. Thiết lập cho Port

Trong trường hợp bạn thích quản lý theo cách truyền thống qua Port, FirewallD cũng hỗ trợ bạn điều đó.  
– Mở Port với tham số --add-port:

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

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

Mở 1 dải port

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

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

Kiểm tra lại

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

9999/tcp 4990-5000/tcp

– Đóng Port với tham số --remove-port:

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

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

4. Cấu hình nâng cao

4.1. Tạo Zone riêng

Mặc dù, các zone có sẵn là quá đủ với nhu cầu sử dụng, bạn vẫn có thể tạo lập zone của riêng mình để mô tả rõ ràng hơn về các chức năng của chúng. Ví dụ, bạn có thể tạo riêng một zone cho webserver **publicweb** hay một zone cấu hình riêng cho DNS trong mạng nội bộ **privateDNS**. Bạn cần thiết lập Permanent khi thêm một zone.

# firewall-cmd --permanent --new-zone=publicweb

success

# firewall-cmd --permanent --new-zone=privateDNS

success

# firewall-cmd --reload

success

Kiểm tra lại

# firewall-cmd --get-zones

block dmz drop external home internal privateDNS public publicweb trusted work

Khi đã có zone thiết lập riêng, bạn có thể cấu hình như các zone thông thường: thiết lập mặc định, thêm quy tắc… Ví dụ:

# firewall-cmd --zone=publicweb --add-service=ssh --permanent

# firewall-cmd --zone=publicweb --add-service=http --permanent

# firewall-cmd --zone=publicweb --add-service=https --permanent

4.2. Định nghĩa services riêng trên FirewallD

Việc mở port trên tường lửa rất dễ dàng nhưng lại khiến bạn gặp khó khăn khi ghi nhớ các port và các services tương ứng. Vì vậy, khi có một services mới thêm vào hệ thống, bạn sẽ có 2 phương án:

* Mở Port của services đó trên FirewallD
* Tự định nghĩa services đó trên FirewallD

Ví dụ, HocVPS Admin Port có thể là 2017, 9999 hay 4 chữ số bất kì nào đó. Bạn sẽ tự định nghĩa servies **hocvps-admin** với port 9999.  
– Tạo file định nghĩa riêng từ file chuẩn ban đầu

# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/hocvps-admin.xml

– Chỉnh sửa để định nghĩa servies trên FirewallD

# nano /etc/firewalld/services/hocvps-admin.xml

<?xml version="1.0" encoding="utf-8"?>

<service>

<short>HocVPS-Admin</short>

<description>Control HocVPS Admin Web Tool</description>

<port protocol="tcp" port="9999"/>

</service>

– Lưu lại và khởi động lại FirewallD

# firewall-cmd --reload

– Kiểm tra lại danh sách services:

# firewall-cmd --get-services

RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc ceph ceph-mon cfengine condor-collector ctdb dhcp dhcpv6 dhcpv6-client dns docker-registry dropbox-lansync elasticsearch freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp ganglia-client ganglia-master high-availability hocvps-admin http https imap imaps ipp ipp-client ipsec iscsi-target kadmin kerberos kibana klogin kpasswd kshell ldap ldaps libvirt libvirt-tls managesieve mdns mosh mountd ms-wbt mssql mysql nfs nrpe ntp openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy proxy-dhcp ptp pulseaudio puppetmaster quassel radius rpc-bind rsh rsyncd samba samba-client sane sip sips smtp smtp-submission smtps snmp snmptrap spideroak-lansync squid ssh synergy syslog syslog-tls telnet tftp tftp-client tinc tor-socks transmission-client vdsm vnc-server wbem-https xmpp-bosh xmpp-client xmpp-local xmpp-server

Như vậy, hocvps-admin đã được thêm vào danh sách services của FirewallD. Bạn có thể thiết lập như các servies thông thường, bao gồm cả cho phép/chặn trong zone. Ví dụ:

# firewall-cmd --zone=public --add-service=hocvps-admin

# firewall-cmd --zone=public --add-service=hocvps-admin --permanent

5. Kết luận

Có thể thấy, sử dụng tường lửa FirewallD trên CentOS 7 là không quá khó. Bạn đã có lượng kiến thức và kinh nghiệm đủ để thiết lập và quản trị hệ thống FirewallD trong nhu cầu sử dụng thông thường.