Installation, configuration et utilisation d'une infrastructure réseau et Active Directory

Windows Server 2025

Sommaire

1. Cahier des charges – Expression des besoins

1.1 Descriptif de l'existant

Actuellement, le réseau de l'entreprise est plat (non segmenté). Les postes de travail utilisent des comptes d'utilisateurs locaux (Workgroup), ce qui rend la gestion des mots de passe, des droits d'accès et de la sécurité réseau totalement décentralisée et fastidieuse pour le service informatique.

1.2 Besoin(s)

- Segmenter le réseau en isolant le réseau local (LAN) d'Internet (WAN) via un pare-feu matériel ou virtualisé.
- Automatiser l'attribution des adresses IP sur le réseau local.
- Centraliser l'authentification des utilisateurs et la gestion des ordinateurs via un annuaire d'entreprise.
- Intégrer les postes clients à ce nouveau domaine sécurisé.

1.3 Contrainte(s)

- **Architecture :** Déployer une maquette complète isolée (3 machines virtuelles) simulant l'architecture finale.
- **Cohérence réseau :** Le pare-feu devra distribuer les adresses IP (Serveur DHCP), mais il devra impérativement indiquer aux postes clients d'utiliser le serveur de domaine comme serveur DNS principal pour que l'intégration à l'annuaire fonctionne.

2. Ressources

2.1 Ressources mises à disposition

- **Environnement de virtualisation :** Un hyperviseur de type 2 (VMware Workstation) disposant de ressources matérielles confortables (Processeur multicœurs, 32 Go de RAM minimum).
- **Réseau virtuel :** Capacité à créer un réseau privé isolé (VMnet / LAN Segment) dédié aux communications internes de l'entreprise.

2.2 Ressources nécessaires

- **pfSense (Pare-feu/Routeur) :** 1 vCPU, 1 Go RAM, 2 cartes réseau (1 NAT pour le WAN, 1 LAN isolé).
- **Windows Server 2022/2019 (Contrôleur de Domaine) :** 2 vCPU, 4 Go RAM, 1 carte réseau (LAN isolé).
- **Windows 11 Pro (Poste Client) :** 2 vCPU, 4 Go RAM, 1 carte réseau (LAN isolé).

2.3 Gestion des ressources

La charge système sera répartie. Le pfSense consommera très peu de ressources pour le routage et le pare-feu. Le Windows Server nécessitera de la mémoire pour faire tourner les rôles AD DS (Active Directory Domain Services) et DNS.

3. Analyse

3.1 Descriptifs des solutions

- **L'approche centralisée Microsoft :** Utilisation de Windows Server pour le rôle de routeur (RRAS), DHCP, DNS et AD. *Inconvénient :* Mettre le serveur d'annuaire en frontal (routeur) est une très mauvaise pratique de sécurité.
- **L'approche modulaire (Choisie) :** Séparation des rôles. Un équipement dédié à la sécurité et au réseau (pfSense) en bordure, et un serveur dédié à l'identité (Windows Server) à l'intérieur du réseau protégé.

3.2 Comparaison des composants (Sécurité de la bordure)

Fonctionnalité	**Windows Server (RRAS)**	**pfSense (Choisi)**
Sécurité par défaut	Ouverte / Permissive	**Fermée (Bloque tout le WAN)**
Système	Windows (Cible fréquente)	**FreeBSD (Robuste et allégé)**
Gestion du DHCP	Service lourd à installer	**Intégré nativement**

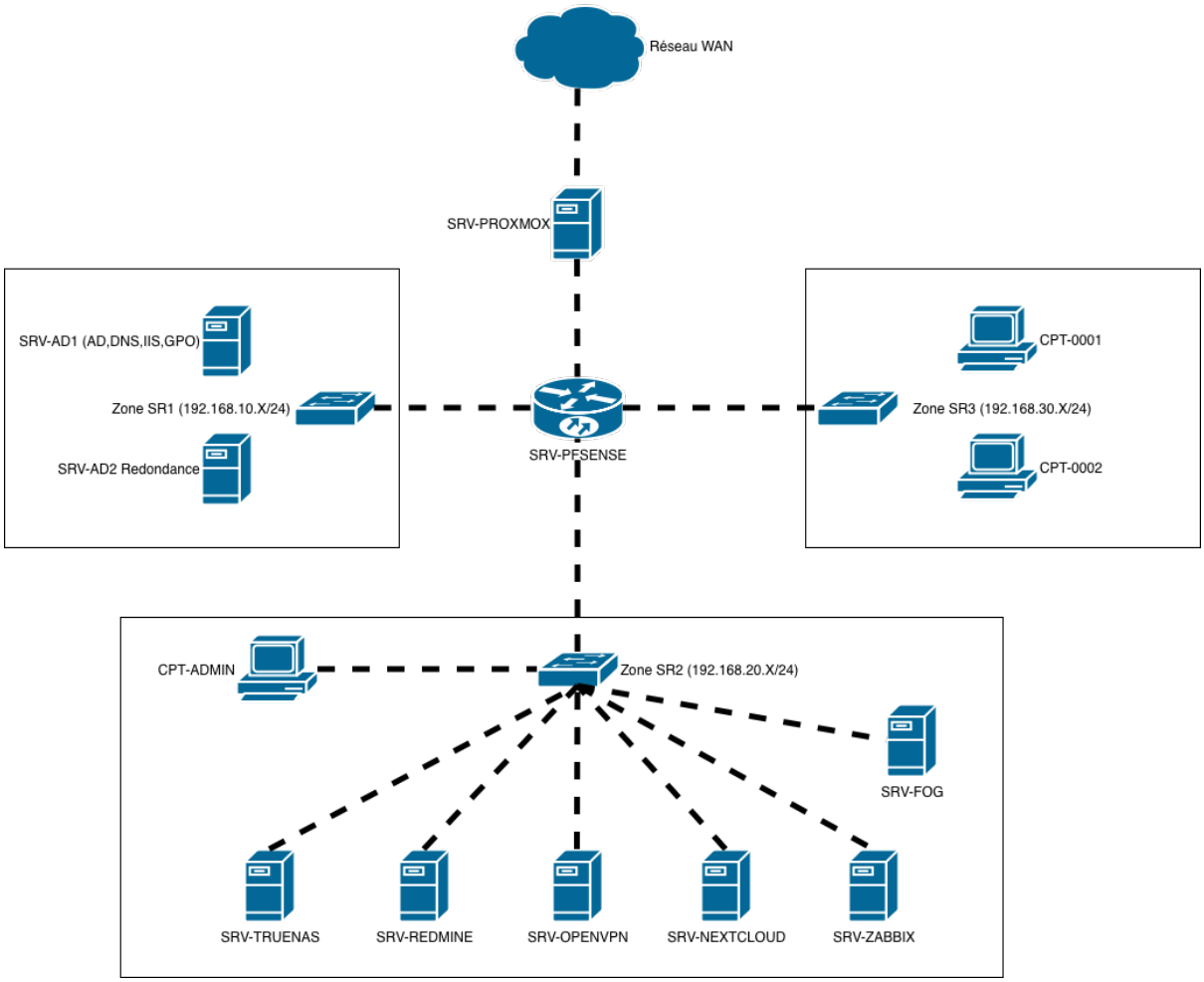
3.3 Choix d'une solution – Argumentation

L'architecture modulaire est le standard en entreprise. pfSense gérera la sécurité de périmètre et le service DHCP pour soulager le serveur. Le serveur Windows se concentrera sur son rôle fondamental : l'Active Directory et la résolution DNS interne. Le poste client Windows Pro sera ainsi sécurisé par le pare-feu et administrable par le domaine.

3.4 Étude de l'impact sur le SI existant

- **Sécurité :** Les utilisateurs ne pourront plus se connecter avec des comptes locaux non contrôlés. Les stratégies de groupe (GPO) pourront être appliquées ultérieurement.
- **Réseau :** La résolution DNS sera modifiée. Les clients interrogeront le serveur AD pour le DNS, et le serveur AD utilisera le pfSense comme "Redirecteur" pour les requêtes Internet.

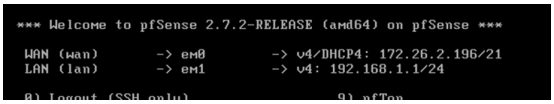
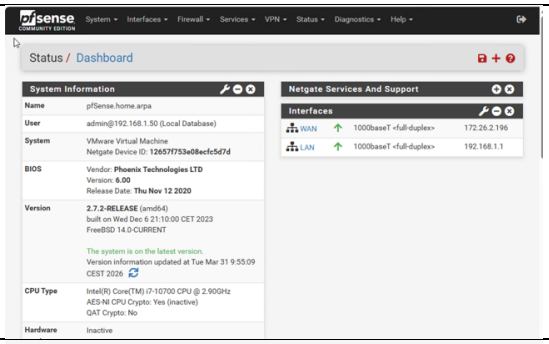
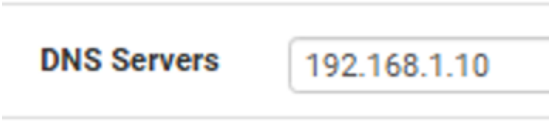
3.5 Topologie Réseau et Plan d'Adressage



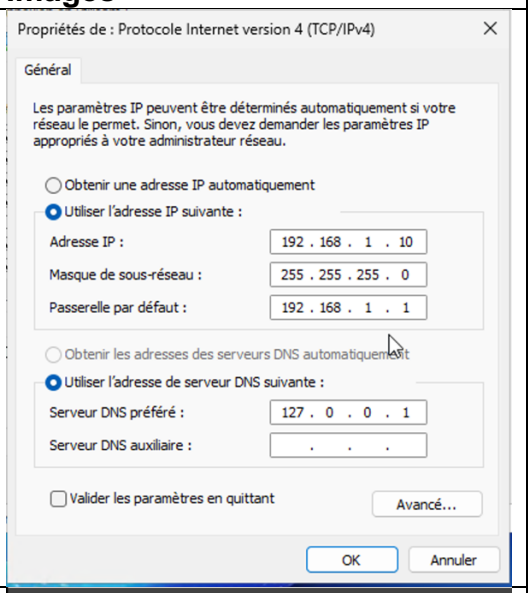
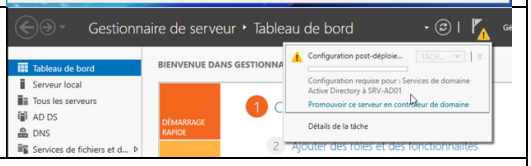
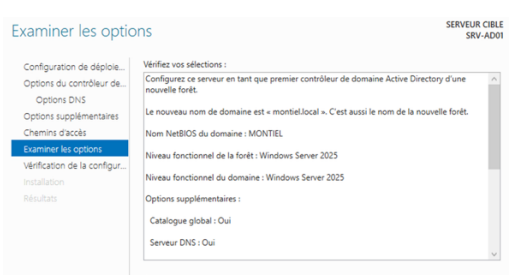
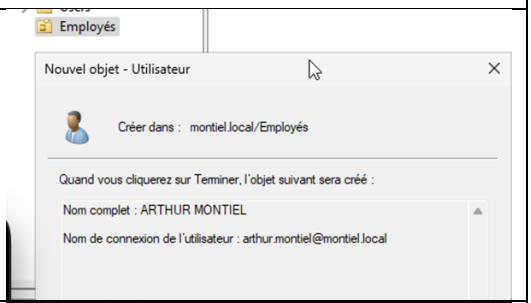
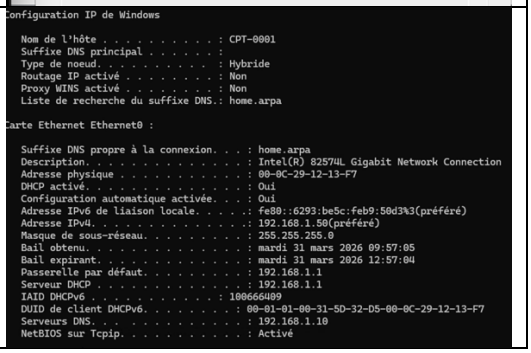
Zone / VLAN	Nom de la machine	IP Fixe / DHCP	Passerelle	Serveur DNS
SR1 (Infra)	**110 (SRV-PFSENSE)**	192.168.10.1	*(WAN)*	127.0.0.1
	111 (SRV-AD1)	192.168.10.10	192.168.10.1	127.0.0.1
	112 (SRV-AD2)	192.168.10.11	192.168.10.1	192.168.10.10
SR2 (Services)	**Interface pfSense**	192.168.20.1	-	-
	201 (CPT-ADMIN)	192.168.20.10	192.168.20.1	192.168.10.10
	220 (SRV-TRUENAS)	192.168.20.20	192.168.20.1	192.168.10.10
	230 (SRV-REDMINE)	192.168.20.30	192.168.20.1	192.168.10.10
	240 (SRV-OPENVPN)	192.168.20.40	192.168.20.1	192.168.10.10
	250 (SRV-NEXTCLOUD)	192.168.20.50	192.168.20.1	192.168.10.10
	260 (SRV-ZABBIX)	192.168.20.60	192.168.20.1	192.168.10.10
	270 (SRV-FOG)	192.168.20.70	192.168.20.1	192.168.10.10
SR3 (Clients)	**Interface pfSense**	192.168.30.1	-	-
	301 (CPT-0001)	DHCP (.30.x)	192.168.30.1	192.168.10.10
	302 (CPT-0002)	DHCP (.30.x)	192.168.30.1	192.168.10.10

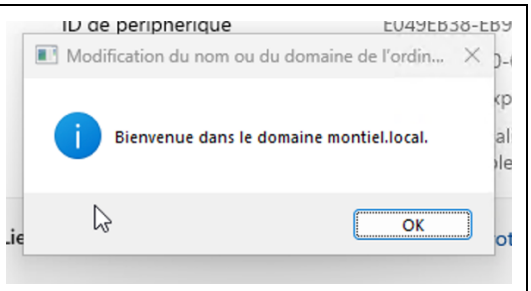
4. Mise en place

4.1 Partie 1 : Configuration du Pare-feu pfSense et du rôle DHCP

Étape	Description	Images
1	**Assignation des interfaces (Console) :** Après l'installation de pfSense, identification et assignation des cartes réseau virtuelles. Le WAN est configuré en DHCP (côté Box/Internet) et le LAN se voit attribuer une IP statique (ex : 192.168.1.1/24).	
2	**Accès WebGUI :** Depuis une machine connectée au réseau LAN, connexion à l'interface graphique via https://192.168.1.1. Finalisation du "Setup Wizard" (Fuseau horaire, mots de passe admin).	
3	**Configuration du Serveur DHCP :** Dans le menu *Services* > *DHCP Server*, activation du service sur l'interface LAN. Définition de la plage d'adresses distribuables (ex : 192.168.10.50 à 192.168.10.200).	
4	**Redirection DNS (Point Critique) :** Toujours dans les paramètres DHCP, obligation de forcer l'IP du futur contrôleur de domaine (ex : 192.168.1.1) dans le champ **DNS Servers**. C'est vital pour que les clients trouvent l'annuaire Active Directory.	
5	**Règles de filtrage (Firewall) :** Vérification dans *Firewall* > *Rules* > *LAN* de la présence de la règle par défaut autorisant le réseau LAN à sortir vers "Any" (Internet), tout en bloquant nativement tout le trafic entrant sur le WAN.	

4.2 Partie 2 : Configuration du Windows Server (AD) et intégration du Client

Étape	Description	Images
1	**Préparation réseau du Serveur :** Sur le Windows Server 2022, configuration manuelle de la carte réseau. IP fixe (192.168.1.10), masque (255.255.255.0), passerelle pfSense (192.168.1.1) et serveur DNS sur lui-même (127.0.0.1). Changement du nom d'hôte (ex: SRV-AD01).	
2	**Déploiement Active Directory :** Via le Gestionnaire de serveur, installation des rôles "Services AD DS" et "Serveur DNS".	
3	**Promotion du Contrôleur de Domaine :** Lancement de l'assistant de promotion. Création d'une nouvelle forêt avec un nom de domaine racine (ex: montiel.local). Définition du mot de passe de restauration DSRM et redémarrage.	
4	**Création des objets AD :** Ouverture du composant *Utilisateurs et ordinateurs Active Directory*. Création d'une Unité d'Organisation (OU) "Employés" et d'un utilisateur de test (ex: arthur.montiel).	
5	**Vérification du Client :** Sur le poste Windows 11, ouverture de l'invite de commande (cmd) et exécution de ipconfig /all. Vérification de l'obtention de l'IP fournie par pfSense et, surtout, de la présence du serveur DNS 192.168.1.10.	

6	**Jonction au Domaine :** Dans les paramètres système avancés du PC client, modification du groupe de travail vers le domaine montiel.local. Saisie des identifiants Administrateur du domaine pour valider la jonction, puis redémarrage.	

4.3 Rapport de tests finaux

Test de conformité	Action effectuée	Résultat attendu	Résultat obtenu
Routage et Accès Web	Depuis le Client, ping 8.8.8.8	Le pfSense route correctement le trafic vers Internet	**OK**
Résolution DNS Interne	Depuis le Client, ping montiel.local	Le Client résout l'IP du serveur (192.168.1.10)	**OK**
Authentification IAM	Sur le Client, connexion avec la session montiel\arthur.montiel	Ouverture du bureau avec le profil utilisateur du domaine	**OK**

5. Bilan

5.1 Conclusion

Le déploiement de cette infrastructure réseau et système complète est un succès. L'architecture mise en place reproduit fidèlement les standards de sécurité et de gestion d'une PME. La bordure réseau est sécurisée par le pare-feu **pfSense** qui assure également la distribution dynamique des adresses IP (DHCP). À l'intérieur du réseau local protégé (LAN), le serveur **Windows Server** centralise l'authentification des utilisateurs et la résolution de noms (DNS) via l'**Active Directory**. Les postes clients sont désormais administrables de manière centralisée et sécurisée.

5.2 Auto-critique / Auto-évaluation

- **Points forts :** La séparation claire des rôles (Routage/Sécurité sur appliance dédiée vs Annuaire sur serveur Microsoft) garantit une excellente sécurité et facilite le diagnostic en cas de panne. L'automatisation de la configuration réseau du client via le DHCP de pfSense rend l'intégration de nouveaux postes "Plug & Play".
- **Difficultés rencontrées / Points de vigilance :** La liaison entre le DHCP de pfSense et le DNS de l'Active Directory est l'étape la plus sensible. Si le pfSense distribue sa propre adresse IP comme serveur DNS au lieu de celle du Windows Server, les postes clients seront incapables de résoudre le nom de domaine (gpa.local) et la jonction échouera systématiquement. L'ordre de démarrage des machines est aussi important : le pare-feu, puis le serveur, et enfin les clients.
- **Évolutions possibles :** Déployer des Stratégies de Groupe (GPO) depuis le serveur AD pour automatiser le montage d'un lecteur réseau partagé ou restreindre l'accès au panneau de configuration sur les PC clients.

5.3 Compétence(s) SISR mobilisée(s)

Ce projet global valide plusieurs blocs de compétences majeurs du référentiel BTS SIO (Option SISR) :

- **Administrer et sécuriser les infrastructures :** Segmentation réseau (WAN/LAN) et paramétrage du routage.
- **Gérer le patrimoine informatique :** Déploiement et administration d'un annuaire centralisé (AD DS / DNS).
- **Mettre à disposition des utilisateurs un environnement de travail :** Intégration d'un poste client à un domaine d'entreprise.