firewalld

Gestionnaire de firewall dynamique

firewalld fournis une gestion dynamique du firewall. Il supporte IPv4 et IPv6.

OPTIONS

–debug [=level] mode debug, de 1 à 10. le debug est écris dans /var/log/firewalld

–debug-gc Affiche les informations sur les fuites du collecteur. Le collecteur se lance toutes les 10 secondes, et s'il y a des fuites, il les affiche.

–nofork ne fork pas le service

–nopid désactive l'écriture du fichier pid.

Concepts

firewalld a une interface D-Bus pour la configuration du firewall des services et applications. Il a également un client pour l'utilisateur. Les services ou applications utilisant déjà D-Bus peuvent demander des changements au firewall directement via D-Bus.

firewalld fournis un suppport pour les zones, des services prédéfinis et les types ICMP et a une séparation des options de configuration permanentes et en temps-réel. La configuration permanente est chargé depuis des fichiers XML dans /usr/lib/firewalld ou /etc/firewalld

Si NetworkManager n'est pas utilisé et que firewalld est démarré après que le réseau soit déjà définis, les connexions et interfaces créées manuellement ne sont pas liées à la zone spécifiée dans le fichier ifcfg. Les interfaces sont automatiquement géré par la zone par défaut. firewalld est également notifié sur les renommages de périphériques réseaux. Tout cela s'applique également aux interfaces qui ne sont pas contrôlés par NetworkManager si NM_CONTROLED=no est mis.

On peut ajouter ces interfaces à une zone avec firewall-cmd [–permanent] –zone=zone –add-interface=interface. S'il y a un fichier ifcfg-interface, firewalld tente de changer ZONE=zone dans ce fichier.

Si firewalld est rechargé, il va restaurer les liaisons d'interface qui étaient en place avant de recharger pour conserver les liaisons d'interfaces stables dans le cas d'interface non contrôlés par NetworkManager. Ce mécanisme n'est pas possible dans le cas du redémarrage de firewalld.

Il est essentiel de conserver le paramètre ZONE= dans les fichiers ifcfg consistant avec les liaisons dans firewalld dans le cas d'interfaces non controlé par NetworkManager.

Zones

Une zone réseau ou firewall définis le niveau de confiance de l'interface utilisée pour une connexion. Il y a de nombreuses zones prédéfinies fournis par firewalld.

Services

Un service peut être une liste de ports locaux, protocoles, et destination et additionnellement une liste de modules firewall automatiquement chargé si un service est activé. L'utilisation de services prédéfinis simplifient l'activation/désactivation des accès à un service.

Types ICMP

ICMP est utilisé pour échanger les informations et messages d'erreur dans IP. les types ICMP peuvent être utilisé dans firewalld pour limiter l'échange de ces messages.

Configuration temps-réel

La configuration temps-réel est la configuration active et n'est pas permanente. Une fois le service rechargé/redémarré ou après un reboot système, les paramètres temps réel sont perdus s'ils ne sont pas également dans la configuration permanente.

Configuration permanente

Le configuration permanente est stockée dans les fichiers de configuration et est chargé au démarrage du service.

Interface directe

L'interface directe est principalement utilisée par les services ou application pour ajouter des règles firewall spécifiques.

Répertoires

/usr/lib/firewalld Configuration par défaut, types icmp, services et zones.

/etc/firewalld Configuration système ou utilisateur.

Signaux

SIGHUP