Basic Firewall Configuration

Unit objectives

After completing this unit, you should be able to:

- Intro to firewalld
- Zones
- Services
- Ports
- Checking firewalld Status
- Managing firewalld
- Configure Zone
- Understanding and Managing ICMP traffic
- Port Forwarding

Introducing Firewalld

- Dynamic firewall manager, uses nftables framework
- v8 uses firewalld to manage firewall rules instead of iptables (netfilter)
- Less complex compares to iptables
- Control incoming (only) traffic
- By default is enabled and configured
- Key elements:
  - Zones
  - Interfaces
  - Services
  - Ports

Zones

- Group of interfaces
- Allow or denied ips / services / ports
- Drop zone:
  - Most secured. Only outgoing traffics are permitted
- Block zone:
  - Similar to Drop zone with exception incoming ICMP is rejected with notification
- Home zone:
  - Allow almost all incoming traffics
  - Use with cautious.
- Public (active)
  - Newly added interfaces
  - Allowed ICMP, SSH
- Additional zone can be created

More Zones

- External zone:
  - Used with internal but applied to interface connected to public network
- Internal zone:
  - Used with external and applied to interface connected to private network
- DMZ (demilitarized) zone:
  - are publicly accessible but isolated from internal network
- Work zone:
  - Used when working with work network / environment.
- Trusted:
  - Least secured zone. Trust everyone by default.

Services

- TCP/IP defined services
- Services = port_number/transport_protocol
- Example:
  - HTTP: 80/tcp
  - HTTPS: 443/tcp
  - TFTP : 69/udp
  - Email : 25/tcp
- Look into IANA or /etc/services

Pre-defined Services

Service name	Configuration
ssh	Local SSH server. Traffic to 22/tcp
dhcpv6-client	Local DHCPv6 client. Traffic to 546/udp on the fe80::/64 IPv6 network
ipp-client	Local IPP printing. Traffic to 631/udp.
samba-client	Local Windows file and print sharing client. Traffic to 137/udp and 138/udp.
mdns	Multicast DNS (mDNS) local-link name resolution. Traffic to 5353/udp to the 224.0.0.251 (IPv4) or ff02::fb (IPv6) multicast addresses.

Note

Many pre-defined services are included in the *firewalld* package. Use **firewall-cmd --get-services** to list them. Configuration files for pre-defined services are found in **/usr/lib/firewalld/services**, in a format defined by **firewalld.zone**(5).

Either use the pre-defined services or directly specify the port and protocol required. The Web Console graphical interface is used to review pre-defined services and to define additional services.

Ports

- Customized services
- Special application registered with customized transport layer port number
- Example:
  - Cockpit : 9090/tcp
  - Web container : 8080/tcp

Verify configuration

- Verify Firewalld package is installed

  # rpm –qa firewalld*

- IF not installed, install it

  # dnf install –y firewalld

- Verify Firewalld service is running

  # systemctl status firewalld

- If not running, enable it

  # systemctl enable --now firewalld

Manage firewalld

- Stop fiirewall service
  - ✓Clear all rules from memory
  - # systemctl stop firewalld
- Start fiirewall service
  - ✓Reload all rules from disk to memory
  - # systemctl start firewalld
- Temporarily disable firewall service
  - ✓ No rules been removed from memory hence very fast reactivated upon unmask
  - # systemctl mask firewalld

Configure the firewall from command line

- firewalld-cmd <tab><tab> # get list of subcommands
- firewalld-cmd **--permanent**; firewall-cmd **--reload**

firewall-cmd commands	Explanation
--get-default-zone	Query the current default zone.
--set-default-zone=*ZONE*	Set the default zone. This changes both the runtime and the permanent configuration.
--get-zones	List all available zones.
--get-active-zones	List all zones currently in use (have an interface or source tied to them), along with their interface and source information.
--add-source=*CIDR* [--zone=*ZONE*]	Route all traffic coming from the IP address or network/netmask to the specified zone. If no **--zone=** option is provided, the default zone is used.
--remove-source=*CIDR* [--zone=*ZONE*]	Remove the rule routing all traffic from the zone coming from the IP address or network/ netmask network. If no **--zone=** option is provided, the default zone is used.
--add-interface=*INTERFACE* [--	Route all traffic coming from ***INTERFACE*** to

Configure zone

- Add / Remove new zone

```
# firewall-cmd --permanent --new-zone=myoffice
# firewall-cmd --reload
```

- Set created zone as active

```
# firewall-cmd –set-default-zone=myoffice
```

- List all zones

```
# firewall-cmd --list-all-zone
# firewall-cmd --get-zones
```

- Remove new zone

```
# firewall-cmd --permanent --delete-zone=myoffice
# firewall-cmd --reload
```

Configure rules

- Asssign all traffic coming from 192.168.0.0/24 to myoffice zone

```
# firewall-cmd --permanent --zone=myoffice --add-source=192.168.0.0/24
```

- Allow few services into myoffice zone

```
#  firewall-cmd --permanent --zone=myoffice --add-service=mysql
# firewall-cmd --permanent --add-service={https,smtp}
```

- Remove mysql service from myoffice zone

```
#  firewall-cmd --permanent --zone=myoffice --remove-service=mysql
```

- Reload configuration

```
#  firewall-cmd --reload
```

Changing zone/interface assignments

- View interfaces

```
# firewall-cmd --list-interfaces
```

- Get interfaces from specific zone

```
# firewall-cmd --list-interfaces --zone=public
```

- Place interface into specific zone

```
# firewall-cmd --change-interface=ens37 --zone=myoffice
# firewall-cmd --reload
```

Controlling SELinux Port Labeling

- Network traffic also tightly enforced by SELinux policy
- Label network ports
- Example : Well-known applications

Application	Network service/port	Label
Secured Shell	22/TCP	ssh_port_t
Web Servers	80/TCP and 443/TCP	http_port_t
MySQL Servers	1433/TCP and 1434/TCP	mysql_port_t
PostgreSQL Servers	5432/TCP and 9898/TCP	postgresql_port_t
NFS Service	2049/TCP and 2049/UDP	nfs_port_t

- Customized applications / non-standard port
  - Add manually using semanage port

List all existing port labels

semanage port –l

```
lmtp_port_t                    udp      24
lsm_plugin_port_t              tcp      18700
luci_port_t                    tcp      8084
mail_port_t                    tcp      2000, 3905
mailbox_port_t                 tcp      2004
matahari_port_t                tcp      49000
matahari_port_t                udp      49000
memcache_port_t                tcp      11211
memcache_port_t                udp      11211
milter_port_t                  tcp      8890, 8891, 8893
mmcc_port_t                    tcp      5050
mmcc_port_t                    udp      5050
mongod_port_t                  tcp      27017-27019, 28017-28019
```

```
port_label_t     tcp|udp     comma,separated,list,of,ports
```

Managing Port Labales

- Add customized port 71/tcp as gopher_port_t

```
# semanage port -at gopher_port_t -p tcp 71
```

- Add additional customized port 8800 to httpd

```
# semanage port -at http_port_t -p tcp 8800
```

- Quickly check newly added port label

```
# semanage port -l -C
```

Important

Most standard services available in the Linux distribution provide an SELinux policy module that sets labels on ports. You cannot change the labels on those ports using **semanage**; to change those, you need to replace the policy module. Writing and generating policy modules falls outside the scope of this course.

Modify and Remove Port bindings

- Removing port labels

```
# semanage port -dt gopher_port_t -p tcp 71
```

- Switch **8800/tcp** from http_port_t to gopher_port_t

```
# semanage port -mt gopher_port_t -p tcp 8800
```

- Again check modified port label

```
# semanage port -l -C
```

Important

Most standard services available in the Linux distribution provide an SELinux policy module that sets labels on ports. You cannot change the labels on those ports using **semanage**; to change those, you need to replace the policy module. Writing and generating policy modules falls outside the scope of this course.

Checkpoint

1. Configure firewall to allow following service : smtp
   a) systemctl start --now smtp
   b) firewall-cmd start --now smtp
   c) systemctl --permanent start --now smtp
   d) firewall-cmd --permanent --add-service smtp

2. You have # firewall-cmd --permanent --add-port 1111/tcp. But the traffic still got rejected. Why?
   a) Because firewalld service is not started
   b) You have to reload firewalld service by systemctl --reload
   c) You have to reload firewalld service by firewall-cmd –reload
   d) Because systemd service is not started

3. During weekend, you encounter some issues with the server, you need to suspend the firewall service and resume it later quickly. What should you do?
   a) Restart the server into rescue mode
   b) Run # systemctl mask firewalld
   c) Run # firewall-cmd --permanent mask
   d) Run # systemctl stop firewalld

4. True or False: Most standard services has port labelling done for you.

Checkpoint

1. Configure firewall to allow following service : smtp
   a) systemctl start --now smtp
   b) firewall-cmd start --now smtp
   c) systemctl --permanent start --now smtp
   d) firewall-cmd --permanent --add-service smtp

2. You have # firewall-cmd --permanent --add-port 1111/tcp. But the traffic still got rejected. Why?
   a) Because firewalld service is not started
   b) You have to reload firewalld service by systemctl --reload
   c) You have to reload firewalld service by firewall-cmd –reload
   d) Because systemd service is not started

3. During weekend, you encounter some issues with the server, you need to suspend the firewall service and resume it later quickly. What should you do?
   a) Restart the server into rescue mode
   b) Run # systemctl mask firewalld
   c) Run # firewall-cmd --permanent mask
   d) Run # systemctl stop firewalld

4. True or False: Most standard services has port labelling done for you.

Unit summary

Having completed this unit, you should be able to:

- Understand firewalld
- Understand Zones,Services, Ports
- Check firewalld Status
- Manage firewalld
- Configure Zone
- Understand and Manage ICMP traffic
- Configure Port Forwarding