SUSE

Présentation de `firewalld`

CONTENU

Découvrez `firewalld`, un outil important pour la sécurisation des serveurs et services Linux. Il s'agit du mécanisme de défense réseau par défaut et principal sur de nombreuses distributions modernes. La gestion intuitive basée sur les zones et les fonctionnalités de configuration dynamique permettent un contrôle précis du trafic réseau sans interruption de service.

MOTIF

`firewalld` est essentiel, car il fournit un moyen moderne, dynamique et convivial de gérer la sécurité réseau sur les systèmes Linux en simplifiant les règles de pare-feu complexes en zones et services intuitifs.

EFFORT

La lecture de cet article vous prendra au maximum 30 minutes.

OBJECTIF

Gérer et améliorer efficacement la sécurité d'un système Linux.

CONDITIONS REQUISES

- Privilèges `sudo` ou `root`, car les commandes `firewalld`, en particulier celles qui apportent des modifications permanentes aux règles de pare-feu, nécessitent des privilèges élevés.
- `firewalld` est le pare-feu par défaut sur de nombreuses distributions Linux modernes ; s'il n'est pas préinstallé sur votre système, vous devez installer le paquet `firewalld`.
- Une compréhension de base du terminal Linux est essentielle.

Date de publication : 11 déc 2025

Table des matières

1 À propos de `firewalld` 3

2 Gestion des règles et des zones de pare-feu 7

3 Commandes `firewalld` courantes 12

4 Dépannage de `firewalld` 15

5 Informations complémentaires 18

6 Mentions légales 19

A GNU Free Documentation License 19

1 À propos de `firewalld`

`firewalld` est un service de gestion de pare-feu dynamique qui offre un moyen flexible et efficace de contrôler le trafic réseau sur les systèmes Linux. Il permet d'apporter des modifications sans interrompre les connexions existantes. Les avantages de l'utilisation de `firewalld` sont les suivants :

- *Configuration dynamique :* appliquez les modifications instantanément sans rompre les connexions existantes.
- *Interface conviviale :* les zones et les services simplifient les règles de pare-feu complexes.
- *Abstraction :* il n'est pas nécessaire de manipuler directement les règles `nftables` pour les scénarios courants.
- *Configuration persistante :* gestion facile des règles qui survivent aux redémarrages.
- *Configuration persistante :* par défaut `firewalld` fonctionne sur un principe `deny-all` en bloquant tout le trafic entrant, sauf si explicitement autorisé.

1.1 Zones `firewalld`

Une zone de pare-feu est un ensemble prédéfini de règles qui dictent la façon dont le trafic réseau entrant et sortant est géré pour une interface réseau ou une adresse IP source spécifique. Chaque zone représente un niveau de confiance différent pour le réseau auquel elle est associée. Vous pouvez appliquer différentes stratégies de sécurité en fonction de l'origine de la connexion réseau.

Les zones sont comme des profils de sécurité. Par exemple, vous pouvez souhaiter appliquer des règles de pare-feu différentes pour une connexion Wi-Fi publique et votre réseau domestique sécurisé. Les zones `firewalld` vous permettent de définir ces ensembles distincts de règles et de les appliquer en conséquence. Une connexion réseau n'est soumise aux règles que d'une seule zone `firewalld`. Une zone `firewalld` peut comporter de nombreuses interfaces réseau ou adresses IP sources.

Le répertoire `/usr/lib/firewalld/zones/` stocke les zones prédéfinies. Par exemple :

```
> /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
```

Certains des paramètres par défaut des zones prédéfinies sont les suivants :

`drop`

- *Niveau d'approbation :* aucune fiabilité.
- *Comportement :* tous les paquets réseau entrants sont abandonnés sans aucune réponse. Seules les connexions sortantes initiées à partir du système sont autorisées. Cela fournit un mode « furtif » dans lequel le système apparaît comme inexistant pour les pirates informatiques externes.
- *Cas d'utilisation :* utilisé pour une furtivité et une sécurité maximales, en ignorant complètement le trafic indésirable. Convient comme valeur par défaut stricte pour un serveur qui ne devrait jamais accepter de connexions entrantes.

`block`

- *Niveau d'approbation :* très faible.
- *Comportement :* toutes les connexions réseau entrantes sont rejetées avec un message `icmp-host-prohibited` pour IPv4 et `icmp6-adm-prohibited` pour IPv6. Celui-ci informe l'expéditeur que sa connexion a été explicitement rejetée. Seules les connexions sortantes initiées à partir du système sont possibles.
- *Cas d'utilisation :* appliqué lorsque vous souhaitez signaler explicitement aux expéditeurs que leurs tentatives de connexion sont bloquées.

`public`

- *Niveau d'approbation :* non fiable ou public.
- *Comportement :* représente les réseaux publics non approuvés sur lesquels vous ne faites pas confiance aux autres systèmes. Seules les connexions entrantes sélectionnées sont acceptées par défaut, par exemple, SSH, client DHCPv6, etc.
- *Cas d'utilisation :* zone par défaut commune pour les interfaces connectées directement à Internet, telles que l'interface WAN de votre routeur. Également pour les connexions à un réseau sur lequel vous n'avez aucun contrôle sur les autres périphériques.

`external`

- *Niveau d'approbation :* externe avec masquage d'adresse IP.
- *Comportement :* destiné aux réseaux externes lorsque le pare-feu fait office de passerelle ou de routeur. En général, le masquage NAT est activé par défaut. Seules les connexions entrantes sélectionnées sont acceptées, en supposant que vous ne faites pas confiance aux autres systèmes de ce réseau.
- *Cas d'utilisation :* utilisé lorsque votre machine Linux fait office de routeur, en connectant un réseau privé interne à l'Internet public. L'interface externe est placée dans cette zone pour masquer la topologie du réseau interne, tout en permettant aux clients internes d'accéder à des ressources externes telles qu'Internet.

`dmz (Demilitarized Zone)`

- *Niveau d'approbation :* accès public limité.
- *Comportement :* pour les systèmes situés dans une zone démilitarisée (DMZ) qui sont accessibles au public, mais avec un accès limité au réseau interne. Seules les connexions entrantes sélectionnées sont acceptées. Les paramètres par défaut incluent généralement SSH et d'autres services que vous exposez.
- *Cas d'utilisation :* convient aux serveurs exposés au public tels que les serveurs Web, de messagerie et DNS. Ces serveurs sont intentionnellement exposés à Internet, mais sont isolés de vos réseaux internes plus fiables. Utile lorsque vous souhaitez héberger des services qui doivent être accessibles sur Internet tout en limitant les risques pour votre infrastructure interne principale.

`work`

- *Niveau d'approbation :* globalement de confiance (environnement de travail).
- *Comportement :* dans un environnement de travail, vous faites généralement confiance aux autres ordinateurs du réseau. Autorise les connexions entrantes sélectionnées qui sont courantes dans un environnement de travail, telles que les clients SSH et DHCPv6.
- *Cas d'utilisation :* convient aux réseaux et systèmes de bureau sur un réseau local (LAN) d'entreprise.

`home`

- *Niveau d'approbation :* globalement de confiance (environnement privé).
- *Comportement :* dans un environnement privé, vous faites généralement confiance aux autres systèmes sur le réseau. Autorise plus de services que les zones publiques ou externes, y compris souvent les services de réseau privé courants tels que le partage de fichiers, les serveurs multimédias et les imprimantes, ainsi que les clients SSH et DHCPv6.
- *Cas d'utilisation :* idéal pour les réseaux privés et les petites configurations de bureau à domicile.

`trusted`

- *Niveau d'approbation :* maximal.
- *Comportement :* toutes les connexions réseau sont acceptées sans aucun filtrage. Le pare-feu n'est pas implémenté pour les connexions affectées à cette zone.
- *Cas d'utilisation :* réservé aux connexions de haute confiance.

1.2 Stratégies et règles `firewalld`

Les stratégies `firewalld` fournissent un moyen plus avancé et plus flexible de gérer le trafic réseau par rapport aux zones traditionnelles. Elles vous permettent de définir des règles riches qui spécifient la source et la destination du trafic, les services, les ports et les actions telles que l'acceptation, le rejet et l'abandon. Ces stratégies sont utiles pour configurer un routage complexe, un réacheminement de port ou la création de segments de réseau isolés au sein d'un seul hôte.

Les stratégies `firewalld` fournissent des zones pour définir des ensembles de règles. Elles appliquent des règles en tenant compte de l'état et dans une seule direction, ce qui signifie que vous définissez le flux de trafic dans une seule direction, et `firewalld` autorise implicitement le chemin de retour. Ces stratégies lient une zone d'entrée (où le trafic entre) à une zone de sortie (où le trafic sort). Cela définit le chemin d'accès et la direction spécifiques auxquels les règles d'une stratégie s'appliquent. Vous pouvez afficher les stratégies, par exemple :

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

Les règles de pare-feu vous permettent de contrôler avec précision le trafic réseau, en l'autorisant ou en le bloquant pour protéger votre système contre les menaces de sécurité. Les règles de pare-feu définissent certains critères en fonction de divers attributs tels que les adresses IP sources et cibles, les ports et les interfaces réseau. `firewalld` sépare les règles de pare-feu en zones et en stratégies. Chaque zone dans `firewalld` dispose d'un ensemble unique de règles qui dicte les autorisations de trafic pour ses interfaces réseau associées.

1.3 Services et ports

Les services sont recommandés lorsqu'un service prédéfini est disponible. Par exemple, au lieu de vous rappeler que HTTP utilise le port TCP 80, vous pouvez simplement ajouter le service `http`. Cette approche est moins sujette aux erreurs et plus facile à gérer. Utilisez les ports lorsqu'un service n'est pas prédéfini ou lorsque vous utilisez un port personnalisé pour un service. Vous pouvez afficher les services et les ports actifs pour les zones par défaut à l'aide des commandes suivantes :

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

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

2 Gestion des règles et des zones de pare-feu

Vous pouvez configurer les zones `firewalld` et leurs règles avec l'interface Web graphique Cockpit ou l'utilitaire **`firewall-cmd`** pour le contrôle de ligne de commande.

2.1 Gestion des règles et des zones de pare-feu à l'aide de l'utilitaire **`firewalld-cmd`**

Vous pouvez utiliser l'interface de ligne de commande (CLI) pour gérer les zones `firewalld`.

2.1.1 Ajout de zones `firewalld`

Pour ajouter une nouvelle zone `firewalld` :

1. Créez une zone, par exemple :

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

2. Définissez le niveau de confiance de la zone qui définit le comportement par défaut :

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

3. Rechargez le service `firewalld` pour appliquer la nouvelle configuration :

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

2.1.2 Ajout d'un service à une zone

Pour ajouter un service à une zone :

1. Listez tous les services pour vérifier si votre service est déjà prédéfini :

```
> 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. Vous pouvez ajouter un service soit temporairement pour la session d'exécution, soit de manière permanente, par exemple :

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

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

L'indicateur `--permanent` garantit que la modification persiste après tous les redémarrages.

3. Rechargez le service `firewalld` pour appliquer la nouvelle configuration :

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

4. Vérifiez les résultats :

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

2.1.3 Ajout d'un port à une zone

Si votre application ne dispose pas d'un service prédéfini, vous pouvez ouvrir un port spécifique ou une plage de ports.

1. Vous pouvez ajouter un port soit temporairement pour la session d'exécution, soit de manière permanente, par exemple :

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

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

L'indicateur `--permanent` garantit que la modification persiste après tous les redémarrages.

2. Rechargez le service `firewalld` pour appliquer la nouvelle configuration :

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

3. Vérifiez les résultats :

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

2.1.4 Suppression de zones `firewalld`

Pour supprimer une zone :

1. Vérifiez que la zone n'est pas celle par défaut ou en cours d'utilisation :

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

Si la zone est en cours d'utilisation ou celle par défaut, définissez-en une autre, par exemple :

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

2. Vérifiez si des interfaces réseau sont liées à la zone :

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

3. Le champ `interfaces` dans la sortie répertorie toutes les interfaces. Ces interfaces doivent être réaffectées à une autre zone. Par exemple :

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

4. Supprimez la zone :

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

5. Rechargez le service `firewalld` pour appliquer la nouvelle configuration :

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

2.2 Gestion des règles et des zones de pare-feu à l'aide de Cockpit

Cockpit vous permet de créer des zones ou de mettre à jour les zones existantes. Dans les paramètres du pare-feu, vous pouvez ajouter des services à une zone ou autoriser l'accès à des ports.

Remarque : le service Cockpit est obligatoire

Ne supprimez pas le service Cockpit de la zone de pare-feu par défaut, car il risque d'être bloqué, ce qui pourrait vous déconnecter du serveur.

2.2.1 Ajout de zones de pare-feu

La *zone publique* est la zone de pare-feu par défaut. Pour ajouter une nouvelle zone, procédez comme suit :

PROCÉDURE 1 : AJOUT DE NOUVELLES ZONES DE PARE-FEU

1. Accédez à la page *Réseautique*.
2. Cliquez sur *Modifier les règles et les zones*.
3. Cliquez sur *Ajouter une zone*.
4. Sélectionnez le *Niveau de confiance*. Chaque niveau de confiance des connexions réseau a un ensemble prédéfini de services inclus (le service Cockpit est inclus dans tous les niveaux de confiance).
5. Définissez les adresses autorisées dans la zone. Sélectionnez l'une des valeurs suivantes :
   - *Ensemble du sous-réseau* pour autoriser toutes les adresses du sous-réseau.
   - *Gamme* : pour une liste d'adresses IP séparées par des virgules, avec le préfixe de routage, par exemple, 192.0.2.0/24, 2001:db8::/32.
6. Continuez avec *Ajouter une zone*.

2.2.2 Ajout de services et de ports autorisés à une zone

Vous pouvez ajouter des services à une zone de pare-feu existante comme décrit ci-dessous :

PROCÉDURE 2 : AJOUT DE SERVICES À UNE ZONE DE PARE-FEU

1. Accédez à la page *Réseautique*.
2. Cliquez sur *Modifier les règles et les zones*.
3. Cliquez sur *Ajouter des services*.
4. Pour ajouter un service, cochez *Services* et sélectionnez les services dans la liste.
5. Pour autoriser les ports personnalisés, cochez la case *Ports personnalisés* et spécifiez la valeur du port pour UDP et/ou TCP. Vous pouvez assigner un identificateur à ce port.

6. Pour confirmer les modifications, cliquez sur *Ajouter des services* ou *Ajouter des ports*, respectivement.

3 Commandes `firewalld` courantes

L'outil de ligne de commande **`firewall-cmd`** permet de configurer et de gérer le daemon `firewalld`. Il s'agit d'un utilitaire dynamique puissant qui permet de créer, de modifier et de supprimer des règles de pare-feu sans nécessiter un redémarrage complet du service, ce qui évite l'interruption des connexions réseau actives.

Voici quelques exemples courants de commandes **`firewall-cmd`** :

- Vérifier si `firewalld` est en cours d'exécution. Les résultats sont les suivants : `running`, `not running` ou `RUNNING_BUT_FAILED`. Par exemple :

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

- Lister toutes les zones disponibles, par exemple :

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

- Afficher la zone par défaut, par exemple :

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

- Afficher les zones actives et les zones assignées, par exemple :

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

- Afficher toutes les règles de la zone par défaut, par exemple :

```
> 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
```

- Afficher toutes les règles d'une zone spécifique, par exemple :

```
> 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
```

- Répertorier tous les services prédéfinis disponibles, par exemple :

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

- Lister les services actuellement autorisés dans la zone par défaut, par exemple :

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

- Ajouter de façon permanente un service à la zone par défaut, par exemple :

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

- Supprimer définitivement un service, par exemple :

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

- Lister les ports actuellement ouverts dans la zone par défaut, par exemple :

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

- Ouvrir temporairement un port TCP spécifique, par exemple :

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

- Supprimer définitivement un port ouvert, par exemple :

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

- Ajouter temporairement une interface à une zone spécifique, par exemple :

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

4 Dépannage de `firewalld`

Le dépannage de `firewalld` implique de vérifier son statut et les règles, et de redémarrer ou de recharger le service. Si vous rencontrez des problèmes, vous pouvez activer le débogage, examiner les journaux et ajuster les règles de pare-feu si nécessaire.

4.1 Vérification du statut de `firewalld`

- Utilisez la commande **`systemctl status`**. Par exemple :

```
> 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
```

- La commande **`firewall-cmd --state`** permet une vérification rapide du statut avec les sorties `running`, `not running` ou `RUNNING_BUT_FAILED`. Par exemple :

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

- Si `firewalld` n'est pas en cours d'exécution, utilisez la commande **`systemctl start firewalld`**.

```
> sudo  systemctl start firewalld
```

- Si le service `firewalld` est masqué, démasquez-le d'abord, puis activez-le et démarrez-le. Par exemple :

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

```
> sudo systemctl enable firewalld
```

```
> sudo systemctl start firewalld
```

4.2 Vérification des règles `firewalld`

- La commande **`firewall-cmd --list-all-zones`** affiche toutes les zones et leurs règles. Par exemple :

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

- La commande **`firewall-cmd --list-ports`** affiche les ports ouverts. Par exemple :

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

- La commande **`firewall-cmd --zone=`***`YOUR_ZONE`* **`--list-all.`** liste les ports de zones spécifiques. Par exemple :

```
> 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 Débogage de `firewalld`

- Activez le débogage dans `/etc/sysconfig/firewalld` en ajoutant `--debug=[level]` à `FIREWALLD_ARGS`. Par exemple :

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

- Démarrez `firewalld` avec l'option `--debug`. Par exemple :

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

Tous les fichiers journaux sont disponibles dans `/var/log/firewalld`.

5 Informations complémentaires

Pour en savoir plus sur `firewalld`, reportez-vous aux ressources suivantes :

- La source officielle pour les concepts, l'architecture, les procédures et les liens vers toutes les pages de manuel. (https://firewalld.org/documentation/)
- La page de manuel essentielle pour comprendre l'interaction de la ligne de commande avec `firewalld`. (https://firewalld.org/documentation/man-pages/firewall-cmd.html)
- Une ressource complète avec d'excellentes explications et des exemples pratiques qui couvrent également `nftables`. (https://wiki.archlinux.org/title/Firewalld)

6 Mentions légales

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.