firewalld.richlanguage

Documentation du langage Rich

Avec ce langage il est possible de créer des règles firewall plus complexes de manière simple. Ce langage utilise des mots clé avec des valeurs et est une représentation abstraite des règles iptables.

Ce langage étends les éléments de zone courantes (service, port, icmp-block, masquerade, forward-port et source-port) avec des adresses source et de destination, logging, actions et limites pour les logs et les actions.

Ce mémo décris ce langage utilisé en ligne de commande et les interfaces D-Bus. Une règle fait partie d'une zone. Une zone peut contenir de nombreuses règles.

Structure de règle générale

```
rule
 [source]
 [destination]
 service|port|protocol|icmp-block|masquerade|forward-port|source-port
 [log]
 [audit]
 [accept|reject|drop|mark]
```

rule [family="ipv4|ipv6] Si la famille n'est pas fournie, la règle s'applique à IPv4 et IPv6.

source [not] address="address[/mask]"|mac="mac-address"|ipset="ipset" Avec l'adresse source l'origine d'une tentative de connexion peut être limitée à l'adresse source.

destination [not] address="address[/mask]" Une cible peut être limitée avec l'adresse de destination

service name="service name" Ajoute le nom du service à la règle.

port port="port value" protocol="tcp|udp" Le peut être être un numéro de port ou une plage de port. le protocole peut être tcp ou udp

protocol value="protocol value" La valeur du protocole est soit un numéro identifiant ou un nom de protocole

icmp-block name="icmptype name" Un des types icmp supporté par firewalld.

masquerade Active le masquerading dans la règle. Une source et également une destination peuvent être fournis pour limiter le masquerading pour cette zone

forward-port port="port value" protocol="tcp|udp" to-port="port value" to-addr="address" port/paquet forwarding depuis un port local vers un autre port local ou une autre machine ou un autre port sur un autre machine. Il n'est pas possible de spécifier une action ici, forward-port utilise l'action accept en interne

source-port port="port value" protocol="tcp|udp" Le port source peut être un port ou une plage de port.

log [prefix="prefix text"] [level="log level"] [limit value="rate/duration"] Log les tentatives de nouvelles connexions avec le logging kernel, par exemple syslog.

audit [limit value="rate/duration"] Utilise auditd pour le logging

accept [limit value="rate/duration"]

reject [type="reject type"] [limit value="rate/duration"]

drop [limit value="rate/duration"]

mark set="mark[/mask]" [limit value="rate/duration"] Une action peut être accept, reject, drop, ou mark

limit value="rate/duration" Limite des logs, audit et action. Un règle utilisant ce tag match jusqu'à ce que cette règle soit atteinte. La durée est en s, m, h ou d. Maximum : 2/d (2 matchs par jour)

zone_log

zone_deny

zone_allow la chaine zone_log peut être ajoutée à toutes les zones, qui contient toutes les règles de logging. Les règles reject et drop sont placées dans zone_deny et les règles accept dans zone_allow

Exemples

Autoriser les nouvelles connexions IPv4 et IPv6 pour le protocole ah
rule protocol value="ah" accept
autoriser les nouvelles connexions IPv4 et IPv6 pour le service ftp et 1 log par minute avec audit
rule service name="ftp" log limit value="1/m" audit accept
Autoriser les connexions IPv4 depuis 192.168.0.0/24 pour tftp et un log par minute en utilisant syslog
rule family="ipv4" source address="192.168.0.0/24" service name="tftp" log prefix="tftp" level="info" limit value="1/m" accept
Les nouvelles connexions de 1 :2 :3 :4 :6 : : vers radius sont rejetées et loggées à un taux de 3 par minute. Les nouvelles connexions depuis les autres sources sont acceptées
rule family="ipv6" source address="1 :2 :3 :4 :6 : :" service name="radius" log prefix="dns" level="info" limit value="3/m" reject
rule family="ipv6" service name="radius" accept
forward les packets IPv6 reçus de 1 :2 :3 :4 :6 : : sur le port 4011 avec tcp vers 1 : :2 :3 :4 :7 sur le port 4012
rule family="ipv6" source address="1 :2 :3 :4 :6 : :" forward-port to-addr="1 : :2 :3 :4 :7" to-port="4012" protocol="tcp" port="4011"
Liste blanche d'adresse source pour autoriser les connexions depuis 192.168.2.2
rule family="ipv4" source address="192.168.2.2" accept
Liste noire pour rejeter toutes les connexions depuis 192.168.2.3
rule family="ipv4" source address="192.168.2.3" reject type="icmp-admin-prohibited"
liste noire pour supprimer toutes les connexions depuis 192.168.2.4
rule family="ipv4" source address="192.168.2.4" drop