MISE EN PLACE D'UN SERVEUR VPN

Cédric BAUDIMENT
AgroMousquetaires – Site d'Antartic 2

BTS SIO SISR
Greta Drôme / Ardèche
2024 / 2026

I/ Cahier des charges

1- Descriptif de l'existant

L'environnement existant repose sur un poste de travail fixe disposant d'une connexion Internet fonctionnelle, servant à la fois de poste d'administration et de plateforme de virtualisation.

Ce poste est équipé du logiciel VMware Workstation, utilisé pour créer, configurer et exploiter plusieurs machines virtuelles destinées à simuler une infrastructure réseau complète. Cette solution de virtualisation permet de reproduire un contexte proche d'un environnement professionnel tout en restant contenu sur une seule machine physique.

Les ressources logicielles actuellement disponibles sont les suivantes :

- Une image ISO de pfSense, utilisée comme pare-feu et routeur virtuel
- Une image ISO de Debian 13, destinée à héberger des services réseau, notamment le futur serveur VPN OpenVPN
- Une image ISO de Windows Server 2022, utilisée pour représenter un serveur au sein du système d'information
- Une image ISO de Windows 10, servant de poste client afin de tester l'accès distant via le VPN.

L'ensemble de ces machines virtuelles est interconnecté au sein de réseaux virtuels gérés par VMware Workstation, permettant de simuler des segments réseau internes et une sortie vers Internet.

Cet environnement constitue une base technique suffisante pour la mise en place, le test et la validation d'une solution VPN OpenVPN, sans impacter un système d'information réel.

2- Besoins

Le projet vise à mettre en place une infrastructure VPN permettant à un poste client situé hors du réseau local d'accéder de manière sécurisée aux ressources internes, et plus particulièrement à un serveur Active Directory.

Le besoin principal est donc d'assurer une connexion distante sécurisée entre un poste externe et le réseau interne de l'entreprise, en garantissant l'intégrité, la confidentialité et l'authentification des échanges. Cette connexion devra permettre au poste distant de se comporter comme s'il était physiquement présent sur le réseau local, notamment pour l'accès aux services fournis par le contrôleur de domaine.

Pour répondre à ce besoin, l'infrastructure virtuelle suivante est requise :

- Une machine virtuelle pfSense, jouant le rôle de pare-feu et de passerelle réseau. Elle assurera la gestion du trafic, la séparation des flux WAN et LAN ainsi que l'hébergement du service OpenVPN. Cette machine est dimensionnée avec 256 Mo de mémoire vive, 5 Go d'espace disque et un processeur monocœur, des ressources suffisantes pour un environnement de test.
- Une machine virtuelle Windows Server 2022, destinée à héberger le service Active Directory et à représenter un serveur du système d'information. Elle dispose de 4 Go de mémoire vive, 40 Go d'espace disque et de deux cœurs processeur afin d'assurer le bon fonctionnement des services d'annuaire.

- Une machine virtuelle Debian 13, utilisée comme serveur applicatif et support technique au projet, notamment pour l'administration ou des services réseau complémentaires. Cette machine est configurée avec 2 Go de mémoire vive, 20 Go de disque et deux cœurs processeur.
- Une machine virtuelle Windows 10, représentant un poste client. Elle sera utilisée pour tester la connexion VPN depuis l'extérieur du réseau local et vérifier l'accès au domaine Active Directory. Elle est dotée de 4 Go de mémoire vive, 40 Go d'espace disque et de deux cœurs processeur.

L'ensemble de ces machines virtuelles est connecté au réseau LAN du pare-feu pfSense, permettant une communication interne cohérente. L'interface WAN du pare-feu est configurée en mode NAT, assurant l'accès à Internet tout en isolant le réseau interne.

Cette infrastructure répond aux besoins fonctionnels du projet en offrant un environnement cohérent, sécurisé et représentatif d'un système d'information réel, tout en restant adapté à un contexte pédagogique et de test.

3- Contraintes

La mise en œuvre de la solution VPN s'inscrit dans un environnement de test virtualisé, ce qui implique plusieurs contraintes techniques et fonctionnelles à prendre en compte.

La principale contrainte concerne la simulation de l'accès WAN. En effet, l'infrastructure ne dispose pas d'un véritable accès à un réseau étendu public. L'interface WAN du pare-feu pfSense est configurée en NAT, avec une adresse IP privée fournie par l'environnement de virtualisation. Cette configuration ne permet pas de reproduire totalement les conditions réelles d'un accès Internet public avec une adresse IP publique fixe ou dynamique.

Cette limitation implique que certains aspects, comme l'exposition directe du service VPN sur Internet ou la gestion avancée de règles de pare-feu en contexte réel, ne peuvent être testés que de manière partielle. Le fonctionnement du VPN reste cependant représentatif d'un usage réel du point de vue du client distant et de l'accès au réseau interne.

Une autre contrainte réside dans les ressources matérielles limitées du poste hôte. Toutes les machines virtuelles étant exécutées sur une seule machine physique, le dimensionnement des ressources (mémoire, processeur et stockage) doit rester raisonnable afin de garantir la stabilité globale de l'environnement.

Ces contraintes sont acceptées dans le cadre du projet, car elles n'empêchent pas la validation des objectifs principaux, à savoir la mise en place et le test d'une connexion VPN sécurisée permettant l'accès à un serveur Active Directory depuis un poste distant.

II/ Ressources

1- Ressources mises à disposition

Pour la réalisation de ce projet, plusieurs ressources matérielles et logicielles sont mises à disposition afin de permettre la conception, la mise en place et les tests de l'infrastructure VPN.

La ressource matérielle principale est un poste de travail fixe disposant d'une capacité suffisante pour exécuter plusieurs machines virtuelles simultanément. Ce poste bénéficie d'une connexion Internet

fonctionnelle, indispensable pour les mises à jour des systèmes, le téléchargement des composants nécessaires et la simulation d'un accès distant via le VPN.

Sur le plan logiciel, l'environnement de virtualisation repose sur VMware Workstation, utilisé pour créer et administrer l'ensemble des machines virtuelles constituant l'infrastructure. Cet outil permet la gestion des réseaux virtuels, l'allocation des ressources matérielles et l'isolation des différents rôles serveur et client.

Les systèmes d'exploitation suivants sont également mis à disposition sous forme d'images ISO :

- pfSense, utilisé comme pare-feu et passerelle réseau, intégrant les fonctionnalités nécessaires à la mise en place du service OpenVPN
- Debian 13, destiné à héberger des services réseau et à participer à l'architecture serveur
- Windows Server 2022, utilisé pour le déploiement des services Active Directory
- Windows 10, servant de poste client pour les tests de connexion VPN et d'accès aux ressources internes.

L'ensemble de ces ressources constitue une base complète et cohérente pour mener à bien le projet de mise en place d'un serveur VPN OpenVPN dans un environnement virtualisé.

2- Ressource nécessaire à la mise en place

En complément des ressources déjà mises à disposition, certaines ressources supplémentaires sont nécessaires afin d'assurer la mise en œuvre correcte et fonctionnelle de la solution VPN.

Sur le plan logiciel, la mise en place du service VPN nécessite l'utilisation du service OpenVPN, intégré nativement à pfSense. Cela implique l'accès aux modules de gestion des certificats, à l'outil de configuration du serveur OpenVPN ainsi qu'aux fonctionnalités de gestion des règles de pare-feu et de routage.

La configuration d'un accès sécurisé requiert également la gestion d'une infrastructure de certificats. Celle-ci est assurée par pfSense à travers la création d'une autorité de certification, de certificats serveur et de certificats clients, indispensables à l'authentification des connexions VPN.

Des droits d'administration sur l'ensemble des machines virtuelles sont nécessaires afin de permettre :

- la configuration réseau des systèmes
- l'installation et la configuration des services (Active Directory, OpenVPN)
- l'intégration du poste client Windows 10 au domaine Active Directory après connexion VPN.

Par ailleurs, un temps de mise en œuvre et de test doit être prévu afin de configurer l'infrastructure, vérifier le bon fonctionnement des services et corriger d'éventuelles erreurs de paramétrage, notamment au niveau du routage et des règles de sécurité.

Enfin, une documentation technique (guides d'installation, documentation officielle de pfSense et d'OpenVPN, documentation Microsoft pour Active Directory) est nécessaire pour garantir une configuration conforme aux bonnes pratiques et faciliter le dépannage en cas de dysfonctionnement.

Ces ressources complémentaires sont indispensables pour assurer une mise en place maîtrisée, sécurisée et fonctionnelle de la solution VPN dans l'environnement défini.

3- Gestion des ressources

La gestion des ressources repose sur l'utilisation de la virtualisation afin d'optimiser l'exploitation du matériel disponible.

Les ressources matérielles du poste hôte (processeur, mémoire vive et espace disque) sont réparties entre les différentes machines virtuelles en fonction de leur rôle. Chaque machine virtuelle est configurée avec des ressources fixes, évitant ainsi les conflits ou la surconsommation de ressources.

Les machines virtuelles sont isolées les unes des autres et dédiées à une fonction précise :

- une machine pour le pare-feu et le VPN
- une machine pour le serveur Active Directory
- une machine pour les services sous Linux
- une machine pour le poste client.

Cette organisation permet une administration simplifiée, une meilleure lisibilité de l'infrastructure et un environnement stable pour les phases de configuration et de test.

III/ Analyse

1- Descriptifs des solutions

Dans le cadre de ce projet, trois solutions VPN ont été étudiées afin de répondre au besoin de connexion sécurisée entre un poste distant et le réseau interne : OpenVPN Access Server, OpenVPN Community Edition et WireGuard.

La solution OpenVPN Access Server est une version commerciale d'OpenVPN. Elle propose une interface d'administration web complète permettant de gérer facilement les utilisateurs, les certificats et les connexions VPN. Cette solution est conçue pour simplifier le déploiement et l'administration d'un VPN, notamment dans des environnements professionnels. Une version gratuite existe, mais elle est limitée à un nombre restreint de connexions simultanées.

La solution OpenVPN Community Edition est une version open source et gratuite d'OpenVPN. Elle repose principalement sur une configuration manuelle via des fichiers de configuration et l'utilisation de certificats pour l'authentification. Cette solution est largement utilisée dans les environnements professionnels et pédagogiques, notamment pour sa robustesse, sa flexibilité et son intégration native dans des solutions comme pfSense. Elle nécessite cependant des compétences techniques plus avancées pour sa mise en œuvre et son administration.

Enfin, WireGuard est une solution VPN open source plus récente, conçue pour être simple, rapide et légère. Elle utilise des mécanismes de chiffrement modernes et une configuration minimaliste basée sur des clés publiques et privées. WireGuard est reconnu pour ses performances élevées et sa simplicité de configuration. En revanche, il offre moins de fonctionnalités avancées que OpenVPN en matière de gestion fine des utilisateurs et d'intégration avec certains environnements existants, notamment Active Directory.

Ces trois solutions répondent au besoin de connexion VPN sécurisée, mais présentent des approches, des niveaux de complexité et des fonctionnalités différentes, qui feront l'objet d'une comparaison afin de déterminer la solution la plus adaptée au contexte du projet.

2- Comparaisons des solutions

Critères	OpenVPN Access Server	OpenVPN Community Edition	WireGuard
Type de solution	Commerciale (avec version gratuite limitée)	Open source	Open source
Facilité de mise en œuvre	Élevée (interface web)	Moyenne à complexe (configuration manuelle)	Élevée (configuration simple)
Administration	Interface web complète	Fichiers de configuration	Configuration par clés
Authentification	Certificats, utilisateurs/mots de passe	Certificats	Clés publiques / privées
Intégration avec pfSense	Possible mais non native	Native	Native
Intégration Active Directory	Oui	Possible	Limitée
Performances	Bonnes	Bonnes	Très élevées
Flexibilité de configuration	Élevée	Très élevée	Moyenne
Adaptation à un contexte pédagogique	Moyenne (licence)	Très bonne	Bonne
Coût	Gratuit limité / Payant	Gratuit	Gratuit

3- Choix d'une solution

Après comparaison des différentes solutions VPN, OpenVPN Community Edition est retenue pour ce projet.

Les principaux arguments en faveur de ce choix sont les suivants :

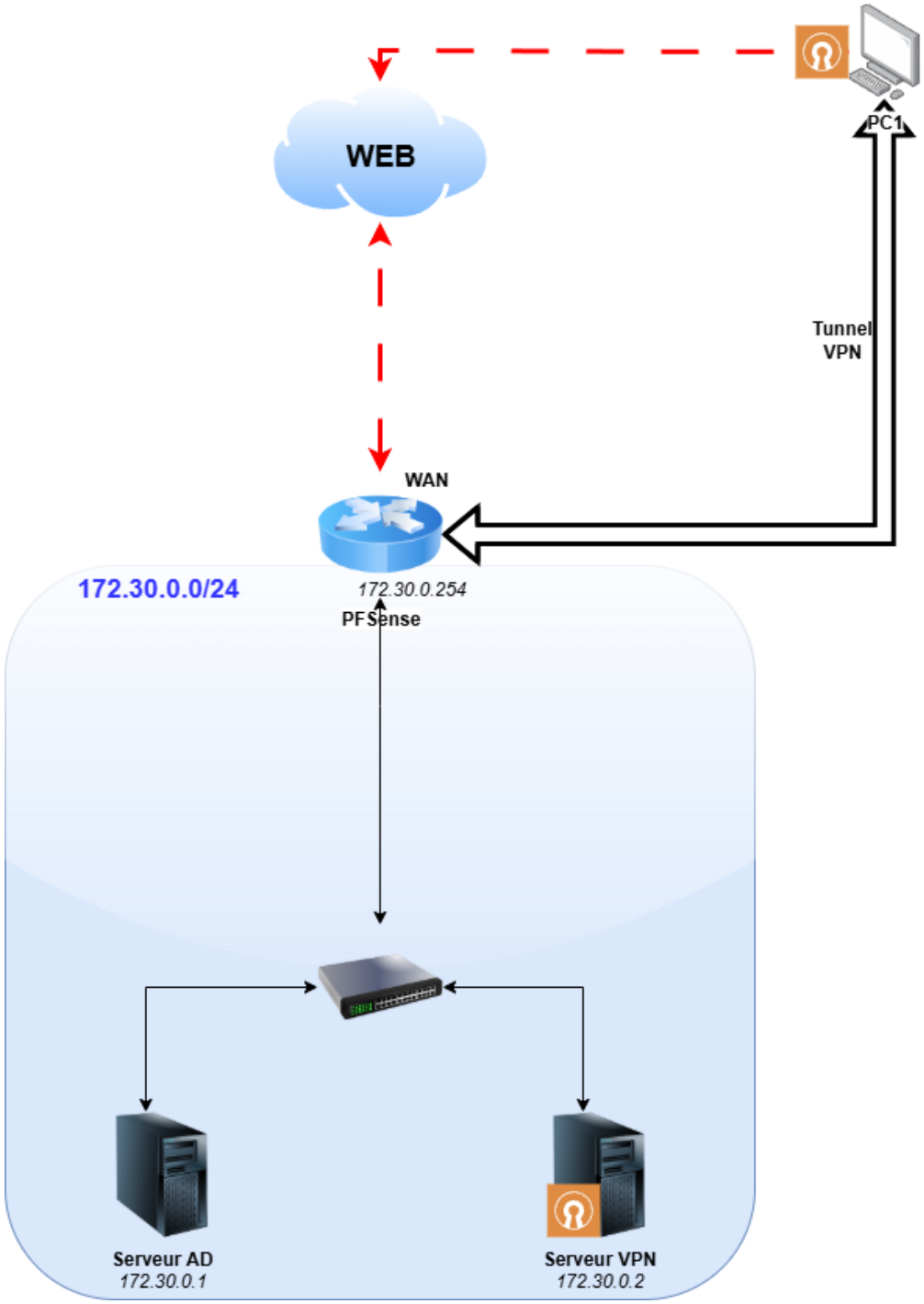
- Compatibilité avec pfSense : OpenVPN Community Edition est entièrement intégré à pfSense, ce qui permet de configurer facilement le serveur VPN, de gérer les certificats et d'administrer le réseau virtuel dans un environnement unifié.
- Gratuité et flexibilité : contrairement à la version Access Server, cette édition est totalement gratuite et offre une flexibilité importante pour la configuration et l'adaptation à l'infrastructure existante.
- Robustesse et fiabilité : OpenVPN Community est largement utilisé dans les environnements professionnels et pédagogiques, garantissant des protocoles de chiffrement éprouvés et une sécurité fiable pour l'accès distant.
- Dimension pédagogique : sa mise en œuvre est plus technique que la version Access Server, nécessitant la gestion manuelle des certificats et des fichiers de configuration. Cette complexité est formatrice et permet de développer des compétences pratiques solides en administration réseau.

Bien que WireGuard présente des performances supérieures et une configuration simple, sa compatibilité limitée avec Active Directory et certaines fonctions avancées de gestion des utilisateurs en font un choix moins adapté pour ce projet centré sur un environnement Windows et pfSense.

Ainsi, OpenVPN Community Edition répond à la fois aux besoins techniques, aux contraintes de l'environnement de test et aux objectifs pédagogiques, tout en permettant une expérimentation complète du VPN dans le cadre du BTS.

4- Cartographie du réseau

a) Schéma



b) Plan d'adressage

Réseau	172.30.0.0
Masque	255.255.255.0
1ère Adresse	172.30.0.1
Dernière Adresse	172.30.0.254
Serveur AD	172.30.0.1
Serveur VPN	172.30.0.2
Plage DHCP	172.30.0.10 - 172.30.0.20
Passerelle	172.30.0.254
Broadcast	172.30.0.255

c) Tables de routage

- **Routage Pare-Feu :**

Réseau	Adresse	Masque	Passerelle	Interface
Réseau AD	172.30.0.0	255.255.255.0	172.30.0.254	LAN
Default	0.0.0.0	0.0.0.0	FAI	WAN

5- Etude de l'impact sur le SI existant

a) Sécurité

L'intégration d'un serveur VPN améliore globalement le niveau de sécurité du système d'information en permettant un accès distant chiffré aux ressources internes.

Les communications entre le poste distant et le réseau local sont protégés par un tunnel VPN chiffré, garantissant la confidentialité et l'intégrité des données échangées. L'utilisation de certificats pour l'authentification des clients renforce la sécurité en limitant les risques d'accès non autorisé.

Le pare-feu pfSense joue un rôle central dans la sécurisation de l'infrastructure. Il permet de contrôler précisément les flux entrants et sortants, en n'autorisant que les connexions VPN nécessaires et en bloquant les accès directs au réseau interne depuis le WAN.

Cependant, l'ouverture d'un accès distant constitue également un nouveau point d'entrée potentiel dans le système d'information. Une mauvaise configuration du VPN, des règles de pare-feu ou des certificats pourrait exposer le réseau interne à des risques de sécurité. Cela nécessite une configuration rigoureuse et une gestion stricte des accès utilisateurs.

Dans l'ensemble, l'impact sur la sécurité est positif, à condition que la solution VPN soit correctement configurée et administrée.

b) Performance

La mise en place d'un serveur VPN entraîne un léger impact sur les performances du réseau.

Le chiffrement et le déchiffrement des données génèrent une charge supplémentaire sur le pare-feu pfSense. Dans le cadre de cet environnement de test, le nombre de connexions VPN est limité, ce qui permet de conserver des performances satisfaisantes.

Cependant, plus le nombre de connexions VPN simultanées augmente, plus la charge sur le routeur et le serveur VPN est importante. Cela peut entraîner une baisse des performances, notamment en termes de débit et de latence.

Afin de supporter un nombre plus élevé de connexions VPN, il serait nécessaire d'augmenter les ressources matérielles du routeur, et éventuellement celles du serveur hébergeant le service VPN, notamment en mémoire vive et en puissance de calcul.

L'impact sur les performances reste donc acceptable dans le contexte actuel, mais il doit être pris en compte dans le cadre d'un déploiement à plus grande échelle.

6- Phasage de l'intervention

La mise en place du serveur VPN est réalisée selon un phasage structuré afin d'assurer une intervention progressive et maîtrisée.

Dans un premier temps, l'environnement de virtualisation est préparé. Les machines virtuelles nécessaires sont créées et configurées avec les ressources matérielles définies dans le cahier des charges. Les systèmes d'exploitation sont installés et mis à jour.

Ensuite, l'infrastructure réseau est mise en place. Le pare-feu pfSense est configuré avec ses interfaces WAN et LAN, le plan d'adressage est appliqué et la connectivité entre les différentes machines virtuelles est vérifiée.

La phase suivante consiste à déployer les services internes. Le serveur Windows Server 2022 est configuré en tant que contrôleur de domaine Active Directory, et les services nécessaires au fonctionnement du réseau sont validés.

Une fois l'infrastructure interne opérationnelle, le serveur VPN OpenVPN est configuré sur le pare-feu pfSense. Cela inclut la création de l'autorité de certification, des certificats serveur et clients, ainsi que la mise en place des règles de pare-feu et du routage nécessaires.

Enfin, le poste client Windows 10 est configuré pour se connecter au VPN. Des tests de connexion sont réalisés afin de valider l'accès sécurisé au réseau interne et aux ressources du domaine Active Directory.

Ce phasage permet de limiter les risques d'erreurs, de faciliter les tests intermédiaires et d'assurer une mise en œuvre progressive de la solution.

7- Prévision des tests de validation

Afin de vérifier le bon fonctionnement de la solution VPN, plusieurs tests de validation sont prévus après la mise en place de l'infrastructure.

Dans un premier temps, des tests de connectivité réseau sont réalisés pour s'assurer que toutes les machines virtuelles communiquent correctement sur le réseau local et que le pare-feu pfSense assure bien le routage entre le LAN et le WAN.

Des tests de connexion VPN sont ensuite effectués depuis le poste client Windows 10. L'objectif est de vérifier l'établissement correct du tunnel VPN, l'authentification du client à l'aide des certificats et l'attribution d'une adresse IP issue du réseau VPN.

Une fois la connexion VPN établie, des tests d'accès aux ressources internes sont réalisés, notamment l'accès au serveur Windows Server 2022 et aux services Active Directory. Cela permet de valider que le poste distant se comporte comme un poste présent sur le réseau local.

Enfin, des tests de stabilité sont effectués afin de vérifier le maintien de la connexion VPN dans le temps et l'absence de coupures lors de l'utilisation des services.

Ces tests permettent de valider que la solution VPN répond aux besoins définis dans le cahier des charges et qu'elle est pleinement opérationnelle avant le déploiement final.

8- Déploiement

Le déploiement de la solution VPN est réalisé dans l'environnement de test défini, sans impact sur un système d'information en production.

Une fois la configuration du serveur VPN OpenVPN, les paramètres de connexion sont exportés sous forme de fichiers de configuration client. Ces fichiers sont ensuite installés sur le poste Windows 10 destiné aux tests.

Le déploiement comprend également l'application des règles de pare-feu nécessaires pour autoriser le trafic VPN et l'accès aux ressources internes du réseau, tout en maintenant un niveau de sécurité adapté.

Après le déploiement, une phase de vérification est effectuée afin de s'assurer que les utilisateurs peuvent se connecter au VPN et accéder aux services du réseau interne, notamment au serveur Active Directory, dans des conditions normales d'utilisation.

Ce déploiement progressif permet de valider la solution avant toute généralisation ou adaptation à un environnement réel.

IV/ Mise en place

1- Réalisation

a) Installation et configuration des machines virtuelles

Quatre VMs seront nécessaires pour la mise en place de cette infrastructure test :

- Une VM PFSense :
  - 256 Go de RAM
  - 5 Go d'espace disque
  - 1 cœur
  - Deux interfaces réseaux :
    - WAN : NAT, adresse définie via DHCP
    - LAN : 172.30.0.254
  - Installation de PFSense
  - Pour ce TP, il est possible de configurer un serveur DHCP sur PFSense afin de fournir une configuration réseau automatiquement aux postes clients. Préciser une plage d'adresse disponible comprise entre 172.30.0.10 et 172.30.0.20 par exemple.
- Une VM Windows server 2022 pour le serveur DNS et Active Directory :
  - 4 Go de RAM
  - 40 Go d'espace disque
  - 2 cœurs
  - Adresse IP : 172.30.0.1
  - Installation de Windows server 2022

- Une VM Debian 13 pour le serveur VPN :
  - 2 Go de RAM
  - 20 Go d'espace disque
  - 2 cœurs
  - Adresse IP : 172.30.0.2
  - Installation de Debian 13
- Une VM Windows 10 en guise de poste client :
  - 4 Go de RAM
  - 40 Go d'espace disque
  - 2 cœurs
  - Adresse IP configurée en DHCP. Ce poste sera connecté directement sur le réseau dans un premier temps puis connecté sur un réseau à part pour le test de la connexion VPN.
  - Installation de Windows 10

b) Installation et configuration d'un serveur DNS et d'active directory sur le serveur AD

- Installation et configuration d'un serveur DNS Nous choisirons pour notre test le nom de domaine MySocCBt.fr.
- Installation et configuration du serveur AD Il est possible de créer de nouveaux utilisateurs pour notre test correspondants aux utilisateurs des postes clients. Ils serviront pour s'y connecter même s'il est tout à fait possible de s'y connecter avec les logins admin.

c) Installation et configuration d'OpenVPN sur le serveur VPN

Dans le cadre de l'installation et de la configuration du serveur VPN OpenVPN, une infrastructure à clés publiques (PKI) est mise en place afin de sécuriser l'authentification et les échanges entre les clients et le serveur VPN.

Une PKI (Public Key Infrastructure) est un ensemble de mécanismes permettant de gérer des certificats numériques. Ces certificats servent à identifier de manière fiable les différents acteurs d'une communication (serveur et clients) et à chiffrer les échanges. Elle repose principalement sur une autorité de certification (CA), chargée de délivrer et de signer les certificats.

Le fonctionnement de la PKI repose sur le principe de la cryptographie asymétrique. Chaque entité dispose d'une paire de clés :

- une clé publique, intégrée dans le certificat et partagée
- une clé privée, conservée de manière confidentielle.

Lors de la mise en place d'OpenVPN, une autorité de certification est créée. Cette autorité permet de générer :

- un certificat serveur, utilisé par le serveur OpenVPN pour s'identifier
- des certificats clients, attribués à chaque poste autorisé à se connecter au VPN.

Lorsqu'un client tente d'établir une connexion VPN, le serveur et le client échangent leurs certificats. Le serveur vérifie que le certificat client est bien signé par l'autorité de certification de confiance. Si la vérification est valide, le tunnel VPN est établi et les échanges sont chiffrés.

L'utilisation d'une PKI permet d'assurer :

- l'authentification des clients et du serveur
- la confidentialité des données échangées
- la gestion fine des accès, grâce à la possibilité de révoquer un certificat en cas de compromission ou de perte d'un poste client.

Ce mécanisme renforce significativement la sécurité de la solution VPN et correspond aux bonnes pratiques utilisées dans les environnements professionnels.

Dans un environnement professionnel disposant d'un annuaire Active Directory (AD), il est également possible d'intégrer la PKI directement au sein de l'infrastructure Microsoft, via le rôle Active Directory Certificate Services (AD CS). Cette approche permet de centraliser la gestion des certificats au niveau du domaine : les certificats peuvent être émis, renouvelés et révoqués automatiquement pour les utilisateurs et les machines du domaine, sans intervention manuelle. L'autorité de certification devient ainsi une CA d'entreprise, pleinement intégrée à l'annuaire, ce qui facilite l'administration et renforce la cohérence de la politique de sécurité. Dans le cadre d'OpenVPN, les certificats clients et serveur peuvent alors être générés et signés par cette CA Active Directory, en remplacement d'une PKI autonome type Easy-RSA.

Pour mettre en place cette PKI, vous pouvez consulter la procédure suivante :

- Installation et configuration d'OpenVPN avec PKI sur un serveur Debian 13

Il est également possible d'installer OpenVPN avec une clé statique, c'est-à-dire une clé de chiffrement pré-partagée générée aléatoirement qui sert à la fois pour l'authentification et le chiffrement du tunnel VPN.

Contrairement à une PKI qui utilise des certificats X.509, la clé statique est identique sur le serveur et tous les clients. Cette méthode est simple à mettre en œuvre mais présente des limites de sécurité : si la clé est compromise, tout le VPN est vulnérable, et il est impossible de révoquer l'accès d'un client sans changer la clé pour tous.

- Installation et configuration d'OpenVPN avec clé statique sur un serveur Debian 13

2- Rapport de tests

Cette phase de tests a pour objectif de valider le bon fonctionnement du serveur VPN OpenVPN ainsi que l'accès aux ressources du réseau interne depuis un poste distant. Les tests sont réalisés depuis le poste client Windows 10 après établissement de la connexion VPN.

a) Connexion VPN

Objectif : Vérifier que le poste client peut établir une connexion VPN sécurisée vers le réseau interne.

Méthode : Le client OpenVPN est lancé sur le poste Windows 10 à l'aide du fichier de configuration et du certificat client fournis lors du déploiement. Une tentative de connexion est effectuée vers le serveur OpenVPN hébergé sur le pare-feu pfSense.

Validation : Le test est considéré comme réussi lorsque le tunnel VPN est établi sans erreur et que le poste client reçoit une adresse IP issue du réseau VPN.

b) Accès au domaine Active Directory

Objectif : Vérifier l'accès aux services Active Directory depuis le poste connecté au VPN.

Méthode : Une fois la connexion VPN établie, le poste Windows 10 tente de communiquer avec le serveur Windows Server 2022. Des tests de résolution de noms et d'accès aux services du domaine sont réalisés afin de s'assurer que le contrôleur de domaine est joignable via le VPN.

Validation : Le test est validé lorsque le poste client peut accéder au domaine Active Directory et utiliser les services associés, démontrant son intégration logique au réseau interne.

c) Accès aux dossiers partagés

Objectif : Vérifier l'accès aux ressources partagées du réseau interne via le VPN.

Méthode : Depuis le poste client connecté au VPN, une tentative d'accès à des dossiers partagés hébergés sur le serveur Windows Server 2022 est effectuée, en utilisant les droits d'accès définis dans l'Active Directory.

Validation : Le test est considéré comme réussi lorsque les dossiers partagés sont accessibles en lecture et en écriture selon les autorisations attribuées à l'utilisateur.

d) Conclusion des tests

Les tests réalisés démontrent que la connexion VPN fonctionne correctement et permet un accès sécurisé aux ressources internes du réseau, notamment au domaine Active Directory et aux dossiers partagés. La solution mise en place répond ainsi aux besoins définis dans le cahier des charges.

3- Rapport de déploiement

Le déploiement de la solution VPN OpenVPN a été réalisé dans l'environnement de test défini au préalable, sans impact sur un système d'information en production.

Après la configuration du serveur OpenVPN, les paramètres de connexion ont été générés sous forme de fichiers de configuration client intégrant les certificats nécessaires. Ces fichiers ont ensuite été déployés sur le poste client Windows 10.

Les règles de pare-feu et de routage nécessaires au bon fonctionnement du VPN ont été appliquées afin d'autoriser les flux VPN et l'accès aux ressources internes du réseau, tout en maintenant un niveau de sécurité adapté.

Une vérification finale a été effectuée afin de s'assurer que la connexion VPN est opérationnelle et que le poste client peut accéder aux services du réseau interne, notamment au serveur Active Directory et aux dossiers partagés.

Le déploiement s'est déroulé sans incident et la solution VPN est pleinement fonctionnelle dans le cadre de l'environnement de test.

V/ Bilan

1- Conclusion

Ce projet avait pour objectif la mise en place d'une solution VPN permettant à un poste situé hors du réseau local d'accéder de manière sécurisée aux ressources internes, notamment à un serveur Active Directory.

La solution retenue, OpenVPN Community Edition, a permis de répondre pleinement aux besoins définis dans le cahier des charges. L'utilisation d'une infrastructure à clés publiques (PKI) a renforcé la sécurité des échanges en assurant l'authentification des clients et le chiffrement des communications.

Les différentes phases du projet, de l'analyse des besoins à la réalisation des tests, ont permis de valider le bon fonctionnement de l'infrastructure. Les tests de connexion VPN, d'accès à l'Active Directory et aux dossiers partagés ont confirmé que le poste distant peut accéder aux ressources internes comme s'il était présent sur le réseau local.

Malgré les contraintes liées à l'environnement de test, notamment l'utilisation d'un WAN en adresse IP privée, la solution mise en place est fonctionnelle, cohérente et conforme aux bonnes pratiques réseau. Elle constitue une base solide pouvant être adaptée à un environnement réel moyennant un dimensionnement matériel approprié.

Ce projet a ainsi permis de mettre en œuvre une solution VPN sécurisée tout en développant des compétences techniques essentielles en administration réseau et systèmes.

2- Auto-évaluation

La réalisation de ce projet a permis de mobiliser et de renforcer plusieurs compétences techniques liées à l'administration des réseaux et des systèmes.

La mise en place de l'infrastructure virtualisée a permis de consolider les connaissances en virtualisation, en configuration réseau et en gestion des machines virtuelles. La configuration du pare-feu pfSense et du serveur VPN OpenVPN a renforcé la compréhension des mécanismes de sécurité réseau, notamment le routage, le filtrage et le chiffrement des communications.

L'utilisation d'une infrastructure à clés publiques (PKI) a permis d'approfondir les notions d'authentification par certificats et de bonnes pratiques en matière de sécurité des accès distants. La configuration et les tests d'accès à un serveur Active Directory ont également contribué à renforcer les compétences liées aux environnements Windows Server.

Ce projet a aussi permis de développer une méthodologie de travail structurée, avec une analyse des besoins, un phasage de l'intervention, des tests de validation et une documentation claire des actions réalisées.

Dans l'ensemble, les objectifs du projet ont été atteints et les compétences acquises sont directement exploitables dans un contexte professionnel. Des améliorations pourraient être envisagées, notamment en termes de montée en charge, de supervision ou de sécurisation avancée, dans le cadre d'un déploiement à plus grande échelle.