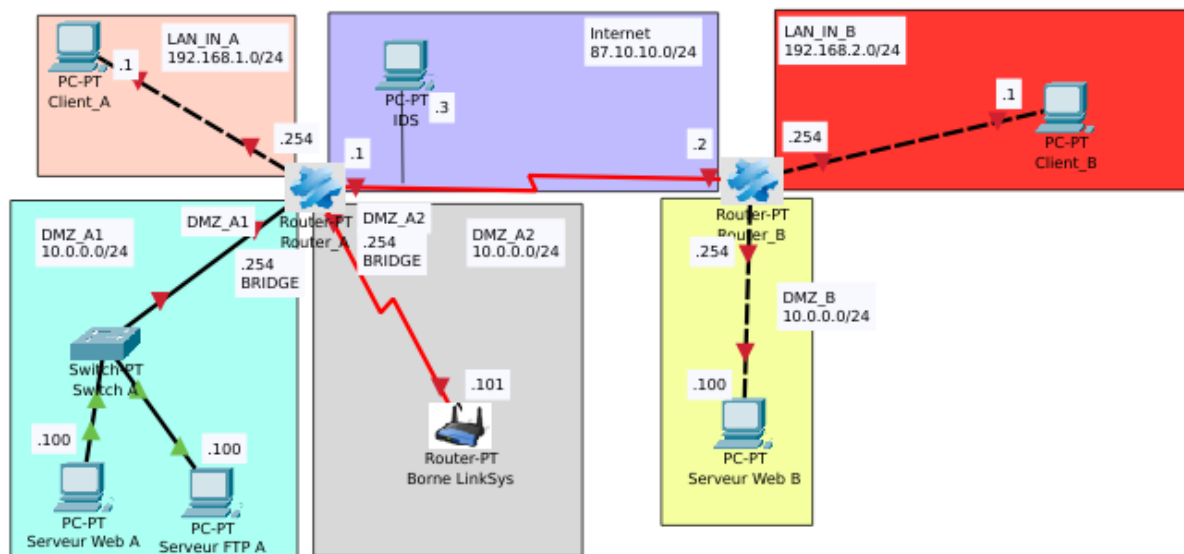


Tâche 2 : Configuration des firewalls Stormshield

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 :

Rechercher...

+ Nouvelle règle X Supprimer ↑ ↓ Couper Copier Coller Chercher dans les logs

	État	Trafic original (avant translation)			Trafic après translation			
		Source	Destination	Port dest.	Source	Port src.	Destination	Port dest.
PAT (contient 1 règles, de 1 à 1)								
1	on	Network_in interface: in	Internet interface: out	Any	→	Firewall_out	ephemeral_fw	
NAT (contient 2 règles, de 2 à 3)								
2	on	Serveur_Web_FTP	Any interface: out	Port_Web_Ftp	→	Firewall_		
3	on	Any interface: out	Firewall_out	Port_Web_Ftp	→			Serveur

Page 1 sur 1

VALIDATEUR DE CONFIGURATION

ANNULER APPLIQUER

Terminal SN210W17C2183A7@...

Mise en place de la même PAT sur le firewall B

(5) Filter 05 Activer cette politique Editer Exporter

FILTRAGE NAT

Rechercher...

+ Nouvelle règle X Supprimer ↑ ↓ Couper Copier Coller Chercher dans les logs

	État	Trafic original (avant translation)			Trafic après tra...	Options	Commentaire
		Source	Destination	Port dest.	Source		
PAT Clients IN (contient 1 règles, de 1 à 1)							
1	on	Network_in interface: in	Internet interface: out	Any	→	Firewall_out	ephemeral_fw
NAT Serveur DMZ (contient 2 règles, de 2 à 3)							
2	on	Serveur_dmz_B interface: dmz1	Internet	Ports_Web	→	Firewall_out	
3	on	Internet interface: out	Firewall_out	Ports_Web	→		S

Page 1 sur 1

Page courante 1 - 5 sur 5

- Mise en place du filtrage.

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

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(5) Filter 05 Editer Exporter i

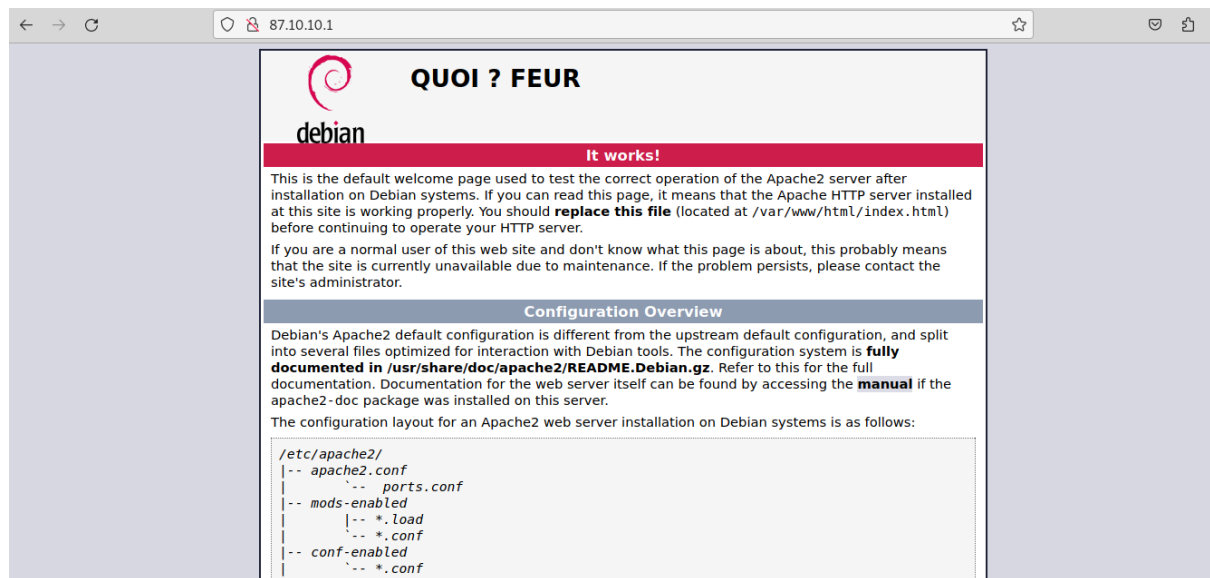
FILTRAGE NAT

Rechercher... + Nouvelle règle X Supprimer ↑ ↓ ↶ ↷ Couper Copier Coller Chercher dans les logs

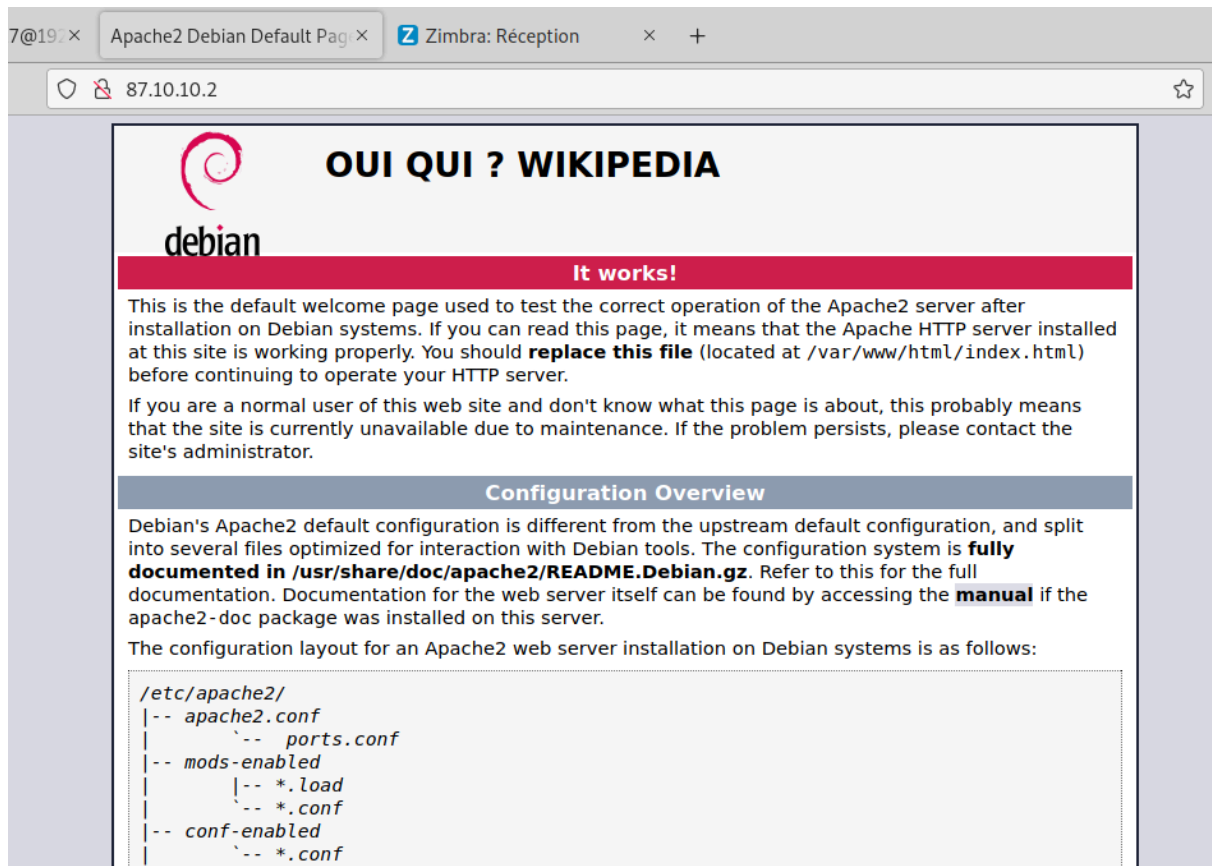
	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
1	off	passer	Any	Any	Any		IPS	Créée le 2024-03-26 09:43:
2	on	bloquer	Réseau_DMZ Réseaux_Extérie	Network_in	Any		IPS	Créée le 2024-03-26 10:21:
3	on	passer	Network_in interface: in	Serveur_Web_FTP	Port_Web_Ftp		IPS	Créée le 2024-03-26 10:24:
4	on	passer	Network_in interface: in	Internet	Any		IPS	Créée le 2024-03-26 10:26:
5	on	passer	Internet interface: out	Firewall_out	Port_Web_Ftp		IPS	Créée le 2024-03-26 10:27:

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.