DOCUMENTATION TECHNIQUE

MDS49

SIO2
ROUVREAU Mathis
RAIMBAULT Evan
TOUZEAU Julien

Sommaire

1. Introduction

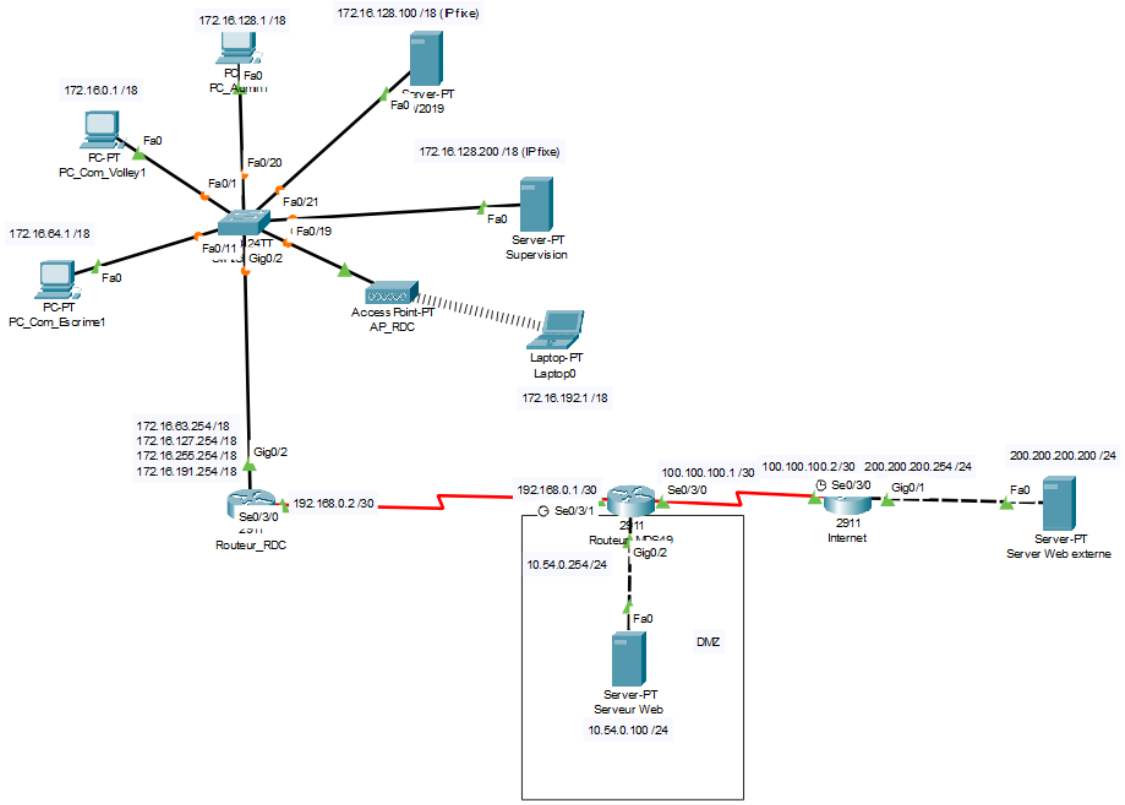
Cette documentation présente l'intégralité de la mise en œuvre du projet PPE3 au sein de la Maison Départementale des Sports 49 (MDS49). Le but du projet est de concevoir une infrastructure réseau sécurisée, segmentée et fonctionnelle conforme au cahier des charges. Toutes les configurations présentes dans ce document proviennent exclusivement des captures réelles et du travail effectué sur l'infrastructure.

2. Contexte et Objectifs

L'infrastructure réseau **MDS49** repose sur une architecture segmentée et sécurisée visant à séparer les flux internes, les zones sensibles et les services exposés.
Le réseau interne est divisé en **quatre sous-réseaux utilisateurs**, chacun représenté par un VLAN correspondant à un comité (Administratif, Volley, Escrime, Partenaires).
Ces VLAN sont transportés via un switch d'accès et un routeur de distribution qui assure le routage inter-VLAN au sein du bâtiment.

Un **contrôleur de domaine Active Directory** sous Windows Server 2019 est responsable de l'authentification et de la centralisation des utilisateurs.
Un **serveur Web interne**, positionné en DMZ, héberge les pages institutionnelles et peut être joint depuis l'extérieur grâce au NAT/PAT réalisé par le routeur MDS49 (routeur central).

La supervision est assurée via un **serveur Zabbix**, permettant de suivre l'état du réseau, des serveurs et équipements actifs.
Enfin, une **borne WiFi** fournit deux SSID : l'un pour les partenaires (VLAN 100), et un second sécurisé par **WPA2-Enterprise via un serveur Radius**, connecté à l'Active Directory.



Arborescence de MDS49.local:

MDS49.local

└── UO_Employés

  ├── Gr_Employés

  ├── UO_Bureaux_Administratifs

  │ ├── Gr_Bureaux_Administratifs / Commun : Commun_Bureaux_Administratifs

  │ │ ├── BODIN Hélène / Perso : Bodinh

  │ │ └── SALAIN Claire / Perso : Salainc

  │

  ├── UO_Comité_Escrime

  │ ├── Gr_Comité_Escrime / Commun : Commun_Comité_Escrime

  │ │ ├── HERVOUET Paul / Perso : Hervouetp

  │ │ └── VERNEUIL Alice / Perso : Verneuila

Voici le lien trello où la méthode Agile a été réalisé :
https://trello.com/invite/b/68dfbbd5fbfa584f19dc53a8/ATTI67643ad9d0d509f1dc56a13924497f181BAC131A/ap3

L'objectif est donc de déployer une maquette complète représentant la future architecture sécurisée de la MDS49, incluant :

- Isolation réseau par VLAN (Volley, Escrime, Administratif, DMZ, Wifi Partenaires)
- Mise en place d'un serveur AD/DHCP/DNS Windows Server 2019
- Routage inter-VLAN + OSPF
- Mise en place d'un serveur web interne + un serveur web externe
- Mise en place d'un NAT/PAT sur le routeur de bordure
- Mise en place d'ACL filtrant les flux entre VLAN
- Supervision Nagios (structure prévue)
- Tests internes et externes

3. Configuration du Routeur RDC

Ce routeur assure le routage interne du bâtiment entre les VLAN et envoie le trafic vers le routeur central.

Des sous-interfaces sont configurées sur **Gig0/0/0**, chacune associée à un VLAN :

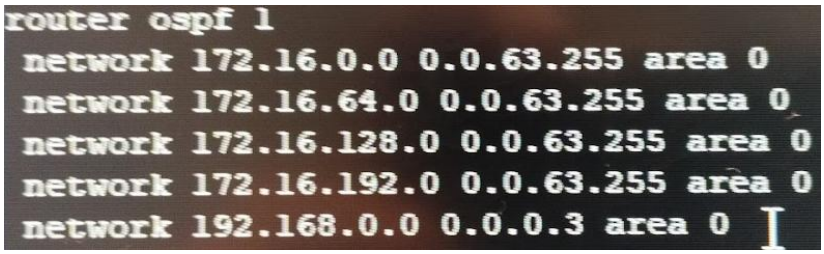
VLAN	Sous-réseau	Passerelle	Interface
10 (Volley)	172.16.0.0/18	172.16.63.254	g0/0/0.10
20 (Escrime)	172.16.64.0/18	172.16.127.254	g0/0/0.20
100 (Partenaires)	172.16.192.0/18	172.16.255.254	g0/0/0.100
30 (Administratif)	172.16.128.0/18	172.16.191.254	g0/0/0.30

```
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 172.16.63.254 255.255.192.0
 ip helper-address 172.16.128.100
 ip access-group 1 out
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 172.16.127.254 255.255.192.0
 ip helper-address 172.16.128.100
 ip access-group 1 out
!
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 172.16.191.254 255.255.192.0
 ip helper-address 172.16.128.100
!
interface GigabitEthernet0/0/0.100
 encapsulation dot1Q 100
 ip address 172.16.255.254 255.255.192.0
 ip helper-address 172.16.128.100
!
interface GigabitEthernet0/0/1
 ip address 192.168.0.2 255.255.255.252
 negotiation auto
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
```

Le routeur RDC prend en charge l'interconnexion des VLAN, les sous-interfaces 802.1Q, le DHCP relay, des ACL de filtrage et des routes statiques.

Un ip-helper est configuré pour chaque sous-réseau ce qui signifie que le DHCP pourra se diffuser sur les autres sous-réseaux en fonction de l'adresse réseau.

Les routes du routeur ont été configurées en OSPF.



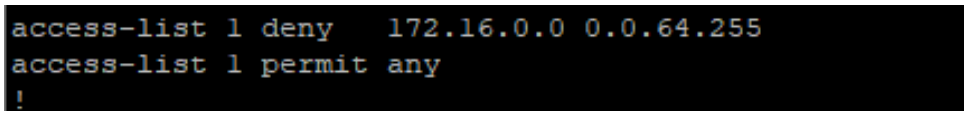
Une ACL standard bloque un comité par rapport à un autre :

access-list 1 deny 172.16.0.0 0.0.64.255

access-list 1 permit any

interface g0/0/1

ip access-group 1 in



4. Routeur MDS49

Il réalise :

- Le routage entre DMZ, entreprise et Internet.
- Le NAT/PAT
- Les ACL standards et étendue

Interfaces du routeur MDS49 :

Interface	Adresse	Fonction
g0/0/1	192.168.0.1/30	Vers Routeur_RDC
g0/0/0	10.54.0.254/24	DMZ
s0/1/0	100.100.100.1/30	Vers Internet

```
interface GigabitEthernet0/0/0
 ip address 10.54.0.254 255.255.255.0
 ip nat inside
 negotiation auto
!
interface GigabitEthernet0/0/1
 ip address 192.168.0.1 255.255.255.252
 ip nat inside
 negotiation auto
!
interface Serial0/1/0
 ip address 100.100.100.1 255.255.255.252
 ip nat outside
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
ip nat pool POOL_MDS49 8.8.8.2 8.8.8.4 netmask 255.255.255.240
ip nat inside source static tcp 10.54.0.100 80 8.8.8.1 80 extendable
ip nat inside source list 1 pool POOL_MDS49 overload
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
```

De plus, cette ligne a été ajouté dans l'interface GigabitEthernet0/0/0 : *ip access-group WEB in*

Des routes ont été configurés en OSPF sur le routeur.

```
router ospf 1
 network 10.54.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.3 area 0
```

Et enfin plusieurs ACL ont été faites :

- 2 ACL standard ayant pour but d'autoriser les sous-réseaux et le serveur web (10.54.0.100) a accéder au serveur web externe. Ces ACL sont en lien avec le NAT/PAT

```
access-list 1 permit 172.16.0.0 0.0.255.255
access-list 2 permit 10.54.0.0 0.0.0.255
```

- 1 ACL étendue permettant à tous les hôtes (internes ou externes) d'accéder seulement au service HTTP du serveur interne (10.54.0.100)

5.

```
ip access-list extended WEB
 permit tcp any host 10.54.0.100 eq www
 permit tcp host 10.54.0.100 any established
 deny   ip any any
```

Le switch va être utilisé pour interconnecter les différents postes et serveurs mais avec des VLANs différents :

- VLAN 10 — Volley
- VLAN 20 — Escrime
- VLAN 30 — Administratif
- VLAN 100 — Partenaires

Un port Trunk a été configuré sur le port GigabitEthernet 1/0/24

```
interface GigabitEthernet1/0/1 à 1/0/7
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/8 à 1/0/14
 switchport access vlan 20
```

```
 switchport mode access
!
interface GigabitEthernet1/0/15 à 1/0/21
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/22
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet1/0/24
 switchport mode trunk
```

6. Serveur Windows 2019 – AD / DHCP / DNS

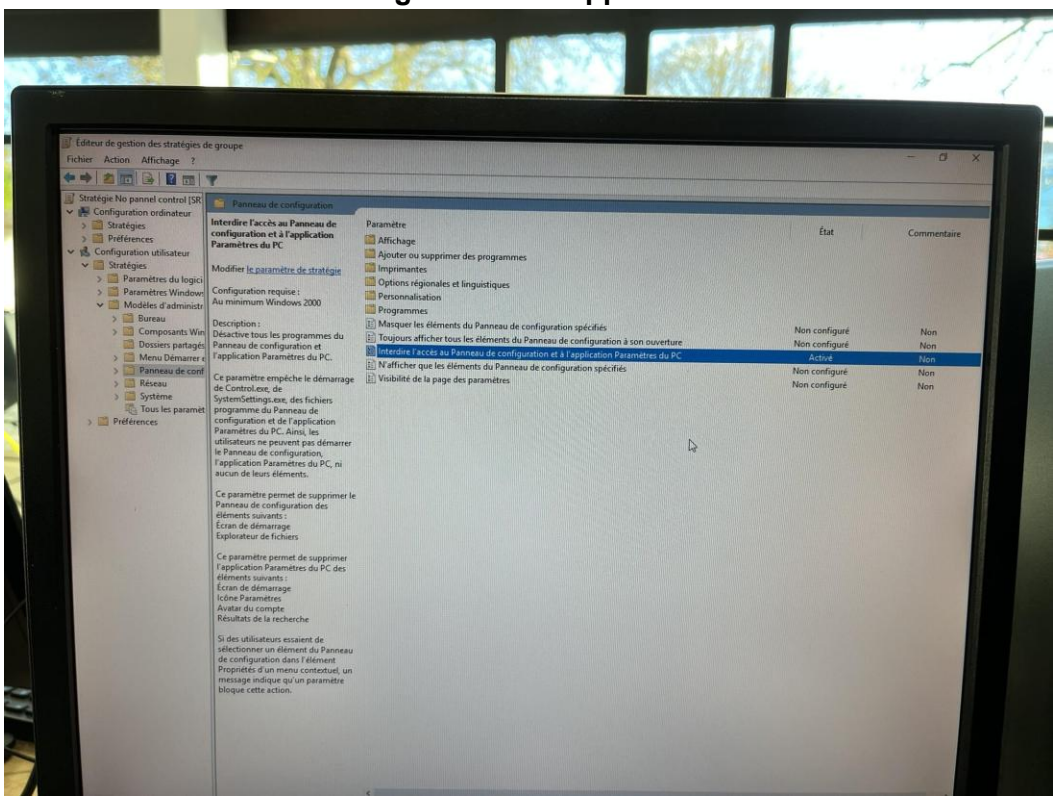
L'Active Directory repose sur le domaine **MDS49.local**, créé lors de l'installation de Windows Server 2019.
Afin d'organiser les utilisateurs, plusieurs **Unités d'Organisation (OU)** ont été définies : Bureaux_Administratifs, Comité_Volley, Comité_Escrime et Partenaires.
Chaque OU contient un groupe de sécurité associé (GR_Bureaux_Administratifs, GR_Comité_Volley, GR_Comité_Escrime, GR_Partenaires).

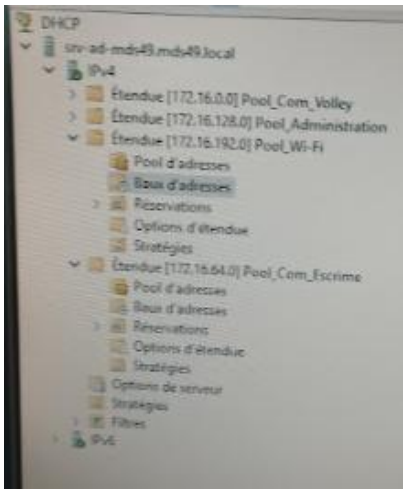
Les utilisateurs sont créés selon la nomenclature **nom+premierelettreduprénom (ex : challain)** permettant cohérence et gestion simplifiée.

De plus, chaque utilisateur a un répertoire personnel de créé et un répertoire commun en fonction de leur groupe. Seuls les responsables peuvent écrire dans leur répertoire commun c'est-à-dire que les autres employés ont que le droit de lecture.

Une GPO a été créée pour interdire l'accès au panneau de configuration aux utilisateurs. Ce paramètre se situe dans **Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration** et se nomme "**Interdire**

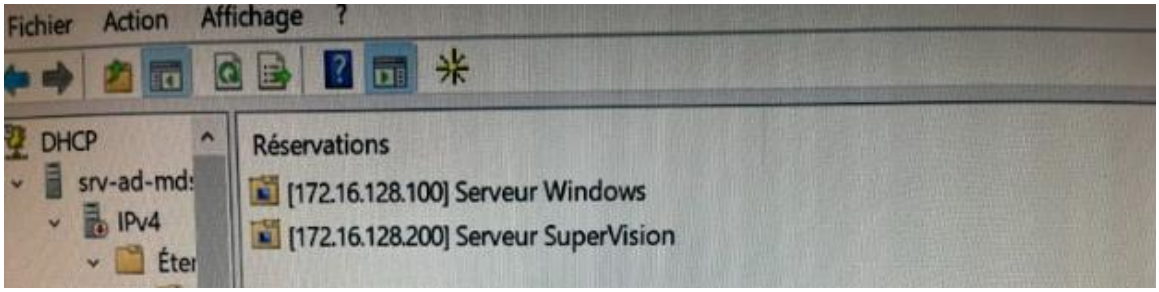
l'accès au Panneau de configuration et l'application Paramètres du PC".





Le rôle **DHCP** est activé sur le serveur AD afin de fournir automatiquement les adresses IP aux clients.

2 réservation ont été faites pour le serveur de supervision Zabbix et pour le serveur Windows.



Comme le DHCP ne se trouve pas sur le même réseau que tous les VLAN, un **DHCP Relay (IP Helper address)** est configuré sur le routeur RDC.

Le rôle **DNS** est installé automatiquement, fournissant les services de résolution internes au domaine.

7. Serveur Web Debian – Apache2

Un serveur Debian héberge le site Web interne.
Il est placé dans la **DMZ 10.54.0.0/24**, à l'adresse :

- Serveur Web : **10.54.0.100**
- Passerelle DMZ : **10.54.0.254**

Apache2 est installé et configuré pour exposer le site web interne via la commande :

Apt install apache2 -y

Le routeur MDS49 réalise un **NAT/PAT** de l'adresse publique 8.8.8.1:80 vers l'adresse privée 10.54.0.100:80, permettant un accès externe sécurisé et contrôlé.

8. Serveur Zabbix

Le serveur Zabbix supervise :

- le serveur AD
- le serveur web (DMZ)
- les routeurs
- le switch

Pour le serveur AD et le serveur Web interne, Zabbix agent est installé.

Pour les routeurs des commandes ont été ajouté sur chaque routeur pour permettre au Zabbix de connaître l'état de ces appareills via le SNMP :

```
snmp-server community cisco RO
snmp-server location labo
snmp-server contact random@sio.fr
snmp-server host 172.16.128.200 version 2c cisco
!
```

Pour le switch, c'est la même chose que les routeurs sauf qu'on remplace RO par SW :

```
snmp-server community cisco RO SW
snmp-server location labo
snmp-server contact random@sio.fr
snmp-server host 172.16.128.200 version 2c cisco
```

9. Borne WiFi

Une borne WiFi Cisco a été configuré dans le VLAN 100 avec le SSID **accesspoint**

Son nom est **cisco** et a l'adresse IP **172.16.255.253**

```
WLAN ID  WLAN Profile Name / SSID                                  Status    Interface Name
-------  -----------------------------------                     --------  --------------------
1        AccessPoint / AccessPoint                                Enabled   management
```

Une configuration pour le radius a été commencée.

```
Idx  Type  Server Address     Port    State     Tout  MgmtTout  RFC3576  IPSec -
state/Profile Name/RadiusRegionString
---  ----  ----------------  ------  --------  ----  --------  -------  --------
-----------------------------------------------
3    NM    172.16.128.100    1812    Enabled   5     5         Disabled  Disable
d - /none
```

10. Serveur Radius

Le serveur Radius (FreeRadius) est installé sous Debian.
Il est intégré à l'Active Directory grâce à **Winbind**.

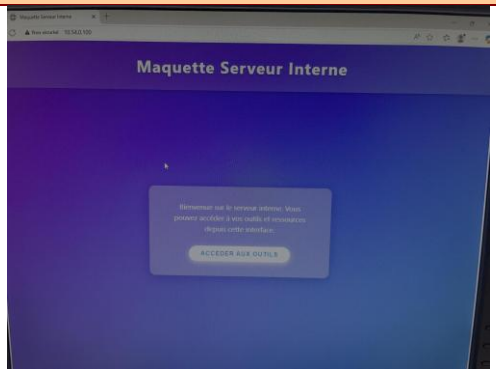
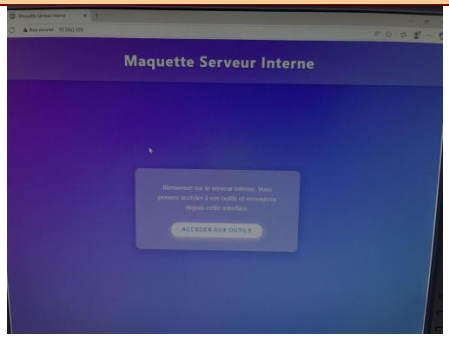
- Authentification 802.1X
- Contrôle d'accès dynamique via AD

11. Tests Réalisés

11.1. Plan de test site web externe

Historique des révisions

Version	Date	Modification	Auteur
1.0	24/11/2025	RAS	Raimbault Evan

Test Fonctionnel : [CT-FUNC] Test d'installation de l'application				
Objectif : Afficher une page web à travers un navigateur internet				
Eléments à tester : Serveur Web				
Pré requis : Une station sous debian12 avec apache2 et une station cliente sous Windows. Les deux stations ne sont pas sur le même réseau mais communiquent entre elles.				
Initialisation : Les deux postes sont sous tension et le serveur web démarré. Sur le client, un navigateur est ouvert.				
Scénario :				
Id	**Démarche**	**Résultats attendus**	**Résultats obtenus**	**OK / NOK**
1	Sur le client, dans le navigateur internet, tapez **10.54.0.100** dans la barre de navigation.			OK

Total	100 /100%
Seuil de conformité	100 %
Rapport de test ❑ **Testé par :Julien**	**Le :24/11/2025**
Commentaire :	
Approbation :	
Fiches d'anomalies émises :	

11.2. Plan de test site web interne

Historique des révisions

Version	Date	Modification	Auteur
1.0	24/11/2025	RAS	ROUVREAU Mathis

Test Fonctionnel : [CT-FUNC] Test d'installation de l'application

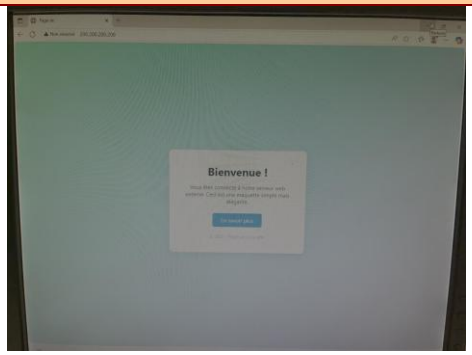
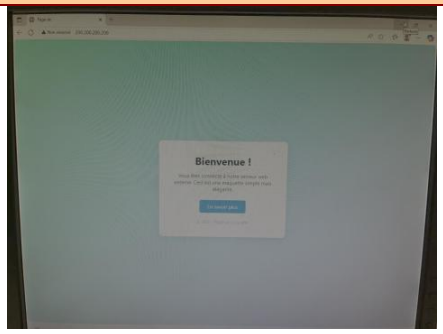
Objectif : Afficher une page web à travers un navigateur internet

Eléments à tester : Serveur Web externe

Pré requis : Une station sous debian12 avec apache2 et une station cliente sous Windows. Les deux stations ne sont pas sur le même réseau mais communiquent entre elles.

Initialisation : Les deux postes sont sous tension et le serveur web démarré. Sur le client, un navigateur est ouvert.

Scénario :

Id	Démarche	Résultats attendus	Résultats obtenus	OK / NOK
1	Sur le client, dans le navigateur internet, tapez **200.200.200.200** dans la barre de navigation.			OK

Total 100 /100%

Seuil de conformité 100 %

Rapport de test ❑ **Testé par :Evan** **Le :24/11/2025**

Commentaire :

Approbation :
Fiches d'anomalies émises :

11.3. Plan de test DHCP

Historique des révisions

Version	Date	Modification	Auteur
1.0	24/11/2025	RAS	ROUVREAU Mathis

Test Fonctionnel : [CT-FUNC] Test d'installation de l'application

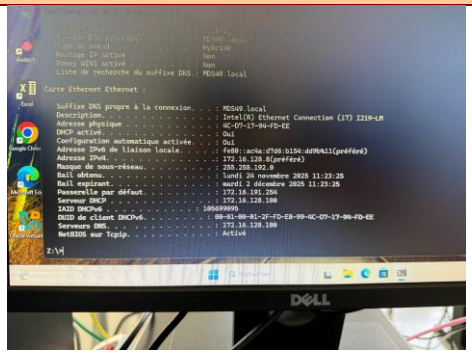
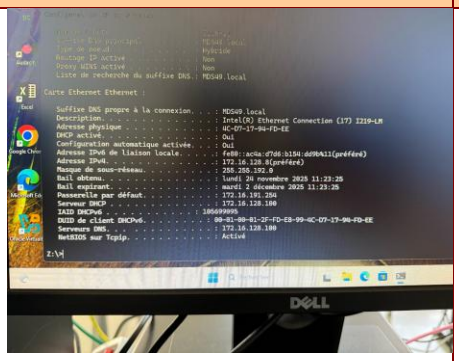
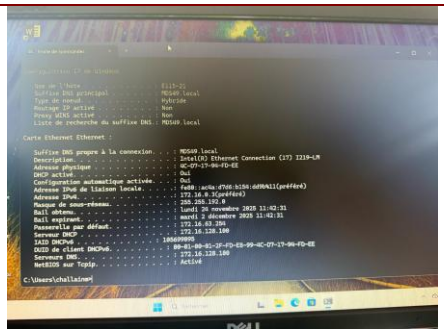
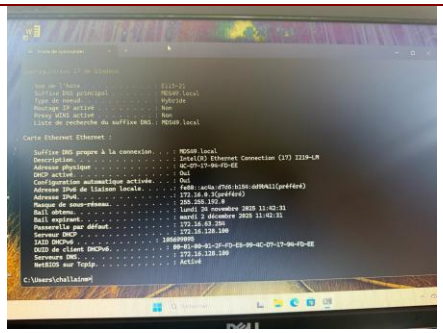
Objectif : Tester la distribution d'adresses

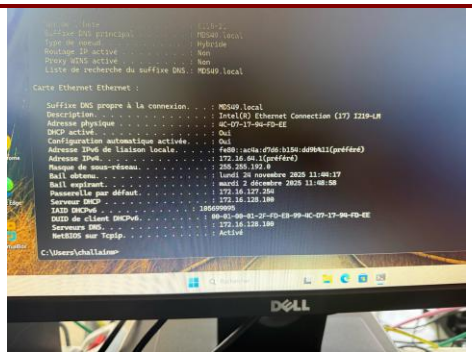
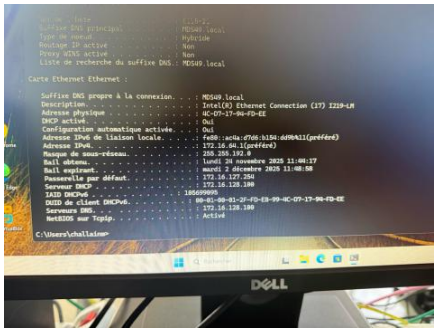
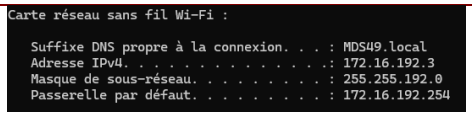
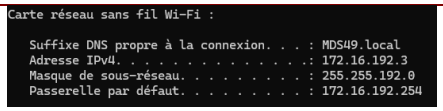
Eléments à tester : DHCP

Pré requis : Un serveur DHCP allumé une machine cliente sous Windows 11

Initialisation :le serveur DHCP est allumé et le client Windows 11. Le client est en configuration dynamique.

Scénario :

Id	Démarche	Résultats attendus	Résultats obtenus	OK / NOK
1	Sur la machine Windows branché sur le Vlan Administration le cmd est ouvert et l'utilisateur tape la commande ipconfig /all			OK
2	Sur la machine Windows branché sur le Vlan Volley le cmd est ouvert et l'utilisateur tape la commande ipconfig /all			

3	Sur la machine Windows branché sur le Vlan Escrime le cmd est ouvert et l'utilisateur tape la commande ipconfig /all			
4	Sur la machine Windows branché sur le Vlan Wifi le cmd est ouvert et l'utilisateur tape la commande ipconfig /all			

Total	100 /100%
Seuil de conformité	100 %

Rapport de test ❑ **Testé par :Julien** **Le :24/11/2025**

Commentaire :

Approbation :

Fiches d'anomalies émises :

11.4. Plan de test NAT/PAT

Historique des révisions

Version	Date	Modification	Auteur
1.0	24/11/2025	RAS	TOUZEAU Julien

Test Fonctionnel : [CT-FUNC] Test d'installation de l'application

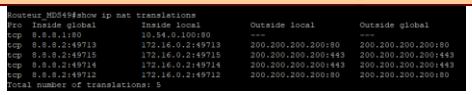
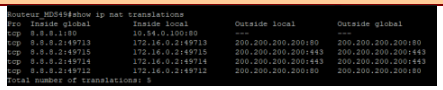
Objectif : Translater les adresses IP

Eléments à tester : NAT/PAT

Pré requis : Un routeur Cisco (Routeur_MDS49) allumé, une machine Windows contenant le logiciel PuTTY

Initialisation : Une connexion en SSH a été créée entre la machine Windows et le routeur au niveau 1 c'est à dire en tant qu'utilisateur, une machine a précédemment accéder au serveur web externe.

Scénario :

Id	Démarche	Résultats attendus	Résultats obtenus	OK / NOK
1	Sur la machine Windows, dans la fenêtre PuTTY tapez la commande show ip nat translations			OK

Routeur_MDS49#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 8.8.8.1:80 10.54.0.100:80 --- ---
tcp 8.8.8.2:49713 172.16.0.2:49713 200.200.200.200:80 200.200.200.200:80
tcp 8.8.8.2:49715 172.16.0.2:49715 200.200.200.200:443 200.200.200.200:443
tcp 8.8.8.2:49714 172.16.0.2:49714 200.200.200.200:443 200.200.200.200:443
tcp 8.8.8.2:49712 172.16.0.2:49712 200.200.200.200:80 200.200.200.200:80
Total number of translations: 5

Total 100 /100%

Seuil de conformité 100 %

Rapport de test ❑ **Testé par :Mathis** **Le :24/11/2025**

Commentaire :

Approbation :

Fiches d'anomalies émises :

11.5. Plan de test VLAN (avec un autre truc pour les comités qui fonctionnent pas)

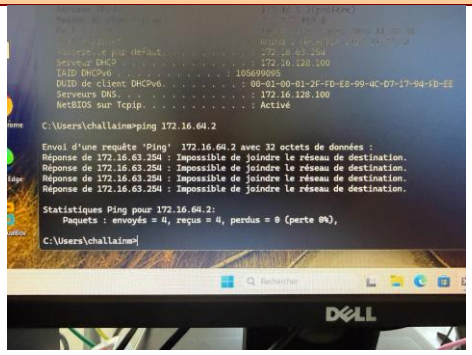
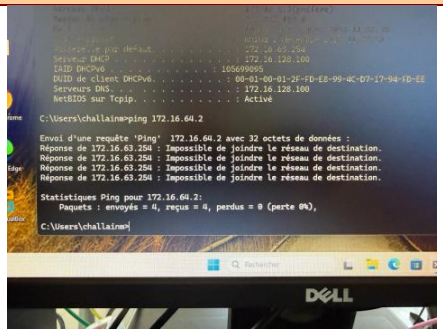
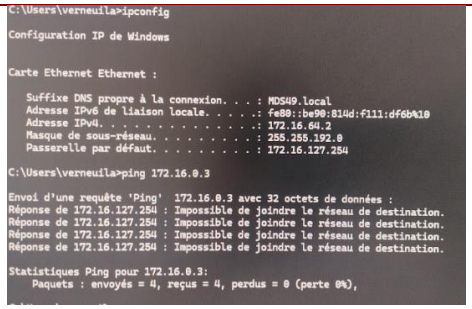
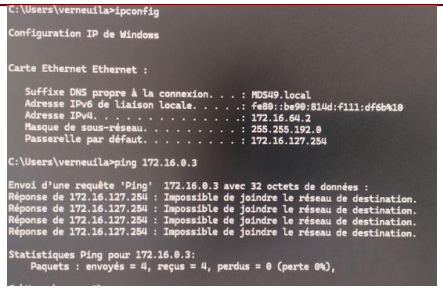
Test Fonctionnel : [CT-FUNC] Test d'installation de l'application
Objectif : Tester la non communication inter-vlan

Eléments à tester : communication inter-vlan

Pré requis : deux poste client sous windows 11

Initialisation : les deux poste sont connectés sur des vlans différent les deux postes on le cmd d'ouvert le poste du vlan Volley à l'adresse 172.16.0.3 et le poste du vlan Escrime à l'adresse 172.16.64.2

Scénario :

Id	Démarche	Résultats attendus	Résultats obtenus	OK / NOK
1	Le poste du vlan Volley tape la commande ping 172.16.64.2			OK
2	Le poste du vlan escrime tape la commande ping 172.16.64.2			OK

Total	100 /100%
Seuil de conformité	100 %

Rapport de test ❑ **Testé par :Mathis** **Le :24/11/2025**

Commentaire :
Approbation :
Fiches d'anomalies émises :

12. Captures d'Écran

```
Routeur_MDS49#show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  8.8.8.1:80            10.54.0.100:80        ---                   ---
tcp  8.8.8.2:49713         172.16.0.2:49713      200.200.200.200:80    200.200.200.200:80
tcp  8.8.8.2:49715         172.16.0.2:49715      200.200.200.200:443   200.200.200.200:443
tcp  8.8.8.2:49714         172.16.0.2:49714      200.200.200.200:443   200.200.200.200:443
tcp  8.8.8.2:49712         172.16.0.2:49712      200.200.200.200:80    200.200.200.200:80
Total number of translations: 5
```

Figure : Capture_routeur_MDS49_NAT_PAT.png

```
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 20
 switchport mode access
!
```

Figure : Capture_switch_part1.png

```
interface GigabitEthernet1/0/16
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/19
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/20
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/21
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/22
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
 switchport mode trunk
!
```

Figure : Capture_switch_part2.png

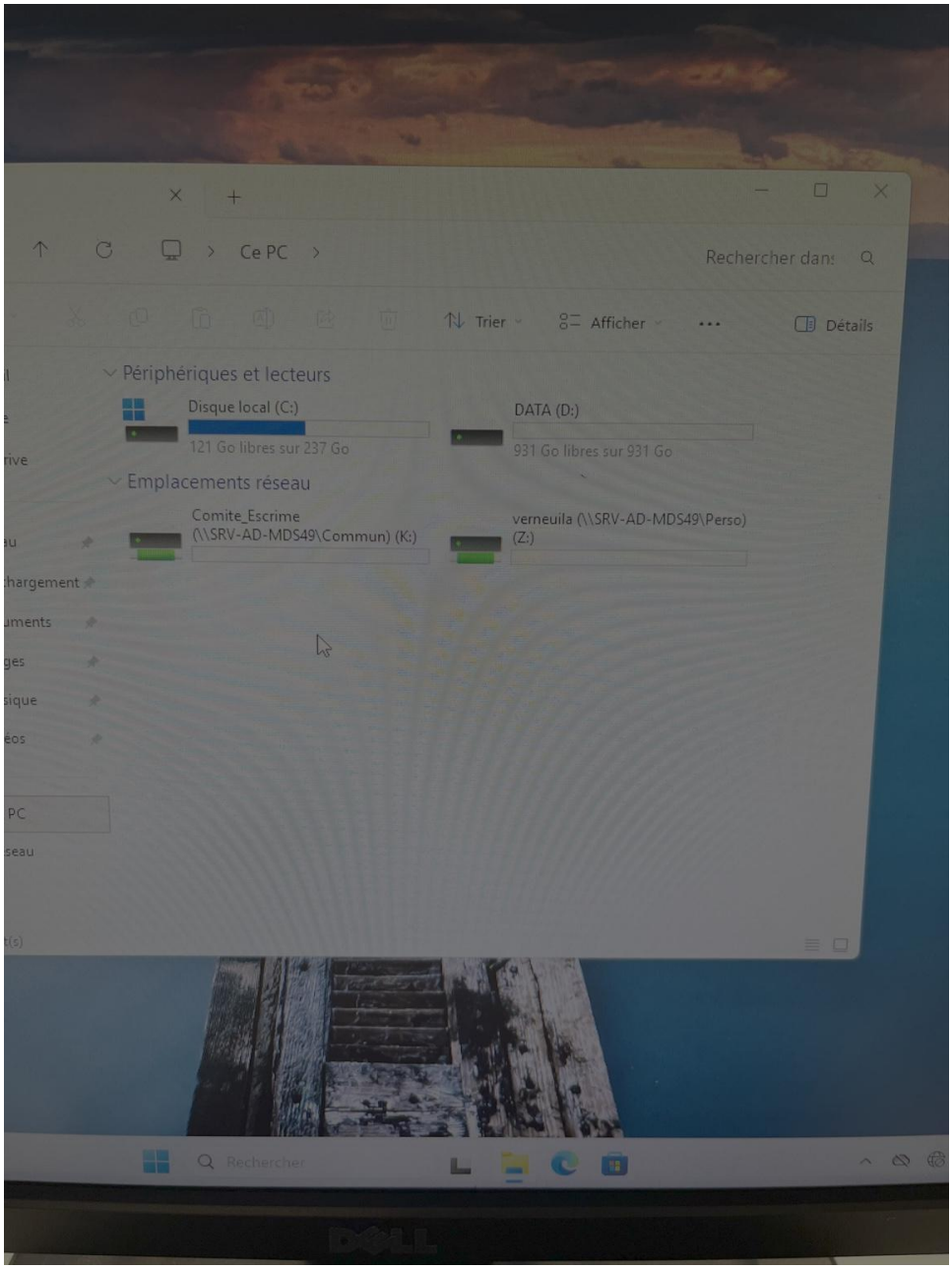


Figure : IMG_2584.jpeg

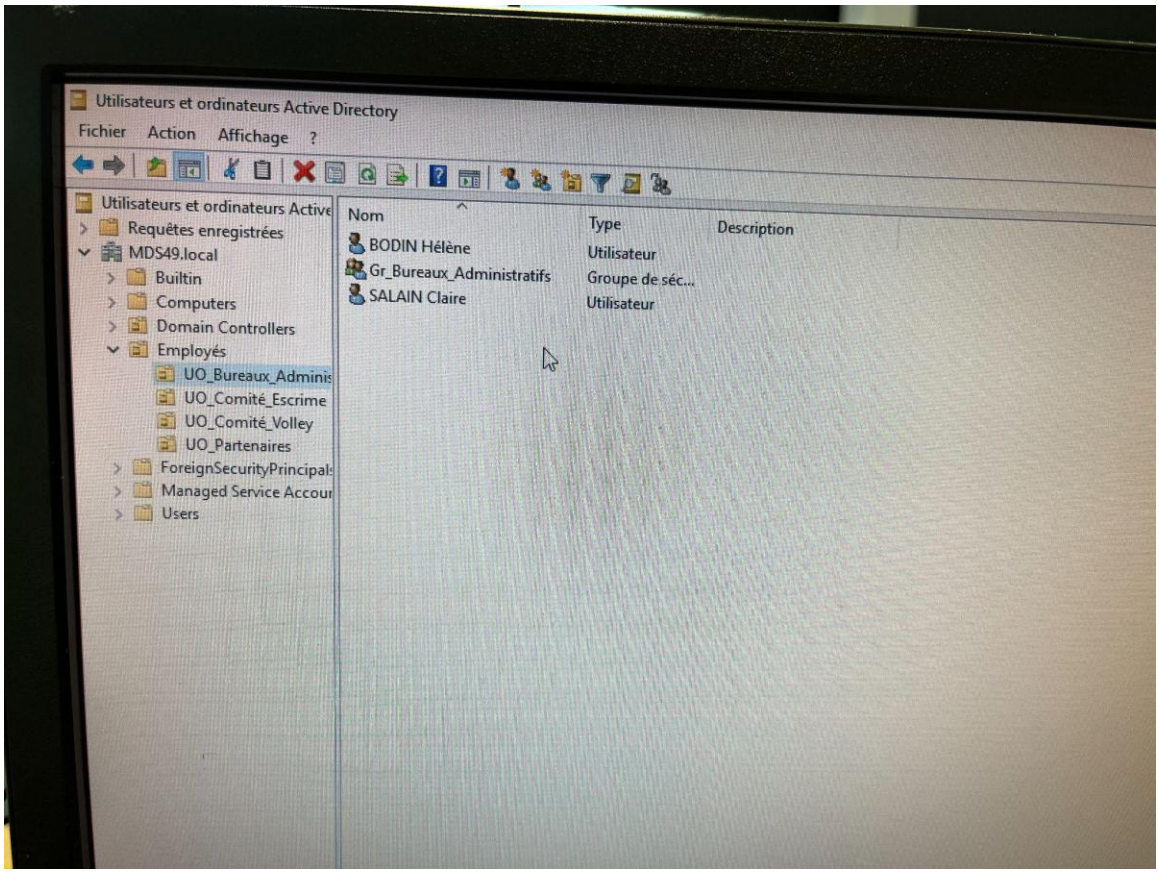


Figure : UO_Bureaux_Administratifs.jpeg

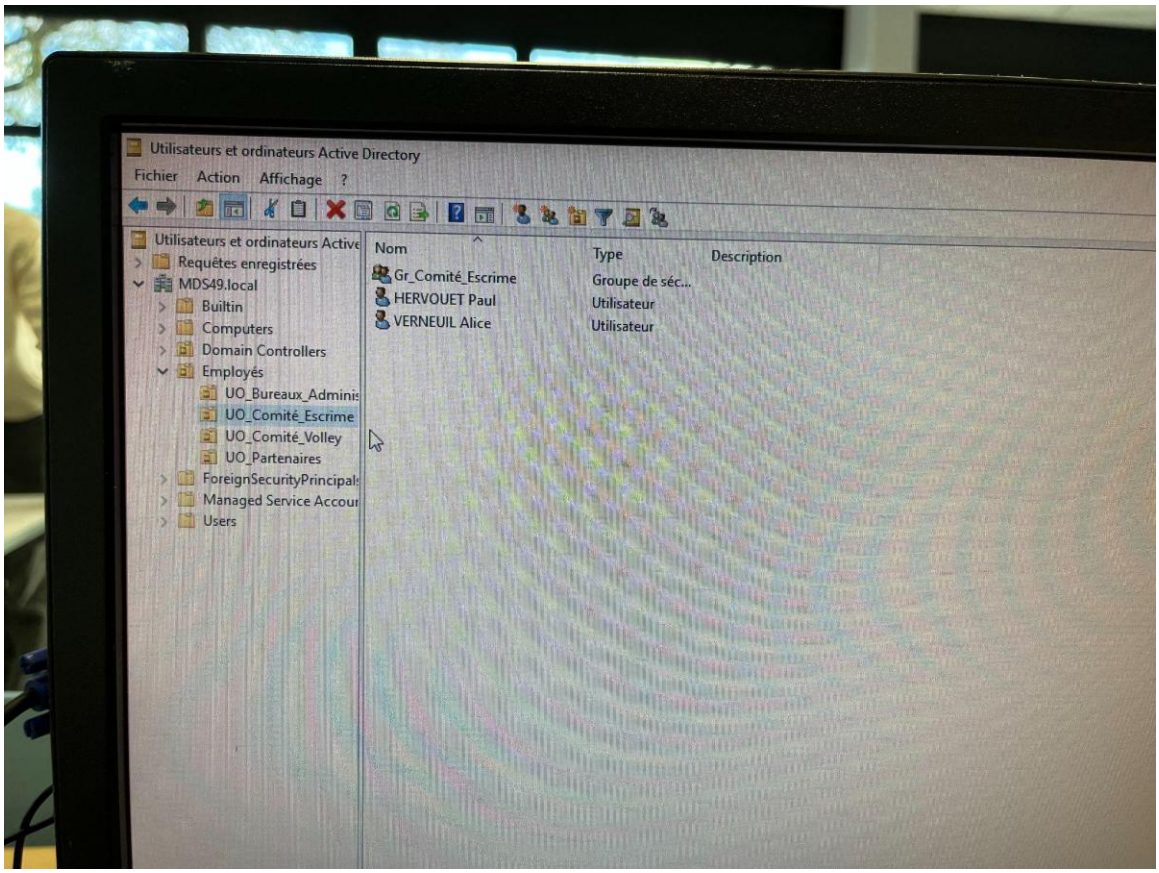


Figure : UO_Comité_Escrime.jpeg

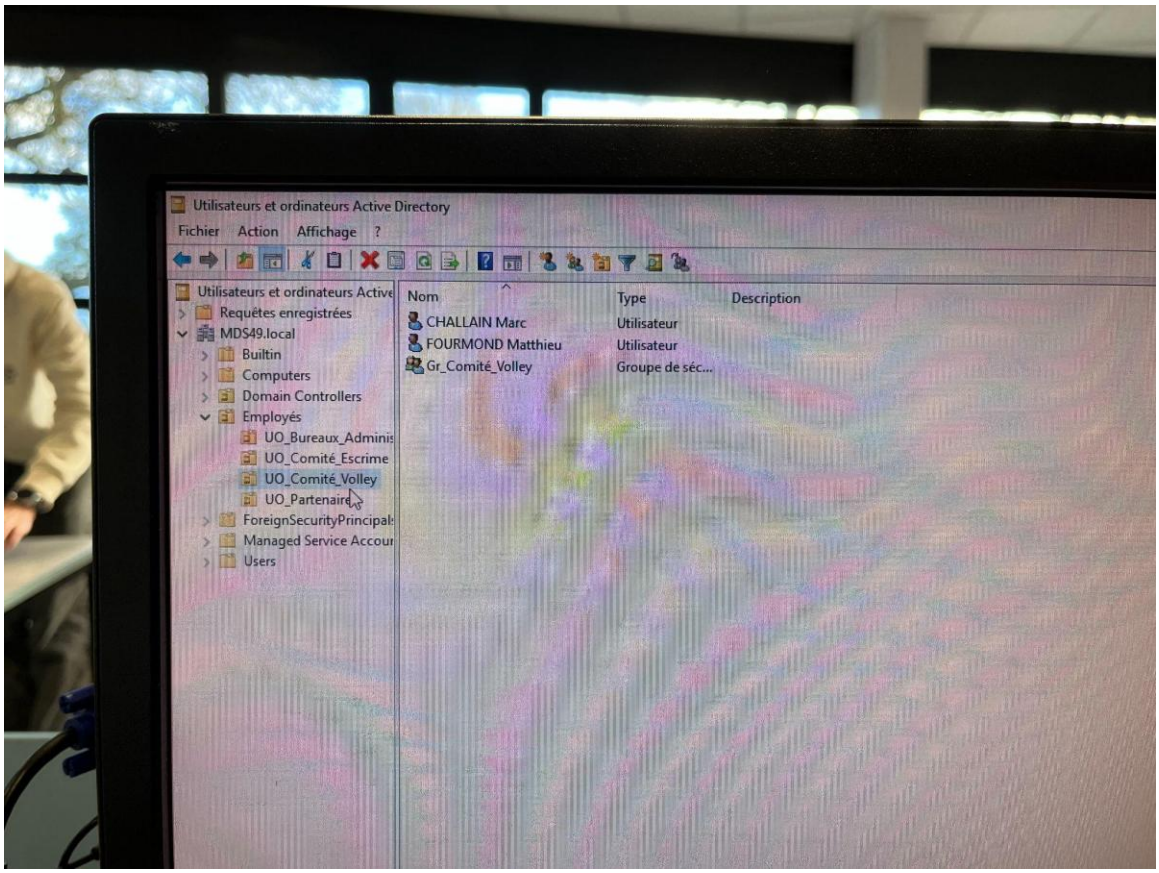


Figure : UO_Comité_Volley.jpeg

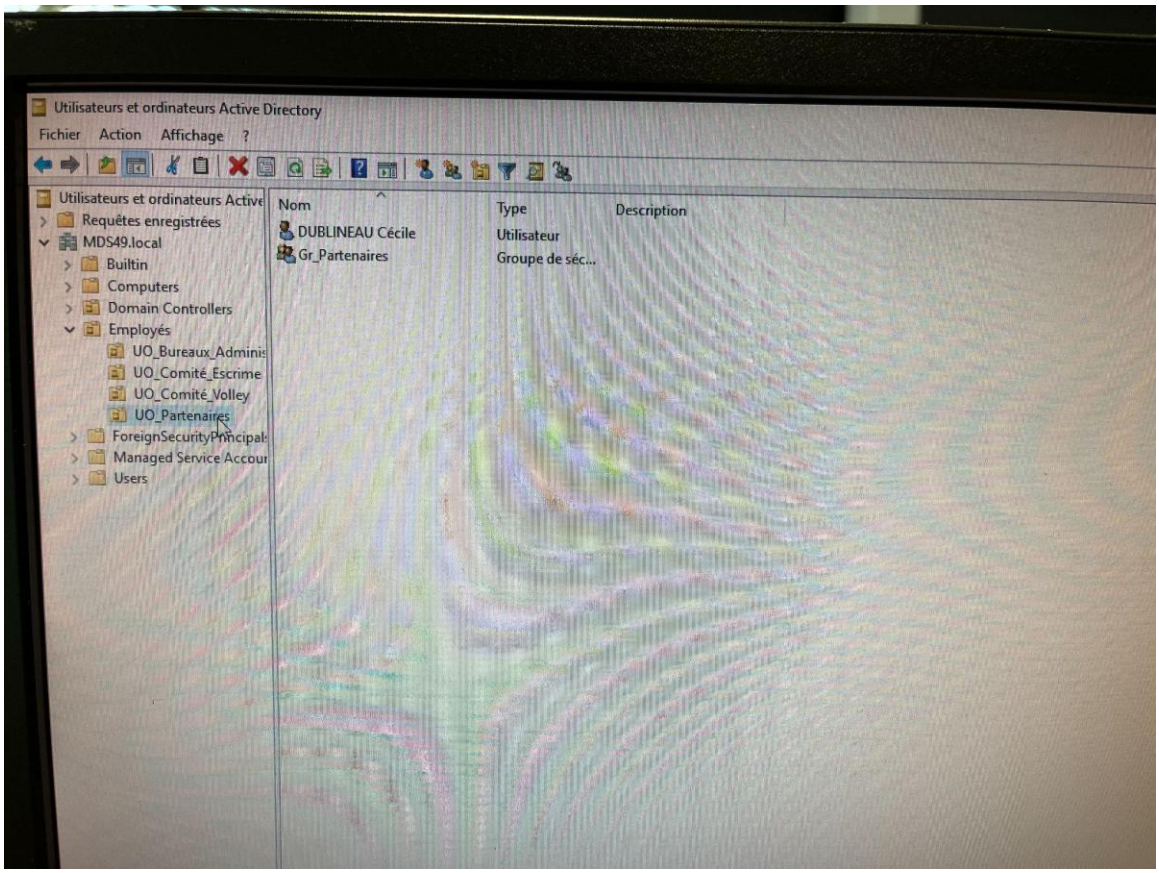


Figure : UO_Partenaire.jpeg