firewalld.zone

Fichiers de configuration de zone firewalld

Un fichier de configuration de zone contient les informations pour une zone.

Structure d'un fichier de configuration de zone

```
<?xml version="1.0" encoding="utf-8"?>
<zone [version="versionstring"] [target="ACCEPT|%%REJECT%%|DROP"]>
 [ <short>short description</short> ]
 [ <description>description</description> ]
 [ <interface name="string"/> ]
 [ <source address="address[/mask]"|mac="MAC"|ipset="ipset"/> ]
 [ <service name="string"/> ]
 [ <port port="portid[-portid]" protocol="tcp|udp"/> ]
 [ <protcol value="protocol"/> ]
 [ <icmp-block name="string"/> ]
 [ <icmp-block-inversion/> ]
 [ <masquerade/> ]
 [ <forward-port port="portid[-portid]" protocol="tcp|udp" [to-port="portid[-portid]"]
[to-addr="ipv4address"]/> ]
 [ <source-port port="portid[-portid]" protocol="tcp|udp"/> ]
 [
  <rule [family="ipv4|ipv6"]>
  [ <source address="address[/mask]"|mac="MAC"|ipset="ipset" [invert="True"]/> ]
  [ <destination address="address[/mask]" [invert="True"]/> ]
  [
   <service name="string"/> |
   <port port="portid[-portid]" protocol="tcp|udp"/> |
   <protocol value="protocol"/> |
   <icmp-block name="icmptype"/> |
   <masquerade/> |
   <forward-port port="portid[-portid]" protocol="tcp|udp" [to-port="portid[-portid]"] [to-addr="address"]/>
  ]
  [ <log [prefix="prefixtext"] [level="emerg|alert|crit|err|warn|notice|info|debug"]> [<limit
value="rate/duration"/>] </log> ]
  [ <audit> [<limit value="rate/duration"/>] </audit> ]
  [
   <accept> [<limit value="rate/duration"/>] </accept> |
   <reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |
   <drop> [<limit value="rate/duration"/>] </drop> |
   <mark set="mark[/mask]"> [<limit value="rate/duration"/>] </mark>
  ]
  </rule>
 ]
</zone>
```

zone définis la zone. Obligatoire et ne peut exister qu'une seule fois. Ses attributs optionnels sont :

version="string" Version de la zone

target="ACCEPT|%%REJECT%%|DROP" Accèpte, rejète ou supprime tout paquets qui ne correspond à aucune règle.

short Description courte pour la zone

description Description complète de la zone

interface Permet de lier une interface à une zone. Peut être spécifié plusieurs fois. l'attribut name="string" spécifie le nom de l'interface.

source Permet de lier une adresse source, plage d'adresse, adresse MAC ou ipset à une zone. Peut être spécifié plusieurs fois. Les attributs sont :

address="address[/mask]" IP ou réseau source.

mac="MAC" Adresse MAC source

ipset="ipset" ipset source

service Spécifie un service. Peut être spécifié plusieurs fois. l'argument name="string" spécifie un service à activer

port Port à ajouter. Peut être spécifié plusieurs fois

port="portid[-portid]" Port ou plage de port

protocol="tcp|udp" protocole à utiliser

protocol Spécifie un protocole supporté par le système. (voir /etc/protocols). Peut être spécifié plusieurs fois. l'argument value="string" spécifie le nom du protocol.

icmp-block l'argument name="string est le nom d'un type ICMP (firewall-cmd –list=icmptypes pour les lister)

icmp-block-inversion Inverse icmp-block

masquerade IPv4 uniquement. Active le masquerading pour la zone

forward-port IPv4 uniquement. Peut être spécifié plusieurs fois

port="portid[-portid]" Port ou plage de ports

protocol="tcp|udp" Protocole utilisé

to-port="portid[-portid] Port ou plage de port de destination

to-addr="address" adresse IPv4 de destination

source-port Spécifie un port source. Peut être spécifié plusieurs fois

port="portid[-portid]" Port ou plage de ports

protocol="tcp|udp" Protocole utilisé

rule Définis une règle en langage rich. peut être spécifié plusieurs fois. La structure générale est :

```
<rule [family="ipv4|ipv6"]>
 [ <source address="address[/mask]" [invert="True"]/> ]
 [ <destination address="address[/mask]" [invert="True"]/> ]
 [
  <service name="string"/> |
  <port port="portid[-portid]" protocol="tcp|udp"/> |
  <protocol value="protocol"/> |
  <icmp-block name="icmptype"/> |
  <masquerade/> |
  <forward-port port="portid[-portid]" protocol="tcp|udp" [to-port="portid[-portid]"] [to-addr="address"]/> |
  <source-port port="portid[-portid]" protocol="tcp|udp"/> |
 ]
 [ <log [prefix="prefixtext"] [level="emerg|alert|crit|err|warn|notice|info|debug"]/> [<limit
value="rate/duration"/>] </log> ]
 [ <audit> [<limit value="rate/duration"/>] </audit> ]
 [
  <accept> [<limit value="rate/duration"/>] </accept> |
  <reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |
  <drop> [<limit value="rate/duration"/>] </drop> |
  <mark set="mark[/mask]"> [<limit value="rate/duration"/>] </mark>
 ]
</rule>
```

La structure de règle pour les listing black ou white source :

```
<rule [family="ipv4|ipv6"]>
 <source address="address[/mask]" [invert="True"]/>
 [ <log [prefix="prefixtext"] [level="emerg|alert|crit|err|warn|notice|info|debug"]/> [<limit
value="rate/duration"/>] </log> ]
 [ <audit> [<limit value="rate/duration"/>] </audit> ]
 <accept> [<limit value="rate/duration"/>] </accept> |
 <reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |
 <drop> [<limit value="rate/duration"/>] </drop>
</rule>
```