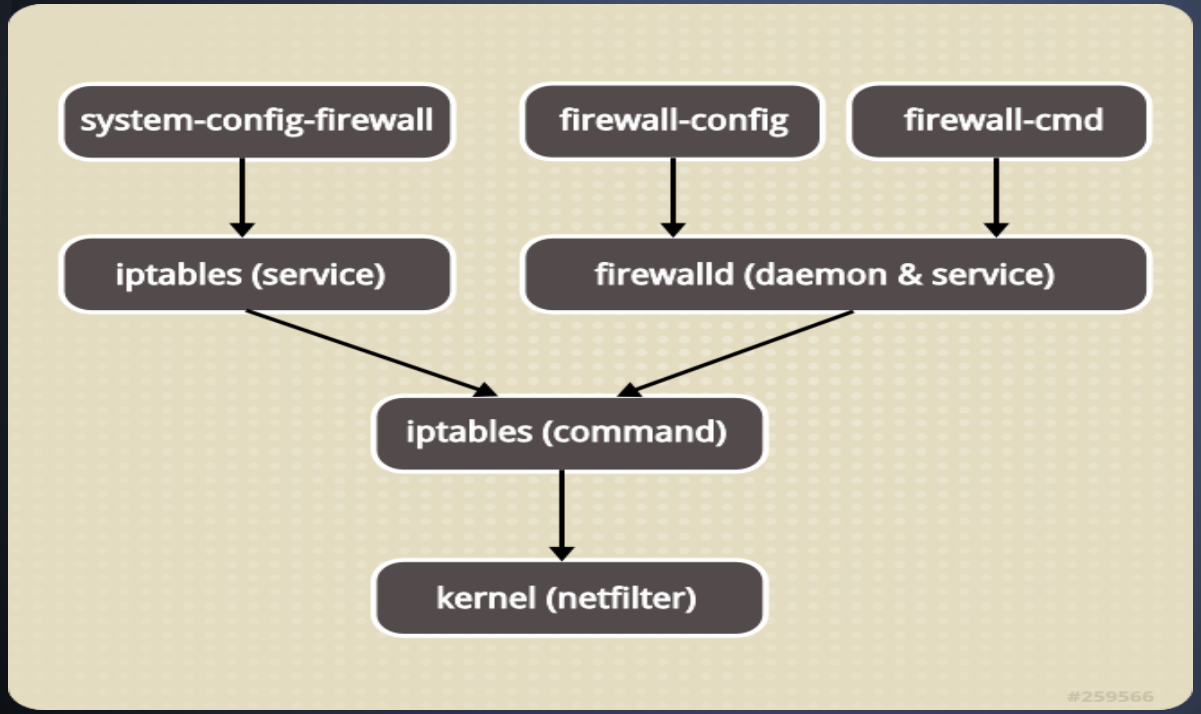
Firewalld

Jiří Popelka

Overview

- introduction
- features
- how to use it
- debugging

firewalld vs. iptables service



iptables/system-config-firewall

- like NM vs. ‘network’ service
- static, i.e. restart with every change
- libvirt
  - own firewall rules
  - iptables’ restart flushes libvirt’s rules

Why dynamic ?

- runtime (in place) changes
- changes announced via D-Bus signals
- other services (libvirt) informed about restart

Configuration

- permanent
  - on disk, active after restart
  - /usr/lib/firewalld/[zones|services]
  - /etc/firewalld/
- runtime
  - in place, active immediately
  - until restart
  - rhel-7.1: runtimeToPermanent
- D-Bus (for applications)

services

- ports
- netfilter helper modules (samba/ftp)
- destination IP address/network (mdns)
- predefined in /usr/lib/firewalld/services/
- customizable
- man firewalld.service

services - examples

```
# cat /usr/lib/firewalld/services/samba-client.xml
<service>
  <short>Samba Client</short>
  <description>To access Windows file and printer sharing networks.</description>
  <port protocol="udp" port="137"/>
  <port protocol="udp" port="138"/>
  <module name="nf_conntrack_netbios_ns"/>
</service>

# cat /usr/lib/firewalld/services/mdns.xml
<service>
  <port protocol="udp" port="5353"/>
  <destination ipv4="224.0.0.251" ipv6="ff02::fb"/>
</service>
```

zones

- level of trust of network connection
- ‘home’ vs. ‘pub’
- NetworkManager, NM GUI, ‘ZONE=’ in ifcfg-*
- maybe the most confusing on firewalld
- default zone, /etc/firewalld/firewalld.conf
- man firewalld.zones

zones

- services, ports, ICMP blocks
- forward ports, masquerade
- interfaces - fallback
- /usr/lib/firewalld/zones, /etc/firewalld/zones/
- man firewalld.zone

zones - examples

```
$ cat /usr/lib/firewalld/zones/external.xml
<zone>
  <short>External</short>
  <description>For use on external networks. ...</description>
  <service name="ssh"/>
  <masquerade/>
</zone>
$ cat /usr/lib/firewalld/zones/drop.xml
<zone target="DROP">
  <short>Drop</short>
  <description>Unsolicited incoming network packets are dropped.</description>
</zone>
```

man firewalld.zone

$ man firewalld.zone

<zone [target="ACCEPT|%%REJECT%%|DROP"]>

[<short>short description</short>]

[<description>description</description>]

[<interface name="string"/>]

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

[<service name="string"/>]

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

[<icmp-block name="string"/>]

[<masquerade/>]

[<forward-port port="portid[-portid]" protocol="tcp|udp" [to-port="portid[-portid]"] [to-addr="ipv4address"]/>]

</zone>

Rich Language

- man firewalld.richlanguage
- extends zone elements
- source/destination address
- logging/auditing (limit)
- actions (accept, reject, drop)
- firewall-cmd, firewall-config, XML (permanent)

Rich Language

rule
  [source]
  [destination]
  service | port | protocol | icmp-block | masquerade | forward-port
  [log]
  [audit]
  [accept | reject | drop]

Direct interface

- direct access to ip(6)tables
- knowledge of tables,chains,commands,targets
- cli, gui, xml (man firewall.direct)
- chain: ipv table name
- rule: ipv table chain args
  - chain_direct if built-in chain
- passthrough: ipv args
  - no special (_direct) chains like with rule
  - does not ‘remember’, just pass-through

Lockdown

- lock settings
- whitelist - commands, contexts, users
- man firewalld.lockdown-whitelist
- /etc/firewalld/lockdown-whitelist.xml

```
<command name="/usr/bin/python -Es /usr/bin/firewall-config"/>
<user id="0"/>
<selinux context="system_u:system_r:virtd_t:s0-s0:c0.c1023"/>
<selinux context="system_u:system_r:NetworkManager_t:s0"/>
```

firewall-cmd examples

--get-default-zone, --set-default-zone=work

--get-services, --list-all[-zones]

--add-service=http, --add-port=80/tcp

[--zone=<zone>] [--permanent]

--reload

--runtime-to-permanent (new in 7.1)

--add-rich-rule=’rule family=ipv4 source address=192.168.2.3 drop’

--direct --passthrough ipv4 -I INPUT -j ACCEPT

iptables service -> firewalld

- configuration created via system-config-firewall
  - firewall-offline-cmd (no arguments)
- hand written /etc/sysconfig/iptables
  - no automated tool
  - either create firewalld conf. from scratch
  - or keep using iptables service

debugging

- FIREWALLD_ARGS=--debug=2 > /etc/sysconfig/firewalld
- /var/log/firewalld
- iptables -L, iptables-save

iptables-save

-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -j INPUT_direct

-A INPUT -j INPUT_ZONES

-A INPUT_ZONES -i wlp4s2 -g IN_home

-A INPUT_ZONES -g IN_public

-A IN_home -j IN_home_log

-A IN_home -j IN_home_deny

-A IN_home -j IN_home_allow

-A INPUT -p icmp -j ACCEPT

-A INPUT -j REJECT --reject-with icmp-host-prohibited