SUSE

Introducción a `firewalld`

DESCRIPCIÓN

Descubra `firewalld`, una herramienta fundamental para proteger los servidores y servicios de Linux. Es el mecanismo de defensa de red predeterminado y principal en muchas distribuciones modernas. La gestión intuitiva basada en zonas y las capacidades de configuración dinámica permiten un control preciso sobre el tráfico de red sin interrupción del servicio.

INTENCIÓN

`firewalld` es esencial porque proporciona una forma actual, dinámica y fácil de usar de gestionar la seguridad de la red en sistemas Linux convirtiendo reglas de firewall complejas en zonas y servicios intuitivos.

ESFUERZO

Leer este artículo le llevará unos 30 minutos.

OBJETIVO

Gestionar y mejorar eficazmente la seguridad de un sistema Linux.

REQUISITOS

- Privilegios de `sudo` o `root`, ya que los comandos de `firewalld`, especialmente los que realizan cambios permanentes en las reglas del firewall, requieren privilegios elevados.
- `firewalld` es el firewall por defecto en muchas distribuciones modernas de Linux. Si no está preinstalado en su sistema, debe instalar el paquete `firewalld`.
- Es esencial una comprensión básica del terminal de Linux.

Fecha de publicación: 11 Dic 2025

Contenido

1 Acerca de `firewalld`

`firewalld` es un servicio dinámico de gestión de firewall que proporciona una forma flexible y eficiente de controlar el tráfico de red en sistemas Linux. Permite modificaciones sin interrumpir las conexiones existentes. Estas son las ventajas de usar `firewalld`:

- *Configuración dinámica.* Aplique cambios al instante sin interrumpir las conexiones existentes.
- *Interfaz fácil de usar.* Las zonas y los servicios simplifican las complejas reglas de firewall.
- *Abstracción.* No hay necesidad de manipular directamente reglas de `nftables` para los escenarios habituales.
- *Configuración persistente.* Fácil gestión de reglas que sobreviven a los reinicios.
- *Configuración persistente.* De forma predeterminada, `firewalld` opera bajo un principio `deny-all`, bloqueando todo el tráfico entrante a menos que se permita explícitamente.

1.1 Zonas de `firewalld`

Una zona de firewall es un conjunto predefinido de reglas que dictan cómo se maneja el tráfico de red entrante y saliente para una interfaz de red específica o una dirección IP de origen. Cada zona representa un nivel diferente de confianza para la red a la que está asociada. Puede aplicar diferentes directivas de seguridad en función de dónde se origine la conexión de red.

Las zonas son como perfiles de seguridad. Por ejemplo, querrá aplicar diferentes reglas de firewall para una conexión Wi-Fi pública y su red doméstica segura. Las zonas de `firewalld` permiten definir estos conjuntos distintos de reglas y aplicarlas en consecuencia. Una conexión de red está sujeta a las reglas de una sola zona de `firewalld`. Una zona de `firewalld` puede tener muchas interfaces de red o direcciones IP de origen.

Las zonas predefinidas se guardan en el directorio `/usr/lib/firewalld/zones/`. Por ejemplo:

```
> /usr/lib/firewalld/zones ls
block.xml  dmz.xml  docker.xml  drop.xml  external.xml  home.xml  internal.xml  nm-
shared.xml  public.xml  trusted.xml  work.xml
```

Estas son algunas de las configuraciones predeterminadas de las zonas predefinidas:

`drop`

- *Nivel de confianza:* sin confianza alguna.
- *Comportamiento:* todos los paquetes de red entrantes se descartan sin ninguna respuesta. Solo se permiten las conexiones salientes iniciadas desde el sistema. Esto proporciona un modo de "sigilo" en el que el sistema parece no existir para los atacantes externos.
- *Caso práctico:* se utiliza para conseguir el máximo sigilo y seguridad, ignorando por completo el tráfico no deseado. Adecuado como configuración predeterminada estricta para un servidor que nunca debe aceptar conexiones entrantes.

`block`

- *Nivel de confianza:* muy bajo.
- *Comportamiento:* todas las conexiones de red entrantes se rechazan con un mensaje `icmp-host-prohibited` para IPv4 y `icmp6-adm-prohibited` para IPv6. Se informa al remitente de que su conexión se ha rechazado explícitamente. Solo se permiten las conexiones salientes iniciadas desde el sistema.
- *Caso práctico:* se aplica cuando desea indicar explícitamente a los remitentes que se están bloqueando sus intentos de conexión.

`public`

- *Nivel de confianza:* sin confianza o es público.
- *Comportamiento:* representa a las redes públicas que no son de confianza en las que no se confía en otros sistemas. Solo se aceptan de forma predeterminada las conexiones entrantes seleccionadas, por ejemplo, SSH, cliente DHCPv6, etc.
- *Caso práctico:* es la zona predeterminada común para interfaces conectadas directamente a Internet, como la interfaz WAN del enrutador. También se usa cuando hay una conexión a una red en la que no se tiene control sobre otros dispositivos.

`external`

- *Nivel de confianza:* externa con enmascaramiento.
- *Comportamiento:* está diseñada para redes externas cuando el firewall actúa como gateway o router. Por lo general, el enmascaramiento NAT está habilitado de forma predeterminada. Solo se aceptan las conexiones entrantes seleccionadas, bajo el supuesto de que no confía en otros sistemas de esta red.
- *Caso práctico:* se utiliza cuando su equipo Linux actúa como router, conectando una red privada interna a la Internet pública. La interfaz externa se coloca en esta zona para ocultar la topología de red interna y permitir que los clientes internos accedan a recursos externos como Internet.

`dmz (Demilitarized Zone)`

- *Nivel de confianza:* acceso público limitado.
- *Comportamiento:* para sistemas en una zona DMZ que son de acceso público pero con acceso limitado a la red interna. Solo se aceptan conexiones entrantes seleccionadas. Generalmente, por defecto incluye SSH y otros servicios que expone.
- *Caso práctico:* es adecuada para servidores públicos como servidores Web, de correo y DNS. Estos servidores están expuestos intencionadamente a Internet, pero están aislados de sus redes internas más confiables. Resulta útil cuando se desea hospedar servicios que deben ser accesibles a través de Internet y minimizar el riesgo para la infraestructura interna principal.

`work`

- *Nivel de confianza:* mayormente confiable (ambiente de trabajo).
- *Comportamiento:* en un entorno de trabajo, normalmente confía en otros equipos de la red. Permite conexiones entrantes seleccionadas que son comunes en un entorno de trabajo, como SSH y cliente DHCPv6.
- *Caso práctico:* adecuada para redes y sistemas de oficina en una LAN corporativa.

`home`

- *Nivel de confianza:* mayormente confiable (ambiente doméstico).
- *Comportamiento:* en un entorno doméstico, confía principalmente en los otros sistemas de la red. Permite más servicios que las zonas públicas o externas, que a menudo incluyen servicios de red doméstica comunes como el uso compartido de archivos, servidores multimedia e impresoras, junto con el cliente SSH y DHCPv6.
- *Caso práctico:* es la mejor opción para redes domésticas y pequeñas configuraciones de oficinas en casa.

`trusted`

- *Nivel de confianza:* el más alto.
- *Comportamiento:* todas las conexiones de red se aceptan sin ningún filtro. El firewall no se implementa para las conexiones asignadas a esta zona.
- *Caso práctico:* está reservada para conexiones de alta confianza.

1.2 Directivas y reglas de `firewalld`

Las directivas de `firewalld` proporcionan una forma más avanzada y flexible de gestionar el tráfico de red que las zonas tradicionales. Permiten definir reglas complejas que especifican el origen y el destino del tráfico, los servicios, los puertos y acciones como aceptar, rechazar y eliminar conexiones. Estas directivas son útiles para configurar enrutamiento complejo, reenvío de puertos o crear segmentos de red aislados dentro de un solo host.

Las directivas de `firewalld` aprovechan las zonas para definir conjuntos de reglas. Aplican reglas con estado y en una dirección, lo que significa que define el flujo de tráfico en una dirección, y `firewalld` permite implícitamente la vía de retorno. Estas directivas vinculan una zona de entrada (donde entra el tráfico) con una zona de salida (donde sale el tráfico). Esto define la vía y la dirección específicas a las que se aplican las reglas de una directiva. Puede ver las directivas, por ejemplo:

```
> /usr/lib/firewalld/policies ls
allow-host-ipv6.xml
```

Las reglas de firewall permiten controlar con precisión el tráfico de red, permitiéndolo o bloqueándolo para proteger su sistema de amenazas de seguridad. También definen ciertos criterios basados en varios atributos, como direcciones IP de origen y destino, puertos e inter-

faces de red. `firewalld` segrega las reglas de firewall en zonas y directivas. Cada zona de `firewalld` tiene un conjunto único de reglas que dicta los permisos de tráfico para sus interfaces de red asociadas.

1.3 Servicios y puertos

Los servicios se recomiendan cuando hay un servicio predefinido disponible. Por ejemplo, en lugar de recordar que el protocolo HTTP usa el puerto TCP 80, simplemente puede añadir el servicio `http`. Se consigue así una menor propensión a errores y más facilidad para la administración. Utilice puertos cuando un servicio no esté predefinido o cuando utilice un puerto personalizado para un servicio. Puede ver los servicios y puertos activos para las zonas predeterminadas con lo siguiente:

```
> sudo firewall-cmd --list-services
```

```
> sudo firewall-cmd --list-ports
```

2 Gestión de reglas y zonas de firewall

Puede configurar zonas de `firewalld` y sus reglas con la interfaz gráfica Web Cockpit o con la utilidad de línea de comandos **`firewall-cmd`**.

2.1 Gestión de reglas y zonas de firewall con la utilidad `firewalld-cmd`

Puede utilizar la interfaz de línea de comandos para gestionar zonas de `firewalld`.

2.1.1 Adición de zonas de `firewalld`

Para añadir una zona de `firewalld` nueva:

1. Cree una nueva zona, por ejemplo:

   ```
   > sudo firewall-cmd --permanent --new-zone=test
   ```

2. Establezca el nivel de confianza de la zona que definirá el comportamiento predeterminado:

```
> sudo firewall-cmd --permanent --zone=example --set-target=trusted
```

3. Vuelva a cargar el servicio `firewalld` para aplicar la nueva configuración:

```
> sudo firewall-cmd --reload
```

2.1.2 Adición de un servicio a una zona

Para añadir un servicio a una zona:

1. Muestre todos los servicios para comprobar si su servicio ya está predefinido:

```
> sudo firewall-cmd --get-services
      0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-
client amqp amqps anno-1602
      anno-1800 apcupsd audit ausweisapp2 bacula bacula-client bareos-director
 bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet
 bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-
agent civilization-iv civilization-v cockpit collectd condor-collector cratedb ctdb
 dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic
 dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client
 etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-
ldaps freeipa-replication freeipa-trust ftp galera
      ganglia-client ganglia-master git gpsd grafana gre http http3 https ident imap
 imaps ipfs ipp ipp-client ipsec irc ircs
      [...]
```

2. Puede añadir un servicio temporalmente para la sesión de tiempo de ejecución o de forma permanente, por ejemplo:

```
> sudo  firewall-cmd --zone=public --add-service=http
```

```
> sudo  firewall-cmd --zone=public --permanent --add-service=http
```

   El indicador `--permanent` garantiza que el cambio persista en todos los reinicios.

3. Vuelva a cargar el servicio `firewalld` para aplicar la nueva configuración:

```
> sudo firewall-cmd --reload
```

4. Compruebe los resultados:

```
> sudo firewall-cmd --zone=public --list-services
```

2.1.3 Adición de un puerto a una zona

Si la aplicación no tiene un servicio predefinido, puede abrir un puerto específico o un intervalo de puertos.

1. Puede añadir un puerto temporalmente para la sesión de tiempo de ejecución o de forma permanente, por ejemplo:

```
> sudo  firewall-cmd --zone=public --add-port=8080/tcp
```

```
> sudo  firewall-cmd --zone=public --permanent --add-port=8080/tcp
```

   El indicador `--permanent` garantiza que el cambio persista en todos los reinicios.

2. Vuelva a cargar el servicio `firewalld` para aplicar la nueva configuración:

```
> sudo firewall-cmd --reload
```

3. Compruebe los resultados:

```
> sudo firewall-cmd --zone=public --list-ports
```

2.1.4 Supresión de zonas de `firewalld`

Para suprimir una zona:

1. Compruebe que la zona no es la predeterminada o no está en uso:

```
> sudo  firewall-cmd --get-default-zone
```

   Si la zona está en uso o es la predeterminada, establezca una zona diferente, por ejemplo:

```
> sudo  firewall-cmd --set-default-zone=NEW_DEFAULT_ZONE
```

2. Compruebe si hay alguna interfaz de red vinculada a la zona:

```
> sudo firewall-cmd --zone=ZONE_TO_BE_DELETED --list-all
```

3. El campo `interfaces` del resultado muestra todas las interfaces. Estas interfaces deben reasignarse a otra zona. Por ejemplo:

```
> sudo firewall-cmd --zone=public --permanent --change-interface=ITERFACE_NAME
```

4. Suprima la zona:

```
> sudo firewall-cmd --permanent --delete-zone=ZONE_TO_BE_DELETED
```

5. Vuelva a cargar el servicio `firewalld` para aplicar la nueva configuración:

```
> sudo firewall-cmd --reload
```

2.2 Gestión de reglas y zonas de firewall con Cockpit

Cockpit permite crear nuevas zonas o actualizar las existentes. En la configuración del firewall, puede añadir servicios a una zona o permitir el acceso a los puertos.

Nota: el servicio de Cockpit es obligatorio

No elimine el servicio Cockpit de la zona de firewall por defecto, ya que podría bloquearse y desconectarse del servidor.

2.2.1 Adición de zonas de firewall

La *zona pública* es la zona de firewall por defecto. Para añadir una zona nueva, haga lo siguiente:

PROCEDIMIENTO 1: ADICIÓN DE NUEVAS ZONAS DE FIREWALL

1. Diríjase a la página *Redes*.
2. Haga clic en *Editar reglas y zonas*.
3. Haga clic en *Añadir zona*.
4. Seleccione *Nivel de confianza*. Cada nivel de confianza de las conexiones de red tiene un conjunto predefinido de servicios incluidos (el servicio de Cockpit se incluye en todos los niveles de confianza).

5. Defina las direcciones permitidas dentro de la zona. Seleccione uno de los valores:
    - *En toda la subred* para permitir todas las direcciones de la subred.
    - *Rango* es una lista separada por comas de direcciones IP con el prefijo de encaminamiento; por ejemplo, 192.0.2.0/24, 2001:db8::/32.
6. Continúe con *Añadir zona*.

2.2.2 Adición de servicios y puertos permitidos a una zona

Puede añadir servicios a una zona de firewall existente como se describe a continuación:

PROCEDIMIENTO 2: ADICIÓN DE SERVICIOS A UNA ZONA DE FIREWALL

1. Diríjase a la página *Redes*.
2. Haga clic en *Editar reglas y zonas*.
3. Haga clic en *Añadir servicios*.
4. Para añadir un servicio, seleccione *Servicios* y seleccione los servicios de la lista.
5. Para permitir puertos personalizados, seleccione *Puertos específicos* y especifique el valor del puerto para UDP o TCP. Puede asignar un identificador a este puerto.
6. Para confirmar los cambios, haga clic en *Añadir servicios* o *Añadir puertos*, respectivamente.

3 Comandos comunes de `firewalld`

La herramienta de línea de comandos **`firewall-cmd`** se utiliza para configurar y gestionar el daemon `firewalld`. Es una utilidad potente y dinámica que permite la creación, modificación y eliminación de reglas de firewall sin necesidad de reiniciar el servicio por completo, lo que evita que las conexiones de red activas se interrumpan.

Ejemplos comunes del comando **`firewall-cmd`**:

- Comprobar si `firewalld` se está ejecutando. El resultado es `running`, `not running` o `RUNNING_BUT_FAILED`. Por ejemplo:

```
> sudo firewall-cmd --state
```

```
running
```

- Mostrar todas las zonas disponibles, por ejemplo:

```
> sudo firewall-cmd --get-zones
 block dmz docker drop external home internal nm-shared public trusted work
```

- Ver la zona predeterminada, por ejemplo:

```
> sudo firewall-cmd --get-default-zone
public
```

- Ver las zonas activas y las asignadas, por ejemplo:

```
> sudo firewall-cmd --get-active-zones
docker
interfaces: docker0
public (default)
interfaces: lo enp1s0
```

- Ver todas las reglas de la zona predeterminada, por ejemplo:

```
> sudo firewall-cmd --list-all
public (default, active)
target: default
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
interfaces: enp1s0 lo
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
rule family="ipv4" source address="192.168.1.100" service name="ssh" accept
```

- Ver todas las reglas de una zona específica, por ejemplo:

```
> sudo firewall-cmd --zone=public --list-all
public (default, active)
target: default
```

```
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
interfaces: enp1s0 lo
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
rule family="ipv4" source address="192.168.1.100" service name="ssh" accept
```

- Mostrar todos los servicios predefinidos disponibles, por ejemplo:

```
> sudo firewall-cmd --get-services
  0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client
 amqp amqps anno-1602 anno-1800
  apcupsd audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon
 bareos-storage bb bgp bitcoin bitcoin-rpc
  bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon
 cfengine checkmk-agent civilization-iv civilization-v
  cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp
 dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls
  docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server
 factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap
  freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-
master git gpsd grafana gre http http3 https ident imap imaps
  ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect
 kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
  kube-control-plane kube-control-plane-secure kube-controller-manager kube-
controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-
secure
  [...]
```

- Mostrar los servicios permitidos actualmente en la zona predeterminada, por ejemplo:

```
> sudo firewall-cmd --list-services
cockpit dhcpv6-client ssh
```

- Añadir un servicio a la zona predeterminada de forma permanente, por ejemplo:

```
> sudo firewall-cmd --permanent --add-service=http
success
```

- Eliminar un servicio de forma permanente, por ejemplo:

```
> sudo firewall-cmd --permanent --remove-service=http
success
```

- Mostrar los puertos abiertos actualmente en la zona predeterminada, por ejemplo:

```
> sudo firewall-cmd --list-ports
22/tcp
```

- Abrir un puerto TCP específico temporalmente, por ejemplo:

```
> sudo firewall-cmd --add-port=8080/tcp
success
```

- Eliminar un puerto abierto de forma permanente, por ejemplo:

```
> sudo firewall-cmd --permanent --remove-port=8080/tcp
success
```

- Añadir una interfaz a una zona específica temporalmente, por ejemplo:

```
> sudo firewall-cmd --zone=trusted --add-interface=eth1
success
```

4 Resolución de problemas de `firewalld`

Para solucionar problemas de `firewalld` hay que comprobar su estado, verificar las reglas y reiniciar o recargar el servicio. Si tiene problemas, puede habilitar la depuración, examinar los registros y ajustar las reglas de firewall según sea necesario.

4.1 Comprobación del estado de `firewalld`

- Use el comando **`systemctl status`**. Por ejemplo:

```
> sudo systemctl status  firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
Active: active (running) since Thu 2025-07-17 09:47:36 CEST; 5min ago
Invocation: a7ea482f16d2431fa92d6204c297ebd9
```

```
Docs: man:firewalld(1)
Main PID: 921 (firewalld)
Tasks: 2
CPU: 262ms
CGroup: /system.slice/firewalld.service
        └─921 /usr/bin/python3.13 /usr/sbin/firewalld --nofork --nopid
```

- El comando **`firewall-cmd --state`** hace una comprobación rápida e indica si el estado es `running`, `not running` o `RUNNING_BUT_FAILED`. Por ejemplo:

```
> sudo firewall-cmd --state
running
```

- Si `firewalld` no se está ejecutando, use el comando **`systemctl start firewalld`**.

```
> sudo  systemctl start firewalld
```

- Si el servicio `firewalld` está enmascarado, desenmascárelo y, luego, habilítelo e inícielo. Por ejemplo:

```
> sudo systemctl unmask --now firewalld
```

```
> sudo systemctl enable firewalld
```

```
> sudo systemctl start firewalld
```

4.2 Comprobación de reglas de `firewalld`

- El comando **`firewall-cmd --list-all-zones`** muestra todas las zonas y sus reglas, por ejemplo:

```
> sudo firewall-cmd --list-all-zones
        block
          target: %%REJECT%%
          ingress-priority: 0
          egress-priority: 0
          icmp-block-inversion: no
          interfaces:
          sources:
          services:
          ports:
          protocols:
          forward: yes
```

```
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

dmz
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

docker (active)
  target: ACCEPT
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  [...]
```

- El comando **`firewall-cmd --list-ports`** muestra los puertos abiertos, por ejemplo:

```
> sudo firewall-cmd --list-ports
22/tcp
```

- El comando **`firewall-cmd --zone=`***`YOUR_ZONE`* **`--list-all.`** muestra los puertos para zonas específicas, por ejemplo:

```
> sudo firewall-cmd --zone=dmz --list-all
               dmz
                 target: default
                 ingress-priority: 0
                 egress-priority: 0
                 icmp-block-inversion: no
                 interfaces:
                 sources:
                 services: ssh
```

```
                ports:
                protocols:
                forward: yes
                masquerade: no
                forward-ports:
                source-ports:
                icmp-blocks:
                rich rules:
```

4.3 Depuración de `firewalld`

- Habilite la depuración en `/etc/sysconfig/firewalld` añadiendo `--debug=[level]` a `FIREWALLD_ARGS`. Por ejemplo:

```
> sudo  vi /etc/sysconfig/firewalld
# firewalld command line args
# possible values: --debug
FIREWALLD_ARGS=--debug=[level]
```

- Ejecute `firewalld` con la opción `--debug`, por ejemplo:

```
> sudo firewalld --nofork --debug
2025-07-23 11:10:05 DEBUG1: start()
2025-07-23 11:10:05 DEBUG1: Loading firewalld config file '/etc/firewalld/
firewalld.conf'
2025-07-23 11:10:05 DEBUG1: CleanupOnExit is set to 'True'
2025-07-23 11:10:05 DEBUG1: CleanupModulesOnExit is set to 'False'
2025-07-23 11:10:05 DEBUG1: IPv6 rpfilter is enabled
2025-07-23 11:10:05 DEBUG1: LogDenied is set to 'off'
2025-07-23 11:10:05 DEBUG1: FirewallBackend is set to 'nftables'
2025-07-23 11:10:05 DEBUG1: FlushAllOnReload is set to 'False'
2025-07-23 11:10:05 DEBUG1: RFC3964_IPv4 is set to 'True'
2025-07-23 11:10:05 DEBUG1: NftablesFlowtable is set to 'off'
2025-07-23 11:10:05 DEBUG1: NftablesCounters is set to 'False'
2025-07-23 11:10:05 DEBUG1: Loading lockdown whitelist
2025-07-23 11:10:05 ipset not usable, disabling ipset usage in firewall. Other set
 backends (nftables) remain usable.
2025-07-23 11:10:05 iptables-restore and iptables are missing, IPv4 direct rules
 won't be usable.
2025-07-23 11:10:05 ip6tables-restore and ip6tables are missing, IPv6 direct rules
 won't be usable.
2025-07-23 11:10:05 ebtables-restore and ebtables are missing, eb direct rules won't
 be usable.
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
address-unreachable.xml'
```

```
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/bad-
header.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
beyond-scope.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
communication-prohibited.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/icmptypes/
destination-unreachable.xml'
[...]
```

Todos los archivos de registro están disponibles en `/var/log/firewalld`.

5 Más información

Para obtener más información sobre `firewalld`, consulte los siguientes recursos:

- La fuente oficial de conceptos, arquitectura, procedimientos y enlaces a todas las páginas de manual. (https://firewalld.org/documentation/)
- La página de manual es esencial para comprender la interacción de la línea de comandos con `firewalld` (https://firewalld.org/documentation/man-pages/firewall-cmd.html)
- Un recurso completo con excelentes explicaciones y ejemplos prácticos que también cubren `nftables`. (https://wiki.archlinux.org/title/Firewalld)

6 Información legal

Toda la información recogida en esta publicación se ha compilado prestando toda la atención posible al más mínimo detalle. Sin embargo, esto no garantiza una precisión total. Ni SUSE LLC, ni sus filiales, ni los autores o traductores serán responsables de los posibles errores o las consecuencias que de ellos pudieran derivarse.

A GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material

on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with…Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.