TP 2_2 : Firewalld

Firewalld est un pare-feu sous Linux qui est facile à mettre en oeuvre et paramétrer, par rapport à iptables ou son successeur nftables.

Il est livré par défaut sous CentOS et Fedora, mais il est possible de l'installer sur d'autres distributions Linux telles que Gentoo ou Debian.

1. Informations générales sur firewalld

Si le service n'est pas présent sur le système, il convient de l'installer via la commande suivante :

```
# yum install firewalld
```

Une fois le service installé, il faut alors l'activer et redémarrer son serveur :

```
# systemctl enable firewalld
```

En tant que service, on peut administrer firewalld en l'arrêtant :

```
# systemctl stop firewalld
```

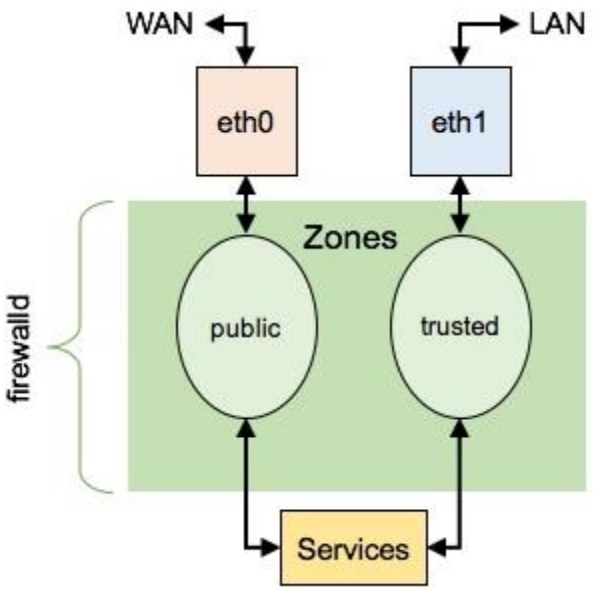
Ou, au contraire, en le démarrant :

```
# systemctl start firewalld
```

Pour connaître l'état de son pare-feu :

```
# firewall-cmd --state
```

2. Concept des zones



On distingue les zones prédéfinies suivantes :

- **zone drop:** le niveau le plus bas de confiance. Toute connexion entrante est supprimée sans notification et seules les connexions sortantes sont autorisées.

- **zone block:** zone similaire à celle-ci-dessus, mais au lieu de supprimer les connexions entrantes sans notification, ces flux sont rejetés à l'aide d'un message *icmp-host-prohibited* (ou *icmp6-adm-prohibited* pour IPv6).

- **zone public:** représente l'ensemble des réseaux publics ou non sécurisés. On ne fait pas confiance aux autres ordinateurs ou serveurs mais, on peut traiter les connexions entrantes au cas par cas à l'aide de règles.

- **zone external:** représente les réseaux externes lorsque l'on utilise le pare-feu local comme une passerelle. Dans ce cas, la zone est configurée pour le "*masquerading NAT*" et les réseaux internes demeurent ainsi privés mais accessibles.

- **zone internal:** représente l'autre face de la zone *external*, utilisée pour la portion interne d'une passerelle. Les serveurs sont totalement accrédités et certains services supplémentaires peuvent mêmes être disponibles.

- **zone dmz:** utilisée pour les serveurs au sein d'une zone démilitarisée ou DMZ. Seules quelques connexions entrantes sont alors autorisées.

- **zone work:** utilisées pour des machines de travail permettant de faire confiance à la plupart des serveurs du réseau. Quelques services supplémentaires pourront être autorisés.

- **zone home:** une zone de sécurité personnelle. Cela implique la plupart du temps que l'on fait confiance aux autres machines et que certains autres services peuvent aussi être accrédités.

- **zone trusted:** permet de faire confiance à toutes les machines du réseau. Il s'agit du niveau de confiance le plus élevé à utiliser avec précaution.

a. Lister le paramétrage des zones

Pour lister les différentes zones disponibles il faut exécuter l'instruction :

```
# firewall-cmd --get-zones
```

```
[root@srv1 ofppt]# firewall-cmd --get-zones
block dmz drop external home internal libvirt nm-shared public trusted work
[root@srv1 ofppt]#
```

Il est aussi possible de lister la configuration de l'ensemble des zones via la commande :

```
# firewall-cmd --list-all-zone
```

```
[root@srv1 ofppt]# firewall-cmd --list-all-zone
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

dmz
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
```

Il est possible de détailler l'ensemble de la configuration d'une zone particulière en exécutant la commande ci-dessous:

```
# firewall-cmd --zone=work --list-all
```

```
[root@srv1 ofppt]# firewall-cmd --zone=work --list-all
work
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@srv1 ofppt]#
```

b. Gestion de la zone par défaut

Pour vérifier la zone utilisée par défaut :

```
# firewalld-cmd --get-default-zone
```

Pour définir une autre zone par défaut (exemple avec une définition de la zone par défaut sur work) :

```
# firewall-cmd --set-default-zone=work
```

c. Créer et supprimer des zones

Pour créer sa propre zone, par exemple ici avec la zone "ofppt" :

```
# firewall-cmd --new-zone=ofppt --permanent
```

Pour supprimer des zones personnalisées :

```
# firewall-cmd --delete-zone=Nom de la zone  --permanent
```

d. Affecter des zones aux interfaces

Chaque interface du système peut être attribuée à une zone.

Si on ne précise pas le **--zone=Nom de la zone** la commande s'effectuera sur la zone par défaut.

Pour ajouter l'interface ens33 à la zone work en l'enlevant de sa précédente zone :

```
#firewall-cmd --change-interface=ens33 --zone=work --permanent
```

Pour ajouter l'interface ens33 à la zone work (interface non affectée à une zone) :

```
# firewall-cmd --add-interface=ens192 --zone=work  --permanent
```

e. Affecter des zones aux sources (sous-réseau / IP)

Pour ajouter le sous-réseau 192.168.21.0/24 à la zone work :

```
# firewall-cmd --zone=work --add-source=192.168.21.0/24  --permanent
```

Pour ajouter une IP seule (192.168.21.200) à la zone work :

```
# firewall-cmd --zone=work --add-source=192.168.21.200 --permanent
```

Pour retirer le sous-réseau 192.168.21.0/24 de la zone work :

```
# firewall-cmd --zone=work --remove-source=192.168.21.0/24  --permanent
```

Pour ajouter le sous-réseau 192.168.21.0/24 à la zone work en l'enlevant de sa précédente zone :

```
# firewall-cmd --zone=work --change-source=192.168.21.0/24  --permanent
```

3. Gestion des services :

Firewalld dispose de services préconfigurés. Ainsi, il sera plus facile d'ouvrir un port et un protocole grâce à son nom.

Pour lister les services autorisés ou disponibles :

```
# firewall-cmd --get-services
```

```
[root@srv1 ofppt]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps
apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bi
tcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-
collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry
 docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger forem
an foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeip
a-trust ftp galera ganglia-client ganglia-master git grafana gre high-availabili
ty http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins
 kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-apiserver ld
ap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns mem
cache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd n
fs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-
vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy pro
metheus proxy-dhcp ptp pulseaudio puppetmaster quassel radius rdp redis redis-se
ntinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc
sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spo
tify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syner
gy syslog syslog-tls telnet tentacle tftp tftp-client tile38 tinc tor-socks tran
smission-client upnp-client vdsm vnc-server wbem-http wbem-https wsman wsmans xd
mcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@srv1 ofppt]#
```

Pour autoriser un service spécifique permanente, il suffit alors d'utiliser l'option ***--add-service.***

Pour lister les services autorisés dans une zone

```
# firewall-cmd --list-services --zone Nom del a zone
```

Pour lister les services autorisés dans une zone (exemple avec la zone work) :

```
# firewall-cmd --list-services --zone work
```

```
[root@srv1 ofppt]# firewall-cmd --list-services --zone work
cockpit dhcpv6-client ssh
[root@srv1 ofppt]#
```

f. Autoriser Apache

Pour avoir des infos sur le service Web

```
# firewall-cmd --info-service=http
```

```
[root@srv1 ofppt]# firewall-cmd --info-service=http
http
  ports: 80/tcp
  protocols:
  source-ports:
  modules:
  destination:
  includes:
  helpers:
[root@srv1 ofppt]#
```

Pour **ajouter** le service Web utiliser la commande

```
#firewall-cmd --permanent  --add-service=http
```

```
[root@srv1 ofppt]# firewall-cmd --zone=public --add-service=http
success
```

Remarque :

La commande prendra effet dès la validation. Cependant, si le parefeu est redémarré ou la configuration rechargée, la commande n'est pas mémorisée. Il faudra pour cela ajouter l'option **--permanent** à la commande.

Pour ajouter le service web (tcp/80 ou HTTP) pour la zone public:

```
#firewall-cmd --zone=public --add-service=http
```

```
[root@srv1 ofppt]# firewall-cmd --permanent --add-service=https
success
[root@srv1 ofppt]#
```

Pour ajouter Apache via HTTPS, il faut également ouvrir le port 443 en activant le service https :

```
#firewall-cmd --permanent --add-service=https
```

Ensuite, recharger le pare-feu pour appliquer ces nouvelles règles :

```
#firewall-cmd --reload
```

```
[root@srv1 ofppt]# firewall-cmd --reload
success
[root@srv1 ofppt]#
```

Pour supprimer un service, par exemple https

```
#firewall-cmd --permanent --remove-service=https
```

```
[root@srv1 ofppt]# firewall-cmd --permanent --remove-service=https
success
[root@srv1 ofppt]#
```

g. Autoriser SAMBA

Autoriser Samba pour la zone public

```
#firewall-cmd --permanent --zone=public --add-service=samba
```

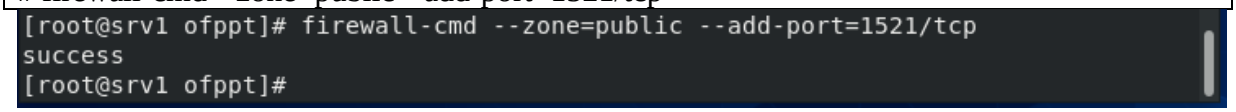
```
[root@srv1 ofppt]# firewall-cmd --permanent --zone=public --add-service=samba
success
[root@srv1 ofppt]#
```

4. La gestion des ports

Il existe des scenarios où les services ne répondent pas aux prérequis de notre infrastructure. Dans cette situation, on peut alors ouvrir spécifiquement un port sur la zone en question, de la même façon qu'on l'a fait pour la gestion des services.

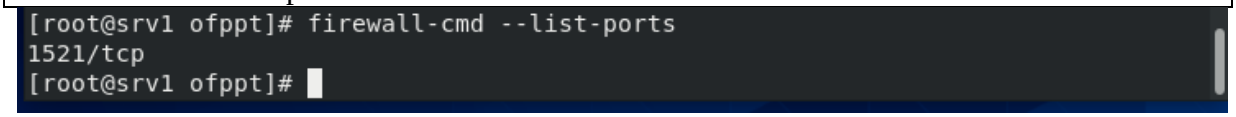
Ainsi, l'ouverture d'un port spécifique s'effectuera à l'aide de l'option **--add-port** de la façon suivante :

```
# firewall-cmd --zone=public --add-port=1521/tcp
```



On peut alors vérifier que l'opération se termine correctement en exécutant la commande ci-dessous, permettant d'afficher les ports ouverts dans la zone par défaut:

```
# firewall-cmd --list-ports
```



5. Reference

https://www.linuxtricks.fr/wiki/firewalld-le-pare-feu-facile-sous-linux

https://www.it-connect.fr/centos-7-utilisation-et-configuration-de-firewalld/

https://www.linuxtricks.fr/wiki/print.php?id=614