Cách sử dụng firewall:

Enable and Disable firewalld

- firewalld cung cấp các init scripts cho hệ thống bằng cách sử dụng VsysVinit cung như systemd service file

- Nó khuyến cáo sử dụng iptables khi firewalld đang chạy, nó có thể gây ra 1 số lỗi ngoài mong muốn

- Nếu user xóa đi base rules or chains của chain structure, firewalld reload có thể cần việc tạo lại chúng

Enable and Disable firewalld

- Nếu iptables, ip6tables, ebtables and ipset services đang được sử dụng:

systemctl disable --now iptables.service

systemctl disable --now ip6tables.service

systemctl disable --now etables.service

systemctl disable --now ipset.service

dnf install firewalld firewall-config firewall-applet

systemctl unmask --now firewalld.service

systemctl enable --now firewalld.service

- Kiểm tra firewalld state có 2 tùy chọn

#systemctl status firewalld

#### KQ

$ systemctl status firewalld

● firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor pr

Active: active (running) since Wed 2016-06-29 14:28:51 CEST; 1 weeks 6 days a

Docs: man:firewalld(1)

Main PID: 24540 (firewalld)

Tasks: 2 (limit: 512)

CGroup: /system.slice/firewalld.service

└─24540 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork –nopid

#firewall-cmd --state.

running

Install and enable iptables, ip6tables, ebtables and ipset services

- Khi firewalld đang enabled, bạn muốn sử dụng đồng thời Install and enable iptables, ip6tables, ebtables and ipset services

dnf install iptables-services ebtables ipset-service

systemctl mask --now firewalld.service

systemctl enable --now iptables.service

systemctl enable --now ip6tables.service

systemctl enable --now etables.service

systemctl enable --now ipset.service

- The use of the mask line is recommended as systemd will start firewalld if there is another service requires it or if the D-Bus interface of firewalld is used. If the service only gets disabled, then it will not be auto started anymore.

Get firewalld State

With firewall-cmd

- To get the firewalld state with firewall-cmd, use the following command:

$firewall-cmd --state

running

- It returns an exit code 0 if it is active, NOT\_RUNNING otherwise (see the firewalld “Exit Codes”). The command will also print the state to STDOUT.

With systemctl

$ systemctl status firewalld

● firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor pr

Active: active (running) since Wed 2016-06-29 14:28:51 CEST; 1 weeks 6 days a

Docs: man:firewalld(1)

Main PID: 24540 (firewalld)

Tasks: 2 (limit: 512)

CGroup: /system.slice/firewalld.service

└─24540 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid

Reload firewalld

With firewall-cmd

- To reload firewalld, you can use the command line client firewall-cmd:

firewall-cmd --reload

- Reload firewall rules and keep state information. Current permanent configuration will become new runtime configuration, i.e. all runtime only changes done until reload are lost with reload if they have not been also in permanent configuration.

firewall-cmd --complete-reload

- Reload firewall completely, even netfilter kernel modules. This will most likely terminate active connections, because state information is lost. This option should only be used in case of severe firewall problems. For example if there are state information problems that no connection can be established with correct firewall rules.

Using a signal

- As root you can send the HUP signal to the firewall daemon to initiate reload:

# killall -HUP firewalld

Open a Port or Service

- có nhiều cách để mở port (range) hoặc service. Chúng tùy thuộc vào use case và mục địch

- Đối với các service được định nghĩa sẵn, không cần quan tâm đến port default (VD: http:80)

- có thể thay đổi port mặc định của các service, và tạo mới các custom service

How to open port 80/tcp with firewall-cmd:

firewall-cmd --zone=public --add-port=80/tcp

- Nó sẽ mở port 80, zone public, nó sẽ có giá trị đến khi service restart, stop, system reboot

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

- Nếu bạn muốn tạo các thay đổi perman. Chúng sẽ tồn tại đến khi được xóa

How to open a service with firewall-cmd:

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

- This opens the service in the public zone of the runtime environment.

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

- This also opens the service in public zone of the permanent environment.

Add a Service

- có nhiều cách để add 1 service. 1 new service chỉ có thể thấy được trong môi trường runtime nếu chúng khi chúng đã được add.

With firewall-cmd

- To add a new and empty service, use the --new-service altogether with the --permanent option:

firewall-cmd --permanent --new-service=myservice

- Cấu hình service vừa tạo

firewall-cmd --permanent --service=service --set-description=description

firewall-cmd --permanent --service=service --set-short=description

firewall-cmd --permanent --service=service --add-port=portid[-portid]/protocol

firewall-cmd --permanent --service=service --add-protocol=protocol

firewall-cmd --permanent --service=service --add-source-port=portid[-portid]/protocol

firewall-cmd --permanent --service=service --add-module=module

firewall-cmd --permanent --service=service --set-destination=ipv:address[/mask]

- Có thể add 1 service mới từ 1 file có trước

firewall-cmd --permanent --new-service-from-file=myservice.xml

- Tạo 1 service dựa trên các trường định nghĩa trong file có trước

firewall-cmd --permanent --new-service-from-file=myservice.xml --name=mynewservice

- This adds a new service using the service settings from the file. But the new service will have the name mynewservice.

With firewall-offline-cmd

- To add a new and empty service, use the --new-service option:

firewall-offline-cmd --new-service=myservice

- Configure the service:

firewall-offline-cmd --service=service --set-description=description

firewall-offline-cmd --service=service --set-short=description

firewall-offline-cmd --service=service --add-port=portid[-portid]/protocol

firewall-offline-cmd --service=service --add-protocol=protocol

firewall-offline-cmd --service=service --add-source-port=portid[-portid]/protocol

firewall-offline-cmd --service=service --add-module=module

firewall-offline-cmd --service=service --set-destination=ipv:address[/mask]

- Alternativly you can add a new service using an existing file:

firewall-offline-cmd --new-service-from-file=myservice.xml

- This adds a new service using all settings from the file including the servie name.

firewall-offline-cmd --new-service-from-file=myservice.xml --name=mynewservice

- This adds a new service using the service settings from the file. But the new service will have the name mynewservice.

Copy a file in the services directory in /etc/firewalld

- sử dụng quyền root copy file service định nghĩa

# cp myservice.xml /etc/firewalld/services

- sau khi copy khoảng 5s, service sẽ được thêm vào firewalld

Place a file in the services directory in /usr/lib/firewalld

- This is the way how a package or system service could add a new service to firewalld.

- Lợi ích của việc lưu service trong /usr/lib/firewalld/services là bất kỳ admin hay user đề có thể modify service và sau đó quay lại original service easily, loading the defaults of the service.

- Then the by firewalld created and modified copy in /etc/firewalld/services will be renamed to <service>.xml.old and the original service in /usr/lib/firewalld/services will be used again. The original service will be effective in the run time environment only after a reload.

- A package that is placing the service in the /usr/lib/firewalld/services diretory should require the firewalld package or sub package that is providing the path. In an RPM based distribution that is using or that bases on the firewalld provided spec file this package is firewalld-filesystem.

Debug firewalld

- bạn có thế add debug option tới firewalld arg trong “/etc/sysconfig/firewalld” hoặc trong firewalld service file, hoặc firewalld trong terminal sai khi dừng server

The sysconfig file

- This file does not exist in all distributions. In Fedora or RHEL based distributions it usable:

# firewalld command line args

# possible values: --debug

FIREWALLD\_ARGS=

-To enable the debugging mode, add --debug[=<level>] to FIREWALLD\_ARGS. For a list of the supported debug levels, please have a look furter down

The firewalld systemd service file

- This is the firewalld systemd service file on Fedora for example:

$ cat /usr/lib/systemd/system/firewalld.service

[Unit]

Description=firewalld - dynamic firewall daemon

Before=network-pre.target

Wants=network-pre.target

After=dbus.service

After=polkit.service

Conflicts=iptables.service ip6tables.service ebtables.service ipset.service

Documentation=man:firewalld(1)

[Service]

EnvironmentFile=-/etc/sysconfig/firewalld

ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD\_ARGS

ExecReload=/bin/kill -HUP $MAINPID

# supress to log debug and error output also to /var/log/messages

StandardOutput=null

StandardError=null

Type=dbus

BusName=org.fedoraproject.FirewallD1

KillMode=mixed

[Install]

WantedBy=multi-user.target

Alias=dbus-org.fedoraproject.FirewallD1.service

- To enable debugging, you can add the --debug[=<level>] option to ExecStart. For a list of the supported debug levels, please have a look furter down.

Start in terminal

- As user root you can start the firewall daemon in a termal for debugging:

# firewalld --nofork --debug

- With the --nofork option the daemon is not doing a fork and stays in the foreground. It is possible to use another debug level with --debug[=<level>].

The debug levels

- Different debug levels are supported here. The default is debug level 1 if –debug is added to the command line. Higher debug levels can be specified with –debug=. The higher the debug level the more output. The highest debug level is 10.

|  |  |
| --- | --- |
| Debug level | Output |
| 1 | Loading config files, D-Bus method calls |
| 2 | + Backend calls, D-Bus Introspect method calls, access checks |
| 3 | + Rules that are added by the backends |
| 4 | + Transaction steps |
| 5 - 9 | Currently unused |
| 10 | + Introspection XML data |

e