firewalld.zones

Zones firewalld

Une zone réseau définis le niveau de confiance des connexions réseaux. C'est une des nombreuses relations, qui signifie qu'une connexion peut seulement faire partie d'une zone, mais une zone peut être utilisé pour de nombreuses connections réseaux. La zone définis les fonctionnalités firewall qui sont activés dans cette zone :

Services prédéfinis un service est une combinaison de ports et/ou protocols. Optionnellement, des modules netfilter peuvent être ajoutés ainsi que des adresses de destination IPv4 et IPv6

Protocoles et ports Définition de ports tcp ou udp, où les ports peuvent être un simple port ou une plage de ports.

Masquerading Les adresses d'un réseau privé sont mappés et cachés derrière une adresse IP publique.

Forward ports Un forward port est soit mappé au même port dans un autre hôte ou à un autre port dans le même hôte ou un autre port dans un autre hôte.

Règles de langage rich Le langage rich étend les éléments avec des adresses source et destination additionnels, logging, actions et limites pour les logs et actions. Il peut être utilisé pour les hôtes ou listing de réseau blanc ou noir.

zones disponibles

Il y a des zones fournies par firewalld triés en accord avec le niveau avec le niveau de confiance des zones :

drop Tous les paquets sont supprimés, sans réponse. Seul les connexions sortantes sont possibles

block Les connexions réseau entrantes sont rejetées avec un message icmp-host-prohibited pour IPv4 et icmp6-adm-prohibited pour IPv6. Seul les connexions initiées dans ce système sont possibles

public À utiliser dans les zones publiques. Ne pas faire confiance aux autres machines. Seuls les connections entrantes séléctionnées sont acceptés.

external À utiliser dans les réseaux externes avec le masquerading activé. Pas de confiance aux autres machines. Seules les connexions entrantes sélectionnées sont acceptées

dmz Pour les machines dans une zone démilitarisée publiquement accessibles avec accès limité au réseau interne. Seules les connections entrantes sélectionnées sont acceptés

work À utiliser dans les zones de travail. Fait confiance aux autres machines dans les réseaux de la machine. Seules les connexions entrantes sélectionnées sont acceptées

home À utiliser dans les réseaux personnels. Fait confiance aux autres machines du réseau. Seules les connections entrantes sélectionnées sont acceptées

internal À utiliser dans les réseaux interne. Fait confiance aux autres machines dans le réseaux non liés à la machine. Seules les connections entrantes séléctionnées sont acceptées

trusted Toutes les connections réseaux sont acceptées

Zones à utiliser

Un réseau WIFI publique par exemple, ne doit pas être de confiance, une connexion filaire personnelle devrait être de confiance.

Configurer ou ajouter une zone

Pour configurer ou ajouter une zone, utiliser les interfaces firewalld. Il y a un outils de configuration graphique firewall-config, un outil en ligne de commande firewall-cmd ou l'interface D-Bus. Il est également possible de copier un fichier de zone dans /usr/lib/firewalld/zones dans /etc/firewalld/zones.

La zone est stockée dans ifcfg de la connexion avec l'option ZONE=. Si l'option est manquante ou vide, la zone par défaut est utilisée.

Si la connexion est contrôlée par NetworkManager, on peut également utiliser nm-connection-editor pour changer la zone

Pour l'ajout ou la modifications d'interfaces non contrôlées par NetworkManager, firewalld tente de changer le paramètres ZONE dans le fichier ifcfg, s'il existe.

Pour les interfaces non contrôlées par NetworkManager, lors de la suppression firewalld ne tente pas de changer la ZONE dans le fichier ifcfg. Cela permet de s'assuser qu'un ifdown ne réinitialise pas les paramètres de zone.