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 :

```
1
     [Unit]
 2
     Description=/etc/rc.local
     ConditionPathExists=/etc/rc.local
 5
     [Service]
 6
     Type=forking
 7
     ExecStart=/etc/rc.local start
 8
     TimeoutSec=0
9
     StandardOutput=tty
     RemainAfterExit=yes
10
     SysVStartPriority=99
11
12
13
     [Install]
14
     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,

```
1 | chmod +x nom du fichier
```

ROUTEUR

```
#!/bin/bash
1
2
3
4
    #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
5
     iptables -t nat -F #Supprime toute les règles nat
6
7
     iptables -t mangle -F #Supprime toute les règles mangle
8
9
     iptables -P FORWARD DROP
10
     iptables -P INPUT DROP
11
     iptables -P OUTPUT DROP
12
13
     14
15
     # 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
16
17
18
19
     # Autorise le retour des requêtes DNS depuis ns1
20
     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
21
22
                                                                                    #
     # Autorise le routeur à faire des requetes DNS sur ns1
23
     iptables -A OUTPUT -j ACCEPT -p udp --dport 53 -d 10.31.248.53
24
     iptables -A OUTPUT -j ACCEPT -p tcp --dport 53 -d 10.31.248.53
                                                                                    #
25
26
                                                                                    #
27
     # Autorise ns1 à répondre aux requetes DNS du routeur
                                                                                    #
28
     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
29
                                                                                    #
30
                                                                                    #
    #Autorise les requetes DNS à destination de ns1
```

```
iptables -A FORWARD -j ACCEPT -p udp --dport 53 -s 10.31.248.53
                                                                                       #
33
     iptables -A FORWARD -j ACCEPT -p udp --sport 53 -d 10.31.248.53
                                                                                       #
34
     iptables -A FORWARD -j ACCEPT -p tcp --dport 53 -s 10.31.248.53
35
                                                                                       #
     iptables -A FORWARD -j ACCEPT -p tcp --sport 53 -d 10.31.248.53
36
                                                                                       #
37
                                                                                       #
     #Autorise les requetes à destionation et venant des réseaux 240 et 248
38
                                                                                       #
     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
39
                                                                                       #
40
                                                                                       #
     iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -d 10.31.240.0/25
41
                                                                                       #
     iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -d 10.31.248.0/25
42
43
     iptables -A FORWARD -j ACCEPT -p tcp --dport 443 -s 10.31.240.0/25
44
     iptables -A FORWARD -j ACCEPT -p tcp --dport 443 -s 10.31.248.0/25
45
     iptables -A FORWARD -j ACCEPT -p tcp --sport 443 -d 10.31.240.0/25
46
47
     iptables -A FORWARD -j ACCEPT -p tcp --sport 443 -d 10.31.248.0/25
48
49
50
     #iptables -A FORWARD -j ACCEPT -p tcp --dport 80 -d 10.31.248.80
51
     #iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -s 10.31.248.80
                                                                                       #
52
                                                                                       #
53
     #iptables -A FORWARD -j ACCEPT -p tcp --dport 80 -d 10.31.240.80
                                                                                       #
54
     #iptables -A FORWARD -j ACCEPT -p tcp --sport 80 -s 10.31.240.80
                                                                                       #
55
                                                                                       #
56
     #iptables -A FORWARD -j ACCEPT -p tcp --dport 443 -d 10.31.248.80
                                                                                       #
57
     #iptables -A FORWARD -j ACCEPT -p tcp --sport 443 -s 10.31.248.80
58
                                                                                       #
     #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
59
60
                                                                                       #
61
                                                                                       #
     #iptables -A FORWARD -j ACCEPT -p udp --dport 445
62
                                                                                       #
     #iptables -A FORWARD -j ACCEPT -p tcp --dport 445
63
                                                                                       #
     #iptables -A FORWARD -j ACCEPT -p udp --sport 445
64
                                                                                       #
     #iptables -A FORWARD -j ACCEPT -p tcp --sport 445
65
                                                                                       #
66
67
     #iptables -A FORWARD -j ACCEPT -p udp --dport 3306
68
     iptables -A FORWARD -j ACCEPT -p tcp --dport 3306
     #iptables -A FORWARD -j ACCEPT -p udp --sport 3306
69
70
     iptables -A FORWARD -j ACCEPT -p tcp --sport 3306
71
     72
73
74
     iptables -A FORWARD -j ACCEPT -p icmp
     iptables -A INPUT -j ACCEPT -p icmp
75
     iptables -A OUTPUT -j ACCEPT -p icmp
76
77
78
79
     #ACCES INTERNET
80
     iptables -A INPUT -p tcp --dport 80 -j ACCEPT
81
     iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
     iptables -A INPUT -p tcp --dport 443 -j ACCEPT
82
83
     iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT
84
85
     #ouverture du port 22 pour le routeur
86
     iptables -A INPUT -p tcp --dport 22 -j ACCEPT
87
     iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
88
89
     iptables -A INPUT -p tcp --sport 22 -j ACCEPT
     iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT
90
91
92
     #SSH pour tout le monde
93
     iptables -A FORWARD -p tcp --dport 22 -d 10.31.240.0/25
94
     iptables -A FORWARD -p tcp --sport 22 -s 10.31.240.0/25
95
96
97
     iptables -A FORWARD -j ACCEPT -p tcp --dport 22
     iptables -A FORWARD -j ACCEPT -p tcp --sport 22
98
```

VM HTTP PUB

```
1
    #!/bin/bash
2
3
    #Ecrire le script ci-dessous va effacer tout ce qui a été fati précédemment pour eviter d
4
    iptables -t nat -F #Supprime toute les règles nat
5
    iptables -t mangle -F #Supprime toute les règles mangle
6
7
    iptables -P FORWARD DROP
8
    iptables -P INPUT
                      DROP
9
    iptables -P OUTPUT DROP
10
11
12
    # Autorisation des bases de données
13
    iptables -A INPUT -p tcp --dport 3306 -j ACCEPT #
14
    iptables -A INPUT -p tcp --sport 3306 -j ACCEPT # iptables -A OUTPUT -p tcp --dport 3306 -j ACCEPT #
15
16
    iptables -A OUTPUT -p tcp --sport 3306 -j ACCEPT #
17
    18
19
20
    # Autorisation du DNS
21
    22
23
    iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT #
24
    iptables -A OUTPUT -p udp --dport 53 -j ACCEPT #
25
    iptables -A OUTPUT -p tcp --sport 53 -j ACCEPT #
26
    iptables -A OUTPUT -p udp --sport 53 -j ACCEPT #
27
28
    iptables -A INPUT -p tcp --sport 53 -j ACCEPT #
29
    iptables -A INPUT -p udp --sport 53 -j ACCEPT #
30
    iptables -A INPUT -p tcp --sport 53 -j ACCEPT #
31
    iptables -A INPUT -p udp --sport 53 -j ACCEPT #
32
    33
34
35
36
    # Autorisation DHCP
37
    iptables -A INPUT  -p tcp --sport 67 -j ACCEPT #
iptables -A INPUT  -p tcp --sport 67 -j ACCEPT #
38
39
    iptables -A OUTPUT -p tcp --sport 67 -j ACCEPT #
40
    iptables -A OUTPUT -p tcp --sport 67 -j ACCEPT #
41
    42
43
44
    #Autorisation SSH
45
    iptables -A FORWARD -j ACCEPT -p tcp --dport 22
    iptables -A INPUT
                       -j ACCEPT -p tcp --dport 22
46
    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
iptables -A OUTPUT -j ACCEPT -p tcp --sport 22
```

 $sisr2-afrique/mission_15.txt \cdot Derni\`ere\ modification:\ 2021/12/16\ 16:50\ de\ d-marguinaud$