01/03/2022

PROJET CUBE 3

SNTS

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

LAPOUJADE Sylvain ERYANI Farida
FLOTTARD Nicolas PUJOL Edouard

Table des matières

Introduction

La communauté de commune de Castillon Pujol a été créée en 2013 et regroupe les communes de Gardegan et Toutirac, Saint Michel de Montaigne, Saint Magne de Castillon, Mouliets et Villemartin, Montcaret, Vélines, Sainte Terre, Pessac sur Dordogne, Pujols, Juliac, Gensac et Castillon-la-bataille, douze communes de Gironde à l'Est de Libourne.

La Communauté de commune a mutualisé un certain nombre de services (espaces verts, voirie, éclairage public et éducation). Il en est de même pour les écoles de la communauté de commune.

Les écoles ont été regroupés en 7 sites. Certains sites regroupant plusieurs localités au sein d'une même école.

Castillon-la-bataille, Mouliets et Villemartin, Saint Magne de Castillon : école Jules Ferry (20 classes)

Pessac sur Dordogne, Juliac, Gensac : école Simone Veil (17 classes)

Pujols : école Robert Badinter (13 classes)

Vélines Montcaret : école Robert Debré (15 classes)

Gardegan et Tourtirac : école Louis Pasteur (15 classes)

Sainte Terre : école Emile Zola (16 classes)

Saint Michel de Montaigne : école Louise Michel (15 classes)

L'installation d'un service centralisé dédié au numérique scolaire pour les douze communes a été faite. Quatre Agents ont été recrutés, ils ont en charge la reprise en main du fonctionnement global des outils numériques des écoles de la communauté de Commune.

Le SNTS (Service Numérique et Technologique Scolaire)

Installé dans les locaux communaux disponibles, équipés et précâblés (électricité, téléphonie et câblage informatique cat6), situé au 30 avenue de l'Europe (anciennement Avenue Camille Maumey) à Castillon-la-bataille, sur une surface de 330m².

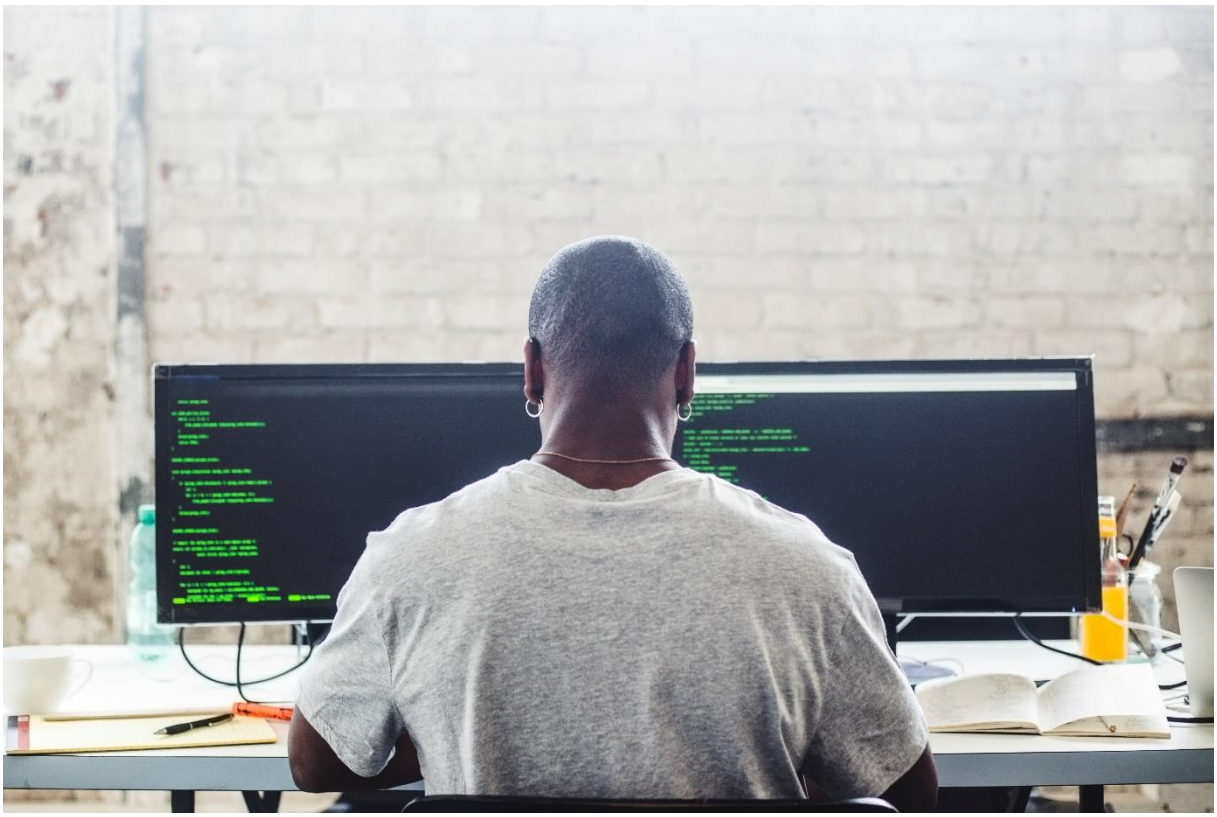
Le SNTS est composé de 4 employés, un chef de service, Sylvain LAPOUJADE, supervisera le travail l'équipe composé de trois technicien et technicienne informatique, Farida ERYNAI, Nicolas FLOTTARD et Edouard PUJOL.

Ce service poursuit la restructuration de l'informatique des écoles entamé fin 2022.

En effet, en premier lieu l'ensemble des postes utilisateurs (ordinateurs portables, postes fixes en libre-service et postes administratifs) ont été renouvelés.

Dans un second temps, les différents serveurs des écoles ont été renouvelés puis paramétrés.

Le SNTS a donc maintenant pour tâche de déployer et d'administrer le nouveau parc informatique, dans l'optique de l'uniformiser et de le sécuriser.



Masterisation

Contextualisation

Au vu du nombre d'équipement, nous avons besoin de paramétrer plusieurs centaines de pc. Nous ne pouvons pas nous permettre de passer une demi-journée par ordinateur pour installer l'image ainsi que les logiciels. Nous devons donc formaliser et automatiser la tâche.

Besoin

Nous avons besoin d'une méthode uniforme, rapide et efficace pour déployer la bonne configuration. Ce projet nous demande de créer plusieurs images différentes : Une image classique de Windows pour les utilisateurs, et une image personnalisée.

Solutions possibles

Nous avons plusieurs solutions possibles sur le marché : premièrement nous pouvons le faire manuellement, on peut également le faire sous-traiter par une entreprise tierce et pour finir il existe plusieurs logiciels tels que Microsoft Deployment Toolkit, Smart Deploy …

Choix

Voici une pondération des solutions cités plus haut :

	Manuellement	Sous-traiter	MDT (Microsoft Deployment Toolkit)	Smart Deploy
Tarif (1-5)	2	3	1 (inclus dans la license windows)	4
Temps passé (en jours)	150	20	3	3
Nombre de technicien requis	10	0	1	1
Facile d'utilisation (/5)	5	1	4	4

Matrice de choix Masterisation

Pour donner suite à notre tableau de comparaisons ci-dessus, nous avons retenu la solution : MDT : MICROSOFT DEPLOYMENT TOOLKIT

L'outil Microsoft Deployment Toolkit est un ensemble d'outils, de processus et de conseils pour l'automatisation du déploiement de bureau et de serveur. Nous pouvons l'utiliser pour créer des images de référence ou alors comme solution de déploiement. MDT est l'un des outils les plus importants aujourd'hui dans le monde des professionnels de l'informatique.

Microsoft Deployment Toolkit permet de réduire le temps de déploiement et de normaliser les images de bureau et de serveur, mais permet également de gérer plus facilement la sécurité et les configurations en cours. MDT s'appuie sur les principaux outils de déploiement du kit de déploiement WINDOWS ADK.

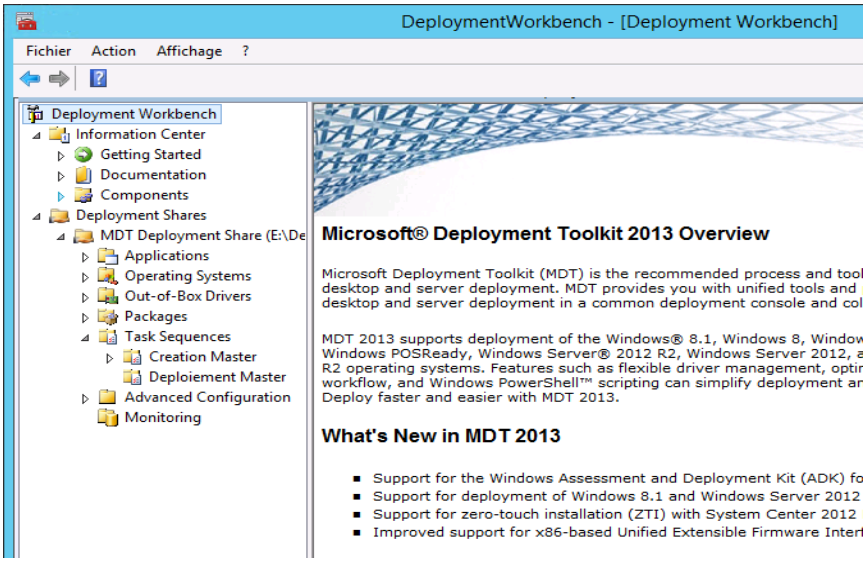
Microsoft Deployment Toolkit prend en charge le déploiement de Windows 10, ainsi que Windows 7, Windows 8 et Windows Server.

Configuration et déploiement

Faut-il réserver un serveur uniquement pour l'utilisation de MDT ?

La réponse est non. Nous pouvons utiliser un poste Microsoft Deployment Toolkit basé sur un système Windows 10 en version 32 bits ou 64 bits. En effet, ceux qu'on pourrait appeler "poste d'administration MDT" peuvent être un système Windows, poste de travail ou bien un serveur sur lequel est installé l'outils MDT "Microsoft Deployment Toolkit" ainsi que l'outil ADK "Windows Automated Installation Kit".

L'outil MDT possède une console qui s'appelle "Deployment WorkBench" qu'on peut traduire en français "Atelier de déploiement", voici une capture d'écran pour vous montrer à quoi cela ressemble.



Deployment Workbench

Partage de déploiement :

Nous appelons un partage de déploiement, un fichier partagé sur le serveur et qui contient tous les fichiers du programme d'installation ainsi que les scripts nécessaires au déploiement. Il conserve également les fichiers de configuration (appelés règles) qui sont rassemblés lorsqu'on déploie un ordinateur. De plus, dans ce fichier nous pouvons retrouver d'autres scripts externes que nous avions créés.

Règles :

Nous utilisons des règles qui sont le cœur de MDT. Elles contrôlent l'assistant de déploiement Windows sur le client. Elles peuvent fournir par exemple le nom de l'ordinateur, domaine à joindre dans le pc, paramètre régionaux…

Image de démarrage :

Les images de démarrage sont les fichiers de pré installation de Windows qui sont utilisés pour lancer le déploiement. Les images peuvent être démarrées à partir d'un DVD, d'un CD, d'un fichier iso ou bien d'une clé USB, mais également sur le réseau à l'aide d'un serveur PXE.

Les images de démarrage se connectent au fichier partage de déploiement expliqué plus haut, et démarrent le déploiement.

Systèmes d'exploitation :

Nous pouvons déployer une image Windows, ou bien une image que nous avons personnalisé et créée.

Applications :

Deployment Workbench, la console du service de déploiement, permet également d'ajouter les applications que l'on souhaite ajouter à notre déploiement. Cependant nous devions trouver le fichier .exe de l'application qu'on souhaite ajouter à notre image de déploiement.

Référentiel de pilotes :

En ce qui concerne les pilotes, Deployment Workbench prend en charge ces derniers seulement s'ils sont référencés dans le référentiel de pilotes qui réside sur le serveur.

Packages :

Deployment Workbench permet également d'ajouter tous les packages Microsoft que l'on souhaite utiliser. Les packages les plus ajoutés sont des modules linguistiques. Nous pouvons aussi proposer des mises à jour de sécurité et d'autres mises à jour de cette façon, cependant WSUS est mieux recommandé pour effectuer ce type d'action. Toutefois, il existe des exceptions telles que les mises à jour de correctifs logiciels critiques qui ne sont pas disponibles via les services WSUS.

Séquences de Tâches :

Une séquence de tâche dans MDT contient l'ensemble des actions qui vont être effectuées sur le poste durant le déploiement. Les séquences de tâches sont essentielles à la solution de déploiement. Lorsque vous créez une séquence de tâches, vous devez sélectionner un modèle. Les modèles se trouvent dans le dossier Modèles du répertoire d'installation MDT et déterminent les actions par défaut présentes dans la séquence.

Actions :

On nous donne six semaines pour réaliser leur demande. Du côté MDT, cela rentre dans les temps. Nous avons choisi MDT car premièrement le cahier des charges nous le demande, mais deuxièmement c'est l'outil le plus complet, le plus simple et sans oublier le plus rapide pour déployer plusieurs pcs, donc nous gagnerons en temps, et donc en argent.

Microsoft Deployment Toolkit est gratuit et disponible pour tout le monde.

Budget

La solution Microsoft Deployment Toolkit est un des services en libre accès sur les serveurs. Il n'y aura donc aucun frais supplémentaire pour obtenir MDT si nous avons déjà acheté le serveur auparavant.

Synthèse partie

Pour conclure, nous avions donc besoin d'une technique pour automatiser la tâche et déployer rapidement, efficacement et facilement.

La solution Microsoft Deployment Toolkit a été retenue pour ces caractéristiques.

MDT est un logiciel disponible gratuitement sur Microsoft Server, pour cette solution nous avons besoin d'un seul technicien requis pour un minimum de temps passé.

Une fois les postes informatiques des écoles de la communauté de communes paramétrés, avec les déploiements d'image spécifique au type d'utilisation du poste (direction, postes fond de classe, postes CDI, Ordinateurs enseignant).

Nous devons réfléchir un système efficace et automatisé pour maintenir ces postes à jour.

Création des mises à jour

Présentation du service WSUS

Windows Server Update Services (WSUS) est un service permettant de distribuer les mises à jour pour Windows et d'autres applications Microsoft sur les différents ordinateurs fonctionnant sous Windows au sein d'un parc informatique.

Contexte

La communauté de communes du Castillonnais regroupe 7 écoles au sein d'une seule et même entité juridique, celle-ci a pour but de simplifier la gestion de chaque école, dans notre cas les écoles sont reliés entre elle via une fibre optique, ceci peut faciliter le déploiement de mise à jour au sein du même réseau.

Besoin

Comme dit précédemment les 7 écoles possèdent un parc conséquent sur 7 sites différent de poste fixe est portable allant de Windows 7 à Windows 10, l'objectif est de déployer des packs d'update de sécurité de Microsoft sur l'ensemble des écoles sans avoir à trop utiliser la bande passante.

Les Choix Disponible

Il existe plusieurs solutions, disponible comparable à WSUS, malgré l'ensemble des features proposé par ces logiciels le prix par feature reste un argument important,

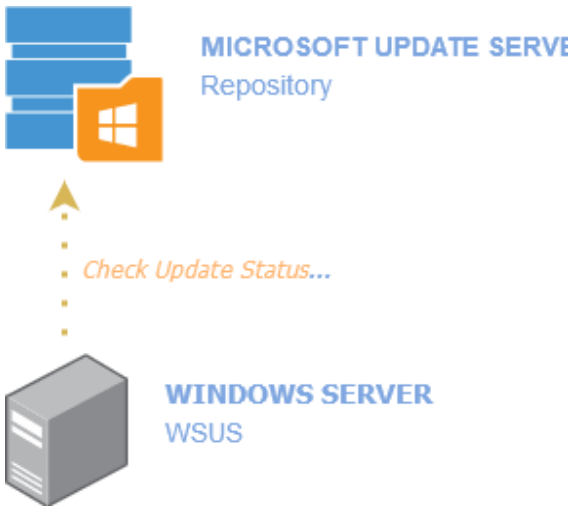
WSUS lui embarque l'ensemble des fonctionnalités compatible avec un large éventail de version de Windows y compris les versions Serveur tout cela compris dans la licence Windows Server 2019.

Nom	Essai gratuit	Feature	Prix
SolarWinds Patch Manager	30 jour	l'outil peut mettre à jour les logiciels sur Mac OS, Unix, Linux et Windows, mais le logiciel ne fonctionne que sur Windows Server.	1.909 € à l'année
ManageEngine Patch Connect Plus	30 jour	Gestion des correctifs avec déploiement automatisé, système de test des mises à jour et rapports d'audit de l'état des versions pour les logiciels résidant sur Windows, Mac OS, Linux et le Cloud.	5,495 € à l'année
Ivanti Patch Link	Non	Un ensemble d'outils techniques pour les MSP qui comprend un gestionnaire de correctifs automatisé. Il s'agit d'un système basé sur le cloud.	6,495 € à l'année
WSUS	Non	Capable de gérer les mises à jour des logiciels Microsoft et des logiciels tiers. Il s'installe sur Windows Server.	Compris dans la licence Windows Serveur

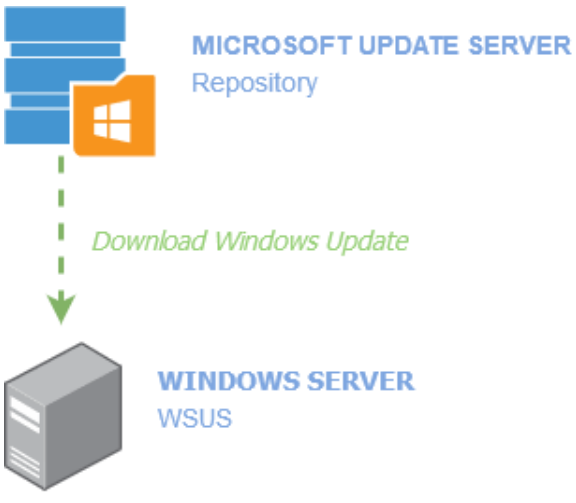
Solutions déploiement de mises à jour

Fonctionnement du serveur de mise à jour Windows :

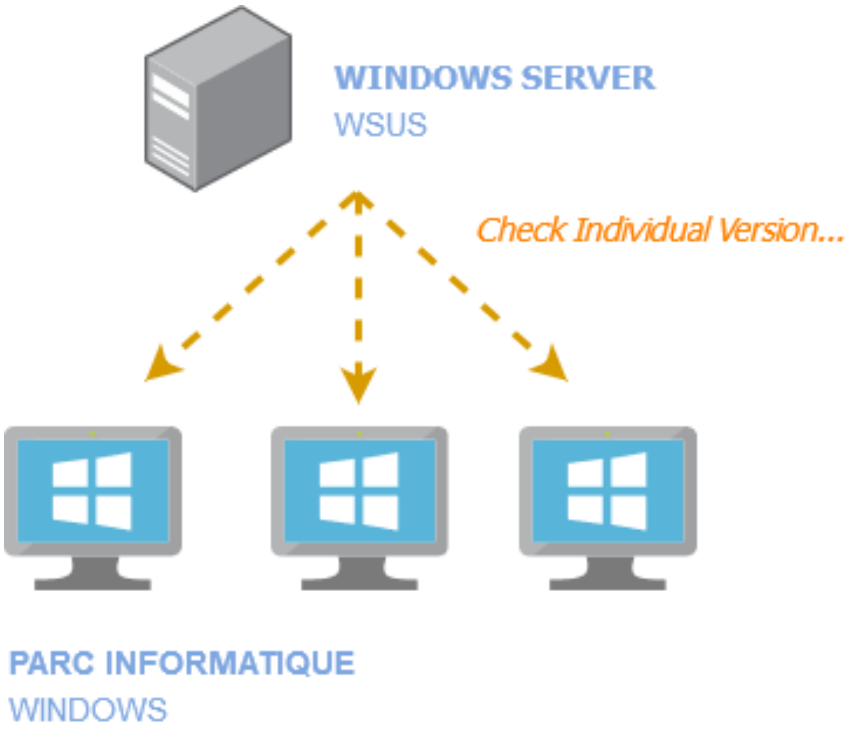
Le serveur WSUS demande les mises à jour au serveur Microsoft Update.



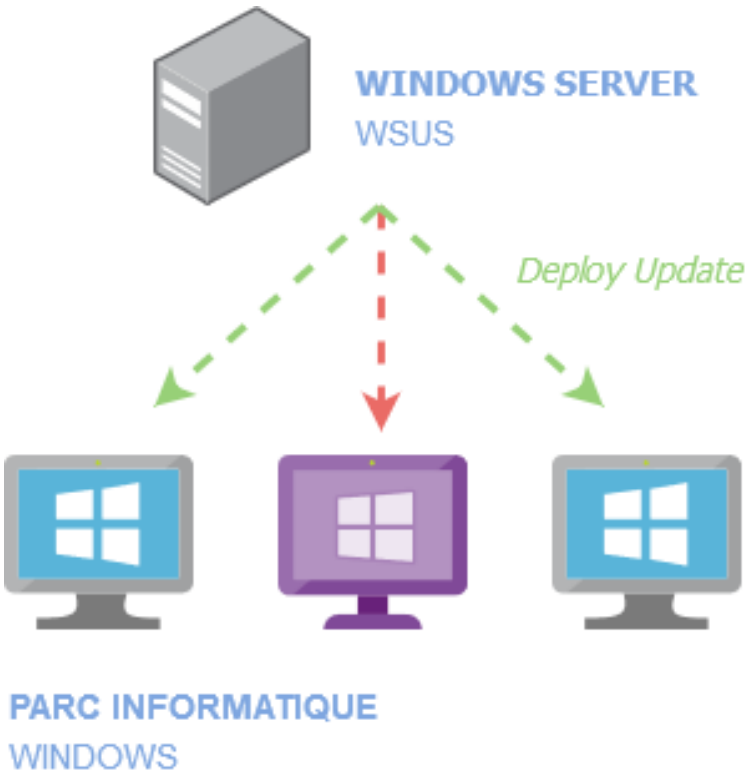
Le Serveur Microsoft envoie les mises à jour demandée



Le serveur Microsoft envoie les mises à jour demandées



Le serveur WSUS envoie les updates aux machines clients qui sont dans son réseau local.



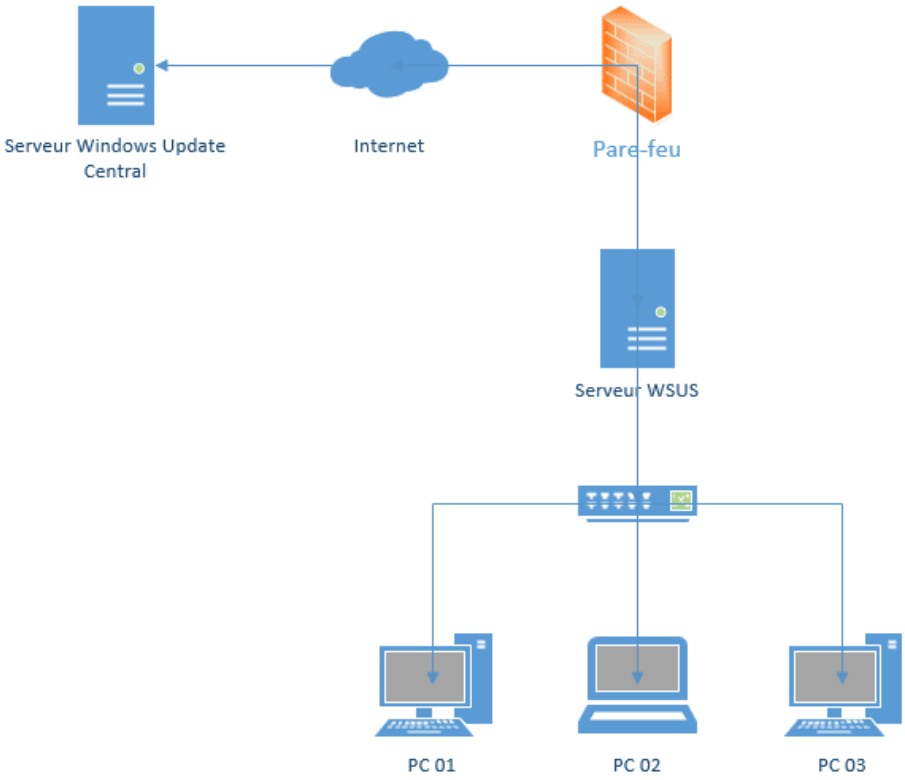


Schéma généralisé

Conclusion

Avec WSUS Il est possible d'effectuer une mise à jour de manière automatique, de plus, ce fonctionnement permet la mise en place de groupe de tests par école, après la validation du correctif, l'approbation peut être effectuée pour un groupe donné.

Grâce à ce système, nous maîtrisons le déploiement des mises à jour de sécurité de Windows sur l'ensemble du parc informatique de la communauté des communes sans un surcoût en bande passante ou utilisation de logiciel tiers.

Sécurisation du Parc

Contextualisation

Le parc informatique géré par le SNTS ne dispose pas à l'heure actuelle d'une sécurisation suffisante et efficace.

N'ayant aucune protection vers l'extérieur, nous sommes donc éligibles aux cyberattaques, sans trop de difficultés pour les hackers.

Ceci est un problème critique dans les temps actuels, les cyberattaques venant des pays de l'ouest de l'Europe, visant les infrastructures d'un grand nombre de pays, sont en recrudescence.

Il est obligatoire de se doter d'un système de protection complexe et efficace.

La communication informatique entre les différents utilisateurs est compliquée, l'architecture actuelle ne permet pas des échanges simples et sécurisés.

La direction et les enseignants n'ont pas d'outils à disposition pour utiliser le réseau de l'établissement depuis l'extérieur, ce qui ne facilite donc pas le télétravail.

Les serveurs ne sont pas isolés, que ce soit physiquement ou virtuellement.

Besoins

Nous devons assurer les échanges entre tous les utilisateurs, en assurant une protection des données internes et contre les attaques extérieures.

Tout d'abord en essayant de plus possible de bloquer les attaques à l'entrée de notre réseau.

Cependant aucun système n'est infaillible, nous devons aussi nous doter d'un système de protection nous permettant de segmenter notre réseau afin de pouvoir isoler les parties infectées.

Nous devons avoir des protections matériels, paramétrable et administrable depuis un accès distant.

Ainsi que de prévoir plusieurs couches de niveaux de sécurités.

Mais aussi en équipant les postes d'antivirus

Solutions

Ayant besoin d'une sécurisation optimale, nous allons utiliser plusieurs couches de protections, nous allons détailler dans ce paragraphe ces différentes couches.

PARE-FEU

a. Qu'est-ce qu'un pare-feu ?

Le pare-feu est un système de sécurité qui protège votre ordinateur. Il fonctionne comme une cloison ou un mur qui protège les ordinateurs du réseau Internet. C'est une passerelle contrôlant l'arrivée des données sur le réseau.

C'est un élément de sécurité de premier plan au sein d'un réseau informatique.

b. Pourquoi utiliser un Pare-feu ?

Les cyberattaques sont de plus en plus fréquentes et récurrentes

Son but est de filtrer le trafic réseau et d'empêcher les personnes extérieures d'accéder aux données personnelles sur l'ordinateur. Les pares-feux bloquent non seulement le trafic indésirable, mais ils peuvent également aider à empêcher les logiciels malveillants d'infecter votre ordinateur, tels que les applications non-sécurisées ou les virus.

Son rôle concret est de protéger le réseau en empêchant les pirates et utilisateurs non autorisés d'accéder aux données. En d'autres termes, les équipements non équipés d'un pare-feu sont vulnérables.

Un pare-feu peut aussi avoir d'autres fonctions, comme définir manuellement quels types de contenus bloquer, surveiller et limiter la bande passante, et configurer manuellement des accès VPN, synchroniser et filtrer le flux de tout activité et des donnés par liaison High Aviability (haute disponibilité), isoler tous les serveurs des attaques extérieures et intérieures par DMZ puis nous pouvons activer IPS pour éliminer tous des attaques à intérieurs.

c. quels sont les types de pare-feu ?

Il existe deux types de pare-feu (**annexe 1**) : le matériel et le logiciel (pare-feu virtuel)

1. Les pare-feu matériels sont des périphériques installés physiquement sur le réseau.

2. Un pare-feu logiciel est une solution de protection du réseau installé sur un ordinateur ou un serveur.

Il y a 4 catégories de filtrage :

1. 1re génération Inspection dynamique : pare-feu à filtrage de paquets

2. 2e génération : pare-feu d'application, exemple filtrage de type proxy :

3. 3e génération : pare-feu multicouche avec états (Statefull)

4. 4e génération : NGPF = Nouvelle génération Pare-feu (voir sur **annexe 2**).

Les pares-feux de nouvelle génération offrent une technique de sécurité avancée.

Ce type offre de nombreuses fonctionnalités supplémentaires qui renforcent le niveau de sécurité des équipements informatiques.

e. Comment fonctionnent les pares-feux ?

Les pares-feux analysent le trafic réseau en fonction des règles de sécurité des utilisateurs. Le pare-feu n'accepte que les connexions entrantes dont l'acceptation a été confirmée.

Cela se fait en autorisant ou en bloquant certains paquets de données entrantes en fonction des règles de sécurité préalablement définies par l'utilisateur.

Le fonctionnement d'un pare-feu se fait en 2 points.

1. Analyse des activités

Lorsqu'un pare-feu est installé sur un équipement informatique, l'activité faite par l'utilisateur est analysée et filtrée, en cas d'activité « douteuse » le pare-feu prendra la décision de bloquer certains sites web ou pages internet en comparant l'activité de l'utilisateur à sa base de données des menaces.

2. Récupération d'informations Internet.

Le pare-feu utilise sa base de données afin de protéger l'utilisateur et son système informatique.

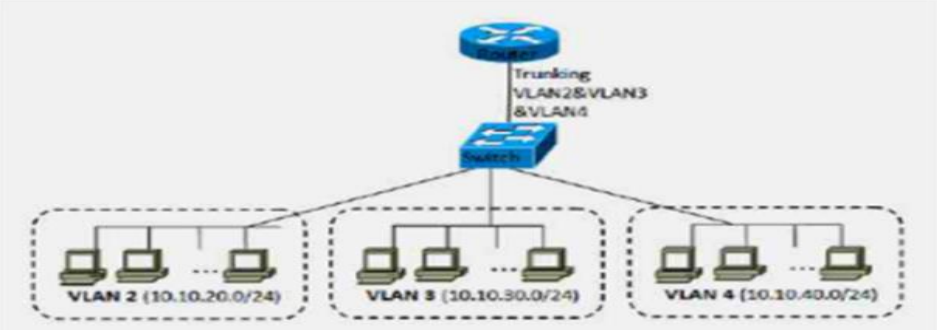
IPS

Qu'est-ce que l'IPS ?

IPS (I*ntrusion Prevention System* où Système de Prévention d'Intrusion). Peut être inclus dans un pare-feu. Son rôle est d'analyser tous les paquets et de bloquer directement les indésirables. Il va au-delà en bloquant ou en prévenant les risques de sécurité. Un IPS peut à la fois surveiller les événements malveillants et prendre des mesures pour empêcher qu'une attaque ne se produise.

VLAN

2. Qu'est-ce qu'un VLAN ?



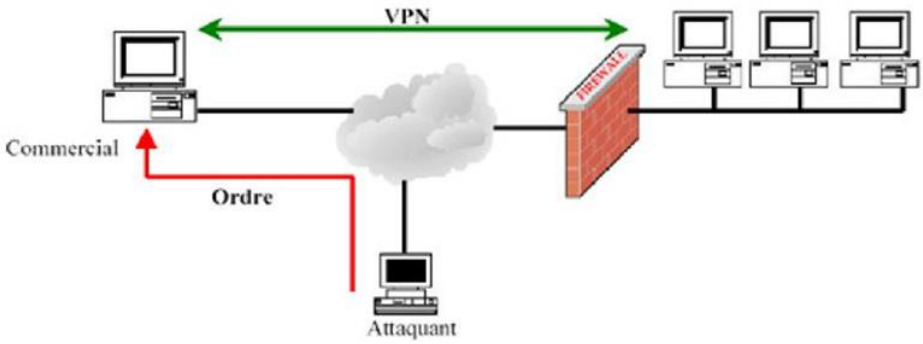
Schématisation VLANs

Un VLAN est un réseau informatique virtuel (Virtual Local Area Network).

Plusieurs VLAN peuvent se trouver sur le même réseau LAN.

Pour simplifier, des VLAN servent à « diviser » de manière virtuelle un réseau LAN.

VPN

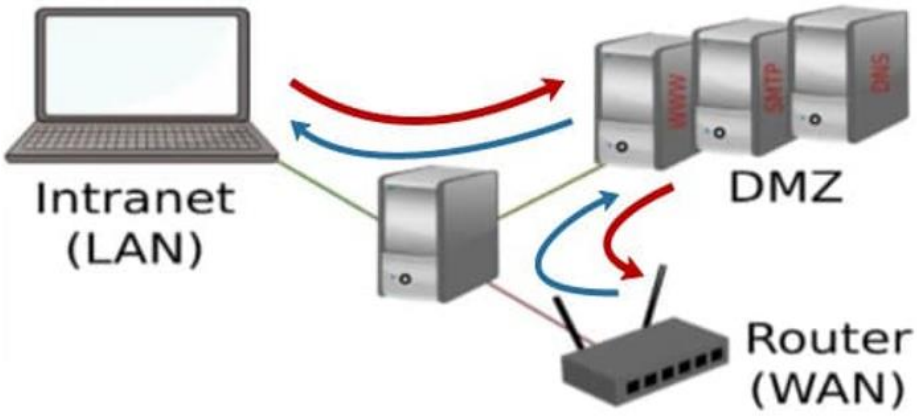


Fonctionnement VPN

Qu'est-ce que le VPN ?

Le VPN (Réseau Privé Virtuel) est une technologie permettant d'accéder aux ressources d'un réseau distant, à partir d'un autre réseau. Cela permet de se connecter à un réseau sécurisé si on ne se trouve pas sur le site de l'entreprise ou de l'administration dans laquelle on travaille.

DMZ



Schématisation DMZ

Un DMZ (Zone Démilitarisée) est un sous-réseau séparé du réseau local et isolé d'internet via le pare-feu. Le but est de sécuriser tous les serveurs dans ce sous-réseau.

Le DMZ sert donc à protéger les données et à empêcher les intrusions indésirables. Cela ajoute une sécurité en plus du pare-feu.

HA

HA (High Availability), permet de garantir la disponibilité de tous les outils sur le réseau. Il y a différente façon de le faire HA.

WITNESS

Witness est une application qui permet d'attribuer des rôles aux différents serveurs (Maître/Esclave).

L'application est témoin des échanges clients/serveurs et distribue les requêtes envoyées par les utilisateurs au bon serveur.

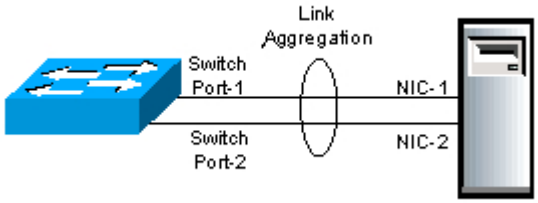
Disponible en version gratuite, Witness est le moyen le plus efficace et le meilleur logiciel en gestion de flux production.

LACP

LACP est le "Link Aggregation Control Protocol".

L'agrégation de liens est une technique utilisée dans les réseaux informatiques, permettant le regroupement de plusieurs ports réseau et de les utiliser comme s'il s'agissait d'un seul. En cas de panne physique d'un câble, le câble de secours prendra le relais pour assurer le service

(redondance). Cela nécessite un câble Ethernet RJ45 cat 6 ainsi que de la mémoire vive environ d'un Go. On configurera les switchs Cisco via la console de commande.



Schématisation LACP

Antivirus

En ce moment nous utilisons ESET 32 Nod. Nous proposons de migrer vers Bitdefender pour plus de performance et un meilleur prix. Voir tableau comparatif en Annexe 4.

Choix

Nous choisissons un pare-feu de nouvelle génération car ils offrent une technique de sécurité avancée.

Les pares-feux de nouvelle génération fournissent la prévention la plus avancée avec un système administration intégrée :

Ils sont conçus pour empêcher toute cyberattaque.

Leur utilisation est simplifiée grâce à une interface lisible.

Prix achat très minime avec des fonctionnalités très complètes (VLAN, VPN, IPS, IDS, DMZ, HA inclue)

Une fois ce choix de pare-feu nouvelle génération acté, nous allons l'utiliser pour mettre en place l'IPS, car cela rajoute une couche de protection à l'intérieur pare-feu.

L'IPS sert à protéger le réseau local.

Notre réseau local étant ainsi protégé, nous allons introduire des sécurités supplémentaires via l'utilisation de VLANs.

Les VLANs permettent une meilleure attribution des adresses IP.

Par exemple, notre école compte 125 encadrants et 2266 élèves.

Concrètement, au sein de notre réseau, cela fait 78 équipements IP répartis sur 7 écoles, soit 546 adresses IP.

Le but des VLANs ici est de conserver un adressage IP en classe C en créant un VLAN par école.

Si tous les équipements du réseau ne se trouvent pas sur le même réseau virtuel, la sécurité se trouve renforcée en cas de cyberattaque. Du fait du cloisonnement des réseaux, la navigation entre les différents VLANs n'est pas aisée.

Ils permettent une meilleure gestion des domaines de diffusion.

On peut regrouper plus facilement les utilisateurs par groupe, par fonction ou par service. Afin de mieux segmenter notre réseau et d'avoir une meilleure flexibilité en fonction des situations.

L'administration d'un VLAN se fait via l'architecture réseau. Donc, un utilisateur nomade à juste à se connecter au réseau sur lequel il se trouve pour être attribué au bon VLAN.

Notre choix se porte maintenant sur la façon dont laquelle les utilisateurs vont pouvoir se connecter à distance pour accéder au réseau gérer notre équipe.

Notre choix se porte sur un VPN, car c'est le moyen le plus simple de se connecter aux ressources d'un réseau distant.

La connexion se fait directement entre le serveur et le client (ordinateur). L'utilisation d'un VPN est donc sécurisée.

De plus, le réseau privé virtuel sert à crypter votre connexion internet. De cette façon, vos données et activités sur Internet ne peuvent pas être espionnées par d'autres personnes ou systèmes.

Certains FAI limitent la consommation internet de ses utilisateurs. Un serveur VPN peut contourner cette limitation.

Les pare-feu nouvelle génération permettent de compléter la sécurisation de notre réseau via l'implantation d'une DMZ ce qui nous conforte dans le choix de ce pare-feu, ainsi que de paramétrer la fonction HA, nécessaire dans notre projet de maintien de l'activité via l'utilisation d'un Witness et de liaisons LACP.

CHOIX	**Pare-Feu**	**IPS**	**VLAN**	**VPN**	**DMZ**	**HA**	**WITNESS**	**LACP**
Centralisation	*5*	0	3	2	*5*	3	0	0
Sécurisation	*5*	*5*	*5*	*5*	*5*	*5*	*5*	*5*
Rapidité	*5*	*5*	4	3	*5*	*5*	4	*5*
Synchronicité	*5*	*5*	0	2	0	*5*	*5*	*5*
Partage	*5*	0	*5*	1	*5*	4	0	0
Accessibilité	*5*	*5*	4	*5*	0	*5*	0	4
Flux continu	*5*	0	3	4	0	*5*	*5*	*5*
Total	35	20	24	22	20	32	19	24

Matrice de choix Options de sécurisation (notation /5)

Ordre de priorité : Pare-feu → HA → VLAN et LACP → VPN → IPS et DMZ → Witness

On choisit comme pare-feu, le Fortigate 100E (sur annexe 2-3), en effet son interface est simple et intuitive. Il protège une grande partie des cyberattaques via un fonctionnement complexe et complet. (Réseau, des données, infrastructure, des endpoints, des applications…).

Configuration & Installation

Pare-Feu ~ FORTIGATE 100E :

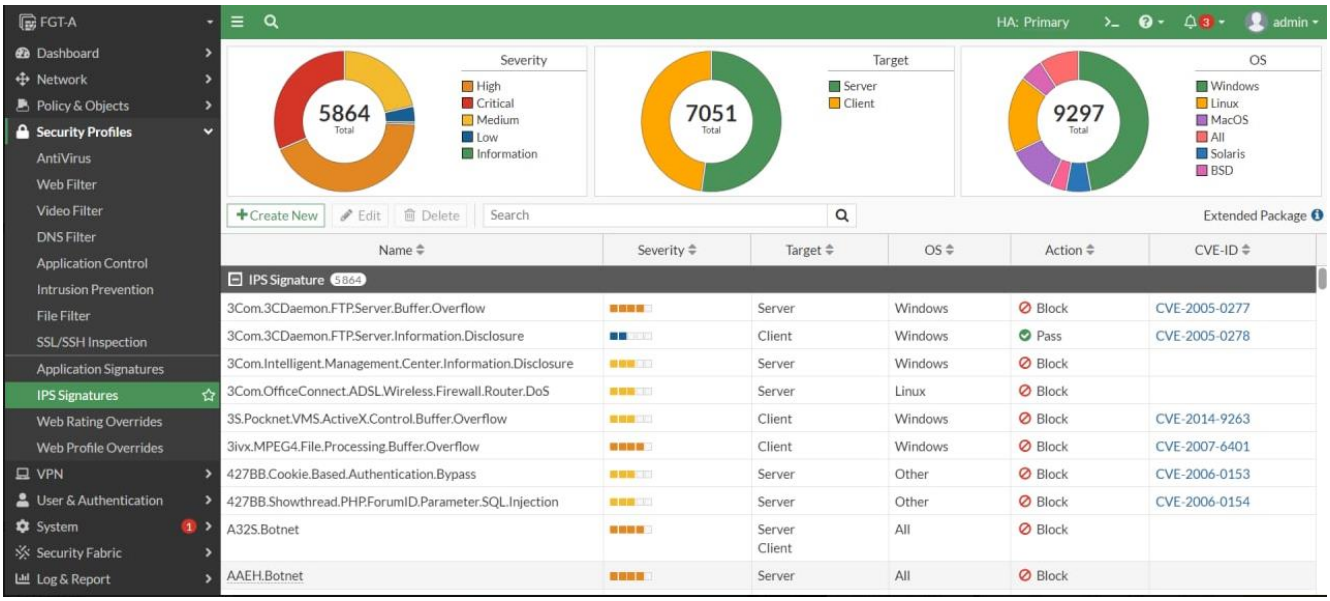
Nous déploierons deux pares-feux en redondance. En cas de panne, le relais se fera avec le second. Cette redondance se fera via un cluster HA

Les pares-feux auront la même configuration avec l'activation de l'IPS et la configuration de plusieurs VLANs. L'instauration de DMZ et l'utilisation de VPN sera aussi administrer via les pares-feux Fortigate. Ils fourniront les adresses IP aux équipements des 7 écoles via un serveur DHCP intégré.

Nous allons maintenant préciser le paramétrage de ces pares-feux.

IPS

On active l'IPS dans l'interface Fortigate 100E.



Menu d'administration IPS

VLAN

Nous allons en créer 3 :

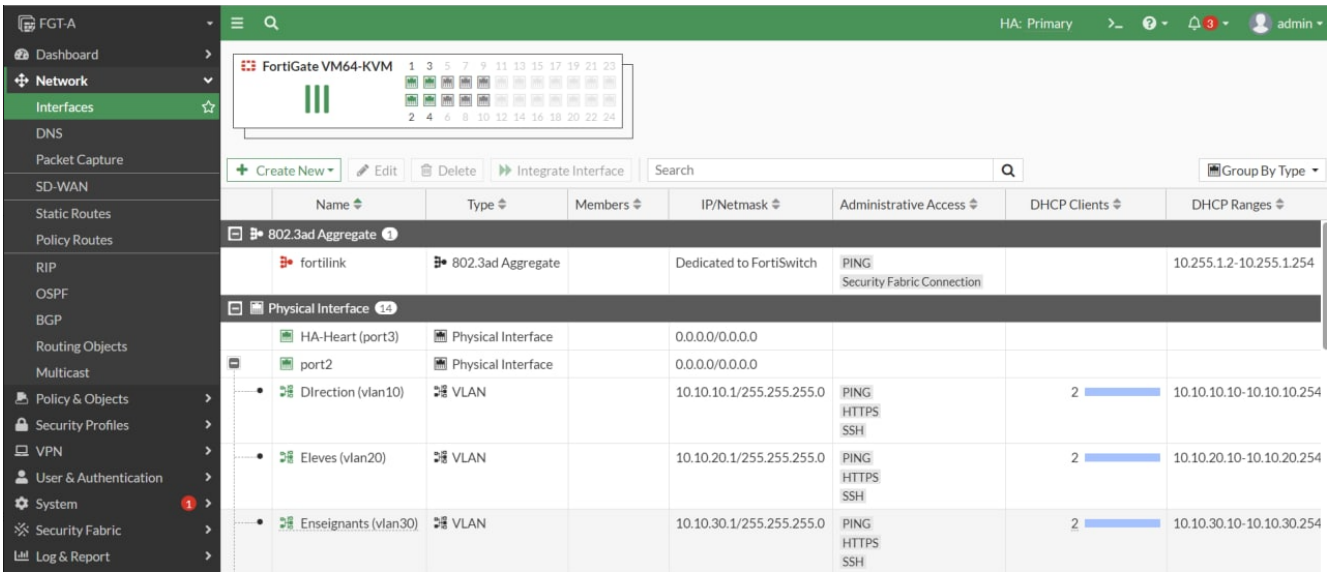
VLAN 10 : direction

VLAN 20 : élèves

VLAN 30 : enseignants

Le but de ces VLAN est de privatiser les accès par groupes d'utilisateurs.

Le serveur DHCP du pare-feu Fortigate attribuera les adresses IP aux bons VLANS.



Menu d'administration VLAN

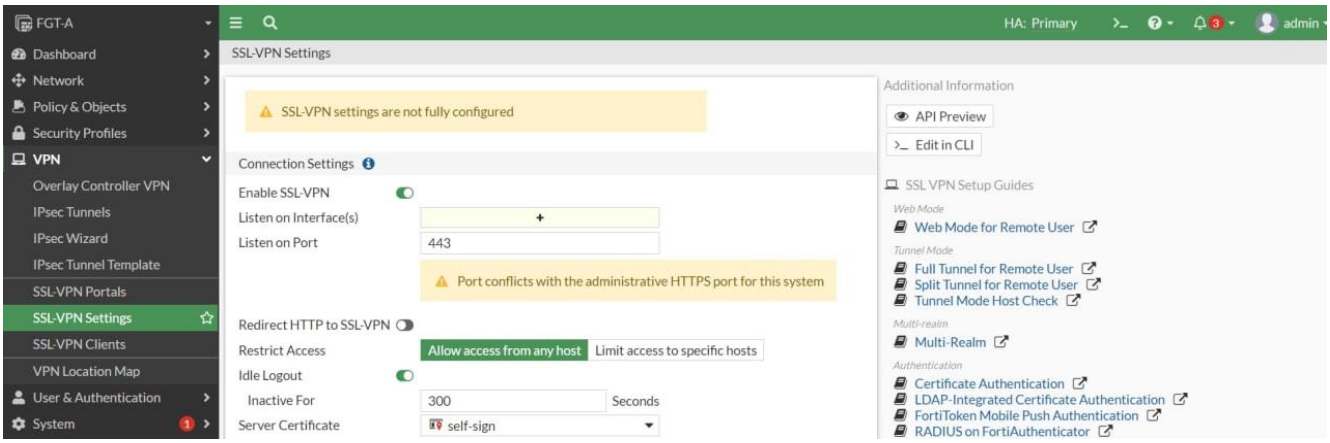
VPN

Pour que le VPN fonctionne, il y a 2 choses à créer (VPN Serveur et VPN Clients) :

1 VPN Serveur.

125 VPN Clients (directions et enseignants), nos utilisateurs pourront y accéder via un URL(version light) renseigné sur un navigateur internet .

Il leur suffira de s'identifier



Menu d'administration VPN

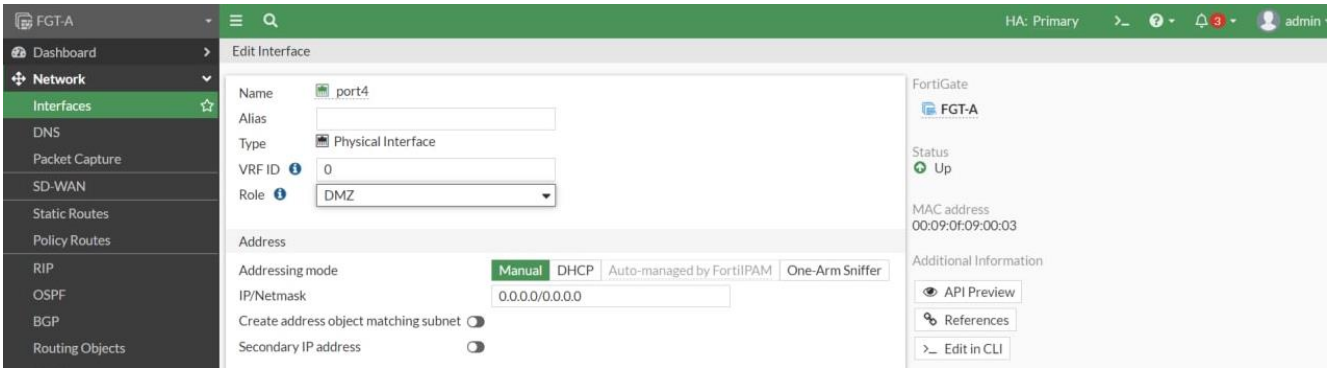
DMZ

Nous aurons 2 DMZ identiques, 1 à la mairie, 1 à la SNST.

Il y a deux activités principales dans la DMZ : proxy-inverse et WAF.

La DMZ fera liaison en internet et les utilisateurs via le proxy-inverse.

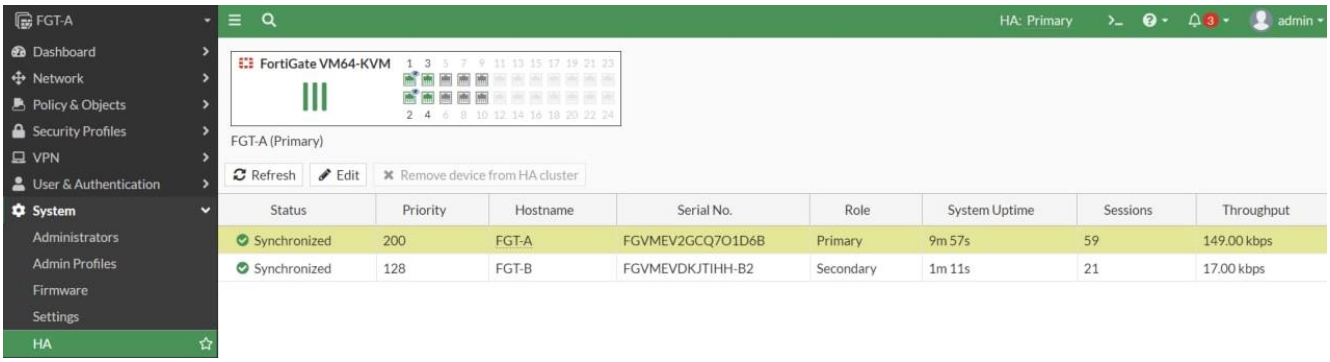
L'activation du WAF (Pare-feu d'application) dans la DMZ permettra de bloquer le contenu indésirable passant par le port http (port 80).



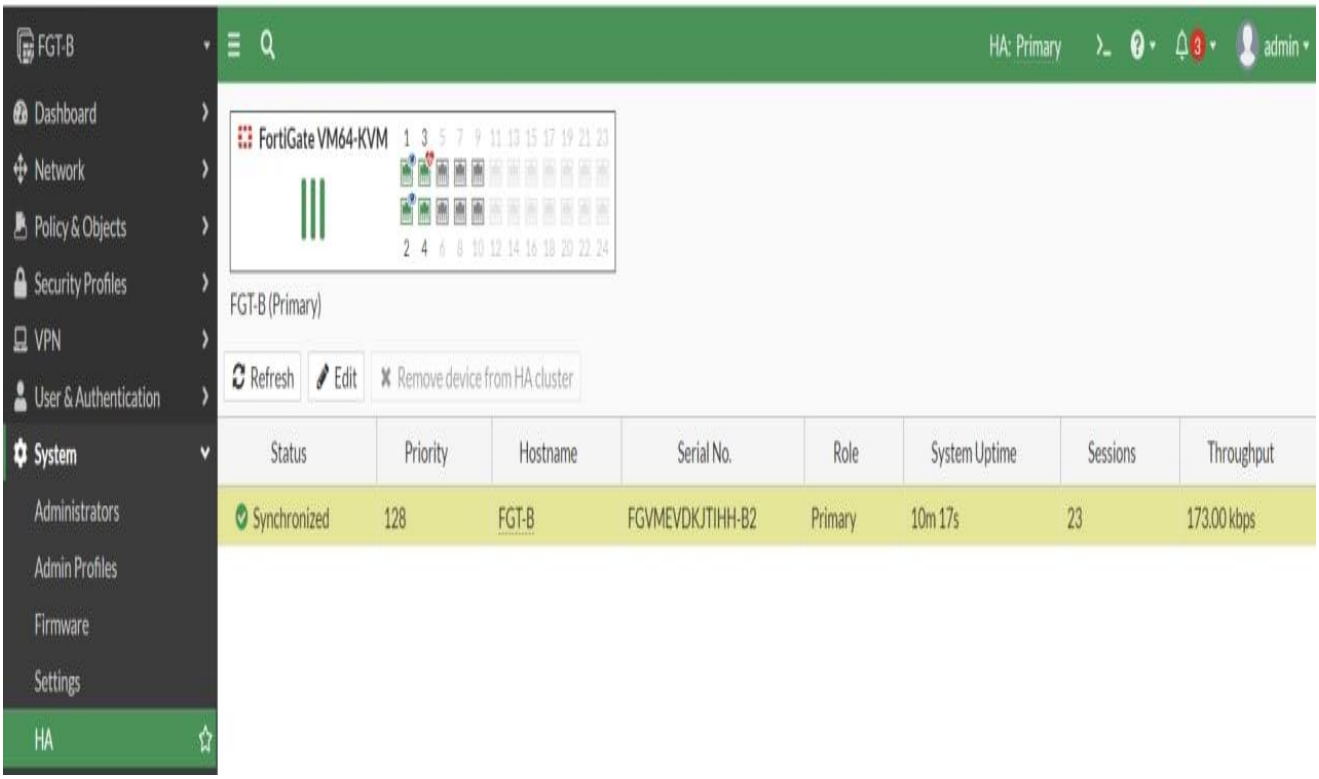
Menu d'administration DMZ

HA

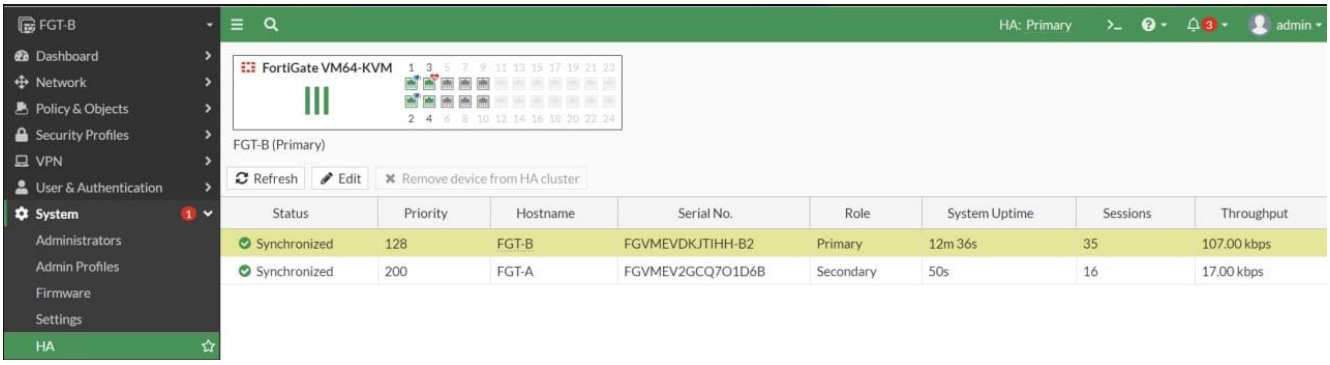
Redondance haute disponibilité, en statut : « *active-active* ». Cela permet la prise de relais automatiquement en cas de panne sans coupure de service.



Menu d'administration Système Fortigate



Mise en place HA sur le deuxième pare-feu en cas de défaillance du premier



Menu d'administration HA pour les deux pares-feux

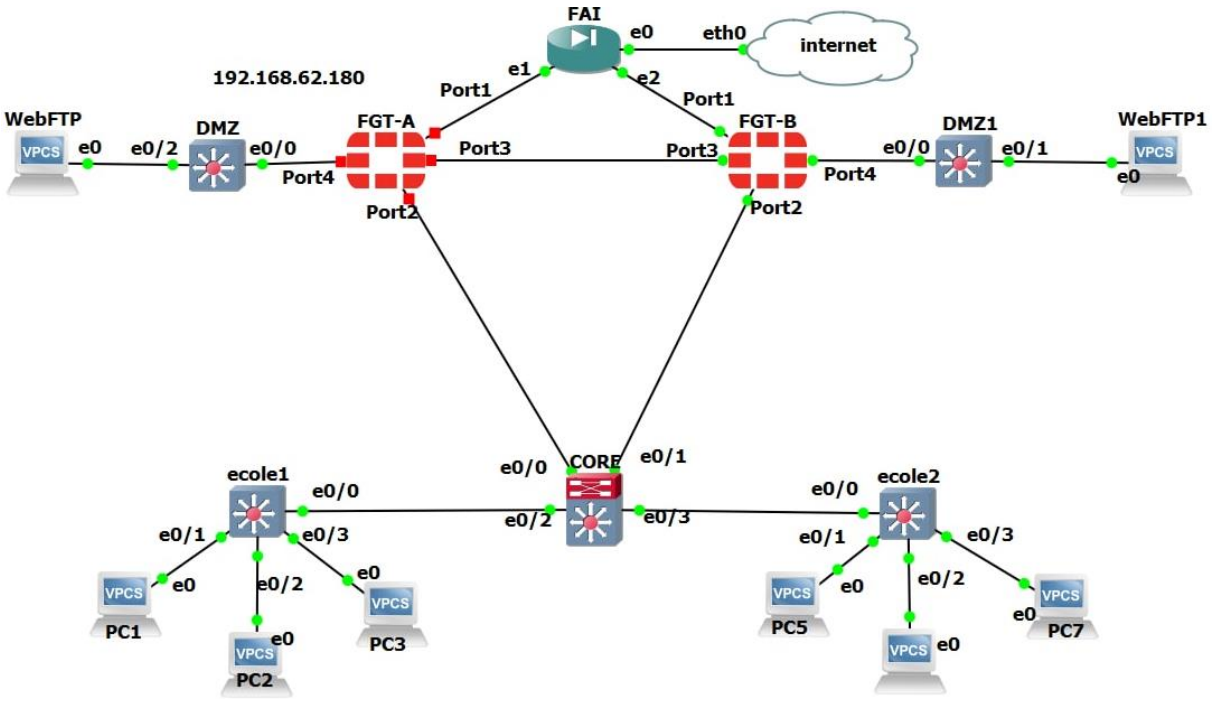


Schéma simplifié du réseau SNTS

On a 4 HA :

HA-FAI = 2 câbles connectés en parallèle. En cas de panne, le second prendra le relais. Il sera connecté sur le port SD-WAN du pare-feu.

HA-Fortigate = en condition active-active.

HA-switch = en redondance parallèle, si le premier switch tombe en panne, le système va automatiquement basculer sur le second switch. Le contrôle se faisant via le serveur Witness. Configurer directement via les pares-feux. (cf partie : Maintien de l'activité)

HA-Serveurs = présence de deux serveurs en parallèle, redondance active-active. Les données des serveurs des écoles seront sauvegardées sur ces 2 machines. Deux lieux de sauvegarde distincts. (cf partie : Maintien de l'activité)

WITNESS

Le Witness sera installé dans l'école 4 qui se situe géographiquement au centre du réseau. (cf Schéma réseau STNS)

LACP

Chaque école a besoin de 2 câbles LACP pour connecter les 2 switchs. Nous choisirons des câbles réseau avec pour débit 1 Gbits/s.

.

Les équipements seront séparés sur deux lieux : les locaux du SNTS et la Mairie.

Chaque lieu accueillant des infrastructures seront identiques (un FAI, un pare-feu Fortigate 100e, un switch Core, un Switch DMZ, un serveur FTP).

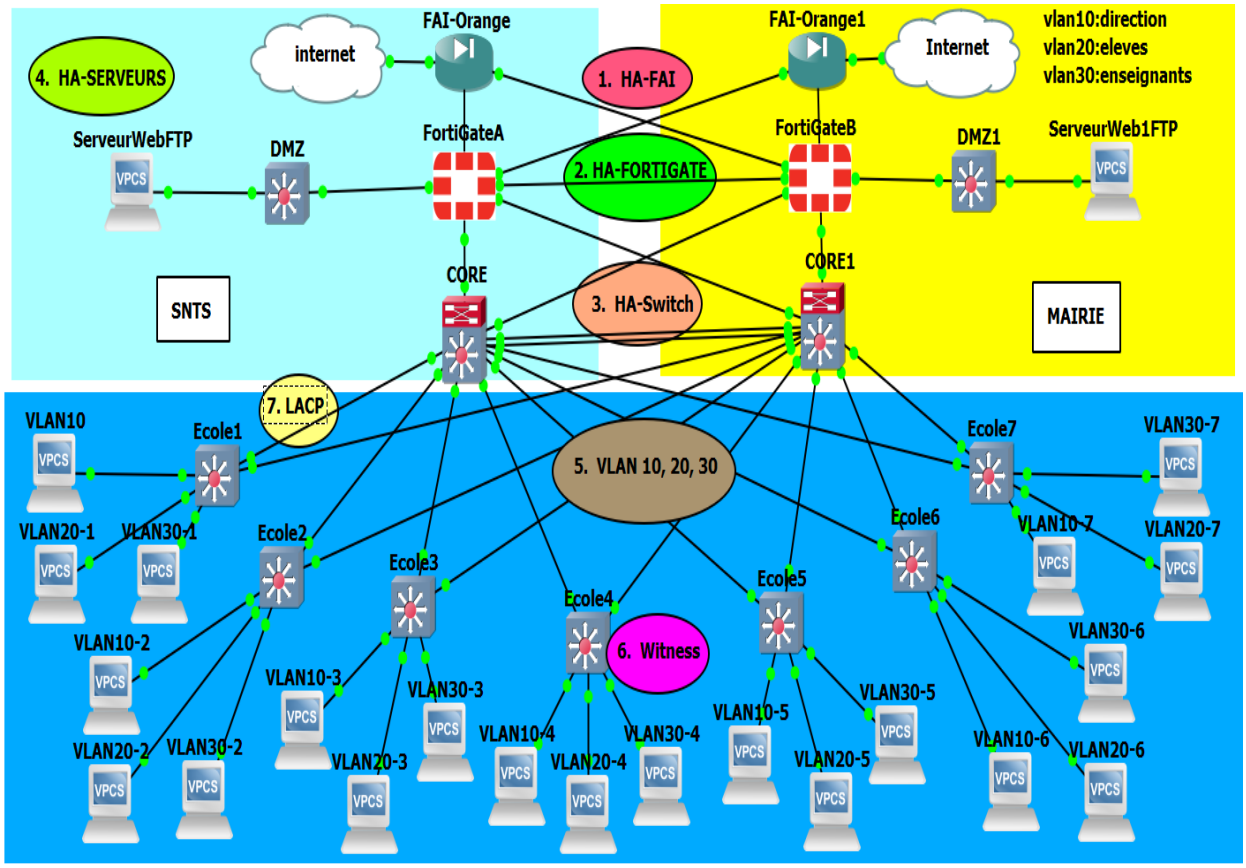


Schéma détaillé du SNTS

Antivirus

Nous avions déjà sélectionné l'antivirus pour les postes lors du renouvellement des postes informatiques effectué précédemment. Les antivirus seront déployés via l'image utilisé par MDT.

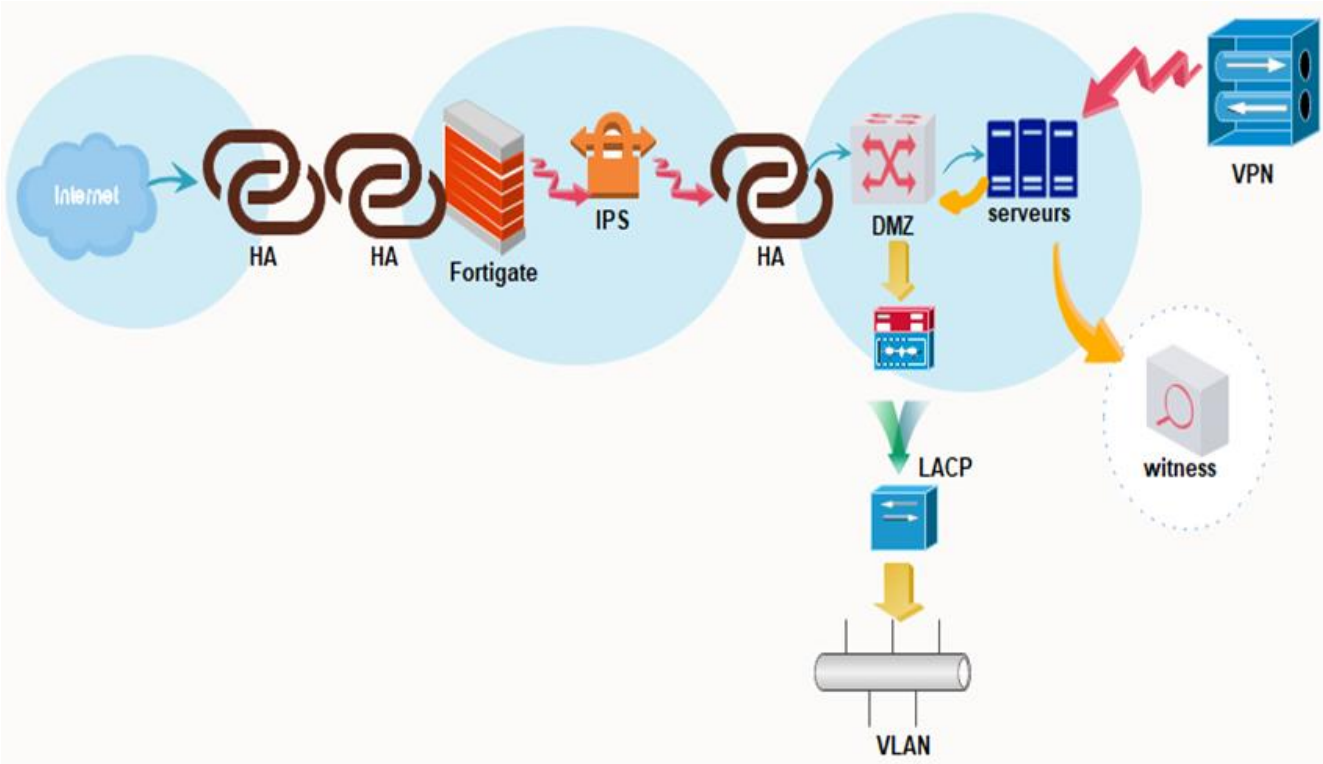
Budget

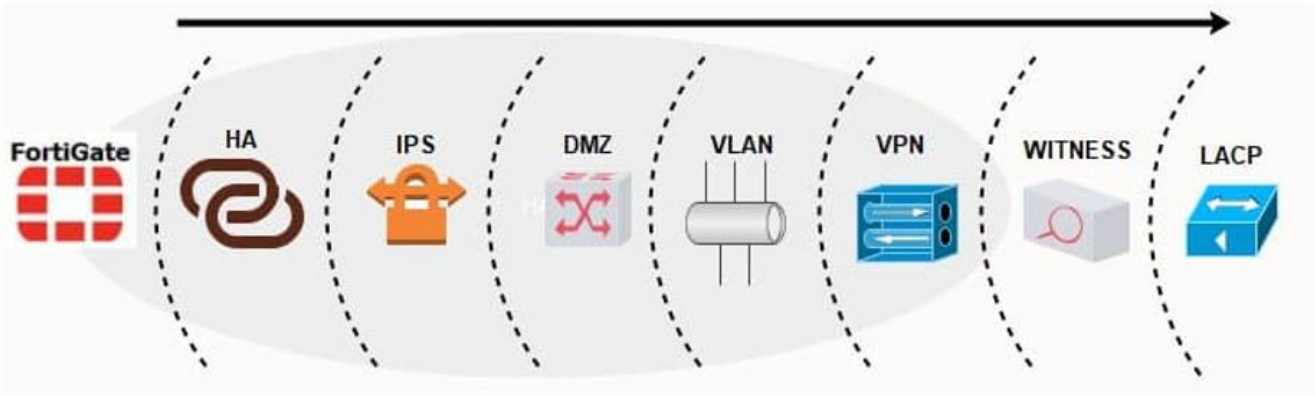
On décide de prendre Fortigate version 100E, avec le prix minimum et l'efficacité du blocage maximum **(annexe 3)**.

Pour un budget de 1676,80 € HT d'achat de matériels.

L'achat des licences ESETnod32 (antivirus) ayant déjà été effectué lors du renouvellement du parc, il ne rentre pas en compte dans le budget de sécurisation.

Synthèse





Sécurisation du réseau SNTS

Nous avons finalement 8 couches de sécurité, dont les 6 premières étant à l'intérieur du pare-feu Fortigate.

Pour le reste, nous avons besoin d'un serveur Witness et des câbles LACP pour sécuriser notre réseau de toutes les interférences externes et internes.

Les 8 couches sont nécessaires pour que notre réseau soit sûr, rapide, synchrone, en flux continu, et ne sois jamais en panne quoi qu'il arrive.

La sécurisation du parc informatique et du réseau ayant été prévu, nous allons maintenant définir un moyen efficace d'administrer les utilisateurs.

Centralisation du Parc

Scripting efficace

Contexte

Lors de la reprise du contrôle de l'informatique des écoles de la communauté de communes du Castillonnais par le SNTS, nous avons repensé et réorganisé son fonctionnement.

Premièrement en changeant les postes utilisateurs, portables ou fixes, qui le nécessitaient, en établissant des plans de maintenance préventive et curative, en organisant le réseau sans fil et filaire des écoles.

Dans un second temps, l'intégralité des serveurs ont été changés dans les écoles.

Cela amenant une gestion de sept annuaires d'utilisateur, un pour chaque regroupement d'école.

Besoins

Le regroupement des écoles de la communauté de communes du Castillonais en 7 pôles, ces pôles tous géré et administrer par le STNS, amène une gestion d'un très grand nombre d'utilisateurs.

De ce fait, nous avons besoin d'outils qui permettent la création et le paramétrage d'un très grand nombre d'utilisateurs de manière simple et efficace.

D'un outil ayant une interface simple et claire, qui permettent une bonne visualisation de notre annuaire de compte.

De plus, nous allons devoir faire pour chaque rentrée scolaire de lourd changement sur tous les comptes des élèves et sur les comptes enseignants. De part, les suppressions des comptes des élèves quittant l'établissement, les créations des comptes des élèves nouvellement inscrit à l'école, ainsi que par les changements de tous les élèves de classe et de niveaux chaque début d'année.

Notre solution d'administration doit pouvoir s'adapter, et permettre de faire des modifications automatisées.

La communauté de communes des écoles du Castillonais souhaite établir des règles de sécurité concernant les dossiers personnels de chaque membre des écoles, les dossiers partagés de chaque classe et des accès plus importants pour les enseignants et les membres de la direction.

Ces accès doivent être restreint par des heures de connexions selon chaque type d'utilisateurs.

Les solutions possibles

Nous avons donc besoin d'un annuaire d'utilisateur permettant l'administration et l'authentification des étudiants et du personnel encadrant des écoles.

Ils existent plusieurs solutions disponibles sur le marché. Qu'elles soient libres de droit ou payante, supporter par Microsoft ou développer par des équipes sur Linux.

Nous pouvons donc choisir d'utiliser sur une solution libre de droit tel que Samba AD ou OpenLDAP. Ces solutions fonctionnent sous un environnement Linux.

Samba AD possède des fonctionnalités de partage de fichier et d'imprimantes ainsi qu'une fonction Active Directory.

OpenLDAP est un annuaire informatique, annuaire libre il permet la gestion, jusqu'à un très grand nombre d'utilisateur. Il ne stock pas directement des données, il doit être utilisé une bibliothèque tierce. A noter qu'il est possible de créer un serveur OpenLDAP sous Windows soit via des entreprises tierces et donc des solutions payantes, soit grâce à un développeur, Lucas Bergman qui a effectué les modifications nécessaires aux sources pour avoir une version prête à l'emploi sous Windows.

Comme toutes les solutions Linux, ces solutions sont principalement paramétrables et administrables par via des lignes de commandes. Ce qui permet une administration rapide si on maîtrise l'utilisation des lignes de commandes. Mais ce qui peut être très déroutant si on découvre l'utilisation d'un serveur en ligne de commande.

Nous pouvons aussi nous tourner vers la solution d'annuaire présente sur les serveurs Microsoft, AD DS (Active Directory Domain Service).

Qui permet la gestion des profils et des droits sur l'annuaire, ainsi que l'authentification sur le domaine. Via l'installation d'une fonctionnalité sur un serveur Windows. Ce processus est facilité et aiguillé par Windows.

Grâce à un interface graphique, sa prise en main et intuitive, cependant cette interface ne permet pas de créer un grand nombre d'utilisateur d'un seul coup.

Pour cela on doit utiliser PowerShell, un langage de script fondé sur la programmation orientée objet, disponible sur le système d'exploitation Windows (serveur ou utilisateur).

Via un système de commandes et d'utilisation de fichier au format CSV, il est possible de créer en un script de commande plusieurs centaines d'utilisateurs.

Le choix de PowerShell

Le choix de l'utilisation de PowerShell s'impose à nous. En effet nous avons déjà installé une infrastructure Windows Server dans les écoles de la communauté de communes du Castillonais.

Nous allons utiliser le service AD DS dans ces mêmes écoles, pour administrer l'annuaire, déployer les groupes de sécurités et gérer les dossiers utilisateurs.

Travaillant dans un environnement Windows, c'est donc tout naturellement que nous avons prévu d'utiliser PowerShell.

Développer pour l'environnement Windows et notamment Windows Server, PowerShell nous permettra d'automatiser des tâches. Notamment des tâches répétitives et peu complexes. PowerShell nous permettra de limiter le blocage de technicien pour ces tâches, d'empêcher les erreurs humaines lors de la grande répétition de ces tâches.

Cela fera gagner du temps à notre équipe de technicien, du fait de l'automatisation, mais aussi grâce à la fiabilité des scripts, qui empêchent des erreurs humaines.

Ces erreurs qui peuvent amener à l'immobilisation d'un ou plusieurs techniciens, des failles de sécurités ou à des blocages de l'infrastructure.

Nous arriverons grâce à l'utilisation de PowerShell à un gain d'argent pour le SNTS, et un gain de temps pour les techniciens, du temps qui leurs permettra d'être disponible pour utilisateurs dans le besoin mais aussi à élaborer les améliorations possibles de l'infrastructure réseau.

Déploiement

Grâce à une liste complète des élèves, des enseignants et des membres de la direction.

Nous avons écrit un ensemble de scripts PowerShell, pour créer et paramétrer les différents utilisateurs devant avoir accès à une session sur le réseau SNTS.

```
1   New-ADOrganizationalUnit "Direction"
2   New-ADOrganizationalUnit "Enseignants"
3   New-ADOrganizationalUnit "Eleves"
```

Création des UO

Ces trois lignes permettent la création des unités d'organisation de l'AD, qui sont la base de l'arborescence de notre annuaire

```
1   $var = import-csv "C:\CSV-PW\Classe.csv"
2   foreach ($item in $var)
3   {
4       New-ADOrganizationalUnit -Name $item.OUName -Path "Ou=Eleves,DC=JulesFerry,DC=ecole"
5       Write-Host "Creation de l'OU : " $item.OUName
6   }
7
```

Créations des sous unités d'organisation, les classes

Ce script va chercher le fichier Classe.csv, qui contient comme vous pouvez le voir ci-dessous, une colonne avec les différentes classes à créer. Pour chaque ligne, le script va une créer une sous OU, dans l'OU Eleves. Il est important de bien renseigner où est ranger le fichier CSV.

Ces fichiers pour indications sont une liste comprise par PowerShell. Elle indique les attributs ou les objets dont il a besoin pour exécuter les commandes avec les bons paramètres. Ces

paramètres qui seraient à renseigner à chaque nouvelle exécution de la commande sont prés-renseignés dans le CSV et sont récupéré par PowerShell.

La première ligne indique la nature des attributs et les lignes en dessous le nombre d'itérations dont on a besoin.

Dans le cas précis, nous devons créer des OU pour chaque classe, nous avons donc défini le nom de l'attribut dans nous avons besoin « OUName » et les noms de chaque classe à créer dans le listing.

```
OUName
Classe1
Classe2
Classe3
Classe4
Classe5
```

Listing Classe

```
$Users = import-csv -path "C:\CSV-PW\ElevesJulesFerry.csv" -delimiter ";"

foreach($user in $users)
{
$pass= $user.pass
$nom= $user.name
$surname= $user.surname
$prenom= $user.givenname
$SamAccountName= $user.SamAccountName
$ou= $user.ou

New-ADUser -name $nom -GivenName $prenom -Surname $surname  -SamAccountName $SamAccountName -Path $ou -AccountPassword (ConvertTo-SecureString -AsPlainText $pass -Force) -Enable $true -ChangePasswordAtLogon $true
}
```

Création des comptes Elèves

Via PowerShell, il est possible de créer une multitude d'utilisateur en une seule fois.

Comme vu précédemment pour les classes, via un fichier CSV, chaque ligne correspondant à un élève et chaque colonne à un paramètre du compte AD, le tout séparer par des points-virgules, car nous avons défini dans le script que le point-virgule marquerait le changement d'attribut.

ElevesJulesFerry - Bloc-notes

Fichier Edition Format Affichage Aide

```
givenname;surname;name;SamAccountName;ou;pass
Theo;ABBOU;Theo ABOOU;tabbou;OU=Classe1,OU=Eleves,DC=JulesFerry,DC=ecole;JulesFERRY2021!*
Candice;CARMEGOM;Candice CARMEGOM;ccarmegom;OU=Classe2,OU=Eleves,DC=JulesFerry,DC=ecole;JulesFERRY2021!*
Jonathan;VILATTE;Jonathan VILATTE;jvilatte;OU=Classe3,OU=Eleves,DC=JulesFerry,DC=ecole;JulesFERRY2021!*
Lukas;MAZAUD;Lukas MAZAUD;lmazaud;OU=Classe4,OU=Eleves,DC=JulesFerry,DC=ecole;JulesFERRY2021!*
Jade;PEREY;Jade PEREY;jperey;OU=Classe5,OU=Eleves,DC=JulesFerry,DC=ecole;JulesFERRY2021!*
```

Détail CSV importation comptes Elèves

Ici on paramètre chaque compte Elèves avec un nom, prénom, un nom complet, un login, l'endroit où il doit être créer et le mot de passe du compte (qui doit être changé à la première connexion).

```powershell
$Users = import-csv -path "C:\CSV-PW\EnseignantsDirectionJulesFerry.csv" -delimiter ";"

foreach($user in $users)
{
$pass= $user.pass
$nom= $user.name
$surname= $user.surname
$prenom= $user.givenname
$SamAccountName= $user.SamAccountName
$ou= $user.ou

New-ADUser -name $nom -GivenName $prenom -Surname $surname  -SamAccountName $SamAccountName -Path $ou -AccountPassword (ConvertTo-SecureString -AsPlainText $pass -Force) -Enable $true -ChangePasswordAtLogon $true
}
```

Création comptes Enseignants et Direction

Le fonctionnement reste le même que pour la création des comptes AD des élèves. Avec également un CSV contenant la liste des comptes à créer et les attributs que l'on souhaite intégrer.

```
surname;givenname;name;SamAccountName;ou;pass
SCHIFFER;Lia;Lia SCHIFFER;lschiffer;OU=Enseignants,DC=JulesFerry,DC=ecole;JulesFERRY2021!%
TONON;Joelle;Joelle TONON;jtonon;OU=Enseignants,DC=JulesFerry,DC=ecole;JulesFERRY2021!%
MARTIN;Laure;Laure MARTIN;lmartin;OU=Enseignants,DC=JulesFerry,DC=ecole;JulesFERRY2021!%
BAYSSETTE;Laurence;Laurence BAYSSETTE;lbayssette;OU=Enseignants,DC=JulesFerry,DC=ecole;JulesFERRY2021!%
BOUHLAIS;Veronique;Veronique BOUHLAIS;vbouhlais;OU=Enseignants,DC=JulesFerry,DC=ecole;JulesFERRY2021!%
ROBICHET;Robert;Robert ROBICHET;rrobichet;Ou=Direction,Dc=JulesFerry,DC=ecole;JulesFERRY2021!%
PATULACCI;Marcel;Marcel PATULACCI;mpatulacci;Ou=Direction,Dc=JulesFerry,DC=ecole;JulesFERRY2021!%
RENAUD;Line;Line RENAUD;lrenaud;Ou=Direction,Dc=JulesFerry,DC=ecole;JulesFERRY2021!%
```

Détail CSV importation comptes Directions et Enseignants

Une fois chaque compte utilisateur créé et ranger dans la bonne unité d'organisation grâce à du Scripting avancé.

Nous allons utiliser PowerShell pour nous permettre une bonne gestion des horaires de connexions et des dossiers partagés et personnels. En déployant des paramètres à un grand nombre d'utilisateur.

```powershell
New-ADGroup "Direction" -Path "OU=Direction,DC=JulesFerry,DC=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
New-ADGroup "Enseignants" -Path "OU=Enseignants,DC=JulesFerry,DC=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
New-ADGroup "Eleves" -Path "OU=Eleves,DC=JulesFerry,DC=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
```

Création des groupes de sécurité globaux

Ces lignes de code permettent dans chaque OU principale, un groupe de sécurité global qui lui est attitré. Ces dits groupes seront utiles pour le paramétrage des dossiers partagés.

```powershell
New-ADGroup "Classe1" -Path "OU=Classe1,OU=Eleves,DC=JulesFerry,Dc=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
New-ADGroup "Classe2" -Path "OU=Classe2,OU=Eleves,DC=JulesFerry,Dc=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
New-ADGroup "Classe3" -Path "OU=Classe3,OU=Eleves,DC=JulesFerry,Dc=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
New-ADGroup "Classe4" -Path "OU=Classe4,OU=Eleves,DC=JulesFerry,Dc=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
New-ADGroup "Classe5" -Path "OU=Classe5,OU=Eleves,DC=JulesFerry,Dc=ecole" -GroupCategory Security -GroupScope Global -PassThru -Verbose
```

Création groupes de sécurité par classe

De même pour les groupes de sécurités globaux de chaque classe.

Extraction des membres d'une unité d'organisation

Pour le paramétrage des horaires de connexions de chaque compte, nous avons eu besoin d'avoir la liste de tous les élèves et tous les enseignants.

```
Get-AdUser -filter {enabled -eq $true} -SearchBase "OU=Enseignants,DC=JulesFerry,DC=ecole" | select samaccountname | export-csv -delimiter ',' -path 'C:\Horaires\Enseignants.csv'
```

Script extraction OU Enseignants

Grâce à cette ligne de code, nous avons pu obtenir tous les logins des enseignants de cette école, afin d'y appliquer des restrictions horaires.

```
Get-AdUser -filter {enabled -eq $true} -SearchBase "OU=eleves,DC=JulesFerry,DC=ecole" | select samaccountname | export-csv -delimiter ',' -path 'C:\Horaires\eleves.csv'
```

Script extraction OU Elèves

```
import-CSV C:\CSV-PW\Eleves.csv -Header samaccountname | ForEach-Object {Add-AdGroupMember -Identity "Eleves" -members $_.samaccountname}
```

Attribution de groupe de sécurité Elèves chaque élève

L'export que nous avons fait précédemment de tous les logins de chaque, permet avec ce script, de les ajouter tous en même temps dans le groupe de sécurité Elèves.

Limitations horaires de connexions

Le paramétrage et le déploiement des horaires de connexion sur les comptes des élèves se fait avec deux commandes Shell, en utilisant les deux exports des logins des enseignants et des élèves.

```
For /F "skip=1 tokens=1 delims=," %%i IN (C:\Horaires\eleves.csv) DO (net user %%i /time:L-V,9:00AM-5:00PM;)
pause
```

Pour les élèves.

```
For /F "skip=1 tokens=1 delims=," %%i IN (C:\Horaires\Enseignants.csv) DO (net user %%i /time:L-V,7:00AM-8:00PM;)
pause
```

Et pour les enseignants.

Shell est différent de PowerShell mais, il est adopté dans notre situation, grâce à cet éditeur de commande, on peut appliquer les paramètres horaires à tous les comptes qui en ont besoin, et cela sans avoir à rentrer dans l'AD et à faire des manipulations sur chaque profil.

Au cours de la première année, nous allons attribuer à un technicien la tâche de rédiger et de tester un script PowerShell permettant de mettre à jour les annuaires, c'est-à-dire, un script qui

automatise les changements de classe de chaque nouvelle année pour les élèves et les enseignants, ainsi que la suppression des élèves quittant les écoles et la création des élèves arrivants. Tout en réutilisant le script Shell pour appliquer les restrictions horaires.

Budget

L'automatisation via PowerShell ne rajoute pas de surcout à notre budget, en effet, les serveurs ont déjà acheter lors d'un précédent projet. C'est pour cela le Scripting via PowerShell est un gain d'argent et un gain de temps pour le SNTS.

Synthèse

L'utilisation de PowerShell et d'un Scripting avancé permet d'administrer son parc de manière efficace, rapide et en limitant les erreurs humaines.

Cela nécessite un solide travail en amont. Une fois une période de test et les scripts fonctionnels. Les changements à apporter en début d'année scolaire se feront en seulement quelques manipulations. La bonne rédaction des fichiers CSV nécessite une attention particulière un fois cette étape fastidieuse faite, le Scripting est simple.

Nous avons sécurisé notre réseau et nos postes, prévu l'administration de utilisateurs de manière automatisé et de manière à réduire les erreurs humaines.

Nous allons maintenant réfléchir à un moyen de maintenir l'activité informatique des écoles de manière le plus optimal possible.

Maintien de l'activité

Contextualisation

Nous avons un bureau SNTS (Services Numériques et Technologiques Scolaire) qui supervise sept écoles au total. Nous devons choisir un moyen pour maintenir en bon fonctionnement l'infrastructure du SNTS et donc des sept écoles différentes.

En effet nous ne pouvons pas nous permettre de perdre des données scolaires ou que les professeurs ou membres de la direction ne puisse pas accéder à notre réseau pendant un laps non négligeable.

Besoins

Nous avons besoin d'un système qui permettrait de maintenir tout le réseau, et l'infrastructure du SNTS et des écoles en fonctionnement, si jamais un des équipements ne cesse de fonctionner. Cette solution doit être rapide, nous ne pouvons pas nous permettre de rester plusieurs heures sans avoir accès au réseau.

Si possible, ne nécessitant pas ou peu l'intervention d'un technicien, cette solution doit être autonome si possible.

En cas d'impossibilité de récupérer les données des écoles, nous devons avoir une solution qui nous permette de repartir sur une image antérieure du réseau. Dans le but de permettre un retour à la normale le plus vite possible.

Solutions possibles

Nous avons deux solutions possibles dans ce cas-là :

Le PCA : plan de continuité d'activité, comme son nom l'indique il permet de continuer à pouvoir utiliser le réseau, travailler sans être touché dû à la défaillance d'un objet. Il est utilisé dans les entreprises qui ne peuvent pas se permettre de mettre tout à l'arrêt pendant un intervalle trop long.

Le PRA : plan de reprise d'activité, comme son l'indique lui aussi, il permet de reprendre l'activité de l'infrastructure après un problème, un arrêt immédiat d'un objet ou d'une machine. Contrairement au plan de continuité d'activité, les utilisateurs sont fortement touchés lorsque le PRA est mis en place. Ils ne peuvent donc pas travailler jusqu'à ce que le service informatique trouve une solution au problème rencontré.

Choix

Souhaitant limiter au maximum l'intervention et le blocage d'un ou plusieurs techniciens, notre solution devra être autonome.

Elle devra limiter au maximum la perte de données, maintenir l'accès au réseau et aux données.

Nous devrons aussi pouvoir retrouver les données en cas de défaut majeur de l'infrastructure réseau.

Nous devons avoir une solution complète, c'est pour cela que nous souhaitons privilégier un PCA, que nous souhaitons développer au maximum pour permettre une continuité maximale de l'activité.

Pour cela nous allons doubler notre infrastructure, doubler tous les équipements.

Avec deux accès internet pour alimenter notre réseau, un à la mairie, et un au SNTS.

Acheter deux pares-feux Fortigate que nous avons déjà choisi dans la partie sécurisation du parc, deux onduleurs.

	Eaton 5p 650iR	Eaton Ellipse pro 1200	Eaton ATS 16 Netpack
Est-il rackable ?	Oui	Non	Oui
Prix (HT) en euros	357	239	1047

Tableau Comparatif Onduleur

Celui qui correspond le mieux à nos attentes est l'onduleur Eaton 5p 650iR, c'est un onduleur rackable a un prix imbattable

Nous devons aussi doubler les serveurs, nous en possédons un au SNTS, mais nous devons en acheter un pour le local de la mairie qui sera le serveur esclave

	Dell EMC R340	Dell PER540PLM03	Dell SRV-800
Est-il Rackable ?	Oui	Oui	Non
Prix (HT) en euros	1287,6	1962	

Tableau comparatif Serveur

Nous choisissons donc le DELL EMC R340, celui-ci est rackable et est affiché au prix de 1287 € Hors taxe.

Avec en parallèle, une sauvegarde régulière de toutes nos données, stockée chez un hébergeur pour permettre une reprise si nous perdons totalement notre infrastructure.

Nous mettons en place une sauvegarde journalière ainsi qu'une plus grosse hebdomadaire.

Nous avons comparé trois systèmes de sauvegardes

	Veeam	Arcserve	Windows Sauvegarde
Prix /5	3	3	1
Facile d'utilisation /5	5	2,5	4
Facile d'accès /5	5	2	4

Tableau comparatif Logiciel de sauvegarde

À la suite de notre comparaison entre différents systèmes de sauvegarde, deux logiciels nommés Veeams Backup et Acserve UDP backup. Nous avions également la possibilité de sauvegarder les fichiers sur le serveur directement à l'aide d'une fonctionnalité proposé par Windows Server.

Nous avons choisi Le logiciel Veeam Backup pour sa facilité d'utilisation de sauvegarde et récupération mais également pour son prix attractif qui est de 1670,74 HT.

Configurations et déploiements

Plan de continuité d'activité :

Nous avons donc mis en place une double infrastructure, une au service SNTS Services Numériques et Technologiques Scolaire qu'on appellera l'infrastructure Maître, et la seconde qui se trouvera à la mairie, cette dernière on lui donnera comme nom l'infrastructure secondaire (esclave).

Pourquoi avoir choisi de mettre deux infrastructures ?

Simplement, si une machine ne cesse de fonctionner au bureau SNTS, celle de la mairie prendra le relai sans intervention humaine et surtout sans arrêt du système informatique.

Nous allons doubler l'accès à internet à l'entrée de notre réseau, au cas où l'un flanche et ne parvient plus à fournir l'accès à un point, l'autre peut prendre le relais.

Nous avons besoin de mettre en place un pare-feu.

Vu que nous doublons les équipements, nous aurons deux pares-feux, un maître et un esclave. L'esclave prendra le relai sur le maître, si ce dernier tombe en panne.

Le 2ème pare-feu sera en redondance avec le 1er. En cas de panne, il prendra donc le relais en temps réel.

Nous allons aussi acheter deux onduleurs, pour en placer un à la mairie et un au local du SNTS, qui doivent alimenter tous les équipements, dont deux serveurs

Nous avons aussi deux switchs, un au SNTS et un à la mairie.

Avec les liens doublés, tous cela pour aboutir à un schéma réseau comme montrer ci-dessous.

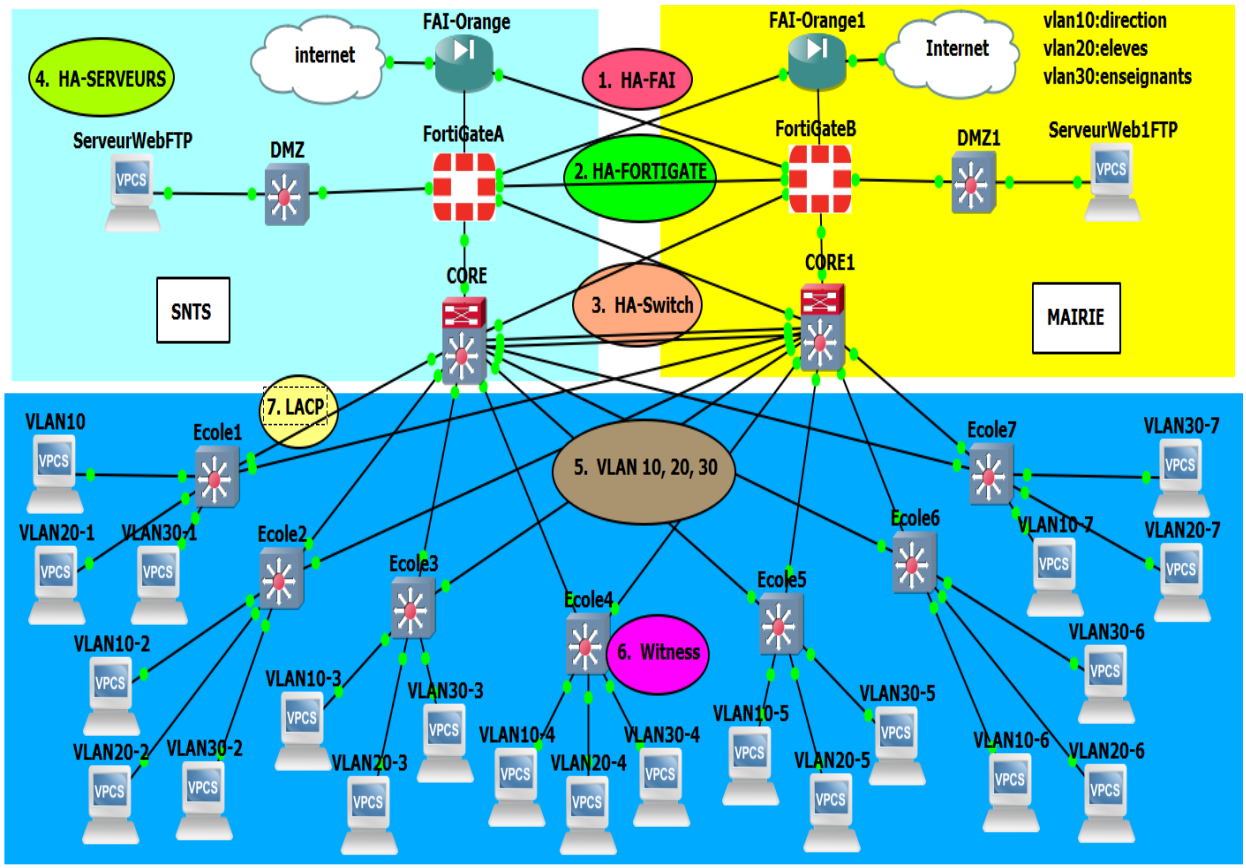


Schéma détaillé réseau SNTS

Grâce au doublement de toute notre infrastructure, de l'accès FAI jusqu'au switch. Nous permettons une disponibilité optimale de notre réseau et de nos données.

Le paramétrage en mode HA (High availability), autrement haute disponibilité, permet grâce à l'utilisation couplé d'un Witness et de l'agrégation de liens (LACP) de palier à une panne d'un des équipements. L'équipement de secours (slave)prendra le relais en cas de défaillance de l'équipement principal (master).

Comme indiqué dans les documents ci-dessous comprennent un schéma du fonctionnement du cluster HA, ainsi qu'un tableau indiquant les différents chemins réseaux en fonction d'un élément en panne.

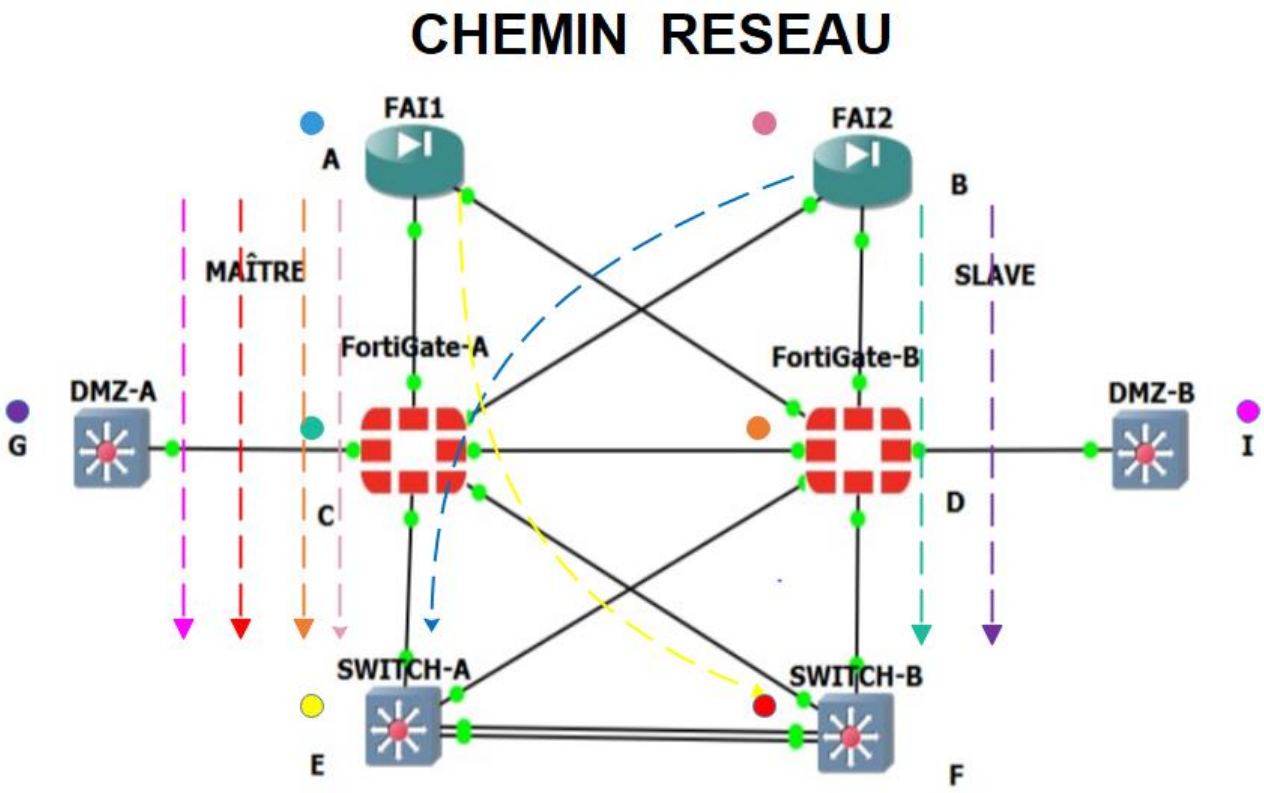


Schéma Fonctionnement cluster HA

Cas	Etat équipement	Chemin réseau
1	A éteint	B-C-E
2	B éteint	A-C-E
3	C éteint	B-D-F
4	D éteint	A-C-E
5	E éteint	A-C-F
6	F éteint	A-C-E
7	G éteint	B-D-F
8	I éteint	A-C-E

Tableau des différents cas de fonctionnement

Concernant les données, elles sont sauvegardées en permanence, sur les serveurs présents à la mairie et au SNTS. Ces serveurs sont en redondance active, et s'écrive en même temps afin que si l'un flanche l'autre prendre le relais.

Pour avoir une couche de sécurisation supplémentaire, nous allons grâce à Veeam Backup effectué des sauvegardes de toutes les données. Données qui seront stockés chez un hébergeur professionnel, OVH, que nous avons choisi car c'est un hébergeur français, reconnu, et au coût accessible.

Une sauvegarde journalière des dossiers utilisateurs sera faite en fin de journée à 20H. La sauvegarde effacera la sauvegarde de la veille.

Une sauvegarde hebdomadaire sera effectuée le samedi à 23H, pour sauvegarder l'ensemble de l'infrastructure des écoles, qui effacera la sauvegarde précédente.

Ainsi nous pourrons récupérer les données des dossiers personnels à J-1 afin de minimiser la perte de données en cas de défaillance majeure ainsi que de pouvoir faire une récupération des serveurs complète des serveurs si besoin est dans un cas extrême.

Budget

Ce niveau de sécurisation implique de prévoir un budget conséquent.

En effet, un tel choix de sécurisation nous amène à avoir un achat de matériel conséquent.

En se basant sur les devis que nous avons établis (présents en annexe de ce document).

Le coût total de la mise en place de notre solution de maintien de l'activité sur les 7 écoles est de 19 401,14 € HT pour les 12 premiers mois de fonctionnements.

Pour les années suivantes, jusqu'au remplacement de matériel informatique, le coût annuel de notre solution sera d'approximativement de 15 722,74 € HT par année, en fonction de l'évolution des prix de l'hébergement externe et du coût de la licence annuelle permettant de faire la sauvegarde

Synthèse

Nous avons fait le choix de partir sur une solution de maintien de l'activité complète et la plus performante possible. En axant notre réflexion de manière à fournir une solution autonome le plus possible, via un doublement des équipements informatiques. Equipements paramétrés dans des clusters hautes disponibilités, palliant les pannes éventuelles.

En effet via un témoin placé dans une école, le système est capable de détecter un élément du réseau en panne. Permettant au système de changer le réseau afin de maintenir son activé

Le tout soutenu par une sauvegarde externalisé pour avoir un troisième lieu de stockage dans le cas d'une crise extrême.

Cette solution de maintien de l'activité vient compléter notre projet en ajoutant une couche de sécurisation supplémentaire pour permettre aux équipements des écoles et à leurs utilisateurs de travailler.

Conclusion

Ce nouveau projet, nous a permis d'aborder de manière efficace la gestion et la sécurisation d'un parc informatique.

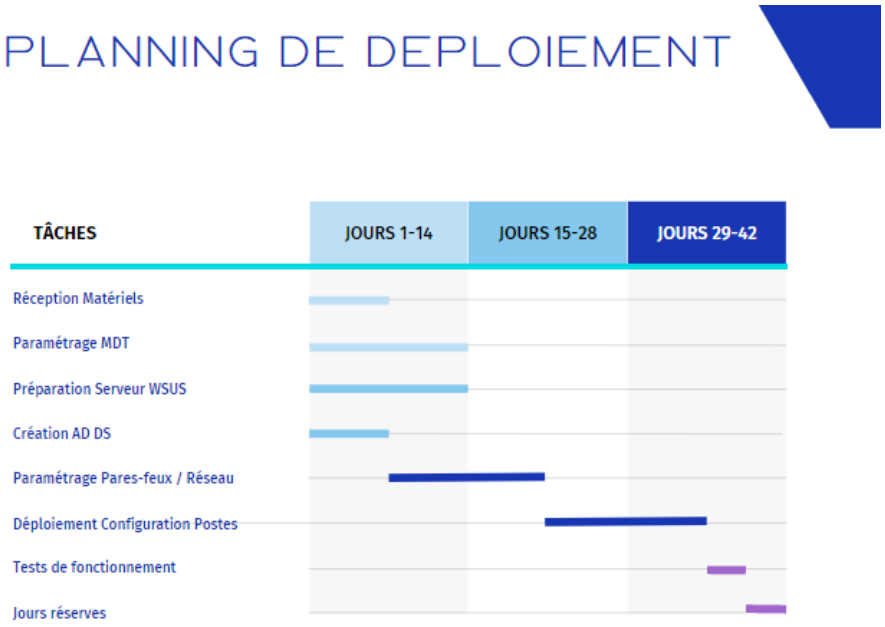
Au travers de ce document, les membres de l'équipe du SNTS ont mis en commun leurs compétences et leurs esprits, chacun apportant sa pierre à cet édifice qui a été la conception de ce projet.

Nous avons accès notre plan d'action en privilégiant les solutions favorisant l'automatisation des tâches et en réduisant le plus possible les tâches répétitives pour nos techniciens.

Nous avons gardé en tête l'aspect sécuritaire.

Via le déploiement de configuration par MDT, le maintient du parc à jour par WSUS et la gestion de l'AD DS par Scripting PowerShell. Nos techniciens ne se seront pas obnubilés par des tâches répétitives et pourront se concentrer plus aisément sur l'amélioration contenu du SNTS dans toutes ces missions.

Nous avons prévu un plan de sécurisation complet et complexe, en utilisant au mieux les possibilités offertes par les pares-feux de dernière génération. En pensant au pire, via un backup externe des données pour pouvoir permettre une reprise d'activité rapide en cas de perte majeur de données.



Planning de déploiement

Nous avons prévu un planning de déploiement n'excédant pas 6 semaines, dans l'optique de respecter notre vision de ce projet, nous avons souhaité nous laisser le temps de nous adapter et de résoudre les problèmes auxquels nous allons être confortés dans la mise en œuvre de ce projet.

Il est important de ne pas déployer un projet aussi important dans l'urgence, toujours dans le but de limiter au maximum les erreurs humaines. Nous avons prévu une phase de tests afin de les réparer et les corriger tous en gardant des jours de réserves en cas de retard lors de cette mise en application.

Annexes

Annexe 1 :

Type de Pare-feu	Cible	Avantages	Inconvénients	Exemple
Matériel	Petites et grande entreprises	- Intégré au matériel réseau - Administration simple - Bon niveau de sécurité	- Mises à jour peu flexibles suivant le constructeur - Coût peut être assez élevé.	Cisco ASA, Fortinet, Juniper, CheckPoint, Palo Alto, SonicWall
Logiciels	Personnels / Domestique	- Sécurité en bout de chaîne (installé sur le poste client) -Personnalisation facile - Moins chère que le pare-feu matériel	-Plus facilement contournable par son grand nombre d'utilisation -Ne protège que le poste sur lequel la licence est installée	Windows
Logiciels	Professionnel	-Personnalisable - Bon niveau de sécurité - Moins chère que le pare-feu matériel	- Nécessite une administration LINUX supplémentaire	Linux

Comparatif Types Pare-feu

Annexe 2 :

États travail	Cible	Avantages	Inconvénient	Exemple
Couches 1, 2, 3, 4 de TCP/IP = Liaison, réseau, transport, application. Il Contrôle : 1. des protocoles, des états, des ports. 2. WAF (couche 4), IDS, IPS, DMZ (couche 1,2,3).	Petites et Moyenne grandes entreprises	- Il fonctionne dans toutes les couches TCP/IP - Inclut des protections antivirus, - Filtrage de spams - VPN - VLAN - DMZ - IPS	-	- Fortinet - Forcepoint - Palo Alto Network - Sonicwall - Cisco Barracuda Network - Versa Network -Watchguard - Checkpoint - Sopho -Stormshield

Fonctionnalités des pares-feux nouvelle génération

Annexe 3 :

Pare-feu NGPF ~	Efficacité du blocage	Prix d'achat HT (Serie)
Fortinet	99%	1048€ (FG-100E)
ForcePoint	99%	1599€ (Serie 321)
Sonic Wall	95%	1200€ (TZ670)
Palo Alto Network	95%	2900€ (PA200R)
Cisco	95%	3500€ (Meraki)
Barracuda Networks	90%	2280€ (CloudGend vF100)
Watchguard	90%	2114€ (CN2AE8 XTM1050)
Check Point	90%	2199€ (SG1590 Security)
sospho	90%	2000€ (XG Serie)
StormShield	Niveau militaire	1320€ (SN310)

Tableau Comparatif prix achat pare-feu HT

FG-100E

System Specs	FortiGate 30E	FortiGate 50E	FortiGate 60E	FortiGate 80E	FortiGate 100E
Operating System	FortiOS	FortiOS	FortiOS	FortiOS	FortiOS
Interfaces	4xGE RJ45 Switch Ports, 1xGE RJ45 WAN Port, 1 USB, 1 Console	5xGE RJ45 Switch Ports, 2xGE RJ45 WAN Port, 1 USB, 1 Console	7xGE RJ45 Internal Ports, 2xGE RJ45 WAN Port, 1xDMZ Port, 1 USB, 1 Console	12xGE RJ45 Ports, 2xGE RJ45/SFP Port, 2xGE RJ45 DMZ/HA Ports, 1 USB, 1 Console	14xGE RJ45 Ports, 2xGE RJ45/SFP Port, 2xGE RJ45 WAN Ports, 2xGE RJ45 HA Ports, 1xGE DMZ Port, 1 Management, 1 USB, 1 Console
Firewall Throughput	950 Mbps	2.5 Gbps	3.0 Gbps	4.0 Gbps	7.4 Gbps
IPS Throughput	300 Mbps	350 Mbps	400 Mbps	450 Mbps	500 Mbps
NGFW Throughput	200 Mbps	220 Mbps	250 Mbps	360 Mbps	360 Mbps
Threat Protection Throughput	150 Mbps	160 Mbps	200 Mbps	250 Mbps	250 Mbps
IPSec VPN Throughput	75 Mbps	90 Mbps	2.0 Gbps	2.5 Gbps	4.0 Gbps
SSL VPN Throughput	35 Mbps	100 Mbps	150 Mbps	200 Mbps	250 Mbps
Concurrent Connections (TCP)	90,000	1,300,000	1,300,000	1,300,000	2,000,000
New Connections per Sec (TCP)	15,000	21,000	30,000	30,000	30,000
Max FortiAPs	2 / 2	10 / 5	30 / 10	32 / 16	64 / 32
Max FortiSwitches	8	8	8	8	24
Max FortiTokens	500	500	500	500	5,000
Recommended Max SSL-VPN Users	100	200	200	200	500
Form Factor	Desktop	Desktop	Desktop	Desktop	1U Rack Mountable
Power Supply	External 100–240V AC, 60–50 Hz	External 100–240V AC, 60–50 Hz	External 100–240V AC, 60–50 Hz	External 100–240V AC, 60–50 Hz	External 100–240V AC, 60–50 Hz

Comparatif des différents pares-feux Fortigate

Annexe 4 :

Classement – Prix Annuel / poste	Nom de l'antivirus	Les points forts
1 32 €	Bitdefender total Security	· Meilleur antivirus pour Windows 10. · Assure la sécurité des données · Détecte les virus, Malware, phishing · Protection en temps réel · Bloque les activités indésirables · Avertit l'utilisateur des menaces · Protège les données · Optimise les performances de l'appareil
2 49.99 €	Norton 360 Premium	· Protection en temps réel · Protège des activités indésirables · Protocoles de protections supérieurs à la moyenne · Grand nombre de services de protections
3 34.99 €	Kaspersky Total Security	· Un des meilleurs niveaux de sécurité · Protection et analyse rapide · Gestionnaire de mots de passe · Authentification à 2 facteurs · Grand nombre de services de protection

4 44.99 €	F-Sécure Total	· Simple d'usage · Protège la vie privée · VPN illimité · Bonne efficacité
5 69.95 €	ESET Smart Security Premium	· Technologie de Cryptage des données · 1 licence pour plusieurs utilisateurs multiplateformes (Windows, Linux, MAC, Android…) · Bonne protection des transactions
6 56 €	G-DATA Total sécurity	· Antivirus Léger · Très personnalisable (pour les experts)
7 99.95 €	McAfee Total Protection	· Fonctionnalités complètes · Interface conviviale · Optimisation du système avec la technologie « Cloud-based Thread » · Inclus un bloqueur de publicités
8 99.95 €	Avira Prime	· VPN illimité · Elimine les ransomware · Bonne protection · Garantie les données de comptes bancaires · Protection des e-mails · Réparation des fichiers endommagés

9 69.95	Trend Micro Maximum Sécurity	· 100 % de blocages des échantillons lors d'un test de protection · Protection multi-appareils · Inclus « Folder Shield » pour protéger les fichiers précieux, que ce soit en locale ou sur cloud
10 69.95 €	Malwarebytes Premium	· Meilleur Antimalware · Très rapide · Nettoie le PC rapidement · Garantie la sécurité des fichiers

Comparatif Différents Antivirus

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

Société d'Etude en Service Informatique (SESI)
32 Rue Maran, 31400 Toulouse, France
Référence devis : 442
Emis par : Emilie KILO

SNTS
LAPOUJADE Sylvain
30, avenue de l'Europe
33108 Castillon-La-Bataille
France

Date du devis

Description	Quantité	Prix unitaire HT	Prix total HT
VEEAM Veeam backup et réplication	1	1670,74 €	1670,74 €

Total HT	1670,74 €
TVA (20,00 %)	334,15 €
Total TTC	2 004,89 €

Devis achat VEEAM

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

Société d'Etude en Service Informatique (SESI)
32 Rue Maran, 31400 Toulouse, France
Référence devis : 442
Emis par : Emilie KILO

SNTS
LAPOUJADE Sylvain
30, avenue de l'Europe
33108 Castillon-La-Bataille
France

Date du devis	03/02/2022

Description	Quantité	Prix unitaire HT	Prix total HT
Fortinate FG-100E Pare-feu	2	838,40 €	1676,80 €

Total HT	1676,80 €
TVA (20,00 %)	419,20 €
Total TTC	2096,00 €

Devis achat pares-feux

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

Société d'Etude en Service Informatique (SESI)
32 Rue Maran, 31400 Toulouse, France
Référence devis : 442
Emis par : Emilie KILO

SNTS
LAPOUJADE Sylvain
30, avenue de l'Europe
33108 Castillon-La-Bataille
France

Date du devis

Description	Quantité	Prix unitaire HT	Prix total HT
Server Sauvegarde 2To SSD 48 Go RAM OVH location pour 1 mois	1	1171 €	1171 €

Total HT	1171 €
TVA (20,00 %)	222,49 €
Total TTC	1393,49 €

Devis achat Stockage CLOUD

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

Société d'Etude en Service Informatique (SESI)
32 Rue Maran, 31400 Toulouse, France
Référence devis : 442
Emis par : Emilie KILO

SNTS
LAPOUJADE Sylvain
30, avenue de l'Europe
33108 Castillon-La-Bataille
France

Date du devis

Description	Quantité	Prix unitaire HT	Prix total HT
Eaton 5p 650iR Onduleur rackable	2	357 €	714 €

Total HT	714 €
TVA (20,00 %)	142,80 €
Total TTC	856,80 €

Devis achat Onduleurs

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

Société d'Etude en Service Informatique (SESI)
32 Rue Maran, 31400 Toulouse, France
Référence devis : 442
Emis par : Emilie KILO

SNTS
LAPOUJADE Sylvain
30, avenue de l'Europe
33108 Castillon-La-Bataille
France

Date du devis

Description	Quantité	Prix unitaire HT	Prix total HT
Serveur Dell EMC R340 / 4TB QSAN	1	1287,60 €	1287,60 €

Total HT	1287,60 €
TVA (20,00 %)	257,52 €
Total TTC	1545,12 €

Devis achat Serveur

Compte rendu réunion du 10/09/2021

Participants à la réunion :

ERYANI Farida

FLOTTARD Nicolas

PUJOL Edouard

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Découvrir le nouveau projet CUBES

Définir un Team Leader

Réflexion sur l'infrastructure

Répartitions des tâches

Marco Planning

Compte rendu :

Nous avons pris connaissance du nouveau projet et avons discuté de l'approche global de celui-ci.

À la suite d'un tour de table, Sylvain a été choisi comme Team leader.

Nous avons discuté et échangé autour du projet. Déterminer ce qui est attendu dans chaque partie. Déterminer quelles tâches va être à faire.

Nous avons découpé le sujet en tâches et nous nous les sommes répartis en fonction des compétences et des envies de chacun.

Masterisation via MDT (Nicolas FLOTTARD)

Mises à jour via WSUS (Edouard PUJOL)

Sécurisation du parc :

PCA (en équipe)

PRA (en équipe)

Firewall (Farida ERYANI)

VPN (Farida ERYANI)

Layer de sécurité (en équipe)

Antivirus (Farida ERYANI)

VLAN (Farida ERYANI)

A développer

PowerShell avancé

Création des utilisateur (Sylvain LAPOUJADE)

DFS (Edouard PUJOL)

DFS-R (Edouard PUJOL)

Relation d'approbation (Sylvain LAPOUJADE)

A développer

Centralisation du réseau

PRA salle serveur MAIRIE (en équipe)

Infrastructure à réfléchir et développer en matière de centralisation.

Nous avons prévu des réunions bimensuelles, deux mercredis soir de 19h30 à 20h30 par mois.

MACROPLANNING

Fin octobre Infrastructure Réseau défini

Fin novembre WSUS / DMT

Fin décembre Scripts PW / Sécurisation (Firewall / VPN / Antivirus)

Fin janvier PRA/PCA

Soutenance et rendu projet en février

Prochaines actions

Pour la réunion du 29/09, réflexion sur l'infrastructure réseau, infrastructure serveurs.

Noter toutes les questions et les interrogations que l'on peut avoir.

Compte rendu réunion du 29/09/2021

Participants à la réunion :

ERYANI Farida

FLOTTARD Nicolas

PUJOL Edouard

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Infrastructure réseau

Présentation MDT

Présentation WSUS

Réflexion sur l'antivirus / VPN

Compte rendu :

Nicolas et Edouard nous ont expliquer le fonctionnement du MDT et WSUS, nous avons eu une discussion concernant le choix de ces deux solutions.

Nous avons dressé un inventaire des différentes solution VPN / Firewall que chacun utilise.

Le réseau est défini comme un Lan entre les locaux du SNTS et les écoles comme un boucle. La mairie possédant un rac serveur qui sera utilisé comme sauvegarde pour l'utilisation comme PRA si jamais un plan de reprise d'activité est nécessaire.

Une sauvegarde au SNTS et une autre sauvegarde dans les locaux de la mairie.

Prochaine Réunion le 13/10/2021

Prochaines actions :

Réflexion sur le paramétrage de MDT et WSUS.

Utilisation de PowerShell, dans quel cas et pourquoi ?

Compte rendu réunion du 13/10/2021

Participants à la réunion :

ERYANI Farida

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Deux personnes absentes, bloqué au travail et malade

Réunion décalée au 28/10/2021

Compte rendu :

Prochaine réunion planifiée au 28/10/2021 lorsque tous les membres du groupe seront présents.

Compte rendu réunion du 28/10/2021

Participants à la réunion :

ERYANI Farida

FLOTTARD Nicolas

PUJOL Edouard

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Automatisation POWERSHELL

Installation pare-feu

WDS

Compte rendu :

Compte rendu des scripts POWERSHELL du projet 2 / recherche d'axe d'amélioration pour la gestion d'un AD au fur et à mesure du temps

Pare-feu fortigate, pare-feu intégré au switch, pare-feu physique, VPN en client lourd ? (Paramétrage via GNS3)

WDS procédure installation complète (De la capture à la distribution d'une image golden)

Prochaines actions :

Retravailler les scripts pour les réunir en un, commencer à écrire les scripts de contrôle, regarder comment les automatiser.

Continuer le paramétrage pare-feu, renseignement sur le VPN, matrice de choix

Effectuer des recherches sur le WSUS

Faire une documentation sur le MDT

Date de la prochaine réunion :

Prochaine réunion semaine 47 lors des cours du CESI

Compte rendu réunion du 24/11/2021

Participants à la réunion :

ERYANI Farida

FLOTTARD Nicolas

PUJOL Edouard

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Définition de l'infrastructure

Réunion des documents

Compte rendu :

Nous avons bien défini l'infrastructure que nous souhaitons mettre en place lors de ce projet afin que chacun sache sur quel environnement il travaille.

Nous avons défini de mettre en place un google drive afin que chacun puisse remplir un document comportant ses travaux.

Pour que chacun puisse y avoir accès.

Prochaines actions :

Prochaine réunion début janvier en sortie des fêtes de Noel

Compte rendu réunion du 12/01/2022

Participants à la réunion :

ERYANI Farida

FLOTTARD Nicolas

PUJOL Edouard

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Définition des tâches a priorisé en ce retour de vacances

Point sur les interrogations

Planning

Compte rendu :

Nous avons défini les tâches de fin que nous allons traiter en priorité, notamment en termes de sécurisation de parc pour bien définir ce que nous allons préconiser en fonctions des besoins des écoles et du cahier des charges.

Discussions autour du PCA / PRA.

Mise en place d'un planning avec des deadlines pour terminer la rédaction du projet

Mise en place deadline pour l'envoi final du rendu projet.

Demande de Farida pour avoir une relecture des parties qu'elle a rédigé.

Prochaines actions :

Réunion prévue avec Farida le 19/01/2022

Réunion avec tout le groupe le 31/01/2022

Compte rendu réunion du 19/01/2022

Participants à la réunion :

ERYANI Farida

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Relecture des notes de Farida (VPN / VLAN / PAREFEU / …)

Compte rendu :

Nous avons relu les notes de Farida concernant la sécurité de notre réseau, dans le but d'en extraire les informations les plus importantes et les plus cohérentes à conserver dans notre projet.

Surlignage des éléments principaux

Prochaines actions :

Deuxième réunion de prévu pour relire ce qui aura été modifié grâce à la sélection des éléments principaux.

Compte rendu réunion du 28/01/2022

Participants à la réunion :

ERYANI Farida

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Lecture des parties qui ont été modifié sur les notes de Farida pour donner suite à la réunion du 19/01/2022

Compte rendu :

Relecture des parties rerédiger afin d'enlever des parties techniques et de pouvoir rentrer dans le nombre de pages nécessaires.

Prochaines actions :

Réunion commune avec tout le groupe fin janvier

Compte rendu réunion du 31/01/2022

Participants à la réunion :

ERYANI Farida

FLOTTARD Nicolas

PUJOL Edouard

LAPOUJADE Sylvain

Rubriques à l'ordre du jour :

Préparation de la rédaction du compte rendu Final

Définition des achats à prévoir

Discussion autour du PCA

Préparation des tâches à faire pour la prochaine journée de travail

Compte rendu :

Tout le monde a présenté succinctement le fruit de son travail.

Estimation du nombre de page que chaque partir va prendre, afin de respecter le cahier des charges du rendu final.

Définition des achats matériel à effectuer afin de de préparer des demandes de devis.

(Serveurs de stockages de données / Pare-feu / FAI / Onduleur / Espace CLOUD)

Nous avons échangé autour du PCA que nous allons privilégier, en effet, en se basant sur les aspects sécuritaires que Farida à développer pour notre infrastructure.

Prochaines actions :

Développement du PCA / PRA

Cout de sauvegarde Infra

Mise en commun des travaux pour rédaction du projet final