Brief Introduction to FirewallD

Presented by
Zamir SUN

About me

- Chinese Name 孙子谦 SUN Ziqian
- Known as zsun or Zamir SUN in Fedora community
- Fedora XFCE User
- Helping with FUDCon Beijing 2014
- RHCE for 2 years
- seeking for a job

Topics

1. FirewallD and it's basis
2. Comparing with iptables
3. Basic using of FirewallD
4. FirewallD Rich Language

FirewallD
and it's basis

FirewallD and it's basis

- First introduced into Fedora 15 by Thomas Woerner from Red Hat
- Default firewall in Red Hat Enterprise Linux 7
- Use D-Bus to communicate with kernel
- Zones
- Dynamic firewall
- Rich Language
- Lock Down

Comparing with iptables

Comparing with iptables

- D-Bus vs netlink
- Dynamic vs static
  - As is said on FirewallD wiki, FirewallD can be dynamically configured
  - In my opinion, FirewallD tell kernel to change rules while iptables change the rules and then send the changed settings to kernel
- Change rules by services or applications
- Default zone vs default policy

Basic using of FirewallD

Basic using of FirewallD

- GUI: firewall-config
  - just like the system-config-firewall for iptables

Basic using of FirewallD

- CLI: firewall-cmd
- Example:
  - firewall-cmd --permanent --add-service=http
  - firewall-cmd --zone=home --add-port=80-89/tcp
  -

FirewallD
Rich Language

FirewallD Rich Language

- A high level language to have more complex firewall rules for IPv4 and IPv6 without the knowledge of iptables syntax.
- Can be configured using CLI or GUI or zone config file

FirewallD Rich Language

- With firewall-cmd
  - rule [family="<rule family>"]
  - [source address="<address>" [invert="True"]]
  - [destination address="<address>" [invert="True"]]
  - [<element>]
  - [log [prefix="<prefix text>"] [level="<log level>"] [limit value="<rate/duration>"]]
  - [audit [limit value="<rate/duration>"]]
  - <action>

FirewallD Rich Language

- Allow new IPv4 connections from address 192.168.0.0/24 for service tftp and log 1 per minutes using syslog
- firewall-cmd –add-rich-rule='
  - rule family="ipv4"
  - source address="192.168.0.0/24"
  - service name="tftp"
  - log prefix="tftp"
  - level="info"
  - limit value="1/m"
  - accept '

FirewallD Rich Language

- In zone config file
- <rule [family="<rule family>"]>
-   [<source address="<address>" [invert="True"]/>]
-   [<destination address="<address>" [invert="True"]/>]
-   element
-   [<log [prefix="<prefix text>"] [level="<log level>"]/>]
-   [<audit/>]
-   action
- </rule>

FirewallD Rich Language

```
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Public</short>
  <description>some description</description>
  <service name="ssh"/>
  <rule family="ipv4">
    <source address="192.168.1.209"/>
    <accept/>
  </rule>
</zone>
```

Lock Down

Lock Down

- Lock the firewall configuration so that only allowed application are able to request firewall changes.
- Turned off by default.

Call for Localization

Reference & L10N

- https://fedoraproject.org/wiki/FirewallD
- https://fedoraproject.org/wiki/Features/FirewalldRichLanguage
- https://fedoraproject.org/wiki/Features/FirewalldLockdown
- L10N Wanted!

Questions?

Contact:
zsun@fedoraproject.org