Dans l’infrastructure actuelle, le pfSense redirige les requêtes HTTPS vers le routeur Kali qui lui redirige vers l’IP virtuelle partagée entre les deux nœuds du Heartbeat.

Cependant, nous avons autorisé une seconde règle qui autorise les requêtes RDP (port 3389, bureau à distance), le pfSense redirige ces dernières vers le routeur qui lui va les rediriger vers directement le serveur Active Directory.

Il ne s’agit pas de manipuler mais de détecter directement par le biais du schéma réseaux, de pourquoi il existe un serveur Active Directory sur ce dernier, et les failles possibles qui existent sur ce type de machine.

Sans cette ouverture de port 3389, il ne serait pas possible de réaliser l’attaque RDP.