DOSSIER PROFESSIONNEL - MR MICHELE MASTROGIACOMO –
BTS S.I.O. OPTION S.I.S.R.

SOMMAIRE :

Introduction Pag.3

Présentation du contexte professionnel (stage) Pag.3

- Présentation de la structure du stage
- Objectifs du stage « création d'un éco-site à énergie positive »

Analyse des besoins et des contraintes Pag.4

- Besoins fonctionnels
- Contraintes techniques et organisationnelles
- Contraintes environnementales et énergétiques

Présentation de l'architecture réseau Pag.5

Schéma réseau projet

- DMZ Pag.6
- Organisation du réseau interne
- Accès Wi-Fi

Solutions techniques mises en œuvre Pag.7

Pare-feu et routage – pfSense

- Rôle et fonctionnalités
- Contribution à la sécurisation et à la maîtrise des flux

DMZ

- Principe
- Serveur Web
- Serveur FTP / SFTP

Services réseau internes Pag.8

- Active Directory
- DNS
- Serveur de fichiers

Serveur de fichiers

Sauvegarde et continuité des services – NAS Pag.9

Sécurité du système d'information Pag.10
- Segmentation logique du réseau

Schéma adressage IP VLAN
- Filtrage et contrôle des flux réseau Pag.11

Schéma Réglages DMZ
- Gestion des accès utilisateurs Pag.12

Schema Utilisateur Etudiants Pag.13

Schema GPO Restriction Etudiants Pag.13
- Sécurisation des services Pag.14
- Protection des données et sauvegardes

Démarche éco-responsable de l'infrastructure Pag.14
- Optimisation de la consommation énergétique
- Gestion durable de l'infrastructure

Tests, validation et limites Pag.15
- Tests de fonctionnement
- Tests de sécurité Pag.15

Test Connexion DMZ , FTP et Serveur de Fichiers Pag.16

Test Connexion PC Administration , Serveur de Fichiers et DMZ Pag.16
- Limites du projet

Conclusion : Évolutions possibles Pag.17
- Renforcement de la sécurité
- Haute disponibilité et continuité de service
- Optimisation des performances réseau
- Renforcement des solutions écologiques

Introduction

Le projet présenté dans ce dossier consiste à concevoir l'architecture réseau d'un lycée composé de plusieurs bâtiments : un bâtiment administratif, un bâtiment destiné aux classes, un bâtiment pour les ateliers et un bâtiment informatique servant de local technique. Ce projet est entièrement virtualisé pour sa présentation avant déploiement et s'inscrit dans la continuité du stage effectué autour de la création d'un éco-site à énergie positive.

L'architecture repose sur l'utilisation d'un pare-feu pfSense, assurant le rôle de routeur et de dispositif de sécurité entre Internet, une zone démilitarisée (DMZ) et le réseau interne. La DMZ héberge les services accessibles depuis Internet, tels qu'un serveur Web et un serveur FTP/SFTP, tout en restant isolée du réseau interne.

Les serveurs internes sont centralisés dans le bâtiment informatique : ils comprennent un serveur Windows assurant les services d'Active Directory, de DNS, un serveur de fichiers pour le stockage des données, ainsi qu'un NAS dédié à la sauvegarde.

Les autres bâtiments ne disposent que de postes clients, limitant ainsi la consommation énergétique et les coûts de maintenance. L'authentification centralisée via Active Directory permet une gestion efficace des accès tout en réduisant les ressources matérielles nécessaires.

Présentation du Stage professionnel

Le stage s'est déroulé dans le cadre d'un projet intitulé **« Création d'un éco-site à énergie positive »**, dont l'objectif principal était de concevoir et mettre en œuvre des solutions permettant de réduire la consommation énergétique d'un site tout en favorisant l'utilisation d'énergies renouvelables.

Au cours de ce stage, différentes problématiques liées à la gestion de l'énergie, à la durabilité des infrastructures techniques ont été abordées.

Ce projet s'inspire ainsi de ce contexte en proposant une architecture réseau centralisée, limitant la multiplication des équipements et favorisant une meilleure maîtrise de la consommation énergétique. Le regroupement des serveurs dans un bâtiment informatique unique permet une gestion plus efficace des ressources matérielles, une maintenance simplifiée et une optimisation de l'alimentation électrique.

La conception de l'infrastructure réseau intègre également une **démarche éco-responsable**, inspirée du stage réalisé autour de la création d'un **éco-site à énergie positive**, et adaptée au contexte d'un établissement scolaire.

L'objectif est de proposer une architecture permettant de réduire la consommation énergétique, d'optimiser l'utilisation des ressources matérielles et de limiter l'impact environnemental du système d'information

Analyse des besoins et des contraintes

Pour mettre en place cette infrastructure c'est recommandable d'effectuer une analyse des besoins fonctionnels ainsi que des contraintes techniques, organisationnelles et environnementales

Besoins fonctionnels :

Le lycée doit disposer d'un accès Internet fiable et sécurisé afin de répondre aux besoins pédagogiques et administratifs.

La **centralisation des services informatiques** permet de simplifier l'administration du système d'information et concerne notamment l'authentification des utilisateurs, la gestion des adresses réseau et le stockage des données.

L'**authentification centralisée** via un annuaire est indispensable afin de gérer efficacement les comptes utilisateurs, les droits d'accès et les ressources partagées. Elle permet également de renforcer la sécurité en évitant la multiplication de comptes locaux sur les postes clients.

Le système doit aussi permettre un **accès sécurisé aux services internes et externes**. Les services accessibles depuis Internet (site Web, serveur FTP/SFTP) doivent être disponibles tout en restant isolés du réseau interne, afin de limiter les risques de compromission.

Enfin, **l'infrastructure doit être évolutive**.

Contraintes techniques et organisationnelles :

La principale contrainte technique concerne la **sécurité du système d'information**. Le réseau doit être protégé contre les intrusions extérieures, les accès non autorisés et les erreurs de manipulation. Cela implique la mise en place d'un pare-feu performant, d'une segmentation logique du réseau et d'une gestion des droits d'accès.

Les postes clients sont répartis géographiquement, tandis que les serveurs doivent être regroupés dans un bâtiment informatique dédié.

La **maintenance et l'administration** du réseau doivent rester simples et efficaces.

La **continuité de service** dont les données administratives et pédagogiques doivent être protégées contre les pertes, ce qui nécessite la mise en place de solutions de sauvegarde fiables.

Contraintes environnementales et énergétiques

Dans le cadre du Stage une attention particulière est portée aux **contraintes environnementales**. L'infrastructure doit limiter sa consommation énergétique et réduire son impact environnemental.

La réduction du nombre d'équipements physiques constitue un axe prioritaire. La centralisation des serveurs permet de limiter la dispersion du matériel, de réduire les besoins énergétique..

L'infrastructure doit être conçue de manière à être compatible avec une alimentation issue d'énergies renouvelables, tout en garantissant la stabilité et la continuité du service.
Enfin, le choix de matériels adaptés et sobres énergétiquement s'inscrivent dans une démarche durable, cohérente avec les objectifs pédagogiques et environnementaux du projet.

4. Présentation de l'architecture réseau

L'architecture réseau proposée vise à répondre aux besoins fonctionnels et aux contraintes identifiées précédemment, tout en garantissant un niveau de sécurité élevé. Elle est conçue pour un lycée composé de plusieurs bâtiments interconnectés, avec une centralisation des services dans un bâtiment informatique dédié.

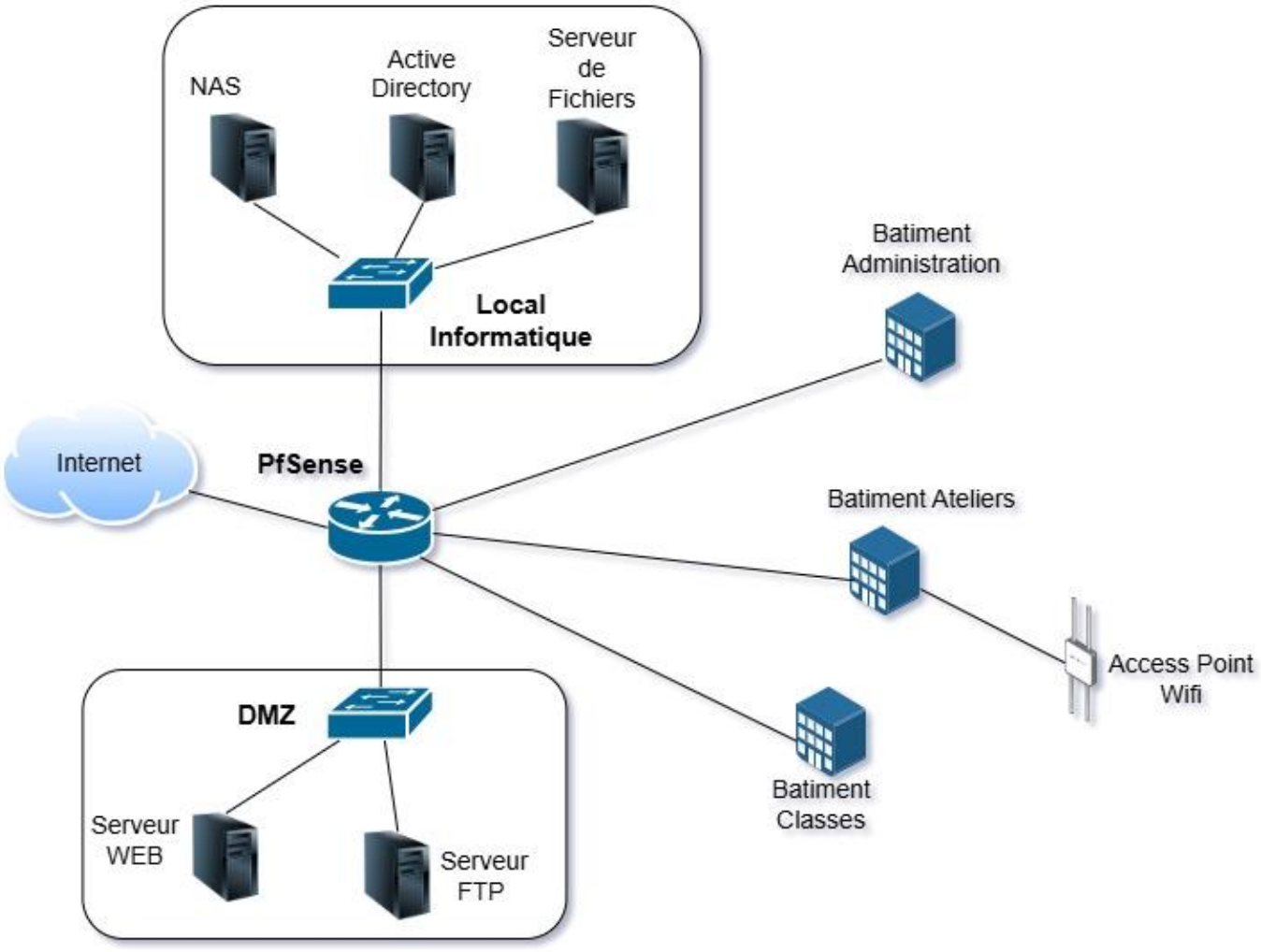


Image 1 : *Schema réseau projet*

L'infrastructure réseau est organisée autour d'un **pare-feu pfSense**, positionné en frontal entre Internet et le réseau interne de l'établissement. Ce pare-feu constitue le point central de l'architecture et assure à la fois le **routage**, le **filtrage des flux** et la **protection du système d'information**.

Le réseau est structuré en trois zones principales :

- **Internet**, représentant l'accès externe, en lien avec le **local informatique**
- une **zone démilitarisée (DMZ)** destinée à héberger les services accessibles depuis l'extérieur,
- le **réseau interne**, réservé aux utilisateurs et aux services internes du lycée.

Cette séparation logique permet de limiter les risques de propagation d'une attaque et d'isoler les différents flux réseau.
Le pare-feu **pfSense** assure la connexion entre les différentes zones du réseau.

La **DMZ** est une zone, contrôlé par pfSense, protégée du Lan interne et héberge les services qui doivent être accessibles depuis l'extérieur, notamment :

- un **serveur Web**,
- un **serveur FTP/SFTP**.

Ces serveurs sont isolés du réseau interne afin de limiter les risques en cas de compromission. Y a 2 Serveur séparé pour plusieurs raisons :

- Si le serveur FTP est compromis → le serveur Web reste intact.
- Meilleure gestion des règles firewall
- Chaque serveur n'expose que les ports nécessaires, on a une réduction de la surface d'attaque
- Si le site grossit on upgrade seulement le serveur Web.

Organisation du réseau interne
Le réseau interne regroupe l'ensemble des postes clients et des serveurs internes.
Les serveurs sont centralisés dans le bâtiment informatique, ce qui permet :

- une administration simplifiée,
- une meilleure maîtrise de la sécurité,
- une optimisation des ressources matérielles et énergétiques.

Les autres bâtiments (administration, classes et ateliers) ne disposent que de postes clients.
Les services internes sont assurés par un serveur Windows qui sont :

- **Active Directory**, pour l'authentification et la gestion des comptes utilisateurs
- **DNS**, pour la résolution de noms ;

Un **serveur de fichiers** permet le stockage et le partage des données, tandis qu'un **NAS** est dédié à la sauvegarde et à la continuité de service.

Accès Wi-Fi
Un **point d'accès Wi-Fi** est présente et couvre l'ensemble du périmètre scolaire, permet de fournir un accès réseau sans fil aux utilisateurs autorisés.

Solutions techniques mises en œuvre
Cette partie présente les différentes solutions techniques retenues pour répondre aux besoins identifiés et aux contraintes du projet. Ce projet est entièrement virtualisé sous le logiciel de simulation réseau qui s'appelle « GNS3 » avec les machines virtuelles en « VMWare ».

Pare-feu et routage – pfSense
Le pare-feu **pfSense** constitue l'élément central de l'architecture réseau. Il est positionné entre Internet, la DMZ et le réseau interne, et assure à la fois les fonctions de routeur et de dispositif de sécurité.
Les principales fonctionnalités mises en œuvre sont :

- le **routage** entre les différentes zones du réseau,
- le **filtrage des flux** à l'aide de règles de pare-feu,
- le contrôle des accès entrants et sortants.

Le choix de pfSense repose sur sa fiabilité, sa flexibilité et son adéquation avec un contexte économique et adaptabilité.

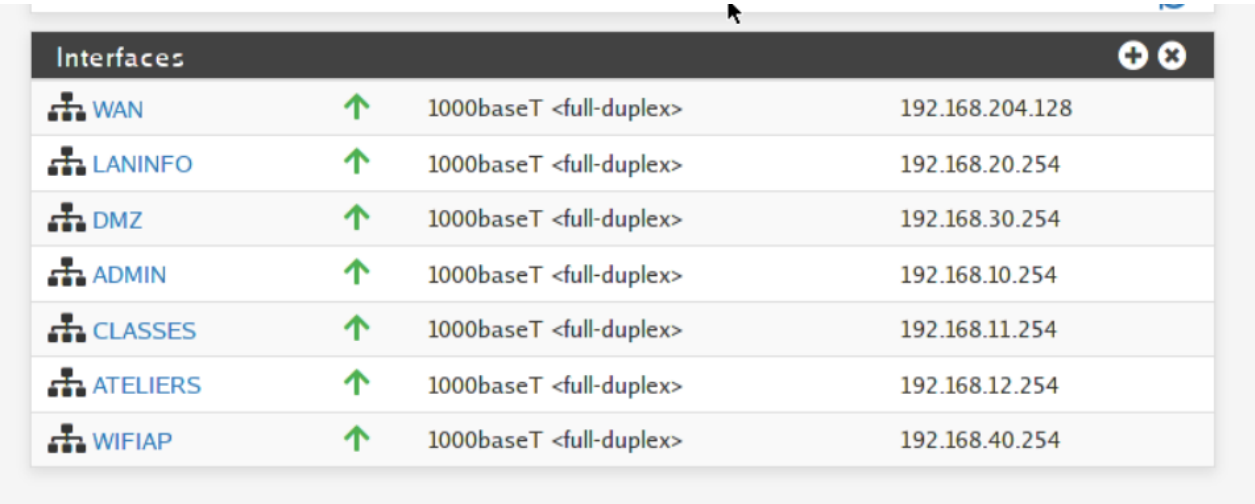


Image 2 : *Liste des Interface sur Pfsense et adresse IP*

Mise en place de la DMZ
La **zone démilitarisée (DMZ)** a pour objectif d'héberger les services devant être accessibles depuis Internet tout en protégeant le réseau interne. Le DMZ comprend :

- un **serveur Web**, destiné à la publication d'informations sur site,
- un **serveur FTP/SFTP**, permettant l'échange sécurisé de fichiers.

Ces serveurs sont isolés du réseau interne et les communications entre la DMZ et le LAN sont strictement limitées aux flux nécessaires. Les règles de filtrage définies sur pfSense permettent d'autoriser uniquement les ports et protocoles requis.
Cette séparation logique limite les risques d'une attaque vers le réseau interne.

Services réseau internes

Les services internes sont centralisés sur un **serveur Windows**, installé dans le bâtiment informatique. Ce serveur assure le rôles de:

- **Active Directory (AD)** :
  Il permet l'authentification centralisée des utilisateurs, la gestion des comptes et des groupes, ainsi que l'application de stratégies de sécurité. Cette centralisation facilite l'administration et renforce la sécurité du système d'information.
- **DNS** :
  Le service DNS assure la résolution de noms au sein du réseau interne.

La centralisation de ces services limite la multiplication des équipements, ce qui contribue à une meilleure maîtrise des ressources matérielles et énergétiques, et de faciliter les opérations de maintenance.

Il est structuré de manière à faciliter la gestion des utilisateurs et à assurer des performances sur l'ensemble des bâtiments.

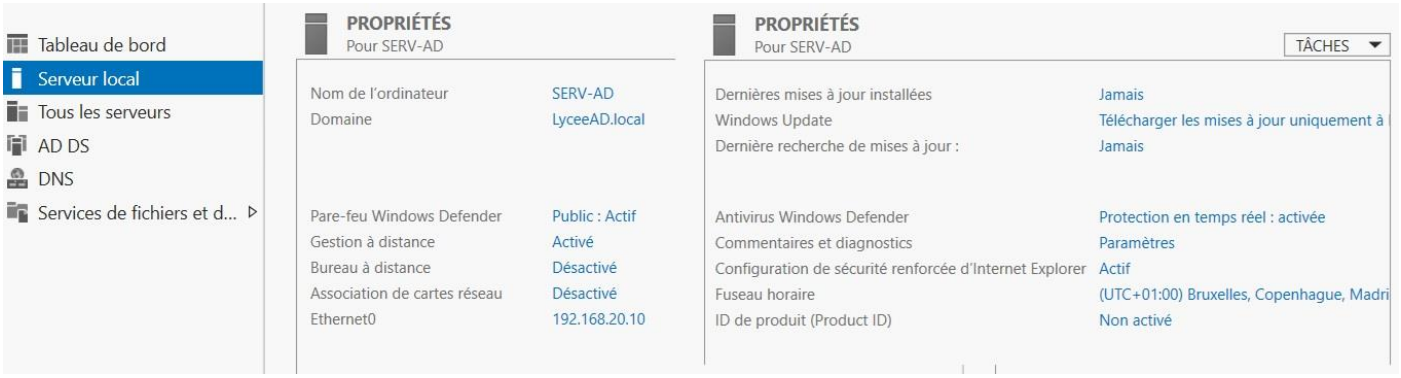


***Image 3** : Information du Serveur pour Active Directory*

Serveur de fichiers

Un **serveur de fichiers** est mis en place afin de centraliser le stockage des données pédagogiques et administratives. Il permet :

- le partage de ressources entre les utilisateurs,
- la gestion des droits d'accès via Active Directory,
- la sécurisation des données sensibles.

Cette solution évite le stockage local sur les postes clients, ce qui facilite la maintenance, améliore la sécurité des données et limite les risques de perte d'informations.

Sauvegarde et continuité de service – NAS

Un **NAS** est dédié à la sauvegarde des données et à la continuité de service. Il permet la mise en œuvre de sauvegardes régulières des serveurs et des fichiers importants.

Cette solution garantit :

- la protection des données en cas de panne ou d'erreur humaine,
- une restauration rapide des services,
- une meilleure fiabilité du système d'information.

Le choix d'un NAS dédié permet de séparer les fonctions de production et de sauvegarde, tout en optimisant l'utilisation des ressources matérielles.

Sécurité du système d'information

La sécurité du système d'information constitue un enjeu majeur pour un établissement scolaire, en raison de la diversité des utilisateurs et de la sensibilité des données traitées. L'architecture proposée intègre plusieurs mécanismes visant à **protéger les ressources**, **contrôler les accès** et **limiter les risques en cas d'incident**.

Segmentation logique du réseau

La sécurité du réseau repose en premier lieu sur une **segmentation logique** claire, permettant de séparer les différents flux et de limiter les interactions entre les zones. L'infrastructure est organisée autour de trois zones distinctes :

- l'accès **Internet** et le **local informatique**
- la **DMZ**, destinée aux services accessibles depuis l'extérieur,
- le **réseau interne**, réservé aux utilisateurs et aux serveurs internes.

Cette segmentation permet d'isoler les services exposés et d'éviter qu'une compromission externe n'impacte directement le réseau interne. Les échanges entre ces zones sont strictement contrôlés par le pare-feu pfSense.

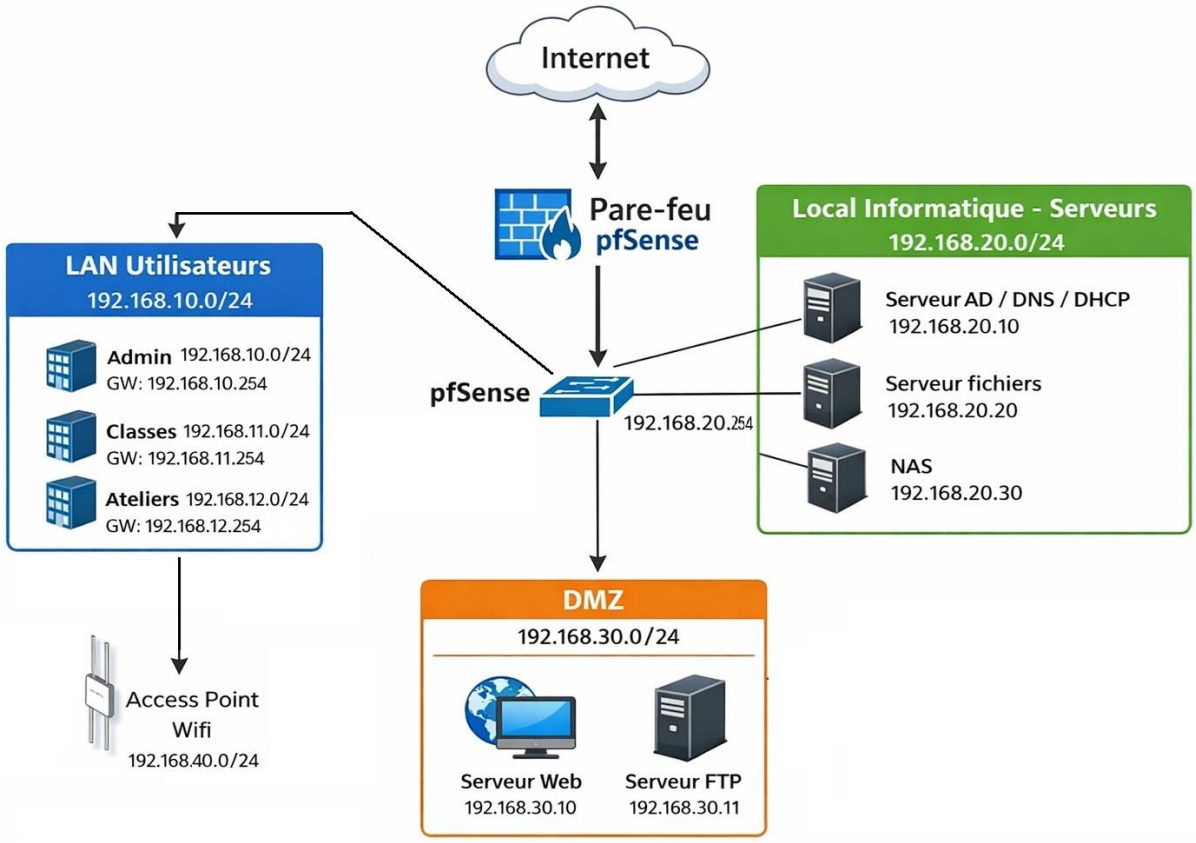


***Image 4** : Schema adresssage IP VLAN*

Filtrage et contrôle des flux réseau

Le pare-feu **pfSense** assure le filtrage des flux réseau à l'aide de règles précises. Seuls les ports et protocoles strictement nécessaires sont autorisés, les principales fonctions assurées sont :

le routage entre Internet, la DMZ et le réseau interne, le filtrage des flux réseau à l'aide de règles de pare-feu, la traduction d'adresses (NAT) pour les services exposés, la surveillance et le contrôle des accès.

Les règles mises en place permettent notamment :

- de limiter les accès entrants depuis Internet vers la DMZ,
- d'empêcher tout accès direct entre Internet et le réseau interne,
- de contrôler les communications entre la DMZ et le réseau interne.

Ce filtrage réduit considérablement la surface d'attaque et contribue à renforcer la sécurité globale de l'infrastructure.

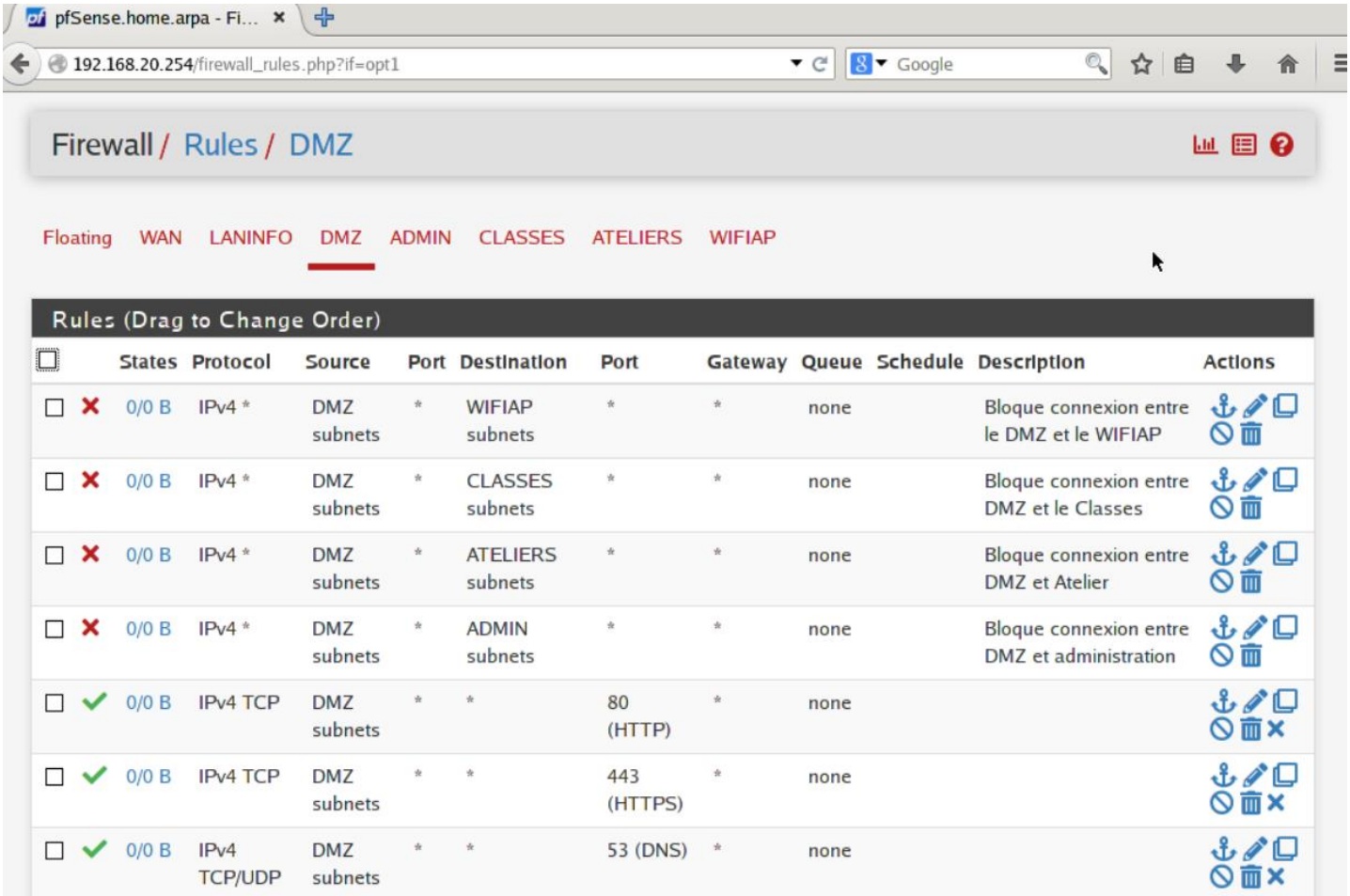
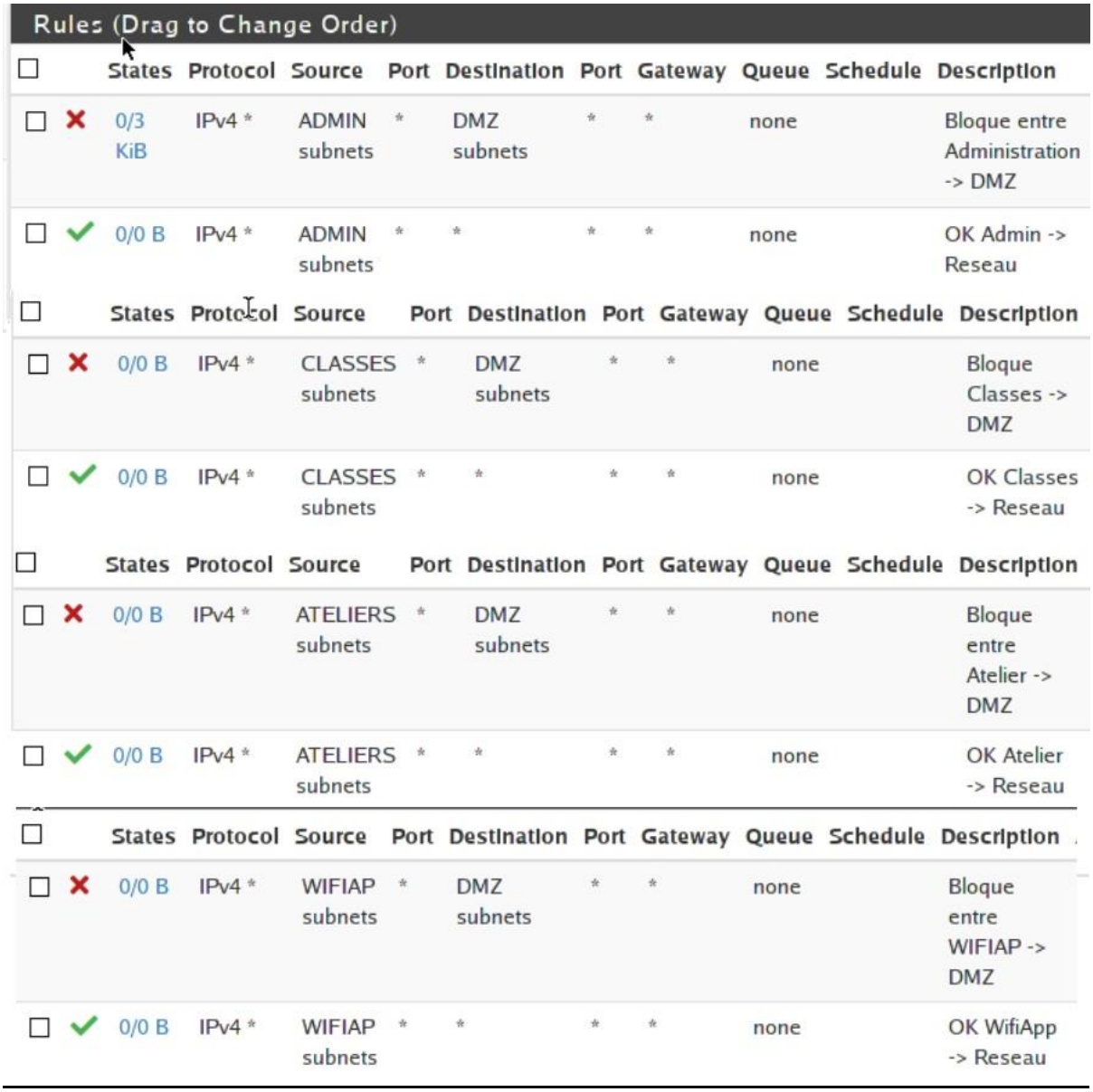


Image 5 *: Règles pare-feu qui bloque communication entre le DMZ et les autre zone sauf pour connexion a Internet*



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✗	0/3 KiB	IPv4 *	ADMIN subnets	*	DMZ subnets	*	*	none		Bloque entre Administration -> DMZ
✓	0/0 B	IPv4 *	ADMIN subnets	*	*	*	*	none		OK Admin -> Reseau

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✗	0/0 B	IPv4 *	CLASSES subnets	*	DMZ subnets	*	*	none		Bloque Classes -> DMZ
✓	0/0 B	IPv4 *	CLASSES subnets	*	*	*	*	none		OK Classes -> Reseau

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✗	0/0 B	IPv4 *	ATELIERS subnets	*	DMZ subnets	*	*	none		Bloque entre Atelier -> DMZ
✓	0/0 B	IPv4 *	ATELIERS subnets	*	*	*	*	none		OK Atelier -> Reseau

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✗	0/0 B	IPv4 *	WIFIAP subnets	*	DMZ subnets	*	*	none		Bloque entre WIFIAP -> DMZ
✓	0/0 B	IPv4 *	WIFIAP subnets	*	*	*	*	none		OK WifiApp -> Reseau

Image 6 *: Règles pare-feu qui bloque communication entre les autre zone et le DMZ*
Ce zone peuvent acceder au site web travers un browser Internet

Gestion des accès utilisateurs

La gestion des accès repose sur une **authentification centralisée via Active Directory**. Chaque utilisateur dispose d'un compte personnel, ce qui permet de :

- contrôler les droits d'accès aux ressources,
- tracer les connexions,
- appliquer des politiques de sécurité adaptées.

Les droits sont attribués en fonction des rôles (admin, enseignants, élèves), limitant l'accès aux ressources sensibles.

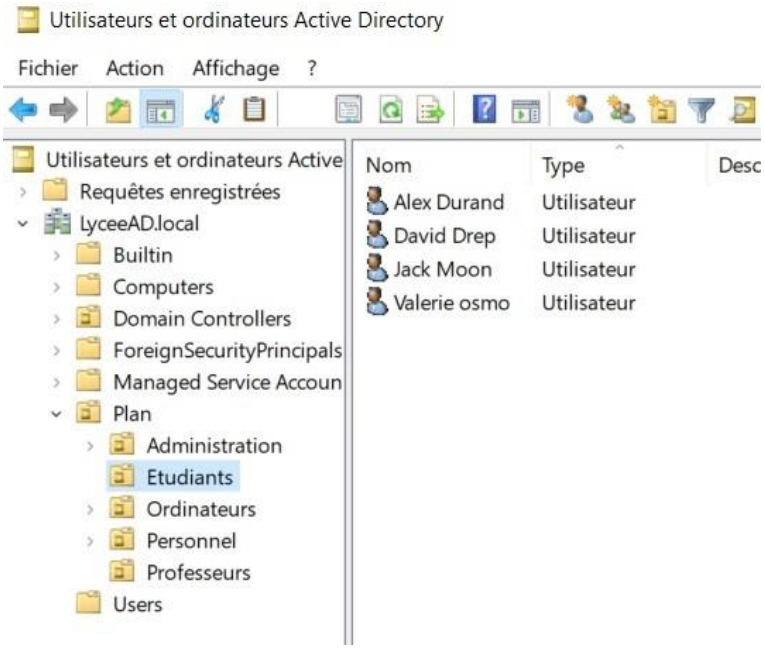


Image 7 *: Une liste exemple des utilisateur Etudiants et le UO séparé par groupes d'identification*

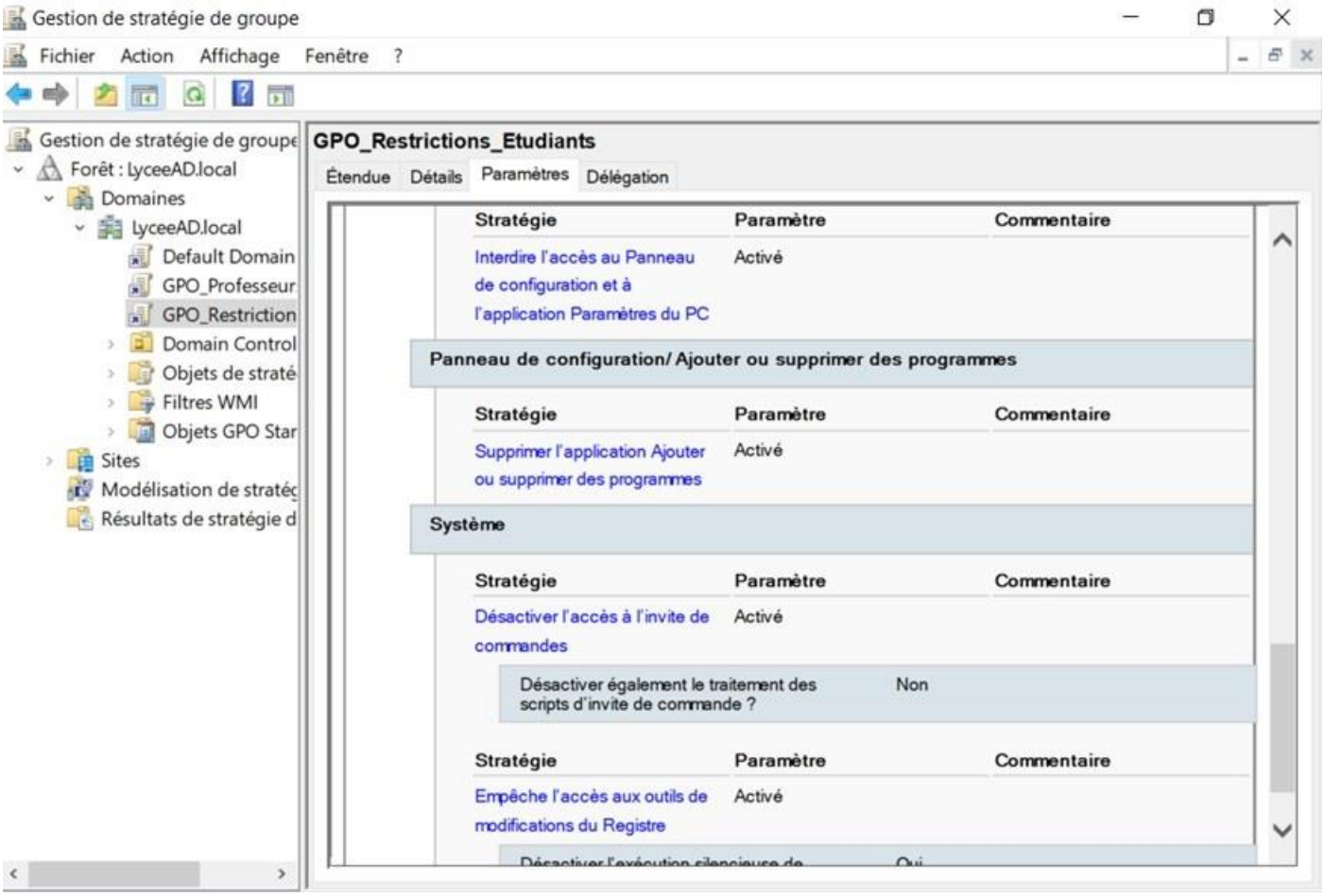


Image 8 *: Règles Stratégie de Groupe (GPO) affecté pour les étudiant pour une sécurité majeure du Système d'informations*

Sécurisation des services

Les services réseau sont sécurisés par différentes mesures complémentaires :

- limitation des services exposés en DMZ,
- utilisation de protocoles sécurisés, tels que SFTP pour les échanges de fichiers,
- restriction des accès aux serveurs internes depuis les postes clients.

Les serveurs internes ne sont pas accessibles directement depuis Internet, ce qui réduit fortement les risques d'intrusion. La DMZ joue ainsi un rôle essentiel de zone tampon entre l'extérieur et le réseau interne.

Protection des données et sauvegardes

La protection des données constitue un importante tache de la sécurité du système d'information. Les données stockées sur le serveur de fichiers font l'objet de sauvegardes régulières vers un NAS dédié. Cette politique de sauvegarde permet :

- de prévenir les pertes de données,
- de restaurer rapidement les services en cas d'incident,
- de garantir la continuité de service.

La séparation entre les serveurs de production et les équipements de sauvegarde renforce la résilience de l'infrastructure.

Démarche éco-responsable de l'infrastructure

Optimisation de la consommation énergétique

L'architecture vise à limiter la consommation énergétique par une centralisation des équipements dans un bâtiment informatique unique. Cette organisation permet de réduire la dispersion du matériel, d'optimiser l'alimentation électrique et de simplifier la gestion du refroidissement.

La limitation du nombre de serveurs physiques, contribue également à une meilleure efficacité énergétique. Cette approche permet de réduire la consommation électrique globale tout en facilitant l'administration du système d'information.

Gestion durable de l'infrastructure

La démarche éco-responsable passe également par une gestion durable de l'infrastructure informatique. La centralisation des services facilite la maintenance, limite les déplacements techniques et contribue à l'allongement de la durée de vie des équipements.

La mise en place de sauvegardes centralisées et d'une organisation structurée permet de réduire les risques de perte de données et d'éviter des remplacements matériels inutiles. Enfin, l'infrastructure est conçue pour être évolutive, permettant l'ajout de nouveaux services ou utilisateurs sans nécessiter une refonte complète du système.

Tests, validation et limites

Une fois l'architecture réseau définie et les solutions techniques mises en œuvre, il est nécessaire de procéder à des **tests de fonctionnement et de sécurité** afin de valider la cohérence et la fiabilité de l'infrastructure proposée. Cette phase permet également d'identifier les limites du projet dans le contexte étudié.

Tests de fonctionnement

Des tests de fonctionnement ont été réalisés afin de vérifier le bon fonctionnement global du réseau et des services mis en place. Ces tests ont permis de valider :

- l'accès des postes clients au réseau interne,
- l'authentification des utilisateurs via Active Directory,
- l'attribution automatique des adresses IP,
- la résolution des noms grâce au service DNS,
- l'accès aux ressources partagées sur le serveur de fichiers.

Les résultats de ces tests confirment que l'architecture permet une utilisation normale des services par les différents utilisateurs du lycée, dans des conditions conformes aux besoins identifiés.

Tests de sécurité

Des tests de sécurité ont également été effectués afin de vérifier l'efficacité des mécanismes de protection mis en place. Ils ont notamment permis de valider :

- le filtrage des flux réseau par le pare-feu pfSense, **[Image5** et **Image6]**
- l'impossibilité d'un accès direct depuis Internet vers le réseau interne,
- l'isolement de la DMZ par rapport au LAN, [**Image9**]
- la restriction des accès aux services internes.

Ces tests montrent que la segmentation du réseau et les règles de filtrage permettent de limiter les risques d'intrusion et de protéger efficacement le système d'information.

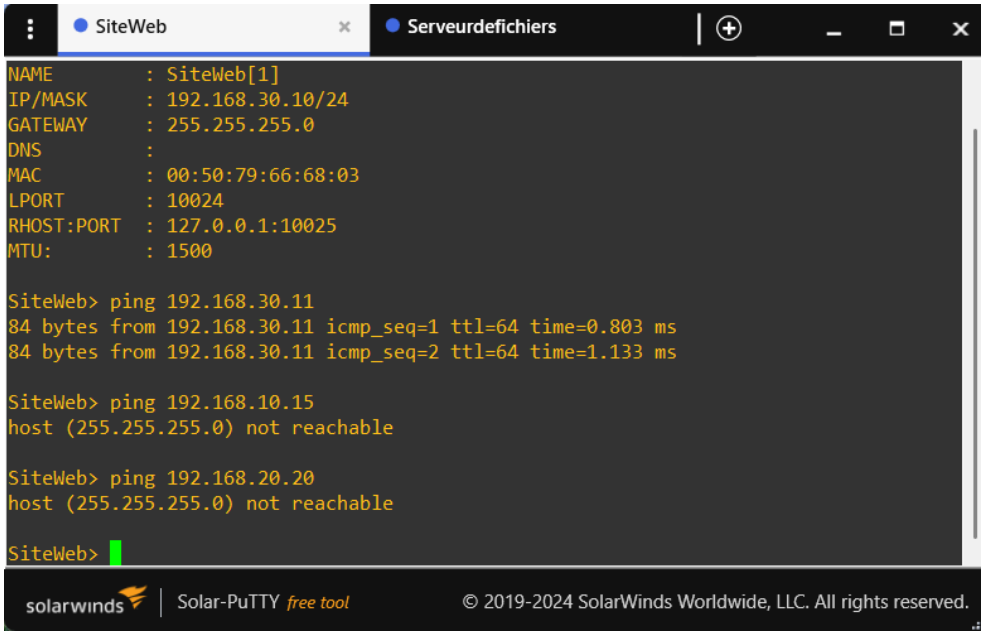


Image 9 *: Test Connexion entre le DMZ , FTP, et blocaque de connexion au Serveur des fichiers*

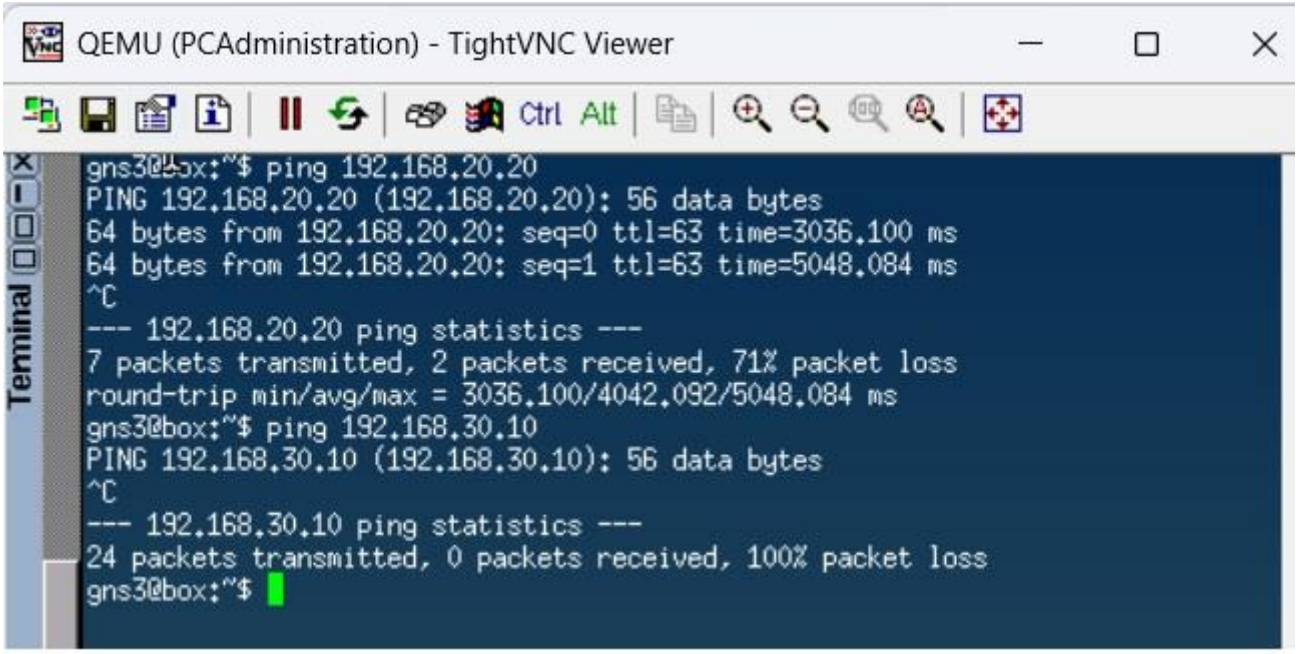


Image 10 *: Test Connexion entre le PC des Administration qui communique avec le serveur de fichiers mais bloque le connexion au DMZ*

Les tests réalisés permettent de valider la **cohérence globale de l'architecture réseau**.
L'infrastructure proposée est adaptée à un établissement scolaire, tant du point de vue de la gestion des utilisateurs que de la maintenance et de l'évolutivité.

Limites du projet

Malgré les résultats satisfaisants obtenus, y a des **limites** car le projet repose sur une architecture théorique simulée. Enfin, le projet ne prend pas en compte l'ensemble des aspects liés à la haute disponibilité ou à la redondance complète des équipements.

Conclusion : Évolutions possibles de l'infrastructure

L'architecture réseau proposée répond aux besoins actuels de l'établissement, cependant elle a été conçue de manière **évolutive** afin de pouvoir s'adapter à de futures contraintes techniques, pédagogiques et organisationnelles.

Renforcement de la sécurité

Une première évolution possible concerne le renforcement des mécanismes de sécurité. Il serait envisageable de mettre en place :

- un système de **détection et de prévention d'intrusion (IDS/IPS)**,
- une gestion plus fine des journaux et des alertes de sécurité,
- une politique de mots de passe renforcée et des stratégies de groupe plus avancées.

Haute disponibilité et continuité de service

Afin d'améliorer la continuité de service, des solutions de **redondance** pourraient être mises en œuvre. Cela inclut :

- la redondance du pare-feu,
- la duplication de certains serveurs critiques,
- l'amélioration des stratégies de sauvegarde avec des sauvegardes externalisées.

Optimisation des performances réseau

L'infrastructure pourrait également évoluer vers une optimisation des performances, notamment par :

- l'amélioration des liaisons inter-bâtiments,
- la mise en place de VLAN supplémentaires,
- l'optimisation de la gestion de la bande passante.

Renforcement des solutions écologiques

Dans une logique de continuité avec la démarche éco-responsable, l'infrastructure pourrait évoluer vers une meilleure efficacité énergétique. Cela inclut :

- l'extension de l'installation photovoltaïque,
- l'utilisation d'équipements encore plus économes en énergie,
- une meilleure gestion de l'alimentation et du refroidissement des serveurs.