BTS SIO — Option SISR

Services Informatiques aux Organisations

Déploiement d'une infrastructure réseau sécurisée multi-zones

Réalisé par

Redouane SARAOUI

Apprenti Administrateur Systèmes & Réseaux

BTS SIO SISR — Année 2025/2026

11 mai 2026

Sommaire

1. Contexte et architecture

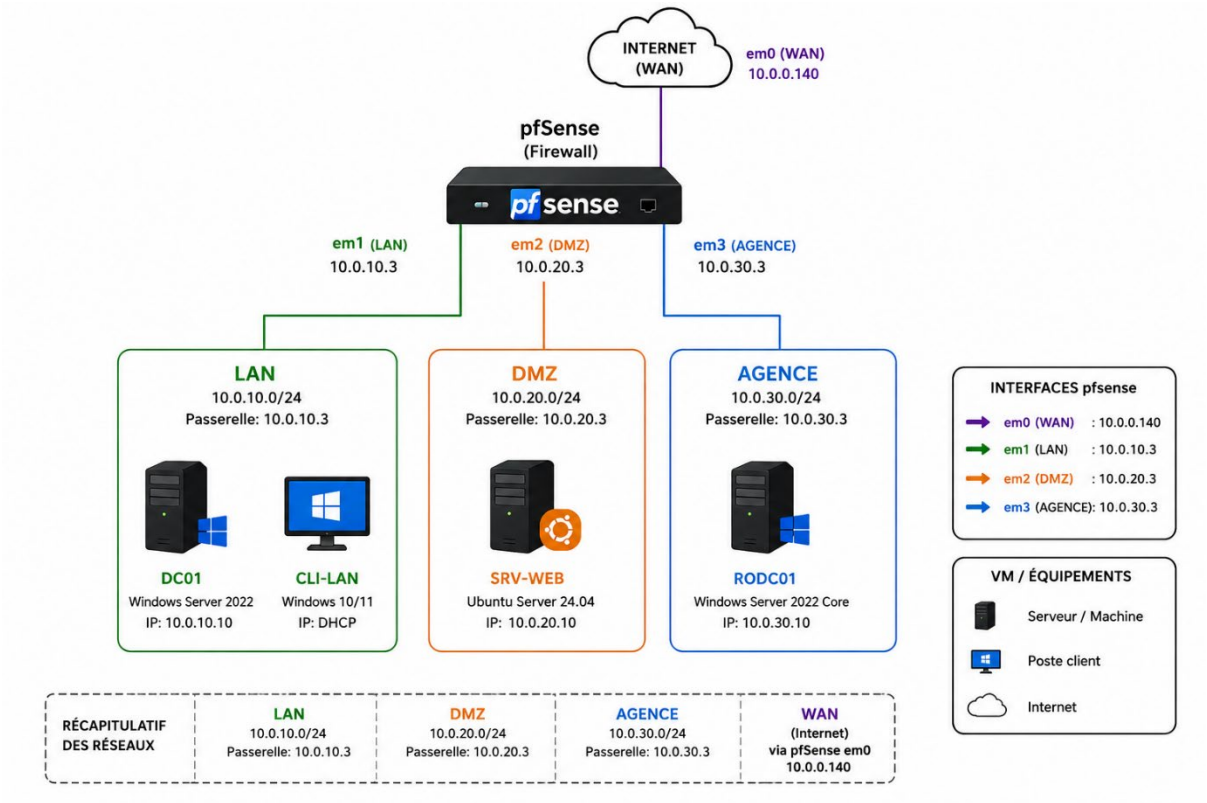
Dans le cadre d'un examen pratique de BTS SIO option SISR, j'ai mis en place une infrastructure réseau sécurisée pour la PME TechnoPlus SARL (20 employés, conseil informatique). L'objectif est de déployer une architecture segmentée incluant un pare-feu pfSense, un contrôleur de domaine principal, un contrôleur de domaine en lecture seule (RODC) sur un site distant, ainsi qu'une DMZ hébergeant un service web conteneurisé via Docker.

Cette documentation détaille l'ensemble des étapes de mise en œuvre, depuis la préparation de l'environnement de virtualisation jusqu'aux tests finaux de validation.

Architecture cible

L'infrastructure repose sur un pare-feu pfSense central disposant de 4 interfaces réseau, chacune connectée à un segment dédié :

- WAN : connexion Internet via NAT VMware
- LAN (10.0.10.0/24) : réseau interne hébergeant DC01 et les postes clients
- DMZ (10.0.20.0/24) : zone démilitarisée hébergeant le serveur web SRV-WEB
- AGENCE (10.0.30.0/24) : site distant hébergeant le RODC01



Récapitulatif des machines virtuelles

VM	OS	RAM	Disque	Réseau
pfSense	pfSense CE 2.7.x	2 Go	20 Go	4 interfaces
DC01	Windows Server 2025	4 Go	60 Go	LAN
RODC01	Windows Server 2025 Core	2 Go	40 Go	AGENCE
SRV-WEB	Ubuntu Server 24.04	2 Go	40 Go	DMZ
CLI-LAN	Windows 10/11	4 Go	60 Go	LAN

Note : *Le système d'exploitation Windows Server 2025 a été utilisé à la place de la version 2022 préconisée dans le sujet, afin de profiter du dernier niveau fonctionnel disponible.*

2. Identifiants et mots de passe

Cette section regroupe l'ensemble des identifiants utilisés dans le cadre du TP. Ces informations sont strictement réservées à l'environnement de laboratoire et ne doivent pas être réutilisées en production.

pfSense

Élément	Valeur
Utilisateur	admin
Mot de passe	p@ssw0rd1

CLI-LAN (Windows 10/11)

Élément	Valeur
Mot de passe chiffrement disque	p@ssw0rd1
Utilisateur	Redouane
Mot de passe	p@ssw0rd1
Questions de sécurité 1, 2 et 3	Redouane

DC01 (Windows Server 2025)

Élément	Valeur
Utilisateur	Administrateur
Mot de passe	p@ssw0rd1
DSRM (Directory Services Restore Mode)	p@ssw0rd1

RODC01 (Windows Server 2025 Core)

Élément	Valeur
Utilisateur	Administrateur
Mot de passe	p@ssw0rd1
SafeModeAdministratorPassword	p@ssw0rd1

SRV-WEB (Ubuntu Server 24.04)

Élément	Valeur
Utilisateur	redouane
Mot de passe	p@ssw0rd1

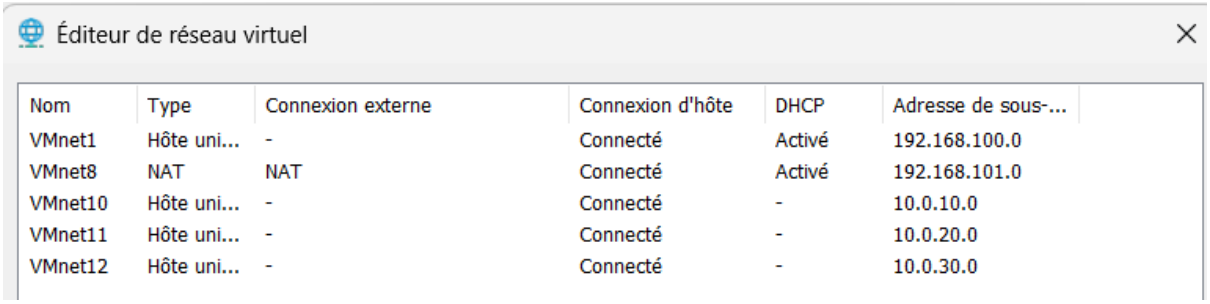
3. Préparation de l'environnement VMware

L'hyperviseur retenu est VMware Workstation Pro. Avant toute installation de VM, j'ai créé les réseaux virtuels nécessaires via le Virtual Network Editor.

Création des VMnets

VMnet	Mode	Rôle
VMnet8	NAT (par défaut)	WAN — accès Internet
VMnet10	Host-only	LAN (10.0.10.0/24)
VMnet11	Host-only	DMZ (10.0.20.0/24)
VMnet12	Host-only	AGENCE (10.0.30.0/24)

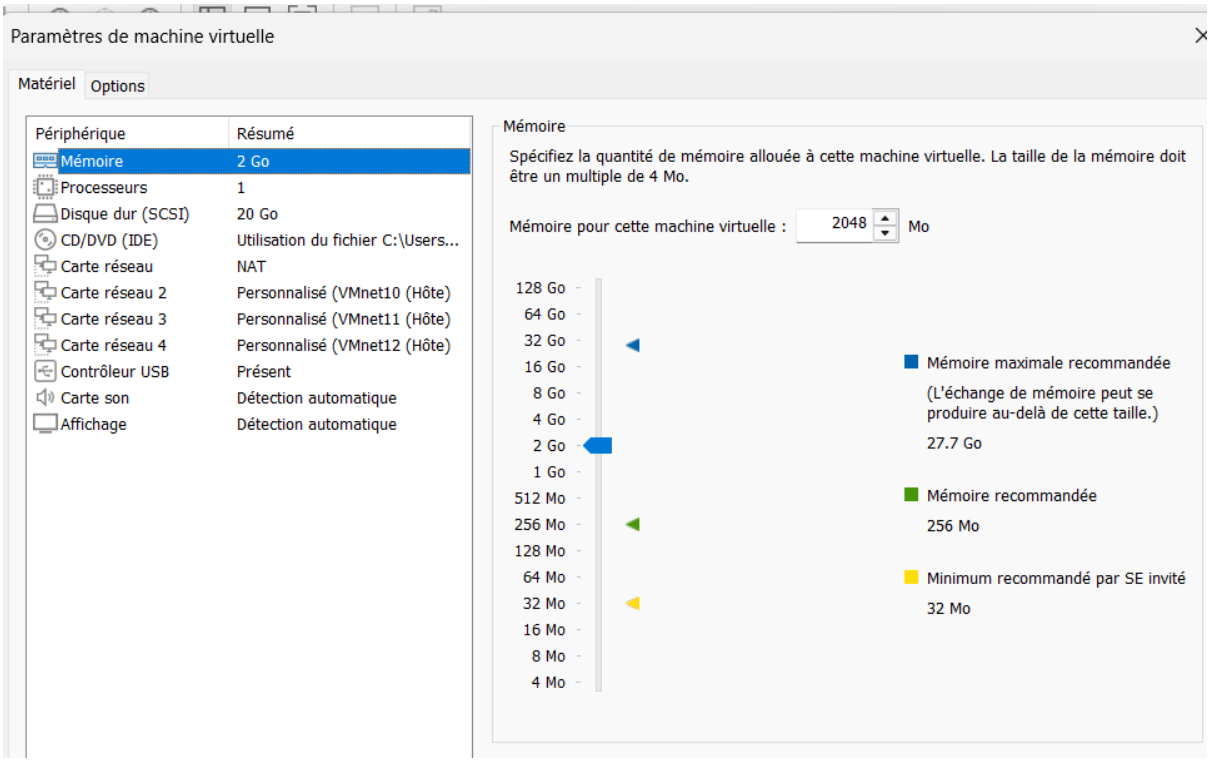
Note : *Les VMnets 10, 11 et 12 ont été configurés en mode Host-only afin que les VMs ne puissent accéder à Internet qu'à travers pfSense, qui assure le contrôle de l'ensemble des flux. Une configuration Bridged ou NAT permettrait aux machines de contourner le pare-feu.*



4. Partie 1 — Configuration de pfSense

4.1 Création de la VM pfSense

La VM pfSense a été créée avec les paramètres suivants : système d'exploitation Other 64-bit (FreeBSD), 2 Go de RAM, 20 Go de disque. Quatre cartes réseau ont été ajoutées et associées respectivement à VMnet8, VMnet10, VMnet11 et VMnet12.



4.2 Installation et attribution des interfaces

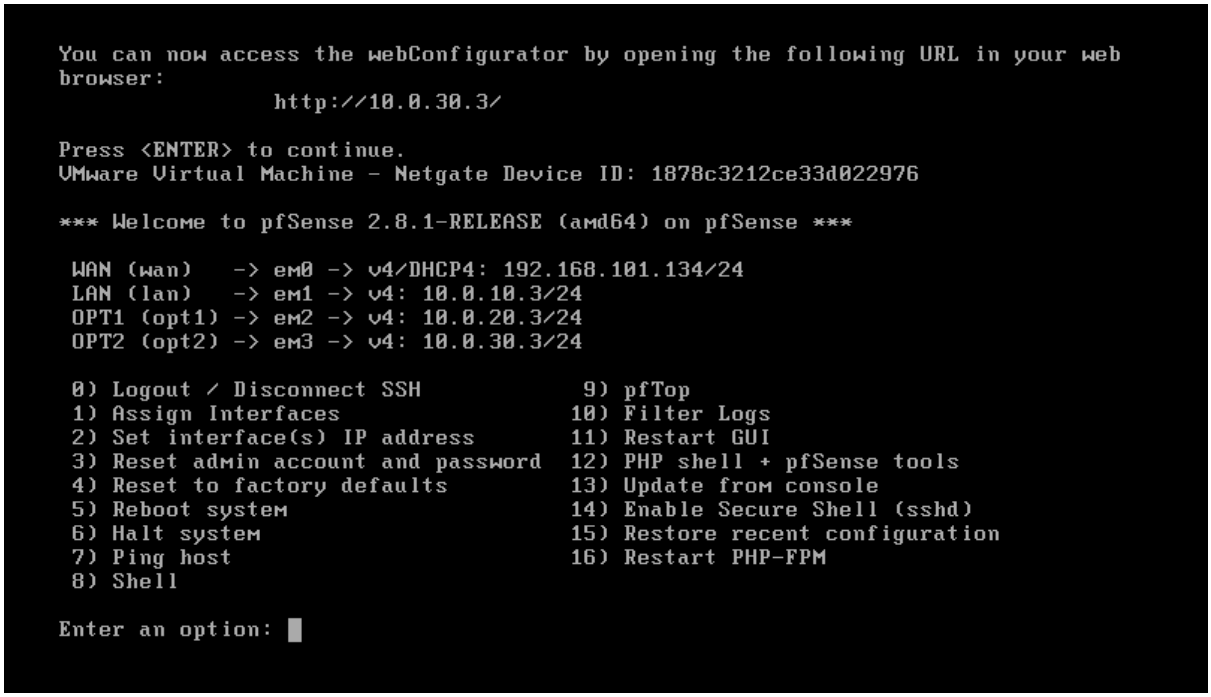
L'installation de pfSense CE 2.7.x s'est effectuée depuis l'ISO officielle, en mode Auto (UFS). Après le redémarrage, la console pfSense propose d'attribuer les interfaces.

À la question « Should VLANs be set up now? », j'ai répondu non car la segmentation réseau est assurée par les VMnets et non par des VLANs.

Attribution des interfaces

Interface pfSense	VMnet	Rôle	Adresse IP
em0	VMnet8 (NAT)	WAN	DHCP automatique
em1	VMnet10	LAN	10.0.10.3 /24
em2	VMnet11	DMZ	10.0.20.3 /24
em3	VMnet12	AGENCE	10.0.30.3 /24

> ***Note :*** *Les adresses .1 et .2 sont réservées par VMware sur les réseaux Host-only (.1 correspond à l'interface VMware sur la machine hôte, .2 à un service interne VMware). Pour cette raison, les interfaces pfSense ont été configurées en .3.*

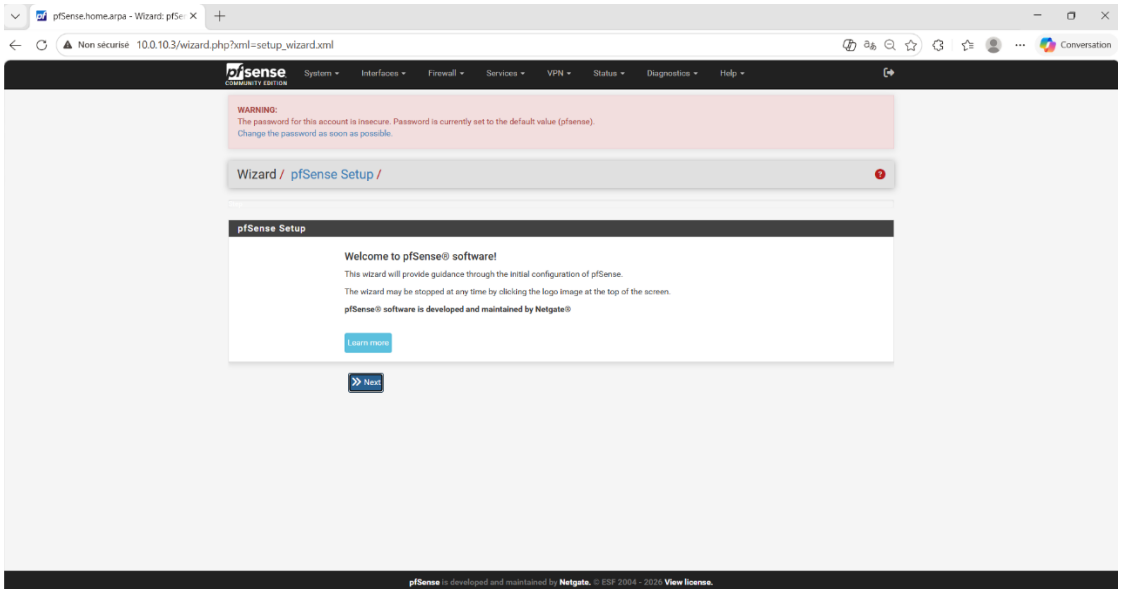

You can now access the webConfigurator by opening the following URL in your web browser:
http://10.0.30.3/
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 1878c3212ce33d022976
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.101.134/24
LAN (lan) -> em1 -> v4: 10.0.10.3/24
OPT1 (opt1) -> em2 -> v4: 10.0.20.3/24
OPT2 (opt2) -> em3 -> v4: 10.0.30.3/24
0) Logout / Disconnect SSH
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset admin account and password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart GUI
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

4.3 Assistant de configuration initiale

L'accès à l'interface web de pfSense s'effectue depuis la VM CLI-LAN connectée au LAN, via l'URL http://10.0.10.3. Lors du premier login (admin / pfsense), l'assistant Setup Wizard s'est lancé.

Paramètres de l'assistant

Paramètre	Valeur
Hostname	pfsense
Domain	global.tp
DNS Servers	8.8.8.8 / 8.8.4.4
Timezone	Europe/Paris
WAN Type	DHCP
LAN IP	10.0.10.3 /24
Admin password	Modifié (cf. section Identifiants)



4.4 Configuration du DHCP

Le service DHCP a été configuré sur les interfaces LAN et AGENCE depuis Services > DHCP Server. La DMZ n'a volontairement pas reçu de configuration DHCP.

DHCP LAN

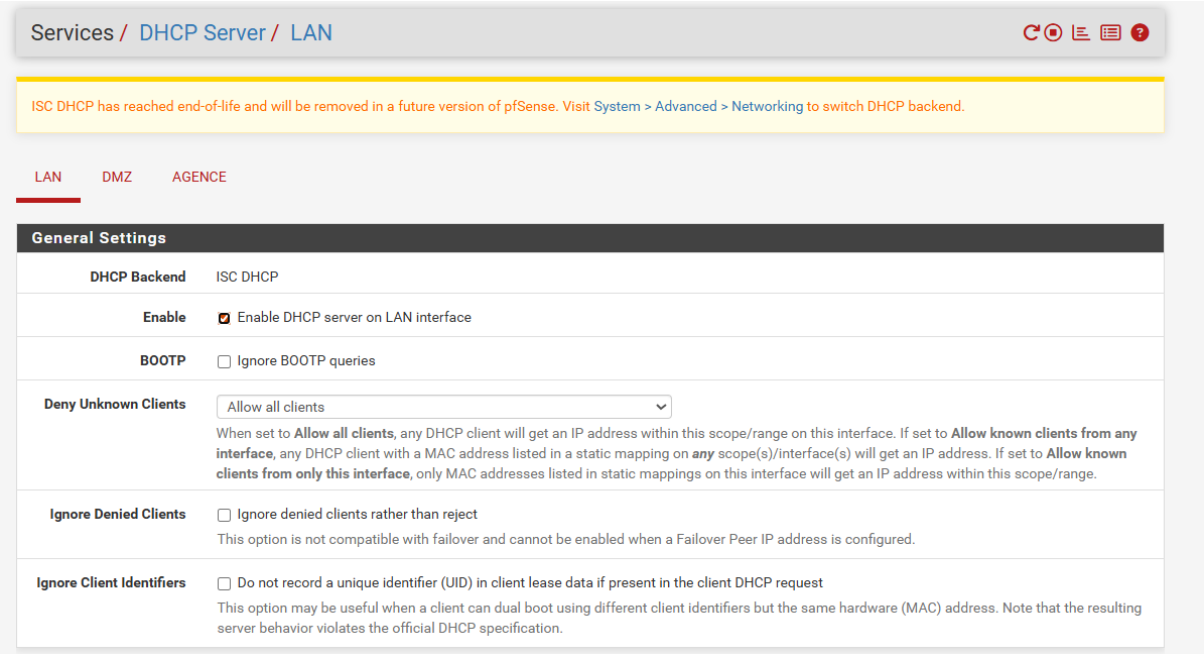
Paramètre	Valeur
Plage d'adresses	10.0.10.50 — 10.0.10.100
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	10.0.10.3
Serveur DNS	10.0.10.10
Domaine	global.tp

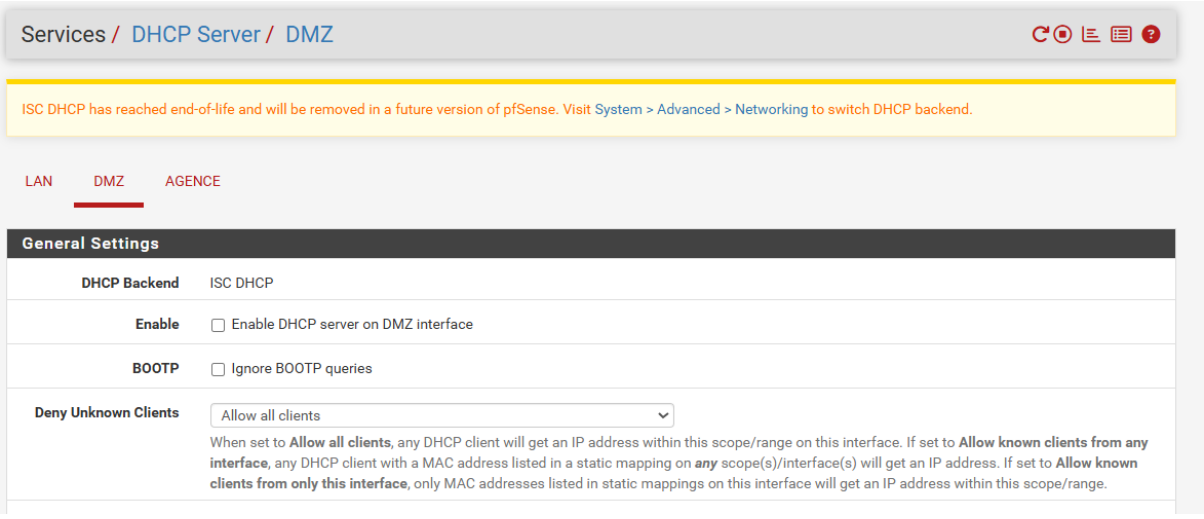
DHCP AGENCE

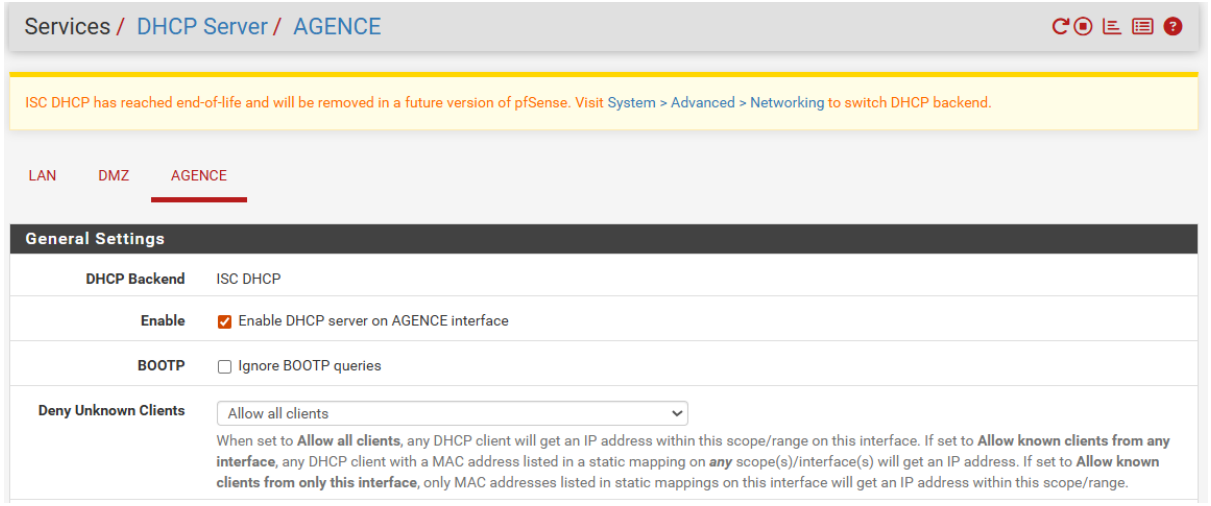
Paramètre	Valeur
Plage d'adresses	10.0.30.50 — 10.0.30.100
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	10.0.30.3
Serveur DNS	10.0.30.10
Domaine	global.tp

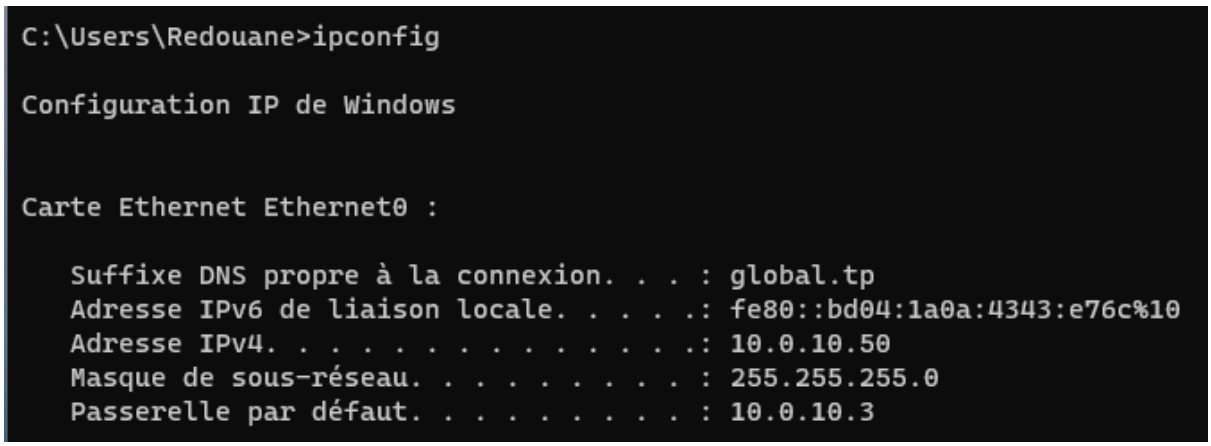
DHCP DMZ — désactivé volontairement

Le DHCP n'a pas été activé sur l'interface DMZ. Les serveurs exposés publiquement doivent obligatoirement utiliser des adresses IP statiques pour garantir un contrôle précis des flux réseau, éviter les erreurs d'attribution d'adresses, et réduire la surface d'attaque en éliminant le trafic DHCP broadcast potentiellement exploitable.






Services / DHCP Server / AGENCE
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
LAN
DMZ
AGENCE
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on AGENCE interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.


C:\Users\Redouane>ipconfig
Configuration IP de Windows
Carte Ethernet Ethernet0 :
Suffixe DNS propre à la connexion. . . : global.tp
Adresse IPv6 de liaison locale. . . . .: fe80::bd04:1a0a:4343:e76c%10
Adresse IPv4. . . . . : 10.0.10.50
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 10.0.10.3

4.5 Règles de filtrage

Les règles de filtrage ont été définies depuis Firewall > Rules pour chaque interface, en respectant le principe de moindre privilège.

Règles LAN

Action	Protocol	Source	Destination	Port	Description
Pass	TCP/UDP	LAN Subnets	*	53, 80, 443	Accès Internet
Pass	TCP	LAN Subnets	10.0.20.10	22, 80, 443	Accès SRV-WEB
Pass	Any	10.0.10.10	10.0.30.10	*	Réplication DC ↔ RODC

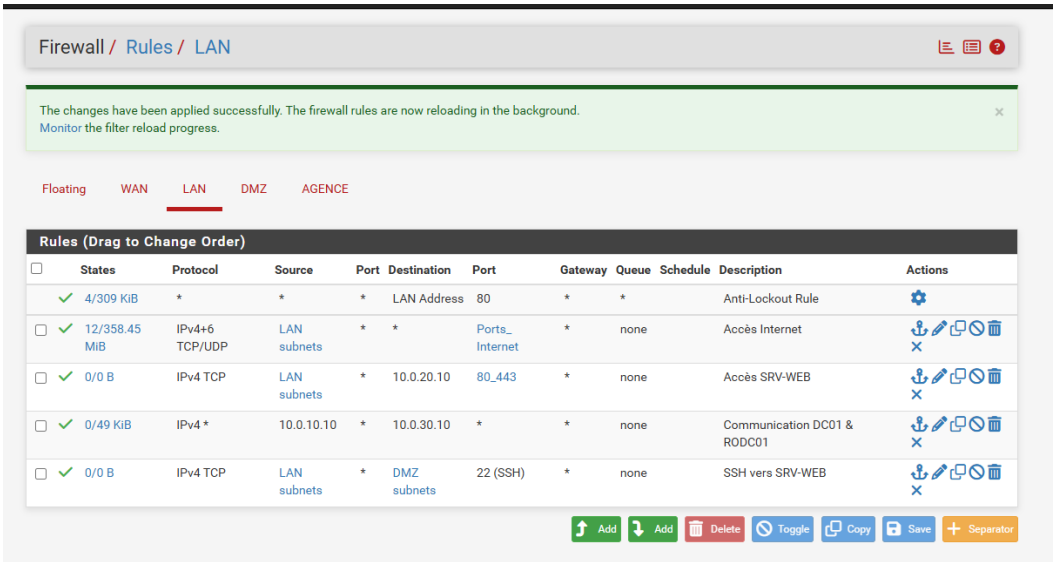
Règles DMZ

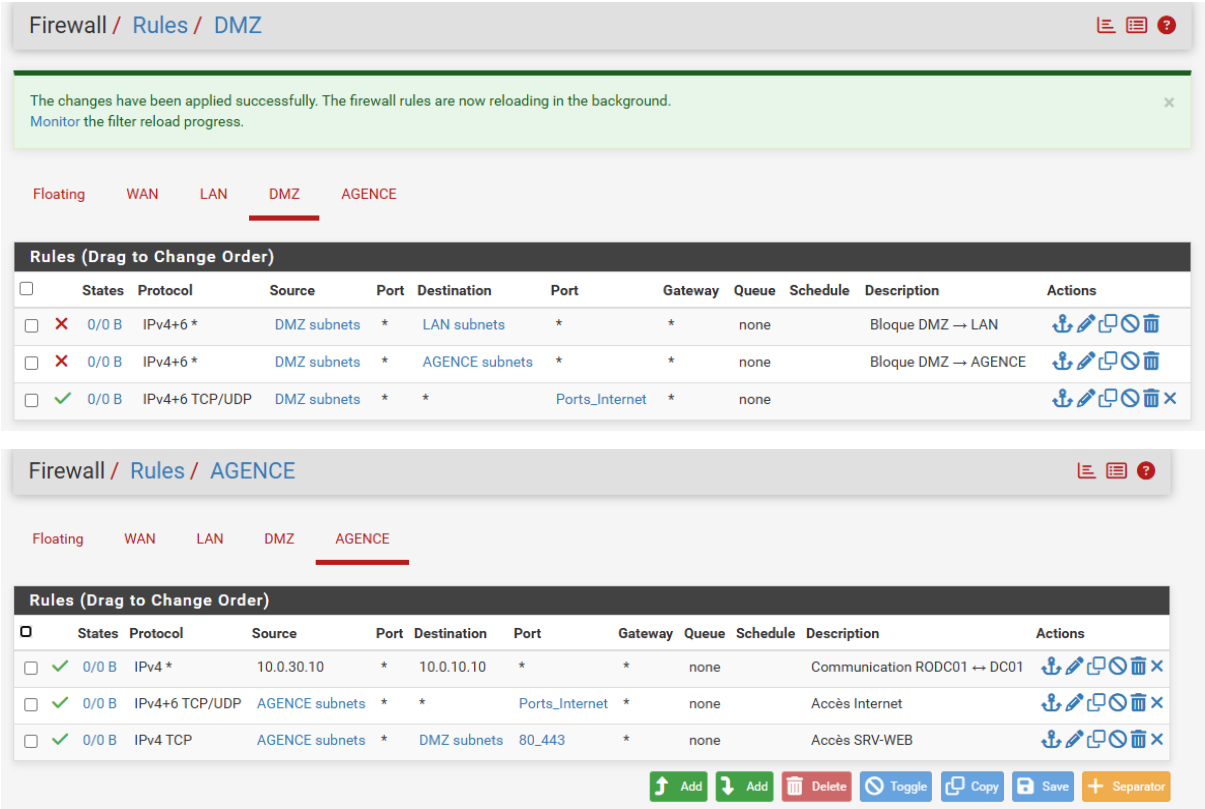
Action	Protocol	Source	Destination	Port	Description
Block	Any	DMZ Subnets	LAN Subnets	Any	Bloque DMZ → LAN
Block	Any	DMZ Subnets	AGENCE Subnets	Any	Bloque DMZ → AGENCE
Pass	TCP/UDP	DMZ Subnets	Any	53, 80, 443	Accès Internet + DNS

> ***Note :*** *Le port 53 (DNS) a été ajouté aux règles DMZ après constat lors de l'installation d'Ubuntu : sans DNS, la résolution de noms échoue et les paquets ne peuvent être téléchargés.*

Règles AGENCE

Action	Protocol	Source	Destination	Port	Description
Pass	TCP	AGENCE Subnets	DMZ Subnets	80, 443	Accès SRV-WEB
Pass	TCP/UDP	AGENCE Subnets	*	53, 80, 443	Accès Internet
Pass	Any	10.0.30.10	10.0.10.10	*	Réplication RODC ↔ DC





Question 1 — Pourquoi bloquer explicitement la DMZ vers le LAN ?

Bloquer explicitement l'accès de la DMZ vers le LAN est essentiel car la DMZ héberge des serveurs exposés à Internet, plus vulnérables aux attaques. Si un attaquant compromet un serveur de la DMZ et que celui-ci peut communiquer librement avec le LAN, il accéderait alors aux ressources internes critiques (postes utilisateurs, contrôleur de domaine), compromettant l'ensemble du système d'information.

Le principe de défense en profondeur repose sur la mise en place de plusieurs couches de sécurité successives. Dans cette architecture, le pare-feu WAN constitue la première barrière contre les attaques externes, la DMZ isole les services exposés, et les règles de filtrage empêchent toute communication non nécessaire entre la DMZ et le LAN.

4.6 Squid + SquidGuard (proxy filtrant)

Un proxy filtrant a été déployé sur pfSense afin de contrôler l'accès Internet et bloquer certaines catégories de sites web.

Installation des packages

Depuis System > Package Manager > Available Packages, j'ai installé dans l'ordre :

- squid-0.5.3 (proxy)
- squidguard-1.4_15 (filtrage URL)

Configuration de Squid

Avant toute configuration de SquidGuard, il est nécessaire de définir le cache local de Squid (Services > Squid Proxy Server > Local Cache), faute de quoi l'enregistrement des paramètres généraux génère une erreur.

Paramètre	Valeur
Squid Proxy	Activé
Proxy Interface	LAN, AGENCE
Proxy Port	3128
Transparent HTTP Proxy	Activé
Allow Users on Interface	Activé
Bypass Proxy for These Destination IPs	10.0.20.0/24

> ***Note :*** *L'exclusion 10.0.20.0/24 a été ajoutée a posteriori : sans cette règle, Squid intercepte les requêtes vers la DMZ et renvoie une erreur de connexion lorsque le client tente d'accéder au serveur web.*

Configuration de SquidGuard

La blacklist de l'Université Toulouse a été téléchargée depuis :

```
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
```

Dans Services > SquidGuard Proxy Filter > General Settings, deux options doivent être cochées :

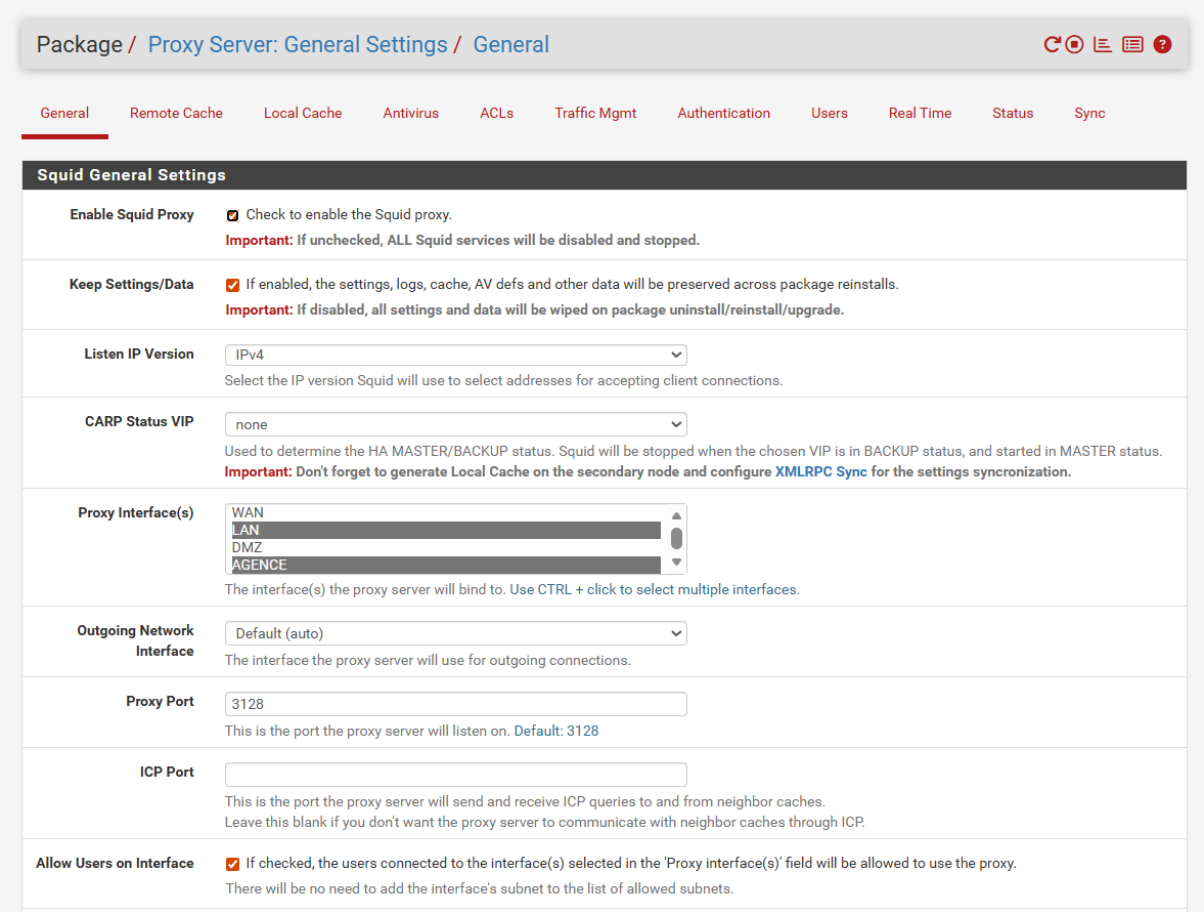
- Enable : active SquidGuard
- Enable Blacklist : rend les catégories de la blacklist disponibles dans Common ACL

> ***Note :*** *Sans la seconde option cochée, les catégories n'apparaissent pas dans la Target Rules List de Common ACL.*

Catégories bloquées

Catégorie	Action	Description
adult	Deny	Contenus à caractère pornographique
malware	Deny	Sites hébergeant des logiciels malveillants
phishing	Deny	Sites d'hameçonnage
gambling	Deny	Jeux d'argent en ligne
publicite	Deny	Bannières publicitaires

Catégorie	Action	Description
warez	Deny	Logiciels piratés
social_networks	Deny	Réseaux sociaux



Target Categories		
[blk_blacklists_adult]	access	deny
[blk_blacklists_agressif]	access	---
[blk_blacklists_ai]	access	---
[blk_blacklists_arjel]	access	---
[blk_blacklists_associations_religieuses]	access	---
[blk_blacklists_astrology]	access	---
[blk_blacklists_audio-video]	access	---
[blk_blacklists_bank]	access	---
[blk_blacklists_bitcoin]	access	---
[blk_blacklists_blog]	access	---
[blk_blacklists_celebrity]	access	---
[blk_blacklists_chat]	access	---
[blk_blacklists_child]	access	---
[blk_blacklists_cleaning]	access	---
[blk_blacklists_cooking]	access	---
[blk_blacklists_cryptojacking]	access	---
[blk_blacklists_dangerous_material]	access	---
[blk_blacklists_dating]	access	---
[blk_blacklists_ddos]	access	---
[blk_blacklists_dialer]	access	---
[blk_blacklists_doh]	access	---
[blk_blacklists_download]	access	---
[blk_blacklists_drogue]	access	---
[blk_blacklists_dynamic-dns]	access	---
[blk_blacklists_educational_games]	access	---
[blk_blacklists_examen_pix]	access	---
[blk_blacklists_exceptions_liste_bu]	access	---
[blk_blacklists_fakenews]	access	---
[blk_blacklists_filehosting]	access	---
[blk_blacklists_financial]	access	---
[blk_blacklists_forums]	access	---
[blk_blacklists_gambling]	access	deny
[blk_blacklists_games]	access	---
[blk_blacklists_hacking]	access	---
[blk_blacklists_jobsearch]	access	---
[blk_blacklists_lingerie]	access	---
[blk_blacklists_liste_blanche]	access	---
[blk_blacklists_liste_bu]	access	---
[blk_blacklists_malware]	access	deny
[blk_blacklists_manga]	access	---
[blk_blacklists_marketingware]	access	---
[blk_blacklists_mixed_adult]	access	---
[blk_blacklists_mobile-phone]	access	---
[blk_blacklists_phishing]	access	deny
[blk_blacklists_press]	access	---
[blk_blacklists_publicite]	access	deny
[blk_blacklists_radio]	access	---
[blk_blacklists_reaffected]	access	---
[blk_blacklists_redirector]	access	---
[blk_blacklists_remote-control]	access	---
[blk_blacklists_residential-proxies]	access	---
[blk_blacklists_sect]	access	---
[blk_blacklists_sexual_education]	access	---
[blk_blacklists_shopping]	access	---
[blk_blacklists_shortener]	access	---
[blk_blacklists_social_networks]	access	deny
[blk_blacklists_special]	access	---
[blk_blacklists_sports]	access	---
[blk_blacklists_stalkerware]	access	---
[blk_blacklists_strict_redirector]	access	---
[blk_blacklists_strong_redirector]	access	---
[blk_blacklists_translation]	access	---
[blk_blacklists_tricheur]	access	---
[blk_blacklists_tricheur_pix]	access	---
[blk_blacklists_update]	access	---
[blk_blacklists_vpn]	access	---
[blk_blacklists_warez]	access	deny
[blk_blacklists_webhosting]	access	---
[blk_blacklists_webmail]	access	---
Default access [all]	access	allow

Test du filtrage

Le test du filtrage est réalisé depuis un poste client du LAN, en exécutant :

```
curl -I http://site-interdit.com
```

Une réponse HTTP 301/302 (redirection vers la page de blocage) ou 403 Forbidden confirme le bon fonctionnement du filtrage. Les logs SquidGuard de pfSense permettent ensuite de vérifier que la requête a bien été interceptée.

5. Partie 2 — Active Directory et GPO

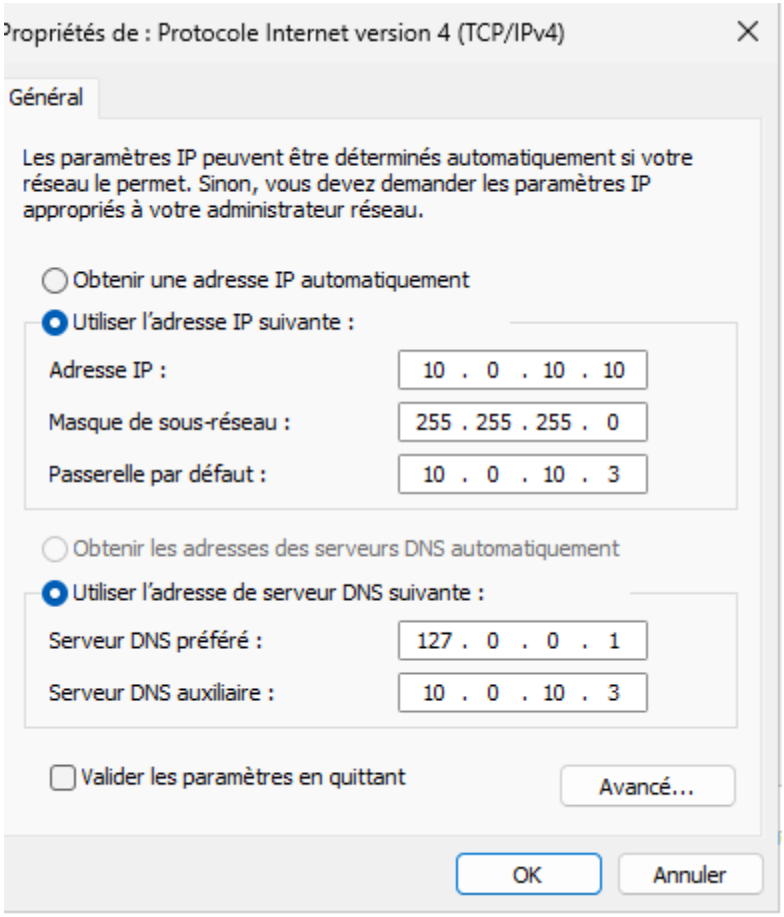
5.1 Création et promotion de DC01

La VM DC01 a été créée avec Windows Server 2025, 4 Go de RAM, 60 Go de disque, et raccordée au VMnet10 (LAN).

Configuration IP statique

Paramètre	Valeur
Adresse IP	10.0.10.10
Masque de sous-réseau	255.255.255.0
Passerelle	10.0.10.3
DNS préféré	10.0.10.10 (lui-même)
DNS alternatif	10.0.10.3

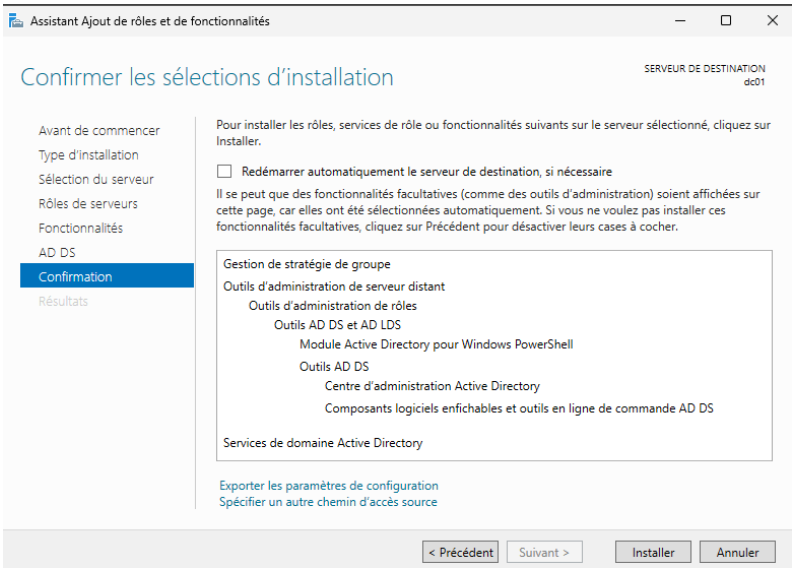
Note : *Un contrôleur de domaine pointe toujours sur lui-même comme DNS préféré, car c'est lui qui fait autorité sur la zone global.tp.*

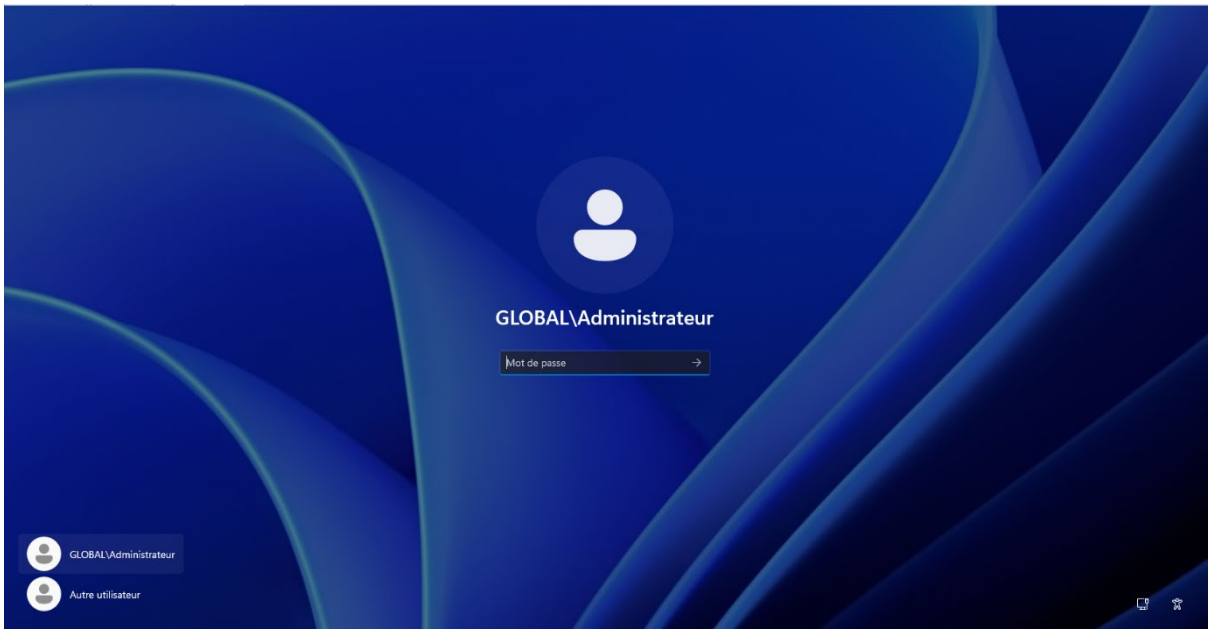


Promotion en contrôleur de domaine

La promotion s'effectue depuis Server Manager via le drapeau d'alerte > « Promote this server to a domain controller ».

Paramètre	**Valeur**
Opération	Ajouter une nouvelle forêt
Nom de domaine racine	global.tp
Niveau fonctionnel forêt	Windows Server 2025
Niveau fonctionnel domaine	Windows Server 2025
Serveur DNS	OUI
Catalogue global	OUI
Créer une délégation DNS	NON
Nom NetBIOS	GLOBAL

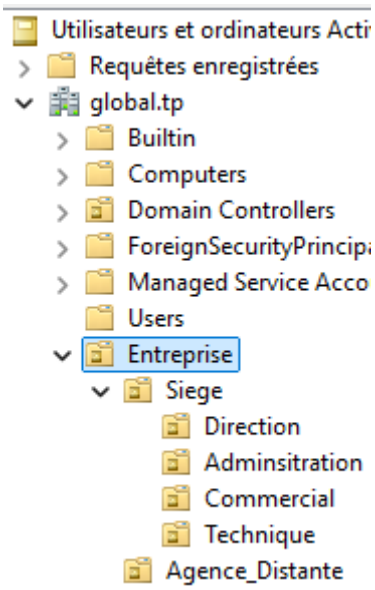




5.2 Création des OUs

L'arborescence des Unités d'Organisation a été créée dans Active Directory Users and Computers (ADUC), avec une OU racine Entreprise contenant deux sous-OUs principales : Siege et Agence_Distante.

```
global.tp
│
└── Entreprise
    │
    ├── Siege
    │   ├── Direction
    │   ├── Administratif
    │   ├── Commercial
    │   └── Technique
    │
    └── Agence_Distante
```



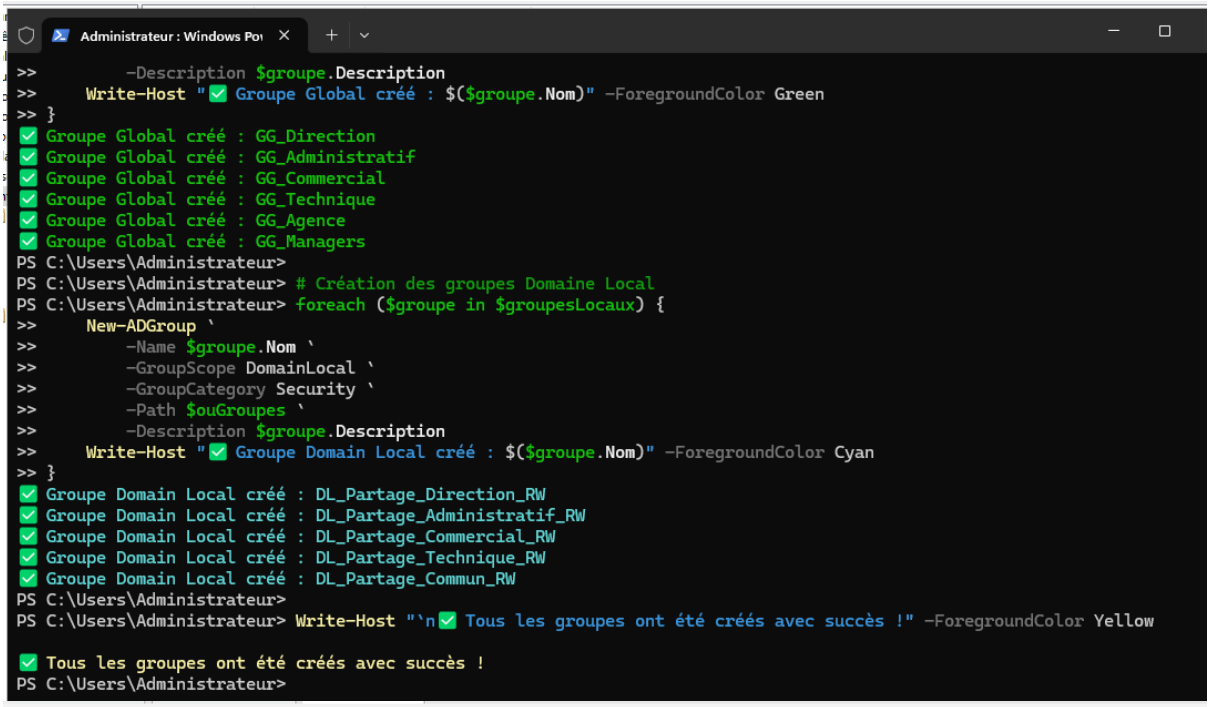
5.3 Création des groupes (AGDLP)

La stratégie AGDLP a été appliquée : les utilisateurs sont placés dans des groupes globaux (GG_*), ces groupes globaux sont membres de groupes domaine local (DL_*), et les permissions NTFS sont appliquées aux groupes DL.

Les groupes ont été créés via un script PowerShell pour gagner en rigueur et reproductibilité :

```
Import-Module ActiveDirectory
$base = "DC=global,DC=tp"
$ouGroupes = "OU=Entreprise,$base"

$groupesGlobaux = @(
    @{ Nom="GG_Direction";    Description="Direction générale" },
    @{ Nom="GG_Administratif"; Description="Services administratifs" },
    @{ Nom="GG_Commercial";   Description="Commerciaux" },
    @{ Nom="GG_Technique";    Description="Personnel informatique" },
    @{ Nom="GG_Agence";       Description="Employés agence distante" },
    @{ Nom="GG_Managers";     Description="Responsables et managers" }
)

$groupesLocaux = @(
    @{ Nom="DL_Partage_Direction_RW" },
```

```
    @{ Nom="DL_Partage_Administratif_RW" },
    @{ Nom="DL_Partage_Commercial_RW" },
    @{ Nom="DL_Partage_Technique_RW" },
    @{ Nom="DL_Partage_Commun_RW" }
)

foreach ($g in $groupesGlobaux) {
    New-ADGroup -Name $g.Nom -GroupScope Global -GroupCategory Security `
        -Path $ouGroupes -Description $g.Description
}
foreach ($g in $groupesLocaux) {
    New-ADGroup -Name $g.Nom -GroupScope DomainLocal -GroupCategory Security `
        -Path $ouGroupes
}
```



5.4 Création des 20 utilisateurs

Les 20 comptes utilisateurs ont également été créés via un script PowerShell automatisé. Chaque utilisateur reçoit le mot de passe initial Azerty123! avec obligation de le changer à la première connexion.

```
Import-Module ActiveDirectory
$password = ConvertTo-SecureString "Azerty123!" -AsPlainText -Force
$base = "DC=global,DC=tp"

$users = @(
    @{ Login="p.moreau"; Nom="Moreau"; Prenom="Philippe";
       OU="OU=Direction,OU=Siege,OU=Entreprise";
       Groupes=@("GG_Direction","GG_Managers") },
    # ... (20 entrées au total)
)

foreach ($user in $users) {
    $ouPath = "$($user.OU),$base"
    New-ADUser -SamAccountName $user.Login `
        -GivenName $user.Prenom -Surname $user.Nom `
        -Name "$($user.Prenom) $($user.Nom)" `
        -UserPrincipalName "$($user.Login)@global.tp" `
        -Path $ouPath -AccountPassword $password `
        -ChangePasswordAtLogon $true -Enabled $true

    foreach ($groupe in $user.Groupes) {
        Add-ADGroupMember -Identity $groupe -Members $user.Login
    }
}
```

Vérification du nombre d'utilisateurs créés :

```
Get-ADUser -Filter * -SearchBase "OU=Entreprise,DC=global,DC=tp" |
    Select-Object Name, SamAccountName | Sort-Object Name
```

```
PS C:\Users\Administrateur> Get-ADUser -Filter * -SearchBase "OU=Entreprise,DC=global,DC=tp" |
>>     Select-Object Name, SamAccountName | Sort-Object

Name               SamAccountName
----               --------------
Hugo Bonnet        h.bonnet
Laura Fontaine     l.fontaine
Aurelie Laurent    a.laurent
Maxime Girard      m.girard
Romain Blanc       r.blanc
Charlotte Henry    c.henry
David Marchand     d.marchand
Isabelle Chevalier i.chevalier
Thomas Garcia      t.garcia
Camille Roux       c.roux
Philippe Moreau    p.moreau
Sophie Bernard     s.bernard
Francois Michel    f.michel
Vincent Simon      v.simon
Nicolas Fournier   n.fournier
Emma Lambert       e.lambert
```

5.5 Partages réseau et permissions NTFS

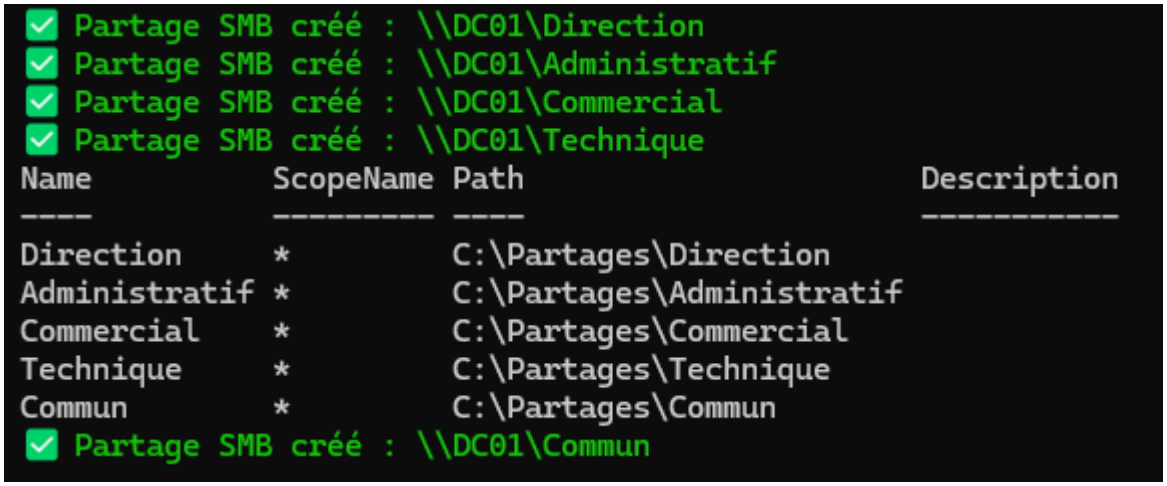
Les dossiers partagés ont été créés sur DC01 dans C:\Partages, avec création des partages SMB et application des permissions NTFS via PowerShell.

```
$racine = "C:\Partages"
New-Item -Path $racine -ItemType Directory -Force

$partages = @(
    @{ Dossier="Direction";    Groupe="DL_Partage_Direction_RW" },
    @{ Dossier="Administratif"; Groupe="DL_Partage_Administratif_RW" },
    @{ Dossier="Commercial";   Groupe="DL_Partage_Commercial_RW" },
    @{ Dossier="Technique";    Groupe="DL_Partage_Technique_RW" },
    @{ Dossier="Commun";       Groupe="DL_Partage_Commun_RW" }
)

foreach ($p in $partages) {
    $chemin = "$racine\$($p.Dossier)"
    New-Item -Path $chemin -ItemType Directory -Force
    New-SmbShare -Name $p.Dossier -Path $chemin `
        -FullAccess "GLOBAL\Administrateur"
    $acl = Get-Acl $chemin
    $rule = New-Object System.Security.AccessControl.FileSystemAccessRule(
        $p.Groupe, "Modify",
        "ContainerInherit,ObjectInherit", "None", "Allow")
    $acl.AddAccessRule($rule)
    Set-Acl -Path $chemin -AclObject $acl
}
```

> ***Note :*** *Lors de la première exécution, l'ajout de l'accès SMB au compte « Administrateur » a échoué (erreur 1332 : « Le mappage entre les noms de compte et les ID de sécurité n'a pas été effectué »). Le préfixe GLOBAL\Administrateur a permis de forcer la résolution du compte dans le domaine et résoudre le problème.*

Récapitulatif des permissions

Dossier	Nom partage	Groupe autorisé	Permissions NTFS
Direction	Direction	DL_Partage_Direction_RW	Modifier
Administratif	Administratif	DL_Partage_Administratif_RW	Modifier
Commercial	Commercial	DL_Partage_Commercial_RW	Modifier
Technique	Technique	DL_Partage_Technique_RW	Modifier
Commun	Commun	DL_Partage_Commun_RW	Modifier


✅ Partage SMB créé : \\DC01\Direction
✅ Partage SMB créé : \\DC01\Administratif
✅ Partage SMB créé : \\DC01\Commercial
✅ Partage SMB créé : \\DC01\Technique
Name ScopeName Path Description
---- --------- ---- -----------
Direction * C:\Partages\Direction
Administratif * C:\Partages\Administratif
Commercial * C:\Partages\Commercial
Technique * C:\Partages\Technique
Commun * C:\Partages\Commun
✅ Partage SMB créé : \\DC01\Commun

5.6 GPO de sécurité

Une GPO nommée GPO_Securite a été créée et liée à l'OU Siege via la console Group Policy Management. Elle applique trois restrictions :

Blocage des périphériques USB

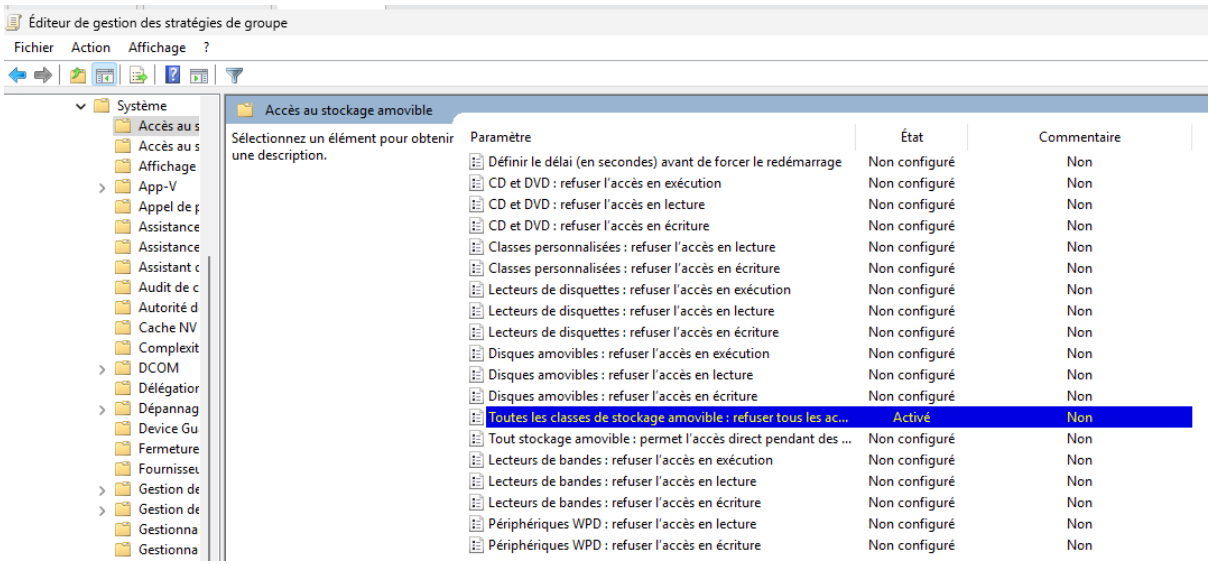
```
Configuration ordinateur > Stratégies > Modèles d'administration
  > Système > Accès au stockage amovible
  → Toutes les classes de stockage amovible : refuser tous les accès
  → Activé
```

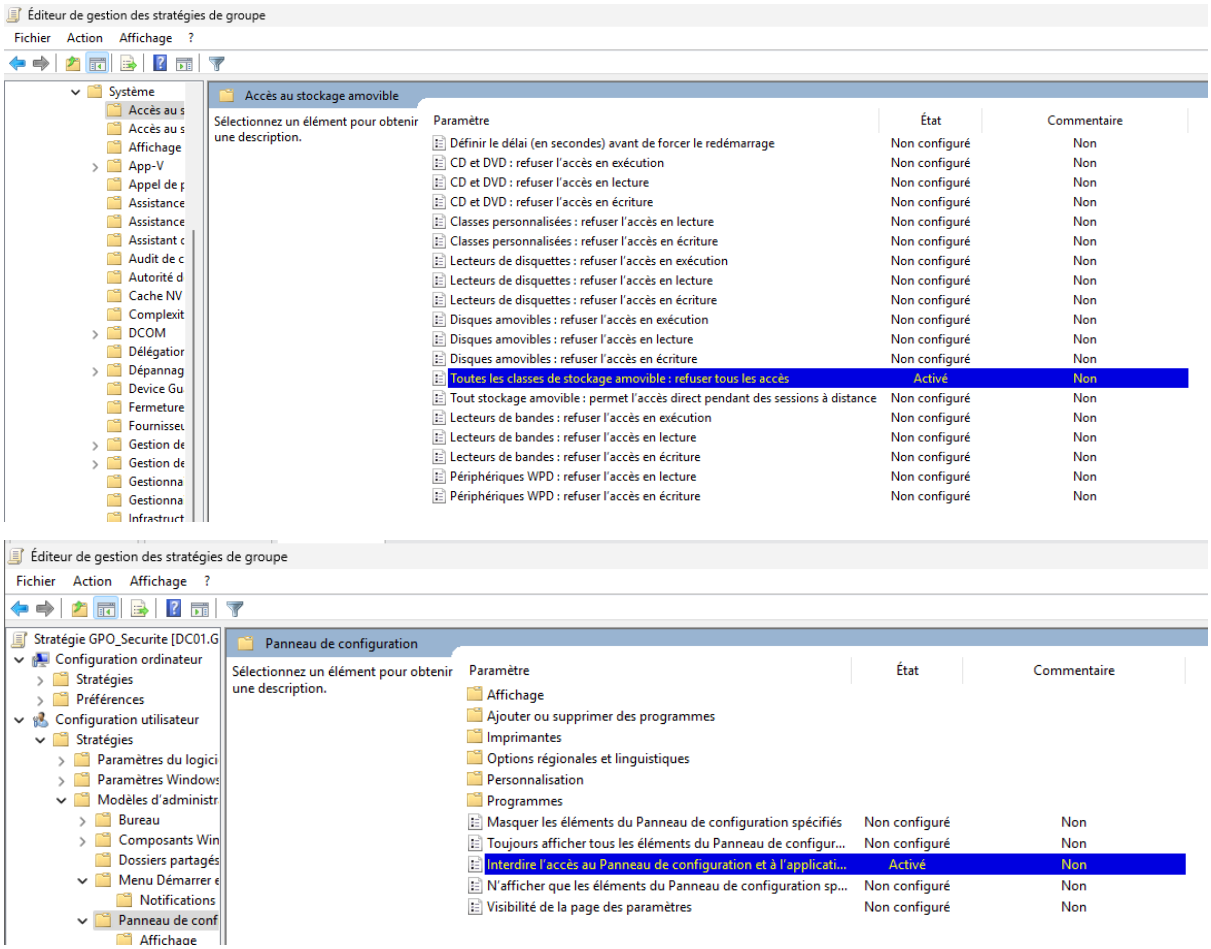
Blocage du Panneau de configuration

```
Configuration utilisateur > Stratégies > Modèles d'administration
  > Panneau de configuration
  → Interdire l'accès au Panneau de configuration et aux paramètres du PC
  → Activé
```

Fond d'écran imposé

```
Configuration utilisateur > Stratégies > Modèles d'administration
  > Bureau > Bureau
  → Papier peint du Bureau : Activé
  → Nom du papier peint : \\DC01\Commun\wallpaper.jpg
  → Style du papier peint : Remplissage
```





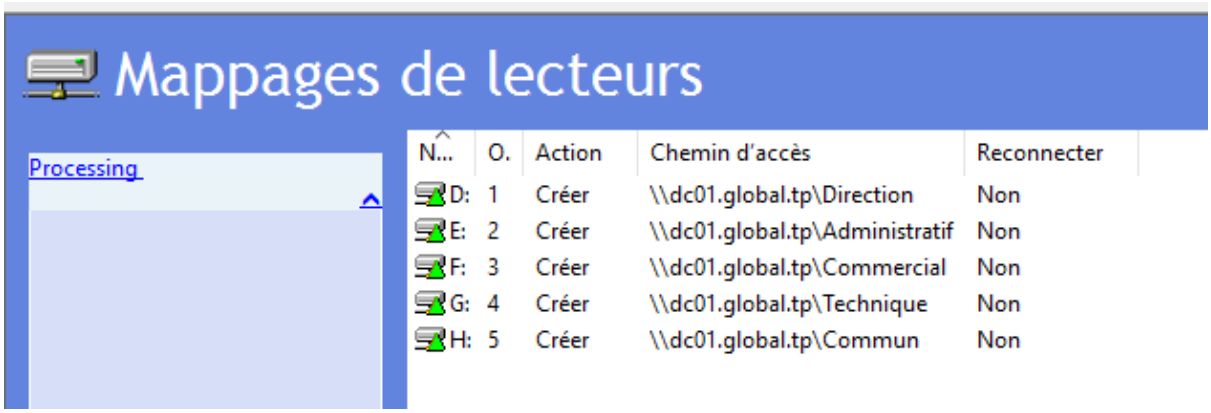
5.7 GPO Lecteurs réseau avec ciblage

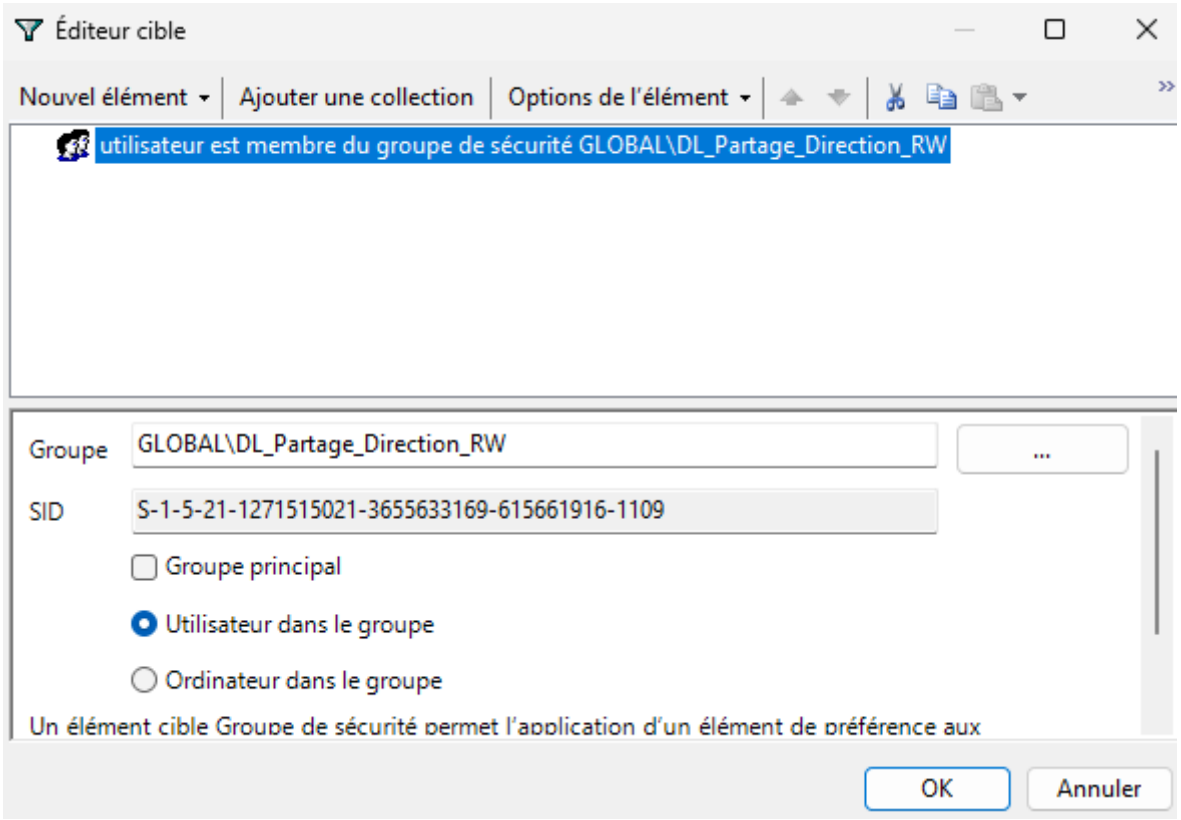
Une seconde GPO, GPO_Lecteurs_Reseau, a été créée pour mapper automatiquement les lecteurs réseau selon le groupe d'appartenance de l'utilisateur.

Le mappage s'effectue depuis Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs.

Lecteur	Chemin UNC	Ciblage (groupe)
D:	\\DC01\Direction	DL_Partage_Direction_RW
E:	\\DC01\Administratif	DL_Partage_Administratif_RW
F:	\\DC01\Commercial	DL_Partage_Commercial_RW
G:	\\DC01\Technique	DL_Partage_Technique_RW
H:	\\DC01\Commun	DL_Partage_Commun_RW

Note : *Pour chaque lecteur, l'onglet Commun > Ciblage au niveau des éléments permet de définir le groupe de sécurité requis. Ainsi, un commercial verra uniquement F: (Commercial) et H: (Commun) ; le compte Direction verra D: et H:, etc.*


Mappages de lecteurs
Processing
N...
O.
Action
Chemin d'accès
Reconnecter
D: 1 Créer \\dc01.global.tp\Direction Non
E: 2 Créer \\dc01.global.tp\Administratif Non
F: 3 Créer \\dc01.global.tp\Commercial Non
G: 4 Créer \\dc01.global.tp\Technique Non
H: 5 Créer \\dc01.global.tp\Commun Non


Éditeur cible
Nouvel élément
Ajouter une collection
Options de l'élément
utilisateur est membre du groupe de sécurité GLOBAL\DL_Partage_Direction_RW
Groupe
GLOBAL\DL_Partage_Direction_RW
...
SID
S-1-5-21-1271515021-3655633169-615661916-1109
Groupe principal
Utilisateur dans le groupe
Ordinateur dans le groupe
Un élément cible Groupe de sécurité permet l'application d'un élément de préférence aux
OK
Annuler

6. Partie 3 — Déploiement du RODC

6.1 Création et configuration de RODC01

La VM RODC01 a été créée sous Windows Server 2025 Core (sans interface graphique), 2 Go de RAM, 40 Go de disque, raccordée au VMnet12 (AGENCE).

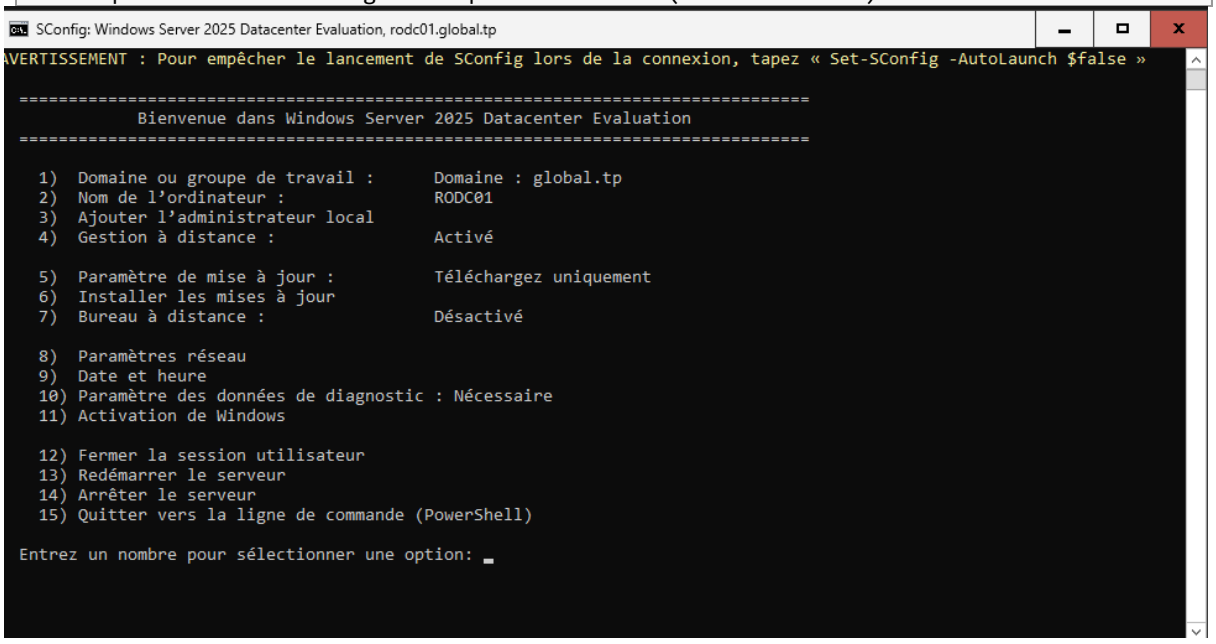
Configuration IP statique

Paramètre	Valeur
Adresse IP	10.0.30.10
Masque	255.255.255.0
Passerelle	10.0.30.3
DNS préféré	10.0.10.10 (DC01)
DNS alternatif	10.0.30.3

> ***Note :*** *Le DNS préféré pointe vers DC01 afin que RODC01 puisse résoudre le domaine global.tp et y être promu. La configuration IP a été appliquée via les paramètres de la carte réseau, et le serveur a été renommé RODC01 avant redémarrage.*

6.2 Jonction au domaine

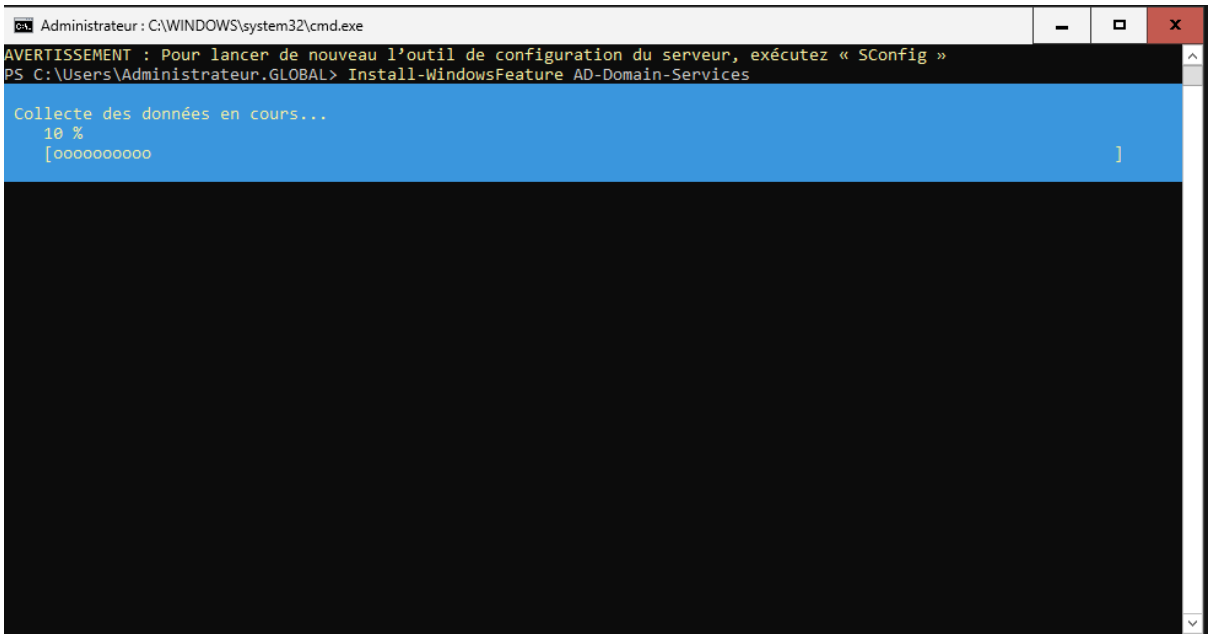
```
Add-Computer -DomainName "global.tp" -Credential (Get-Credential) -Restart
```



6.3 Promotion en RODC

La promotion s'effectue en deux étapes via PowerShell :

```
# Installation du rôle AD DS
Install-WindowsFeature AD-Domain-Services

# Promotion en contrôleur de domaine en lecture seule
Install-ADDSDomainController `
    -DomainName "global.tp" `
    -ReadOnlyReplica:$true `
    -SiteName "Default-First-Site-Name" `
    -InstallDns:$true `
    -Credential (Get-Credential) `
    -Force:$true
```

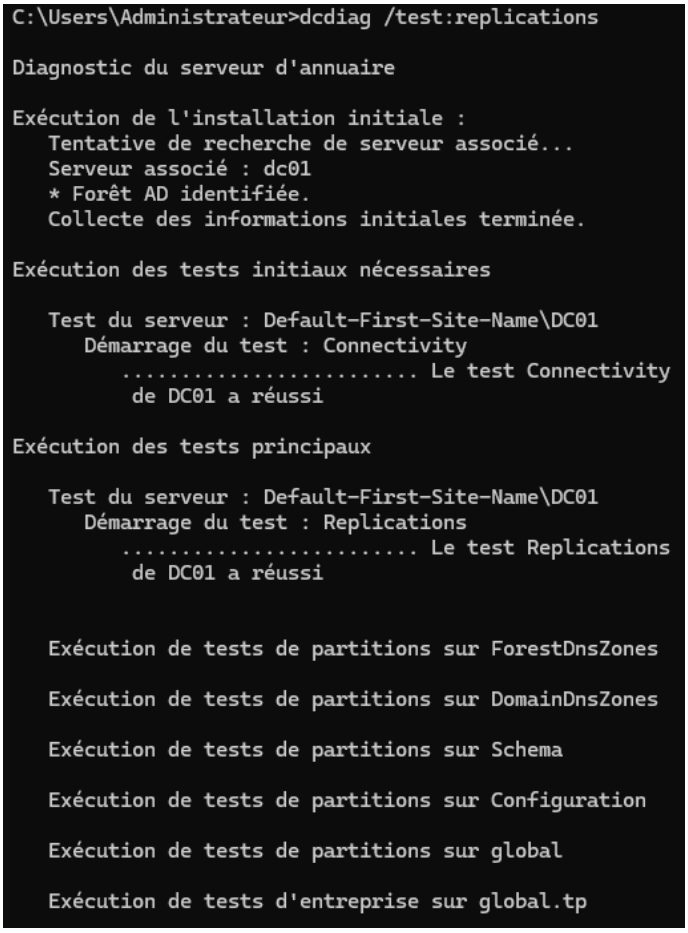


6.4 Vérification de la réplication

Après le redémarrage, la commande repadmin /replsummary a initialement remonté l'erreur (1908). En réalité, le test dcdiag /test:replications confirme que la réplication fonctionne correctement — l'erreur initiale provenait d'un cache obsolète qui se met à jour ensuite.

```
# Test fiable de la réplication
dcdiag /test:replications

# Liste des contrôleurs de domaine
Get-ADDomainController -Filter * | Select-Object Name, IsReadOnly, IPv4Address
```

> ***Note :*** *Lors du diagnostic, le pare-feu Windows a été temporairement désactivé sur RODC01 puis réactivé après vérification : Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True.*



Question 3 — Avantages de sécurité d'un RODC

Le RODC dispose d'une base de données en lecture seule : en cas de compromission (accès physique ou piratage), aucune modification ne peut être propagée vers l'annuaire central, ce qui protège l'intégrité globale de l'Active Directory. De plus, le RODC ne stocke par défaut aucun mot de passe (sauf ceux explicitement autorisés via la Password Replication Policy), ce qui empêche le vol massif d'identifiants critiques en cas de vol du serveur. Enfin, il permet de déléguer l'administration locale du serveur à un utilisateur non-administrateur du domaine.

Le RODC est recommandé dans les sites distants ou agences où la sécurité physique n'est pas garantie (absence de salle serveur sécurisée) et où il n'y a pas de personnel informatique qualifié de confiance sur place.

7. Partie 4 — DMZ et service web conteneurisé

7.1 Création de SRV-WEB

La VM SRV-WEB a été créée sous Ubuntu Server 24.04, 2 Go de RAM, 40 Go de disque, raccordée au VMnet11 (DMZ). L'option « Install OpenSSH server » a été activée durant l'installation.

Configuration réseau (Netplan)

```
# /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    ens33:
      addresses:
        - 10.0.20.10/24
      routes:
        - to: default
          via: 10.0.20.3
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
  version: 2
```

```
sudo netplan apply
```

```
redouane@srv-web:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
fault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
 group default qlen 1000
    link/ether 00:0c:29:2c:83:d8 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.0.20.10/24 brd 10.0.20.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2c:83d8/64 scope link
       valid_lft forever preferred_lft forever
```

7.2 Installation de Docker

```
sudo apt update && sudo apt upgrade -y
sudo apt install ca-certificates curl gnupg -y
sudo install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg \
  | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
echo "deb [arch=$(dpkg --print-architecture) \
signed-by=/etc/apt/keyrings/docker.gpg] \
https://download.docker.com/linux/ubuntu \
$(. /etc/os-release && echo "$VERSION_CODENAME") stable" \
  | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install docker-ce docker-ce-cli containerd.io \
  docker-buildx-plugin docker-compose-plugin -y
sudo systemctl enable --now docker
```

```
redouane@srv-web:~$ docker --version
Docker version 29.4.3, build 055a478
redouane@srv-web:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; prese>
     Active: active (running) since Sun 2026-05-10 18:20:31 UTC; 16s ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 11427 (dockerd)
      Tasks: 9
     Memory: 26.4M (peak: 26.8M)
        CPU: 257ms
     CGroup: /system.slice/docker.service
             └─11427 /usr/bin/dockerd -H fd:// --containerd=/run/containerd>

mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.293156760>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.313462037>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.318791109>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.545565054>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.551549675>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.551786059>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.566538022>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.569933806>
mai 10 18:20:31 srv-web dockerd[11427]: time="2026-05-10T18:20:31.570037405>
mai 10 18:20:31 srv-web systemd[1]: Started docker.service - Docker Applica>
lines 1-22/22 (END)
```

7.3 Déploiement avec Docker Compose

Un dossier de travail ~/site-web a été créé contenant le fichier docker-compose.yml ainsi que les volumes ./html, ./certs et le fichier de configuration ./site.conf.

Fichier docker-compose.yml

```
services:
  web:
    image: nginx:latest
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - ./html:/var/www/html
      - ./site.conf:/etc/nginx/conf.d/default.conf
      - ./certs:/etc/nginx/certs
    depends_on:
      - php
    networks:
      - dmz-net

  php:
    image: php:8.2-fpm
    volumes:
      - ./html:/var/www/html
    networks:
      - dmz-net

networks:
  dmz-net:
    driver: bridge
```

Fichier site.conf (Nginx)

```
server {
    listen 80;
    server_name _;
    root /var/www/html;
    index index.html index.php;

    location ~ \.php$ {
        fastcgi_pass php:9000;
        fastcgi_index index.php;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
}
```

> ***Note :*** *Lors du premier lancement, Docker a créé site.conf comme un dossier (volume monté avant que le fichier n'existe), provoquant un échec du conteneur web. Il a fallu supprimer ce dossier et créer un véritable fichier site.conf avant de relancer docker compose up -d.*

Lancement et vérification

```
sudo docker compose up -d
sudo docker compose ps
```

```
redouane@srv-web:~/site-web$ sudo docker compose ps
NAME            IMAGE          COMMAND                  SERVICE   CREATED              STATUS              PORTS
site-web-php-1   php:8.2-fpm    "docker-php-entrypoi…"   php       About a minute ago   Up About a minute   9000/tcp
site-web-web-1   nginx:latest   "/docker-entrypoint.…"   web       About a minute ago   Up About a minute   0.0.0.0:80->
80/tcp, [::]:80->80/tcp, 0.0.0.0:443->443/tcp, [::]:443->443/tcp
```

7.4 Sécurisation avec UFW

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow from 10.0.10.0/24 to any port 22 proto tcp
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw enable
sudo ufw status
```

```
redouane@srv-web:~/site-web$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       10.0.10.0/24
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
```

Question 4 — Pourquoi un pare-feu local en plus de pfSense ?

Configurer un pare-feu local comme UFW sur le serveur DMZ ajoute une couche de filtrage directement au niveau de l'hôte, en complément du pare-feu périmétrique pfSense. Si un attaquant réussit à contourner ou exploiter une erreur de configuration sur pfSense, UFW peut encore bloquer certains ports ou IP et limiter l'impact de l'intrusion. C'est le principe de la défense en profondeur : multiplier les couches de sécurité pour qu'une faille sur un contrôle ne compromette pas immédiatement tout le système.

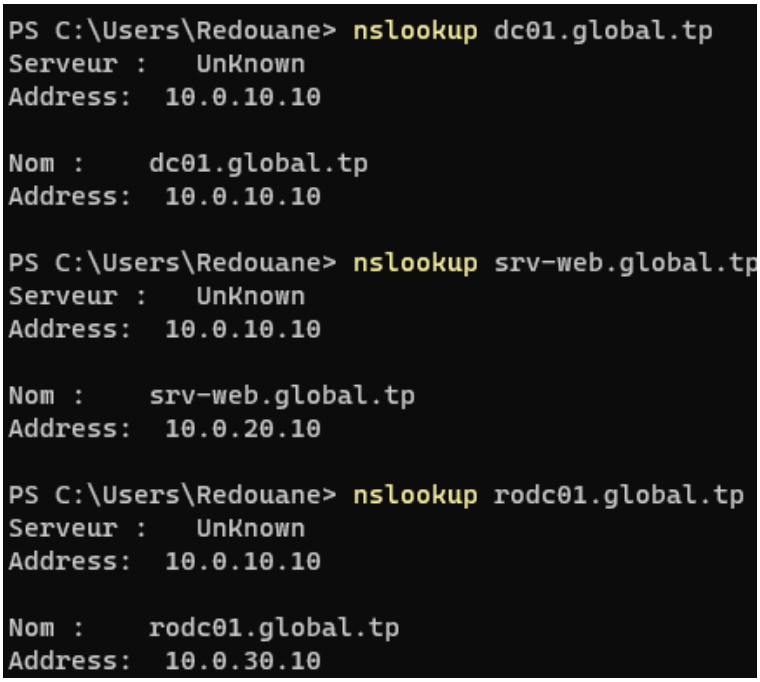
8. Partie 5 — Tests de validation

8.1 Tests de connectivité depuis CLI-LAN

Résolution DNS

```
nslookup dc01.global.tp        → 10.0.10.10
nslookup rodc01.global.tp      → 10.0.30.10
nslookup srv-web.global.tp     → 10.0.20.10
```

> ***Note :*** *L'enregistrement A srv-web a été créé manuellement dans la zone DNS global.tp sur DC01, car aucun enregistrement n'est généré automatiquement pour les machines hors-domaine (Linux).*

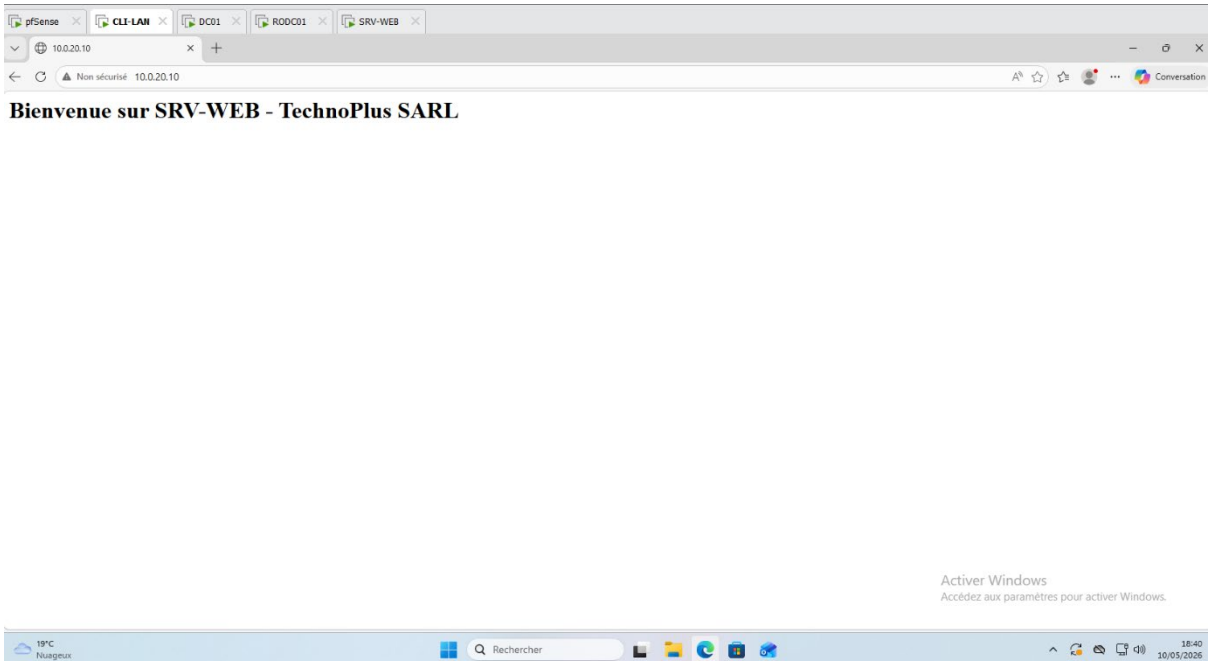


Tests de ping

```
ping 10.0.10.10    # DC01 - OK
ping 10.0.20.10    # SRV-WEB - bloqué par UFW (ICMP non autorisé)
ping 10.0.30.10    # RODC01 - dépend du pare-feu Windows
```

Accès HTTP

```
Invoke-WebRequest -Uri http://10.0.20.10 -UseBasicParsing
# ou depuis cmd.exe :
curl -k http://10.0.20.10
```



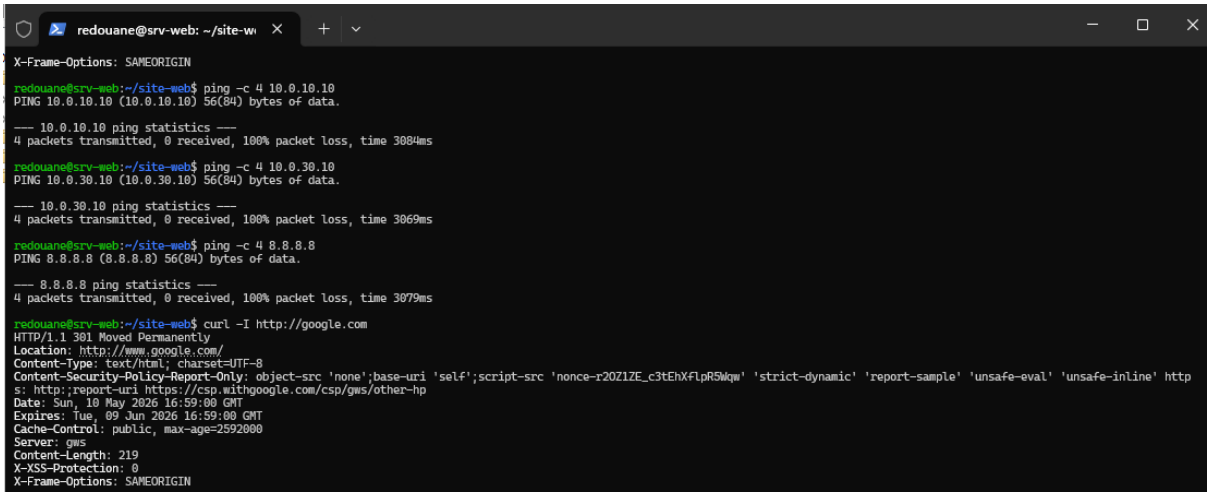
8.2 Tests de sécurité depuis SRV-WEB (DMZ)

```
ping -c 4 10.0.10.10    # ÉCHEC attendu (bloqué par pfSense)
ping -c 4 10.0.30.10    # ÉCHEC attendu (bloqué par pfSense)
curl -I http://google.com  # OK (Internet sortant autorisé)
```

Résultats observés

Test	Résultat	Attendu
DMZ → LAN (ping)	100% packet loss	Bloqué
DMZ → AGENCE (ping)	100% packet loss	Bloqué
DMZ → Internet (HTTP)	200 OK	Autorisé

Note : *Le ping vers Internet ne fonctionne pas car ufw default allow outgoing s'applique au TCP/UDP mais pas à l'ICMP. La validation se fait donc avec curl -I.*



8.3 Vérification Active Directory

```
repadmin /replsummary
dcdiag /test:replications
dcdiag /test:sysvolcheck
Get-ADDomainController -Filter *
Get-ADUser -Filter * | Measure-Object   # ≈ 20 utilisateurs
gpresult /r
```

```
PS C:\Users\Administrateur> Get-ADDomainController -Filter *


ComputerObjectDN           : CN=DC01,OU=Domain Controllers,DC=global,DC=tp
DefaultPartition           : DC=global,DC=tp
Domain                     : global.tp
Enabled                    : True
Forest                     : global.tp
HostName                   : dc01.global.tp
InvocationId               : 69455535-3c9c-488d-aa16-e0742199f40b
IPv4Address                : 10.0.10.10
IPv6Address                :
IsGlobalCatalog            : True
IsReadOnly                 : False
LdapPort                   : 389
Name                       : DC01
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,D
                             C=global,DC=tp
OperatingSystem            : Windows Server 2025 Datacenter Evaluation
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 10.0 (26100)
OperationMasterRoles       : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions                 : {DC=ForestDnsZones,DC=global,DC=tp, DC=DomainDnsZones,DC=global,DC=tp,
                             CN=Schema,CN=Configuration,DC=global,DC=tp, CN=Configuration,DC=global,DC=tp...}
ServerObjectDN             : CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=global,DC=tp
ServerObjectGuid           : 903b0ef2-6791-4b9e-9361-41042a94b85b
Site                       : Default-First-Site-Name
SslPort                    : 636

ComputerObjectDN           : CN=RODC01,OU=Domain Controllers,DC=global,DC=tp
DefaultPartition           : DC=global,DC=tp
Domain                     : global.tp
Enabled                    : True
Forest                     : global.tp
HostName                   : rodc01.global.tp
InvocationId               : 00000000-0000-0000-0000-000000000000
IPv4Address                : 10.0.30.10
IPv6Address                :
IsGlobalCatalog            : True
IsReadOnly                 : True
LdapPort                   : 389
Name                       : RODC01
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=RODC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration
                             ,DC=global,DC=tp
OperatingSystem            : Windows Server 2025 Datacenter Evaluation
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 10.0 (26100)
OperationMasterRoles       : {}
Partitions                 : {CN=Schema,CN=Configuration,DC=global,DC=tp, CN=Configuration,DC=global,DC=tp,
                             DC=global,DC=tp}
ServerObjectDN             : CN=RODC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=global,DC=tp
ServerObjectGuid           : 73d2b02b-7cb6-413d-94da-bf13c877c3bc
Site                       : Default-First-Site-Name
SslPort                    : 636
```

9. Difficultés rencontrées et résolutions

9.1 Squid bloque l'accès à la DMZ

Symptôme : depuis CLI-LAN, l'accès à http://10.0.20.10 retournait une erreur Squid « (61) Connection refused ».

Cause : le proxy transparent intercepte toutes les requêtes HTTP du LAN, y compris celles destinées à la DMZ.

Résolution : ajout du sous-réseau 10.0.20.0/24 dans le champ « Bypass Proxy for These Destination IPs » de la configuration Squid.

9.2 site.conf monté comme un dossier par Docker

Symptôme : le conteneur Nginx ne démarrait pas, avec l'erreur « not a directory: Are you trying to mount a directory onto a file ? ».

Cause : Docker monte les volumes au démarrage. Si le fichier source n'existe pas encore, Docker crée un dossier vide à sa place.

Résolution : suppression du dossier site.conf, création du véritable fichier de configuration Nginx, puis relance via docker compose up -d.

9.3 Erreur 1332 lors du New-SmbShare

Symptôme : l'ajout de l'accès SMB au compte « Administrateur » échouait avec « Le mappage entre les noms de compte et les ID de sécurité n'a pas été effectué ».

Cause : sur un serveur en français contrôleur de domaine, le compte Administrateur doit être qualifié par son domaine pour être résolu correctement.

Résolution : remplacer "Administrateur" par "GLOBAL\Administrateur" dans le paramètre -FullAccess.

9.4 Catégories vides dans Common ACL de SquidGuard

Symptôme : après téléchargement de la blacklist Toulouse, la Target Rules List de Common ACL apparaissait vide.

Cause : deux options distinctes doivent être cochées dans General Settings : Enable (active SquidGuard) et Enable Blacklist (rend les blacklists disponibles dans les ACL).

Résolution : cocher les deux options et appliquer la configuration.

9.5 DNS DMZ manquant dans pfSense

Symptôme : l'installation d'Ubuntu Server n'arrivait pas à télécharger les paquets depuis la DMZ.

Cause : la règle DMZ n'autorisait que les ports 80 et 443, mais pas le port 53 (DNS) nécessaire à la résolution de noms.

Résolution : ajout du port 53 à la règle de sortie DMZ.

10. Conclusion

Ce TP m'a permis de mettre en pratique l'ensemble des compétences acquises au cours de ma formation BTS SIO SISR : virtualisation, segmentation réseau via pare-feu, déploiement d'un Active Directory en architecture multi-sites avec RODC, gestion des stratégies de groupe, conteneurisation, et durcissement de serveurs.

La construction progressive de l'infrastructure m'a confronté à plusieurs problèmes techniques concrets (proxy transparent interceptant la DMZ, montage de volume Docker, résolution de comptes domaine en français) dont la résolution a renforcé ma compréhension des interactions entre les différentes couches du système d'information.

L'application du principe de défense en profondeur — pare-feu périmétrique pfSense, règles de filtrage strictes entre zones, pare-feu local UFW sur le serveur DMZ, RODC en lecture seule sur le site distant, GPO de durcissement des postes — illustre la nécessité de superposer plusieurs couches de protection plutôt que de s'appuyer sur un unique mécanisme de sécurité.

Pour aller plus loin, l'infrastructure pourrait évoluer vers une architecture haute disponibilité (cluster CARP de pfSense, second DC writable, Docker Swarm pour SRV-WEB), ainsi qu'une supervision active via Prometheus, Grafana et Loki.