MISE EN PLACE D'UN SERVEUR NEXTCLOUD

Cédric BAUDIMENT
AgroMousquetaires – Site d'Antartic 2

BTS SIO SISR
Greta Drôme / Ardèche
2024 / 2026

I/ Cahier des charges

1- Descriptif de l'existant

Dans le cadre de l'épreuve E5 du BTS Services Informatiques aux Organisations, option SISR (Solutions d'Infrastructure, Systèmes et Réseaux), une infrastructure réseau complète a été mise en place afin de simuler l'organisation et le fonctionnement d'un système d'information d'entreprise. Cette infrastructure constitue un environnement pédagogique permettant de concevoir, déployer et administrer différents services réseau dans des conditions proches d'un contexte professionnel.

Le réseau est structuré autour d'une architecture segmentée reposant sur l'utilisation de plusieurs réseaux virtuels (VLAN). Cette segmentation permet d'isoler les différents types d'équipements et de mieux contrôler les flux de communication au sein du système d'information.

Plusieurs VLAN ont ainsi été définis pour organiser les ressources du réseau. Le VLAN 10 est dédié aux serveurs principaux de l'infrastructure. Le VLAN 20 est réservé aux serveurs de sauvegarde ainsi qu'aux serveurs redondants assurant la continuité de service. Le VLAN 30 regroupe les postes clients utilisés par les utilisateurs du réseau. Le VLAN 99 est destiné aux équipements d'administration, notamment les postes administrateurs, le bastion d'accès sécurisé ainsi que le serveur d'administration.

En complément de ces réseaux internes, une DMZ a été mise en place afin d'héberger les services accessibles depuis l'extérieur du réseau. Cette zone permet d'isoler les services exposés tout en protégeant le reste de l'infrastructure interne. Actuellement, la DMZ héberge un serveur web destiné à la publication de services accessibles depuis Internet. Dans le cadre du projet, un serveur supplémentaire sera déployé dans cette zone afin d'héberger une instance du logiciel de cloud privé Nextcloud.

Le routage et la sécurisation des communications entre les différents VLAN sont assurés par deux pare-feu configurés en redondance, fonctionnant avec le logiciel pfSense. Cette configuration permet d'assurer à la fois le filtrage des flux réseau et la continuité de service en cas de défaillance d'un des équipements. Les postes utilisateurs du réseau fonctionnent sous le système d'exploitation Windows 11 et accèdent aux différentes ressources mises à disposition sur l'infrastructure. À ce stade, aucun service de stockage centralisé de type cloud privé n'est déployé dans l'environnement, ce qui limite les possibilités de partage de fichiers et d'accès aux données à distance.

Dans ce contexte, la mise en place d'un serveur Nextcloud dans la DMZ vise à ajouter un service de stockage et de synchronisation de fichiers accessible de manière sécurisée, tout en respectant l'architecture réseau existante et les principes de segmentation et de sécurité déjà mis en place dans l'infrastructure.

2- Besoins

Dans le cadre de l'épreuve E5 du BTS Services Informatiques aux Organisations, option SISR (Solutions d'Infrastructure, Systèmes et Réseaux), il est demandé d'intégrer au système d'information une solution permettant le travail collaboratif et le partage de documents entre utilisateurs. Cette solution doit offrir des fonctionnalités comparables à celles proposées par des services de stockage en ligne largement utilisés dans les environnements professionnels, tels que Microsoft OneDrive ou Google Drive.

Le premier besoin identifié est la mise à disposition d'un espace de stockage permettant aux utilisateurs de déposer et d'organiser leurs documents. Cet espace doit permettre le partage de fichiers entre plusieurs utilisateurs afin de faciliter la circulation de l'information et le travail en équipe.

Un second besoin concerne la collaboration sur les documents. Les utilisateurs doivent pouvoir accéder à des fichiers communs et travailler sur les mêmes ressources, ce qui permet d'améliorer l'efficacité du travail collectif et de simplifier la gestion des documents partagés.

La solution doit également permettre un accès distant aux fichiers. Les utilisateurs doivent pouvoir consulter et récupérer leurs documents depuis l'extérieur du réseau de l'infrastructure, à condition de disposer des droits d'accès appropriés. Cette fonctionnalité implique que le service soit accessible depuis Internet tout en respectant les règles de sécurité mises en place dans l'architecture réseau.

Toutefois, pour des raisons de sécurité, il est important de distinguer clairement deux types de services au sein de l'infrastructure. D'une part, un serveur de fichiers interne est présent dans le VLAN 10, dédié aux serveurs. Ce serveur est destiné au stockage interne de l'organisation et n'est accessible que depuis le réseau local. Il ne doit pas être exposé vers l'extérieur afin de limiter les risques de compromission.

D'autre part, le service de cloud. Cette solution permettra de proposer un espace de stockage accessible depuis Internet, tout en restant isolée du serveur de fichiers interne.

Cette séparation des services permet de limiter l'exposition des ressources internes tout en offrant aux utilisateurs une solution de partage et d'accès distant aux documents. Elle s'inscrit dans une logique de segmentation du réseau et de réduction de la surface d'attaque du système d'information.

3- Contraintes

La mise en place de la solution de travail collaboratif s'inscrit dans le cadre du projet réalisé pour l'épreuve E5 du BTS Services Informatiques aux Organisations, option SISR. Dans ce contexte, plusieurs contraintes doivent être prises en compte afin d'assurer la cohérence et la faisabilité du projet.

La première contrainte concerne la gestion du temps. Afin d'organiser efficacement le déploiement de l'infrastructure et de disposer d'une marge pour d'éventuels ajustements, un objectif personnel a été fixé : disposer d'une infrastructure fonctionnelle avant la fin du mois de mars. Cette échéance n'est pas imposée par le cadre de l'épreuve, mais constitue un repère dans la planification du projet. Elle permet de réserver le mois d'avril à la phase de validation, à la résolution d'éventuels problèmes techniques et à l'amélioration de la configuration si nécessaire.

Une seconde contrainte concerne le respect du cahier des charges défini pour l'épreuve. Celui-ci impose l'intégration d'une solution de travail collaboratif au sein de l'infrastructure réseau. La solution retenue doit donc permettre le stockage de fichiers, leur partage entre utilisateurs et l'accès aux documents via une interface accessible depuis un navigateur web. Ces fonctionnalités sont comparables à celles proposées par des services de cloud largement utilisés tels que Microsoft OneDrive ou Google Drive.

Enfin, des contraintes de sécurité doivent être respectées. Le serveur de fichiers interne, situé dans le VLAN dédié aux serveurs, doit rester accessible uniquement depuis le réseau interne. Par conséquent, le service de cloud sera indépendant de ce serveur et ne disposera pas d'accès direct vers celui-ci. Cette séparation permet de limiter les risques liés à l'exposition d'un service accessible depuis Internet.

La prise en compte de ces contraintes dès la phase de conception permet d'assurer un déploiement cohérent avec l'architecture existante et conforme aux objectifs du projet.

II/ Ressources

1- Ressources mises à disposition

L'infrastructure utilisée pour la réalisation du projet repose sur un environnement virtualisé mis à disposition dans le cadre de la formation. Cet environnement est hébergé sur une ferme de serveurs administrée par le GRETA, permettant aux étudiants de déployer et d'administrer différentes machines virtuelles pour leurs travaux pratiques et projets.

La virtualisation est assurée par l'hyperviseur open source Proxmox VE, qui permet de créer et de gérer plusieurs machines virtuelles au sein d'un même environnement physique. Cette plateforme facilite la mise en place d'une infrastructure réseau complète tout en offrant la possibilité de modifier ou de reconstruire rapidement les systèmes en cas de besoin.

L'environnement dispose également d'un accès à Internet, ce qui permet notamment de télécharger les différents systèmes d'exploitation, les logiciels nécessaires au déploiement des services ainsi que les mises à jour de sécurité. Cet accès est également indispensable pour tester les services destinés à être accessibles depuis l'extérieur du réseau, comme le futur service de cloud privé.

Les ressources matérielles allouées à l'infrastructure sont les suivantes :

- un espace de stockage total de 800 Go destiné à l'hébergement des machines virtuelles et de leurs données
- 64 Go de mémoire vive (RAM) permettant de faire fonctionner simultanément plusieurs serveurs et services
- 6 cœurs de processeur dédiés au fonctionnement de l'ensemble des machines virtuelles.

Ces ressources permettent de déployer l'ensemble des éléments de l'infrastructure nécessaires au projet, notamment les serveurs, les pares-feux, les services réseau ainsi que le futur serveur de cloud collaboratif basé sur Nextcloud.

2- Ressource nécessaire à la mise en place

La mise en place de l'infrastructure et des différents services associés nécessite l'utilisation de plusieurs systèmes d'exploitation déployés sous forme de machines virtuelles. Pour cela, différentes images ISO sont utilisées afin d'installer les systèmes nécessaires au fonctionnement du réseau et des services.

Tout d'abord, l'installation de pare-feu virtuels repose sur le système pfSense. Ce logiciel permet d'assurer plusieurs fonctions essentielles au sein de l'infrastructure, notamment le routage entre les différents VLAN, le filtrage des flux réseau et la protection du système d'information. Deux instances sont déployées afin de garantir une redondance et d'améliorer la disponibilité du service.

Le système Windows Server 2025 est utilisé pour l'hébergement de plusieurs services d'infrastructure. Ce type de serveur peut notamment être utilisé pour la gestion de l'administration du réseau, l'hébergement de services internes ou encore la gestion des utilisateurs selon les besoins de l'infrastructure.

Les postes clients du réseau fonctionnent sous Windows 11. Ces machines permettent de tester l'accès aux différents services mis en place dans l'infrastructure, notamment l'accès aux ressources internes et aux services accessibles via le réseau.

Enfin, certaines machines virtuelles reposent sur le système d'exploitation libre Debian, notamment pour l'hébergement de services web ou applicatifs. Ce système est particulièrement adapté pour ce type d'usage en raison de sa stabilité et de sa large compatibilité avec de nombreux logiciels serveur. La version utilisée dans le cadre de ce projet est Debian 13, qui servira notamment de base pour le déploiement du service de cloud privé.

L'ensemble de ces systèmes constitue la base logicielle nécessaire à la création des différentes machines virtuelles de l'infrastructure et au déploiement des services attendus dans le cadre du projet.

3- Gestion des ressources

Dans un environnement virtualisé, la gestion rigoureuse du processeur, de la mémoire vive et du stockage est indispensable pour garantir la stabilité des machines virtuelles. En utilisant la plateforme Proxmox VE, les ressources sont allouées sur mesure et ajustées selon l'importance de chaque service. Les éléments critiques, tels que les pare-feux pfSense et les serveurs applicatifs, bénéficient d'une priorité accrue pour assurer leur performance et la continuité du routage entre les VLAN. Parallèlement, les serveurs Windows Server 2025 et Debian 13 reçoivent des ressources adaptées à leurs rôles respectifs, avec une attention particulière pour le serveur Nextcloud qui nécessite un espace disque conséquent pour le partage de fichiers. Enfin, l'enveloppe globale de 800 Go de stockage est répartie stratégiquement afin de répondre aux besoins actuels tout en conservant une marge de manœuvre pour l'évolution future de l'infrastructure. Cette approche équilibrée permet d'allier performance système et flexibilité opérationnelle.

III/ Analyse

1- Descriptifs des solutions

Afin de répondre au besoin de mise en place d'un service de stockage et de travail collaboratif, plusieurs solutions peuvent être envisagées. Ces solutions doivent permettre le stockage de fichiers, leur partage entre utilisateurs et l'accès aux documents depuis différents appareils. Trois solutions ont été étudiées : une solution de cloud public largement utilisée, une solution équivalente proposée par un autre fournisseur et une solution de cloud privé pouvant être hébergée au sein de l'infrastructure.

La première solution étudiée est Google Drive. Il s'agit d'un service de stockage en ligne proposé par l'entreprise Google. Cette plateforme permet aux utilisateurs de stocker des fichiers dans un espace en ligne, de les partager avec d'autres utilisateurs et de collaborer sur différents types de documents. Elle propose également une intégration avec plusieurs outils bureautiques accessibles directement depuis un navigateur web. L'avantage principal de cette solution est sa simplicité d'utilisation et sa disponibilité immédiate, sans nécessiter d'infrastructure technique interne. En revanche, les données sont hébergées sur l'infrastructure du fournisseur, ce qui implique une dépendance à un service externe et un contrôle limité sur l'hébergement des données.

La seconde solution étudiée est Microsoft OneDrive, développé par l'entreprise Microsoft. Ce service fonctionne sur un principe similaire en proposant un espace de stockage en ligne permettant la synchronisation des fichiers entre différents appareils. Il offre également des fonctionnalités de partage

de documents et de collaboration en ligne. OneDrive est fortement intégré à l'écosystème Microsoft, notamment aux outils bureautiques et aux systèmes d'exploitation de l'entreprise. Comme pour Google Drive, cette solution repose sur une infrastructure cloud externe, ce qui implique que les données sont hébergées en dehors de l'infrastructure locale.

La troisième solution étudiée est Nextcloud. Contrairement aux solutions précédentes, il s'agit d'un logiciel libre permettant de créer un service de cloud privé hébergé directement sur l'infrastructure de l'organisation. Nextcloud offre des fonctionnalités similaires aux solutions de cloud public, notamment le stockage de fichiers, le partage de documents entre utilisateurs et l'accès aux données via une interface web ou des applications clientes. L'avantage principal de cette solution est qu'elle permet de conserver la maîtrise de l'hébergement et de la gestion des données, puisque le service est installé sur un serveur interne. Elle peut également être intégrée à l'architecture réseau existante et configurée selon les besoins de l'organisation.

Ces trois solutions répondent au besoin de mise en place d'un service de stockage et de travail collaboratif, mais elles reposent sur des approches différentes. Les deux premières reposent sur des services cloud publics externalisés, tandis que la troisième permet de déployer une solution équivalente directement au sein de l'infrastructure. La comparaison de ces solutions permettra de déterminer celle qui est la plus adaptée au contexte du projet.

2- Comparaisons des solutions

Critères	Nextcloud	Google Drive	Microsoft OneDrive
Type de solution	Cloud privé auto-hébergé	Cloud public	Cloud public
Hébergement des données	Sur l'infrastructure interne	Sur les serveurs de Google	Sur les serveurs de Microsoft
Accès distant	Oui (configuration du serveur nécessaire)	Oui (service accessible via Internet)	Oui (service accessible via Internet)
Partage de fichiers	Oui	Oui	Oui
Travail collaboratif	Oui (extensions et outils collaboratifs possibles)	Oui (outils collaboratifs intégrés)	Oui (intégration avec la suite bureautique Microsoft)
Coût	Gratuit (logiciel libre) mais nécessite une infrastructure	Gratuit avec stockage limité puis abonnement	Gratuit avec stockage limité puis abonnement
Mise en place	Installation et administration nécessaires	Service prêt à l'emploi	Service prêt à l'emploi
Maintenance	Assurée par l'administrateur du système	Assurée par le fournisseur	Assurée par le fournisseur

3- Choix d'une solution

Après analyse des différentes solutions de stockage et de travail collaboratif, le choix retenu pour le projet est Nextcloud. Cette décision repose sur plusieurs critères liés à la sécurité, à la maîtrise de l'infrastructure et à l'intérêt pédagogique du projet.

Tout d'abord, Nextcloud permet une indépendance totale vis-à-vis des fournisseurs de services cloud externes tels que Google Drive ou Microsoft OneDrive. Les données sont hébergées directement sur le serveur situé dans la DMZ de l'infrastructure, ce qui offre un contrôle complet sur le stockage, la gestion et la confidentialité des fichiers. Cette isolation est essentielle pour garantir la sécurité du système d'information et pour respecter la séparation stricte entre le serveur de fichiers interne et le cloud accessible depuis l'extérieur.

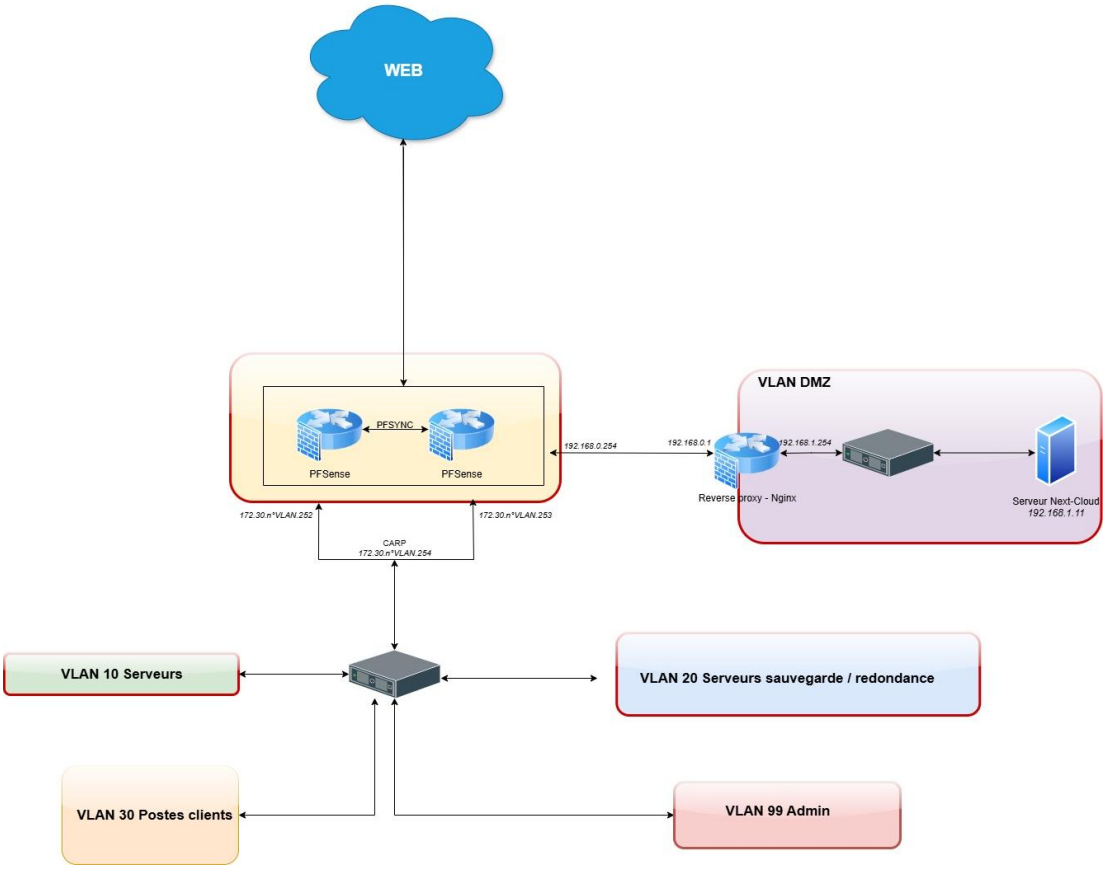
Ensuite, Nextcloud est une solution gratuite et open source, ce qui permet de déployer le service sans coût supplémentaire pour le projet. Cette caractéristique est particulièrement adaptée dans un contexte pédagogique, où l'objectif est de comprendre et de mettre en œuvre les compétences techniques nécessaires à la gestion d'un cloud privé.

Enfin, le déploiement et l'administration de Nextcloud présentent un intérêt pédagogique significatif. Installer, configurer et sécuriser un service de cloud privé permet de mettre en pratique des compétences clés du BTS SIO SISR, telles que la gestion des serveurs, la configuration réseau, la segmentation des VLAN et la mise en place de mesures de sécurité pour un service exposé. Cette solution permet donc de concilier les objectifs fonctionnels du projet avec les objectifs pédagogiques liés à l'épreuve E5.

En résumé, Nextcloud offre la meilleure combinaison entre contrôle des données, sécurité, coût et intérêt pédagogique, ce qui en fait la solution la plus adaptée pour le déploiement d'un service de travail collaboratif dans le cadre de ce projet.

4- Cartographie du réseau

a) Schéma



b) Plan d'adressage

- **Réseau DMZ Externe :**

Réseau	192.168.0.0
Masque	255.255.255.0
1ère Adresse	192.168.0.1
Dernière Adresse	192.168.0.254
Interface Nginx	192.168.0.1
PFSense 1	192.168.0.252
PFSense 2	192.168.0.253
Passerelle CARP	192.168.0.254
Broadcast	192.168.0.255

- **Réseau DMZ Interne :**

Réseau	192.168.1.0
Masque	255.255.255.0
1ère Adresse	192.168.1.1
Dernière Adresse	192.168.1.254
Serveur Nextcloud	192.168.1.11
Passerelle	192.168.1.254
Broadcast	192.168.1.255

c) Tables de routage

- **Reverse Proxy Nginx :**

Réseau	Adresse	Masque	Passerelle	Interface
DMZ Ext	192.168.0.0	255.255.255.0	192.168.0.254	192.168.0.1
DMZ Int	192.168.1.0	255.255.255.0	192.168.1.254	192.168.1.254
Defaut	0.0.0.0	0.0.0.0	192.168.0.254	192.168.0.1

- **PFSense :**

Réseau	Adresse	Masque	Passerelle	Interface
DMZ Ext	192.168.0.0	255.255.255.0	192.168.0.1	192.168.0.254
DMZ Int	192.168.1.0	255.255.255.0	192.168.0.1	192.168.0.254
Defaut	0.0.0.0	0.0.0.0	FAI	WAN

5- Etude de l'impact sur le SI existant

a) Sécurité

L'installation de Nextcloud dans la DMZ permet de protéger le reste du réseau. Le serveur cloud est isolé et n'a aucun accès direct au serveur de fichiers interne, ce qui limite les risques en cas de problème.

Chaque utilisateur dispose d'un compte avec des droits précis, et l'authentification peut être renforcée avec un système à deux facteurs pour sécuriser l'accès.

Le serveur sera également protégé contre les attaques externes grâce à :

- Les pares-feu et le reverse proxy qui filtrent les flux
- des certificats SSL/TLS pour sécuriser les connexions
- des mises à jour régulières pour corriger les vulnérabilités.

Enfin, la journalisation et la surveillance des activités permettront de détecter rapidement tout accès suspect.

En résumé, Nextcloud reste sécurisé grâce à son isolement, au contrôle des accès et aux protections réseau, tout en permettant un accès depuis Internet.

b) Performance

L'ajout de Nextcloud dans l'infrastructure peut affecter les performances si les ressources ne sont pas bien gérées. Le serveur aura besoin d'une partie du processeur, de la mémoire et du stockage disponibles pour gérer les fichiers, les connexions et la synchronisation.

Le trafic vers le serveur passe par les pare-feu et la DMZ, il faut donc que le routage et la bande passante soient suffisants pour éviter des lenteurs, que ce soit pour les utilisateurs internes ou ceux accédant au cloud depuis Internet.

La latence lors de l'accès distant doit rester faible pour que les utilisateurs puissent consulter ou télécharger leurs fichiers rapidement. De plus, Nextcloud peut s'adapter à une augmentation du nombre d'utilisateurs ou de fichiers, mais cette évolutivité dépend des ressources disponibles dans l'environnement virtualisé.

Enfin, grâce à la séparation du serveur Nextcloud dans la DMZ, l'impact sur les autres services internes (serveur de fichiers, sauvegardes, postes clients) reste limité. Un suivi régulier des ressources est toutefois recommandé pour garantir une performance stable.

En résumé, Nextcloud peut fonctionner de manière fluide si les ressources sont bien allouées et que le trafic réseau est correctement géré.

c) Ergonomie

L'intégration de Nextcloud dans l'infrastructure améliore significativement l'ergonomie pour les utilisateurs. Le service offre une interface web intuitive, accessible depuis un navigateur, ainsi que des applications clientes pour Windows, Linux, macOS et appareils mobiles. Cela permet aux utilisateurs de consulter, télécharger et partager leurs fichiers facilement, sans avoir besoin de connaissances techniques avancées.

La solution propose également des fonctions de collaboration, comme le partage de documents, la gestion des droits d'accès et l'édition simultanée de certains fichiers via des extensions compatibles. Ces fonctionnalités facilitent le travail en équipe et simplifient la gestion des documents partagés.

Enfin, l'accès distant depuis Internet offre une flexibilité importante, car les utilisateurs peuvent travailler sur leurs fichiers depuis n'importe quel appareil connecté, tout en conservant un niveau de sécurité adapté grâce à la DMZ et aux mécanismes d'authentification.

En résumé, Nextcloud améliore l'expérience utilisateur en rendant le stockage, le partage et la collaboration sur les fichiers simples et accessibles, tout en restant sécurisé et intégré dans l'infrastructure existante.

6- Phasage de l'intervention

La mise en place de Nextcloud dans l'infrastructure se déroulera en plusieurs étapes :

1. **Préparation de l'environnement**
   - Vérification des ressources disponibles dans Proxmox (CPU, RAM, stockage)
   - Création des VLAN et configuration du routage et des pares-feux si nécessaire
   - Téléchargement des ISO pour les machines virtuelles (Debian 13 pour Nextcloud et pour le reverse proxy, autres serveurs si besoin).
2. **Déploiement de la machine virtuelle pour le reverse proxy**
   - Création d'une VM Debian 13 entre les pares-feux et le serveur Nextcloud
   - Installation et configuration de Nginx en tant que reverse proxy pour sécuriser et gérer le trafic entrant vers Nextcloud.
3. **Déploiement de la machine virtuelle Nextcloud**
   - Création de la VM Nextcloud dans Proxmox avec les ressources allouées
   - Installation du système d'exploitation Debian 13
   - Configuration réseau dans la DMZ pour assurer l'accès via le reverse proxy tout en maintenant l'isolation avec le réseau interne.
4. **Installation et configuration de Nextcloud**
   - Installation du logiciel Nextcloud sur la VM
   - Configuration de la base de données et des paramètres de stockage
   - Création des utilisateurs et attribution des droits d'accès.
5. **Sécurisation du service et du reverse proxy**
   - Mise en place des certificats SSL/TLS sur Nginx pour sécuriser les connexions
   - Configuration des pare-feu et règles de filtrage pour la DMZ
   - Activation de l'authentification renforcée (ex. 2FA) et des logs d'accès sur Nextcloud et Nginx.
6. **Tests fonctionnels**
   - Vérification de l'accès interne et externe au cloud via le reverse proxy
   - Test du partage de fichiers et de la collaboration
   - Contrôle des performances et ajustement des ressources si nécessaire.

L'ajout du reverse proxy Nginx entre les pares-feux et le serveur Nextcloud permet de centraliser le trafic, sécuriser les connexions HTTPS et simplifier la gestion des accès, tout en conservant l'isolation de la DMZ et la protection du réseau interne.

7- Prévision des tests de validation

Pour garantir le bon fonctionnement de Nextcloud et vérifier qu'il répond aux besoins du projet, plusieurs tests seront réalisés avant le déploiement final.

Tout d'abord, des tests d'accès seront effectués pour s'assurer que le serveur Nextcloud est accessible depuis le réseau interne et depuis Internet via le reverse proxy Nginx, avec des connexions sécurisées en HTTPS et des certificats SSL/TLS valides.

Ensuite, des tests fonctionnels permettront de vérifier la création, la modification et la suppression de fichiers, le partage de documents entre utilisateurs avec différents droits d'accès et la collaboration simultanée sur un même document.

Des tests de performance seront réalisés afin de mesurer la rapidité de chargement et de téléchargement des fichiers, de contrôler l'utilisation du processeur, de la mémoire et du stockage, et de tester la montée en charge avec plusieurs utilisateurs connectés simultanément.

Des tests de sécurité vérifieront que le serveur Nextcloud n'a aucun accès au serveur de fichiers interne, que les logs et alertes fonctionnent correctement pour détecter les tentatives d'accès non autorisées et que l'authentification renforcée ainsi que les permissions des utilisateurs sont bien appliquées.

Enfin, des tests de sauvegarde et de récupération seront effectués pour s'assurer que les données stockées sur Nextcloud peuvent être sauvegardées et restaurées correctement en cas de problème.

Ces différents tests permettront de valider que le service est fonctionnel, sécurisé et performant avant sa mise en service pour les utilisateurs.

8- Déploiement

Le déploiement de Nextcloud dans l'infrastructure se fera une fois que toutes les étapes de préparation, d'installation et de tests auront été validées. L'objectif est de mettre le service en production dans la DMZ tout en garantissant la sécurité et la performance de l'ensemble du réseau.

Le déploiement commencera par la mise en service de la machine virtuelle hébergeant le reverse proxy Nginx, qui centralisera le trafic entrant et sécurisera les connexions HTTPS. Ensuite, la machine virtuelle Nextcloud sera activée et connectée au reverse proxy, avec les configurations réseau et les droits d'accès déjà définis lors de la phase de préparation.

Une fois les machines en fonctionnement, des tests de contrôle seront réalisées pour s'assurer que tous les utilisateurs peuvent se connecter et accéder aux fonctionnalités de stockage et de partage de fichiers. Les performances seront également vérifiées pour confirmer que le serveur peut gérer le nombre d'utilisateurs prévus sans impact sur le réseau interne.

Enfin, la documentation de configuration, les guides d'utilisation et les procédures de maintenance seront mis à disposition pour permettre une exploitation efficace du service et faciliter les interventions futures. Le déploiement sera considéré comme finalisé lorsque le service sera pleinement opérationnel, sécurisé et intégré dans l'infrastructure existante.

IV/ Mise en place

1- Réalisation

a) Installation des pares-feu PFSense

- Installation et configuration de PFSense
- Pour la configuration du CARP et de PFSync, se référer à la mise en situation professionnelle Redondance de Pare-feu PFSense

b) Mise en place d'un serveur Nextcloud

- Installation de Debian 13
  - Espace disque : 20 Go
  - Un disque supplémentaire de 100 Go pour stocker les dossiers et fichiers des utilisateurs (dans le cas où une aucune liaison avec le serveur de fichier n'a été faite, ce qui dans le cas d'une DMZ est le plus raisonnable).

- Mémoire : 2 Go
- Cœur : 1

➢ Installation de Nextcloud

c) Mise en place d'un reverse proxy Nginx

➢ Installation de Debian 13
- Espace disque : 20 Go
- Mémoire : 2 Go
- Cœur : 1
- Deux interfaces réseaux :
  - Externe (côté pare-feu) : 192.168.0.1
  - Interne (côté DMZ) : 192.168.1.254

➢ Mise en place d'une DMZ avec le reverse proxy Nginx

2- Rapport de tests

Après l'installation et la configuration du serveur Nextcloud, plusieurs tests ont été réalisés afin de vérifier le bon fonctionnement du service et son intégration dans l'infrastructure réseau.

Dans un premier temps, des tests d'accès ont été effectués. Le service est accessible depuis un navigateur web en passant par le reverse proxy configuré avec Nginx. L'accès au service se fait en HTTPS, ce qui permet de sécuriser les échanges entre le client et le serveur. Les utilisateurs peuvent se connecter avec leurs identifiants et accéder à leur espace de stockage.

Des tests fonctionnels ont ensuite été réalisés pour vérifier les principales fonctionnalités du service. Les utilisateurs peuvent téléverser des fichiers, les télécharger, les modifier et les supprimer. Le partage de fichiers entre utilisateurs fonctionne correctement et les droits d'accès configurés sont respectés.

Des tests de collaboration ont également été effectués afin de vérifier que plusieurs utilisateurs peuvent accéder aux mêmes documents partagés. Les fichiers sont bien synchronisés entre les différents utilisateurs et les modifications sont prises en compte correctement.

Des vérifications de sécurité ont été réalisées pour confirmer que le serveur Nextcloud est bien isolé dans la DMZ et qu'il ne dispose d'aucun accès direct vers le serveur de fichiers interne situé dans le VLAN 10. Le filtrage des flux par les pares-feux configurés avec pfSense fonctionne correctement et garantit l'isolation du réseau interne.

Enfin, l'utilisation des ressources du serveur a été observée afin de vérifier que les performances restent satisfaisantes. L'utilisation du processeur, de la mémoire et du stockage reste stable lors des tests de transfert et d'accès aux fichiers.

L'ensemble de ces tests confirme que le service Nextcloud fonctionne correctement, qu'il est accessible de manière sécurisée et qu'il s'intègre convenablement dans l'architecture réseau mise en place pour le projet.

3- Rapport de déploiement

Une fois l'installation et les tests validés, le service de cloud privé basé sur Nextcloud a été déployé dans l'infrastructure réseau. Le serveur a été installé dans la DMZ afin de permettre un accès depuis Internet tout en maintenant une séparation avec le réseau interne.

Le déploiement s'est déroulé en plusieurs étapes. Une machine virtuelle sous Debian 13 a d'abord été mise en place pour héberger le reverse proxy configuré avec Nginx. Ce serveur joue le rôle d'intermédiaire entre les utilisateurs et le serveur Nextcloud. Il permet de centraliser les connexions entrantes et de gérer la sécurisation des échanges en HTTPS.

Ensuite, une seconde machine virtuelle a été déployée pour héberger l'application Nextcloud. Cette machine est également basée sur Debian 13 et se trouve dans la DMZ derrière le reverse proxy. Le routage et le filtrage des flux entre les différents réseaux sont assurés par les pare-feu configurés avec pfSense, qui permettent de contrôler les communications entre la DMZ et les autres VLAN de l'infrastructure.

Une fois les serveurs installés et configurés, les utilisateurs ont été créés dans Nextcloud et les premiers espaces de stockage ont été mis en place. Des tests finaux ont permis de confirmer que les utilisateurs peuvent se connecter, stocker des fichiers et partager des documents de manière sécurisée.

Le service est désormais opérationnel et accessible via une interface web sécurisée. Grâce à son installation dans la DMZ et à l'utilisation d'un reverse proxy, le système permet un accès distant tout en conservant une bonne isolation avec le reste de l'infrastructure réseau.

V/ Bilan

1- Conclusion

La mise en place d'un service de cloud privé basé sur Nextcloud a permis de répondre aux objectifs définis dans le cahier des charges du projet réalisé dans le cadre de l'épreuve E5 du BTS Services Informatiques aux Organisations, option SISR.

Le service offre désormais une solution de stockage et de partage de fichiers accessible aux utilisateurs, leur permettant de déposer, consulter et partager des documents via une interface web sécurisée. L'accès distant au cloud permet également de travailler sur les fichiers depuis différents appareils connectés à Internet.

L'intégration de ce service dans l'infrastructure existante a été réalisée en respectant l'architecture réseau mise en place, notamment la segmentation par VLAN et l'utilisation d'une zone démilitarisée pour les services exposés. L'ajout d'un reverse proxy configuré avec Nginx et la gestion des flux par les pares-feux sous pfSense permettent d'assurer un accès sécurisé tout en maintenant l'isolation du réseau interne.

Ce projet a également permis de mettre en pratique plusieurs compétences liées à l'administration des systèmes et des réseaux, comme la virtualisation, la configuration de serveurs sous Debian 13, la gestion du routage et du filtrage réseau, ainsi que la sécurisation d'un service accessible depuis Internet.

En conclusion, la solution mise en place répond aux besoins fonctionnels du projet tout en respectant les contraintes techniques et de sécurité de l'infrastructure. Elle constitue également une expérience pédagogique pertinente pour l'apprentissage des pratiques professionnelles liées à l'administration d'un système d'information.

2- Auto-évaluation

La réalisation de ce projet m'a permis de mettre en pratique plusieurs compétences techniques liées à l'administration des systèmes et des réseaux. La mise en place du service de cloud privé avec Nextcloud m'a notamment permis de travailler sur l'installation et la configuration de serveurs sous Debian 13, ainsi que sur l'intégration d'un service dans une architecture réseau segmentée.

Ce projet m'a également permis d'approfondir mes connaissances en matière de sécurité réseau. L'utilisation d'une DMZ, la configuration des règles de filtrage sur les pare-feu sous pfSense et la mise en place d'un reverse proxy avec Nginx m'ont permis de mieux comprendre les mécanismes permettant de protéger un service accessible depuis Internet.

La phase de tests et de validation m'a aussi appris l'importance de vérifier chaque étape du déploiement afin de garantir le bon fonctionnement du service et son intégration dans l'infrastructure existante. Cette démarche est essentielle pour identifier les éventuels problèmes et assurer la stabilité du système.

Avec le recul, ce projet constitue une expérience enrichissante qui m'a permis de consolider mes compétences techniques tout en me confrontant à des problématiques proches de celles rencontrées dans un environnement professionnel. Il m'a également permis de développer une méthode de travail structurée, allant de l'analyse du besoin jusqu'au déploiement et à la validation d'une solution technique.