Version : **2021.01**

Dernière mise-à-jour : 2021/03/01 06:37

LRF402 - Netfilter et Firewalld

Contenu du Module

Les Problématiques

L'IP Spoofing

L'IP Spoofing consiste en faire croire à un serveur que sa machine possède une adresse IP autre que celle réellement attribuée. Le but de cette

opération est de se placer en tant que point de passage obligatoire des paquets envoyés entre le serveur et le vrai *propriétaire* de l'adresse IP spoofée. Le mécanisme est la suivante :

- L'attaquant change son adresse IP en prenant une à laquelle le serveur cible fera confiance,
- L'attaquant envoie une requête au serveur en stipulant une route de communication qui passe par l'adresse IP réelle de l'attaquant,
- L'attaquant reprend son adresse IP réelle,
- Le serveur accepte la requête car elle provient d'une adresse IP à laquelle il peux faire confiance et renvoie une réponse en utilisant la route spécifiée par l'attaquant,
- Le client utilise la route spécifiée par l'attaquant pour répondre au serveur.

Déni de Service (DoS)

Une attaque de déni de service consiste à rendre inopérable une machine en lui envoyant une grande quantité de données inutiles. Un exemple de ce type d'attaque s'appelle un *ping flood* :

- L'attaquant prend l'adresse IP de sa cible,
- Il envoie ensuite un ping à une machine de diffusion,
- La machine de diffusion envoie ce même ping à un grand nombre de clients en spécifiant l'origine de la requête,
- L'attaquant reprend son adresse IP d'origine,
- Tous les clients renvoie une réponse au ping *en même temps* à la cible.

SYN Flooding

Le **SYN Flooding**, aussi appelé un *SYN-ACK Attack*, consiste à envoyer vers une cible de multiples paquets **SYN** très rapidement. La cible répond à chaque paquet reçu avec un paquet **ACK** et attend une réponse **ACK** de l'attaquant. A ce stade pour chaque ACK renvoyé par la cible, une connexion dite *semi-ouverte* existe entre les deux machines. La cible doit réserver une petite partie de sa mémoire pour chaque connexion semi-ouverte jusqu'au *time-out* de la dite semi-connexion. Si l'attaquant envoie très rapidement des paquets SYN, le système de time-out n'a pas la possibilité d'expirer les semi-connexions précédentes. Dans ce cas la mémoire de la cible se remplit et on obtient un *buffer overflow*.

Flood

Le **Flood** consiste à envoyer très rapidement des gros paquets **ICMP** vers la cible.

Le Contre-Mesure

Le contre-mesure est principalement l'utilisation d'un pare-feu.

Le Pare-feu Netfilter/iptables

Netfilter est composé de 5 *hooks* :

- NF_IP_PRE_ROUTING
- NF_IP_LOCAL_IN
- NF_IP_LOCAL_OUT
- NF_IP_FORWARD
- NF_IP_POSTROUTING

Ces hooks sont utilisés par deux branches, la première est celle concernée par les paquets qui entrent vers des services locaux :

- NF_IP_PRE_ROUTING > NF_IP_LOCAL_IN > NF_IP_LOCAL_OUT > NF_IP_POSTROUTING

tandis que la deuxième concerne les paquets qui traversent la passerelle:

- NF_IP_PRE_ROUTING > NF_IP_FORWARD > NF_IP_POSTROUTING

Si IPTABLES a été compilé en tant que module, son utilisation nécessite le chargement de plusieurs modules supplémentaires en fonction de la situation:

- iptable_filter
- iptable_mangle
- iptable_net
- etc

Netfilter est organisé en **tables**. La commande **iptables** de netfilter permet d'insérer des **policies** dans les **chaines**:

- La table **FILTER**
  - La chaîne INPUT
    - Concerne les paquets entrants
      - Policies: ACCEPT, DROP, REJECT
  - La chaîne OUTPUT
    - Concerne les paquets sortants
      - Policies: ACCEPT, DROP, REJECT
  - La chaîne FORWARD
    - Concerne les paquets traversant le par-feu.
      - Policies: ACCEPT, DROP, REJECT

Si aucune table n'est précisée, c'est la table FILTER qui s'applique par défaut.

- La table **NAT**
  - La chaîne PREROUTING
    - Permet de faire la translation d'adresse de destination
      - Cibles: SNAT, DNAT, MASQUERADE
  - La chaîne POSTROUTING
    - Permet de faire la translation d'adresse de la source
      - Cibles: SNAT, DNAT, MASQUERADE
  - Le cas spécifique OUTPUT
    - Permet la modification de la destination des paquets générés localement
- La table **MANGLE**
  - Permet le marquage de paquets générés localement (OUTPUT) et entrants (PREROUTING)

Les **policies** sont:

- ACCEPT
  - Permet d'accepter le paquet concerné
- DROP
  - Permet de rejeter le paquet concerné sans générer un message d'erreur
- REJECT

    - Permet de rejeter le paquet concerné en générant une message d'erreur

Les **cibles** sont:

- SNAT
    - Permet de modifier l'adresse source du paquet concerné
- DNAT
    - Permet de modifier l'adresse de destination du paquet concerné
- MASQUERADE
    - Permet de remplacer l'adresse IP privée de l'expéditeur par un socket public de la passerelle.

IPTABLES peut être configuré soit par des outils tels shorewall, soit en utilisant des lignes de commandes ou un script. Dans ce dernier cas, la ligne prend la forme:

```
# IPTABLES --action CHAINE --option1 --option2
```

Les actions sont:

Action	Abréviation	Déscription
- -append	-A	Ajouter une règle à la fin de la chaîne spécifiée
- -delete	-D	Supprimer une règle en spécifiant son numéro ou la règle à supprimer
- -replace	-R	Permet de remplacer la règle spécifée par son numéro
- -insert	-I	Permet d'insérer une règle à l'endroit spécifié
- -list	-L	Permet d'afficher des règles
- -flush	-F	Permet de vider toutes les règles d'une chaîne

Les options sont:

Option	Abréviation	Déscription
- -protocol	-p	Permet de spécifier un protocol - tcp, udp, icmp, all
- -source	-s	Permet de spécifier une adresse source
- -destination	-d	Permet de spécifier une adresse de destination
- -in-interface	-i	Permet de spécifier une interface réseau d'entrée

Option	Abréviation	Déscription
- -out-interface	-o	Permet de spécifier une interface réseau de sortie
- -fragment	-f	Permet de ne spécifier que les paquets fragmentés
- -source-port	-sport	Permet de spécifier un port source ou une plage de ports source
- -destination-port	-dport	Permet de spécifier un port de destination ou une plage de ports de destination
- -tcp-flags	s/o	Permet de spécifier un flag TCP à matcher - SYN, ACK, FIN, RST, URG, PSH, ALL, NONE
- -icmp-type	s/o	Permet de spécifier un type de paquet ICMP
- -mac-source	s/o	Permet de spécifier une adresse MAC

Les options spécifiques à NET sont:

- -to-destination	s/o	Permet de spécifier l'adresse de destination d'une translation
- -to-source	s/o	Permet spécifier l'adresse source d'une translation

Les options spécifiques aux LOGS sont:

- -log-level	s/o	Permet de spécifier le niveau de logs
- -log-prefix	s/o	Permet de spécifier un préfix pour les logs

L'option spécifique au STATEFUL est:

- -state	s/o	Permet de spécifier l'état du paquet à vérifier

Ce dernier cas fait référence au STATEFUL. Le STATEFUL est la capacité du par-feu à enregistrer dans une table spécifique, l'état des différentes connexions. Cette table s'appelle une **table d'état**. Le principe du fonctionnement de STATEFUL est simple, à savoir, si le paquet entrant appartient à une communication déjà établie, celui-ci n'est pas vérifié.

Il existe 4 états:

- NEW
  - Le paquet concerne une nouvelle connexion et contient donc un flag SYN à 1
- ESTABLISHED
  - Le paquet concerne une connexion déjà établie. Le paquet ne doit contenir **ni** flag SYN à 1, **ni** flag FIN à 1
- RELATED

    - Le paquet est d'une connexion qui présente une relation avec une autre connexion
- INVALID
    - La paquet provient d'une connexion anormale.

LAB #1 - Configuration par Scripts sous RHEL/CentOS 6 et versions Antérieures

Dans l'exemple suivant, expliquez le fonctionnement du script en détaillant les règles écrites :

```
#!/bin/bash
####################################
# proxy server IP
PROXY_SERVER="192.168.1.2"
# Interface connected to Internet
INTERNET="eth1"
# Interface connected to LAN
LAN_IN="eth0"
# Local Interface
LOCAL="lo"
# Squid port
PROXY_PORT="8080"
# DO NOT MODIFY BELOW
# Clean old firewall
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
# Load IPTABLES modules for NAT and IP conntrack support
modprobe ip_conntrack
modprobe ip_conntrack_ftp
# For win xp ftp client
modprobe ip_nat_ftp
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward
# Setting default filter policy
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
# Unlimited access to loop back
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# Allow UDP, DNS and Passive FTP
iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
# set this system as a router for Rest of LAN
iptables --table nat --append POSTROUTING --out-interface $INTERNET -j MASQUERADE
iptables --append FORWARD --in-interface $LAN_IN -j ACCEPT
# unlimited access to LAN
iptables -A INPUT -i $LAN_IN -j ACCEPT
iptables -A OUTPUT -o $LAN_IN -j ACCEPT
# DNAT port 80 request comming from LAN systems to squid 3128 ($SQUID_PORT) aka transparent proxy
iptables -t nat -A PREROUTING -i $LAN_IN -p tcp --dport 80 -j DNAT --to $PROXY_SERVER:$PROXY_PORT
# iptables -t nat -A PREROUTING -i br0 -p tcp --dport 80 -j REDIRECT --to-port 3128
# if it is same system
iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j REDIRECT --to-port $PROXY_PORT
# DROP everything and Log it
iptables -A INPUT -j LOG
iptables -A INPUT -j DROP
```

LAB #2 - La Configuration par firewalld sous RHEL/CentOS 7

firewalld est à Netfilter ce que NetworkManager est au réseau. firewalld utilise des **zones** - des jeux de règles pré-définis dans lesquels sont placés les interfaces :

- **trusted** - un réseau fiable. Dans ce cas tous les ports sont autorisés,
- **work**, **home**, **internal** - un réseau partiellement fiable. Dans ce cas quelques ports sont autorisés,
- **dmz**, **public**, **external** - un réseau non fiable. Dans ce cas peu de ports sont autorisés,
- **block**, **drop** - tout est interdit. La zone drop n'envoie pas de messages d'erreurs.

Important - Une interface ne peut être que dans une zone à la fois tandis que plusieurs interfaces peuvent être dans la même zone.

Le service firewalld doit toujours être lancé :

```
[root@centos7 ~]# systemctl status firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
   Active: active (running) since Tue 2015-07-07 15:53:56 CEST; 1 day 21h ago
 Main PID: 493 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─493 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Jul 07 15:53:56 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
```

La Configuration de Base de firewalld

La configuration par défaut de firewalld se trouve dans **/usr/lib/firewalld** :

```
[root@centos7 ~]# ls -l /usr/lib/firewalld/
total 12
drwxr-x---. 2 root root 4096 Jun  4 09:52 icmptypes
drwxr-x---. 2 root root 4096 Jun  4 09:52 services
drwxr-x---. 2 root root 4096 Jun  4 09:52 zones
[root@centos7 ~]# ls -l /usr/lib/firewalld/zones
total 36
-rw-r-----. 1 root root 299 Mar  6 00:35 block.xml
-rw-r-----. 1 root root 293 Mar  6 00:35 dmz.xml
-rw-r-----. 1 root root 291 Mar  6 00:35 drop.xml
-rw-r-----. 1 root root 304 Mar  6 00:35 external.xml
```

```
-rw-r-----. 1 root root 400 Mar  6 00:35 home.xml
-rw-r-----. 1 root root 415 Mar  6 00:35 internal.xml
-rw-r-----. 1 root root 315 Mar  6 00:35 public.xml
-rw-r-----. 1 root root 162 Mar  6 00:35 trusted.xml
-rw-r-----. 1 root root 342 Mar  6 00:35 work.xml
[root@centos7 ~]# ls -l /usr/lib/firewalld/services
total 192
-rw-r-----. 1 root root 412 Mar  6 00:35 amanda-client.xml
-rw-r-----. 1 root root 320 Mar  6 00:35 bacula-client.xml
-rw-r-----. 1 root root 346 Mar  6 00:35 bacula.xml
-rw-r-----. 1 root root 305 Mar  6 00:35 dhcpv6-client.xml
-rw-r-----. 1 root root 234 Mar  6 00:35 dhcpv6.xml
-rw-r-----. 1 root root 227 Mar  6 00:35 dhcp.xml
-rw-r-----. 1 root root 346 Mar  6 00:35 dns.xml
-rw-r-----. 1 root root 374 Mar  6 00:35 ftp.xml
-rw-r-----. 1 root root 476 Mar  6 00:35 high-availability.xml
-rw-r-----. 1 root root 448 Mar  6 00:35 https.xml
-rw-r-----. 1 root root 353 Mar  6 00:35 http.xml
-rw-r-----. 1 root root 372 Mar  6 00:35 imaps.xml
-rw-r-----. 1 root root 454 Mar  6 00:35 ipp-client.xml
-rw-r-----. 1 root root 427 Mar  6 00:35 ipp.xml
-rw-r-----. 1 root root 517 Mar  6 00:35 ipsec.xml
-rw-r-----. 1 root root 233 Mar  6 00:35 kerberos.xml
-rw-r-----. 1 root root 221 Mar  6 00:35 kpasswd.xml
-rw-r-----. 1 root root 232 Mar  6 00:35 ldaps.xml
-rw-r-----. 1 root root 199 Mar  6 00:35 ldap.xml
-rw-r-----. 1 root root 385 Mar  6 00:35 libvirt-tls.xml
-rw-r-----. 1 root root 389 Mar  6 00:35 libvirt.xml
-rw-r-----. 1 root root 424 Mar  6 00:35 mdns.xml
-rw-r-----. 1 root root 211 Mar  6 00:35 mountd.xml
-rw-r-----. 1 root root 190 Mar  6 00:35 ms-wbt.xml
-rw-r-----. 1 root root 171 Mar  6 00:35 mysql.xml
-rw-r-----. 1 root root 324 Mar  6 00:35 nfs.xml
-rw-r-----. 1 root root 389 Mar  6 00:35 ntp.xml
```

```
-rw-r-----. 1 root root 335 Mar  6 00:35 openvpn.xml
-rw-r-----. 1 root root 433 Mar  6 00:35 pmcd.xml
-rw-r-----. 1 root root 474 Mar  6 00:35 pmproxy.xml
-rw-r-----. 1 root root 544 Mar  6 00:35 pmwebapis.xml
-rw-r-----. 1 root root 460 Mar  6 00:35 pmwebapi.xml
-rw-r-----. 1 root root 357 Mar  6 00:35 pop3s.xml
-rw-r-----. 1 root root 181 Mar  6 00:35 postgresql.xml
-rw-r-----. 1 root root 261 Mar  6 00:35 proxy-dhcp.xml
-rw-r-----. 1 root root 446 Mar  6 00:35 radius.xml
-rw-r-----. 1 root root 517 Mar  6 00:35 RH-Satellite-6.xml
-rw-r-----. 1 root root 214 Mar  6 00:35 rpc-bind.xml
-rw-r-----. 1 root root 384 Mar  6 00:35 samba-client.xml
-rw-r-----. 1 root root 461 Mar  6 00:35 samba.xml
-rw-r-----. 1 root root 550 Mar  6 00:35 smtp.xml
-rw-r-----. 1 root root 463 Mar  6 00:35 ssh.xml
-rw-r-----. 1 root root 393 Mar  6 00:35 telnet.xml
-rw-r-----. 1 root root 301 Mar  6 00:35 tftp-client.xml
-rw-r-----. 1 root root 437 Mar  6 00:35 tftp.xml
-rw-r-----. 1 root root 211 Mar  6 00:35 transmission-client.xml
-rw-r-----. 1 root root 475 Mar  6 00:35 vnc-server.xml
-rw-r-----. 1 root root 310 Mar  6 00:35 wbem-https.xml
[root@centos7 ~]# ls -l /usr/lib/firewalld/icmptypes/
total 36
-rw-r-----. 1 root root 222 Mar  6 00:35 destination-unreachable.xml
-rw-r-----. 1 root root 173 Mar  6 00:35 echo-reply.xml
-rw-r-----. 1 root root 210 Mar  6 00:35 echo-request.xml
-rw-r-----. 1 root root 225 Mar  6 00:35 parameter-problem.xml
-rw-r-----. 1 root root 185 Mar  6 00:35 redirect.xml
-rw-r-----. 1 root root 227 Mar  6 00:35 router-advertisement.xml
-rw-r-----. 1 root root 223 Mar  6 00:35 router-solicitation.xml
-rw-r-----. 1 root root 248 Mar  6 00:35 source-quench.xml
-rw-r-----. 1 root root 253 Mar  6 00:35 time-exceeded.xml
```

Ces fichiers sont au format **xml**, par exemple :

```
[root@centos7 ~]# cat /usr/lib/firewalld/zones/home.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Home</short>
  <description>For use in home areas. You mostly trust the other computers on networks to not harm your computer.
Only selected incoming connections are accepted.</description>
  <service name="ssh"/>
  <service name="ipp-client"/>
  <service name="mdns"/>
  <service name="samba-client"/>
  <service name="dhcpv6-client"/>
</zone>
```

La configuration de firewalld ainsi que les définitions et règles personnalisées se trouvent dans **/etc/firewalld** :

```
[root@centos7 ~]# ls -l /etc/firewalld/
total 8
-rw-r-----. 1 root root 1026 Mar  6 00:35 firewalld.conf
drwxr-x---. 2 root root    6 Mar  6 00:35 icmptypes
-rw-r-----. 1 root root  271 Mar  6 00:35 lockdown-whitelist.xml
drwxr-x---. 2 root root    6 Mar  6 00:35 services
drwxr-x---. 2 root root   23 Mar  6 00:35 zones
[root@centos7 ~]# ls -l /etc/firewalld/zones/
total 4
-rw-r--r--. 1 root root 315 Mar  8 14:05 public.xml
[root@centos7 ~]# ls -l /etc/firewalld/services/
total 0
[root@centos7 ~]# ls -l /etc/firewalld/icmptypes/
total 0
```

Le fichier de configuration de firewalld est **/etc/firewalld/firewalld.conf** :

```
[root@centos7 ~]# cat /etc/firewalld/firewalld.conf
# firewalld config file
```

```
# default zone
# The default zone used if an empty zone string is used.
# Default: public
DefaultZone=public

# Minimal mark
# Marks up to this minimum are free for use for example in the direct
# interface. If more free marks are needed, increase the minimum
# Default: 100
MinimalMark=100

# Clean up on exit
# If set to no or false the firewall configuration will not get cleaned up
# on exit or stop of firewalld
# Default: yes
CleanupOnExit=yes

# Lockdown
# If set to enabled, firewall changes with the D-Bus interface will be limited
# to applications that are listed in the lockdown whitelist.
# The lockdown whitelist file is lockdown-whitelist.xml
# Default: no
Lockdown=no

# IPv6_rpfilter
# Performs a reverse path filter test on a packet for IPv6. If a reply to the
# packet would be sent via the same interface that the packet arrived on, the
# packet will match and be accepted, otherwise dropped.
# The rp_filter for IPv4 is controlled using sysctl.
# Default: yes
IPv6_rpfilter=yes
```

La Commande firewall-cmd

firewalld s'appuie sur netfilter. Pour cette raison, l'utilisation de firewall-cmd est incompatible avec l'utilisation des commandes iptables et system-config-firewall.

Important - firewall-cmd est le front-end de firewalld en ligne de commande. Il existe aussi la commande **firewall-config** qui lance un outi de configuration graphique.

Pour obtenir la liste de toutes les zones prédéfinies, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

Pour obtenir la liste de toutes les services prédéfinis, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-services
RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https
imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql nfs ntp
openvpn pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client smtp ssh
telnet tftp tftp-client transmission-client vnc-server wbem-https
```

Pour obtenir la liste de toutes les types ICMP prédéfinis, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-icmptypes
destination-unreachable echo-reply echo-request parameter-problem redirect router-advertisement router-
solicitation source-quench time-exceeded
```

Pour obtenir la liste des zones de la configuration courante, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-active-zones
public
  interfaces: enp0s3
```

Pour obtenir la liste des zones de la configuration courante pour une interface spécifique, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-zone-of-interface=enp0s3
public
```

Pour obtenir la liste des services autorisés pour la zone public, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=public --list-services
dhcpv6-client ssh
```

Pour obtenir toute la configuration pour la zone public, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=public --list-all
public (default, active)
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

Pour obtenir la liste complète de toutes les zones et leurs configurations, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --list-all-zones
block
  interfaces:
  sources:
```

```
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
dmz
  interfaces:
  sources:
  services: ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
drop
  interfaces:
  sources:
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
external
  interfaces:
  sources:
  services: ssh
  ports:
  masquerade: yes
  forward-ports:
  icmp-blocks:
  rich rules:
home
```

```
  interfaces:
  sources:
  services: dhcpv6-client ipp-client mdns samba-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
internal
  interfaces:
  sources:
  services: dhcpv6-client ipp-client mdns samba-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
public (default, active)
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
trusted
  interfaces:
  sources:
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
```

```
  rich rules:
work
  interfaces:
  sources:
  services: dhcpv6-client ipp-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

Pour changer la zone par défaut de public à work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --set-default-zone=work
success
[root@centos7 ~]# firewall-cmd --get-active-zones
work
  interfaces: enp0s3
```

Pour ajouter l'interface ip_fixe à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-interface=ip_fixe
success
[root@centos7 ~]# firewall-cmd --get-active-zones
work
  interfaces: enp0s3 ip_fixe
```

Pour supprimer l'interface ip_fixe à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-interface=ip_fixe
success
[root@centos7 ~]# firewall-cmd --get-active-zones
work
```

```
  interfaces: enp0s3
```

Pour ajouter le service **http** à la zone **work**, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-service=http
success
[root@centos7 ~]# firewall-cmd --zone=work --list-services
dhcpv6-client http ipp-client ssh
```

Pour supprimer le service **http** de la zone **work**, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-service=http
success
[root@centos7 ~]# firewall-cmd --zone=work --list-services
dhcpv6-client ipp-client ssh
```

Pour ajouter un nouveau bloc ICMP, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-icmp-block=echo-reply
success
[root@centos7 ~]# firewall-cmd --zone=work --list-icmp-blocks
echo-reply
```

Pour supprimer un bloc ICMP, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-icmp-block=echo-reply
success
[root@centos7 ~]# firewall-cmd --zone=work --list-icmp-blocks
[root@centos7 ~]#
```

Pour ajouter le port 591/tcp à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-port=591/tcp
```

```
success
[root@centos7 ~]# firewall-cmd --zone=work --list-ports
591/tcp
```

Pour supprimer le port 591/tcp à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-port=591/tcp
success
[root@centos7 ~]# firewall-cmd --zone=work --list-ports
[root@centos7 ~]#
```

Pour créer un nouveau service, il convient de :

- copier un fichier existant se trouvant dans le répertoire **/usr/lib/firewalld/services** vers **/etc/firewalld/services**,
- modifier le fichier,
- recharger la configuration de firewalld,
- vérifier que firewalld voit le nouveau service.

Par exemple :

```
[root@centos7 ~]# cp /usr/lib/firewalld/services/http.xml /etc/firewalld/services/filemaker.xml
[root@centos7 ~]#
[root@centos7 ~]# cat /etc/firewalld/services/filemaker.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>FileMakerPro</short>
  <description>fichier de service firewalld pour FileMaker Pro</description>
  <port protocol="tcp" port="591"/>
</service>
[root@centos7 ~]#
[root@centos7 ~]# firewall-cmd --reload
success
[root@centos7 ~]#
[root@centos7 ~]# firewall-cmd --get-services
```

```
RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns filemaker ftp high-availability
http https imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql
nfs ntp openvpn pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client
smtp ssh telnet tftp tftp-client transmission-client vnc-server wbem-https
```

La Configuration Avancée de firewalld

La configuration de base de firewalld ne permet que la configuration des zones, services, blocs ICMP et les ports non-standard. Cependant firewalld peut également être configuré avec des **Rich Rules** ou ***Règles Riches***. Rich Rules ou Règles Riches évaluent des **critères** pour ensuite entreprendre une **action**.

Les **Critères** sont :

- **source address=“<adresse_IP>“**
- **destination address=”<adresse_IP>“**,
- **rule port port=”<numéro_du_port>“**,
- **service name=<nom_d'un_sevice_prédéfini>**.

Les **Actions** sont :

- **accept**,
- **reject**,
  - une Action reject peut être associée avec un message d'erreur spécifique par la clause **type=”<type_d'erreur>**,
- **drop**.

Saisissez la commande suivante pour ouvrir le port 80 :

```
[root@centos7 ~]# firewall-cmd --add-rich-rule='rule port port="80" protocol="tcp" accept'
success
```

Important - Notez que la Rich Rule doit être entourée de caractères '.

Saisissez la commande suivante pour visualiser la règle iptables pour IPv4 :

```
[root@centos7 ~]# iptables -L -n | grep 80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 ctstate NEW
```

Saisissez la commande suivante pour visualiser la règle iptables pour IPv6 :

```
[root@centos7 ~]# ip6tables -L -n | grep 80
ACCEPT     udp      ::/0                 fe80::/64           udp dpt:546 ctstate NEW
ACCEPT     tcp      ::/0                 ::/0                tcp dpt:80 ctstate NEW
```

Important - Notez que la Rich Rule a créé deux règles, une pour IPv4 et une deuxième pour IPv6. Une règle peut être créée pour IPv4 seul en incluant le Critère **family=ipv4**. De la même façon, une règle peut être créée pour IPv6 seul en incluant le Critère **family=ipv6**.

Cette nouvelle règle est écrite en mémoire mais non pas sur disque. Pour l'écrire sur disque dans le fichier zone se trouvant dans **/etc/firewalld**, il faut ajouter l'option **–permanent** :

```
[root@centos7 ~]# firewall-cmd --add-rich-rule='rule port port="80" protocol="tcp" accept' --permanent
success
[root@centos7 ~]#
[root@centos7 ~]# cat /etc/firewalld/zones/work.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Work</short>
  <description>For use in work areas. You mostly trust the other computers on networks to not harm your computer.
Only selected incoming connections are accepted.</description>
  <service name="ipp-client"/>
  <service name="dhcpv6-client"/>
  <service name="ssh"/>
```

```
  <rule>
    <port protocol="tcp" port="80"/>
    <accept/>
  </rule>
</zone>
```

Important - Attention ! La règle ajoutée avec l'option –permanent n'est pas prise en compte imédiatement mais uniquement au prochain redémmarge. Pour qu'une règle soit appliquée immédiatement **et** être écrite sur disque, il faut saisir la commande deux fois dont une avec l'option –permanent et l'autre sans l'option –permanent.

Pour visualiser cette règle dans la configuration de firewalld, il convient de saisir la commande suivante :

```
[root@centos7 ~]# firewall-cmd --list-all-zones
...
work (default, active)
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ipp-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
    rule port port="80" protocol="tcp" accept
```

Notez que la Rich Rule est créée dans la Zone par Défaut. Il est possible de créer une Rich Rule dans une autre zone en utilisant l'option **–zone=<zone>** de la commande firewall-cmd :

```
[root@centos7 ~]# firewall-cmd --zone=public --add-rich-rule='rule port port="80" protocol="tcp" accept'
```

```
success
[root@centos7 ~]# firewall-cmd --list-all-zones
...
public
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
    rule port port="80" protocol="tcp" accept
trusted
  interfaces:
  sources:
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
work (default, active)
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ipp-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
    rule port port="80" protocol="tcp" accept
```

Pour supprimer une Rich Rule, il faut copier la ligne entière la concernant qui se trouve dans la sortie de la commande **firewall-cmd –list-all-zones** :

```
[root@centos7 ~]# firewall-cmd --zone=public --remove-rich-rule='rule port port="80" protocol="tcp" accept'
success
```

Le mode Panic de firewalld

Le mode Panic de firewalld permet de bloquer tout le trafic avec une seule commande. Pour connaître l'état du mode Panic, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --query-panic
no
```

Pour activer le mode Panic, il convient de saisir la commande suivante :

```
[root@centos7 ~]# firewall-cmd --panic-on
success
[root@centos7 ~]# firewall-cmd --query-panic
yes
```

Pour désactiver le mode Panic, il convient de saisir la commande suivante :

```
[root@centos7 ~]# firewall-cmd --panic-off
success
[root@centos7 ~]# firewall-cmd --query-panic
no
```

<html>

</html>