Dynamic firewall with firewalld

Thomas Wörner
Red Hat

DevConf.cz 2013
2013-02-24
Overview

- Introduction
- Configuration
- Services
- Zones
- Use of Zones
- Direct Interface
- D-BUS
- Projects using firewalld
- Work in Progress
- Questions and Answers
Introduction

- Why dynamic?
  - system-config-firewall / lokkit
  - In place changes
  - open connections
  - no service restarts
  - helper modules loaded as needed
Configuration

- Runtime and persistent configuration
- Configuration using the D-BUS interface
- Config files
- Default configuration: /usr/lib/firewalld
- System configuration: /etc/firewalld
- D-BUS signals for all changes
- IPv4 and IPv6 simultaneous
Services

- Options
  - port (ranges) with protocol
  - helper modules
  - destination address ipv4 and/or ipv6
- Predefined services: 29
- Customizable
Example services

samba

    <service>
      <port protocol="udp" port="137"/>
      <port protocol="udp" port="138"/>
      <port protocol="tcp" port="139"/>
      <port protocol="tcp" port="445"/>
      <module name="nf_conntrack_netbios_ns"/>
    </service>

mdns/avahi

    <service>
      <port protocol="udp" port="5353"/>
      <destination ipv4="224.0.0.251" ipv6="ff02::fb"/>
    </service>
Zones

- Options
  - Services
  - Port (ranges) with protocol
  - Internet Control Message Protocol (ICMP) blocks
  - Masquerading
  - Port/packet forwardings
- Predefined zones: block, dmz, drop, external, home, internal, public, trusted, work
- Customizable
Example zones

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

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

drop
<zone immutable="True" target="DROP">
</zone>
Use of Zones

- initial default: public
- one zone per connection/interface
- ZONE= in ifcfg or NM config
- single connection: according to trust level of environment
- more connections: decide per connection
- portable system: keep safe default
Direct Interface

- chains
- more complex firewall rules with priorities
- ipv4, ipv6 and bridges
- placed in _direct sub chains in built-in chains
- passthrough: ip*tables and ebtables calls
- persistent rules not supported
D-BUS

- Full featured
- Runtime and persistent configuration
- Used by all tools, also command line client firewall-cmd
- Uses Policykit
Projects using firewalld

- NetworkManager (applet: KDE, general)
- libvirt
- system-config-printer
- partly: gnome printer configuration
Work in Progress

- Rich language
  
  Important additions:
  
  - log, audit support
  - source.
  - explicit ipv4 or ipv6 rules
  - special rules for libvirt

- Lockdown: Forbid changes to the firewall, with application white list

- Allow persistent direct rules

- IPv6 NAT support
Information

- Web: http://fedorahosted.org/firewalld/
- Documentation: http://fedoraproject.org/wiki/FirewallD
- Repository: git://git.fedorahosted.org/git/firewalld
- irc channel: #firewalld on freenode
- Mailing lists:
  - firewalld-users@lists.fedorahosted.org
  - firewalld-devel@lists.fedorahosted.org
Questions and Answers