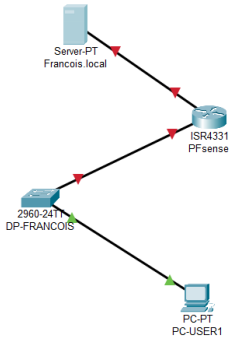
Compte Rendu : Mise en place d’un firewall sous pfSense

1. Contexte

Dans le cadre de ce projet, l’objectif était de mettre en place un pare-feu fonctionnel avec pfSense dans une infrastructure réseau composée d’un serveur, d’un pare-feu pfSense et d’un poste client (PC User).

2. Infrastructure mise en place



Équipements	Adresse IP	VLAN
Serveur	192.168.1.1	-
pfSense LAN	192.168.1.2	-
pfSense WAN	10.10.1.54	-
PC User	192.168.1.10 - 192.168.1.100	-

3. Configuration réalisée

- Installation de pfSense sur une machine virtuelle
- Configuration des interfaces WAN (10.10.1.54) et LAN (192.168.1.2/24)
- Activation du service DHCP sur pfSense (plage : 192.168.1.10 à 192.168.1.100)
- Configuration des règles de pare-feu pour assurer la sécurité du réseau local

4. Règles de sécurité appliquées

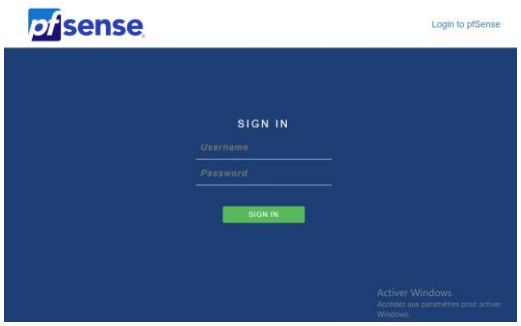
Voici les règles principales configurées dans l'interface LAN de pfSense :

- Autorisation de l’accès HTTPS depuis le serveur vers l’interface pfSense.
- Blocage de l’accès HTTP et HTTPS à pfSense depuis les clients du réseau local.
- Blocage spécifique de l’accès à YouTube via une règle de type alias (nom : Bloque_ytb).
- Autorisation des requêtes ICMP (ping) vers l’extérieur.
- Autorisation des requêtes DNS du serveur vers les DNS Google (8.8.8.8).
- Blocage du trafic DNS pour les autres clients du réseau (hors serveur).

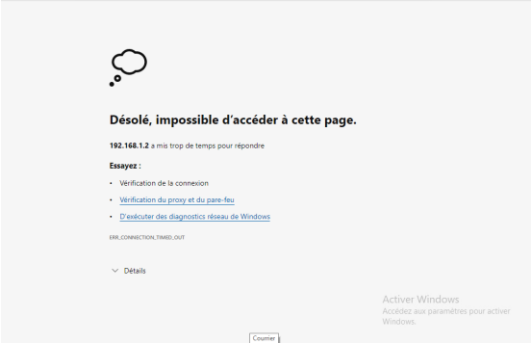
☐	✓	4 /393 KiB	IPv4 TCP	192.168.1.1	*	192.168.1.2	443 (HTTPS)	*	none	ACCES PFSENSE DEPUIS le serveur
☐	✓	0 /2 KiB	IPv4 ICMP any	LAN net	*	*	*	*	none	ACCES AU PING EXTERIEUR
☐	✗	0 /112 KiB	IPv4 TCP/UDP	LAN net	*	Bloque_ytb	80 - 443	*	none	Bloquage youtube
☐	✗	0 /0 B	IPv4 TCP/UDP	LAN net	*	192.168.1.2	80 (HTTP)	*	none	Bloquer accès Web pfsense depuis un PC USER
☐	✗	0 /3 KiB	IPv4 TCP/UDP	LAN net	*	192.168.1.2	443 (HTTPS)	*	none	Bloquage PFSENSE pc user
☐	✓	1 /1.30 MiB	IPv4 TCP/UDP	192.168.1.1	*	8.8.8.8	53 (DNS)	*	none	Autorisation Accès DNS GOOGLE
☐	✗	0 /1.44 MiB	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none	BLOQUAGE DNS GOOGLE pour les pc user

5. Tests et validation

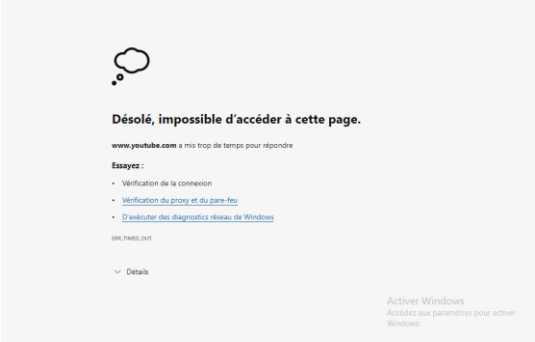
- Le serveur peut accéder à pfSense en HTTPS.



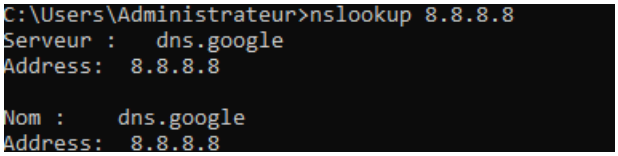
- Le PC User ne peut pas accéder à l'interface Web de pfSense.



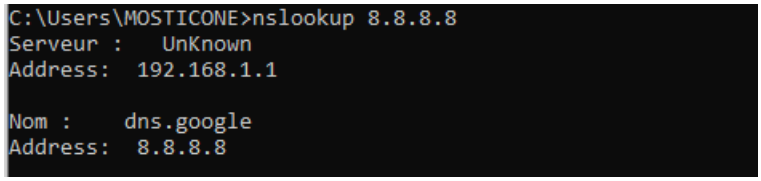
- Le PC User ne peut pas accéder à YouTube.



- Le serveur peut résoudre des noms DNS via 8.8.8.8.



- Les autres clients ne peuvent pas effectuer de requêtes DNS vers l'extérieur.



6. Conclusion

La configuration du pare-feu pfSense a permis de sécuriser le réseau local tout en conservant les fonctionnalités essentielles. Les règles ont été testées et validées avec succès. Le poste client est isolé de l'interface d'administration et les flux sont filtrés conformément aux besoins.