Direct Interface

- direct interface chủ yếu sử dụng bởi services or app cho việc add specific firewall rules.

- Nó yếu cầu các kiến thức cơ bản về ip(6)table concepts (tables, chains, commands, parameters, targets).

- Nó cũng có thể sử dụng để add rules tới firewalld.

Options

- Direct configuration gives a more direct access to the firewall.

- It requires user to know basic ip(6)tables/ebtables concepts, i.e. table (filter/mangle/nat/...), chain (INPUT/OUTPUT/FORWARD/...), commands (-A/-D/-I/...), parameters (-p/-s/-d/-j/...) and targets (ACCEPT/DROP/REJECT/...).

- Direct configuration should be used only as a last resort when it’s not possible to use firewalld.zone(5).

- Firewalld direct config file chứa thông tin về permanent direct chains, rules and passthrough …

Cấu trúc 1 direc config file:

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

<direct>

[ <chain ipv="ipv4|ipv6|eb" table="table" chain="chain"/> ]

[ <rule ipv="ipv4|ipv6|eb" table="table" chain="chain" priority="priority"> args </rule> ]

[ <passthrough ipv="ipv4|ipv6|eb"> args </passthrough> ]

</direct>

Direct

- This tag can only be used once in a direct configuration file.

- There are no attributes for direct.

Chain (chuỗi)

- sử dụng để định nghĩa chains thêm vào. Chain entry có chính xác 3 trường

ipv="ipv4|ipv6|eb"

- IP family là nơi chain sẽ được tạo. Nó có thể là ipv4, ipv6 or eb.

table="table"

- table name là nơi the chain sẽ dược tạo.

- This can be one of the tables that can be used for iptables, ip6tables or ebtables. For the possible values, see TABLES section in the iptables, ip6tables or ebtables man pages.

chain="chain"

- Tên của chain được tạo, đảm bảo không có 2 chain trùng tên.

- Please remember to add a rule or passthrough rule with an --jump or --goto option to connect the chain to another one.

rule

- Có thể dùng lại nhiều lần. Sử dụng để add rules cho việc built-in or added chain.

- A rule entry has exactly four attributes:

ipv="ipv4|ipv6|eb"

- The IP family where the rule will be added. This can be either ipv4, ipv6 or eb.

table="table"

- table name là nơi rule sẽ được add.

- This can be one of the tables that can be used for iptables, ip6tables or ebtables.

- For the possible values, see TABLES section in the iptables, ip6tables or ebtables man pages.

chain="chain"

- name của chain nơi rule được thêm vào.

- This can be either a built-in chain or a chain that has been created with the chain tag. If the chain name is a built-in chain, then the rule will be added to chain\_direct, else the supplied chain name is used. chain\_direct is created internally for all built-in chains to make sure that the added rules do not conflict with the rules created by firewalld.

priority="priority"

- priority được sử dụng để order rules.

- Priority 0 means add rule on top of the chain, with a higher priority the rule will be added further down.

- Rules with the same priority are on the same level and the order of these rules is not fixed and may change. If you want to make sure that a rule will be added after another one, use a low priority for the first and a higher for the following.

- The args can be any arguments of iptables or ip6tables, that do not conflict with the table or chain attributes.

passthrough

- Is an optional element tag and can be used several times. It can be used to add rules to a built-in or added chain. A rule entry has exactly one attribute:

ipv="ipv4|ipv6|eb"

- The IP family where the passthrough rule will be added. This can be either ipv4, ipv6 or eb.

- The args can be any arguments of iptables or ip6tables.

- The passthrough rule will be added to the chain directly. There is no mechanism like for the direct rule above. The user of the passthrough rule has to make sure that there will be no conflict with the rules created by firewalld.

Examples

- Blacklisting of the networks 192.168.1.0/24 and 192.168.5.0/24 with logging and dropping early in the raw table:

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

<direct>

<chain ipv="ipv4" table="raw" chain="blacklist"/>

<rule ipv="ipv4" table="raw" chain="PREROUTING" priority="0">-s 192.168.1.0/24 -j blacklist</rule>

<rule ipv="ipv4" table="raw" chain="PREROUTING" priority="1">-s 192.168.5.0/24 -j blacklist</rule>

<rule ipv="ipv4" table="raw" chain="blacklist" priority="0">-m limit --limit 1/min -j LOG --log-prefix "blacklisted: "</rule>

<rule ipv="ipv4" table="raw" chain="blacklist" priority="1">-j DROP</rule>

</direct>