Mise en place d'un pare-feu

Projet m2l.org

DUMAS Lucie

Table des matières

Pare-feux 3
Mise en place du pare-feu 4
SSH 4
DNS 4
ICMP 4
HTTP 4
HTTPS 4
FTP 5
FTPS 5
Création du script 6

Pare-feux

Un pare-feu est un dispositif ou un logiciel conçu pour protéger un réseau informatique en contrôlant et en filtrant le trafic qui entre ou sort du réseau. Son objectif principal est de prévenir les accès non autorisés, de bloquer les logiciels malveillants et de surveiller les communications pour assurer la sécurité des systèmes informatiques. Il existe deux types principaux de pare-feu :

- Le pare-feu matériel : Il s'agit d'un dispositif physique placé entre le réseau interne et externe, généralement au niveau de la connexion à Internet. Il filtre le trafic en fonction de règles prédéfinies, bloquant ou autorisant le passage du trafic en fonction de certains critères.

- Le pare-feu logiciel : Il s'agit d'un programme installé sur un ordinateur ou un serveur, qui exerce un contrôle sur les connexions réseau entrantes et sortantes. Les pare-feu logiciels sont souvent utilisés pour protéger des ordinateurs individuels ou des serveurs.

Les règles de filtrage d'un pare-feu sont configurables et peuvent être basées sur divers critères tels que les adresses IP, les ports, les protocoles, etc. En plus de la prévention des accès non autorisés, les pare-feu peuvent également fournir des fonctionnalités telles que la détection d'intrusions, la journalisation des événements et la gestion des politiques de sécurité. Ils sont un élément essentiel de la sécurité informatique pour protéger les réseaux contre les menaces potentielles.

Mise en place du pare-feu

Dans un premier temps, nous devons faire une liste des différents protocoles dont le réseau a besoin ainsi que les différentes machines qui seront concernées :

SSH

- Port utilisé : 22
- Machines et réseaux concernés : toutes les machines du réseau de Beaupeyrat doivent pouvoir communiquer avec toutes les machines de mon réseau

DNS

- Port utilisé : 53
- Machine et réseaux concernés : toutes les machines du réseau de Beaupeyrat vers nos DNS, toutes les machines de notre réseau vers nos DNS, nos DNS vers les DNS de Google

ICMP

- Port utilisé : aucun port
- Machines et réseaux concernés : toutes les machines de notre réseau vers l'extérieur, toutes les machines du réseau de Beaupeyrat vers notre réseau

HTTP

- Port utilisé : 80
- Machines et réseaux concernés : toutes les machines du réseau de Beaupeyrat vers notre serveur web, toutes les machines de notre réseau vers l'extérieur (pour pouvoir utiliser la commande apt install)

HTTPS

- Port utilisé : 443
- Machines et réseaux concernés : toutes les machines du réseau de Beaupeyrat vers notre serveur web, toutes les machines de notre réseau vers l'extérieur

FTP

- Ports utilisés : 20,21, >1024
- Machines et réseaux concernés : le serveur FTP vers toutes les machines du réseau de Beaupeyrat, toutes les machiens du réseau de Beaupeyrat vers le serveur FTP

FTPS

- Ports utilisés : 989, 990, >1024
- Machines et réseaux concernés : le serveur FTP vers toutes les machines du réseau de Beaupeyrat, toutes les machiens du réseau de Beaupeyrat vers le serveur FTP

Création du script

Dans un premier temps, nous téléchargeons le paquet nécessaire sur notre routeur :

```
apt update && apt upgrade
apt install iptables
```

Nous créons ensuite un nouveau script :

```
nano /home/iptables.sh
```

Nous attribuons les droits d'exécution du script :

```
chmod +x /home/iptables.sh
```

```
#!/bin/bash
iptables -F
iptables -X
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#--------------------------------------------------------------------------------
#--                    Statefull                                               --
#--------------------------------------------------------------------------------

#Activer le mode statefull, cest-à-dire lping autorisation automatique d'une réponse à une requête
iptables -A FORWARD -m state --state RELATED,ESTABLISHED  -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED  -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED  -j ACCEPT

#--------------------------------------------------------------------------------
#--                      SSH                                                   --
#--------------------------------------------------------------------------------

#Autorise les machines du réseau de beaupeyrat à accéder à mon réseau en SSH
iptables -A FORWARD -p tcp --dport 22 -s 10.187.20.0/24 -d 10.31.96.0/20 -j ACCEPT

#Autorise les machines du réseau de beaupeyrat à accéder à mon routeur en SSH
iptables -A INPUT -p tcp --dport 22 -s 10.187.20.0/24 -j ACCEPT

#Autorise le serveur de mon réseau à accéder à mon routeur en SSH
iptables -A INPUT -p tcp --dport 22 -s 10.31.96.1 -j ACCEPT

#Autorise le routeur à se connecter en SSH sur les machines du réseau de beaupeyrat
iptables -A OUTPUT -p tcp --dport 22 -d 10.187.20.0/24 -j ACCEPT

#Autorise le routeur à se connecter en SSH sur les machines de mon réseau
iptables -A OUTPUT -p tcp --dport 22 -d 10.31.96.0/20 -j ACCEPT
```

```
#-----------------------------------------------------------------------------------
#--                    DNS                                                        --
#-----------------------------------------------------------------------------------

#Autorise les machines du réseau de beaupeyrat à accéder aux conteneurs DNS
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d 10.31.96.53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.187.20.0/24 -d 10.31.96.54 -j ACCEPT

#Autorise les machines de mon réseau à accéder aux DNS de Google
iptables -A FORWARD -p udp --dport 53 -s 10.31.96.53 -d 8.8.8.8 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.96.53 -d 8.8.4.4 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.96.54 -d 8.8.8.8 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -s 10.31.96.54 -d 8.8.4.4 -j ACCEPT

#Autorise le routeur à accéder aux conteneurs DNS
iptables -A OUTPUT -p udp --dport 53 -d 10.31.96.53 -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -d 10.31.96.54 -j ACCEPT

#-----------------------------------------------------------------------------------
#--                    ICMP                                                       --
#-----------------------------------------------------------------------------------

#Autorise les machines du réseau de beaupeyrat à ping les machines de mon réseau
iptables -A FORWARD -p icmp -s 10.187.20.0/24 -d 10.31.96.0/20 -j ACCEPT

#Autorise les machines de mon réseau à ping vers l'extérieur
iptables -A FORWARD -p icmp -s 10.31.96.0/20 -j ACCEPT

#Autorise les machines du réseau beaupeyrat à ping le routeur
iptables -A INPUT -p icmp -s 10.187.20.0/24 -j ACCEPT

#Autorise les machines de mon réseau à ping le routeur
iptables -A INPUT -p icmp -s 10.31.96.0/20 -j ACCEPT

#Autorise le routeur de mon réseau à communiquer avec l'extérieur
iptables -A OUTPUT -p icmp -j ACCEPT
```

```
#--------------------------------------------------------------------------------
#--                    HTTP                                                    --
#--------------------------------------------------------------------------------

#Autorise les machines du réseau de beaupeyrat à faire des requêtes HTTP au serveur web
iptables -A FORWARD -p tcp --dport 80 -s 10.187.20.0/20 -d 10.31.96.80 -j ACCEPT

#Autorise toutes les machines de mon réseau à faire des requêtes HTTP vers l'extérieur
iptables -A FORWARD -p tcp --dport 80 -s 10.31.96.0/20 -j ACCEPT

#Autorise le routeur à faire des requêtes HTTP vers l'extérieur
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

#--------------------------------------------------------------------------------
#--                    HTTPS                                                   --
#--------------------------------------------------------------------------------

#Autorise les machines du réseau de beaupeyrat à faire des requêtes HTTPS au serveur web
iptables -A FORWARD -p tcp --dport 443 -s 10.187.20.0/20 -d 10.31.96.80 -j ACCEPT

#Autorise toutes les machines de mon réseau à faire des requêtes HTTPS vers l'extérieur
iptables -A FORWARD -p tcp --dport 443 -s 10.31.96.0/20 -j ACCEPT

#Autorise le routeur à faire des requêtes HTTPS vers l'extérieur
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT

#--------------------------------------------------------------------------------
#--                     FTP                                                    --
#--------------------------------------------------------------------------------

#Autorise le serveur ftp à communiquer en FTP avec le réseau de beaupeyrat en mode actif
iptables -A FORWARD -p tcp --dport 20 -s 10.31.96.20 -d 10.187.20.0/24 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -s 10.31.96.20 -d 10.187.20.0/24 -j ACCEPT

#Autorise les machines du réseau de beaupeyrat à communiquer en FTP avec le serveur ftp en
mode actif
iptables -A FORWARD -p tcp --dport 20 -s 10.187.20.0/24 -d 10.31.96.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -s 10.187.20.0/24 -d 10.31.96.20 -j ACCEPT

#Autorise les transferts en mode passif du serveur ftp vers le réseau de beaupeyrat
iptables -A FORWARD -p tcp --dport 1024: -m conntrack --ctstate NEW,RELATED,ESTABLISHED
-s 10.187.20.0/24 -d 10.31.96.20 -j ACCEPT

#Autorise les transferts en mode passif du réseau de beaupeyrat vers le serveur ftp
iptables -A FORWARD -p tcp --dport 1024: -m conntrack --ctstate NEW,RELATED,ESTABLISHED
-s 10.31.96.20 -d 10.187.20.0/24 -j ACCEPT
```

```
#-------------------------------------------------------------------------------
#--                      FTPS                                                 --
#-------------------------------------------------------------------------------

#Autorise les machines du réseau de beaupeyrat à communiquer en FTPS avec le serveur ftp
iptables -A FORWARD -p tcp --dport 989 -s 10.187.20.0/24 -d 10.31.96.20 -j ACCEPT
iptables -A FORWARD -p tcp --dport 990 -s 10.187.20.0/24 -d 10.31.96.20 -j ACCEPT

#Autorise le serveur ftp à communiquer en FTPS avec le réseau de beaupeyrat
iptables -A FORWARD -p tcp --dport 989 -s 10.31.96.20 -d 10.187.20.0/24 -j ACCEPT
iptables -A FORWARD -p tcp --dport 990 -s 10.31.96.20 -d 10.187.20.0/24 -j ACCEPT
```