Aller au contenu

Utile

Pour automatiser la mise en route du firewall il suffit de le mettre dans le rc.local :

Voici un petit Tuto :

On crée **nano /etc/systemd/system/rc-local.service** :

Et y écrire pour lancer rc.local :

```
[Unit]
Description=/etc/rc.local
ConditionPathExists=/etc/rc.local

[Service]
Type=forking
ExecStart=/etc/rc.local start
TimeoutSec=0
StandardOutput=tty
RemainAfterExit=yes
SysVStartPriority=99

[Install]
WantedBy=multi-user.target
```

Puis dans /etc/rc.local on lance le script reglesON :

```
#!/bin/bash
./home/reglesON.sh
```

Mise en place d'un firewall

Création d'un script bash pour remettre les paramètres par défauts après une éventuelle mauvaise manip dans **/home** :

```
#!/bin/bash

iptables -t filter -F
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -t nat     -F
iptables -t mangle -F
```

On lui donne les droits d'exécution,

```
chmod +x nom_du_fichier
```

ROUTEUR

```
#!/bin/bash


#Ecrire le script ci-dessous va effacer tout ce qui a été fati précédemment pour eviter d
iptables -t filter -F #supprime toute les règles filter
iptables -t nat    -F #Supprime toute les règles nat
iptables -t mangle -F #Supprime toute les règles mangle

iptables -P FORWARD DROP
iptables -P INPUT   DROP
iptables -P OUTPUT  DROP

# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
                                                                                      #
# Autorise les requetes DNS à destination de ns1                                      #
iptables -A FORWARD -j ACCEPT -p udp --dport 53 -d 10.31.248.53                       #
iptables -A FORWARD -j ACCEPT -p tcp --dport 53 -d 10.31.248.53                       #
                                                                                      #
# Autorise le retour des requêtes DNS depuis ns1                                      #
iptables -A FORWARD -j ACCEPT -p tcp --sport 53 -s 10.31.248.53                       #
iptables -A FORWARD -j ACCEPT -p udp --sport 53 -s 10.31.248.53                       #
                                                                                      #
# Autorise le routeur à faire des requetes DNS sur ns1                                #
iptables -A OUTPUT -j ACCEPT -p udp --dport 53 -d 10.31.248.53                        #
iptables -A OUTPUT -j ACCEPT -p tcp --dport 53 -d 10.31.248.53                        #
                                                                                      #
# Autorise ns1 à répondre aux requetes DNS du routeur                                 #
iptables -A INPUT -j ACCEPT -p tcp --sport 53 -s 10.31.248.53                         #
iptables -A INPUT -j ACCEPT -p udp --sport 53 -s 10.31.248.53                         #
                                                                                      #
#Autorise les requetes DNS à destination de ns1                                      #
```

```
iptables -A FORWARD -j ACCEPT -p udp --dport 53 -s 10.31.248.53                 #
iptables -A FORWARD -j ACCEPT -p udp --sport 53 -d 10.31.248.53                 #
                                                                                #
iptables -A FORWARD -j ACCEPT -p tcp --dport 53 -s 10.31.248.53                 #
iptables -A FORWARD -j ACCEPT -p tcp --sport 53 -d 10.31.248.53                 #
                                                                                #
#Autorise les requetes à destionation et venant des réseaux 240 et 248          #
iptables -A FORWARD -j ACCEPT -p tcp --dport 80 -s 10.31.240.0/25               #
iptables -A FORWARD -j ACCEPT -p tcp --dport 80 -s 10.31.248.0/25               #
iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -d 10.31.240.0/25               #
iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -d 10.31.248.0/25               #
                                                                                #
iptables -A FORWARD -j ACCEPT -p tcp --dport 443 -s 10.31.240.0/25              #
iptables -A FORWARD -j ACCEPT -p tcp --dport 443 -s 10.31.248.0/25              #
iptables -A FORWARD -j ACCEPT -p tcp --sport 443 -d 10.31.240.0/25              #
iptables -A FORWARD -j ACCEPT -p tcp --sport 443 -d 10.31.248.0/25              #
                                                                                #
                                                                                #
#iptables -A FORWARD -j ACCEPT -p tcp --dport 80 -d 10.31.248.80                #
#iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -s 10.31.248.80                #
                                                                                #
#iptables -A FORWARD -j ACCEPT -p tcp --dport 80 -d 10.31.240.80                #
#iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -s 10.31.240.80                #
                                                                                #
#iptables -A FORWARD -j ACCEPT -p tcp --dport 443 -d 10.31.248.80               #
#iptables -A FORWARD -j ACCEPT -p tcp --sport 443 -s 10.31.248.80               #
                                                                                #
#iptables -A FORWARD -j ACCEPT -p tcp --dport 443 -d 10.31.240.80               #
#iptables -A FORWARD -j ACCEPT -p tcp --sport 443 -s 10.31.240.80               #
                                                                                #
#iptables -A FORWARD -j ACCEPT -p udp --dport 445                               #
#iptables -A FORWARD -j ACCEPT -p tcp --dport 445                               #
#iptables -A FORWARD -j ACCEPT -p udp --sport 445                               #
#iptables -A FORWARD -j ACCEPT -p tcp --sport 445                               #
                                                                                #
#iptables -A FORWARD -j ACCEPT -p udp --dport 3306                              #
iptables -A FORWARD -j ACCEPT -p tcp --dport 3306                               #
#iptables -A FORWARD -j ACCEPT -p udp --sport 3306                              #
iptables -A FORWARD -j ACCEPT -p tcp --sport 3306                               #
                                                                                #
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #

iptables -A FORWARD -j ACCEPT -p icmp
iptables -A INPUT -j ACCEPT -p icmp
iptables -A OUTPUT -j ACCEPT -p icmp


#ACCES INTERNET
iptables -A INPUT  -p tcp --dport 80  -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80  -j ACCEPT
iptables -A INPUT  -p tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT


#ouverture du port 22 pour le routeur
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
iptables -A INPUT -p tcp --sport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT

#SSH pour tout le monde
iptables -A FORWARD  -p tcp --dport 22 -d 10.31.240.0/25
iptables -A FORWARD  -p tcp --sport 22 -s 10.31.240.0/25


iptables -A FORWARD -j ACCEPT -p tcp --dport 22
iptables -A FORWARD -j ACCEPT -p tcp --sport 22
```

VM HTTP PUB

```
#!/bin/bash

#Ecrire le script ci-dessous va effacer tout ce qui a été fati précédemment pour eviter d
iptables -t nat    -F #Supprime toute les règles nat
iptables -t mangle -F #Supprime toute les règles mangle

iptables -P FORWARD DROP
iptables -P INPUT   DROP
iptables -P OUTPUT  DROP


# Autorisation des bases de données
# # # # # # # # # # # # # # # # # # # # # # # # # # #
iptables -A INPUT  -p tcp --dport 3306 -j ACCEPT #
iptables -A INPUT  -p tcp --sport 3306 -j ACCEPT #
iptables -A OUTPUT -p tcp --dport 3306 -j ACCEPT #
iptables -A OUTPUT -p tcp --sport 3306 -j ACCEPT #
# # # # # # # # # # # # # # # # # # # # # # # # # # #


# Autorisation du DNS
# # # # # # # # # # # # # # # # # # # # # # # # # # #
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT #
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT #
iptables -A OUTPUT -p tcp --sport 53 -j ACCEPT #
iptables -A OUTPUT -p udp --sport 53 -j ACCEPT #

iptables -A INPUT  -p tcp --sport 53 -j ACCEPT #
iptables -A INPUT  -p udp --sport 53 -j ACCEPT #
iptables -A INPUT  -p tcp --sport 53 -j ACCEPT #
iptables -A INPUT  -p udp --sport 53 -j ACCEPT #
# # # # # # # # # # # # # # # # # # # # # # # # # # #



# Autorisation DHCP
# # # # # # # # # # # # # # # # # # # # # # # # # # #
iptables -A INPUT  -p tcp --sport 67 -j ACCEPT #
iptables -A INPUT  -p tcp --sport 67 -j ACCEPT #
iptables -A OUTPUT -p tcp --sport 67 -j ACCEPT #
iptables -A OUTPUT -p tcp --sport 67 -j ACCEPT #
# # # # # # # # # # # # # # # # # # # # # # # # # # #

#Autorisation SSH
iptables -A FORWARD  -j ACCEPT -p tcp --dport 22
iptables -A INPUT    -j ACCEPT -p tcp --dport 22
iptables -A OUTPUT   -j ACCEPT -p tcp --dport 22
```

```
48
49 iptables -A FORWARD  -j ACCEPT -p tcp --sport 22
50 iptables -A INPUT    -j ACCEPT -p tcp --sport 22
51 iptables -A OUTPUT   -j ACCEPT -p tcp --sport 22
```

sisr2-afrique/mission_15.txt · Dernière modification: 2021/12/16 16:50 de d-marguinaud