TP Services de sécurité 1° partie – Fonctions essentielles : routeur + pare-feu

Table des matières

Partie Évaluée :

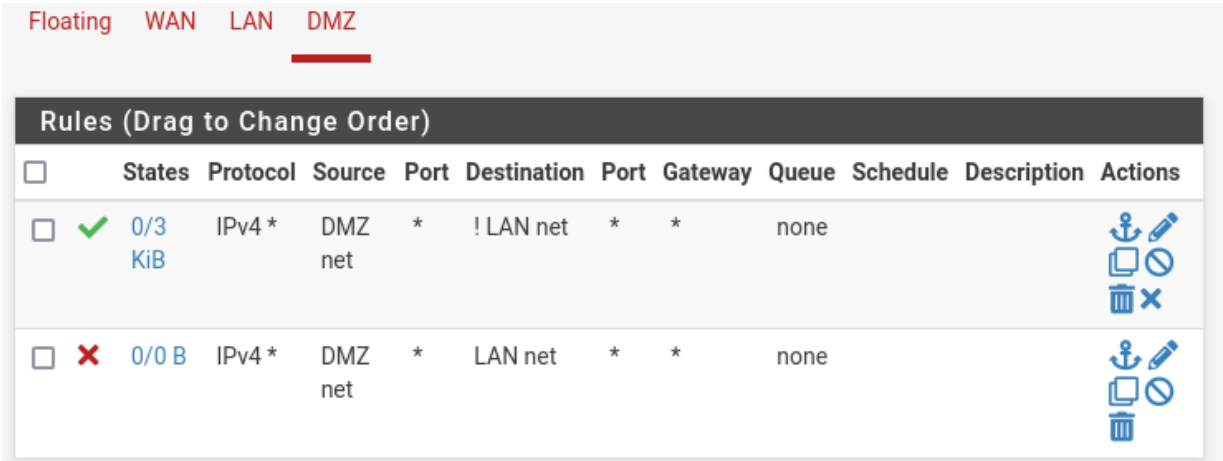
1- Configuration IP du serveur WEB

```
root@serveur-WEB-DMZ:~# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
000
    link/ether 08:00:27:c7:2b:c9 brd ff:ff:ff:ff:ff:ff
    inet 10.10.0.1/28 brd 10.10.0.15 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec7:2bc9/64 scope link
       valid_lft forever preferred_lft forever
root@serveur-WEB-DMZ:~# _
```

Pourquoi ne pas installer un DHCP en DMZ ?

1. **Attribution dynamique d'adresses IP :** Le DHCP attribue dynamiquement des adresses IP aux périphériques sur le réseau. Cela peut rendre difficile la traçabilité des adresses IP utilisées dans la zone DMZ, ce qui peut être un problème en cas d'activités malveillantes.
2. **Risques de sécurité :** Le DHCP peut être exploité par des attaquants pour distribuer de fausses informations de configuration IP aux périphériques de la zone DMZ. Mais surtout, cela freine le hacker malveillant car il va être obligé de chercher le réseau dans lequel se trouve la DMZ pour pouvoir l’exploiter.

2- Règles de Pare-feu DMZ



La première règle permet d’autoriser tous les échanges de données sauf vers le LAN.

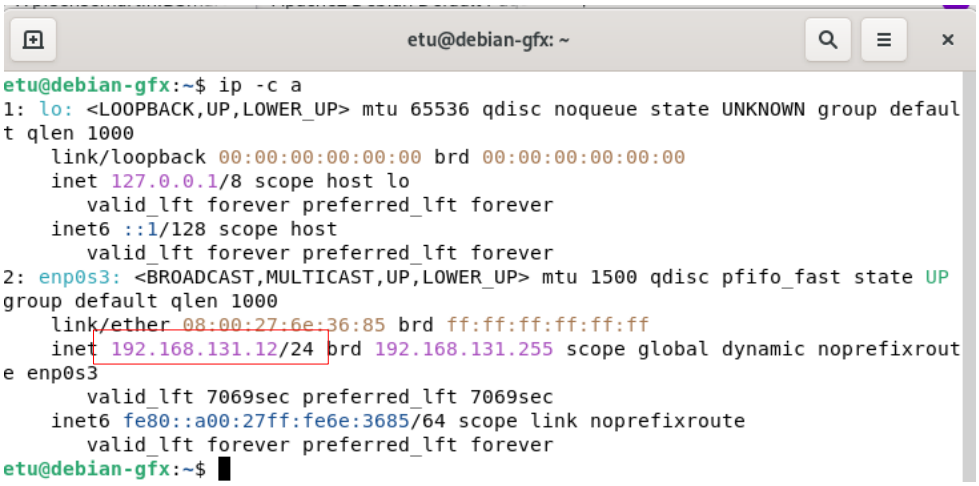
La seconde permet de vérifier qu’aucun échange ne se fait vers le LAN.

3- Vérification/tests

```
FreeBSD/amd64 (FWpfsensemartin.B3martin.lan) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: bdeecc4608f7508bf5cd

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on FWpfsensemartin ***

 WAN (wan)       -> em0        -> v4: 172.16.252.131/22
 LAN (lan)       -> em1        -> v4: 192.168.131.254/24
 DMZ (opt1)      -> em2        -> v4: 10.10.0.14/28

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

a- DMZ to LAN / LAN to DMZ

On va donc tester avec des pings du serveur WEB vers le client dans le LAN :



On a donc ici le client coté LAN avec son adresse IP

On effectue donc maintenant un ping de la DMZ vers ce client

```
root@serveur-WEB-DMZ:~# ping 192.168.131.12
PING 192.168.131.12 (192.168.131.12) 56(84) bytes of data.
^C
--- 192.168.131.12 ping statistics ---
39 packets transmitted, 0 received, 100% packet loss, time 38909ms

root@serveur-WEB-DMZ:~#
```

Puis vers la passerelle du LAN :

```
root@serveur-WEB-DMZ:~# ping 192.168.131.254
PING 192.168.131.254 (192.168.131.254) 56(84) bytes of data.
^C
--- 192.168.131.254 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 13294ms

root@serveur-WEB-DMZ:~# _
```

Mais on peu voir que le LAN peut ping le serveur dans la DMZ :

```
etu@debian-gfx:~$ ping 10.10.0.1
PING 10.10.0.1 (10.10.0.1) 56(84) bytes of data.
64 bytes from 10.10.0.1: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=63 time=0.963 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=63 time=0.965 ms
^C
--- 10.10.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.963/1.065/1.269/0.143 ms
etu@debian-gfx:~$
```

b- DMZ to WAN / WAN to DMZ

Depuis le WAN on n’accède pas directement à la DMZ :

```
C:\Users\Martin>ping 10.10.0.1

Envoi d’une requête 'Ping'  10.10.0.1 avec 32 octets de données :
Délai d’attente de la demande dépassé.
Délai d’attente de la demande dépassé.
Délai d’attente de la demande dépassé.
Délai d’attente de la demande dépassé.

Statistiques Ping pour 10.10.0.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\Martin>_
```

Mais la DMZ accède au WAN en testant par exemple de ping google.com :

```
root@serveur-WEB-DMZ:~# ping google.com
PING google.com (142.250.179.78) 56(84) bytes of data.
64 bytes from par21s19-in-f14.1e100.net (142.250.179.78): icmp_seq=1 ttl=109 time=18.2 ms
64 bytes from par21s19-in-f14.1e100.net (142.250.179.78): icmp_seq=2 ttl=109 time=18.9 ms
64 bytes from par21s19-in-f14.1e100.net (142.250.179.78): icmp_seq=3 ttl=109 time=18.6 ms
64 bytes from par21s19-in-f14.1e100.net (142.250.179.78): icmp_seq=4 ttl=109 time=22.1 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 18.176/19.470/22.135/1.562 ms
root@serveur-WEB-DMZ:~#
```

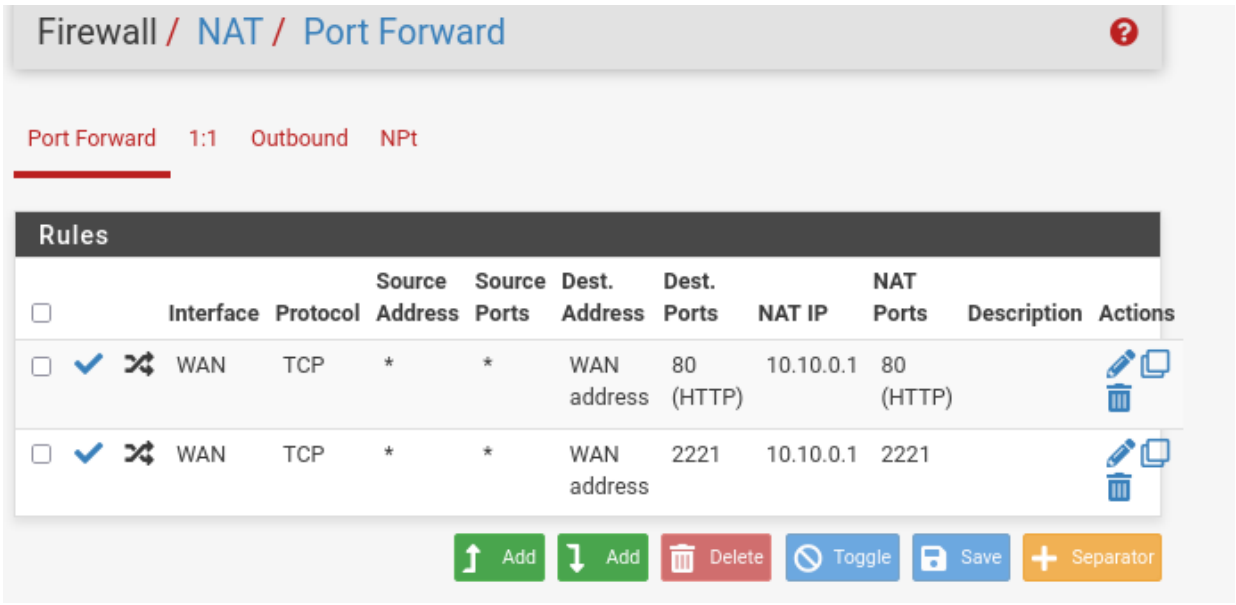
4- Personnalisation de la page WEB :

On se rend dans le fichier index.html pour modifier la page d’accueil (nano /*var*/www/html/index.html) Puis on modifie à notre bon vouloir.

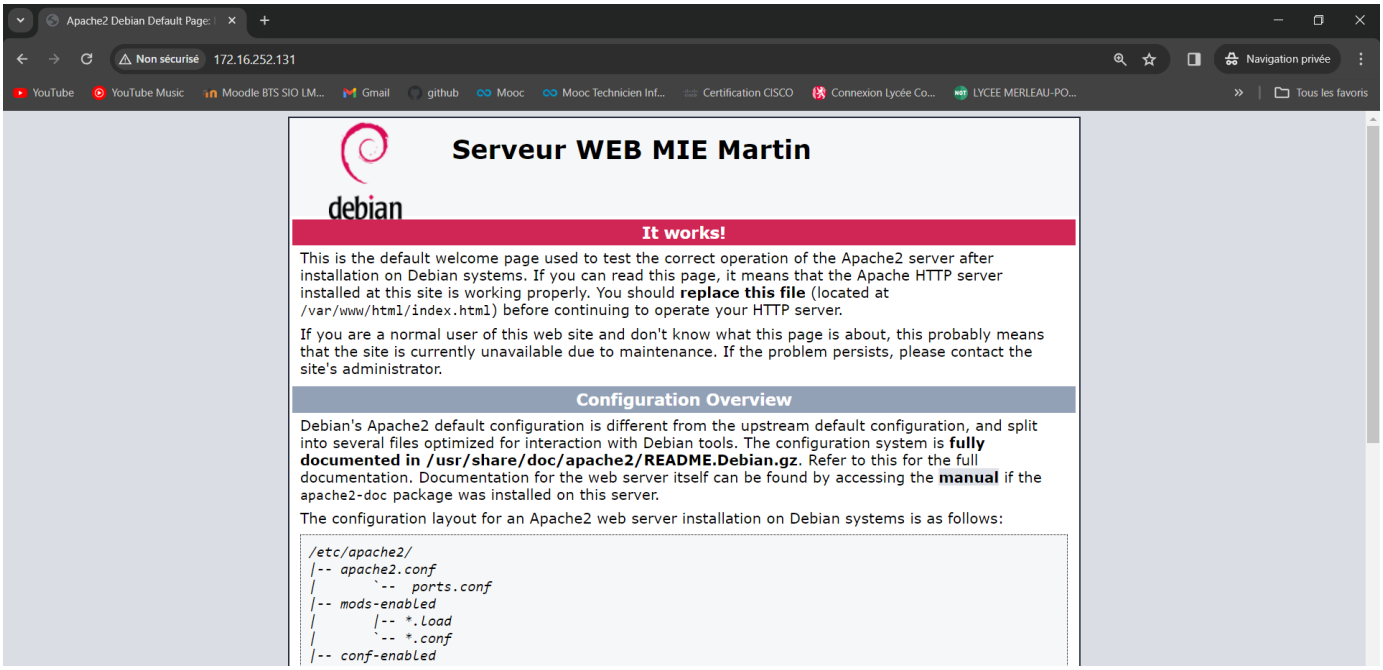
```
  }
    </style>
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
        <span class="floating_element">
         Serveur WEB MIE Martin
        </span>
      </div>
<!--      <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
```

Puis on s'occupe des règles NAT :

Règles	Interface	Protocole	Ad source	Ports source	Ad destination	Ports dest.	IP NAT	Ports NAT
N°1	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.0.1	80 (HTTP)
N°2	WAN	TCP	*	*	WAN address	2221	10.10.0.1	2221



5- Vérification



On tape l’adresse du Pfsense dans la barre de recherche d’un navigateur puis on obtient la page WEB du serveur présent en DMZ

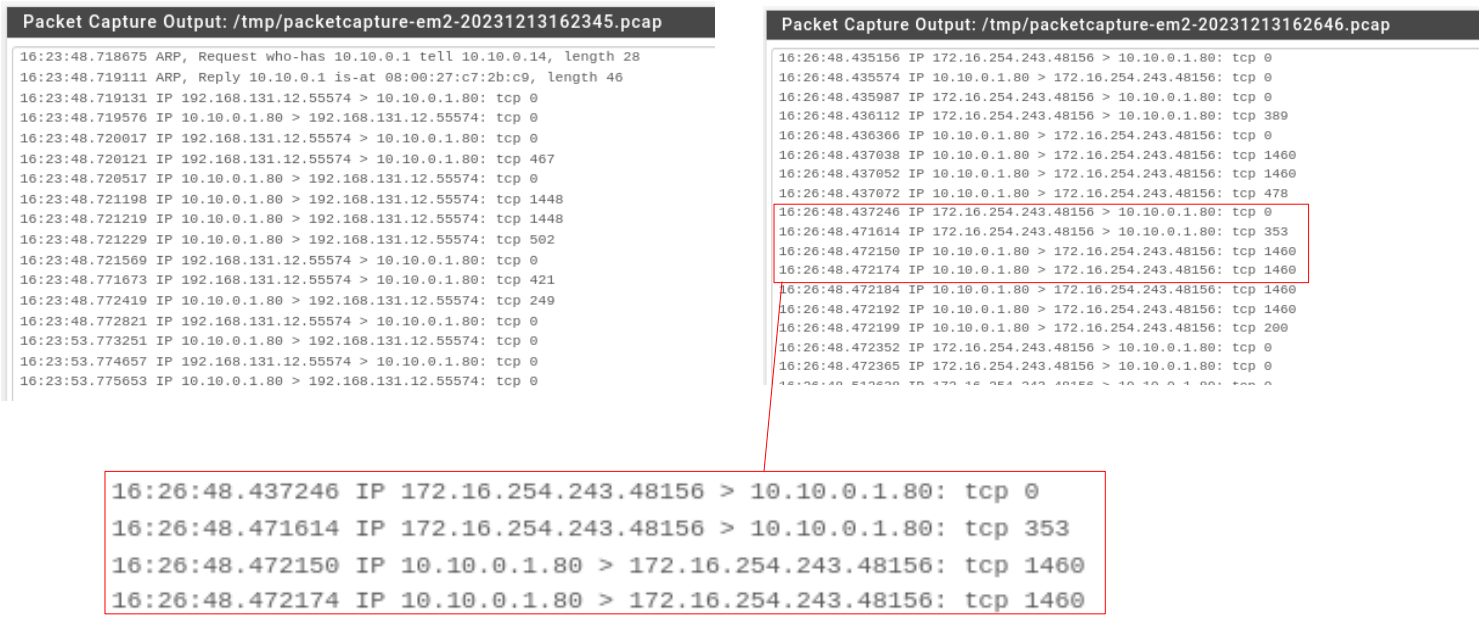
6- URL

Actuellement on tape dans la barre de recherche une adresse IP afin d’accéder à la ressources mais il est également possible de plusieurs façon de passer à un nom de domaine. Notamment avec un alias que l’on peut retrouver dans l’onglet Firewall → Aliases puis remplir les différentes informations (Nom, type, host …) Sinon on peut également faire en sorte d’avoir un serveur DNS dans la DMZ et ainsi déclarer son nom via ce dernier.

7- Capture de Trames :

Pfsense possède un sniffeur de réseau en interne ce qui permet de regarder les requêtes faites vers la DMZ.

Analyse du réseau DMZ :



16:26:48.437246 IP 172.16.254.243.48156 > 10.10.0.1.80: tcp 0
16:26:48.471614 IP 172.16.254.243.48156 > 10.10.0.1.80: tcp 353
16:26:48.472150 IP 10.10.0.1.80 > 172.16.254.243.48156: tcp 1460
16:26:48.472174 IP 10.10.0.1.80 > 172.16.254.243.48156: tcp 1460

Analyse du réseau WAN :

```
16:32:33.694605 IP 172.16.254.148.5353 > 224.0.0.251.5353: UDP, length 33
16:32:33.694661 IP6 fe80::87b:c9f1:bb2f:2a11.5353 > ff02::fb.5353: UDP, length 33
16:32:33.694682 IP 172.16.254.148.5353 > 224.0.0.251.5353: UDP, length 34
16:32:33.694693 IP6 fe80::87b:c9f1:bb2f:2a11.5353 > ff02::fb.5353: UDP, length 34
16:32:33.917829 IP 172.16.252.131 > 172.16.255.254: ICMP echo request, id 27524, seq
13799, length 9
16:32:33.919304 IP 172.16.255.254 > 172.16.252.131: ICMP echo reply, id 27524, seq
13799, length 9
16:32:34.303015 IP 172.16.254.254.63180 > 239.255.255.250.1900: UDP, length 175
16:32:34.315663 IP 172.16.254.254.63183 > 239.255.255.250.1900: UDP, length 174
16:32:34.340367 IP 172.16.255.251 > 224.0.0.18: VRRPv2, Advertisement, vrid 10, prio 0,
authtype none, intvl 1s, length 36
16:32:34.447492 IP 172.16.252.131 > 172.16.255.254: ICMP echo request, id 27524, seq
13800, length 9
16:32:34.448299 IP 172.16.255.254 > 172.16.252.131: ICMP echo reply, id 27524, seq
13800, length 9
```

La terminologie CISCO pour cette configuration NAT est l’adresse globale interne ou NAT dynamique.

8- Client to page WEB

Effectivement les clients accèdent à la ressource en passant par l’adresse IP du serveur WEB en DMZ (donc en 10.10.0.1). A mon sens il n’y a pas d’adresse préférable étant donné que dans une vrai infrastructure professionnelle on n’accédera pas aux ressources via une adresse IP mais plutôt un nom de domaine/adresse textuelle.

9- Translation d’adresse LAN → DMZ

A mon sens non il n’y a pas de translation d’adresse car il n’existe aucune règle interdisant le trafic entre le LAN et la DMZ.