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 :

Une image contenant texte, diagramme, capture d’écran, ligne

Description générée automatiquement

1. Mise en place d’une politique de NAT sur les deux firewalls
   1. 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)

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

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 :

Une image contenant texte, capture d’écran, Police, nombre

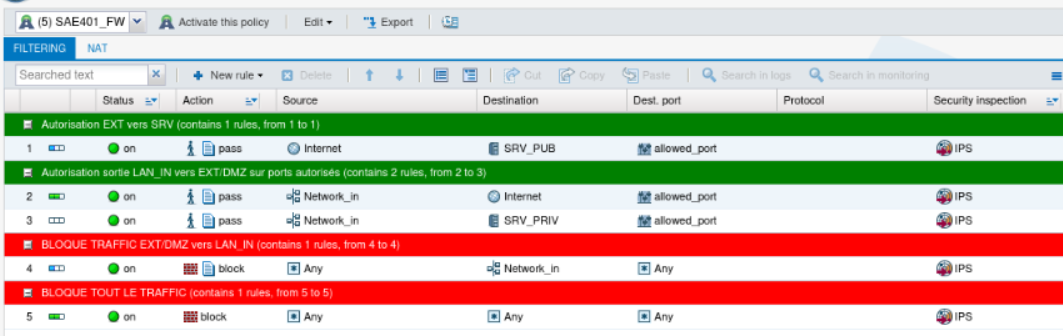
Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

1. 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)

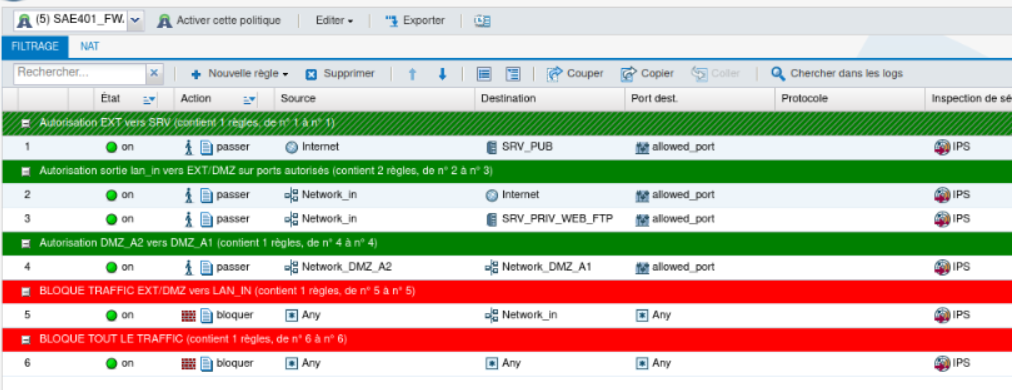
La deuxième et la troisième règle permettent du traffic sur les ports autorisés des machines clientes du réseau interne vers les réseaux externes (DMZ et « internet ») et donc permettent l’accès aux serveurs uniquement sur les ports concernés

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).

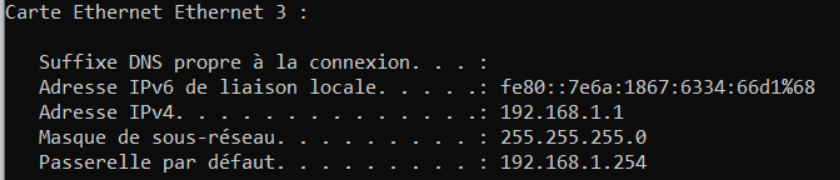
Aussi, nous avons configuré la route par défaut avec l’@IP publique de l’autre firewall dans les deux sens.

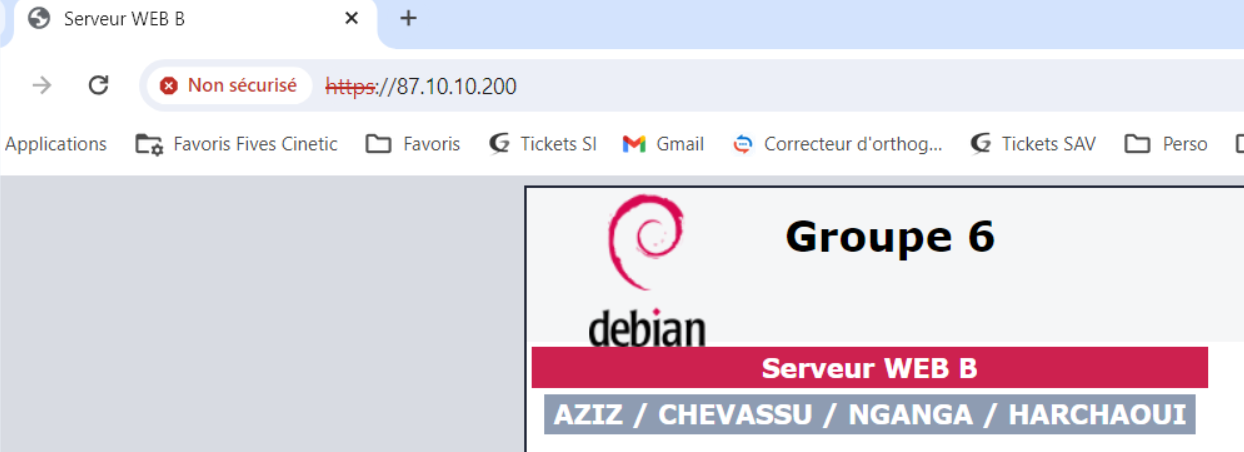
**TEST :**

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.

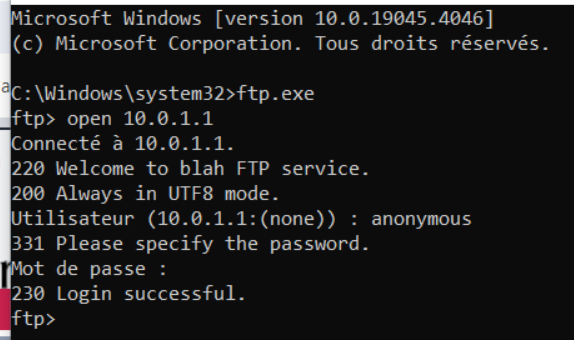
Mais, les sites web sont accessibles par les DMZ et par le réseau ‘internet’ via l’@IP publique.

Client A :





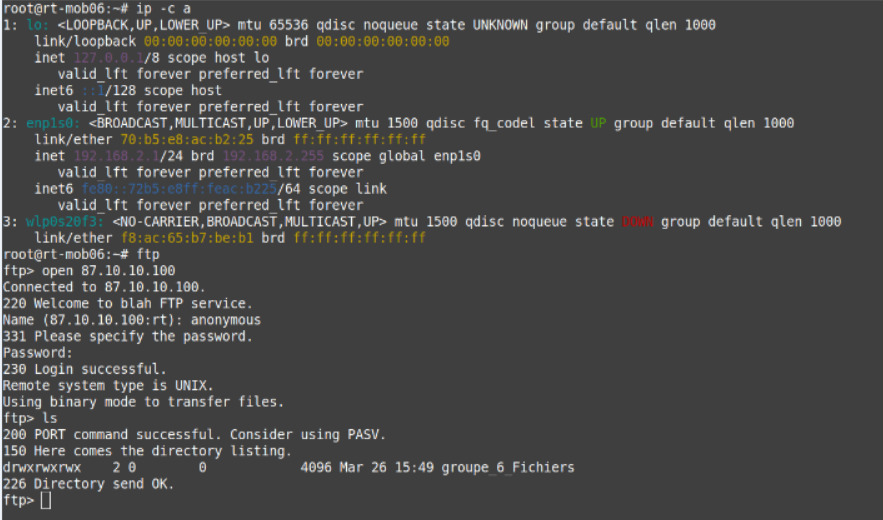
Le client A accède au serveur web B via l’@IP publique 87.10.10.200 (voir plan IP en page 1)

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


Client B :



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



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) :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement