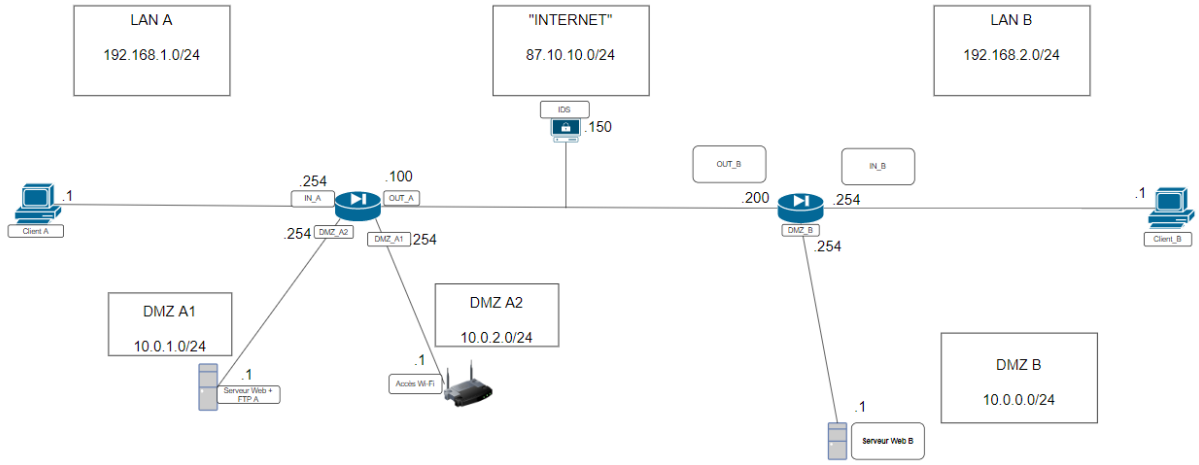
Rapport SAE 401 : Sécurisation d'un SI

Participant : AZIZ Souhayl

Tâche 2 : Configuration des firewalls pour protéger les réseaux internes et DMZ

Pour rappel, voici notre plan IP :




1) Mise en place d'une politique de NAT sur les deux firewalls
   a. Firewall A

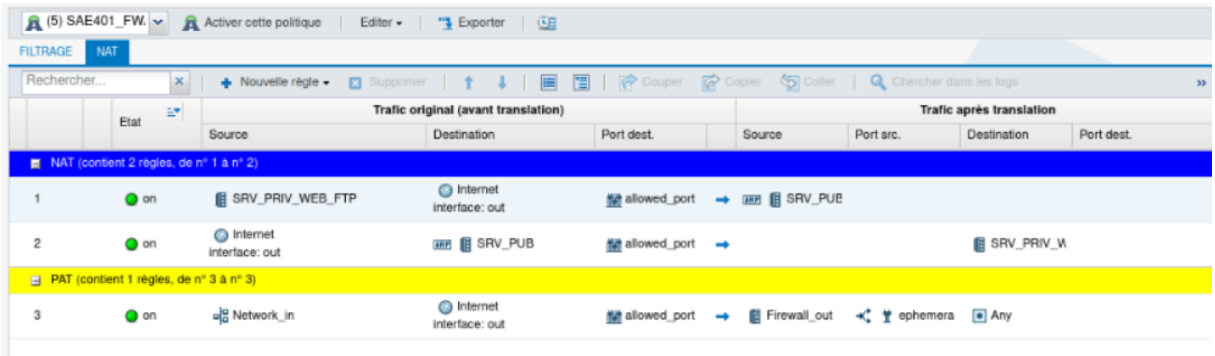
Nous avons créé des objets à savoir :

1 objet machine SRV_PUB qui contient l'@IP publique du firewall (87.10.10.100)

1 objet machine SRV_PRIV_WEB_FTP qui contient l'@IP du serveur ftp/web (10.0.1.1)

1 objet groupe de port ALLOWED_PORT contenant les ports que nous souhaitons autoriser

(ftp/ftps, http/https, ftp-data/ftps-data)

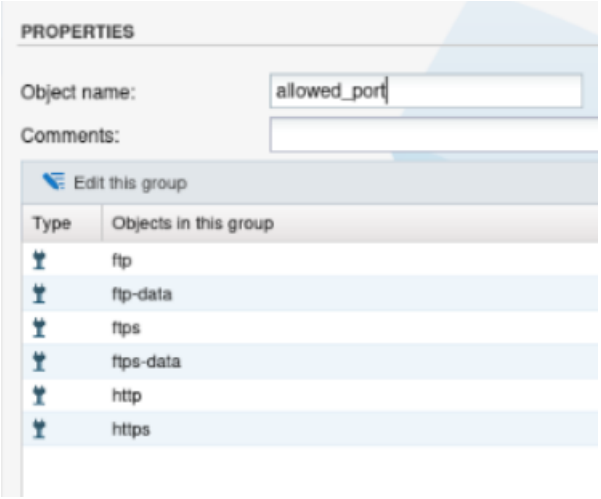


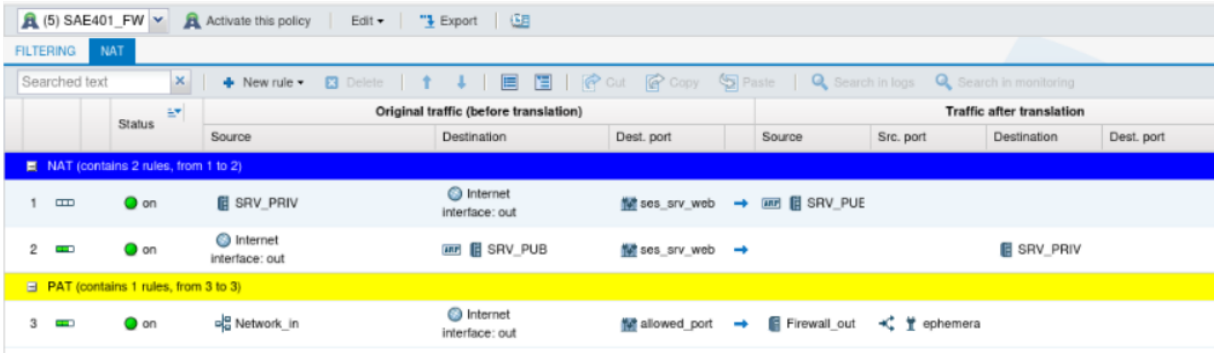

Ici, on a une règle une règle de NAT en deux lignes permettant de traduire l'@IP du serveur ftp/web vers internet sur les ports autorisés. Ceci permet à une machine du réseau « internet » de joindre le serveur de notre DMZ depuis l'@IP publique du firewall.

Aussi, nous avons mis en place une PAT afin que les clients du réseau interne puissent aller sur internet sur les ports autorisés.

B. Firewall B

Pour le deuxième firewall, nous avons entrepris la même démarche que pour le premier, à savoir la création d'objet et la mise en place de NAT et PAT :

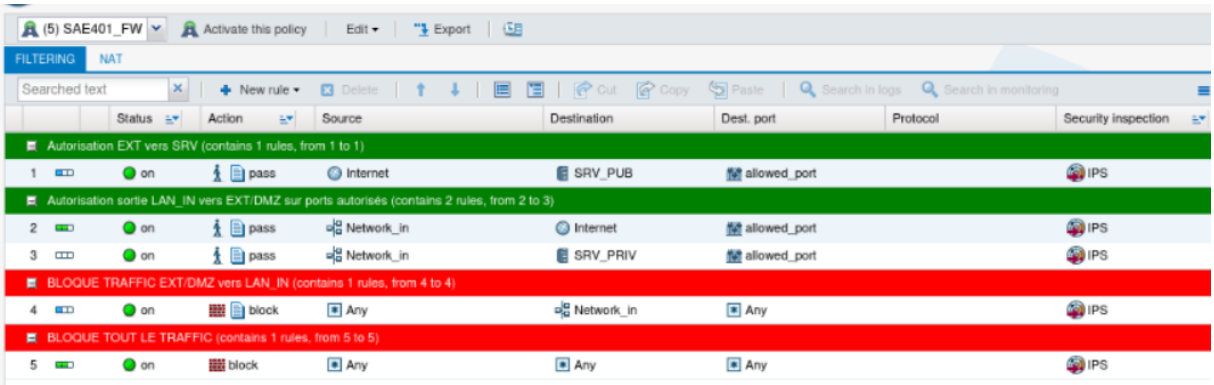



2) Règle de filtrage :

Dans chacun des firewalls, les règles sont identiques sauf quelques exceptions nous allons dans un premier temps détailler les règles identiques

Règle de filtrage du Firewall B :



Toutes ces règles sont aussi présente sur le firewall A. Et chacune de celle-ci sont logué

La première règle autorise les paquets venant d'internet à destination du serveur web / web et ftp. Sur les ports autorisés (groupe de port ALLOWED_PORT)

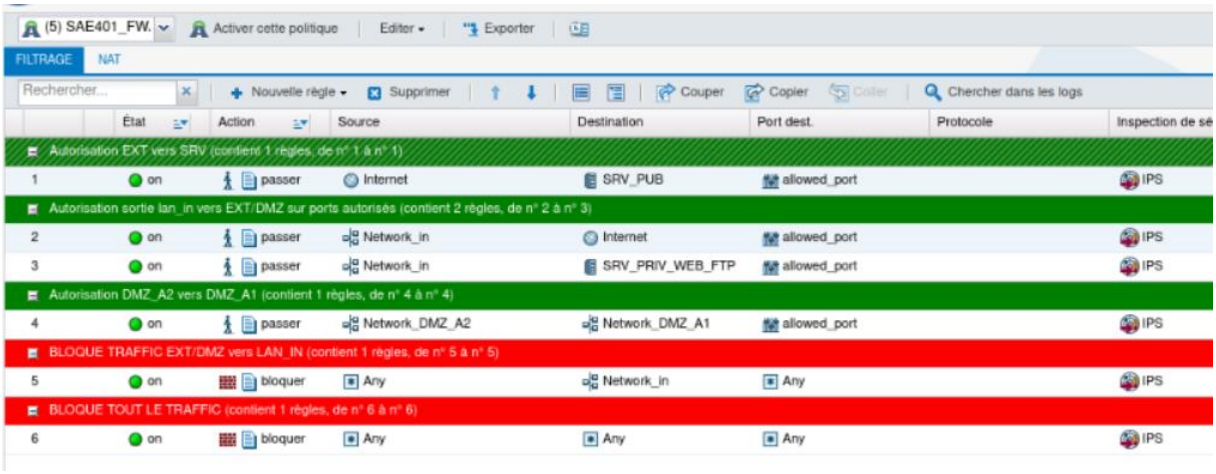
La deuxième et la troisième règle permettent du traffic sur les ports autorisés des machines clientes du réseau interne vers les réseaux externes (DMZ et « internet ») et donc permettent l'accès aux serveurs uniquement sur les ports concernés

La quatrième règle bloque tout traffic externes (DMZ et « internet ») en direction du réseau interne.

Enfin, la dernière règle bloque tout traffic restant. (Traffic ne correspondant à aucune des règles précédentes). Celle-ci n'est pas obligatoire car dans tous les cas le traffic restant est bloqué mais cela permet de loguer le traffic.

Pour chacune des règles, nous ne nous occupons que du sens qui nous intéresse, le sens retour de l'échange se fait seul avec la notion de « stateful ».

Nous retrouverons toutes ces règles sur le firewall A mais on y trouvera une règle supplémentaire permettant l'accès à la DMZ_A1 depuis la DMZ_A2 :




Ici on retrouve toutes les règles ainsi qu'une règle supplémentaire (règle 4).

Aussi, nous avons configuré la route par défaut avec l'@IP publique de l'autre firewall dans les deux sens.

**TEST :**

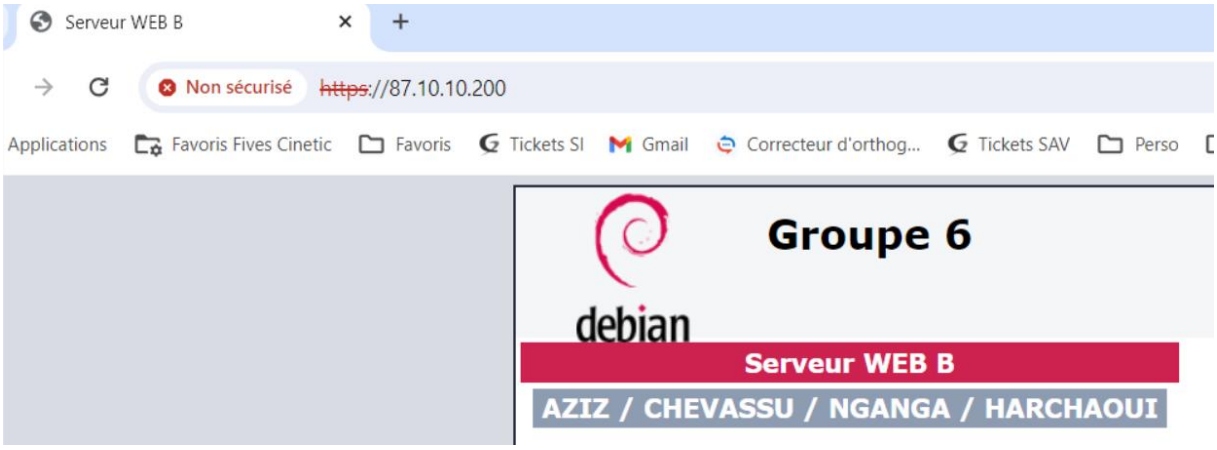
Pour les tests, nous avons effectué des pings et aucun ne passent, ceci s'explique au fait que nous autorisons que les protocoles et ports ftp/ftps et http/https.

Mais, les sites web sont accessibles par les DMZ et par le réseau 'internet' via l'@IP publique.

Client A :

```
Carte Ethernet Ethernet 3 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::7e6a:1867:6334:66d1%68
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.1.254
```




Le client A accède au serveur web B via l'@IP publique 87.10.10.200 (voir plan IP en page 1)

Mais, il accède aussi par la DMZ au serveur de son entreprise par exemple en ftp avec l'@IP privé du serveur ftp :

```
Microsoft Windows [version 10.0.19045.4046]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>ftp.exe
ftp> open 10.0.1.1
Connecté à 10.0.1.1.
220 Welcome to blah FTP service.
200 Always in UTF8 mode.
Utilisateur (10.0.1.1:(none)) : anonymous
331 Please specify the password.
Mot de passe :
230 Login successful.
ftp>
```

Client B :


Ici, on voit que notre client B accède au serveur web A depuis l'@IP publique 87.10.10.100

```
root@rt-mob06:~# 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: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 70:b5:e8:ac:b2:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/24 brd 192.168.2.255 scope global enp1s0
       valid_lft forever preferred_lft forever
    inet6 fe80::72b5:e8ff:feac:b225/64 scope link
       valid_lft forever preferred_lft forever
3: wlp0s20f3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether f8:ac:65:b7:be:b1 brd ff:ff:ff:ff:ff:ff
root@rt-mob06:~# ftp
ftp> open 87.10.10.100
Connected to 87.10.10.100.
220 Welcome to blah FTP service.
Name (87.10.10.100:rt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 0        0            4096 Mar 26 15:49 groupe_6_Fichiers
226 Directory send OK.
ftp>
```

A nouveau, on voit que le client B à l'@IP 192.168.2.1 peux accéder au serveur FTP du réseau A via 87.10.10.100

Enfin, puisque nous avons deux DMZ séparé, nous avons aussi testé l'accès au serveur web du réseau A (DMZ_A1) depuis la DMZ_A2. Le client était connecté en wifi à la borne Linksys (10.0.2.1) :

```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::c5a3:3aeb:d848:ce18%15
   Adresse IPv4. . . . . . . . . . . . . .: 10.0.2.130
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.0.2.1
```