PROJET M2i

AP3

LIVRABLE 1

Création d'un système d'information hautement disponible et interconnecté

PROPOSITION TECHNIQUE ET COMMERCIALE

Date limite de réponse : Dimanche 9 octobre 2022

Les résultats, opinions et recommandations exprimés dans ce rapport émanent de l'auteur ou des auteurs et n'engagent aucunement CCI Grand-Est ou CCI Campus

SOMMAIRE

GLOSSAIRE

LAN : Local Area Network

WAN : Wide Area Network

VPN : Virtual Private Network

NAT/PAT : Network Address Translation / Port Address Translation

IDS/IPS : Intrusion Detection System / Intrusion Prevention System

IPSec : Internet Protocol Security

IKE : Internet Key Exchange

DNS : Domain Name System

DHCP : Dynamic Host Control Protocol

RADIUS : Remote Authentication Dial-In User

DFS : Distributed File System

DFSR : Distributed File System Replication

SAN : Storage Area Network

iSCSI : Internet Small Computer Systems Interface

RAID : Redundant Array of Independant Disks

1) PRESENTATION DU GROUPE

1.1) Composition et présentation

Nous sommes le groupe 6, prestataire informatique de l'entreprise ***CDW SafeSecurity***, composé de :

- **DUPE Corentin** : Chef de projet, spécialiste de la mise en place et sécurisation des infrastructures (redondance des serveurs, haute disponibilité, …);
- **LEFEBVRE Dylan :** Membre de l'équipe de projet, spécialiste de la configuration des pares-feux, et sécurisation du LAN;
- **RAKOTOZAFY Winness** : Membre de l'équipe de projet, spécialiste de la sauvegarde et de la disponibilité des données.

1.2) Définitions des rôles et responsabilités

	RÔLES	RESPONSABILITES
DUPE Corentin	Administrateur système et réseaux	✓ Pilotage du projet ✓ Mise en place d'un annuaire d'authentification et service DHCP (ADDS,DNS); ✓ Configuration du service d'authentification (RADIUS) ; ✓ Mise en place d'un portail captif d'accès internet pour les utilisateurs ;
LEFEBVRE Dylan	Technicien d'infrastructure informatique et sécurité,	✓ Installation et configuration du routeur/pare-feu ; ✓ Mise en place des règles de firewall ; ✓ Mise en place et configuration de la communication inter-sites sécurisée à travers le WAN (VPN)
RAKOTOZAFY Winness	Technicien d'infrastructure informatique et sécurité,	✓ Mise en place d'une solution d'accès de données sur le réseau avec redondance (DFS,DFSR) ; ✓ Mise en place d'une solution de sauvegarde vers TrueNAS ✓ Configuration des clichés instantanés vers TrueNAS

2) RAPPEL DES BESOINS ET DES OBJECTIFS

Dans le cadre du Campus du Numérique, CCI Campus ouvre de nouvelles formations dans le secteur du numérique réparties sous 3 secteurs : le studio digital (web designer et marketing digital), la fabrique développement (développement web et applications), l'atelier infrastructure (administration des systèmes, réseaux et cybersécurité).

Par cet évènement, le projet M2i est né, ayant pour objectif d'ouvrir 2 nouvelles salles informatique :

- Une salle à Mulhouse pour la formation BTS SIO (Bac +2)
- Une salle à Strasbourg pour la formation M2i (Bac+5)

2.1) Les besoins du projet

Les **besoins du projet** selon les décisions prises par la DSI en accord avec la Direction Générale sont :

- Mise à disposition des équipements nécessaires à la création des nouvelles salles informatiques pour les formations de BTS SIO basé à Mulhouse et M2i à Strasbourg
- Aménagement des nouvelles salles informatiques pour répondre au cahier des charges techniques, souhait des professeurs et apprenants.
- Installation des serveurs conformément à la décision de la direction générale et du DSI, et respect de tous règlements et lois du numérique de l'Etat français et l'Union Européenne, tout en assurant l'optimisation et une facilitation d'administration au sein de l'équipe technique.

2.2) Les objectifs du projet

Les **objectifs du projet** sont :

- Amélioration le service aux utilisateurs et faciliter d'administration par la DSI
- Réduction les coûts de possession et d'exploitation pour un retour sur investissement
- Facilitation du travail collaboratif au niveau régional
- Sécurisation des systèmes et des données en respectant les dispositions légales

Plus spécifiquement :

- Mise en œuvre d'une liaison WAN inter-sites chiffrée entre Strasbourg et Mulhouse
- Création de serveurs et rôles/serveurs en haute disponibilité ;
- Mise en œuvre d'un portail captif avec authentification forte ;
- Accès des données stockant les dossiers personnels à partir des deux sites par la redondance des données partagés.

3) SOLUTIONS

3.1) Solutions techniques et logicielles

Afin de répondre aux besoins et aux attentes des clients, les solutions techniques et logicielles et recommandées permettront en finalité une facilité d'administration aux administrateur et technicien de la Direction des Systèmes d'Information.

3.1.1) Annuaire authentification (Active Directory)

Pour l'annuaire d'authentification, nous recommandons de recourir à l'annuaire Active Directory sous Windows Server 2019. Le choix se justifie par le fait qu'il puisse satisfaire les besoins du client, par la présence d'une interface graphique interactive (user-friendly), qui facilite la création, la gestion et l'administration des objets de l'environnement.

Un serveur d'annuaire est un serveur qui fournir un service d'annuaire, permettant une gestion optimale des objets sur le réseau, normalisation, authentification et l'administration de plusieurs utilisateurs/groupes/services sur un large réseau d'un domaine.

Et encore de plus, étant sur un serveur sous Windows Server, primo le service DNS sera automatiquement installé avec le rôle AD DS, mais nous installerons également le service DHCP afin de permettre au client de s'attribuer une adresse IP de manière dynamique.

Avantages :

- Interface user-friendly facilitant la création, gestion et administration des objets de l'environnement ;
- Permet d'unifier l'authentification, par l'implémentation du Single Sign On avec l'utilisation de Kerberos.
- Puissante et très utilisé en entreprise du fait de sa facilité de déploiement.

Inconvénients :

- Nécessite de grandes ressources matérielles (CPU,RAM,Stockage), ainsi coût élevé de mise en place
- Réservé à un environnement Windows et nécessite ainsi d'acheter une licence Windows Server.

3.1.2) Accès des données sur le réseau (DFS) et redondance des données (DFSR)

Pour la solution d'accès des données (utilisateurs, éducatives, organisationnelles) sur le réseau, nous mettrons à disposition le système de fichiers distribués (DFS), disponible dans la licence Windows Server.

Ce système permet de structurer les fichiers partagés sur différents serveurs de réseau de façon logique. Il permet de référencer un ensemble de partages qui sera accessible de

manière uniforme, puis de centraliser l'ensemble des espaces disponibles sur l'ensemble de partage. Le DFS fonctionne avec un système d'espace de noms, qui permet donc de faciliter la tâche de l'administrateur, sans recourir à l'utilisation des chemins UNC (\\nomserver\nompartage).

De plus, DFS se repose sur le partage SMB qui est implémenté de base dans les systèmes de fichiers de Windows, dont nous expliciterons plus spécifiquement dans une documentation technique à destination des administrateurs.

Avantages :

- Simplification d'administration en cas de panne d'une cible DFS (redirection facilité grâce à l'utilisation de l'espace de noms)
- Performance : fonction de mise en cache pour des gains de performance
- Co-fonctionnalité avec les ACL situées au niveau de système de fichiers
- Sécurité : tolérance aux pannes
- Evolutive : en cas d'espace insuffisante, l'ajout d'un disque supplémentaire peut facilement être ajoutée.

Inconvénients :

- Solution propriétaire, et sous licence à Windows
- Donc coûteux, lié aux prix des licences

3.1.3) Solution de sauvegarde complète (SAN, cible iSCSI)

La sauvegarde est un principe, une norme à mettre à disposition dans une environnement de production, et rentre dans un contexte de sécurité, et de disponibilité des données. Elle n'est pas à négliger, et doit être mise en place et redondé sur plusieurs sites, ce que nous vous proposerons dans cette solution.

La sauvegarde complète des données intégrales des serveurs seront stockés dans un stockage SAN montée par TrueNAS, accessible par les serveurs par un montage iSCSI, qui permettra de créer des disques virtuels pointant vers les disques physiques de TrueNAS.

L'intérêt et l'avantage est qu'en cas de panne de nos serveurs, les données seront encore disponibles sur nos servers TrueNAS, et encore, grâce au recours à des disques SAN, nous proposons un gain de performance considérable sur la lecture et l'écrite des disques de sauvegarde, facilitant ainsi la gestion et l'administration des sauvegardes par l'équipe technique.

Aussi, avec les deux disques physiques de notre serveur SAN, nous appliquerons une tolérance aux pannes en configurant et mettant en place un RAID 1 (miroir) afin de garantir la sécurité et la disponibilité des données du corps éducatif de la CCI Campus.

Avantages :

- Tolérance aux pannes : RAID 1 sur les disques physiques TrueNAS.
- Sauvegarde complète des données performant grâce au recours au SAN
- TrueNAS intègre également une solution de snapshots (clichés instantanés) qui pourront être exploitables dans des cas spécifiques.

Inconvénients :

- Nécessite de nombreuse configuration du côté serveur Windows, et le serveur de stockage TrueNAS (requiert l'attention et l'expertise du technicien et administrateur responsable de l'installation/configuration)
- TrueNAS nécessite de grandes ressources matérielles (voir configuration minimum requise).

3.1.4) Solution de clichés instantanés (Shadow Copy)

Shadow Copy utilise l'utilitaire Volume Shadow Copy Service (VSS) afin de restaurer un fichier, un dossier en volume sur un serveur de fichiers. L'intérêt est que VSS permet de prendre les clichés instantanés d'un disque physique entier sans pour autant nuire aux activités du serveurs/disques cibles.

A priori, nous considérerons que les clichés instantanés permettent de faire « une sauvegarde » d'une partition en ne stockant que les fichiers modifiés. Toutefois, les snapshots ne sont pas considérés comme une réelle sauvegarde, dans la mesure où les snapshots seront tout de même stockés sur le disque en usage, en différence d'une sauvegarde délocalisée, et donc n'est pas tolérable aux pannes hormis une configuration permettant de stocker les clichés instantanés sur un point de montage disque virtuel délocalisé.

En tenant compte de la demande et des besoins du clients, l'implémentation de la solution de clichés instantanés est une alternative intéressante en matière de sauvegarde, permettant de dépanner le plus rapidement possible l'utilisateur finale en cas d'une mauvaise manipulation effectuée par ledit utilisateur.

Avantages :

- Permet de faire des restaurations d'un serveur de fichier « à chaud » en prenant peu de ressource sur le serveur.
- Permet de restaurer un fichier rapidement en comparaison de la plupart des logiciels de sauvegarde.

Inconvénients :

- Les clichés instantanés ne remplacent pas une vraie sauvegarde
- Pas tolérable aux pannes matérielles du fait que les clichés instantanés sont stockés sur le même disque en utilisation par défaut.

3.1.5) Routeur/pare-feu (pfSense)

a) Présentation pfSense

Afin de sécuriser votre réseau interne, nous vous proposons d'installer un routeur, qui sera également votre pare-feu afin de minimiser les coûts.

La solution que nous vous recommandons est pfSense, qui est une solution open-source, gratuit, et englobe diverses fonctionnalités. Pfsense a pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD [1].

PfSense utilise le pare-feu à états qui garde en mémoire l'état de connexions réseau, comme les flux TCP, ou les communications UDP qui le traversent. Le fait de garder en souvenir les états de connexions précédents permet de mieux détecter et écarter les intrusions et assurer une meilleure sécurité), introduisant ainsi une fonctionnalité d'IDS/IPS.

Le pare-feu utilisé par pfSense est Packet Filter, (pare-feu logiciel et officiel d'OpenBSD, écrit à l'origine par « Daniel Hartmeier » qui est un logiciel libre gratuit).

PfSense comporte des fonctions de routage et de NAT[2], lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires, et convient aussi bien pour la sécurisation d'un réseau domestique ou d'entreprise.

b) Mise en place et configuration matérielle requise

PfSense peut fonctionner sur du matériel de serveur ou bien domestique, sur des solutions embarquées sans toutefois demander beaucoup de ressources ni de matériel puissant. Toutefois, il est à savoir que l'utilisation de pfSense sur un matériel physique est plus recommandée que le recours à un pare-feu hébergé sur une machine virtuelle.

Voici pour idée la configuration requise :

	Configuration minimale	Configuration recommandée
Processeur	600 Mhz	1Ghz
Mémoire Vive	512 Mo	1 Go
Stockage	Egale ou supérieur à 4 Go	Egale ou supérieur à 20 Go

[1] FreeBSD est un système d'exploitation FreeBSD est une contraction du mot « Free » qui signifie libre et « BSD » qui signifie Berkeley software distribution).

[2] NAT, Network Address Translation, traduction d'adresse réseau, lorsqu'il fait correspondre des adresses IP a d'autre adresses IP

c) Fonctionnalité de pfsense

A présent voici quelque fonctionnalité qu'offre PFSense :

- Pare-feu/Routeur
- NAT/PAT (Network Address Translation / Port Address Translation
- IDS/IPS (Intrusion Detection System/ Intrusion Prevention System)
- VPN (virtual private network) avec 4 options de connectivité de VPN : IPsec, OpenVPN, Point-to-Point tunneling Protocol ou PPTP et Layer 2 tunneling Protocol ou L2TP
- RRD graphique : l'utilisation du processeur, le débit total, état du firewall etc.
- Dynamic DNS
- Portail Captif
- Proxy transparent
- Proxy filtrant

Avantages

- Gratuit et open-source
- Intègre des solutions VPN natifs
- Peu gourmand en ressources
- Intègre des plugins IDS/IPS
- Intègre-le NAT/PAT

Inconvénients

- Prise en main de l'interface difficile au début
- Langue du clavier en ENG par défaut (difficile à prendre en main pour les adeptes du clavier FR)
- Pas de mise à jour régulier en comparaison de ses concurrents

d) Comparatif : pfsense vs OPNsense

OPNsense est un pare-feu/routeur basé sur FreeBSD et un fork de pfSense. En effet, après un désaccord sur le développement de pfSense et au niveau de la licence, des équipes de développeurs ont quitté le projet pour fonder OPNSense en 2015, pour ensuite devenir le concurrent principal de pfSense.

Globalement il est similaire à son « grand frère » pfSense, l'un des changements majeurs est son interface graphique et qui peut paraitre plus agréable à celui de pfSense pour certains, et désagréable pour d'autre.

Parmi les fonctionnalités de OPNSense, nous retrouverons les mêmes, hormis quelques différences :

- VPN : contrairement à pfSense, OPNSense ne propose lui que OpenVPN et IPsec
- RRD Graphics : qualité, le trafic, le système etc.
- Dynamic DNS

- Règle de pare-feu
- Portail Captif : comme pfSense on va retrouver les mêmes modes d'authentification, LDAP, RADIUS, sans authentification.

Avantages OPNSense

- Gratuit et open-source
- Simple et rapide
- Mise à jour régulier du système et des fonctionnalités
- Support : documentation riche sur le site officiel sur l'installation, configuration et exploitation de l'outil

Inconvénients OPNSense

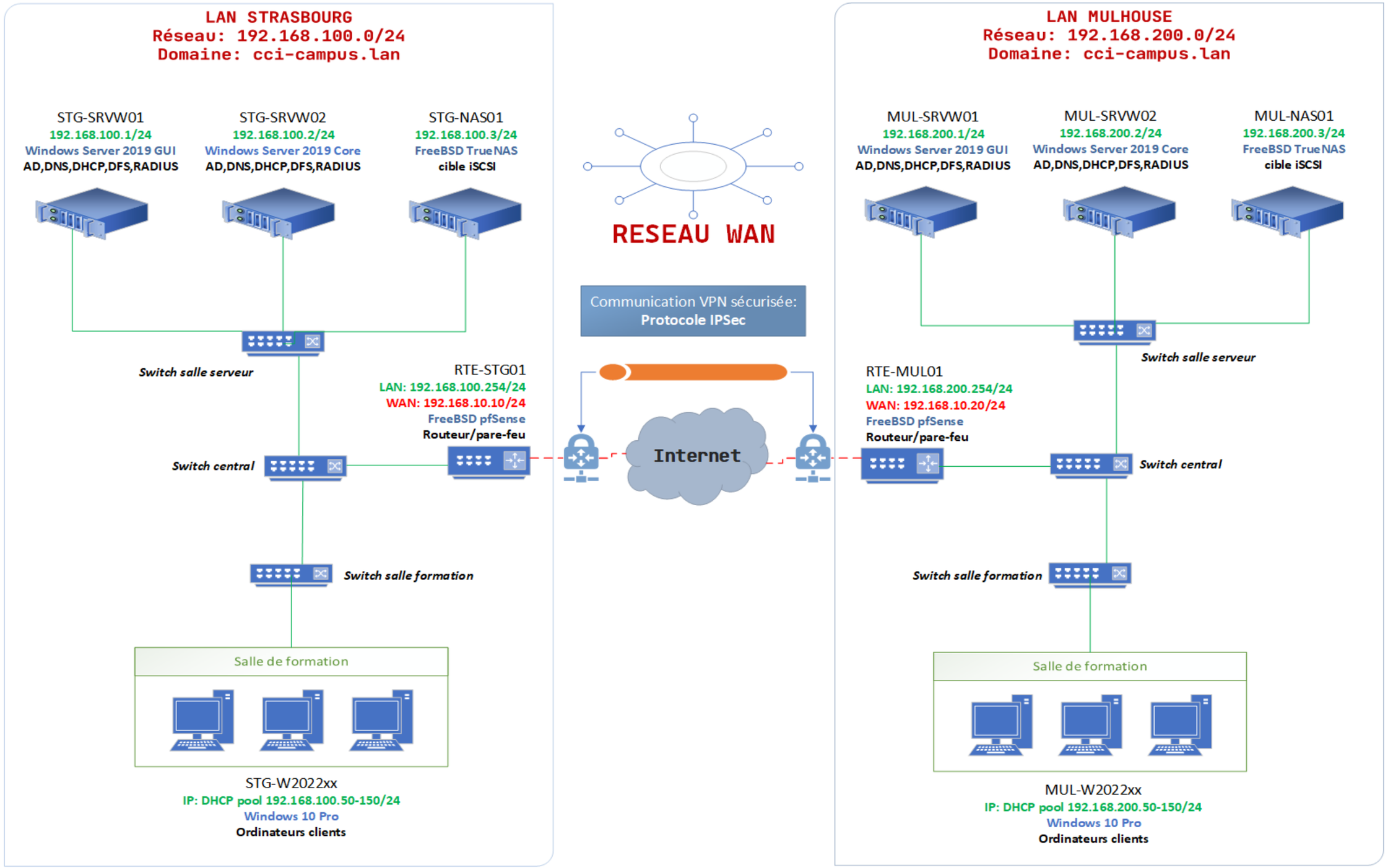
- Nécessite plus de configuration matérielle (voir site officiel https://opnsense.org/)
- Solutions VPN limitées (IPSec et OpenVPN uniquement)

e) Choix retenue pour le routeur/pare-feu

Choisir entre pfSense et OPNSense est ainsi selon les préférences des utilisateurs. En finalité, des deux solutions offrent les mêmes fonctionnalités et offrent une administration similaire au niveau du menu. La guerre des communautés sur les produits continue de s'enflammer sur Internet, mais pour avoir une solution optimale et qui répond à vos besoins, nous avons fait le choix de partir sur la solution de **pfSense**, pour plusieurs raisons :

- L'outil reste gratuit
- L'équipe informatique a déjà dû réaliser des interventions de déploiement de VPN site-à-site sur ce produit vous assurant ainsi une efficacité dans la mise en service de la solution
- Une base connaissance est déjà mis en place ce qui facilite sa mise en place et son dépannage si besoin
- Rationalisation des services au sein d'un seul et même outils ce qui permets de baisser les coûts

3.2) Schéma réseau complet



3.3) Tableau de synthèse

SITES	NOM	ADRESSE IP	MASQUE	PASSERELLE	DNS
STRASBOURG	RTE-STG01	LAN :192.168.100.254 WAN :192.168.10.10	255.255.255.0	WAN :192.168.10.254	192.168.100.1 192.168.100.2
	STG-SRVW01	192.168.100.1	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
	STG-SRVW02	192.168.100.2	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
	STG-NAS01	192.168.100.3	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
	STG-W2022xx	DHCP	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
MULHOUSE	RTE-MUL01	LAN :192.168.200.254 WAN :192.168.10.20	255.255.255.0	WAN :192.168.10.254	192.168.200.1 192.168.200.2
	MUL-SRVW01	192.168.200.1	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
	MUL-SRVW02	192.168.200.2	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
	MUL-NAS01	192.168.200.3	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
	MUL-W2022xx	DHCP	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2

3.4) Etude du choix de la solution VPN Site à Site

Un VPN est un réseau virtuel privé, un système permettant de créer un lien direct entre des ordinateurs distants, qui isole et sécurise leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

On utilise notamment ce terme dans le contexte du « télétravail », ainsi que dans le cadre de « l'informatique en nuage » soit le *cloud computing.*

De nos jours, il existe plusieurs types de protocole VPN, à savoir : PPTP, IPSec et OpenVPN, Wireguard, etc .

Toutefois, le choix du protocole VPN dépend également de l'utilisation et besoins des entreprises. Il existe principalement deux grandes utilisations du VPN :

- ✓ Connectivité client-serveur, qui est fortement utilisé dans un contexte nomade, télétravail ;
- ✓ Connectivité inter-sites avec un serveur VPN sur chaque site créant ainsi un tunnel site-to-site ;

En tenant compte de vos besoins et du cahier des charges, le deuxième cas est le plus amène à répondre à votre demande, ce qui nous mène à choisir entre deux protocoles : IPSec, le protocole intervenant sur la couche 3 du modèle OSI, et OpenVPN, qui opère à la couche 4 du modèle OSI en encryptant la couche Applicative.

3.4.1) IPSec : le protocole VPN de niveau 3

IPSec, pour Internet Protocol Security, est un protocole développé par un groupe de travail à l'IETF (Internet En-gineering Task Force) depuis 1992 afin de sécuriser le protocole IP. Il fait l'objet de plusieurs RFC dont la 2401. Il a été conçu à l'origine pour IPv6, mais son portage sur IPv4 a été formalisé en 1995. IPSec a l'avantage d'offrir l'ensemble des services de sécurité attendus sur un VPN:

- Le tunnelling : ouverture d'un tunnel sécurisé, durant lequel IPSec ajoute un nouvel en-tête au paquet IP en remplaçant les adresses sources et destination du paquet par les adresses du tunnel. Cela rajoute également un en-tête spécifique, le SPI pour Security Parameter Index, qui permet d'identifier les liaisons entre le tunnel source et destination (en statique, ce paramètre est configuré par un administrateur, et en dynamique, il est généré par IKE par un échange de clé partagée) ;
- Le contrôle d'accès: par la Security Policy Database (SPD), qui offre une variété importante de contrôle d'accès grâce aux sélecteurs IP (ceux-ci peuvent contenir en plus des adresses source et destination, le numéro de port du service demandé et autres informations permettant d'étendre le contrôle d'accès) ;
- Le cryptage des données: qui est assurée par un chiffrement des données (symétrique ou asymétrique) ;

- Le contrôle d'intégrité: qui consiste à ajouter à chaque paquet IP le résultat d'un calcul de hachage (SHA-1 ou MD5) portant sur tout ou partie du datagramme. Le calcul d'intégrité est réalisé par l'équipement source pour être systématiquement contrôlé par l'équipement destinataire. Le résultat du calcul d'intégrité s'appelle ICV (Integrity Check Value) ;

Outre le mode **tunnel** expliqué précédemment, IPSec utilise également un autre mode de communication : le mode **transport**. En mode Transport, l' entête spécifique (vue en mode Tunnel) est également ajoutée au paquet IP. La différence réside dans le fait qu'ici l' entête IP d'origine est utilisée tout le long du canal de transmission même lorsqu'on utilise un chiffrement. Seules les données sont protégées. Ce sera le mode privilégié pour le tunneling de bout en bout offert aujourd'hui par des protocoles comme L2TP (protocoles de niveau 2).

Au niveau de l'authentification, IPSec utilise 2 modes :

- AH permet d'assurer l'authentification et l'intégrité des datagrammes IP mais sans cryptage des données. (Il n' y a donc pas de confidentialité).
- ESP permet aussi le cryptage des données, y compris des adresses réelles (dans le cadre d'un mode tunnel). Ce mode est le plus privilégié actuellement dans l'implémentation du VPN site-à-site.

Et enfin, le protocole IPSec nécessite l'utilisation des ports spécifiques dont le port TCP 50 ou 51 selon le protocole de sécurité choisi, et le port UDP 500 pour l'échange de clé par IKE, limitant ainsi sa flexibilité.

Avantages :

- Bonne compatibilité : IPSec est natif sur une grande majorité d'équipement réseau, ne requiert aucun logiciel tiers.
- Optimale pour une communication site-a-site
- Protocole sécurisé dès l'échange IP entre deux sites, utilisant un système d'échange de clé, qui peut être attribué dynamiquement par IKEv2

Inconvénients :

- Système de chiffrement décrypté par la NSA (plusieurs articles en parlent), mais nécessite tout de même une bonne compréhension de la cryptographie
- Peut facilement être bloqué par les règles de pares-feux si les ports spécifiques au tunnel ne sont pas autorisés.
- Requiert l'ouverture de certains ports : 50, 51 et 500, pouvant ainsi être analyser par des un scanner de ports.

3.4.2) OpenVPN : le protocole VPN de niveau 4

OpenVPN est un outil open source utilisé pour construire des VPNs site à site à base du protocole SSL/TLS ou avec des clefs partagées. Son rôle est de "tunneliser", de manière sécurisée, des données sur un seul port TCP/UDP à travers un réseau non sûr comme Internet et ainsi établir des VPNs.

Un protocole OpenVPN permet à des homologues de s'authentifier mutuellement en utilisant une clé secrète pré -partagée, des certificats ou un nom d'utilisateur/mot de passe. Lorsqu'il est utilisé dans une configuration multi client-serveur, il permet au serveur de libérer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification.

Son principal défaut est qu'il n'est natif dans plusieurs équipements réseaux, et nécessite une installation d'une application tierce afin d'établir la connexion sécurisée entre les clients et du site-à-site, qui donnerait un léger avantage à IPSec comme solution VPN inter-site.

Cependant, OpenVPN présente également de nombreuses fonctionnalités :

- VPN couche 2 et 3 : qui permet ainsi de transport les trames Ethernet, les paquets IPs, mais aussi les paquets NetBIOS, qui s'avèrerait problématique sur d'autres solutions.
- Tunneling à travers les pares-feux : fonctionnel en se reposant sur le port 443, qui est généralement autorisé par le pare-feu. Aussi, OpenVPN support les trafics en NAT, ce qui n'est pas toujours le cas des autres protocoles VPN.
- Transparent, peut support les IP dynamiques : il n'est plus nécessaire de configurer les adresses IP en statique sur les deux bouts du tunnel VPN.
- Fiable et sécurisé : son logiciel tiers a passé plusieurs tests et les résultats lui sont favorables. Toutefois, il est toujours connu qu'une application peut à l'avenir présenter des failles de sécurité, ce qui lui ferait défaut du fait qu'OpenVPN rajoute une couche logicielle, ouvrant ainsi une porte aux attaquants en cas de faille.

Avantages :

- Open-source et gratuit
- Ne nécessite pas l'ouverture de ports spécifiques au niveau du pare-feu et autorise le trafic NAT dans le tunnel VPN
- Sécurité : utilise l'encryptions SSL/TLS pour chiffrer le flux des données

Inconvénients :

- Non-natif dans une grande partie des équipements réseaux : nécessite l'installation d'une application tierce
- Difficile à mettre en place, et nécessite la connaissance des cryptographies SSL/TLS pour comprendre son fonctionnement.

3.4.3) Choix de solution VPN site à site

Pour la solution du VPN site à site, parmi les deux solutions proposées, nous avons fait le choix de recourir au protocole **IPSec/IKEv2** par le fait que :

- IPSec est supporté et natif sur une majorité d'équipements réseaux
- IPSec est un standard ouvert : adapté sur plusieurs protocoles d'authentification et algorithmes de chiffrement ;
- IPSec est sécurisé : chiffrement de point à point des communications, et intervient à une couche basse du modèle OSI et TCP/IP (niveau 3) opérant ainsi une sécurité dès le protocole IP avant de transporter les données.

3.5) Etude du choix de la solution de Portail Captif

Un portail captif est un dispositif qui permet de gérer l'authentification des utilisateurs d'un réseau de consultation (LAN) qui souhaitent accéder à un réseau externe (WAN), généralement Internet. Il oblige les utilisateurs du réseau local à s'authentifier avant d'accéder au réseau externe.

En effet, le portail captif capture la demande de connexion par un routage interne et propose à l'utilisateur de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification s'effectue par une requête HTTP vers une page web HTTP stocké sur le serveur (ou pare-feu), qui est la page d'authentification hébergeant le portail captif. Une fois l'utilisateur authentifié, les règles de pare-feu appliqué à l'interface WAN s'appliqueront sur celui-ci, et sa connectivité peut être limité (ou non) par une durée fixée par l'administrateur.

Les identifiants de connexion sont stockés dans une base de données locale ou à travers un serveur distant via le protocole RADIUS.

Ce dispositif offre donc une sécurité du réseau mis à disposition, il permet de respecter la politique de filtrage web de l'entreprise grâce au proxy, et permet également une traçabilité des connexions établies du réseau de consultation en cas d'audit de sécurité.

En bref, le portail captif fonctionne sur le modèle catch and release, c'est-à-dire que lorsqu'un utilisateur souhaite avoir accès à une ressource, il est aussitôt "catch" et redirigé vers le serveur web d'authentification qui ne le "release" qu'au moment où son authentification (login/mot de passe) se sera déroulée avec succès.

Comme choix techniques, nous vous proposerons deux options : le portail captif intégré dans le système de pfSense, et la solution ALCASAR développé par une équipe française, projet mené par Rexy.

3.5.1) Portail captif sous pfSense avec RADIUS

PfSense intègre nativement une fonctionnalité de portail captif qui peut être utilisé soit en utilisant la base de données locale des utilisateurs, soit en redirigeant l'authentification des utilisateurs vers un serveur externe disposant d'un protocole RADIUS (dans notre cas, les serveurs Active Directory).

Qu'est-ce que le protocole RADIUS ? RADIUS est un protocole client-serveur permettant de centraliser des données d'authentification. L'authentification RADIUS permet aux utilisateurs d'un réseau local d'un écosystème Windows de se connecter à notre portail captif en utilisant leurs identifiants Windows.

L'authentification RADIUS nécessite que l'on soit dans un domaine administré par un contrôleur de domaine qui définit les utilisateurs et leur mot de passe. Ainsi, pour mettre en place le portail captif en utilisant les mêmes identifiants Active Directory, en réponse à vos besoins et à votre demande, le serveur RADIUS (avec AD) et le routeur/pare-feu pfsense doivent être dans le même domaine, et ils communiquent dans le but d'autoriser ou non les utilisateurs à se connecter.

L'intérêt de vous proposer la solution de pfSense réside également dans le fait que la solution est gratuite, et génère également moins de coût car elle peut se mettre en place en accord avec les solutions techniques et logicielles proposées précédemment dans *3.1. Solutions techniques et logicielles.*

Toutefois, le portail captif sous pfSense présente des défauts en termes de pratique et d'administration, notamment lié à la conformité à la RGPD et de la CNIL. Pour plus de détails, la journalisation des activités (logs) de connexion des utilisateurs ne sont pas supprimés automatiquement au bout d'un an (durée maximale de conservation des traces de connexions des utilisateurs), mais surtout dans le fait que les utilisateurs ne sont pas avertis à chaque consultation des journaux d'activités des administrateurs pouvant ainsi porter atteinte au respect de la vie privée de ces derniers.

Avantages

- Open-source et gratuit
- Natif dans la solution de routeur/pare-feu
- Centralisation des authentifications par RADIUS : identifiants Active Directory
- Documentation riche en information disponible sur Internet
- Connaissance de l'installation et paramétrage de l'outil par les membres de l'équipe de projet
- Facilité de mise en place du portail captif (nous permettant ainsi de respecter le planning sur le temps de déploiement de la solution)

Inconvénients

- Non conforme à la RGPD : les activités de connexion des utilisateurs sont visibles par l'administrateur du routeur/pare-feu sans chiffrement
- Non conforme à la CNIL : la journalisation des activités de connexion sont stockés sur le routeur/pare-feu sans une fonctionnalité de suppression automatique => Les activités des utilisateurs peuvent donc être stockés à plus d'un an (durée maximale d'une conservation de journal d'activité des utilisateurs)

3.5.2) Portail captif ALCASAR

ALCASAR est un contrôleur sécurisé d'accès à Internet libre et gratuit sous licence GPLv3, qui authentifie, impute et protège les accès des utilisateurs indépendamment des équipements utilisés. Intégrant plusieurs mécanismes de filtrage par utilisateur, il permet de répondre aux besoins des entreprises et des organismes accueillant des mineurs. En France et en Europe, il permet aux responsables d'un réseau connecté à Internet de répondre aux obligations légales et règlementaires.

ALCASAR tourne sur la distribution Mageia de Linux et s'installe par un script d'installation. Une version plus interactive peut être utilisé pour l'installation, une image ISO qui inclut à la fois l'installation de la distribution, et l'outil ALCASAR. Vous trouverez plus d'information sur la partie installation et la présentation d'ALCASAR sur le site officiel du projet : www.alcasar.net.

ALCASAR a le mérite de bien prendre en compte les recommandations de l'ANSSI et de la CNIL sur la mise en place d'un portail captif sur un réseau interne, notamment sur la **journalisation des activités** (journalisation hebdomadaire, et archive supprimée après un an qui est la durée maximale imposé par la CNIL sauf pour motif légitime) et du **filtrage** (protocole, DNS, IP basé sur la blacklist de Toulouse) du réseau de consultation (réseau LAN).

Et encore, la consultation des journaux d'activité des utilisateurs n'est pas accessible sans un motif réel (possibilité ainsi de chiffre les journaux d'activité), qui sera également affiché sur la génération des rapports afin de respecter les droits et les données personnelles des utilisateurs du réseau LAN, et qu'afin d'éviter tout abus, **tous les utilisateurs seront avertis lors de leur prochaine connexion qu'un tel document a été généré,** pour ainsi être conforme au RGPD.

Fonctionnalités et caractéristiques

Pour mettre en place ALCASAR, nous pouvons installer le contrôleur sur un équipement physique, soit sur une machine virtuelle. Dans les deux cas, comme le cas d'un pare-feu, la machine se doit de détenir deux cartes réseaux, dont la première, dédié pour se connecter au réseau d'Internet, et la deuxième pour le réseau interne. En bref, considérons le fait qu'ALCASAR puisse également servir d'une barrière de sécurité qui jouera le rôle du pare-

feu en interne en plus d'un pare-feu natif de notre réseau.

En plus de sa fonctionnalité en tant que portail captif (passerelle d'interception sur le WEB), ALCASAR offre d'autres fonctionnalités, utilisable dans des contextes spécifiques d'utilisation :

- Pare-feu dynamique et routeur filtrant
- Serveurs DHCP, DNS, et NTP
- Serveur d'authentification, d'autorisation et de compatibilité
- Serveur de base de données des utilisateurs
- Connecteurs avec des annuaires externes (LDAP)
- Administration en graphique via une interface web (ALCASAR ACC).

Avantages

- Open-source et gratuit
- Conforme à la RGPD, CNIL, et respecte les recommandations de l'ANSSI
- Maintenance et mise à jour régulière
- Compatible avec un annuaire LDAP
- Communauté/Documentation riche en information sur le site officiel www.alcasar.net et FusionForge sur www.adullact.net

Inconvénients

- Nécessite d'allouer une autre machine pour la mise en place (sauf en cas de machine virtuelle, mais complexité de l'architecture dans le cas présent)
- Nécessite des compétences en système pour la sécurisation du portail captif

3.5.3) Choix de solution de portail captif

Pour répondre aux besoins demandés par l'entreprise, nous avons fait le choix de partir sur la solution du portail captif de **pfSense avec AD RADIUS**.

En effet, le choix s'est porté par le fait que :

- L'outil est gratuit et open-source
- L'équipe de prestataire informatique a des connaissances dans la mise en place de la solution, nous permettant ainsi d'être plus efficace dans le déploiement de la solution.
- Avoir une seule machine dédiée pour pfSense nous permet d'amenuir les coûts d'achats de matériel ou de consommation pour le projet.

3.6) Synthèse des points forts et faibles des solutions retenues

SOLUTIONS	AVANTAGES	INCONVENIENTS
Annuaire authentification : **Active Directory**	- User-friendly GUI - Authentification unifiée - Gestion des services et utilisateurs simplifiés	- Nécessite beaucoup de ressources matérielles - Coûteux (Licence Windows)
Accès des données sur le réseau et redondance des données : **DFS** et **DFSR**	- Tolérances aux pannes - Performant - Sécurité Scalabilité	- Coûteux (Licence Windows) - Solution propriétaire
Solution de sauvegarde complète : **cible iSCSI -> SAN**	- Tolérances aux pannes Performant (vitesse de lecture accrue) - TrueNAS : gratuit	- Configuration méticuleuse - Nécessite beaucoup de ressources matérielles
Solution de clichés instantanés : **Shadow Copy**	- Flexibilité - Vitesse de restauration	- N'équivaut pas une vraie sauvegarde - Non tolérable aux pannes matérielles (sauf délocalisation des clichés) - Solution propriétaire Microsoft
OS routeur/pare-feu : **pfSense**	- Gratuit et open-source - Intègre des solutions VPN natifs - Peu gourmand en ressources - Intègre des plugins IDS/IPS - Intègre-le NAT/PAT	- Prise en main de l'interface difficile au début - Langue du clavier en ENG par défaut (difficile à prendre en main pour les adeptes du clavier FR) - Pas de mise à jour régulier en comparaison de ses concurrents
Solution VPN site à site : **IPSec**	- Natif sur une grande majorité d'équipement réseau - Optimale pour une communication site-a-site - Protocole sécurisé dès l'échange IP entre deux sites	- Système de chiffrement décrypté par la NSA - Requiert l'ouverture de certains ports : 50, 51 et 500, pouvant ainsi être analyser par des un scanner de ports.
Solution portail captif : **pfSense + AD Radius**	- Open-source et gratuit - Natif dans le routeur/pare-feu - Centralisation des authentifications par RADIUS - Diverses documentations disponibles sur Internet - Facilité d'installation	- Non conforme à la RGPD - Non conforme à la CNIL

4) BUDGET

DEVIS N°1

CDW SafeSecurity
2 Boulevard de l'Europe
67000 Strasbourg
09 52 36 87 00
cdw-info@safesecurity.fr

CCI Campus Alsace
204 Avenue de Colmar
67021 Strasbourg
03 88 43 08 00
campus@alsase.cci.fr

Objet : Coût en interne (Devis matériel uniquement)

Description	Quantité	Prix Unitaire HT	TVA	Total HT
TP-Link TL-SF1024 Switch 24 Ports 10/100 Mbps	10	75,20 €	20 %	752,00 €
Routeur/Pare-feu NetGate 7100 1U BASE Pfsense+	2	959,20 €	20 %	1 918,40 €
Serveur Smart Value PowerEdge T150	6	1 124,90 €	20 %	6 749,40 €
Lenovo M80t Celeron G7400 - Sans OS	60	224,50 €	20 %	13 470,00 €
Moniteur LED 21,5" Philips 223V5LSB2/10 - 1920 x 1080 - VGA	60	74,80 €	20 %	4 488,00 €
Clavier USB Lenovo 300	60	9,60 €	20 %	576,00 €
Souris Lenovo	60	7,68 €	20 %	460,80 €
Câble réseau RJ45-Cat6 10 m	200	3,50 €	20 %	700,00 €
Licence Windows Server 2019 (+10 CALs Users Pack)	4	1 344,00 €	20 %	5 376,00 €
Licence Windows 10 Pro Retail	60	119,99 €	20 %	7 199,40 €
Licence Windows CALs Pack 5 Users	12	104,79 €	20 %	1257,48 €

Montant Total HT	42 947,48 €
Total TVA	8 589,50 €
Montant Total TTC	**51 536,98 €**

DEVIS N°2

CDW SafeSecurity
2 Boulevard de l'Europe, 67000 Strasbourg
09 52 36 87 00
cdw-info@safesecurity.fr

CCI Campus Alsace
204 Avenue de Colmar, 67021 Strasbourg
03 88 43 08 00
campus@alsase.cci.fr

Objet : Coût en externe (devis matérielles et prestation informatique)

Description	Quantité (unité/jours)	Prix Unitaire HT	TVA	Total HT
TP-Link TL-SF1024 Switch 24 Ports 10/100 Mbps	10	75,20 €	20 %	752,00 €
Routeur/Pare-feu NetGate 7100 1U BASE Pfsense+	2	959,20 €	20 %	1 918,40 €
Serveur Smart Value PowerEdge T150	6	1 124,90 €	20 %	6 749,40 €
Lenovo M80t Celeron G7400 - Sans OS	60	224,50 €	20 %	13 470,00 €
Moniteur LED 21,5" Philips 223V5LSB2/10 - 1920 x 1080 - VGA	60	74,80 €	20 %	4 488,00 €
Clavier USB Lenovo 300	60	9,60 €	20 %	576,00 €
Souris Lenovo	60	7,68 €	20 %	460,80 €
Câble réseau RJ45-Cat6 10 m	200	3,50 €	20 %	700,00 €
Licence Windows Server 2019 (+10 CALs Users Pack)	4	1 344,00 €	20 %	5 376,00 €
Licence Windows 10 Pro Retail	60	119,99 €	20 %	7 199,40 €
Licence Windows CALs Pack 5 Users	12	104,79 €	20 %	1 257,48 €
Etude du marché et solutions technique	5	300,00 €	20 %	1 500,00 €
Installation et configuration des serveurs Windows en haute disponibilité	30	300,00 €	20 %	9 000,00 €
Installation et configuration des routeurs/pare-feu	30	500,00 €	20 %	15 000,00 €
Mise en place d'une solution de sauvegarde	20	300,00 €	20 %	6 000,00 €
Mise à disposition des équipements en salle de formation	10	300,00 €	20 %	3 000,00 €
Brassage des équipements reseaux	5	300,00 €	20 %	1 500,00 €

Montant Total HT	78 947,48 €
Total TVA	15 789,50 €
Montant Total TTC	**94 736,98 €**

5) PLANNING

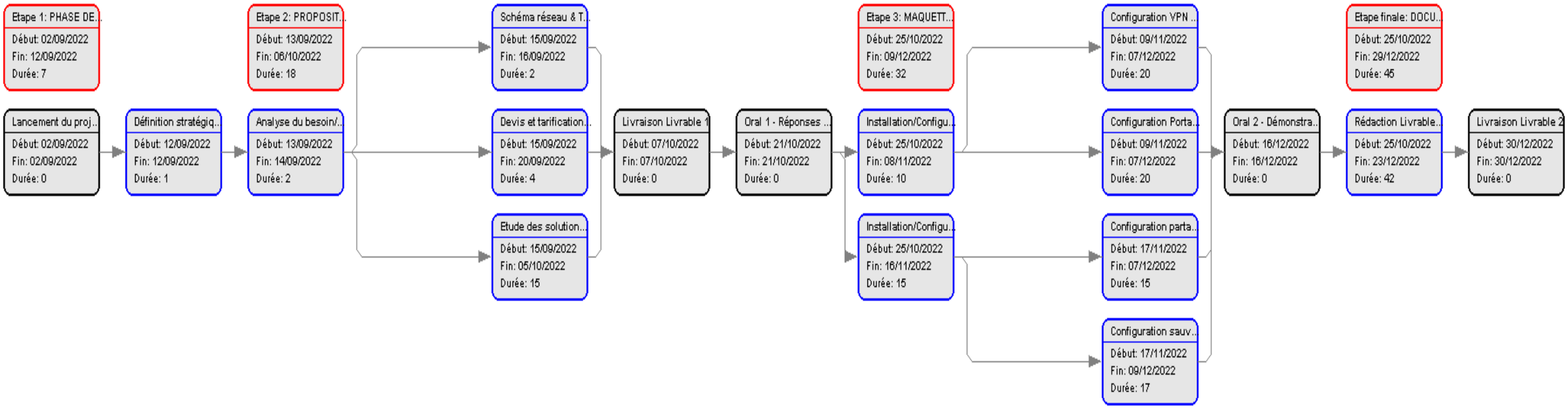
5.1) Planning prévisionnel (Diagramme de Gantt)

Nom	Date ...	Date de fin
Etape 1: PHASE DE PREPARATION	02/09/2022	12/09/2022
Lancement du projet	02/09/2022	02/09/2022
Définition stratégique	12/09/2022	12/09/2022
Etape 2: PROPOSITION COMMERCIALE	13/09/2022	06/10/2022
Analyse du besoin/objectifs	13/09/2022	14/09/2022
Devis et tarification service	15/09/2022	20/09/2022
Schéma réseau & Tableau d'adressage	15/09/2022	16/09/2022
Etude des solutions tech...	15/09/2022	05/10/2022
Livraison Livrable 1	07/10/2022	07/10/2022
Oral 1 - Réponses au CdC	21/10/2022	21/10/2022
Etape 3: MAQUETTE/EXPERIMENTATION	25/10/2022	09/12/2022
Installation/Configurati...	25/10/2022	08/11/2022
Configuration VPN sécurisé	09/11/2022	07/12/2022
Configuration Portail Captif	09/11/2022	07/12/2022
Installation/Configurati...	25/10/2022	16/11/2022
Configuration partage de...	17/11/2022	07/12/2022
Configuration sauvegarde...	17/11/2022	09/12/2022
Oral 2 - Démonstration technique	16/12/2022	16/12/2022
Etape finale: DOCUMENTAT...	25/10/2022	29/12/2022
Rédaction Livrable 2	25/10/2022	23/12/2022
Livraison Livrable 2	30/12/2022	30/12/2022

5.2) Liste des taches prévisionnelles

Nom	Date de début	Date de fin
Etape 1: PHASE DE PREPARATION	02/09/2022	12/09/2022
Date du commencement du projet		
Lancement du projet	02/09/2022	02/09/2022
- Prise en connaissance du sujet *- Remise du cahier des charges par les clients*		
Définition stratégique	12/09/2022	12/09/2022
- Répartition des tâches à effectuer (officielles) *- Le groupe s'est convenu de traiter tous les lots individuellement afin de ne pas être pénaliser lors des épreuves E5* *- Rappel sur les propositions des encadreurs et les bonnes pratiques à avoir au cours du projet*		
Etape 2: PROPOSITION COMMERCIALE	13/09/2022	06/10/2022
Phase de propositon commerciale: *- Etude du marché matériel* *- Calcul main d'oeuvre* *- Etude des solutions techniques et logicielles* *- Mise en conformité du schéma réseau et du tableau d'adressage* *- Planification du projet et liste des taches prévisionnelles*		
Analyse du besoin/objectifs	13/09/2022	14/09/2022
Devis et tarification service	15/09/2022	20/09/2022
Schéma réseau & Tableau d'adressage	15/09/2022	16/09/2022
Etude des solutions techniques et logicielles	15/09/2022	05/10/2022
Livraison Livrable 1	07/10/2022	07/10/2022
Oral 1 - Réponses au CdC	21/10/2022	21/10/2022
Oral de présentation des réponses au cahier des charges: */!\ RESPECTER LE DELAI /!* *- Présenter suscintement le groupe avec leur rôle respectifs* *- Argumenter les choix techniques et logicielles choisies pour la réalisation du projet* *- Expliquer le schéma réseau et le tableau d'adressage (le lien entre les sites, le choix des adresses hôtes, routeurs, etc ..)* *- Expliquer le devis établi sur les matériels et la main d'oeuvre de mise en place* *- Présenter les dates clés du planning et la répartition des tâches*		
Etape 3: MAQUETTE/EXPERIMENTATION	25/10/2022	09/12/2022
Expérimentation et maquette sur les solutions pour le projet: *- Lancement des machines virtuelles* *- Expérimentation sur les besoins demandés dans le CdC* *- Bilan des difficultés rencontrés / délai respecté ou non*		
Installation/Configuration Routeur/pare-feu	25/10/2022	08/11/2022
Configuration VPN sécurisé	09/11/2022	07/12/2022
Configuration Portail Captif	09/11/2022	07/12/2022
Installation/Configuration serveur et redondance	25/10/2022	16/11/2022
Configuration partage de fichiers et redondance	17/11/2022	07/12/2022
Configuration sauvegarde et clichés instantanés vers TrueNAS	17/11/2022	09/12/2022
Oral 2 - Démonstration technique	16/12/2022	16/12/2022
Oral de démonstration technique: */!\ Chaque membre démarrera en amont ses machines virtuelles avec ses snapshots:* *- Snapshot Clean: aucun service installé* *- Snapshot sur chaque manipulation:* *- Snapshot sur le tout installé (image à privilégier au début de la démonstration technique afin de démontrer les succès des opérations)* */!\ RESPECTER LE DELAI /!* *Ordre de passage à l'oral de démonstration:* *Dylan -> Corentin -> Winness*		
Etape finale: DOCUMENTATION TECHNIQUE	25/10/2022	29/12/2022
/!\ CRITIQUE: DELAI A RESPECTER IMPERATIVEMENT /! *Les captures étant déjà pris lors de la maquette et expérimentation, la rédaction ne devrait pas poser problème.* *Il est recommandé de rédiger à la fois expérimenter à chaque avancé pour un gain de temps considérable.* *Ne pas oublier de rédiger les difficultés rencontrés et les solutions apportés pour pallier aux problèmes.*		
Rédaction Livrable 2	25/10/2022	23/12/2022
Livraison Livrable 2	30/12/2022	30/12/2022

5.3) PERT prévisionnel (visualisation temporelle globale des tâches)



Date de début du projet : 02 septembre 2022

Date de fin de projet : 31 décembre 2022

Date clés du projet : 09 octobre 2022 (Rendu livrable 1) / 21 octobre 2022 (Réponses au Cahier des Charges) / 16 décembre 2022 (Démonstration technique) / 31 décembre 2022 (Rendu Livrable 2)