IUT SORBONNE NORD

SAE21 – Construire un Réseau

Mr M'Lik

VAN NGOC Sean

Lepabic Ronan

Grugeard Gabin

Contrevilliers Aymeric

2024-2025

Table des matières

Introduction

Dans le cadre du projet SAE21 – Construire un réseau, nous avons été missionnés par l'entreprise GreenHome Solutions pour concevoir et déployer une infrastructure réseau complète, sécurisée, interconnectée et fonctionnelle entre ses deux sites : Lyon (le siège administratif) et Grenoble (l'unité de production).

Le projet s'est déroulé sur une période de 10 jours, avec une équipe organisée autour de cinq rôles techniques bien définis : chef de projet, architecte réseau, administrateur systèmes, technicien sécurité et testeur qualité.

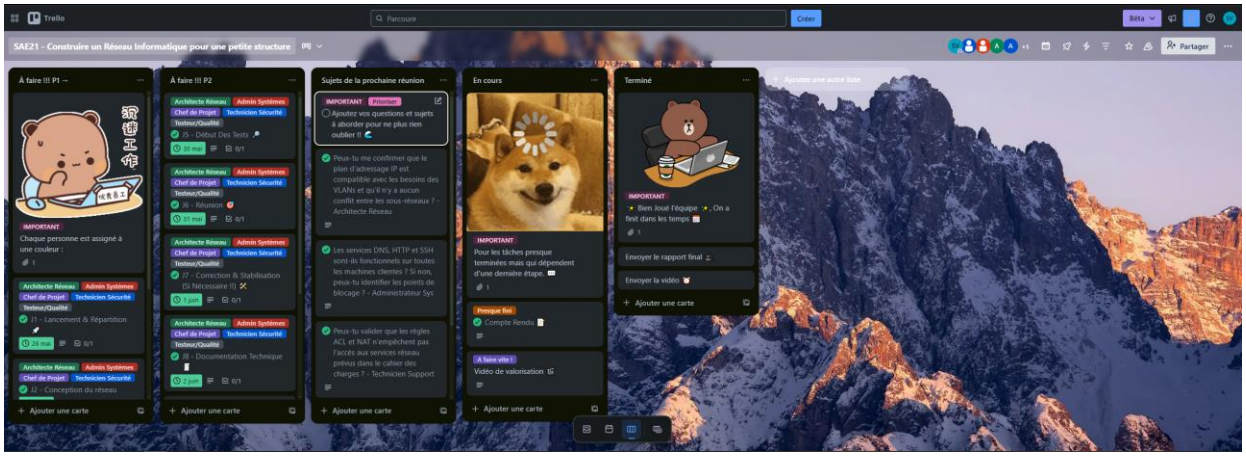
L'objectif était de concevoir un réseau structuré autour de VLANs, d'assurer le routage inter-VLAN, de déployer les services essentiels (DNS, DHCP, Active Directory, HTTP), d'assurer la sécurité réseau avec pare-feu et filtrage, puis de valider le fonctionnement global via des tests de connectivité. Ce rapport présente les contributions de chaque membre, les choix techniques réalisés, ainsi que les résultats obtenus.

1) Travail réalisé – Chef de Projet

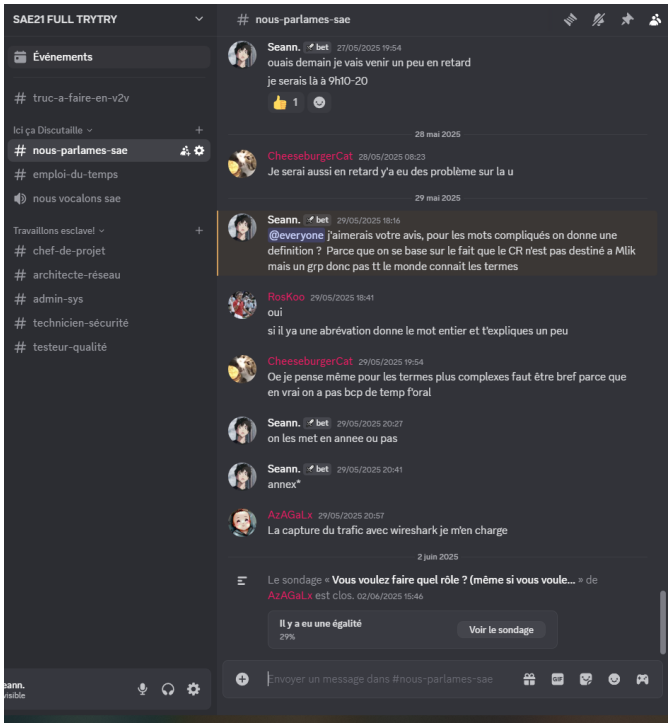
Dans le cadre du projet SAE21 pour GreenHome Solutions, j'ai assuré le rôle de chef de projet, chargé de l'organisation globale, de la répartition des tâches, du suivi de l'avancement et de la consolidation finale des livrables. Ma mission principale a été de coordonner l'équipe de travail, composée de cinq rôles complémentaires, dans un délai limité de 12 jours.

I) Mise en place des outils collaboratifs

Dès le début du projet, j'ai mis en place les outils nécessaires à la collaboration et à la gestion du temps. Un tableau Trello a été créé pour répartir les tâches par jour et par rôle. Chaque membre y disposait de ses propres cartes avec checklist, étiquettes et échéances.



Nous avons également décidé de mettre en place un serveur Discord pour centraliser nos échanges, organiser nos réunions vocales et suivre l'avancement quotidien. Un salon par rôle a permis de fluidifier la communication interne.



Lien du Discord : https://discord.gg/HQRAMvjY

Enfin, un dépôt GitHub / GitLab a été utilisé pour stocker certaines configurations (fichiers .pkt, scripts de configuration) et assurer un suivi de version.

II) Répartition des rôles et gestion du planning

Lors de la réunion de lancement, j'ai attribué les rôles suivants aux membres du groupe :

- Chef de projet (Sean Van ngoc)
- Architecte réseau (Aymeric Contrevilliers)
- Administrateur systèmes (Ronan Lepabic)
- Technicien sécurité (Gabin Grugeard)
- Testeur / qualité (Amaury Moutier)

(Les couleurs sont représentatives de celle du Trello).

Un planning de travail sur 10 jours a été défini dès le départ, avec des objectifs précis chaque jour (ex. : J2 → plan IP, J4 → services, J7 → documentation, etc.).

Disponible sur le Trello :
https://trello.com/invite/b/6831ecb116cd310754a63c1f/ATTIbf53b4f4c59b74480bddec89f4f13c24D53C5A64/sae21-construire-un-reseau-informatique-pour-une-petite-structure

III) Suivi des livrables et coordination

Tout au long du projet, nous avons assuré :

- Le suivi de la progression de chaque membre via Trello et Discord
- La relance des tâches bloquées (goulots d'étranglement)
- La collecte des preuves techniques (captures, scripts, configs)
- La consolidation des contributions pour créer le dossier technique final

J'ai également supervisé la rédaction des fiches de contribution, des journaux de bord individuels et la préparation de la soutenance orale, en répartissant les parties de la présentation.

IV) Finalisation et soutenance

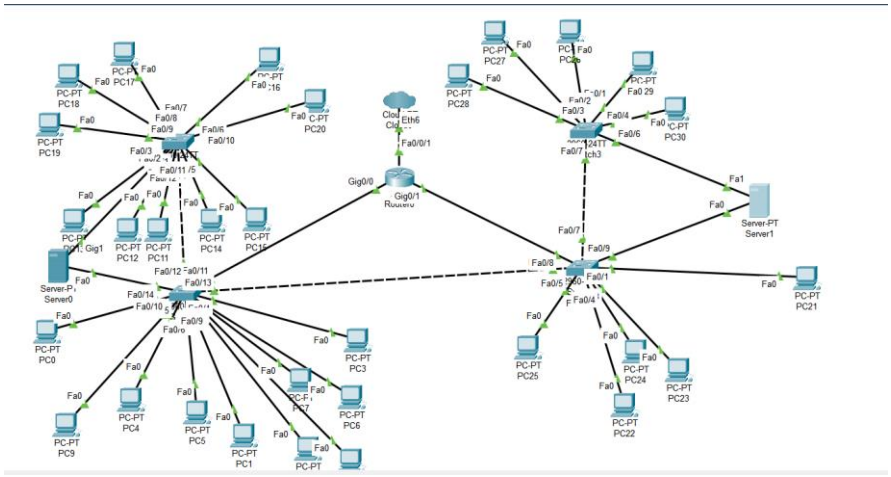
En fin de projet, j'ai :

- Vérifié l'exhaustivité et la cohérence du dossier technique
- Préparé le diaporama de soutenance à partir des apports de chaque membre
- Organisé une répétition générale pour fluidifier l'oral
- Coordonné la remise des livrables (dossier, journaux, fiches)

[Image : Capture de la présentation PowerPoint ou slide d'introduction de la soutenance]

2) Travail réalisé – Architecte Réseau

Dans le cadre de la conception de l'infrastructure réseau de l'entreprise GreenHome Solutions, nous avons mis en place le réseau physique et logique avec segmentation par VLAN, routage inter-VLAN et adressage IP structuré.



I) Création des VLANs

La première étape consiste à définir les VLANs correspondant aux différents services de l'entreprise (Direction, production, commercial). Ces VLANs ont été créés sur chaque switch avec une identification unique que nous appelons (ID) et des noms explicites pour facilités la gestion.

```
Switch(config)#vlan 10
Switch(config-vlan)#name RH
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Informatique
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Securite
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name Commerce
Switch(config-vlan)#exit
Switch(config)#vlan 50
Switch(config-vlan)#name Direction
Switch(config-vlan)#exit
```

Cette configuration permet de cloisonner logiquement les postes utilisateurs tout en maintenant une structure claire et évolutive (pour durer dans le temps).

II) Attribution des ports aux VLANs et configurations des trunks

Une fois les VLANs définis, nous avons attribué les ports des switchs aux VLANs selon les services hébergés par chaque machine. Chaque port a été configuré en mode accès c'est-à-dire : switchport mode access avec l'attribution du VLAN correspondant. Par ailleurs, les liaisons entre les switchs ont été configurés en mode trunk pour permettre la circulation de plusieurs VLANs sur les liens d'interconnexion.

```
Switch(config)#interface range fa0/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa0/3 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#ex
Switch(config-if-range)#exit
Switch(config)#interface range fa0/5 - 6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface range fa0/7 - 8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#interface range fa0/9 - 10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#exit
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode trunk
Switch(config-if)#no shutdown
Switch(config-if)#
```

Ce paramétrage garentit une transmission fluide des trames entre les différents équiepemnts réseau tout en conservant l'isolation logique par les services.

III) Configuration du routage inter-VLAN

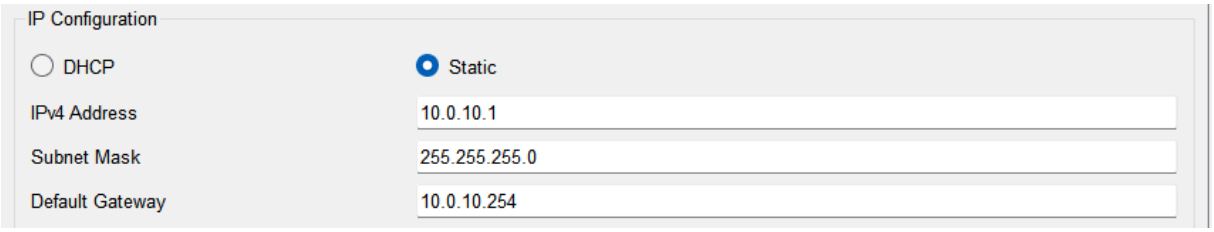
Afin de permettre la communication entre les différents VLANs, nous avons décidé d'activer le routage inter-VLAN sur le routeur principal. Cette opération a été réalisée avec l'interface GigabitEthernet0/0 en créant une sous-interface par VLAN. Chaque sous interface a été configurée avec une encapsulation dot1Q puis avec une adresse IP propre à chaque sous réseau.

```
show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES manual up                    up
GigabitEthernet0/0.10  10.0.10.254     YES manual up                    up
GigabitEthernet0/0.20  10.0.20.254     YES manual up                    up
GigabitEthernet0/0.30  10.0.30.254     YES manual up                    up
GigabitEthernet0/0.40  10.0.40.254     YES manual up                    up
GigabitEthernet0/0.50  10.0.50.254     YES manual up                    up
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/1.10  unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES manual administratively down down
FastEthernet0/0/0      unassigned      YES unset  up                    down
FastEthernet0/0/1      unassigned      YES unset  up                    down
FastEthernet0/0/2      unassigned      YES unset  up                    down
FastEthernet0/0/3      unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Grâce à cette configuration, le routeur est donc capable de faire transiter les données entre les VLANs tout en maintenant leur séparation logique.

IV) Adressage IP des postes clients

Enfin, les postes clients ont été configurés manuellement avec des adresses IP appartenant à leurs sous réseau respectif et une passerelle correspondant à l'IP de la sous interface du routeur dédiée à leur VLAN.



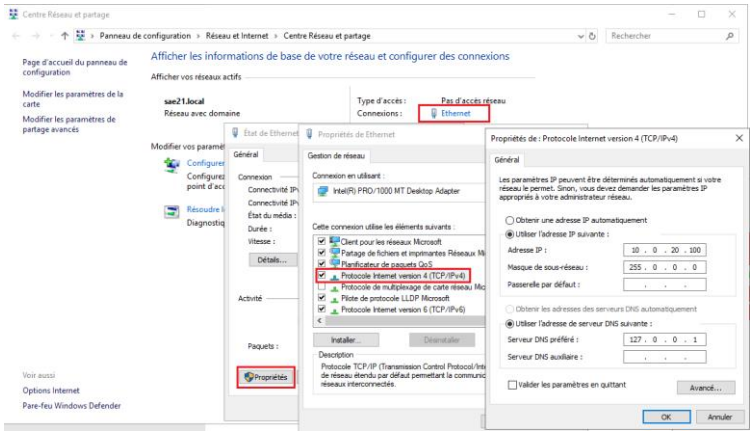
Cette configuration permet donc aux machines de communiquer à l'intérieur de leur VLAN et d'accéder aux autres VLANs (si autorisé bien évidemment) via le routage et à terme d'accéder à Internet (après que l'on a configuré le NAT).

3) Travail réalisé – Administrateur Systèmes

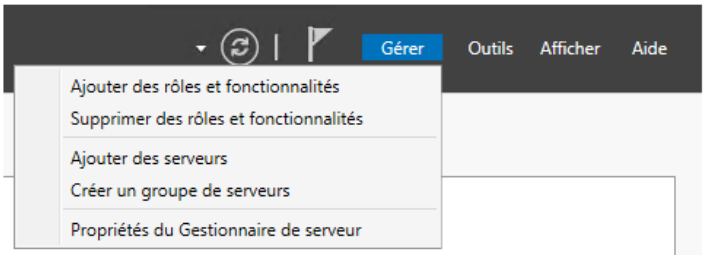
Dans le cadre de la mise en place des services réseau de l'entreprise GreenHome Solutions, nous avons décidé déployer l'ensemble des composants essentiels sur un serveur Windows Server. Les principales missions ont concerné l'installation et la configuration de DNS, Active Directory, DHCP, ainsi que d'un serveur web IIS accessible depuis le réseau local.

I) Configuration initiale du serveur

Nous avons commencé par attribuer une adresse IP statique au serveur afin de garantir sa stabilité sur le réseau et faciliter son identification par les autres machines.

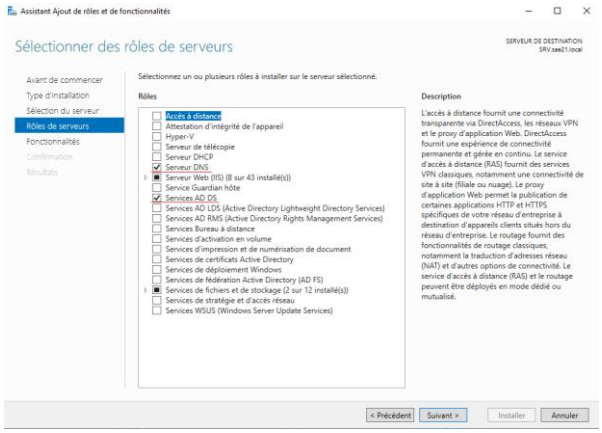


Le serveur a ensuite été renommé SRV, cela permet d'avoir une meilleure visibilité au sein du domaine à venir.



II) Installation du rôle DNS et du domaine Active Directory

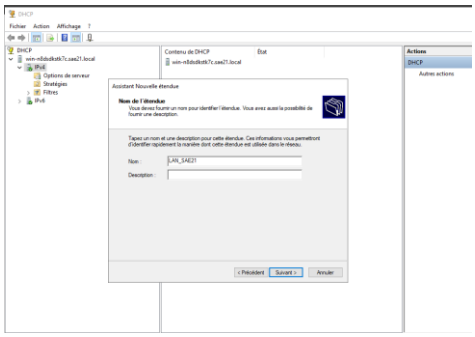
Nous avons procédé à l'installation du rôle DNS qui est nécessaire pour la résolution de noms dans le réseau local ainsi qu'au déploiement de l'Active Directory Domain Services (AD DS). Ces éléments ont été installés depuis le gestionnaire de serveur Windows.

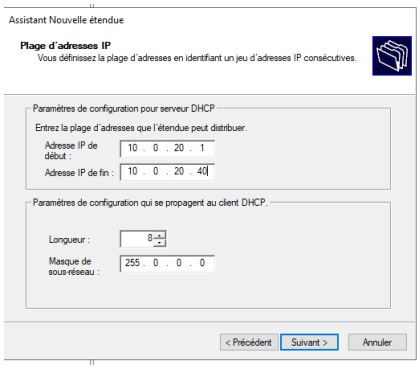


Après la promotion du serveur en tant que contrôleur de domaine, les clients peuvent désormais joindre le domaine pour bénéficier d'une gestion centralisée des comptes et des autorisations.

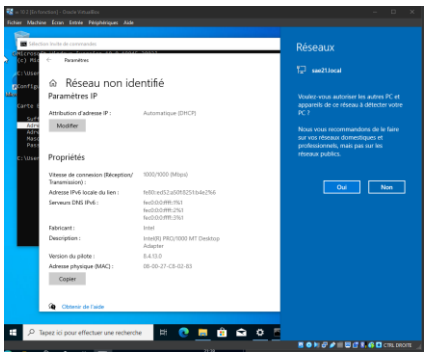
III) Mise en place du DHCP

Pour automatiser l'attribution des adresses IP aux clients, nous avons décidé de configurer un serveur DHCP en créant une étendue personnalisée incluant la plage d'adresses IP, la passerelle et le DNS réseau.



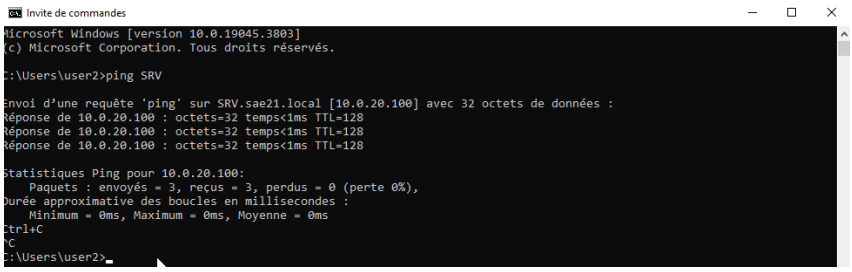


Une fois configuré, le client obtient automatiquement une IP valide lorsqu'il se connecte au réseau. Nous avons validé cela en vérifiant que la machine cliente recevait bien une adresse via DHCP.



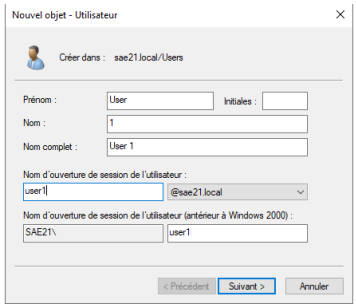
IV) Tests du service DNS

Nous avons ensuite testé le bon fonctionnement du serveur DNS en réalisant un ping du nom du serveur depuis une machine cliente. La résolution de nom s'est bien effectuée ce qui confirme que le DNS marche bien.

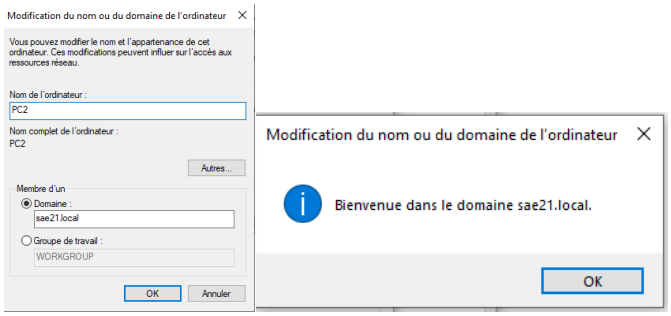


V) Création des utilisateurs et intégration au domaine

Depuis la console "Utilisateurs et ordinateurs Active Directory", nous avons créé plusieurs utilisateurs au sein du domaine. Chaque utilisateur dispose désormais d'un compte centralisé.

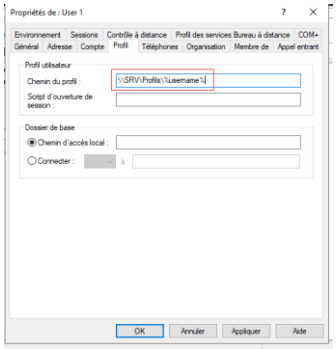


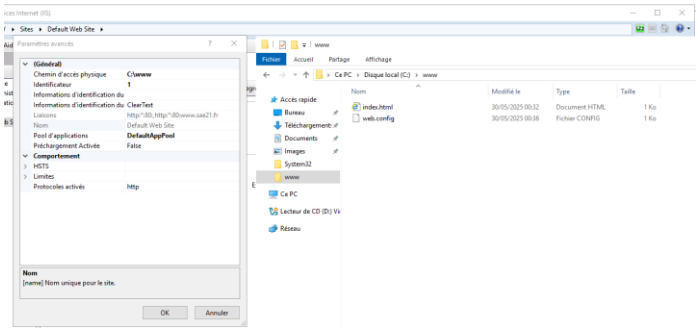
Les machines clientes ont ensuite été liées au domaine, ce qui permet une gestion centralisée des sessions, droits d'accès et ressources.



VI) Mise en place des profils itinérants

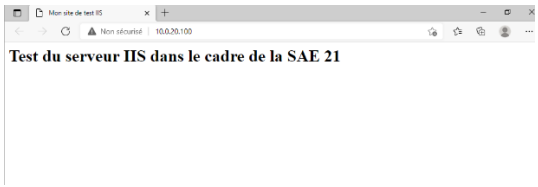
Pour permettre aux utilisateurs de retrouver leur environnement de travail sur n'importe quelle machine du domaine, nous avons mis en place des profils itinérants. Un dossier partagé nommé "Profils" a été créé sur le serveur. Ensuite, dans les propriétés de chaque utilisateur, nous avons indiqué le chemin réseau vers ce dossier.





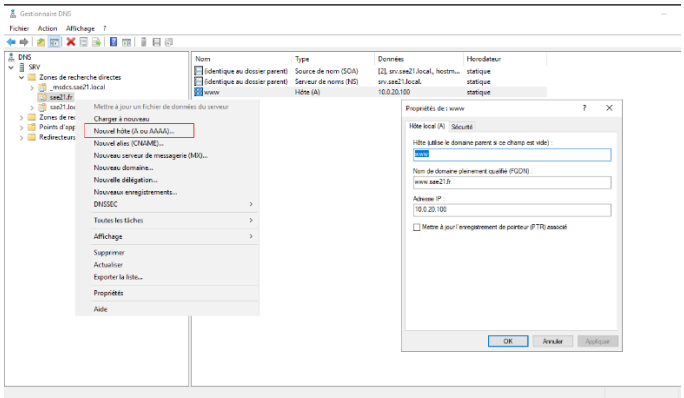
VII) Installation du serveur web IIS

Nous avons installé le serveur web IIS, l'équivalent de Apache2 mais intégré à Windows, pour héberger un site local. Après avoir modifié le répertoire racine, nous avons créé un fichier index.html permettant de tester l'accessibilité du site.



VIII) Configuration DNS pour un alias web (www.sae21.fr)

Afin de rendre le site plus accessible, nous avons ajouté une zone DNS personnalisée "sae21.fr" et un enregistrement de type A pointant vers le serveur web. Cela permet d'accéder au site via l'URL www.sae21.fr.



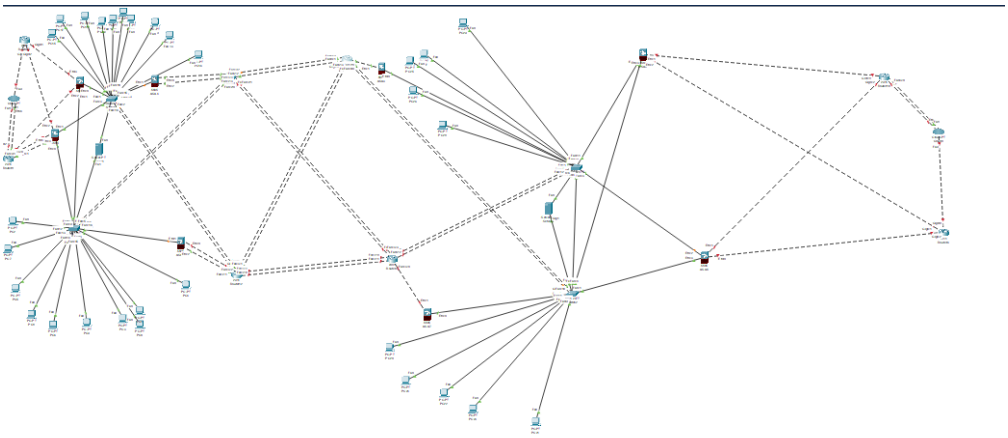
Nous avons confirmé le bon fonctionnement en accédant au site depuis une machine cliente, uniquement via le nom de domaine.

4) Travail réalisé – Technicien Sécurité

Dans le cadre du projet réseau de GreenHome Solutions, nous avons assuré la configuration des éléments de sécurité du réseau, notamment le pare-feu, la traduction d'adresses (NAT) et les règles de filtrage ACL. Ces actions garantissent la protection des flux, le cloisonnement logique et l'accès sécurisé entre les services du réseau.

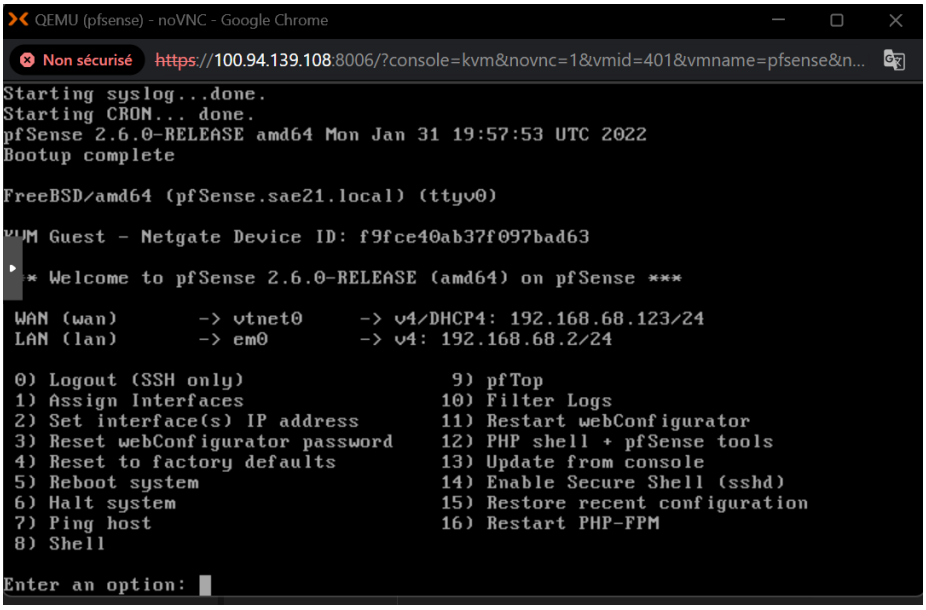
I) Amélioration de la topologie réseau

Nous avons suggéré une amélioration du schéma réseau visant à renforcer la redondance et la tolérance aux pannes. En cas de défaillance sur un lien ou un équipement, cette nouvelle disposition permet de limiter les pertes de connectivité et d'assurer une continuité de service.



II) Configuration du pare-feu (pfSense)

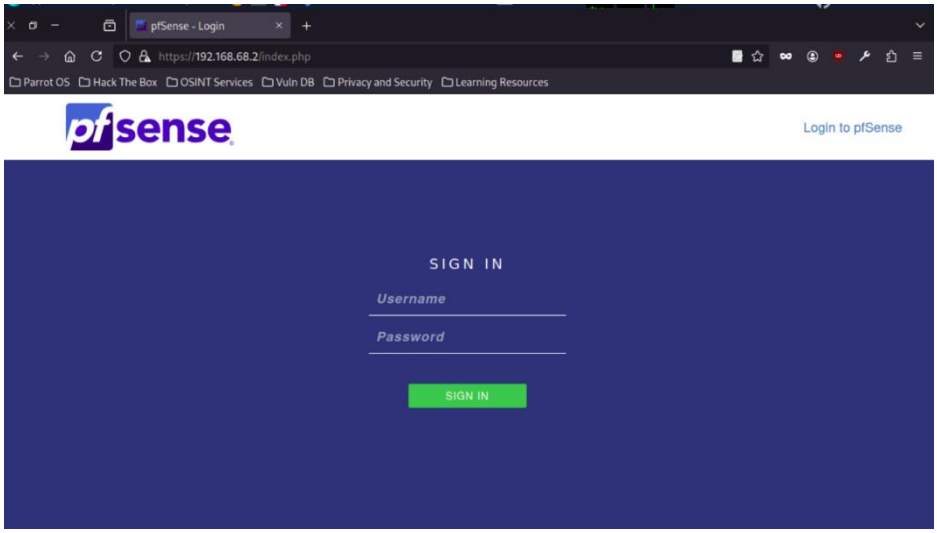
Nous avons mis en place une solution de pare-feu via pfSense, une distribution open source spécialisée dans la sécurité réseau. L'interface LAN a été définie comme point d'entrée interne tandis que l'interface WAN a été configurée pour la sortie vers l'Internet.



Cette séparation permet de contrôler précisément quels types de flux sont autorisés ou bloqués et d'isoler le réseau interne des menaces extérieures.

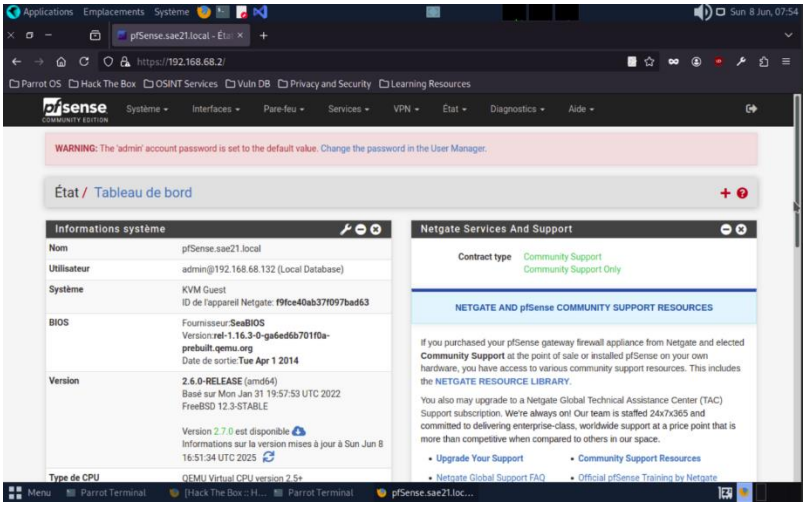
III) Interface web de pfSense

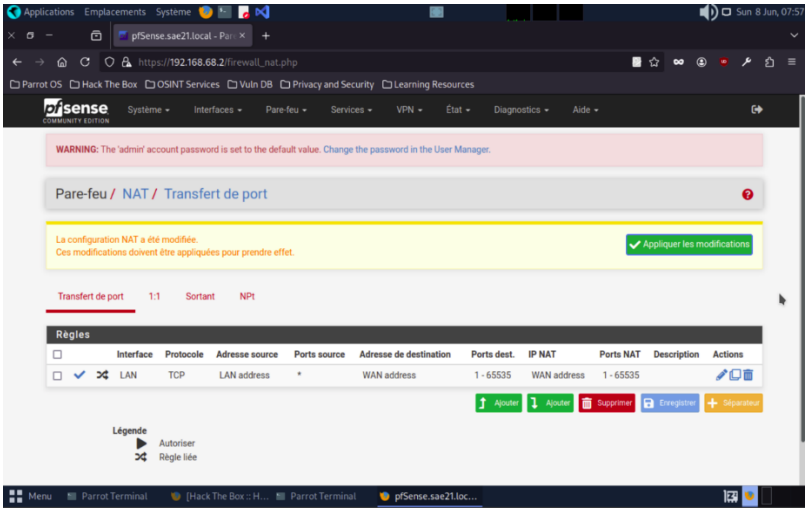
Toutes les règles ont été définies via l'interface web de gestion de pfSense qui offre une visualisation claire des interfaces, du trafic et des règles de filtrage.



IV) Mise en place du NAT

Nous avons configuré les règles de NAT (Network Address Translation) afin de permettre aux machines du réseau local d'accéder à Internet tout en masquant leurs adresses internes.

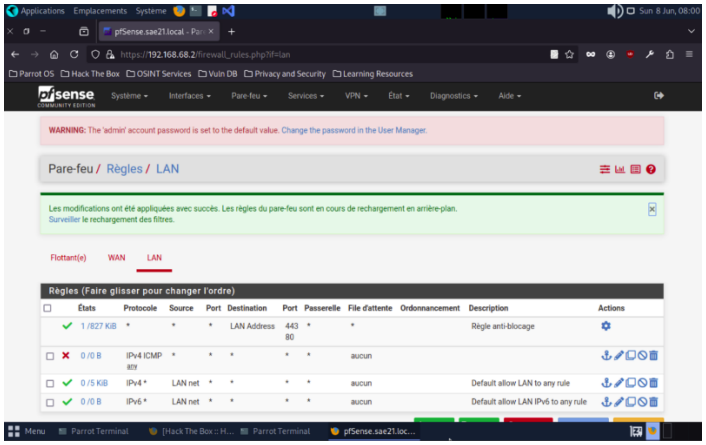




Le NAT dynamique (PAT) a été activé pour que plusieurs machines partagent une même adresse publique lors des accès externes, ce qui optimise la sécurité et la gestion des flux.

V) Application des règles ACL (Access Control List)

Enfin, nous avons mis en place des règles ACL afin de restreindre les communications selon les besoins de sécurité. Par exemple, une règle a été définie pour bloquer les requêtes ICMP (ping) entre certaines zones du réseau.



Ce filtrage permet de limiter la visibilité du réseau et de contrôler la circulation des paquets sensibles entre les VLANs.

5) Travail réalisé – Testeur / Qualité

Dans le cadre du projet de déploiement réseau pour l'entreprise GreenHome Solutions, nous avons assuré le rôle de testeur / qualité, en réalisant une série de tests de connectivité afin de valider la structure logique du réseau, le bon fonctionnement des VLANs et la cohérence des configurations inter-sites. L'objectif principal de cette phase de validation est de garantir que l'architecture réseau est fonctionnelle, stable et conforme aux exigences du projet SAE21.

I) Mise en place de la stratégie de test

Nous avons adopté une approche progressive, en testant les couches physique, réseau, puis logique, à travers des scénarios ciblés de type ping. L'outil principal utilisé a été Cisco Packet Tracer, accompagné de commandes telles que ping et traceroute pour vérifier la connectivité entre les machines virtuelles.

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC11	ICMP
	0.001	PC11	Switch2	ICMP
	0.002	Switch2	Switch0	ICMP
	0.003	Switch0	Switch1	ICMP
	0.004	Switch1	PC21	ICMP
	0.005	PC21	Switch1	ICMP
	0.006	Switch1	Switch0	ICMP
	0.007	Switch0	Switch2	ICMP
Visible	0.008	Switch2	PC11	ICMP

La capture suivante est entre 2 pc : le PC11 a Grenoble et le PC 21 à Lyon. La capture nous montre que le ping est un succès car ces 2 PC même si ils ne sont pas sur le même site , sont sur le même VLAN.

II) Résultats des scénarios de test

Nous avons mené six tests de connectivité couvrant à la fois les communications intra-site (Lyon) et inter-sites (Lyon ↔ Grenoble), entre postes d'un même VLAN ou de VLANs différents.

III.1) Test T001 – Ping entre deux machines du même VLAN, sur le même switch à Lyon

Le test de connectivité entre deux machines appartenant au même VLAN et situées sur le même switch à Lyon a été un succès. Le ping a été réalisé entre les adresses 10.0.10.3 et 10.0.10.4, avec un taux de perte de 0 % et un temps de réponse inférieur à 5 ms.

```
Pinging 10.0.10.4 with 32 bytes of data:

Reply from 10.0.10.4: bytes=32 time=5ms TTL=128
Reply from 10.0.10.4: bytes=32 time=4ms TTL=128
Reply from 10.0.10.4: bytes=32 time=4ms TTL=128
Reply from 10.0.10.4: bytes=32 time=4ms TTL=128

Ping statistics for 10.0.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

III.II) Test T002 – Ping entre deux machines de VLANs différents, même switch à Lyon

Ce test visait à vérifier si deux postes appartenant à des VLANs différents pouvaient communiquer entre eux. Comme attendu, le ping a échoué avec un message "Destination unreachable", confirmant que le cloisonnement logique par VLAN est bien actif.

```
Pinging 10.0.20.3 with 32 bytes of data:

Reply from 10.0.10.254: Destination host unreachable.
Reply from 10.0.10.254: Destination host unreachable.
Reply from 10.0.10.254: Destination host unreachable.

Ping statistics for 10.0.20.3:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
```

III.III) Test T003 – Ping entre deux machines du même VLAN, sur deux switchs différents à Lyon

Le ping effectué entre deux machines du même VLAN, mais connectées à des switchs différents à Lyon, a fonctionné avec succès. Cela confirme que le trunking VLAN entre les switchs est opérationnel et bien configuré.

```
C:\>ping 10.0.10.1

Pinging 10.0.10.1 with 32 bytes of data:

Reply from 10.0.10.1: bytes=32 time=12ms TTL=128
Reply from 10.0.10.1: bytes=32 time=6ms TTL=128
Reply from 10.0.10.1: bytes=32 time=6ms TTL=128

Ping statistics for 10.0.10.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 12ms, Average = 8ms
```

III.IV) Test T004 – Ping entre deux machines de VLANs différents, sur deux switchs à Lyon

Une tentative de communication entre deux VLANs différents répartis sur deux switchs distincts a échoué. L'absence de routage inter-VLAN actif ou la présence de règles de filtrage ACL pourrait expliquer ce blocage.

```
C:\>ping 10.0.20.1

Pinging 10.0.20.1 with 32 bytes of data:

Reply from 10.0.10.254: Destination host unreachable.
Reply from 10.0.10.254: Destination host unreachable.

Ping statistics for 10.0.20.1:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

III.V) Test T005 – Ping entre deux machines du même VLAN, situées sur des sites différents (Lyon → Grenoble)

Le ping entre deux postes du même VLAN, situés respectivement sur les sites de Lyon et de Grenoble, a parfaitement fonctionné. Cela démontre que la communication inter-sites est bien en place pour les VLANs autorisés.

```
C:\>ping 10.0.10.5

Pinging 10.0.10.5 with 32 bytes of data:

Reply from 10.0.10.5: bytes=32 time=16ms TTL=128
Reply from 10.0.10.5: bytes=32 time=8ms TTL=128

Ping statistics for 10.0.10.5:
    Packets: Sent = 3, Received = 2, Lost = 1 (34% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 16ms, Average = 12ms
```

III.VI) Test T006 – Ping entre deux machines de VLANs différents sur des sites différents

Le test entre des machines de VLANs différents situées sur Lyon et Grenoble a échoué, comme attendu. Cela montre que les règles de cloisonnement réseau sont bien maintenues, même à travers les interconnexions entre les deux sites.

```
C:\>ping 10.0.20.5

Pinging 10.0.20.5 with 32 bytes of data:

Reply from 10.0.10.254: Destination host unreachable.
Reply from 10.0.10.254: Destination host unreachable.

Ping statistics for 10.0.20.5:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Conclusion

Ce projet nous a permis de reproduire une situation réelle de déploiement d'un réseau d'entreprise, en mettant en œuvre des compétences techniques, organisationnelles et collaboratives.

L'infrastructure demandée a été conçue, configurée et testée avec succès, conformément aux attentes de GreenHome Solutions. Chaque rôle a apporté sa contribution dans les délais impartis et l'ensemble des livrables a été finalisé dans un cadre structuré et professionnel.

Nous retenons de cette SAE une expérience enrichissante, tant sur le plan technique que méthodologique, avec une meilleure compréhension des enjeux liés à la gestion de projet en réseau informatique, à la cybersécurité, à la configuration système et à la collaboration en équipe.