Firewalld

Seminario de Desarrollo de Software - Casa Central.

Maximiliano Osorio
mosorio@inf.utfsm.cl

Universidad Técnica Federico Santa María

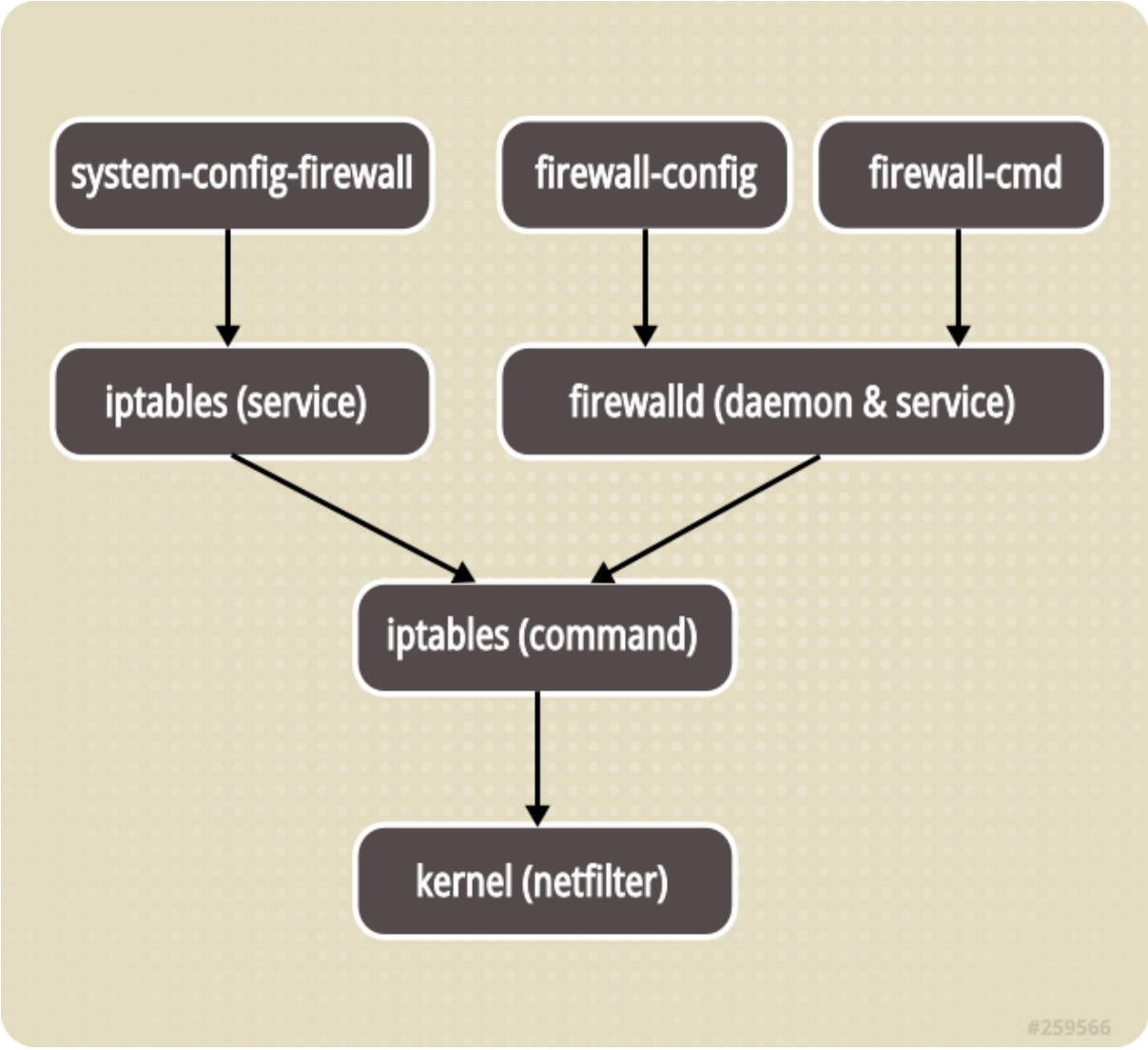
26 de septiembre de 2017

firewalld

Firewalld es metodo por defecto de RHEL 7 para el manejo de firewall.

- Es dinamico porque las reglas se aplican de forma inmediata y sin necesidad de reinicio.
- Soporta IPv4 y IPv6.
- Utiliza iptables (tool) para comunicar con el kernel (netfilter)

Firewalld


system-config-firewall
firewall-config
firewall-cmd
iptables (service)
firewalld (daemon & service)
iptables (command)
kernel (netfilter)
#259566

Zones

firewalld separa todo el *incoming traffic* por red en zonas, cada zona tiene un set de reglas.

- **drop** Any incoming network packets are dropped, there is no reply. Only outgoing network connections are possible.
- **block** Any incoming network connections are rejected with an icmp-host-prohibited message for IPv4 and icmp6-adm-prohibited for IPv6. Only network connections initiated from within the system are possible.
- **public** For use in public areas. You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.
- **external** For use on external networks with masquerading enabled especially for routers. You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.

Zonas

- **dmz**
  For computers in your demilitarized zone that are publicly-accessible with limited access to your internal network. Only selected incoming connections are accepted.
- **work** For use in work areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.
- **home**
  For use in home areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.
- **internal** For use on internal networks. You mostly trust the other computers on the networks to not harm your computer. Only selected incoming connections are accepted.
- **trusted** All network connections are accepted.

Servicios

Existen servicios ya definidos

```
~]# ls /usr/lib/firewalld/services/
```

```
firewall-cmd --get-services
RH-Satellite-6 amanda-client bacula bacula-
    client dhcp dhcpv6 dhcpv6-client dns ftp high
    -availability http https imaps ipp ipp-client
     ipsec kerberos kpasswd ldap ldaps libvirt
    libvirt-tls mdns mountd ms-wbt mysql nfs ntp
    openvpn pmcd pmproxy pmwebapi pmwebapis pop3s
     postgresql proxy-dhcp radius rpc-bind samba
    samba-client smtp ssh telnet tftp tftp-client
     transmission-client vnc-server wbem-https
```

Quickstart

```
~]# yum -y install firewalld
~]# systemctl stop firewalld
~]# systemctl disable firewalld
~]# systemctl start firewalld
~]# systemctl enable firewalld
```

Status

```
~]# systemctl status firewalld
~]$ firewall-cmd --state
running
```

```
~]$ firewall-cmd --state
running
```

Zonas

Añadir un interfaz a una zona.

```
~]# firewall-cmd --zone=public --add-interface=
    em1
```

Zonas

Mostrar las zonas activas

```
~]$ firewall-cmd --get-active-zones
public
  interfaces: em1
```

Zonas

Mostrar la zona de una interfaz

```
~]$ firewall-cmd --get-zone-of-interface=em1
public
```

Zonas

Listas las interfaces en una zona

```
~]# firewall-cmd --zone=public --list-
   interfaces
em1 wlan0
```

Listar

```
firewall-cmd --zone=public --list-ports
firewall-cmd --zone=public --list-services
```

Zonas

Listar servicios y puertos en una zona

```
~]# firewall-cmd --zone=public --list-all
public
  interfaces:
  services: mdns dhcpv6-client ssh
  ports:
  forward-ports:
  icmp-blocks: source-quench
```

Servicios

Listar servicios

```
~]# firewall-cmd --permanent --get-services
```

Añadir un puerto

```
~]# firewall-cmd --zone=dmz --add-port=8080/tcp
~]# firewall-cmd --zone=public --add-port
   =5060-5061/udp
```

Añadir un servicio

```
~]# firewall-cmd --zone=work --add-service=smtp
```

Remueve un servicio

```
~]# firewall-cmd --zone=work --remove-service=
    smtp
```

Permanent

Si quiere que la regla se mantenga después de un reboot, se añade **–permanent** y es **necesario** el reload

```
~]# firewall-cmd --permanent --zone=work --
   remove-service=smtp
~]# firewall-cmd --reload
```

Esto no rompera las conexiones establecidas, si desea hacer eso debe utiliza **–complete-reload**, que va a cortar todas las conexiones establecidas.

Añadir un puerto para ciertos destino

172.25.1.0/24: representa a red de los hosts 172.25.1.0-255.

```
~]# firewall-cmd --zone=work --add-port=8080/
   tcp --add-source 172.25.X.0/24
```

Rich rules

Con el *rich languague*, se pueden crear reglas complejas en una forma sencilla utilizando zonas.

```
firewall-cmd [--zone=zone] --add-rich-rule='
   rule' [--timeout=seconds]
firewall-cmd [--zone=zone] --query-rich-rule='
   rule'
firewall-cmd [--zone=zone] --remove-rich-rule='
   rule'
```

rich rules

```
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 ]
     [ action ]
```

rich rules

```
firewall-cmd  --add-rich-rule='rule family=ipv4
    source address=10.10.15.123/32 reject'
firewall-cmd  --add-rich-rule='rule family=ipv4
    source address=10.10.15.123/32 drop'
firewall-cmd  --add-rich-rule='rule service
   name="ssh" log prefix="SSH PRUEBA!!" level="
   notice" accept'
firewall-cmd  --add-rich-rule='rule  to-port
   ="80" log prefix="HTTP PRUEBA!!" level="
   notice" log limit value="1/m" accept'
```

direct rules

```
# firewall-cmd --permanent --direct --add-rule
   ipv4 filter OUTPUT 0 -p tcp -m tcp --dport=22
    -j ACCEPT
success
# firewall-cmd --permanent --direct --add-rule
   ipv4 filter OUTPUT 1 -p tcp -m tcp --sport=22
    -j ACCEPT
success
# firewall-cmd --permanent --direct --add-rule
   ipv4 filter OUTPUT 9 -j DROP
success
```