Zone

- firewall zone định nghĩa mức độ tin cậy của các kết nối, interface, source address binding

- Tùy thuộc vào các quan hệ, các connection, interface, source có thể là 1 phần 1 zone nhưng 1 zone có thể sử dụng chi nhiều connection, interface, source

Predefined Zones

- Là các zone được cung cấp bởi firewalld, chúng được sắp xếp theo mức đô tin cậy theo từ ko tin cậy -> tin cậy

Drop

- Bắt kỳ các gói tin từ network đến sẽ bị dropped, ko có reply. Chỉ các gói tin ra là được phép

Block

- bắt kỳ các gói tin đến sẽ bị loại bỏ, trả về các icmp-host-prohibited message for IPv4 and icmp6-adm-prohibited for IPv6. Chỉ có các network connection được khởi tạo bởi hệ thống là được phép

Public

- Sử dụng cho public area. Không tin tưởng vào các máy tính khác. Lựa chọn có kết nối tới được phép

External

- sử dụng cho external network (mạng mở rộng) với mặt nạ mạng đặc biệt cho các định tuyến. Không tin các máy tính khác. Lựa chọn liên kết tới để kết nối

DMZ

- Server được đặt public với giới hạn các truy cập tới. Lựa chọn các kết nối tới

Work

- Sử dụng trong vùng làm việc. Tin tưởng vào các pc xung quanh. Lựa chọn kết nối tới

Home

- sử dụng cho vùng làm việc tại nhà. Tin tưởng các pc xung quanh, lựa chọn có kết nối tới

Internal

- Vùng nội bộ. Tìn tường các pc xung quanh. Lựa chọn các kết nối tới

Trusted

- chấp nhận mọi kết nối

Connections, Interfaces and Sources

- Cho phép gán hoặc ánh xạ zone cho các connection, interface, source address

How to set or change a zone for a connection

- Trên hệ thống hỗ trợ ifcfg file cho interface, zone có thể được lưu tại file ifcfg với trường “ZONE = option”.

- Nếu option này ko tồn tại sẽ mặc định kết default zone

Network connections handled by NetworkManager

- firewall trong linux kernel không có khả năng xử lý các connections với tên được hiển thị bởi NetworkManager, nó chỉ có thể xử lý các network interface được kết nối đến. Vì thế NetworkManager hỗ trợ firewalld việc gán network interface đến zone được xác lập.

- Config của các kết nối có thể được config bởi networkmanager hoặc ifcfg

- Nếu zone ko được set cho config file => default zone sẽ được sử dụng

- Networkmanager sẽ báo cho firewalld bó gán zone cho interface khi connection down

- Nếu firewall start, restart, khởi động, NetworkManager sẽ get notified và connection sẽ gắn zone được cấu hình

Network connections handled by network scripts

- Mỗi connection được sử lý bởi network scripts có 1 số giới hạn: ko có daemon tell firewall add zone có connection. Vấn đề này có thể giải quyết bởi ifcfg-post script.

- The zone defines the firewall features that are enabled in this zone.

Configuration of Zones

- Config hoặc add zone, bạn có thể sử dụng firewalld interface để xử lý, thay đổi config như firewall-config. Cũng có thể sử dụng cmd line tool như firewall-cmd hoặc DBUS interface. Hoặc có thể tạo và copy file zone vòi config directory.

- “/usr/lib/firewalld/zones” được sử dụng cho mặc định và fallback config.

- “/etc/firewalld/zones” được sử dụng cho việc tạo cà customized

Default Zone

- Default zone là zine được sử dụng cho mọi thứ nếu chúng không được định nghĩa hoặc gán zones

- Connection được xử lý bởi NetworkManager, NetworkManager sẽ request để add zone binding cho interface sử dụng bởi connection. Cũng như interface dưới control

Use of Zones

- Lựa chọn zone tùy theo mục địch, môi trường mạng

Options

- zone config có thể chứa tag và attribute. Có thế do sự ủy nhiệm hoặc do tùy chọn

Zone

- Zone được ủy nhiệm được bắt đầu và kết thực bằng “”. Tag này chỉ có thể sử dụng cho Zone config file

VD:

version="string" # give zone version

- Có thể sử dụng accept, reject or drop với mọi gói tin khi chúng ko match rule (port, service, etc).

- Accept target sử dụng cho trusted zone, nó accept tất có gói tin ko match rule.

- $$REJECT% target sử dụng cho block zone cho việc reject tất cả packet không matching bất kỳ rule nào.

- DROP target sử dụng cho drop zone, nó drop tất cả packet ko match rule.

- Nếu không định nghĩa target, tất cả packet ko match rule sẽ bị reject

VD:

target="ACCEPT|%%REJECT%%|DROP"

Short

- Is an optional start and end tag and is used to give a zone a more readable name.

Description

- Is an optional start and end tag to have a description for a zone.

Interface

- Is an optional empty-element tag and can be used several times. It can be used to bind an interface to a zone. You don’t need this for NetworkManager-managed interfaces, because NetworkManager binds interfaces to zones automatically. See also ‘How to set or change a zone for a connection?’ in firewalld.zones(5). You can use it as a fallback mechanism for interfaces that can’t be managed via NetworkManager. An interface entry has exactly one attribute:

name="string"

- The name of the interface to be bound to the zone.

source

- Is an optional empty-element tag and can be used several times.

- Nó có thể sử dụng để bind a source address, address range, a MAC address or an ipset to a zone.

- A source entry has exactly one of these attributes:

address="address[/mask]"

- The source is either an IP address or a network IP address with a mask for IPv4 or IPv6. The network family (IPv4/IPv6) will be automatically discovered. For IPv4, the mask can be a network mask or a plain number. For IPv6 the mask is a plain number. The use of host names is not supported.

mac="MAC"

- The source is a MAC address. It must be of the form XX:XX:XX:XX:XX:XX.

ipset="ipset"

- The source is an ipset.

Service

- Is an optional empty-element tag and can be used several times to have more than one service entry enabled. A service entry has exactly one attribute:

name="string"

- The name of the service to be enabled.

- To get a list of valid service names “firewall-cmd --list=services” can be used.

Port

- Is an optional empty-element tag and can be used several times to have more than one port entry. All attributes of a port entry are mandatory:

port="portid[-portid]"

- The port can either be a single port number portid or a port range portid-portid.

protocol="tcp|udp"

- The protocol can either be tcp or udp.

Protocol

- Is an optional empty-element tag and can be used several times to have more than one protocol entry. All protocol has exactly one attribute:

value="string"

- The protocol can be any protocol supported by the system.

- Please have a look at /etc/protocols for supported protocols.

icmp-block

- Is an optional empty-element tag and can be used several times to have more than one icmp-block entry. Each icmp-block tag has exactly one mandatory attribute:

name="string"

- The name of the Internet Control Message Protocol (ICMP) type to be blocked.

- To get a list of valid ICMP types firewall-cmd --list=icmptypes can be used.

icmp-block-inversion

- Is an optional empty-element tag and can be used only once in a zone configuration. This flag inverts the icmp block handling.

- Only enabled ICMP types are accepted and all others are rejected in the zone.

masquerade

- Is an optional empty-element tag. It can be used only once in a zone configuration and is not usable for IPv6. If it’s present masquerading is enabled for the zone. If you want to enable masquerading, you should enable it in the zone bound to the external interface.

forward-port

- Is an optional empty-element tag and can be used several times to have more than one port or packet forward entry. This is for IPv4 only. Use rich language rules for IPv6. There are mandatory and also optional attributes for forward ports:

Mandatory attributes:

- The local port and protocol to be forwarded.

port="portid[-portid]"

- The port can either be a single port number portid or a port range portid-portid.

protocol="tcp|udp"

- The protocol can either be tcp or udp.

Optional attributes:

- The destination of the forward. For local forwarding add to-port only. For remote forwarding add to-addr and use to-port optionally if the destination port on the destination machine should be different.

to-port="portid[-portid]"

- The destination port or port range to forward to. If omitted, the value of the port= attribute will be used altogether with the to-addr attribute.

to-addr="address"

- The destination IPv4 IP address.

source-port

- Is an optional empty-element tag and can be used several times to have more than one source port entry. All attributes of a source port entry are mandatory:

port="portid[-portid]"

- The port can either be a single port number portid or a port range portid-portid.

protocol="tcp|udp"

- The protocol can either be tcp or udp.

rule

- Is an optional element tag and can be used several times to have more than one rich language rule entry.

- The general rule structure:

<rule [family="ipv4|ipv6"]>

[ <source address="address[/mask]" [invert="True"]/> ]

[ <destination address="address[/mask]" [invert="True"]/> ]

[

<service name="string"/> |

<port port="portid[-portid]" protocol="tcp|udp"/> |

<protocol value="protocol"/> |

<icmp-block name="icmptype"/> |

<masquerade/> |

<forward-port port="portid[-portid]" protocol="tcp|udp" [to-port="portid[-portid]"] [to-addr="address"]/> |

<source-port port="portid[-portid]" protocol="tcp|udp"/> |

]

[ <log [prefix="prefixtext"] [level="emerg|alert|crit|err|warn|notice|info|debug"]/> [<limit value="rate/duration"/>] </log> ]

[ <audit> [<limit value="rate/duration"/>] </audit> ]

[

<accept> [<limit value="rate/duration"/>] </accept> |

<reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |

<drop> [<limit value="rate/duration"/>] </drop> |

<mark set="mark[/mask]"> [<limit value="rate/duration"/>] </mark>

]

</rule>

Rule structure for source black or white listing:

<rule [family="ipv4|ipv6"]>

<source address="address[/mask]" [invert="True"]/>

[ <log [prefix="prefixtext"] [level="emerg|alert|crit|err|warn|notice|info|debug"]/> [<limit value="rate/duration"/>] </log> ]

[ <audit> [<limit value="rate/duration"/>] </audit> ]

<accept> [<limit value="rate/duration"/>] </accept> |

<reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |

<drop> [<limit value="rate/duration"/>] </drop>

</rule>

- For a full description on rich language rules, please have a look at firewalld.richlanguage(5).

Examples

Here are some zone examples:

external

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

<zone>

<short>External</short>

<description>For use on external networks. You do not trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.</description>

<service name="ssh"/>

<masquerade/>

</zone>

home

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

<zone>

<short>Home</short>

<description>For use in home areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.</description>

<service name="ssh"/>

<service name="mdns"/>

<service name="samba-client"/>

<service name="dhcpv6-client"/>

</zone>

public

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

<zone>

<short>Public</short>

<description>For use in public areas. You do not trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.</description>

<service name="ssh"/>

<service name="dhcpv6-client"/>

</zone>

trusted

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

<zone target="ACCEPT">

<short>Trusted</short>

<description>All network connections are accepted.</description>

</zone>

drop

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

<zone target="DROP">

<short>Drop</short>

<description>Unsolicited incoming network packets are dropped. Incoming packets that are related to outgoing network connections are accepted. Outgoing network connections are allowed.</description>

</zone>

block

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

<zone target="%%REJECT%%">

<short>Block</short>

<description>Unsolicited incoming network packets are rejected. Incoming packets that are related to outgoing network connections are accepted. Outgoing network connections are allowed.</description>

</zone>