Institut National de Radioélectricité et de Cinématographie

Enseignement technique secondaire de qualification

Accès aux études supérieures



Avenue Jupiter, 188

1190 Forest

Gestion d’un parc informatique

Projet personnel de Kaba Ibrahima.

Pour l’obtention du certificat de qualification

Technicien en informatique

Année scolaire : 2025-2026

Remerciement :

Avant d’entamer ce rapport, je tiens à exprimer ma profonde gratitude envers les personnes qui m’ont soutenu et accompagné tout au long de ce projet.

Mes remerciements s’adressent tout d’abord à mon tuteur, Monsieur Kajjoua, ainsi qu’à Monsieur Mdiker. Je les remercie chaleureusement pour leur grande disponibilité et leurs précieux conseils. Leur guidance m’a permis de garder le cap et de ne jamais m’écarter de l’objectif réel de mon travail.

Je souhaite également remercier mes camarades de classe pour leur soutien et leur aide constante. Le partage de leurs composants électroniques ainsi que nos échanges techniques ont été essentiels à la réalisation concrète de ce projet.

Ma reconnaissance va aussi à mes professeurs d’informatique pour leur accompagnement technique, ainsi qu'à mes professeurs de cours généraux. Je les remercie d'avoir cru en moi et de m'avoir encouragé sans relâche, malgré mes périodes de baisse de régime.

Enfin, je remercie mes parents pour leur soutien moral indéfectible et pour avoir activement cherché avec moi des idées afin d'enrichir ce travail.

Table des matières

Remerciement : 2

Introduction 6

Objectif du TFE 6

Explication de quelque notion : 7

GNS3 : 7

VMware Workstation 7

Windows Server 8

Active Directory 8

DNS 8

DHCP 9

FTP 9

PfSense 9

Portail captif 10

FreeRADIUS 10

Google Authenticator — Double Authentification (2FA) 10

GPO (Group Policy Objects) 11

Microsoft Power Apps 11

Présentation rapide de la solution 12

Analyse des besoins 13

Public cible et utilisateurs 13

Cahier des charges 13

Matériels utilisés : 13

Le projet doit répondre aux exigences suivantes : 14

Étude préalable 15

Solutions existantes : 15

Choix technologiques : 15
Conception du projet 16
Architecture générale : 16
Plan d'adressage IP 16
Topologie réseau : 17
Réalisation 18
Infrastructure réseau (GNS3) : 18
Configuration du routeur Cisco c3620 : 18
Windows Server — Active Directory, DNS, DHCP, FTP 19
Active directory: 19
Service DNS : 20
Service DHCP : 20
Service FTP : 21
PfSense — Firewall et Portail Captif 22
Configuration des interfaces : 22
Règles de firewall : 22
Portail Captif : 23
Authentification à deux facteurs (2FA) 24
FreeRADIUS : 24
Google Authenticator (OTP) : 24
Stratégies de groupe (GPO) 25
Politique de mot de passe : 25
Verrouillage de compte : 25
Restrictions sur les postes clients : 25
Application de ticketing (Power Apps) 26
Tests et validation 27
Tests de connectivité réseau : 27

Tests des services : 28
Difficultés rencontrées et solutions 29
Conclusion 30
Bibliographie / Webographie 31
Documentation officielle 31
Annexes 32
Configuration du routeur Cisco c3620 et captures d'écran des explications cité ci-dessus : 32
Sites internet 39

Introduction

Dans un monde où la transformation numérique s'accélère, la gestion et la sécurisation des infrastructures informatiques sont devenues des enjeux majeurs pour toute organisation. Les entreprises, écoles et institutions font face à des défis croissants : comment gérer efficacement un parc informatique, garantir la sécurité des accès réseau, et assurer la continuité des services tout en protégeant les données sensibles ?

C'est dans ce contexte que s'inscrit mon Travail de Fin d'Études, réalisé dans le cadre de ma 6ème année TQ Informatique à l'INRACI.

Comment concevoir, déployer et sécuriser une infrastructure informatique complète simulant un environnement d'entreprise réel, intégrant la gestion des utilisateurs, la sécurisation des accès réseau, et un système de ticketing pour la gestion des incidents.

Objectif du TFE

Mon projet vise à mettre en place un système complet de gestion de parc informatique ("Gestion de Parc Informatique") qui intègre les éléments suivants :

- La simulation d'un réseau d'entreprise avec GNS3 (routeur Cisco, switch, firewall)
- La gestion centralisée des utilisateurs via Active Directory sur Windows Server
- La sécurisation des accès réseau avec PfSense (firewall, portail captif, A2F)
- La mise en place de politiques de sécurité via les GPO
- Un système de ticketing IT développé avec Microsoft Power Apps

Explication de quelque notion :

GNS3 :

GNS3 (Graphical Network Simulator 3) est un logiciel gratuit qui permet d'émuler des équipements réseau réels comme des routeurs et switches Cisco, sans avoir besoin du matériel physique. Contrairement à un simulateur qui imite le comportement, un émulateur reproduit exactement le fonctionnement réel de l'équipement en utilisant les vraies images IOS Cisco.

Pourquoi je l'ai choisi **?** GNS3 est largement utilisé dans le monde professionnel et par les étudiants en informatique. Il est gratuit et compatible avec les vraies images IOS Cisco, ce qui permet de faire de vraies configurations réseau.

Son rôle dans mon projet GNS3 émule le réseau de l'entreprise avec un routeur Cisco c3620, un switch et un NAT pour la sortie internet.

VMware Workstation

VMware Workstation est un logiciel de virtualisation qui permet de faire tourner plusieurs systèmes d'exploitation en même temps sur un seul PC. Chaque système fonctionne dans une "machine virtuelle" isolée.

Pourquoi je l'ai choisi ? VMware est le standard de l'industrie pour la virtualisation. Il s'intègre parfaitement avec GNS3 grâce aux interfaces VMnet qui permettent aux machines virtuelles de communiquer avec les équipements réseau simulés.

Son rôle dans mon projet VMware fait tourner simultanément Windows Server, PfSense et les machines clientes Windows sur mon PC.

Windows Server

Windows Server est un système d'exploitation développé par Microsoft, spécialement conçu pour les serveurs d'entreprise. Contrairement à Windows classique destiné aux particuliers, Windows Server offre des services avancés comme la gestion centralisée des utilisateurs, le partage de fichiers et la gestion du réseau.

Pourquoi je l'ai choisi ? Windows Server est le système le plus utilisé dans les entreprises belges et européennes. Sa maîtrise est indispensable pour tout technicien informatique.

Son rôle dans mon projet Windows Server héberge les services principaux de l'infrastructure : Active Directory, DNS, DHCP et FTP.

Active Directory

Active Directory est un service de Microsoft qui permet de gérer de façon centralisée tous les utilisateurs, ordinateurs et ressources d'un réseau d'entreprise. C'est comme un annuaire téléphonique numérique qui contient toutes les informations sur qui peut accéder à quoi.

Pourquoi je l'ai choisi ? Active Directory est le standard absolu en entreprise pour la gestion des identités. Il permet à un administrateur de gérer des centaines d'utilisateurs depuis un seul endroit.

Son rôle dans mon projet Active Directory gère les comptes utilisateurs du domaine Ibrahim.loc. Les utilisateurs se connectent avec leurs identifiants AD sur les machines clientes et accèdent aux ressources réseau selon leurs droits.

DNS

Le DNS (Domain Name System) est le système qui traduit les noms de domaine lisibles par les humains (comme google.com) en adresses IP compréhensibles par les machines (comme 142.250.74.46). Sans DNS, il faudrait retenir des adresses IP pour accéder à chaque site.

Son rôle dans mon projet Le serveur DNS résout le nom de domaine interne Ibrahim.loc vers l'adresse IP du serveur (192.168.1.2), permettant aux machines du réseau de se trouver par leur nom plutôt que par leur adresse IP.

DHCP

Le DHCP (Dynamic Host Configuration Protocol) est un service qui attribue automatiquement des adresses IP aux machines qui se connectent au réseau. Sans DHCP, il faudrait configurer manuellement l'adresse IP de chaque ordinateur.

Son rôle dans mon projet Le serveur DHCP distribue automatiquement les adresses IP dans la plage 192.168.1.10 à 192.168.1.100 aux machines clientes qui rejoignent le réseau, ainsi que la passerelle et le serveur DNS.

FTP

Le FTP (File Transfer Protocol) est un protocole réseau permettant le transfert de fichiers entre un client et un serveur. C'est comme une clé USB partagée accessible depuis n'importe quelle machine du réseau.

Son rôle dans mon projet Le serveur FTP permet aux utilisateurs du groupe INRACI_Company de déposer et récupérer des fichiers depuis n'importe quelle machine du réseau en s'authentifiant avec leurs identifiants Active Directory.

PfSense

PfSense est un pare-feu open-source basé sur FreeBSD. Un pare-feu est un système de sécurité qui contrôle le trafic réseau entrant et sortant selon des règles définies par l'administrateur. PfSense est utilisé dans de nombreuses entreprises comme alternative gratuite aux pare-feux commerciaux coûteux.

Pourquoi je l'ai choisi ? PfSense est gratuit, très complet et largement utilisé en entreprise. Il offre de nombreuses fonctionnalités avancées comme le portail captif, le VPN et le filtrage DNS.

Son rôle dans mon projet PfSense sécurise le réseau en filtrant le trafic selon des règles précises, et sert de passerelle pour les utilisateurs qui doivent s'authentifier via le portail captif avant d'accéder à internet.

Portail captif

Un portail captif est une page web qui s'affiche automatiquement quand un utilisateur essaie d'accéder à internet depuis un réseau. L'utilisateur doit s'identifier avant d'être autorisé à naviguer. On retrouve ce système dans les hôtels, aéroports et restaurants qui proposent un WiFi public.

Son rôle dans mon projet Le portail captif intercepte tout le trafic HTTP des utilisateurs non authentifiés et les redirige vers une page de connexion. Une fois authentifiés, ils peuvent accéder à internet normalement.

FreeRADIUS

FreeRADIUS est un serveur d'authentification open-source. RADIUS (Remote Authentication Dial-In User Service) est un protocole standard utilisé pour vérifier l'identité des utilisateurs qui se connectent à un réseau. C'est le système qui reçoit les identifiants et vérifie si l'accès doit être accordé ou refusé.

Son rôle dans mon projet FreeRADIUS est installé sur PfSense et reçoit les demandes d'authentification du portail captif. Il vérifie le nom d'utilisateur, le PIN et le code Google Authenticator avant d'accorder l'accès au réseau.

Google Authenticator — Double Authentification (2FA)

La double authentification (2FA) est un mécanisme de sécurité qui demande à l'utilisateur de prouver son identité de deux façons différentes : quelque chose qu'il connaît (son mot de passe) et quelque chose qu'il possède (son téléphone). Google Authenticator est une application mobile qui génère un code à 6 chiffres qui change toutes les 30 secondes.

Pourquoi c'est important ? Même si un attaquant vole le mot de passe d'un utilisateur, il ne peut pas se connecter sans avoir également accès à son téléphone. Cela renforce considérablement la sécurité du réseau.

Son rôle dans mon projet Chaque utilisateur doit entrer son PIN suivi du code affiché par Google Authenticator sur son téléphone pour accéder au réseau via le portail captif.

GPO (Group Policy Objects)

Les GPO (objets de stratégie de groupe) sont des règles de sécurité et de configuration appliquées automatiquement à tous les ordinateurs et utilisateurs d'un domaine Active Directory. L'administrateur définit ces règles une seule fois et elles s'appliquent à toutes les machines sans intervention manuelle.

Son rôle dans mon projet La GPO nommée GPO-Securite-INRACI applique plusieurs restrictions sur les postes clients : politique de mots de passe forts, verrouillage de compte après 3 tentatives échouées, et blocage de l'accès au panneau de configuration, au CMD et à l'éditeur de registre pour les utilisateurs standards.

Microsoft Power Apps

Microsoft Power Apps est une plateforme de développement d'applications sans code (ou avec peu de code) développée par Microsoft. Elle permet de créer des applications métier connectées à des sources de données comme SharePoint, Excel ou Teams, sans avoir besoin d'être un développeur professionnel.

Son rôle dans mon projet Power Apps a été utilisé pour créer une application de ticketing IT permettant aux utilisateurs de soumettre des incidents et aux administrateurs de les gérer. L'application est connectée à une liste SharePoint comme base de données et envoie des notifications par email via Power Automate.

Présentation rapide de la solution

La solution développée repose sur une architecture virtualisée combinant VMware Workstation pour les machines virtuelles (Windows Server, PfSense, clients Windows) et GNS3 pour l’émulation des équipements réseau Cisco. L'ensemble forme un environnement complet et fonctionnel simulant le réseau d'une entreprise ou d’une école.

Analyse des besoins

L'INRACI, comme toute institution scolaire moderne, dispose d'un parc informatique composé de nombreuses machines, utilisateurs et ressources réseau. La gestion de cet environnement nécessite des outils adaptés permettant de contrôler les accès, gérer les incidents, et sécuriser les communications.

Mon projet simule cette problématique en créant un environnement représentatif d'une entreprise de taille moyenne, avec des rôles distincts (administrateurs et utilisateurs standards), des ressources partagées (serveur de fichiers FTP, domaine Active Directory) et une infrastructure réseau sécurisée.

Public cible et utilisateurs

Le système est destiné à deux types d'utilisateurs :

- Les administrateurs IT : ils gèrent le réseau, les utilisateurs, les politiques de sécurité et traitent les tickets d'incident.
- Les utilisateurs standards : ils accèdent aux ressources réseau via le portail captif et soumettent des tickets en cas de problème.

Cahier des charges

Matériels utilisés :

Matériel	Description	Prix
PC personnel	AMD R5 7600, 32G ram, SSD nvme 1to, RTX 4060	1500€

Le projet doit répondre aux exigences suivantes :

Exigence	Description
Réseau simulé	Topologie avec routeur Cisco, switch, firewall PfSense via GNS3
Gestion des utilisateurs	Active Directory avec domaine Ibrahim.loc, groupes et OU
Services réseau	DNS, DHCP, FTP configurés sur Windows Server
Sécurité réseau	Firewall PfSense avec règles, portail captif et A2F
Politiques de sécurité	GPO pour restreindre les accès sur les postes clients
Gestion des incidents	Application Power Apps de ticketing connectée à SharePoint

Contraintes techniques

- Utilisation exclusive de logiciels libres ou disponibles via la licence scolaire
- Simulation sur un PC puissant (AMD Ryzen 5 7600, 32 Go RAM) pour exécuter plusieurs VMs simultanément
- Compatibilité entre VMware Workstation et GNS3 pour la communication entre VMs et équipements réseau simulés

Étude préalable

Solutions existantes :

Plusieurs solutions existent pour la gestion de parc informatique en entreprise : Microsoft Endpoint Manager (Intune), OCS Inventory. Ces solutions sont généralement coûteuses et nécessitent une infrastructure existante. Pour un environnement scolaire et de simulation, il est plus pertinent de construire soi-même l'infrastructure de zéro afin de comprendre chaque composant.

Choix technologiques :

Technologie	Rôle	Justification
Windows Server 2019	AD, DNS, DHCP, FTP	Standard en entreprise, intégration native avec les clients Windows
GNS3	Émulation réseau Cisco	Outil professionnel gratuit, supporte les images IOS Cisco
PfSense	Firewall & portail captif	Solution open-source professionnelle, très utilisée en entreprise
VMware Workstation	Virtualisation	Permet de faire tourner plusieurs OS simultanément
Microsoft Power Apps	Ticketing	Disponible via licence scolaire, intégration facile avec SharePoint
FreeRADIUS	Authentification 2FA	Standard de l'industrie pour l'authentification réseau
Google Authenticator	OTP (2FA)	Application mobile gratuite, standard TOTP

Conception du projet

Architecture générale :

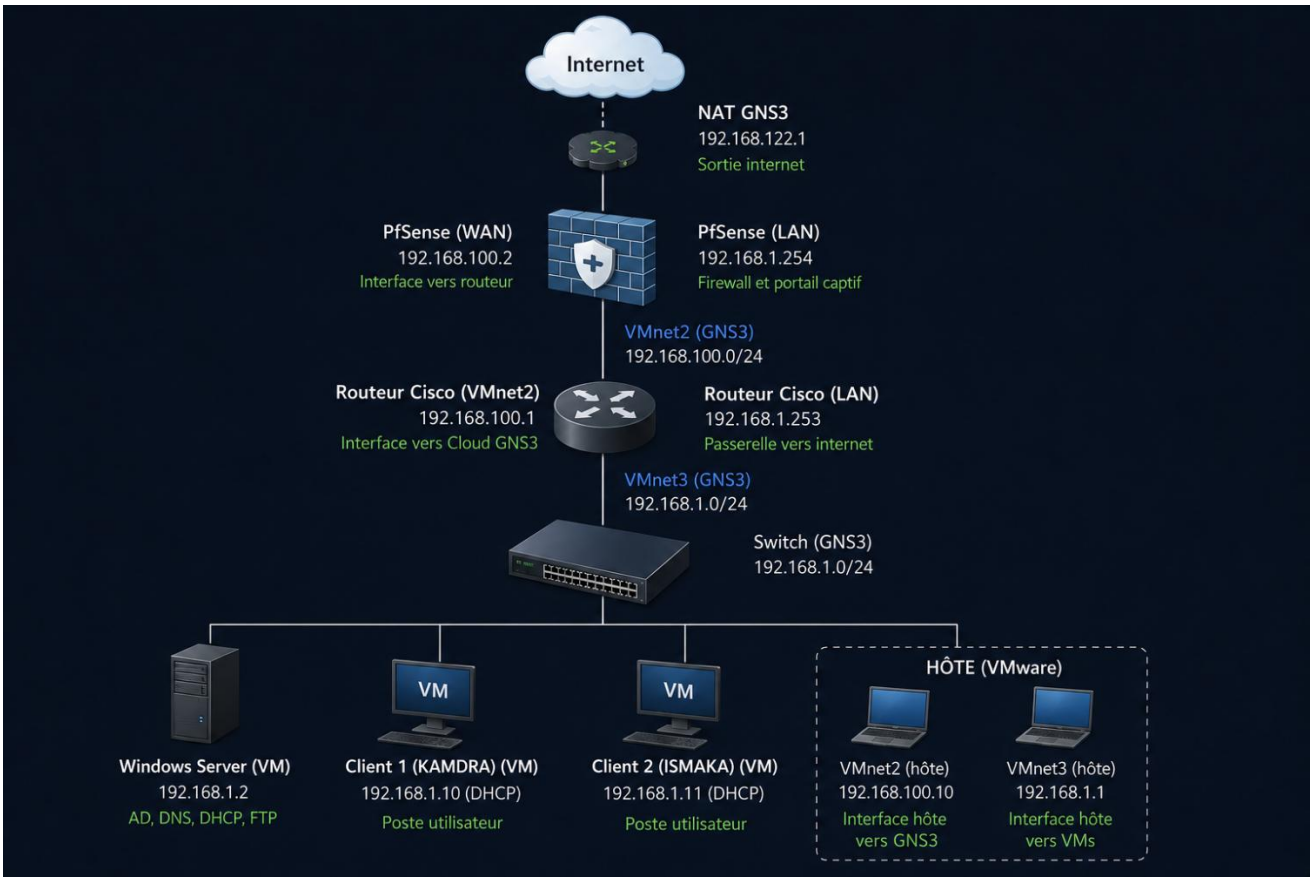
L'infrastructure est organisée en plusieurs zones réseau distinctes, chacune avec un rôle spécifique :

- Zone WAN : connexion internet via le NAT de GNS3
- Zone DMZ : connexion entre le Cloud VMnet2 et le routeur Cisco
- Zone LAN : réseau interne 192.168.1.0/24 où se trouvent tous les serveurs et clients

Plan d'adressage IP

Équipement	Adresse IP	**Rôle**
Routeur Cisco (LAN)	192.168.1.253	Passerelle vers internet
Routeur Cisco (VMnet2)	192.168.100.1	Interface vers Cloud GNS3
PfSense (LAN)	192.168.1.254	Firewall et portail captif
PfSense (WAN)	192.168.100.2	Interface vers routeur
Windows Server	192.168.1.2	AD, DNS, DHCP, FTP
Client 1 (KAMDRA)	192.168.1.10 (DHCP)	Poste utilisateur
Client 2 (ISMAKA)	192.168.1.11 (DHCP)	Poste utilisateur
NAT GNS3	192.168.122.1	Sortie internet
VMnet2 (hôte)	192.168.100.10	Interface hôte vers GNS3
VMnet3 (hôte)	192.168.1.1	Interface hôte vers VMs

Topologie réseau :

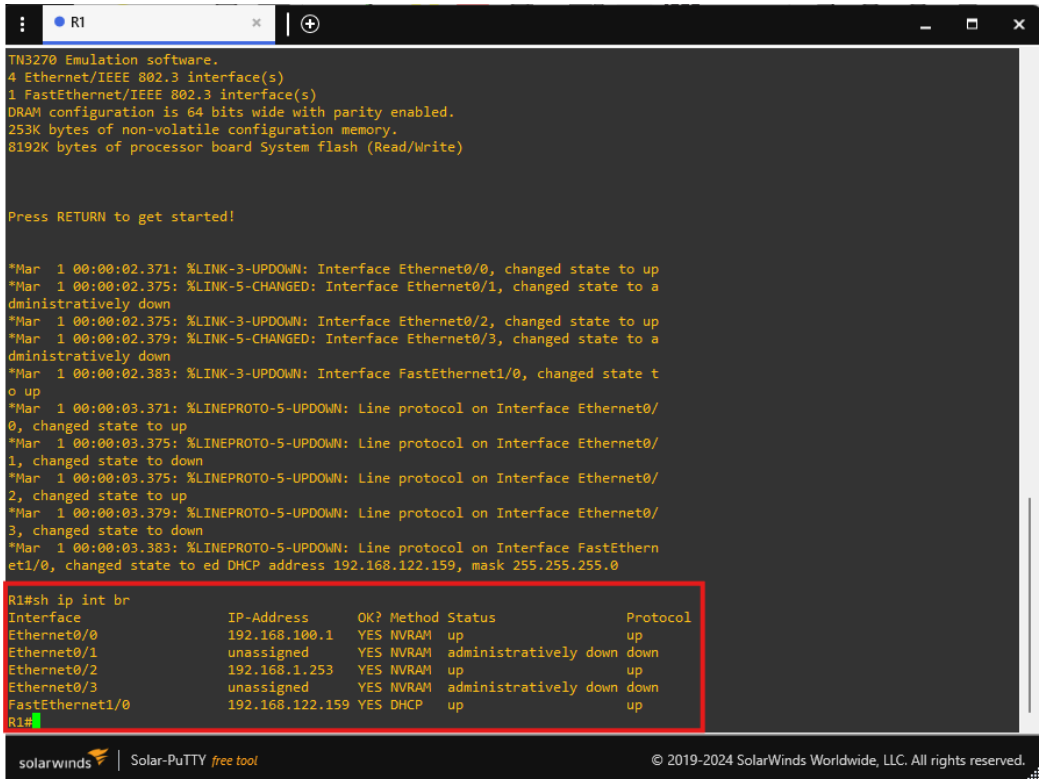


Réalisation

Infrastructure réseau (GNS3) :

Configuration du routeur Cisco c3620 :

Le routeur Cisco c3620 a été configuré avec trois interfaces actives. L'interface Ethernet0/0 est connectée au Cloud VMnet2 avec l'adresse IP 192.168.100.1/24, permettant la communication avec PfSense. L'interface Ethernet0/2 est connectée au Switch avec l'adresse IP 192.168.1.253/24, servant de passerelle pour le réseau LAN. L'interface FastEthernet1/0 obtient son adresse IP via DHCP depuis le NAT GNS3 (192.168.122.0/24) pour la sortie internet.

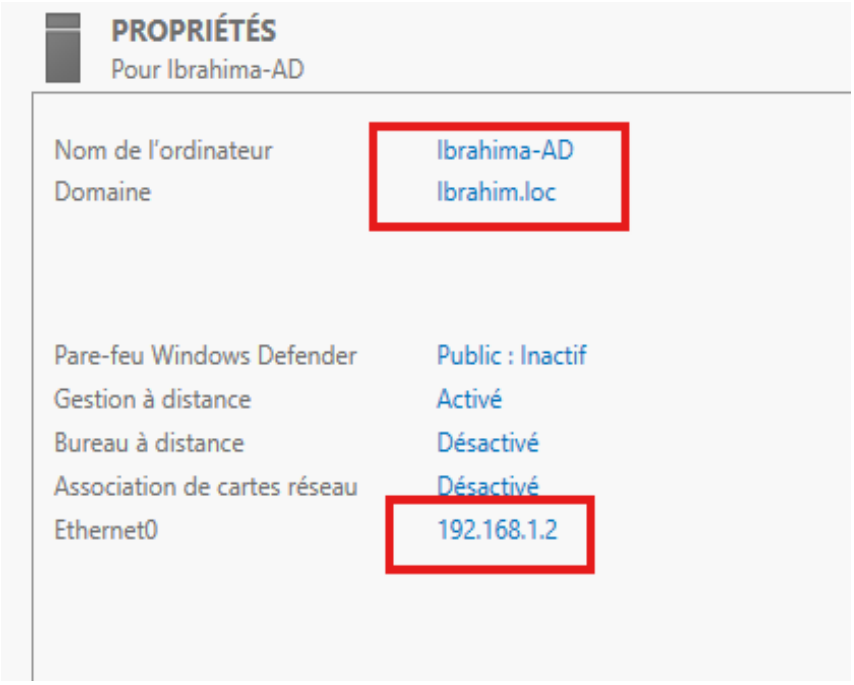


La configuration NAT (PAT) a été mise en place pour permettre aux machines du réseau interne d'accéder à internet via l'interface FastEthernet1/0. Une liste d'accès autorise les sous-réseaux 192.168.1.0/24 et 192.168.100.0/24.

Windows Server — Active Directory, DNS, DHCP, FTP

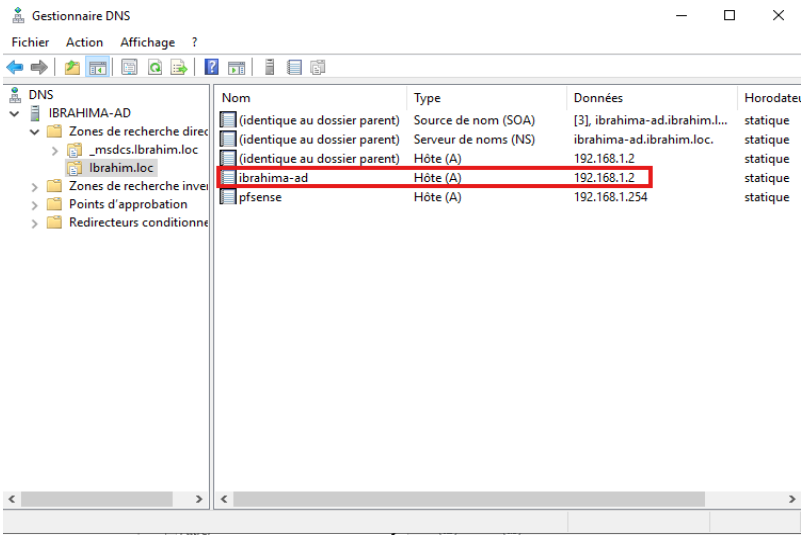
Active directory:

Un domaine Active Directory nommé Ibrahim.loc a été créé sur Windows Server 2019. Les utilisateurs du projet (KAMDRA, ISMAKA) ont été créés dans ce domaine et organisés dans des unités d'organisation (OU). Un groupe de sécurité INRACI_Company a été créé pour regrouper les utilisateurs ayant accès aux ressources partagées.



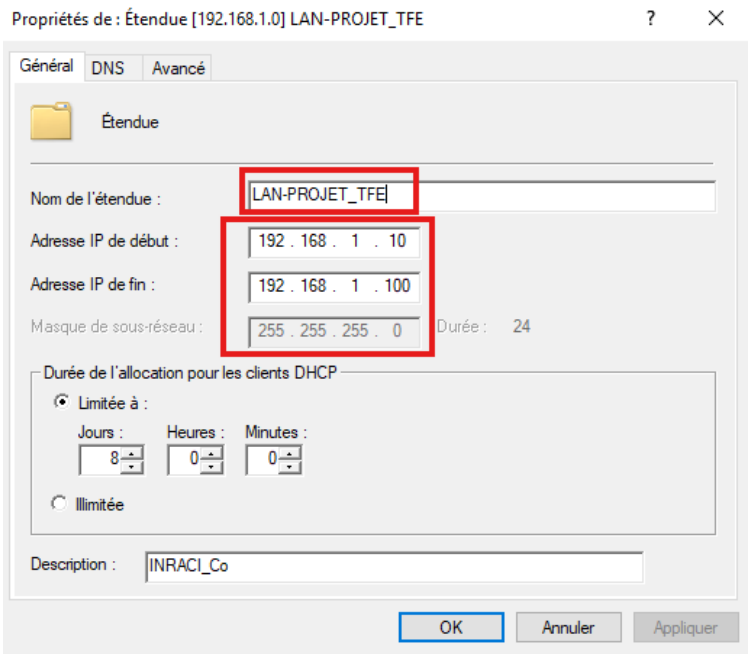
Service DNS :

Le service DNS a été configuré pour résoudre le nom de domaine Ibrahim.loc vers l'adresse IP 192.168.1.2 du serveur. Une zone de recherche directe a été créée avec les enregistrements A nécessaires. Le service écoute sur l'adresse IP 192.168.1.2.



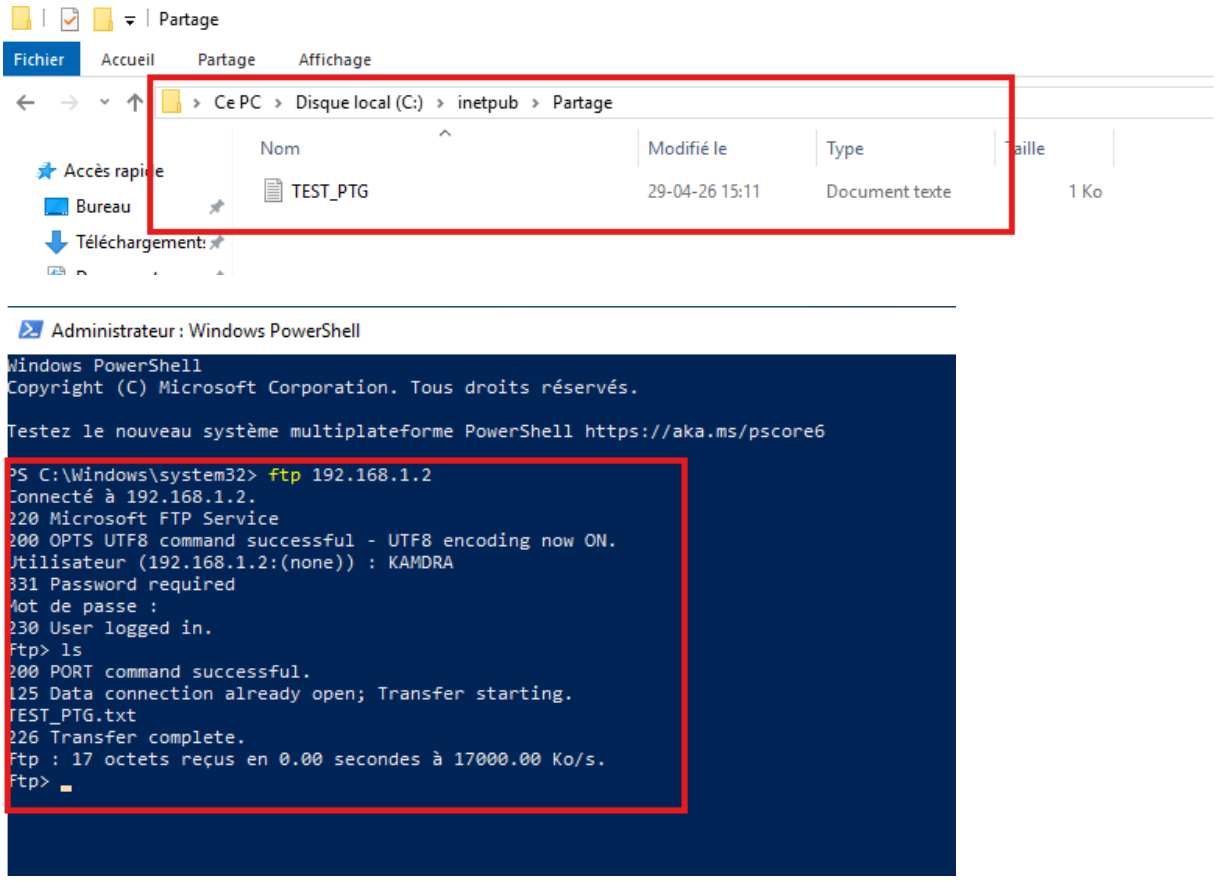
Service DHCP :

Une étendue DHCP nommée LAN-Projet a été configurée pour distribuer automatiquement des adresses IP dans la plage 192.168.1.10 à 192.168.1.100. La passerelle par défaut distribuée aux clients est 192.168.1.254 (PfSense) et le serveur DNS est 192.168.1.2 (Windows Server).



Service FTP :

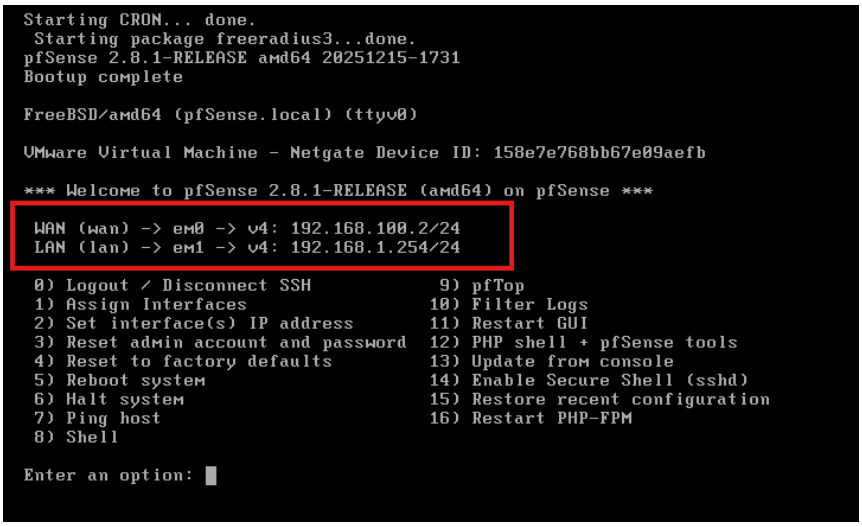
Un site FTP nommé ftpibra a été configuré via IIS Manager sur l'adresse IP 192.168.1.2 port 21. L'authentification de base est activée et le dossier partagé se trouve dans C:\inetpub\ftproot. Le groupe INRACI_Company dispose des permissions de lecture et d'écriture sur ce dossier. L'isolation des utilisateurs a été désactivée pour permettre un accès commun aux dossiers partagés.



PfSense — Firewall et Portail Captif

Configuration des interfaces :

PfSense est configuré avec deux interfaces réseau. L'interface WAN (em0) est connectée à VMnet2 avec l'adresse IP statique 192.168.100.2/24 et une passerelle vers le routeur Cisco (192.168.100.1). L'interface LAN (em1) est connectée à VMnet3 avec l'adresse IP 192.168.1.254/24.



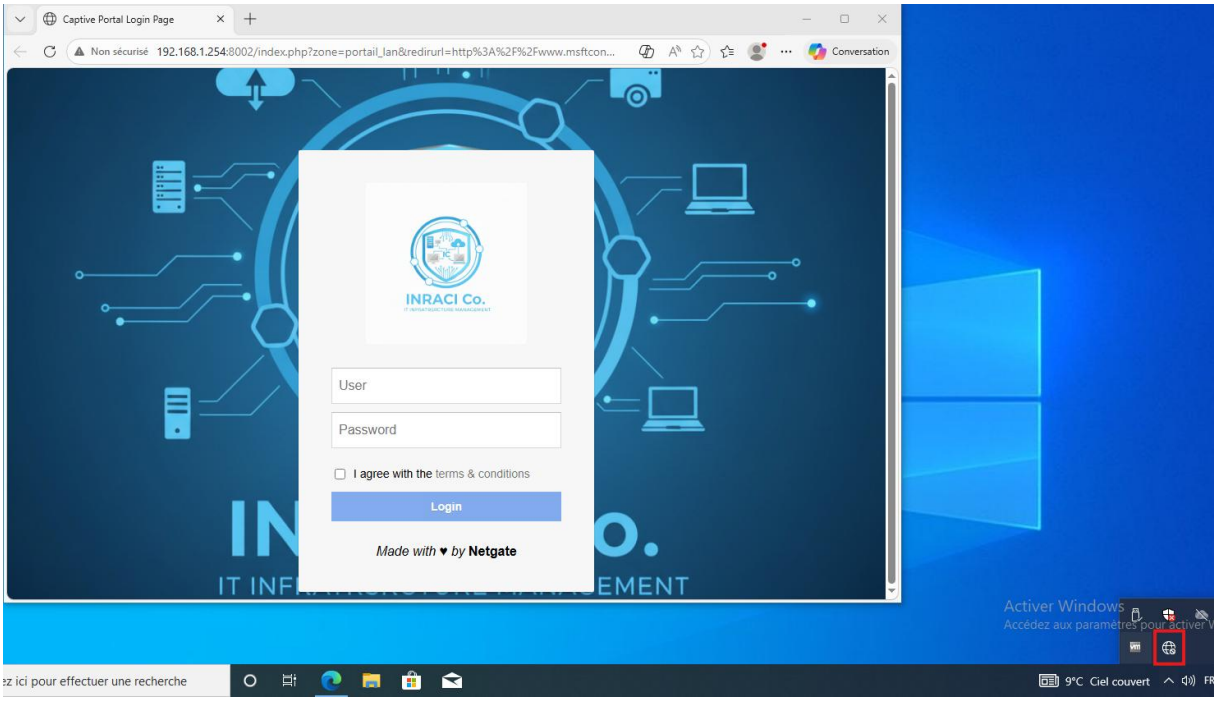
Règles de firewall :

Les règles suivantes ont été configurées sur l'interface LAN, dans l'ordre d'application :

- Anti-Lockout Rule (règle système, non modifiable)
- Autoriser FTP : TCP depuis LAN subnet vers 192.168.1.2 port 21
- Autoriser DNS : TCP/UDP depuis LAN subnet vers 192.168.1.2 port 53
- Autoriser HTTP/HTTPS : TCP depuis LAN subnet vers 192.168.1.2 ports 80-443
- Autoriser tout le trafic LAN : toutes les adresses
- Bloquer tout le reste : règle de refus par défaut en fin de liste

Portail Captif :

Un portail captif nommé portail_lan a été configuré sur l'interface LAN. Il intercepte tout le trafic HTTP des utilisateurs non authentifiés et les redirige vers une page de connexion personnalisée aux couleurs de l'INRACI. L'authentification est assurée par FreeRADIUS avec la méthode PAP.



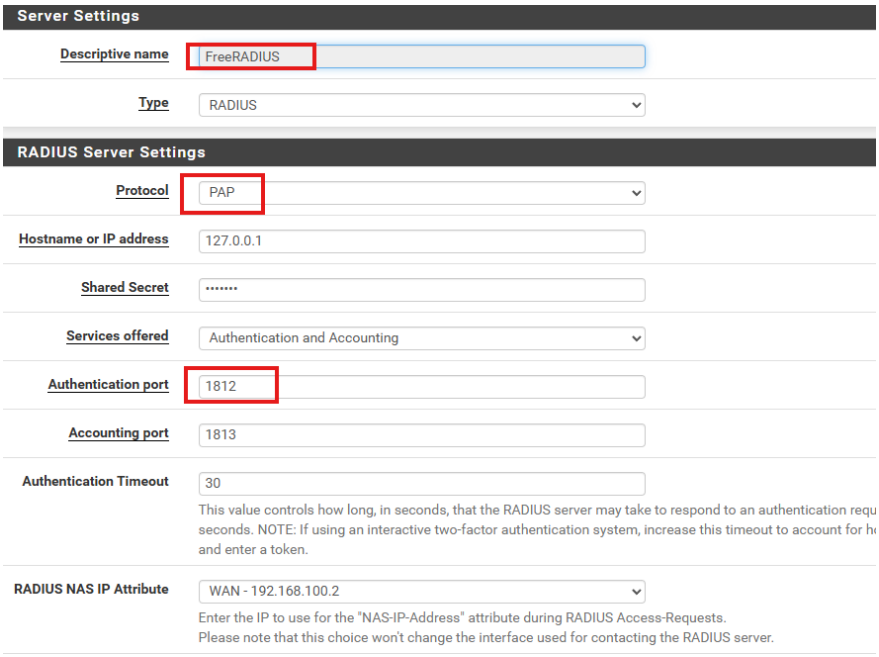
(On peut voir que tant qu'il ne s'est pas connecter sur le portail captif l'utilisateur n'a pas internet)

Authentification à deux facteurs (2FA)

Le système de double authentification a été mis en place en utilisant FreeRADIUS installé sur PfSense et Google Authenticator sur les appareils mobiles des utilisateurs.

FreeRADIUS :

FreeRADIUS a été installé via le gestionnaire de packages de PfSense. Il est configuré pour écouter sur 192.168.1.254 port 1812 en protocole PAP. Un client NAS localhost (127.0.0.1) avec le secret partagé 'pfsense' a été configuré pour permettre au portail captif de s'authentifier auprès de FreeRADIUS.



Google Authenticator (OTP) :

Chaque utilisateur est configuré dans FreeRADIUS avec l'option One-Time Password activée en mode Google Authenticator (TOTP). Un QR Code est généré pour chaque utilisateur et scanné avec l'application Google Authenticator sur leur téléphone. Lors de la connexion au portail captif, l'utilisateur doit entrer son PIN suivi du code à 6 chiffres affiché par Google Authenticator.

Ce mécanisme garantit que même si un mot de passe est compromis, l'attaquant ne peut pas accéder au réseau sans également disposer du téléphone de l'utilisateur.

Stratégies de groupe (GPO)

Une stratégie de groupe nommée GPO-Securite-INRACI a été créée et liée au domaine Ibrahim.loc. Elle comprend les paramètres de sécurité suivants :

Politique de mot de passe :

- Longueur minimale : 8 caractères

Complexité requise : majuscules, minuscules, chiffres et caractères spéciaux

- Durée de vie maximale : 90 jours
- Historique des mots de passe : 5 derniers

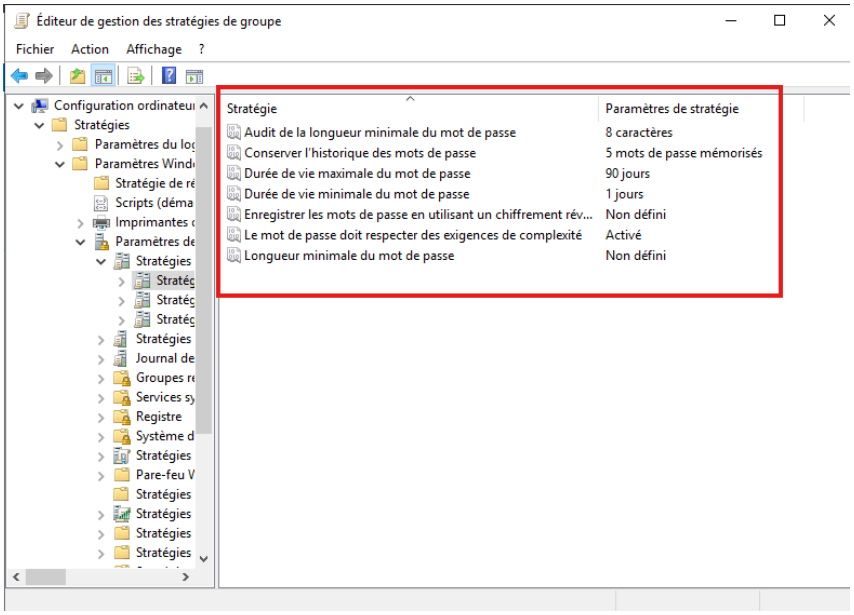
Verrouillage de compte :

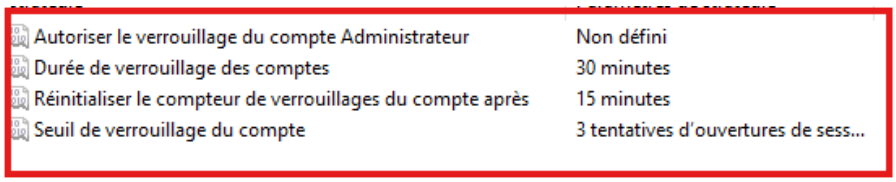
- Seuil de verrouillage : 3 tentatives échouées
- Durée de verrouillage : 15 minutes
- Réinitialisation du compteur : après 15 minutes

Restrictions sur les postes clients :

- Accès au panneau de configuration et aux paramètres : bloqué
- Accès à l'invite de commandes (CMD) : bloqué
- Accès à l'éditeur de registre (Regedit) : bloqué

Le Windows Server a été exclu de l'application de cette GPO afin de préserver les droits d'administration nécessaires à la gestion du domaine.

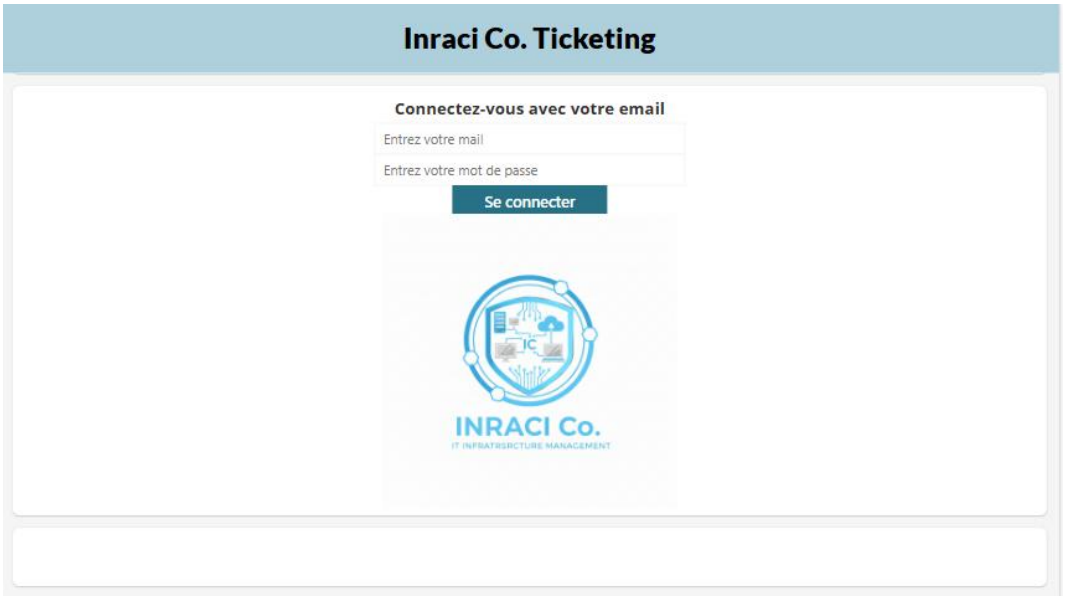




Application de ticketing (Power Apps)

Une application de ticketing a été développée avec Microsoft Power Apps, connectée à une liste SharePoint comme base de données. L'application comporte quatre écrans principaux : Login, Dashboard Admin, Interface Client et Tableau de bord.

La séparation des rôles est assurée par la vérification de l'adresse email de l'utilisateur connecté. Les administrateurs peuvent modifier le statut des tickets, tandis que les clients ne voient que leurs propres tickets. Une automatisation Power Automate envoie un email de notification lors de la création d'un nouveau ticket.



Tests et validation

Tests de connectivité réseau :

Test	Résultat	Observations
Ping PC hôte → Routeur (192.168.100.1)	☑ Succès	Liaison VMnet2 fonctionnelle
Ping Routeur → NAT GNS3 (192.168.122.1)	☑ Succès	Liaison NAT fonctionnelle
Ping Routeur → Internet (8.8.8.8)	☑ Succès	NAT configuré correctement
Ping VM Client → Routeur (192.168.1.253)	☑ Succès	Liaison VMnet3 fonctionnelle
Ping VM Client → Windows Server (192.168.1.2)	☑ Succès	Communication LAN OK
Ping VM Client → PfSense (192.168.1.254)	☑ Succès	Gateway accessible
Ping PfSense → Internet (8.8.8.8)	☑ Succès	Routage PfSense → Internet OK

(Preuve étant que tout fonctionne correctement)

Tests des services :

Service	Résultat	Observations
Résolution DNS (nslookup Ibrahim.loc)	☑ Succès	Résout vers 192.168.1.2
Attribution DHCP	☑ Succès	IP distribuée dans la plage définie
Connexion FTP (ftp 192.168.1.2)	☑ Succès	Authentification AD fonctionnelle
Portail captif (redirection HTTP)	☑ Succès	Redirection vers page de login
A2F Google Authenticator	☑ Succès	Code OTP validé par FreeRADIUS
Refus d'un faux code OTP	☑ Succès	"Invalid credentials" retourné
GPO - Blocage CMD	☑ Succès	CMD inaccessible sur les clients
GPO - Blocage Panneau de configuration	☑ Succès	Accès refusé sur les clients
Jointure au domaine Ibrahim.loc	☑ Succès	Clients membres du domaine

Difficultés rencontrées et solutions

Plusieurs difficultés techniques ont été rencontrées durant la réalisation du projet :

- Conflit d'IP entre le routeur Cisco et PfSense (tous deux à 192.168.1.254) : résolu en changeant l'IP du routeur à 192.168.1.253.
- Le ping depuis le routeur vers le PC hôte était bloqué par le firewall Windows : partiellement résolu, mais non bloquant pour le projet car la communication inverse (PC → routeur) fonctionne.
- FreeRADIUS refusait les connexions depuis le portail captif : résolu en forçant le protocole PAP dans la configuration du serveur d'authentification.
- La connexion VMnet3 se perdait parfois après redémarrage de GNS3 : résolu en débranchant et rebranchant le câble du Cloud VMnet3 dans GNS3.

Conclusion

Ce Travail de Fin d'Études m'a permis de concevoir et déployer une infrastructure informatique complète simulant l'environnement réseau d'une entreprise. En partant de zéro, j'ai mis en place tous les composants essentiels d'un réseau d'entreprise sécurisé : gestion des identités avec Active Directory, services réseau (DNS, DHCP, FTP), sécurisation des accès avec PfSense et le 2FA, politiques de groupe pour restreindre les accès, et un système de ticketing pour la gestion des incidents.

Les objectifs fixés au départ ont été largement atteints. L'infrastructure est fonctionnelle et tous les services ont été testés et validés. Le système de double authentification (A2F) avec Google Authenticator constitue un élément de sécurité particulièrement efficace, garantissant que seuls les utilisateurs autorisés peuvent accéder au réseau.

Ce projet m'a permis de développer et consolider de nombreuses compétences techniques : administration système Windows Server, configuration d'équipements réseau Cisco, gestion de firewall, virtualisation avec VMware et GNS3, développement d'applications avec Power Apps, et sensibilisation à la cybersécurité.

Ce projet m'a confirmé l'importance d'une approche méthodique et structurée dans la gestion de projets informatiques complexes, compétence essentielle pour ma future carrière professionnelle.

Bibliographie / Webographie

Documentation officielle

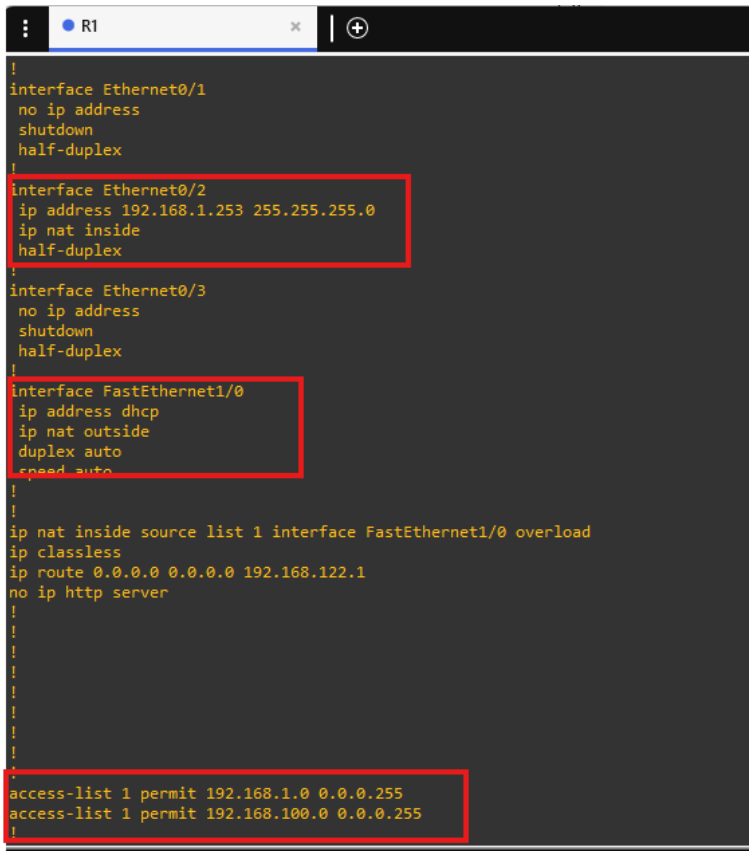
- MICROSOFT, « Documentation Windows Server », sur https://docs.microsoft.com/fr-fr/windows-server/, consulté en 2025.
- PFSENSE, « pfSense Documentation », sur https://docs.netgate.com/pfsense/, consulté en 2025.
- GNS3, « GNS3 Documentation », sur https://docs.gns3.com/, consulté en 2025.
- VMWARE, « VMware Workstation Documentation », sur https://docs.vmware.com/, consulté en 2025.
- MICROSOFT, « Power Apps Documentation », sur https://docs.microsoft.com/fr-fr/power-apps/, consulté en 2026.
- GNS3« vidéo youtube », sur https://www.youtube.com/watch?v=_bShU45Q70g&pp=ygURY29uZmlndXJlIGducczMgdm0%3D

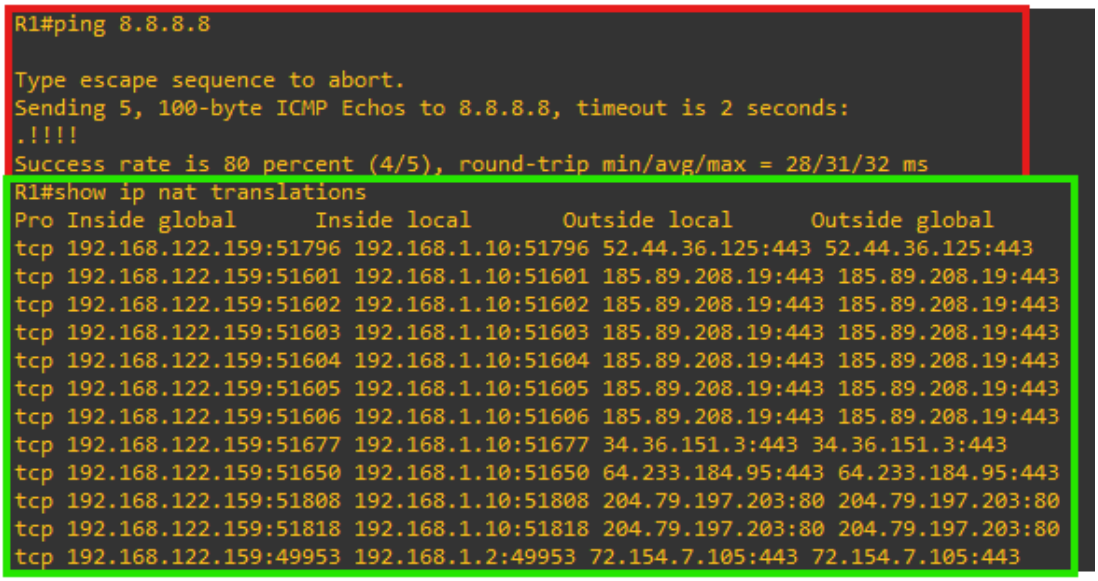
Annexes

Configuration du routeur Cisco c3620 et captures d'écran des explications cité ci-dessus :

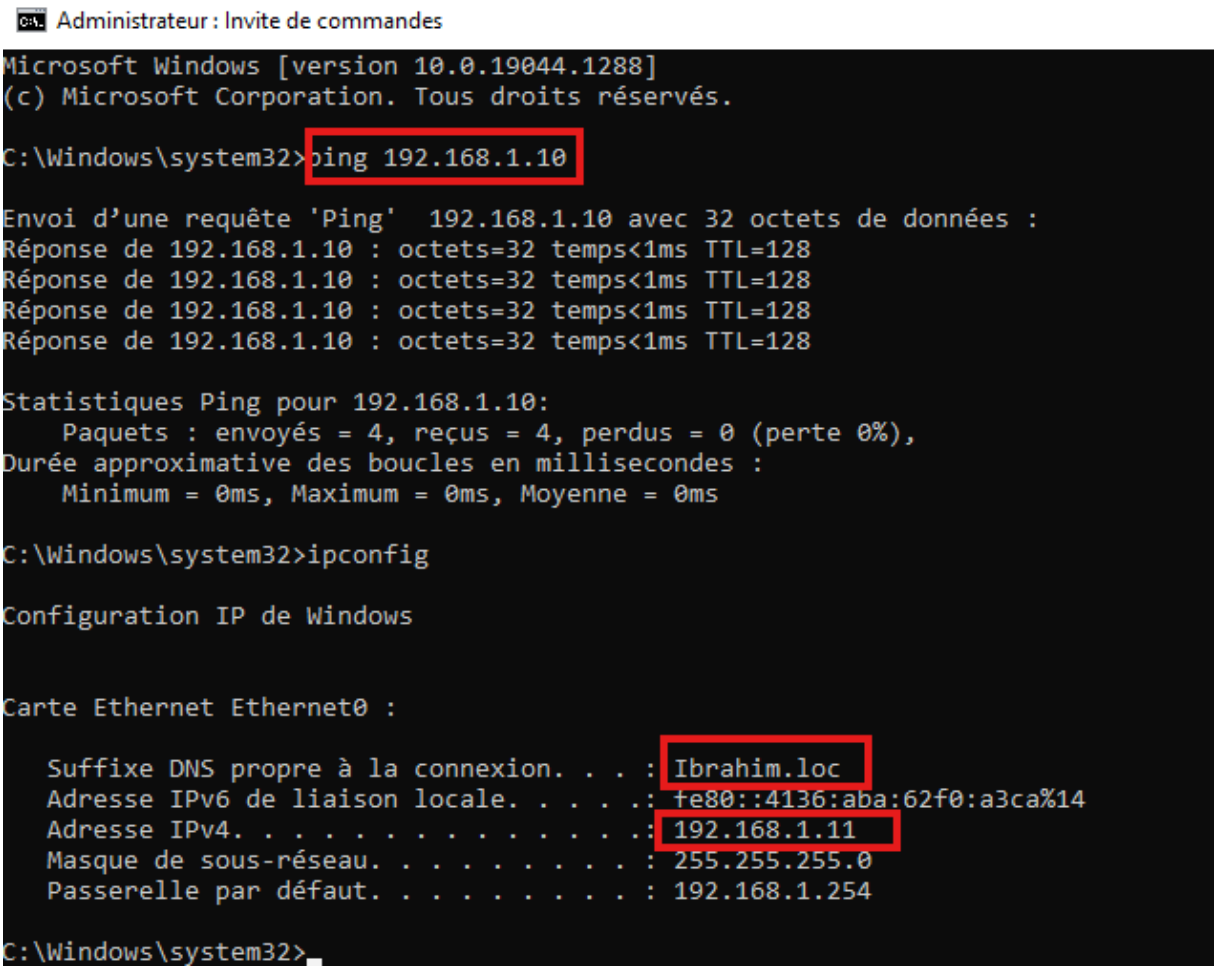
Commandes de configuration principales appliquées sur le routeur :

```
hostname R1-Projet
interface Ethernet0/0
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
 no shutdown
interface Ethernet0/2
 ip address 192.168.1.253 255.255.255.0
 ip nat inside
 no shutdown
interface FastEthernet1/0
 ip address dhcp
 ip nat outside
 no shutdown
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.100.0 0.0.0.255
ip nat inside source list 1 interface FastEthernet1/0 overload
ip route 0.0.0.0 0.0.0.0 192.168.122.1
```

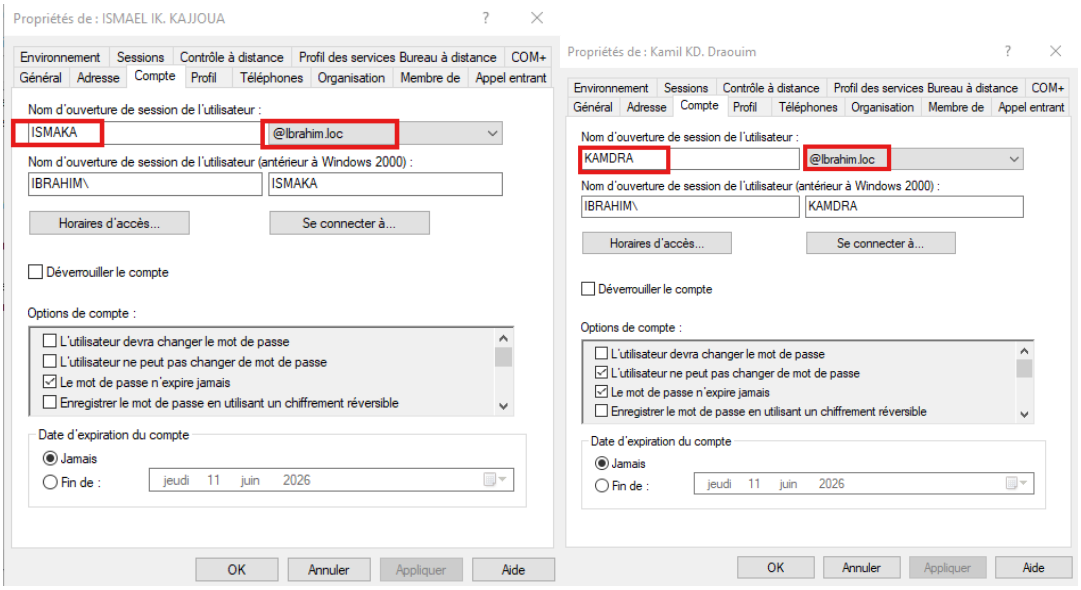


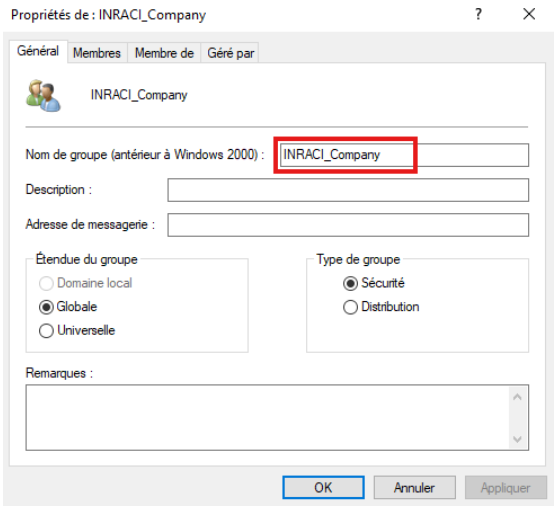


(ping 8.8.8.8 le nat fonctionne)



(ping d'un client à l'autre)



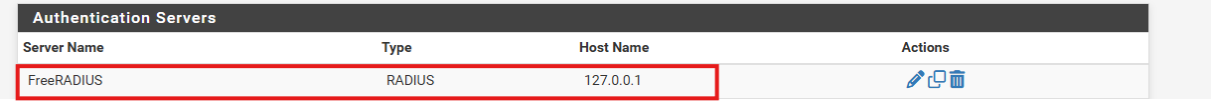


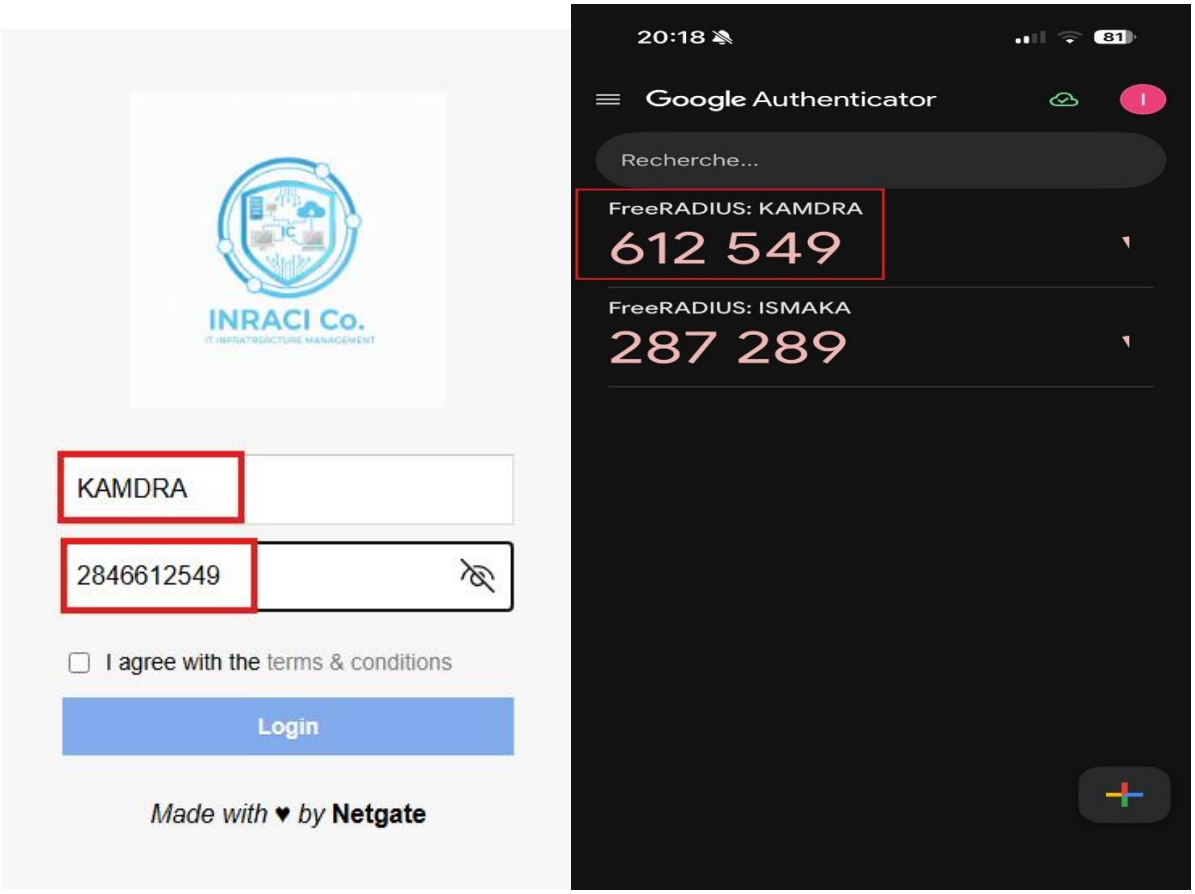
Rules (Drag to Change Order)

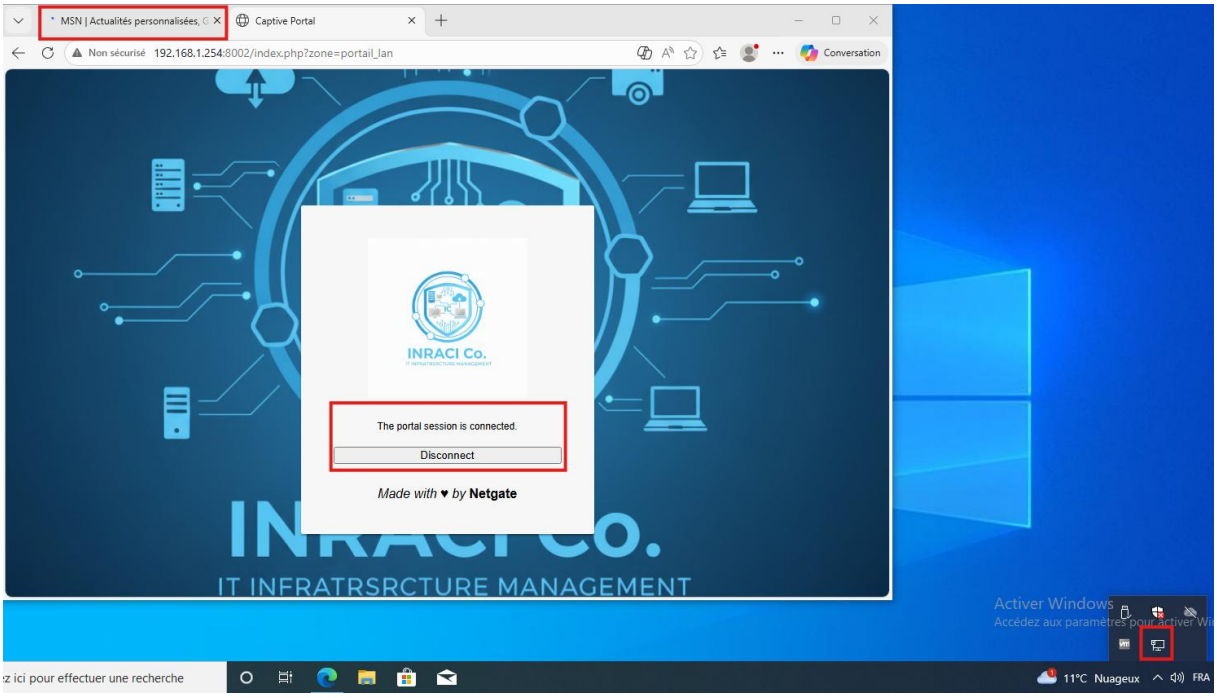
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓ 6/988 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
☐	✓ 0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Autoriser tout le trafic LAN	
☐	✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.1.2	80 - 443	*	none		Autoriser HTTP/HTTPS	
☐	✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.1.2	53 (DNS)	*	none		Autoriser DNS	
☐	✓ 0/0 B	IPv4 TCP	LAN subnets	*	192.168.1.2	21 (FTP)	*	none		Autoriser FTP	
☐	✓ 0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
☐	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
☐	✗ 0/0 B	IPv4 *	*	*	*	*	*	none		Bloquer tout le reste	

Captive Portal Zones

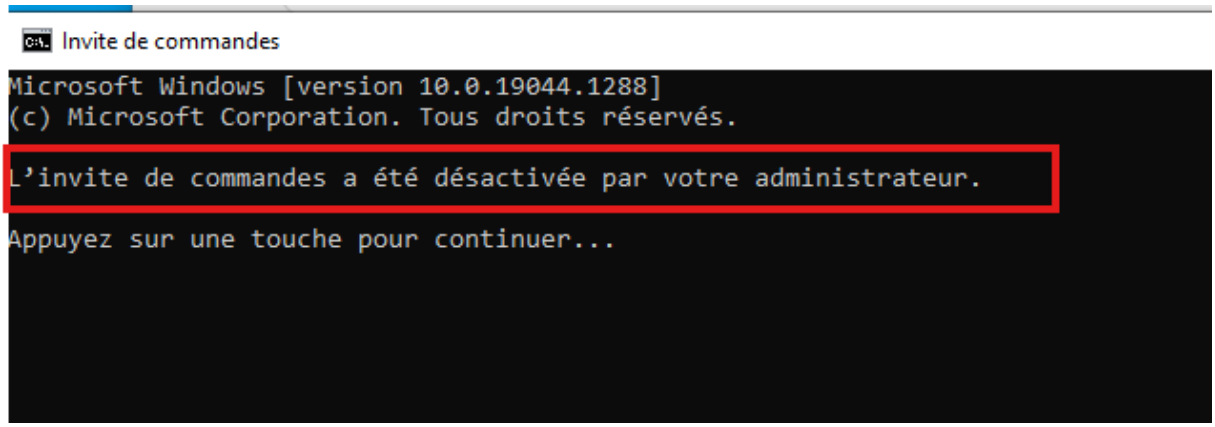
Zone	Interfaces	Number of users	Description	Actions
portail_lan	LAN	0	Portail captif du réseau LAN	



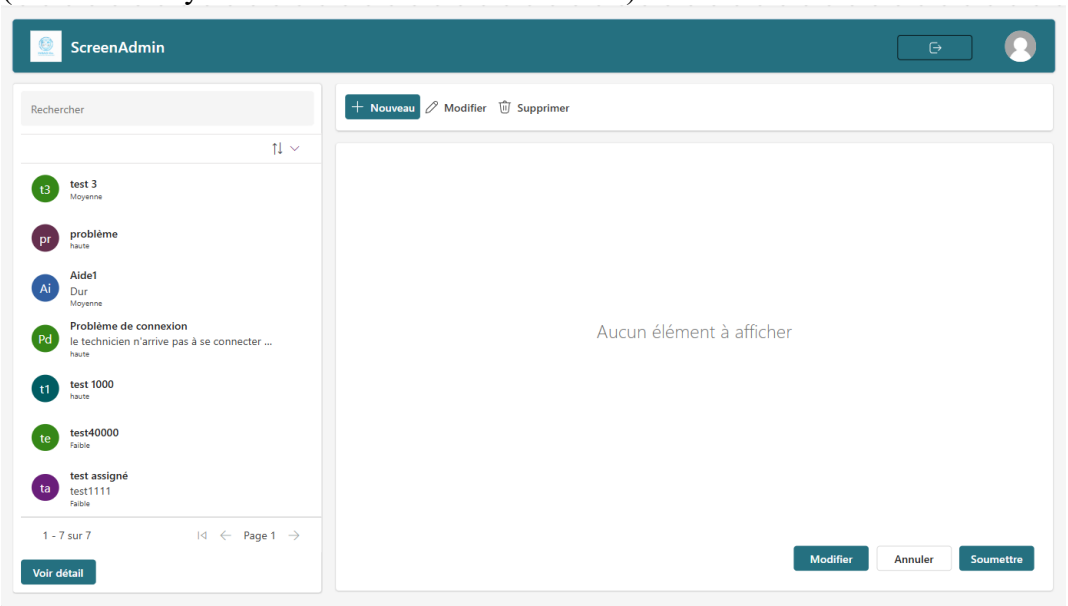




(on peut voir que lorsque le client est connecter au compte il a accès à internet)



(un client essaye de lancer l'invite de commande)



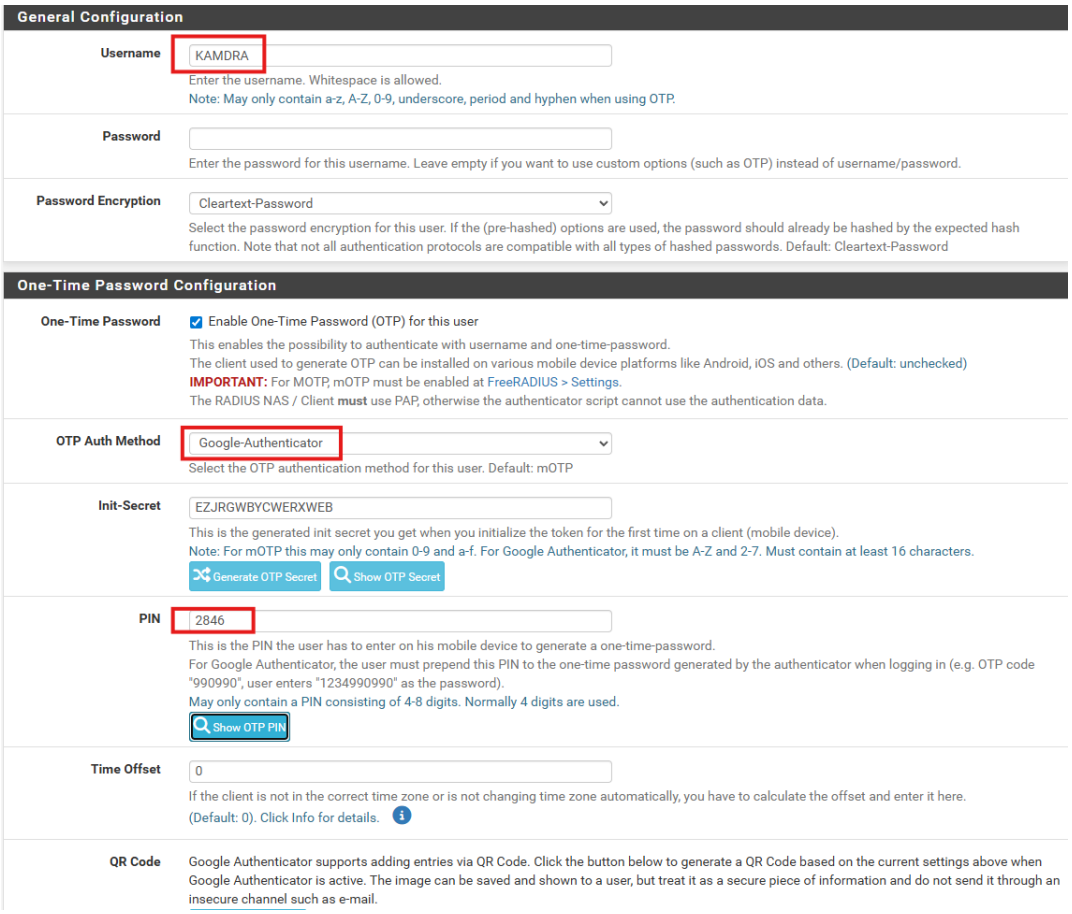
(DashboardAdmin)



(Ticket de l'utilisateur connecter)



(Page de création de ticket pour le client)



Sites internet

https://kaba-ibrahima.be/