



Rapport SAE 303

CONCEVOIR UN RÉSEAU MULTI-SITES

Altay CEVIK

Fatih KURUL

Nicolas RABERGEAU

Bilal BAKOUCHE

Xavier KNOEPFFLER-POUT

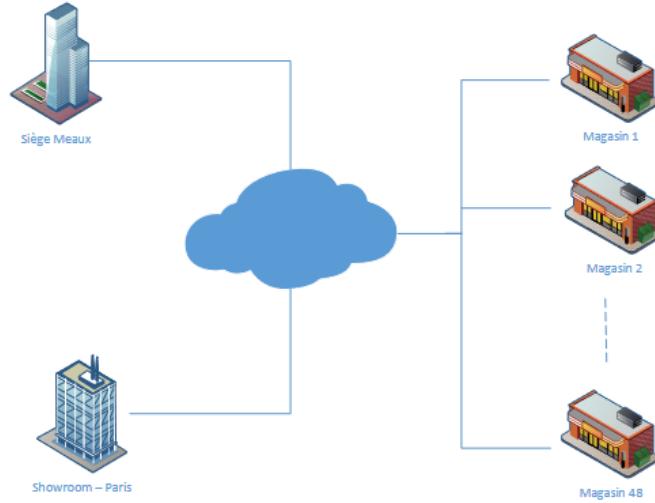
SOMMAIRE

- I. Déroulement du projet
 - A. Partie commune
 - B. Parties spécifiques
 - 1. Partie IOM
 - 2. Partie Cyber
- II. Coeur de réseau (*Fait par Bilal et Fatih*)
 - A. Configuration de base
 - 1. DHCP
 - 2. OSPF
 - 3. BGP
 - 4. MPLS pour VPN
 - 5. VLAN
 - B. Configuration avancée
 - 1. VRF
 - 2. VRRP (Cyber)
- III. Réseau sans fil (*Fait par Nicolas*)
 - A. Point d'accès
 - B. Portail captif
 - 1. Installation Pfsense
 - 2. Configuration Pfsense
 - 3. Tests Pfsense
- IV. Serveur Téléphonique (*Fait par Xavier*)
 - 1. FreePBX
 - 2. Grandstream GXV3000
- V. Serveurs d'infrastructure (*Fait par Nicolas*)
 - A. DNS
 - B. Active Directory
 - C. Radius (Cyber)
 - D. Windows Terminal services
- VI. Serveurs d'applications (*Fait par Nicolas*)
 - A. Nextcloud
 - B. Messagerie, webmail
 - C. Serveur web
- VII. Conclusion

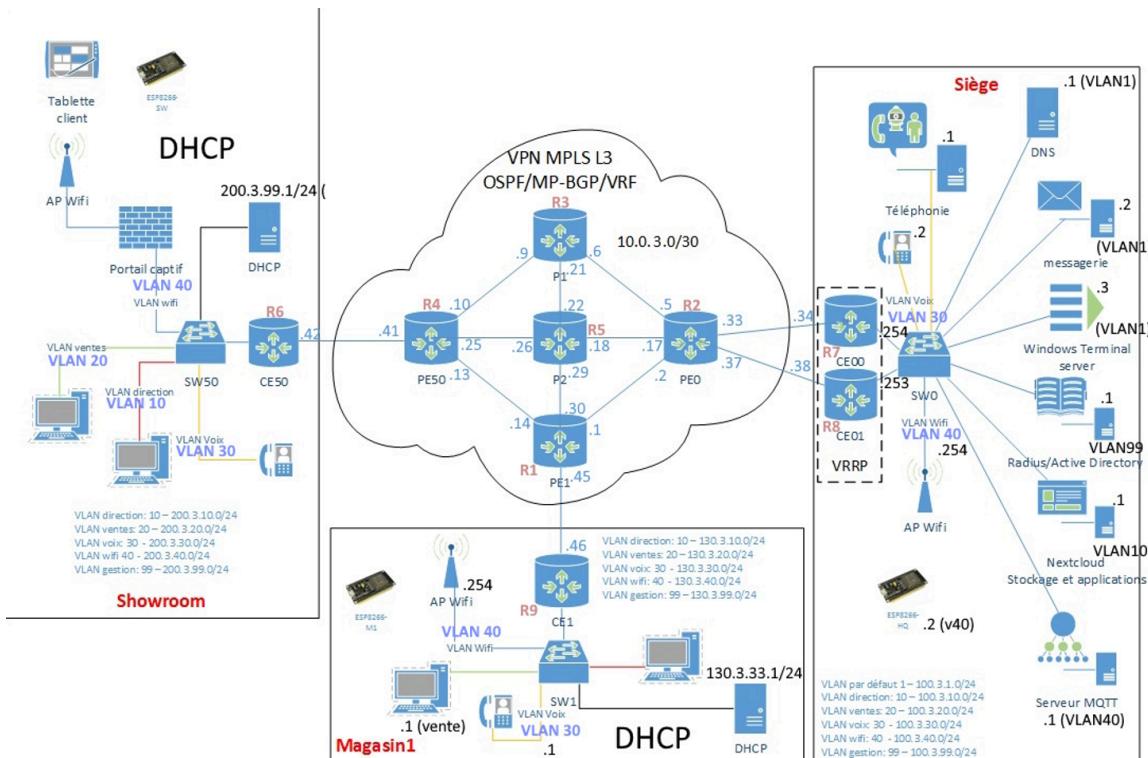
I. Déroulement du projet

A. Partie Commune

La partie commune, et le but principal de notre projet était de créer une nouvelle infrastructure réseau et informatique pour l'entreprise de chaussée sportive Beerok.



Voici le schéma global de l'infrastructure, celui-là permet de nous donner un aperçu du réseau, mais on en a une plus détaillé avec tout les service et serveur que nous avons installé, de plus il nous a également servi de plan d'adressage :



B. Partie Spécifique

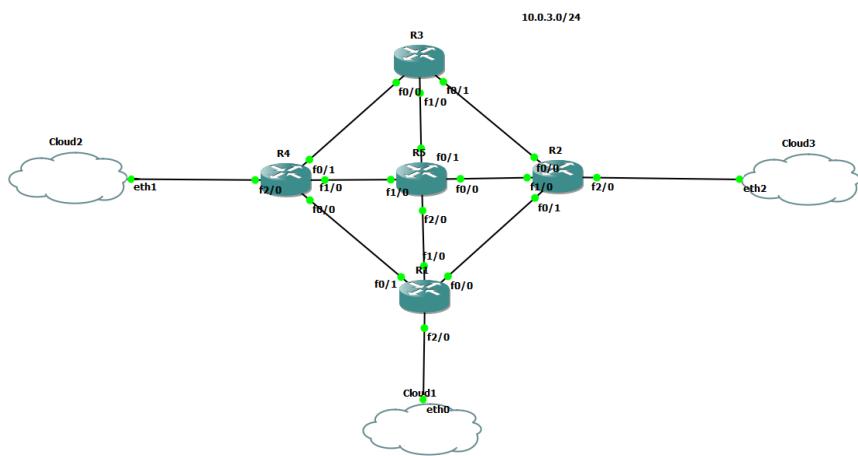
1. Partie IOM

L'IoM est le sujet de l'interconnexion entre l'internet et les objets, permettant ainsi une communication entre le physique et le numérique. Ces formes de connexions permettent de rassembler de nouvelles masses de données sur le réseau et donc, de nouvelles connaissances et formes de savoirs.

2. Partie Cyber

La Cybersécurité consiste en la sécurisation des systèmes d'informations. Il est nécessaire de comprendre comment celui-ci fonctionne pour pouvoir localiser les failles éventuelles. Il existe également des outils aidant à tester la sécurité d'un système. L'audit de sécurité est un moyen de repérer ces failles et de hiérarchiser ces dites failles pour les trier du plus au moins menaçant dans un contexte précis. Le Pentest est aussi un autre moyen de tester la sécurité d'un système, il permet cependant de mettre à l'épreuve la faille éventuellement trouvée pour s'introduire dans le système.

II. Coeur de Réseau



Le cœur de réseau est constitué de plusieurs routeurs reliés entre eux, ils permettent l'acheminement des paquets d'un lieu à un autre. Ces routeurs sont configurés avec le protocole de routage ospf. Le cœur de réseau relie les autres lieux avec le protocole bgp qui est un protocole permettant la liaison de 2 entreprises.

A. Configuration de Base

1. DHCP

DHCP, signifie Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et configurer des serveurs de noms comme DNS ou WINS.

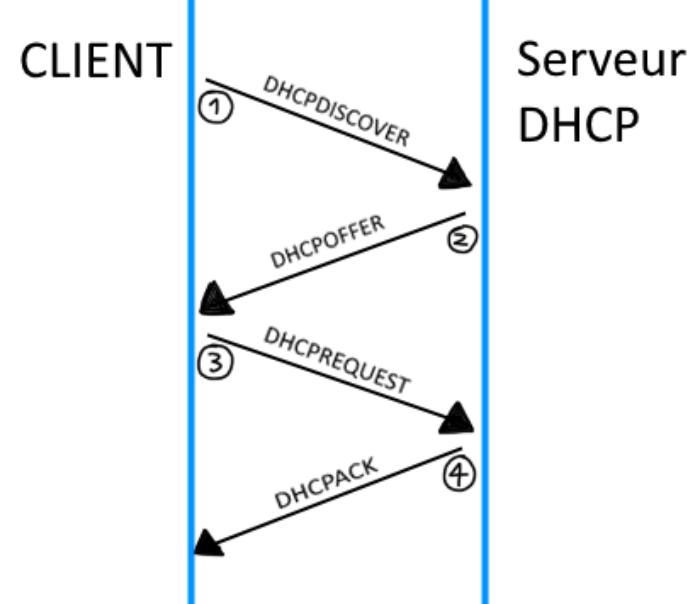
Pour le fonctionnement du protocole DHCP, un ordinateur équipé d'une carte réseau, envoie en diffusion un datagramme dit (DHCP Discover).

Quand un serveur DHCP reçoit ce dernier datagramme, il renvoie une offre DHCP (DHCP OFFER) au client, cette offre comporte une adresse IP et un masque de sous-réseau.

Le client retient alors l'offre reçue et envoie une requête DHCP (DHCP Request). Ce datagramme comporte l'adresse IP du serveur et celle qui vient d'être proposée au client. Elle a pour effet de demander au serveur choisi, l'assignation de cette adresse, l'envoie éventuel des valeurs des paramètres, et d'informer les autres serveurs qui ont fait une offre que cette dernière n'a pas été retenue.

Le serveur DHCP élabore ensuite un datagramme d'accusé de réception (DHCP ACK (ACK signifiant acknowledge)) qui assigne au client l'adresse IP et son masque de sous-réseau et la durée de bail de cette adresse.

Pour configurer DHCP, le routeur cisco permet de créer des pools d'adresse pour attribuer des adresses ip aux hôtes demandant une adresse. Notre routeur utilise un pool d'adresse pour chacun des réseaux des sous interfaces créées sur le routeur.



2. OSPF

OSPF, signifiant “**Open Shortest Path First**” est un protocole de routage interne IP de type “à état de lien”. Chaque routeur établit des relations d’adjacence avec ses voisins immédiats en envoyant des messages “hello” à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (dit LSA) propager de proche en proche à tous les routeurs du réseau. La méthode de mise en place de ce protocole consiste à identifier les réseaux voisins pour ensuite les indiquer au routeur. Le protocole a été implémenté sur le cœur de réseau pour qu’ils puissent communiquer entre eux.

3. BGP

BGP, signifiant **Border Gateway Protocol**, est un protocole d’échange de route externe utilisé notamment sur les réseaux internes.

Les connexions entre deux voisins BGP sont configurées explicitement entre deux routeurs. Ils communiquent alors entre eux via une session TCP sur le port 179 initiée par l’un des deux routeurs.

Les routeurs voisins sont identifiés par leur routeur ID, un identifiant de quatre octets, unique pour chacun des routeurs d’un “Autonomous System” (AS) donné qui peut être choisi arbitrairement mais qui est généralement une adresse IPv4 loopback de chaque routeur.

Ce protocole sera donc celui qui va lier les routeurs du cœur aux routeurs des autres lieux (Siège, Showroom, magasins,...)

4. MPLS pour VPN

MPLS (Multiprotocol Label Switching) est un mécanisme de transport de données utilisé dans les réseaux. Il repose sur la commutation de labels, où des étiquettes sont insérées à l'entrée du réseau MPLS et retirées à sa sortie. MPLS permet d'acheminer différents types de trafic sur une unique infrastructure tout en les isolant. Les routeurs de départ utilisent ces labels pour déterminer le routeur de sortie du réseau, sans que les routeurs intermédiaires aient besoin de consulter une table de routage volumineuse.

Avec ce même protocole, on a aussi la capacité de créer des Tunnels, avec les différents tunnels, on parvient facilement à faire des connexions de routeur en routeur. Ces tunnels peuvent être prédefinis, ou dynamiques et peuvent être utiles au cas où qu'une connexion arrête de marcher.

5. VLAN

Les VLAN sont des termes signifiant "Réseau local virtuel", ce sont des réseaux informatiques logiques indépendants. De nombreux VLAN peuvent coexister sur un même commutateur réseau aussi nommé "switch".

B. Configuration Avancée

1. VRF

Le VRF est un mécanisme de segmentation des réseaux IP. Il permet à plusieurs instances d'une table de routage de coexister dans le même routeur en même temps. Chaque instance de routage est indépendante, ce qui signifie que des adresses IP identiques ou qui se chevauchent peuvent être utilisées sans conflit. La fonctionnalité réseau est améliorée, car les réseaux IP peuvent être segmentés sans nécessiter plusieurs routeurs. Une VRF peut être implémentée dans un périphérique réseau par une paire de tables de routage et de transmission distinctes, une par instance de routage.

2. VRRP (Cyber)

Le VRRP est un protocole standard conçu pour augmenter la disponibilité de la

passerelle par défaut des hôtes d'un même réseau. Il fonctionne en définissant une adresse IP virtuelle comme passerelle par défaut pour les hôtes du réseau, référençant un groupe de routeurs. Dans un groupe VRRP, il y a un routeur maître associé à l'adresse IP virtuelle. Ce routeur répond aux requêtes ARP des clients sur cette adresse IP. Plusieurs routeurs de secours peuvent reprendre le rôle de maître en cas de défaillance du routeur maître.

III. Réseau sans fil (*Fait par Nicolas*)

A. Point d'accès

Tout d'abord, j'ai relié mon PC perso à l'AP via un port LAN, puis j'ai effectué une réinitialisation de l'AP en maintenant enfoncé le bouton RESET pendant 30 secondes. Une fois cette opération terminée, j'ai démarré l'AP et j'ai accédé à son interface via un navigateur web. Là, j'ai défini un mot de passe personnalisé pour sécuriser l'accès à l'interface et j'ai mis une adresse IP statique.

WIFI AP Magasin

The screenshot shows the 'Local Network' configuration page of a DD-WRT router. The 'LAN Status' section displays the following information:

MAC Address	C0:56:27:19:B3:FC
IP Address	130.3.40.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

The 'Active Clients' section shows one connected client:

Hostname	IP Address	MAC Address	Conn. Count	Ratio [1024]
LaptopNR	130.3.40.120	14:13:33:8B:E4:1D	69	7%

Ensuite, j'ai vérifié le bon fonctionnement de l'AP en consultant les onglets Status/LAN/WAN de l'interface. J'ai configuré l'accès en SSH uniquement via le menu "Services" pour renforcer la sécurité. Enfin, j'ai réalisé une sauvegarde de la configuration de DD-WRT pour pouvoir restaurer les paramètres en cas de besoin.

Pour la configuration du réseau, j'ai configuré le SSID et choisi un canal dans la partie Wireless/Basic Settings. J'ai ensuite vérifié le bon fonctionnement du serveur DHCP avec un client Wi-Fi. Dans la partie Setup, j'ai activé le serveur DHCP pour les tests.

Enfin, j'ai sécurisé le réseau en définissant le mode de sécurité WPA2 Personal

TKIP+AES dans l'onglet Wireless/Wireless Security. Après avoir effectué ces étapes, j'ai testé le bon fonctionnement depuis un client pour m'assurer que tout fonctionnait correctement.

- B. Portail captif
 1. Installation Pfsense



Tout d'abord, j'ai téléchargé l'image ISO de Pfsense depuis le site web www.pfsense.org/download. Pfsense étant basé sur FreeBSD, j'ai créé une machine virtuelle FreeBSD 64 bits avec 1 Go de RAM et 2 Go de disque. J'ai configuré trois interfaces réseau avec des pilotes virtio : une pour OPT en mode bridge sur l'interface connectée à mon réseau d'infrastructure, une autre pour LAN en mode bridge connectée au switch LAN de l'AP correspondant au réseau ouvert, et une troisième pour WAN en mode bridge connectée au réseau de l'IUT.

Ensuite, j'ai inséré l'image ISO de Pfsense dans le lecteur CD et j'ai procédé à l'installation par défaut. Pendant l'installation, j'ai vérifié que Pfsense utilisait la première carte réseau (vtnet0 ou em0) pour mon réseau d'infrastructure (OPT), la deuxième carte réseau (vtnet1 ou em1) pour le LAN, et la troisième carte réseau (vtnet2 ou em2) pour le WAN.

2. Configuration Pfsense

Une fois l'installation terminée, je me suis connecté à l'interface LAN en utilisant les identifiants par défaut (admin/mot de passe : pfsense). Sur la page d'accueil de Pfsense, j'ai vérifié que les adresses IP des interfaces correspondaient aux spécifications du cahier des charges.

Dans la partie Services/Captive Portal de Pfsense, j'ai activé le portail captif en cochant "Enable Captive Portal" sur l'interface LAN. J'ai choisi "Local User Manager" dans la partie Authentification, puis j'ai créé deux utilisateurs dans la partie System/User Manager/Users et je les ai édités pour les placer dans le groupe "User - Services: Captive Portal login".

Ensuite, dans la partie Services/DHCP Server/LAN, j'ai activé le serveur DHCP avec une étendue conforme aux exigences du cahier des charges, en laissant les autres options par défaut.

Sur l'AP, j'ai désactivé le serveur DHCP dans l'onglet Setup, car c'est désormais Pfsense qui s'en charge. Dans la partie Network Setup de l'AP, j'ai également défini la passerelle par défaut vers Pfsense.

Enfin, sur Pfsense, dans la partie Services/DNS forwarder, j'ai coché la case "Enable DNS forwarder".

3. Tests Pfsense

Une fois toutes ces étapes réalisées, j'ai testé le portail captif en me connectant avec un client wifi du réseau ouvert et en lançant un navigateur. Le portail captif demande de me connecter pour accéder à Internet.

IV. Serveur Téléphonique (*Fait par Xavier*)

1. FreePBX



Pour créer le serveur Téléphonique demander, nous avons utilisé FreePBX.

FreePBX est un logiciel de téléphonie open-source fait principalement pour les entreprises et les centres de contact qui se repose sur le framework Asterisk.

Nous avons commencé par prendre un ordinateur hôte installé sur le siège, et nous avons installé FreePBX sur une machine virtuelle en utilisant VirtualBox.

Après son installation terminée, nous avons pu facilement nous connecter sur la page d'accueil d'administration de FreePBX en écrivant son adresse IP dans un navigateur web.

Depuis cette page, nous avons ajouté les différentes extensions demander, une extension signifiant un utilisateur définie car un numéro que l'on pourra appeler

2. Grandstream GXV3000

Dans chaque réseau, nous avons aussi installer des téléphones Grandmaster GXV3000



Non seulement est ce qu'il sont facile à utiliser, avec une caméra intégrée, mais ces téléphones IP permettent de facilement se connecter grâce à FreePBX.

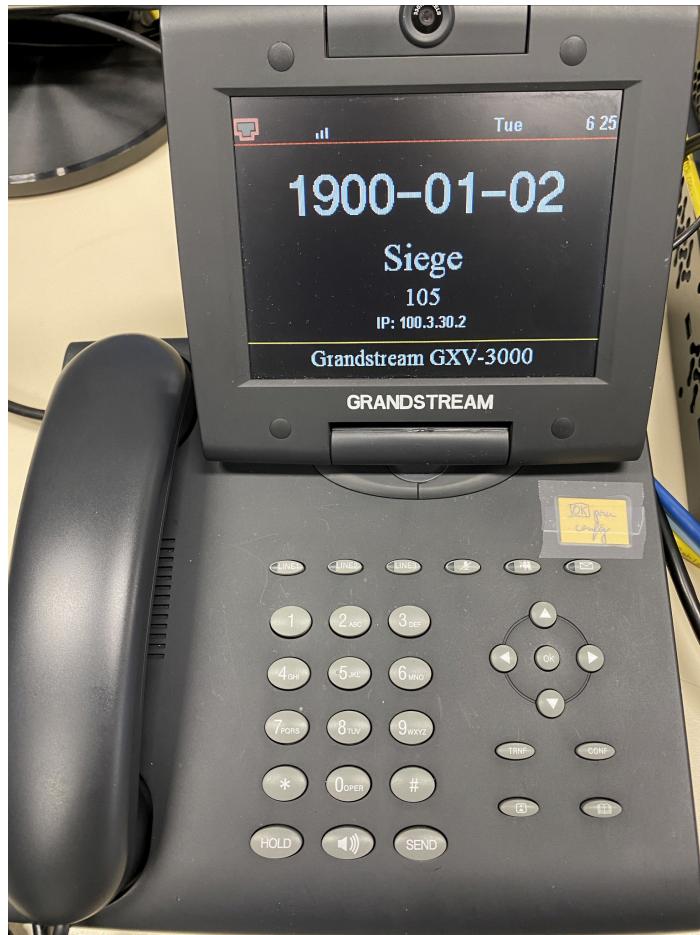
On commence d'abord par les connecter dans les VLAN 30, où ils recevront une adresse IP automatiquement grâce au DHCP.

Grandstream Device Configuration

STATUS **BASIC SETTINGS** **ADVANCED SETTINGS** **ACCOUNT 1** **ACCOUNT 2** **ACCOUNT 3**

Account Active:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Account Name:	105 (e.g., MyCompany)
SIP Server:	100.3.30.1 (e.g., sip.mycompany.com, or IP address)
Outbound Proxy:	100.3.30.1 (e.g., proxy.myprovider.com, or IP address, if any)
SIP User ID:	105 (the user part of an SIP address)
Authenticate ID:	105 (can be identical to or different from SIP User ID)
Authenticate Password:	(purposely not displayed for security protection)
Name:	Siege (optional, e.g., John Doe)

Dans leur configuration, et après leur avoir donné l'adresse IP du serveur FreePBX, les téléphone VoIP save maintenant où se diriger pour faire leur appelle, qui permet alors à une connexion sans problème et un appel directe.



On a donner les numéros suivant:

Pour les téléphones situés sur le Siège, on à donner des numéros de téléphones en 100.
(101, 102, 103, 104, 105)

Pour les téléphones situés dans le magasin, on à donner des numéros de téléphones en 200.

(201, 202, 203, 204, 205)

Pour les téléphones situés dans le Showroom à Paris, nous avons donné des numéros de téléphones en 300.

(301, 302, 303, 304, 305)

V. Serveurs d'infrastructure (*Fait par Nicolas*)

Je commence par mettre en place mon environnement virtuel sur le serveur Proxmox, en créant des machines virtuelles à partir des templates Windows. J'ai configuré ces machines avec des interfaces réseau spécifiques pour la connexion NAT, le réseau interne et les proxmox. J'ai également vérifié que les noms Windows des machines virtuelles sont corrects en respectant le cahier des charges.

Ensuite, j'ai configuré les adresses IP statiques pour le serveur Windows sur les interfaces vmbr0 et vmbr1, en spécifiant également les paramètres DNS. Pour le client Windows, j'ai activé le DHCP pour ses interfaces réseau et j'ai vérifié la connectivité en désactivant le pare-feu.

A. DNS

J'ai également installé le rôle Serveur DNS sur le serveur Windows et configuré une zone de recherche directe. J'ai veillé à ce que les paramètres DNS soient correctement configurés dans DHCP pour une résolution adéquate des noms.

B. Active Directory

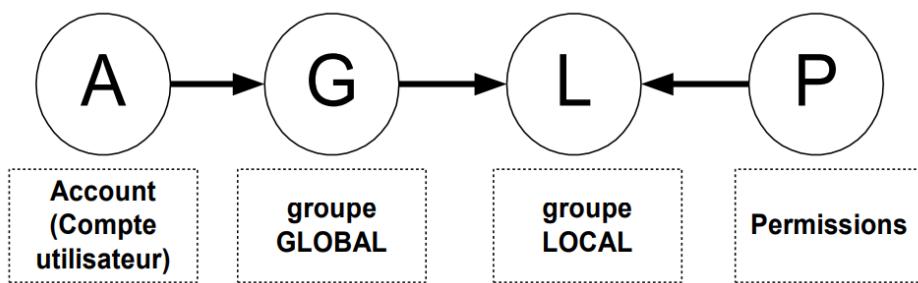


Active Directory

The screenshot displays two windows side-by-side. The left window is titled 'Utilisateurs et ordinateurs Active Directory' and shows a tree view of a domain structure under 'beerk.com'. The right window is titled 'Dossier Services de domaine Active Directory' and shows a file sharing interface for a folder named 'G_ventes'. It includes a 'Partager' (Share) dialog box where users like 'Administrateur' and 'Administrateurs' are granted 'Lecture/écriture' (Read/Write) permissions.

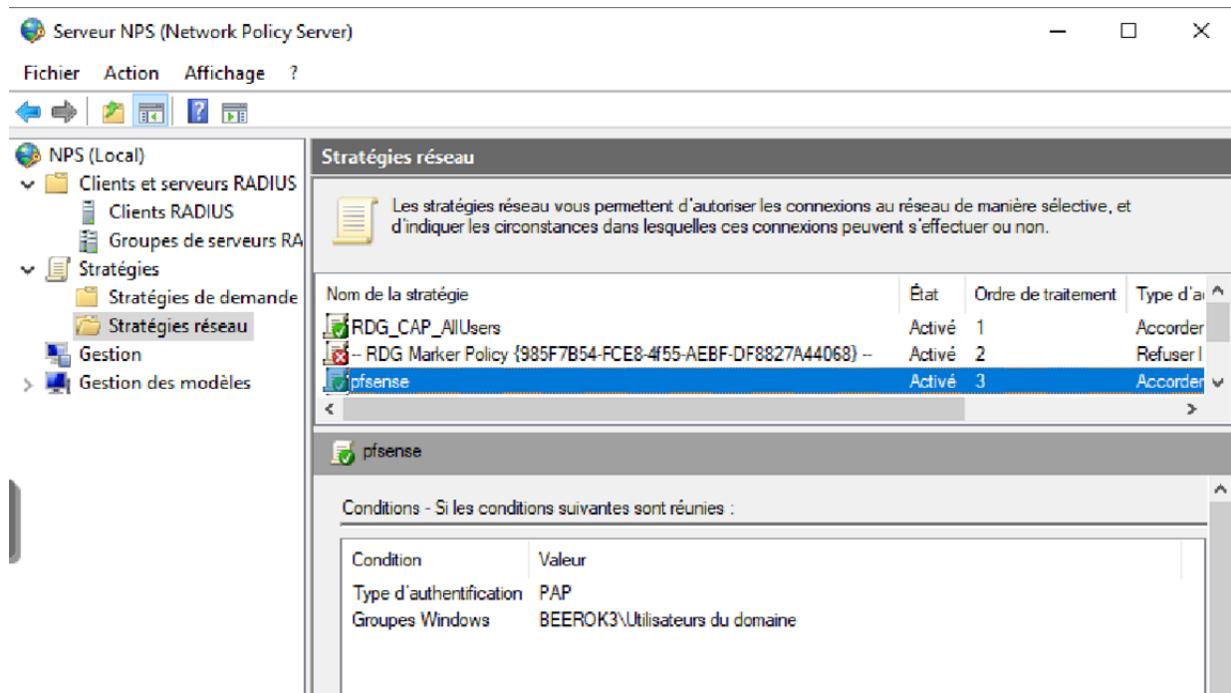
11

Active Directory étant essentiel pour la gestion des utilisateurs et des ordinateurs, j'ai procédé à son installation en suivant les paramètres spécifiés. J'ai créé des Unités Organisationnelles et des comptes d'utilisateurs conformément à la structure existante, en suivant la méthode AGLP pour la gestion des groupes.



C. Radius (Cyber)

Pour l'authentification des utilisateurs, j'ai configuré le serveur RADIUS en installant le rôle Network Policy Server (NPS) et en le reliant à Active Directory. Cela m'a permis de valider les accès au portail captif pour les utilisateurs autorisés.



D. Windows Terminal Service

Enfin, j'ai mis en place les services Bureau à Distance en installant les composants nécessaires et en configurant les applications RemoteApp pour permettre l'exécution de programmes à distance. J'ai veillé à ce que tout fonctionne correctement en testant chaque étape du processus.

VI. Serveurs d'applications (*Fait par Nicolas*)

Pour la configuration des serveurs d'application, j'ai suivi les instructions du cahier des charges. J'ai commencé par préparer mon environnement sur le serveur Proxmox, en mettant en place trois machines virtuelles : une pour Nextcloud et une autre pour la Messagerie, ainsi qu'une machine cliente Linux Debian.

Pour la configuration IP statique, j'ai désinstallé certains paquets et modifié le fichier /etc/network/interfaces pour spécifier les adresses IP et les paramètres de réseau pour chaque interface. J'ai également effectué les vérifications nécessaires et redémarré le réseau pour appliquer les changements.

A. Nextcloud



En ce qui concerne Nextcloud, j'ai opté pour l'installation via snap. Après l'installation, j'ai activé HTTPS et testé la connexion depuis différents clients web. J'ai également intégré Nextcloud à Active Directory en utilisant l'application LDAP user and group backend.

B. Messagerie, webmail

Pour la Messagerie, j'ai installé Postfix en configurant les enregistrements DNS et en ajustant les paramètres dans /etc/postfix/main.cf. J'ai également configuré Dovecot pour le stockage des mails et testé l'envoi et la réception de mails entre utilisateurs.

Enfin, j'ai mis en place un frontal web pour la Messagerie en installant SquirrelMail et en configurant Apache et PHP. J'ai sécurisé le système de messagerie en mettant en place le chiffrement SSL/TLS et j'ai intégré la Messagerie avec Nextcloud en configurant l'application Mail dans Nextcloud pour utiliser le serveur de messagerie.

VII. Conclusion

Le projet qui nous a été donné durant la semaine, et par l'entreprise Beerok nous a beaucoup aider, non seulement pour apprendre comment faire un serveur telle quelle, mais aussi pour nous apprendre à travailler en groupe, même si chacun de nous n'était pas exactement dans le même domaine.

On a souvent remarqué, que tous les problèmes qui était venu dans notre chemin étaient souvent débloqués grâce à l'aide d'un autre membre de notre groupe, qui nous a montrer la synergie qui est possible dans un groupe qui est compris de professionnel dans plusieurs domaines différents.

En tout, ce projet nous a permis de nous aider à non seulement affiner nos connaissances, mais aussi nous préparer à devenir des en forme de T; des employés qui sont vraiment forts dans un domaines, mais qui sont aussi capable de prouver leur connaissances dans tout autre domaines qui ne sont pas directement leur expertise.