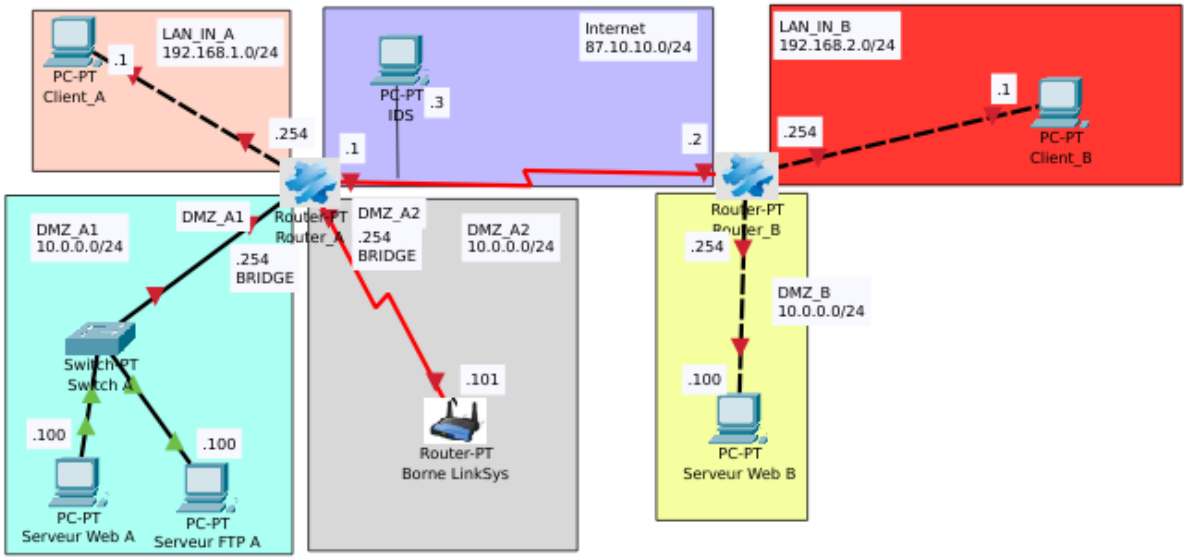
Tâche 2 : Configuration des firewalls Stormshield

Julien	50%	
Etienne	50%	
Antonin	0%	
Maxence	0%	

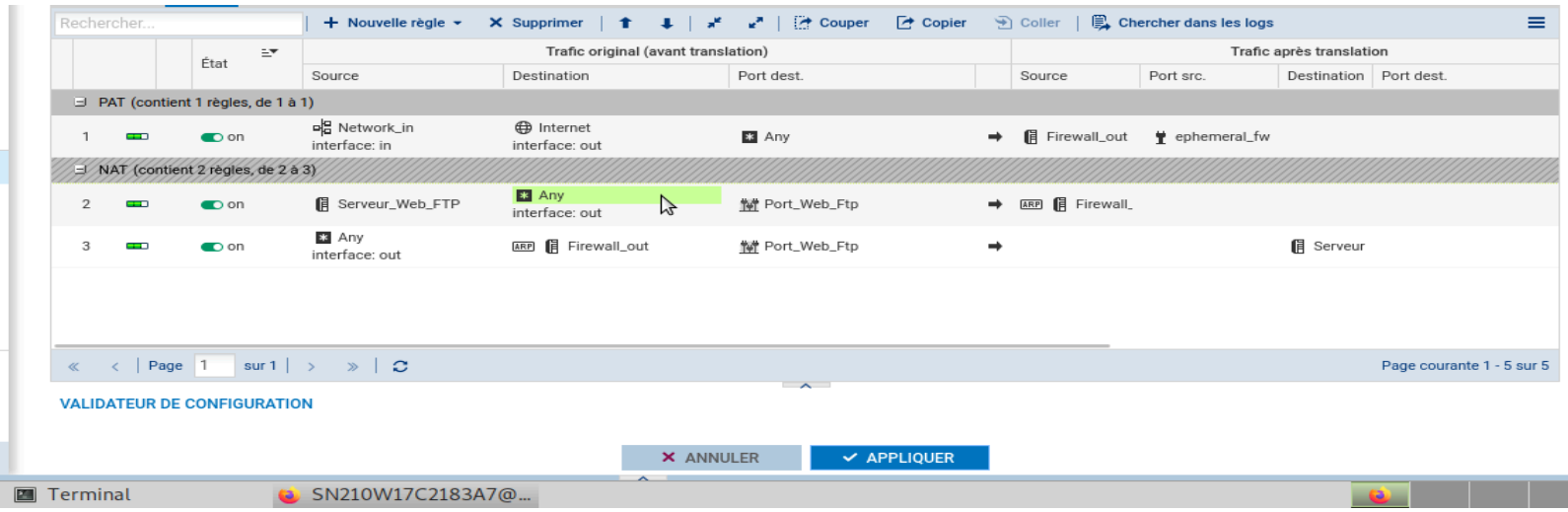
Le but de cette tâche est de configurer le filtrage et la NAT sur nos firewall et par la suite de sécuriser le réseau interne. Nous avons suivi le plan d'adressage IP suivant afin de réaliser le filtrage et la NAT.



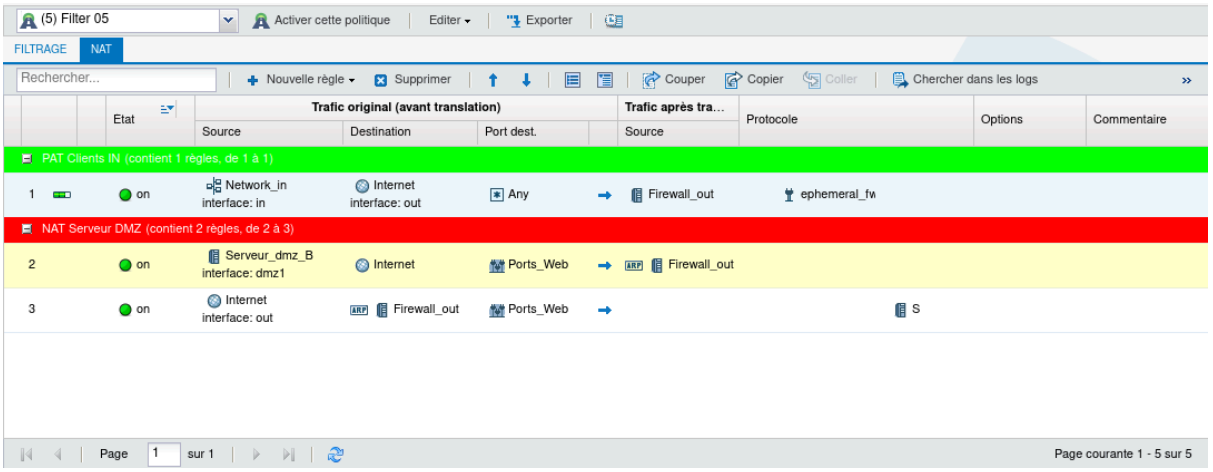
Nous avons tout d'abord configurer la NAT :

- Mise en place d'une PAT sur les 2 firewalls pour les utilisateurs internes.
- Mise en place d'une NAT pour le réseau DMZ de chaque firewall sur l'interface externe pour les ports http et https.

Mise en place d’une PAT sur le firewall A :

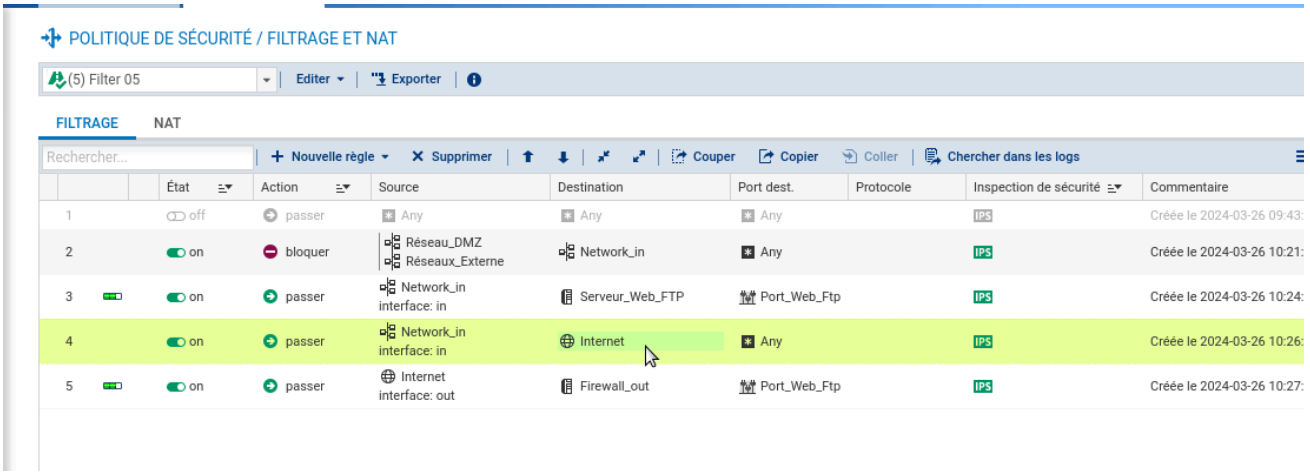


Mise en place de la même PAT sur le firewall B



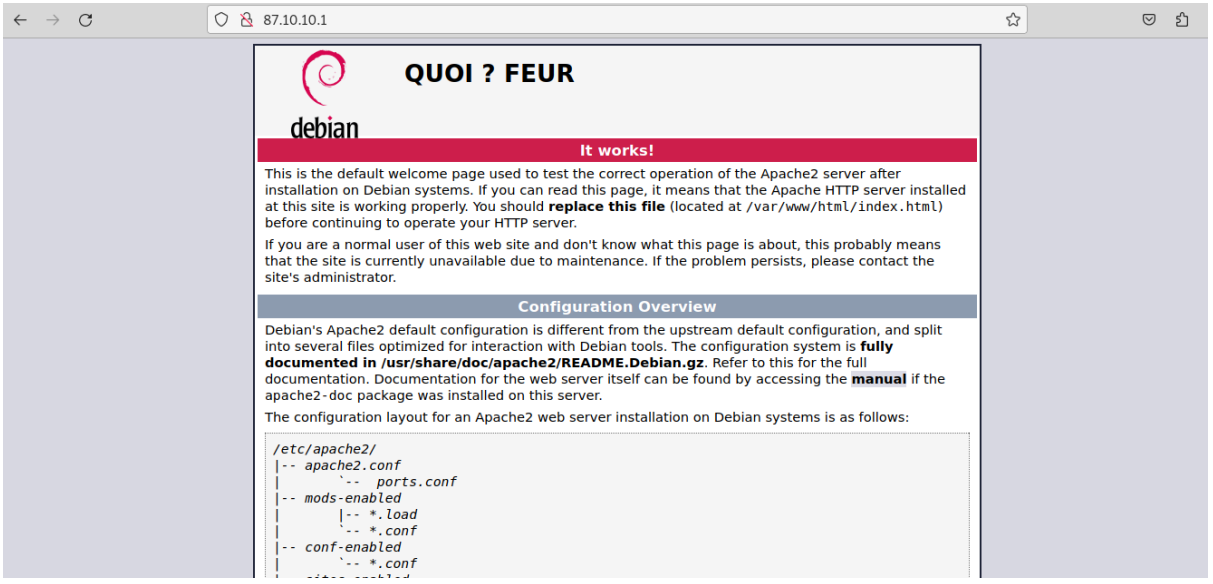
- Mise en place du filtrage.

Le filtrage reste quasiment le même sur les deux firewalls, nous vous présentons la configuration du firewall A :

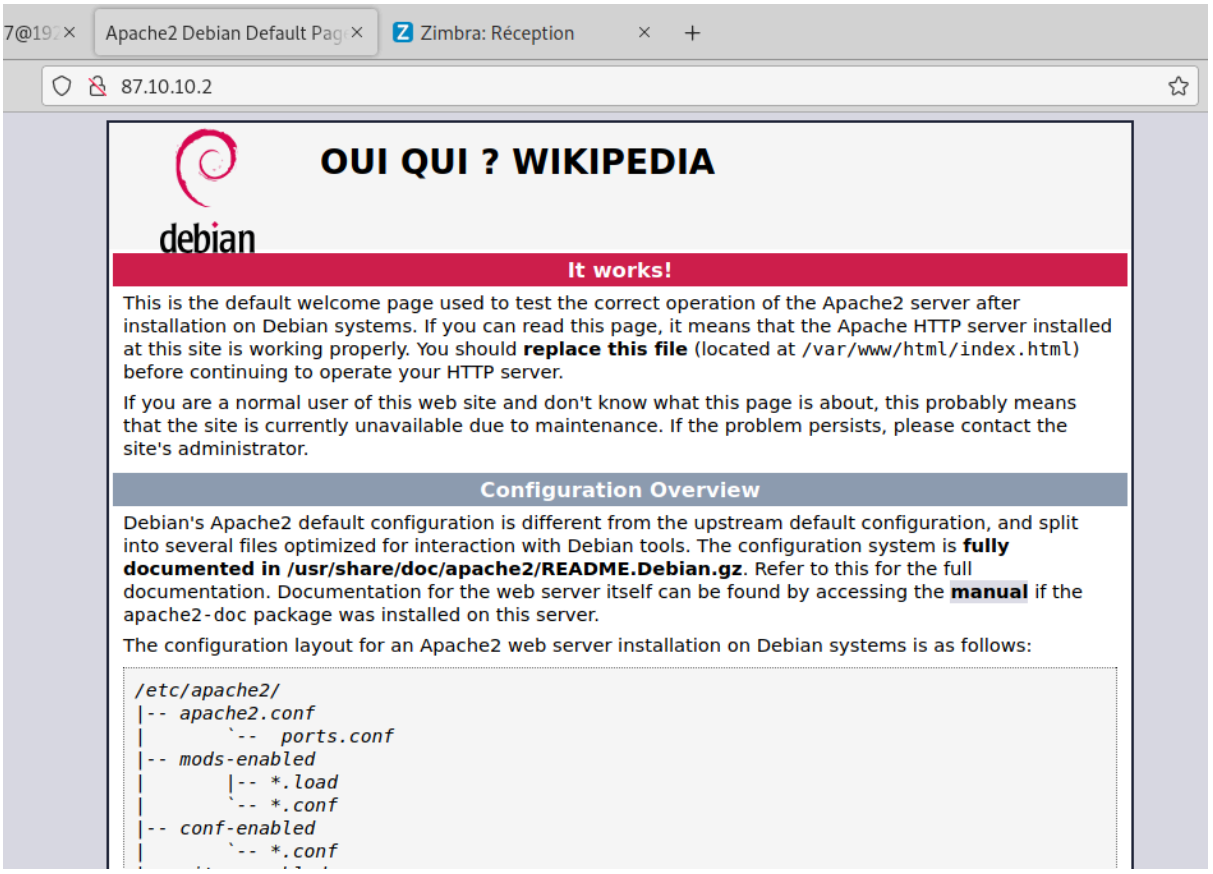


Ici, les PC présent dans le réseau interne peuvent accéder au serveur web/ftp et internet
Les paquets venant du réseau externe et du réseau de la DMZ ne peuvent pas accéder au réseau interne. Les paquets en provenance d'internet peuvent accéder à l'interface "out" du pare-feu.

Afin de tester ces règles, nous pouvons nous connecter sur l'interface out du pare feu A depuis le client B :



Nous pouvons également nous connecter sur l'interface out du pare feu B depuis le Client A :



Notre configuration fonctionne alors. Cependant, durant la configuration, nous avons eu quelques problèmes. Le premier problème était que nous n'arrivions pas à faire communiquer nos deux pare-feux sans filtrage. Pour cela, nous avons repris la configuration à zéro, puis réalisé le filtrage et la NAT étapes par étapes, en commençant par la NAT et en vérifiant le comportement escompté de chaque machine avec la configuration mise en place. Cette méthode nous à permis de trouver le problème et le solutionné.