Firewalld

Thomas Woerner
Red Hat, Inc.

NFWS 2015
June 22

Introduction

- Central firewall management service using D-Bus
- Supports
  - IPv4: iptables
  - IPv6: ip6tables
  - Bridges: ebtables
- Sends signals for all actions over D-Bus
- Run-time and persistent configuration
- Default configuration (fallbacks)
- Services
- Zones

Services

- Options
  - Port (ranges) with protocol
  - Netfilter helper modules
  - Destination address (range) for IPv4 and/or IPv6
- Nearly 70 built-in services
- Adaptable via D-Bus, files

Service Examples

dns

```
<service>
  <port protocol="tcp" port="53"/>
  <port protocol="udp" port="53"/>
</service>
```

https

```
<service>
  <port protocol="tcp" port="443"/>
</service>
```

tftp

```
<service>
  <port protocol="udp" port="69"/>
  <module name="nf_conntrack_tftp"/>
</service>
```

dhcpv6-client

```
<service>
  <port protocol="udp" port="546"/>
  <destination ipv6="fe80::/64"/>
</service>
```

Zones

- Options
  - Services
  - Ports (ranges) with protocols
  - Rich language rules
  - Internet Control Message Protocol (ICMP) blocks
  - Masquerading
  - Port/packet forwardings
- Completely adaptable

Zones

- Zone can be seen as a complete firewall
- Initial default: public
- One zone per connection with NetworkManager
  - `ZONE=<name>` in ifcfg file or NM configuration
- One zone per interface or source address (range)
- Internal firewall rule ordering according to action
  - log → deny → allow

Zone Examples

public

```
<zone>
  <service name="ssh"/>
  <service name="dhcpv6-client"/>
</zone>
```

drop

```
<zone target=”DROP”>
</zone>
```

custom

```
<zone>
  <interface name="em2"/>
  <source address="10.0.1.0/24"/>
  <service name="ssh"/>
  <service name="ipp-client"/>
  <service name="dhcpv6-client"/>
  <rule><protocol value="ah"/><accept/></rule>
</zone>
```

Rich Rules

- Source address (range): optional
- Destination address (range): optional
- One Element
  - Service, port, protocol, icmp-block, masquerade, forward-port
  - Limit: optional
- Logging: optional
  - Log and/or audit
  - Limit: optional
- One Action: accept, reject, drop
  - Limit optional

Rich Rules • Examples

Allow new IPv4 and IPv6 connections for service ftp and log 1 per minute using audit

```
rule service name="ftp" log limit value="1/m" audit accept
```

Allow new IPv4 connections from address 192.168.0.0/24 for service tftp, log 1 per minute using syslog

```
rule family="ipv4" source address="192.168.0.0/24" service name="tftp"
log prefix="tftp" level="info" limit value="1/m" accept
```

New IPv6 connections from 1:2:3:4:6:: to service radius are rejected and logged at a rate of 3 per minute. New IPv6 connections from other sources are accepted

```
rule family="ipv6" source address="1:2:3:4:6::" service name="radius" log
prefix="radius" level="info" limit value="3/m" reject
rule family="ipv6" service name="radius" accept
```

Direct Interface

- More complex rules, globally, not in zones
- Rules
  - ip*tables/ebtables syntax
  - priority for rule ordering
  - added to _direct chains for netfilter built-in chains or own chains
- Passthrough rules (For highly experienced users)
  - Used by libvirt and docker

Direct Interface Examples

Create custom chain blacklist in raw table for IPv4, log and DROP

```
firewall-cmd --direct --add-chain ipv4 raw blacklist
firewall-cmd --direct --add-rule ipv4 raw blacklist 0 -m limit --limit
1/min -j LOG --log-prefix “blacklist: “
firewall-cmd --direct --add-rule ipv4 raw blacklist 1 -j DROP
```

Add black listed IPv4 address to blacklist

```
firewall-cmd --direct --add-rule ipv4 raw PREROUTING 0 -s 192.168.1.0/24
-j blacklist
```

Persistent direct configuration

```
<?xml version="1.0" encoding="utf-8"?>
<direct>
  <chain ipv="ipv4" table="raw" chain="blacklist"/>
  <rule ipv="ipv4" table="raw" chain="PREROUTING" priority="0">-s
192.168.1.0/24 -j blacklist</rule>
  <rule ipv="ipv4" table="raw" chain="blacklist" priority="0">-m limit
--limit 1/min -j LOG --log-prefix "blacklist: "</rule>
  <rule ipv="ipv4" table="raw" chain="blacklist" priority="1">-j
DROP</rule>
</direct>
```

Future Plans

- Tracing mode
- ipset support
- Security environments (zone interaction)
- Direct rules in zones
- nftables support

More Information

- Web:
  - http://www.firewalld.org/
- Documentation: http://fedoraproject.org/wiki/FirewallD
- Man pages for firewalld, firewalld.zone, firewalld.service, firewalld.direct, firewalld.richlanguage, firewall-cmd, ..
- Repository: git://github.com/t-woerner/firewalld
- irc channel: #firewalld on freenode
- Mailing lists:
  - firewalld-users@lists.fedorahosted.org
  - firewalld-devel@lists.fedorahosted.org