SUSE

Introdução ao `firewalld`

O QUE É?

Saiba mais sobre o `firewalld`, uma ferramenta importante para proteger os servidores e serviços Linux. Trata-se do principal mecanismo de proteção de rede padrão em muitas distribuições modernas. O gerenciamento intuitivo baseado em zonas e os recursos de configuração dinâmica permitem um controle preciso do tráfego de rede sem interrupção do serviço.

POR QUÊ?

O `firewalld` é essencial porque oferece uma maneira moderna, dinâmica e fácil de gerenciar a segurança da rede em sistemas Linux, abstraindo as regras complexas de firewall em zonas e serviços intuitivos.

DEDICAÇÃO

A leitura deste artigo leva no máximo 30 minutos.

META

Gerenciar e reforçar a segurança de um sistema Linux com eficácia.

REQUISITOS

- Privilégios de `sudo` ou `root`, porque os comandos do `firewalld`, em especial aqueles que fazem alterações permanentes nas regras de firewall, exigem privilégios elevados.
- O `firewalld` é o firewall padrão em muitas distribuições Linux modernas. Se ele não foi pré-instalado no sistema, você precisa instalar o pacote `firewalld`.
- É essencial ter um conhecimento básico do terminal Linux.

Data de Publicação: 11/12/2025

Conteúdo

1 Sobre o `firewalld`

O `firewalld` é um serviço de gerenciamento de firewall dinâmico que oferece uma maneira flexível e eficaz de controlar o tráfego de rede em sistemas Linux. Ele permite modificações sem interromper as conexões existentes. Os benefícios do uso do `firewalld` são:

- *Configuração dinâmica:* Aplique as alterações instantaneamente, sem interromper as conexões existentes.
- *Interface fácil de usar:* As zonas e os serviços simplificam as regras complexas de firewall.
- *Abstração:* Não há necessidade de manipular diretamente as regras `nftables` em cenários comuns.
- *Configuração persistente:* Fácil gerenciamento das regras que são mantidas após as reinicializações.
- *Configuração persistente:* Por padrão, o `firewalld` opera com base no princípio `deny-all` bloqueando todo o tráfego de entrada, a menos que seja explicitamente permitido.

1.1 Zones do `firewalld`

A zona do firewall é um conjunto predefinido de regras que determinam como processar o tráfego de entrada e de saída da rede para uma interface de rede específica ou um endereço IP de origem. Cada zona representa um nível diferente de confiança na rede à qual está associada. Você pode aplicar políticas de segurança diferentes com base na origem da conexão de rede.

As zonas são como perfis de segurança. Por exemplo, você deseja aplicar regras de firewall diferentes a uma conexão Wi-Fi pública e à sua rede doméstica segura. As zonas do `firewalld` permitem que você defina esses conjuntos distintos de regras e os aplique adequadamente. Uma conexão de rede está sujeita apenas às regras de uma zona do `firewalld`. Uma zona do `firewalld` pode ter muitas interfaces de rede ou endereços IP de origem.

O diretório `/usr/lib/firewalld/zones/` armazena as zonas predefinidas. Por exemplo:

```
> /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
```

Algumas das configurações padrão das zonas predefinidas são:

`drop`

- *Nível de confiança:* Totalmente não confiável.
- *Comportamento:* Todos os pacotes de rede recebidos são removidos sem qualquer resposta. Somente as conexões de saída iniciadas pelo sistema são permitidas. Isso oferece um modo "furtivo", em que o sistema parece inexistente a invasores externos.
- *Caso de uso:* Usado para máxima ocultação e segurança, ignorando completamente o tráfego indesejado. Ideal como padrão rigoroso para um servidor que nunca deve aceitar conexões de entrada.

`block`

- *Nível de confiança:* Muito baixo.
- *Comportamento:* Todas as conexões de rede de entrada são rejeitadas com a mensagem `icmp-host-prohibited` para IPv4 e `icmp6-adm-prohibited` para IPv6. Isso informa ao remetente que a conexão foi explicitamente rejeitada. Apenas as conexões de saída iniciadas pelo sistema são possíveis.
- *Caso de uso:* Aplicado quando você deseja sinalizar explicitamente aos remetentes que as tentativas de conexão deles estão sendo bloqueadas.

`public`

- *Nível de confiança:* Não confiável ou público.
- *Comportamento:* Representa redes públicas não confiáveis para execução de outros sistemas. Apenas conexões de entrada selecionadas são aceitas por padrão, por exemplo, SSH, cliente DHCPv6 etc.
- *Caso de uso:* Uma zona padrão comum para interfaces conectadas diretamente à Internet, como a interface WAN do seu roteador. Também inclui a conexão com uma rede na qual você não tem controle sobre outros dispositivos.

`external`

- *Nível de confiança:* Externo com mascaramento.
- *Comportamento:* Voltado a redes externas quando o firewall atua como gateway ou roteador. Normalmente, o mascaramento NAT está habilitado por padrão. Apenas conexões de entrada selecionadas são aceitas, sob a premissa de que você não confia nessa rede para executar outros sistemas.
- *Caso de uso:* Usado quando a máquina Linux atua como roteador, conectando uma rede privada interna à Internet pública. A interface externa é colocada nessa zona para ocultar a topologia de rede interna e permitir que os clientes internos acessem recursos externos, como a Internet.

`dmz (Demilitarized Zone)`

- *Nível de confiança:* Acesso público limitado.
- *Comportamento:* Para sistemas em uma zona DMZ que são acessíveis ao público, mas com acesso limitado à rede interna. Apenas conexões de entrada selecionadas são aceitas. Geralmente, o padrão inclui SSH e outros serviços que você expõe.
- *Caso de uso:* Ideal para servidores voltados ao público, como Web, de e-mail e DNS. Esses servidores são intencionalmente expostos à Internet, mas estão isolados de suas redes internas mais confiáveis. Útil quando você deseja hospedar serviços que precisam ficar acessíveis pela Internet, mas minimizando o risco à infraestrutura interna principal.

`work`

- *Nível de confiança:* Bastante confiável (ambiente de trabalho).
- *Comportamento:* Em um ambiente de trabalho, você geralmente confia na rede para conectar outros computadores. Permite conexões de entrada selecionadas que são comuns em um ambiente de trabalho, como SSH e cliente DHCPv6.
- *Caso de uso:* Ideal para redes e sistemas de escritório em uma LAN corporativa.

`home`

- *Nível de confiança:* Bastante confiável (ambiente doméstico).
- *Comportamento:* Em um ambiente doméstico, você confia bastante na rede para conectar outros sistemas. Permite mais serviços do que as zonas públicas ou externas, geralmente incluindo serviços comuns de rede doméstica, como compartilhamento de arquivos, servidores de mídia e impressoras, além de SSH e cliente DHCPv6.
- *Caso de uso:* Ótimo para redes domésticas e instalações de home office de pequeno porte.

`trusted`

- *Nível de confiança:* Máximo.
- *Comportamento:* Todas as conexões de rede são aceitas sem qualquer filtragem. O firewall não é implementado para conexões atribuídas a essa zona.
- *Caso de uso:* Reservado para conexões altamente confiáveis.

1.2 Políticas e regras do `firewalld`

As políticas do `firewalld` oferecem uma maneira mais avançada e flexível de gerenciar o tráfego de rede em comparação com as zonas tradicionais. Elas permitem que você defina regras detalhadas que especificam a origem e o destino do tráfego, os serviços, as portas e as ações, como aceitar, rejeitar e remover. Essas políticas são úteis para configurar roteamento complexo, encaminhamento de portas ou criar segmentos de rede isolados em um único host.

As políticas `firewalld` usam as zonas para definir conjuntos de regras. Elas aplicam regras com estado em uma direção, o que significa que você define o fluxo do tráfego em uma direção, e o `firewalld` permite implicitamente o caminho de volta. Essas políticas vinculam uma zona de entrada (por onde o tráfego entra) a uma zona de saída (por onde o tráfego sai). Isso define o caminho e a direção específicos aos quais as regras de uma política se aplicam. Você pode ver as políticas, por exemplo:

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

As regras de firewall permitem controlar com precisão o tráfego da rede, autorizando-o ou bloqueando-o para proteger o sistema contra ameaças à segurança. As regras de firewall definem determinados critérios com base em vários atributos, como endereços IP de origem e de destino,

portas e interfaces de rede. O `firewalld` separa as regras de firewall em zonas e políticas. Cada zona no `firewalld` tem um conjunto exclusivo de regras que determinam as permissões de tráfego para as interfaces de rede associadas.

1.3 Serviços e portas

Os serviços são recomendados quando há um serviço predefinido disponível. Por exemplo, em vez de lembrar que o HTTP usa a porta TCP 80, você pode apenas adicionar o serviço `http`. Esse procedimento é menos propenso a erros e mais fácil de gerenciar. Use as portas quando um serviço não estiver predefinido ou quando você usar uma porta personalizada para um serviço. Você pode ver os serviços e as portas ativos nas zonas padrão com o seguinte comando:

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

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

2 Gerenciando regras e zonas de firewall

Você pode configurar zonas do `firewalld` e as respectivas regras com a interface gráfica da Web Cockpit ou o utilitário **`firewall-cmd`** para controle de linha de comando.

2.1 Gerenciando regras e zonas de firewall com o utilitário `firewalld-cmd`

Você pode usar a interface CLI para gerenciar as zonas do `firewalld`.

2.1.1 Adicionando zonas do `firewalld`

Para adicionar uma nova zona do `firewalld`:

1. Crie uma nova zona, por exemplo:

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

2. Defina o nível de confiança da zona que determina o comportamento padrão:

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

3. Recarregue o serviço `firewalld` para aplicar a nova configuração:

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

2.1.2 Adicionando o serviço a uma zona

Para adicionar o serviço a uma zona:

1. Liste todos os serviços para verificar se o seu já 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. Você pode adicionar um serviço temporariamente durante a sessão de runtime ou permanentemente, por exemplo:

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

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

   O sinalizador `--permanent` garante que a alteração seja mantida em todas as reinicializações.

3. Recarregue o serviço `firewalld` para aplicar a nova configuração:

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

4. Verifique os resultados:

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

2.1.3 Adicionando a porta a uma zona

Se o aplicativo não tem um serviço predefinido, você pode abrir uma porta específica ou um intervalo de portas.

1. Você pode adicionar uma porta temporariamente durante a sessão de runtime ou permanentemente, por exemplo:

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

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

   O sinalizador `--permanent` garante que a alteração seja mantida em todas as reinicializações.

2. Recarregue o serviço `firewalld` para aplicar a nova configuração:

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

3. Verifique os resultados:

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

2.1.4 Excluindo as zonas do `firewalld`

Para excluir uma zona:

1. Verifique se a zona não é a padrão ou está em uso:

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

   Se a zona estiver em uso ou for a padrão, defina outra zona, por exemplo:

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

2. Verifique se há uma interface de rede vinculada à zona:

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

3. O campo `interfaces` na saída lista todas as interfaces. Essas interfaces precisam ser reatribuídas a outra zona. Por exemplo:

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

4. Exclua a zona:

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

5. Recarregue o serviço `firewalld` para aplicar a nova configuração:

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

2.2 Gerenciando regras e zonas de firewall com o Cockpit

O Cockpit permite criar novas zonas ou atualizar as existentes. Nas configurações de firewall, você pode adicionar serviços a uma zona ou permitir acesso a portas.

Nota: O serviço Cockpit é obrigatório

Não remova o serviço Cockpit da zona de firewall padrão, pois ele pode ser bloqueado, e você pode ser desconectado do servidor.

2.2.1 Adicionando zonas de firewall

A *zona pública* é a zona de firewall padrão. Para adicionar uma nova zona, faça o seguinte:

PROCEDIMENTO 1: ADICIONANDO NOVAS ZONAS DE FIREWALL

1. Navegue até a página *Rede*.
2. Clique em *Editar regras e zonas*.
3. Clique em *Adicionar zona*.
4. Selecione o *Nível de confiança*. Cada nível de confiança das conexões de rede tem um conjunto predefinido de serviços incluídos (o serviço Cockpit está incluído em todos os níveis de confiança).
5. Defina os endereços permitidos na zona. Selecione um dos valores:
   - *Toda a sub-rede* para permitir todos os endereços na sub-rede.
   - *Intervalo*: uma lista de endereços IP separados por vírgula com o prefixo de roteamento, por exemplo, 192.0.2.0/24, 2001:db8::/32.

6. Clique em *Adicionar zona* para prosseguir.

2.2.2 Adicionando serviços e portas permitidos a uma zona

Você pode adicionar serviços a uma zona de firewall existente conforme descrito a seguir:

PROCEDIMENTO 2: ADICIONANDO SERVIÇOS A UMA ZONA DE FIREWALL

1. Navegue até a página *Rede*.
2. Clique em *Editar regras e zonas*.
3. Clique em *Adicionar serviços*.
4. Para adicionar serviços, marque *Serviços* e selecione-os na lista.
5. Para permitir portas personalizadas, marque *Portas customizadas* e especifique o valor da porta para UDP e/ou TCP. Você pode atribuir um identificador a essas portas.
6. Para confirmar as mudanças, clique em *Adicionar serviços* ou *Adicionar portas*, respectivamente.

3 Comandos comuns do `firewalld`

A ferramenta de linha de comando **`firewall-cmd`** é usada para configurar e gerenciar o daemon `firewalld`. Trata-se de um utilitário avançado e dinâmico que permite a criação, modificação e exclusão de regras de firewall sem exigir a reinicialização completa do serviço, o que evita a interrupção das conexões de rede ativas.

Alguns exemplos comuns do comando **`firewall-cmd`** são:

- Verificar se o `firewalld` está em execução. As saídas são `running`, `not running` ou `RUNNING_BUT_FAILED`. Por exemplo:

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

- Listar todas as zonas disponíveis, por exemplo:

```
> sudo firewall-cmd --get-zones
```

```
 block dmz docker drop external home internal nm-shared public trusted work
```

- Ver a zona padrão, por exemplo:

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

- Ver as zonas ativas e atribuídas, por exemplo:

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

- Ver todas as regras da zona padrão, por exemplo:

```
> 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 as regras de uma zona específica, por exemplo:

```
> 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
```

- Listar todos os serviços predefinidos disponíveis, por exemplo:

```
> 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
  [...]
```

- Listar os serviços atualmente permitidos na zona padrão, por exemplo:

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

- Adicionar um serviço à zona padrão permanentemente, por exemplo:

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

- Remover um serviço permanentemente, por exemplo:

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

- Listar as portas atualmente abertas na zona padrão, por exemplo:

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

- Abrir temporariamente uma porta TCP específica, por exemplo:

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

- Remover uma porta aberta permanentemente, por exemplo:

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

- Adicionar temporariamente uma interface a uma zona específica, por exemplo:

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

4 Solução de problemas do `firewalld`

A solução de problemas do `firewalld` envolve verificar o status e as regras, além de reiniciar ou recarregar o serviço. Se você encontrar problemas, poderá habilitar a depuração, examinar os registros e ajustar as regras de firewall conforme necessário.

4.1 Verificar o status do `firewalld`

- Use o comando **`systemctl status`**, por exemplo:

```
> 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
```

- O comando **`firewall-cmd --state`** retorna uma rápida verificação de status com as saídas `running`, `not running` ou `RUNNING_BUT_FAILED`. Por exemplo:

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

- Se o `firewalld` não estiver em execução, use o comando **`systemctl start firewalld`**.

```
> sudo  systemctl start firewalld
```

- Se o serviço `firewalld` estiver mascarado, desmascare-o primeiro para depois habilitá-lo e iniciá-lo, por exemplo:

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

```
> sudo systemctl enable firewalld
```

```
> sudo systemctl start firewalld
```

4.2 Verificar as regras do `firewalld`

- O comando **`firewall-cmd  --list-all-zones`** exibe todas as zonas e as regras, por exemplo:

```
> 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
  [...]
```

- O comando **`firewall-cmd --list-ports`** mostra as portas abertas, por exemplo:

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

- O comando **`firewall-cmd --zone=`***`YOUR_ZONE`* **`--list-all.`** lista as portas de zonas específicas, por exemplo:

```
> 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 Depurando o `firewalld`

- Habilite a depuração em `/etc/sysconfig/firewalld` adicionando `--debug=[level]` a `FIREWALLD_ARGS`, por exemplo:

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

- Inicie o `firewalld` com a opção `--debug`, por exemplo:

```
> 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 os arquivos de registro estão disponíveis em `/var/log/firewalld`.

5 Mais informações

Para saber mais sobre o `firewalld`, consulte os seguintes recursos:

- A fonte oficial para conceitos, arquitetura, procedimentos e links para todas as páginas de manual. (https://firewalld.org/documentation/)
- Página de manual essencial para entender a interação da linha de comando com o `firewalld` (https://firewalld.org/documentation/man-pages/firewall-cmd.html)
- Um recurso abrangente com excelentes explicações e exemplos práticos que também abrangem o `nftables`. (https://wiki.archlinux.org/title/Firewalld)

6 Informações legais

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.