

LP Réseaux ASR –
2020/2021



Projet Tuteuré

Etudiants : Julien ALBA – Hugo
DE SOUZA – Adel BENZERGA

Tuteur : Jacques ACHARD

FUTURZO



Les réseaux du futur

SOMMAIRE

Préambule	- 4 -
Partie 1 : Phase de préparation et d'audit	- 6 -
1.1) Etat des lieux.....	- 6 -
1.1.1) Audit de l'existant	- 6 -
1.1.2) Aspect Juridique	- 7 -
1.1.3) Aspect Financier	- 7 -
1.1.4) Prise de contact.....	- 8 -
1.2) Acteurs & Partenaires.....	- 8 -
1.3) Expression des besoins	- 8 -
Partie 2 : Phase d'analyse et de réflexion	- 10 -
2.1) Les différentes études	- 10 -
2.1.1) Cahier des charges	- 10 -
2.1.2) Etude juridique	- 10 -
2.1.2.1) RGPD	- 10 -
2.1.2.2) Charte Informatique	- 10 -
2.1.3) Etudes techniques.....	- 10 -
2.1.4) Etude financière	- 11 -
2.2) Les scénarios envisagés	- 11 -
2.2.1) Partie « Déploiement Infrastructures Physiques et logicielles ».....	- 11 -
2.2.1.1) Description de la solution retenue	- 11 -
2.2.1.2) Plan de Sauvegardes.....	- 13 -
2.2.1.3) PRA	- 13 -
2.2.2) Partie « Mise en place de la SSI »	- 13 -
2.2.2.1) Description de la solution retenue	- 14 -
2.2.2.2) Solution Anti-virus.....	- 14 -
2.2.2.3) Station Blanche.....	- 15 -
Partie 3 : Déploiement des solutions choisies	- 17 -
3.1) Planning de déploiement	- 17 -
3.2) Matrice des flux.....	- 17 -
3.3) Personnels & Main d'œuvre.....	- 17 -
3.4) Architecture & Topologie	- 17 -
3.5) Déploiement des solutions	- 18 -

3.3.1) Routeur	- 18 -
3.3.1.1) Agrégation des liens	- 19 -
3.3.1.2) Routage et pare-feu	- 20 -
3.3.1.3) Relais DHCP	- 23 -
3.3.1.4) Proxy	- 24 -
3.3.1.5) Filtrage Accès Web	- 26 -
3.3.1.6) VPN	- 28 -
3.3.1.7) Wi-Fi.....	- 29 -
3.3.2) Switchs	- 29 -
3.3.2.1) VLANs.....	- 29 -
3.3.2.2) Configuration physique des commutateurs	- 29 -
3.3.2.2.1) Configuration générique des switchs.....	- 30 -
3.3.2.2.2) Switch 1 : RDC	- 32 -
3.3.2.2.3) Switch 2 : 1 ^{er} étage	- 33 -
3.3.2.2.4) Switch 3 : 2 ^{ème} étage	- 35 -
3.3.3) Serveurs	- 36 -
3.3.3.1) Physique	- 36 -
3.3.3.1.1) Contrôleur de Domaine	- 36 -
3.3.3.1.1.1) Hyper-V.....	- 37 -
3.3.3.1.1.2) DNS	- 38 -
3.3.3.1.1.3) DHCP	- 38 -
3.3.3.1.1.4) AD DS.....	- 40 -
3.3.3.1.1.5) DFS	- 41 -
3.3.3.1.1.6) GPO	- 41 -
3.3.3.1.1.7) Sauvegarde distante.....	- 42 -
3.3.3.1.2) Recyclage de l'ancien serveur pour configuration en NAS	- 42 -
3.3.3.2) Virtuels	- 46 -
3.3.3.2.1) Serveur de Supervision.....	- 46 -
3.3.3.2.2) Serveur de Mails	- 50 -
3.3.3.2.3) Serveur Applications Métiers	- 51 -
3.3.3.2.4) Serveur Web	- 51 -
3.3.3.2.5) Serveur Anti-Virus.....	- 53 -
3.3.4) Machines	- 56 -
3.3.4.1) Client	- 56 -
3.3.4.2) Station Blanche.....	- 56 -

Partie 4 : Mise en place du contexte de Sécurité	- 57 -
4.1) Protection pro-active	- 57 -
4.1.1) Formation à la CYBERDEFENSE	- 57 -
4.1.2) Fiches-réflexes	- 57 -
4.3.3) Mémento Utilisateur	- 57 -
4.3.1) Sensibilisation à la CYBERDEFENSE.....	- 57 -
4.2) Protection Active du Réseau et des Systèmes.....	- 58 -
4.2.1) Solution Anti-virus.....	- 58 -
4.2.2) Station Blanche	- 58 -
Partie 5 : Suivi de la mise en production	- 59 -
5.1) Livraison du produit final	- 59 -
5.2) Retour d'expérience	- 59 -
Annexes	- 60 -

Préambule

Dans le cadre de de la licence professionnelle métiers des réseaux informatiques et télécommunications parcours administration et sécurité des réseaux, nous avons été amenés à réaliser un projet tuteuré.

Dans ce projet, il a fallu et apporter la réponse à un besoin spécifique émis par la mairie de Signes dont le responsable informatique est M. ACHARD Jacques.

Sujet 1 :

La mairie de Signes vient de changer son serveur passant d'un Windows server 2003 à un Windows server 2019.

Elle veut profiter de cette occasion pour remettre en bon état de fonctionnement son réseau et essayer d'apporter un peu de rigueur dans son infrastructure.

Elle veut le faire sans réaliser des investissements importants et en utilisant au maximum les équipements existants.

Elle veut en profiter pour :

- Activer le WIFI avec deux types d'accès :
 - Un accès permettant juste d'utilisation la connexion internet
 - Un accès permettant d'accéder au réseau local et à tous ses périphériques.

L'identification se fera en se basant sur les comptes AD existants.

- Permettre à un intervenant extérieur d'utiliser le réseau pour se connecter au Web et utiliser uniquement les imprimantes réseaux existantes. Aucun accès aux autres ressources du réseau n'étant permis. (Attention log des utilisations)
- Permettre un accès distant (Covid et télétravail obligeant) aux ressources locales
- Disposant de deux accès internet (VDSL / SDL) elle souhaite les agréger via son routeur.
- Utiliser l'ancien serveur pour en faire une unité de sauvegarde en sus de celle existante.
- Elle veut aussi bloquer/filtrer les accès sur les réseaux sociaux / youtube / Sauf pour des postes qui seront pleinement identifiés (Communication par exemple, administrateur aussi,...)
- Mettre en place un logiciel de messagerie, afin de gérer les mails de ses collaborateurs.

Sujet 3 :

La mairie de Signes a également exprimé d'autres souhaits, notamment vis-à-vis de la sécurisation des installations, la sensibilisation du personnel, des phases de sauvegardes et de PRA.

Une demande concernant une démarche pro-active a été formulée ainsi que des solutions à mettre en œuvre dans le cas où la protection s'est avérée inefficace.

Les solutions seront à appliquer aussi bien sur le serveur que sur les postes clients. La protection portera sur les accès internet, la gestion de mails, le filtrage internet, accès physique aux postes.

Pour répondre à ce besoin, nous avons décidé de nous mettre en situation en imaginant nous même une entreprise et en lui donnant un nom. C'est pourquoi nous avons utilisé le nom "FUTURZO, les réseaux du futur" car les solutions apportées seront en lien avec les futures compétences que nous acquérerons lors de notre parcours professionnel.

Pour mener à bien ce projet nous avons décidé d'adopter une démarche professionnelle en tant que l'entreprise FUTURZO au sein de laquelle chaque membre de notre équipe a tenu un rôle bien précis.

Nous avons donc effectué un audit au préalable afin de pouvoir proposer une solution adaptée qui réponde au mieux au cahier des charges de la mairie de Signes.

Le résultat de cette étude nous a permis de scinder notre travail en 5 parties :
Audit – Analyse – Déploiement – Contexte de sécurité – Suivi de la production

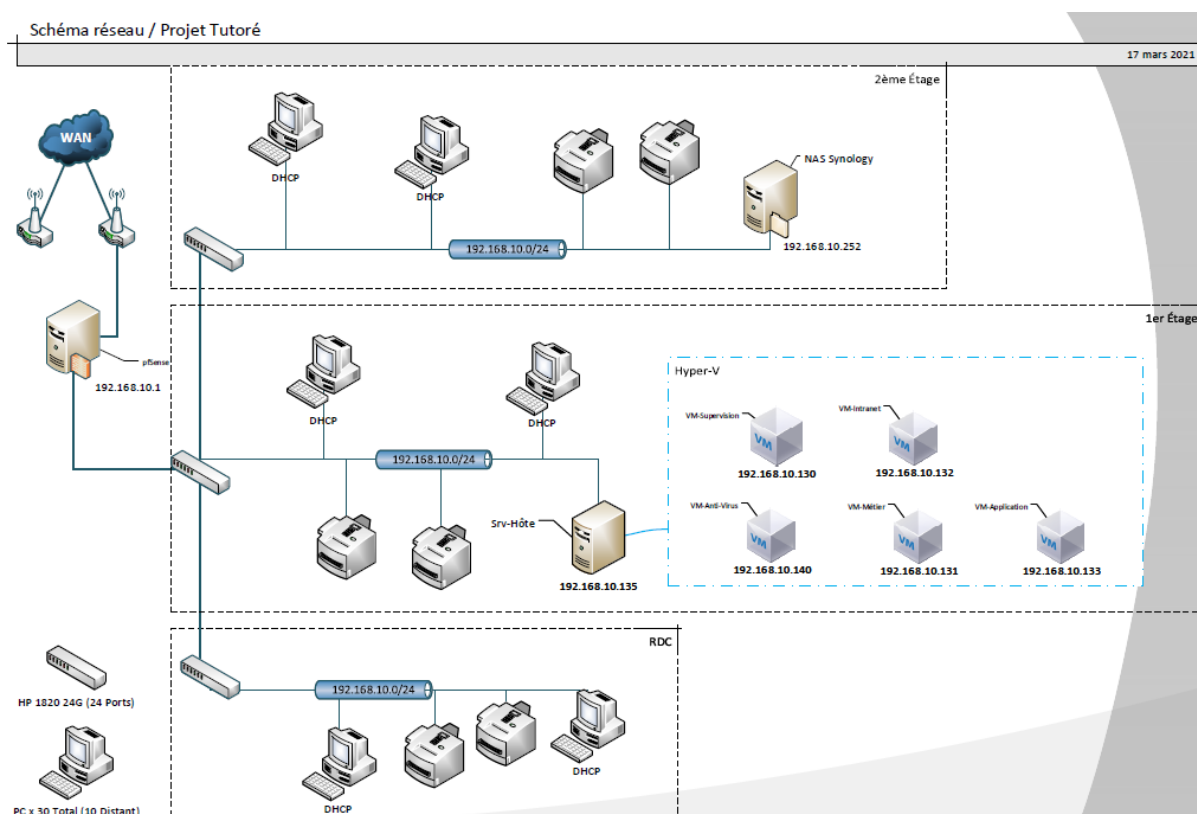
Partie 1 : Phase de préparation et d'audit

1.1) Etat des lieux

L'état des lieux dressé à ce jour reflète une architecture et une configuration non-optimisée et fait l'objet de 2 questionnaires réalisés préalablement dans le but d'avoir le maximum d'informations.

1.1.1) Audit de l'existant

L'architecture existante se présente comme suit :



Architecture Logique :

Plage d'adresses IP utilisée : 192.168.10.0/24

Matériel :

- 3 switch HP 1820 24G - .20 / .21 / .22
- 1 Routeur Pfsense Provya - .1
- 6 Imprimantes/Copieur - IP - .200 / .201 / .203 / .204
- 1 LIVEBOX PRO VDSL
- 1 LIVEBOX SDSL - 16 MG
- PC Clients en ip dynamique
- Serveurs

- **SRV Windows 2019 - .135**
- **SRV Application - .133**
- **SRV Métiers - .135**
- **ANTIVIRUS - .140**
- **SUPERVISION - .130**
- **INTRANET - .132**
- **NAS Synology – .150**

De plus, après un entretien avec le responsable informatique de la mairie de Signes, différentes informations nous ont été communiquées par à savoir :

- Pas de VLAN existants sur les switchs
- Port mirroring sur certains ports
- Sauvegardes = environ 250Go
- Tous les postes peuvent imprimer sur toutes les imprimantes
- Pas de quotas au niveau du partage de fichiers
- Filtrage des images pornos à faire mais pas au niveau de la liste blanche
- Pas de sécurité physique des locaux (Serveur accessible par n'importe qui)
- Pas de sécurité des équipements (pas de bloqueurs USB/RJ45, tout est ouvert)

1.1.2) Aspect Juridique

Les déclarations des différents SI employés au sein de la Mairie de Signes ont été déclarés à la CNIL. Les licences systèmes et logiciels sont en règle.

La Mairie de Signes n'a pas d'assurance cyber-risque (perte de données et/ou d'exploitation).

La Mairie de Signes n'a pas mis en place de charte informatique ni de RGPD, ce qui fera l'objet d'une étude ultérieure dans ce document.

1.1.3) Aspect Financier

Après discussion avec le responsable informatique de la Mairie de Signes, il se trouve que cette dernière souhaite ré-utiliser au maximum les équipements qu'elle possède déjà.

Il n'y aura donc pas de budget prévu pour un éventuel investissement en termes de matériel informatique réseau.

Les prestations resteront cependant facturées et feront l'objet d'une étude financière ultérieure.

1.1.4) Prise de contact

Lors de cette étape, nous prenons contact avec la mairie de Signes afin de mettre en place les rendez-vous préparatoires à la rédaction du cahier des charges avec le responsable des réseaux & télécommunications ainsi que de l'informatique de la Mairie de Signes.

1.2) Acteurs & Partenaires

Le client :

- Cabinet du Maire (validation du projet) ;
- Direction informatique et télécommunications d'information (validation technique) ;
- Service juridique (validation charte informatique et RGPD) ;
- Responsable informatique de la Mairie (audit – suivi du déploiement)

Prestataires externes :

- Nous-mêmes, « FUTURZO », entreprise d'expertise réseau, intégration de solutions matérielles et logicielles, conseils et formations ainsi que Cyberdéfense.

1.3) Expression des besoins

Concernant les besoins du sujet 1, la Mairie de Signes souhaite donc :

- Activer le WIFI avec deux types d'accès :
 - Un accès permettant juste d'utilisation la connexion internet
 - Un accès permettant d'accéder au réseau local et à tous ses périphériques.

L'identification se fera en se basant sur les comptes AD existants.

- Permettre à un intervenant extérieur d'utiliser le réseau pour se connecter au Web et utiliser uniquement les imprimantes réseaux existantes.

Aucun accès aux autres ressources du réseau n'étant permis.

- Permettre un accès distant (Covid et télétravail obligent) aux ressources locales

- Disposant de deux accès internet (VDSL / SDL) elle souhaite les agréger via son routeur.

- Utiliser l'ancien serveur pour en faire une unité de sauvegarde en sus de celle existante.

- Elle veut aussi bloquer/filtrer les accès sur les réseaux sociaux / youtube / sauf pour des postes qui seront pleinement identifiés (Communication par exemple, administrateur aussi,....)

- Mettre en place un logiciel de messagerie, afin de gérer les mails de ses collaborateurs.

Les besoins du sujet 3 concerneront entre autres :

- Sécuriser les installations.
- Sensibiliser le personnel.
- Effectuer des sauvegardes des installations et des systèmes.
- Mettre en place un PRA.

De plus, une démarche pro-active sera donc adoptée plus loin dans le détail concernant le sujet 3.

Partie 2 : Phase d'analyse et de réflexion

2.1) Les différentes études

2.1.1) Cahier des charges

La Commune de Signes ayant une demande particulière sans forcément avoir les compétences en interne d'analyse suffisante, le cahier des charges a été réalisé par notre société en prenant provisoirement la place du client.

2.1.2) Etude juridique

2.1.2.1) RGPD

La société informatique FUTURZO a réalisé une charte RGPD et l'a proposé au responsable informatique de la mairie de Signes

La charte RGPD est disponible en **annexe 1**.

2.1.2.2) Procédure d'utilisation du logiciel VeraCrypt

La société informatique a réalisé une procédure d'installation et d'exploitation du logiciel VeraCrypt (logiciel de chiffrement de disque et données) et l'a proposé au responsable informatique de la mairie de Signes.

La Procédure d'exploitation de VeraCrypt est disponible en **annexe 2**.

2.1.3) Etudes techniques

Notre proposition va s'orienter sur les solutions suivantes :

- Test et Mise en place d'une solution routeur/pare-feu ;
- Test et Mise en place d'une architecture de 3 switchs composés de plusieurs VLANs ;
- Test et mise en place du serveur Windows 2019 et des machines virtuelles qui composent la structure de la mairie de Signes ;
- Proposition d'un plan de formation et de sensibilisation des utilisateurs ;
- Proposition d'un plan de désinfection et d'un complément pour le plan de reprise d'activité ;
- Modification plan d'adressage IP ;
- Modification configuration du serveur de domaine.

Après étude du cahier des charges et de l'audit, un certain nombre de points n'entrant pas dans le cadre du projet seront portés à l'attention du client afin de dégager la responsabilité de la société FUTURZO.

Deux audits ont donc été réalisés afin de connaître les attentes et les besoins concernant les travaux à faire et sont disponibles en **annexes 3 et 4** :

- [Annexe 3 – Audit Sujet 1](#)
- [Annexe 4 – Audit Sujet 3](#)

2.1.4) Etude financière

L'ensemble des éléments financiers, devis et réponse financière au format du cahier des charges sont disponibles en [annexe 5](#).

2.2) Les scénarios envisagés

2.2.1) Partie « Déploiement Infrastructures Physiques et logicielles »

En tant que société d'expertise réseaux et de conseil, nous avons proposé au responsable informatique plusieurs scénarios :

- Proposition d'une architecture déployée par nos soins avec remplacement de matériel (routeur notamment),
- Proposition d'une architecture réutilisant les moyens et les équipements déjà présents.

2.2.1.1) Description de la solution retenue

A l'issue de l'entretien préliminaire avec le responsable informatique de la mairie de Signes, nous avons pu faire le point par rapport à tout ce qui relevait des contraintes (techniques, financières, organisationnelles).

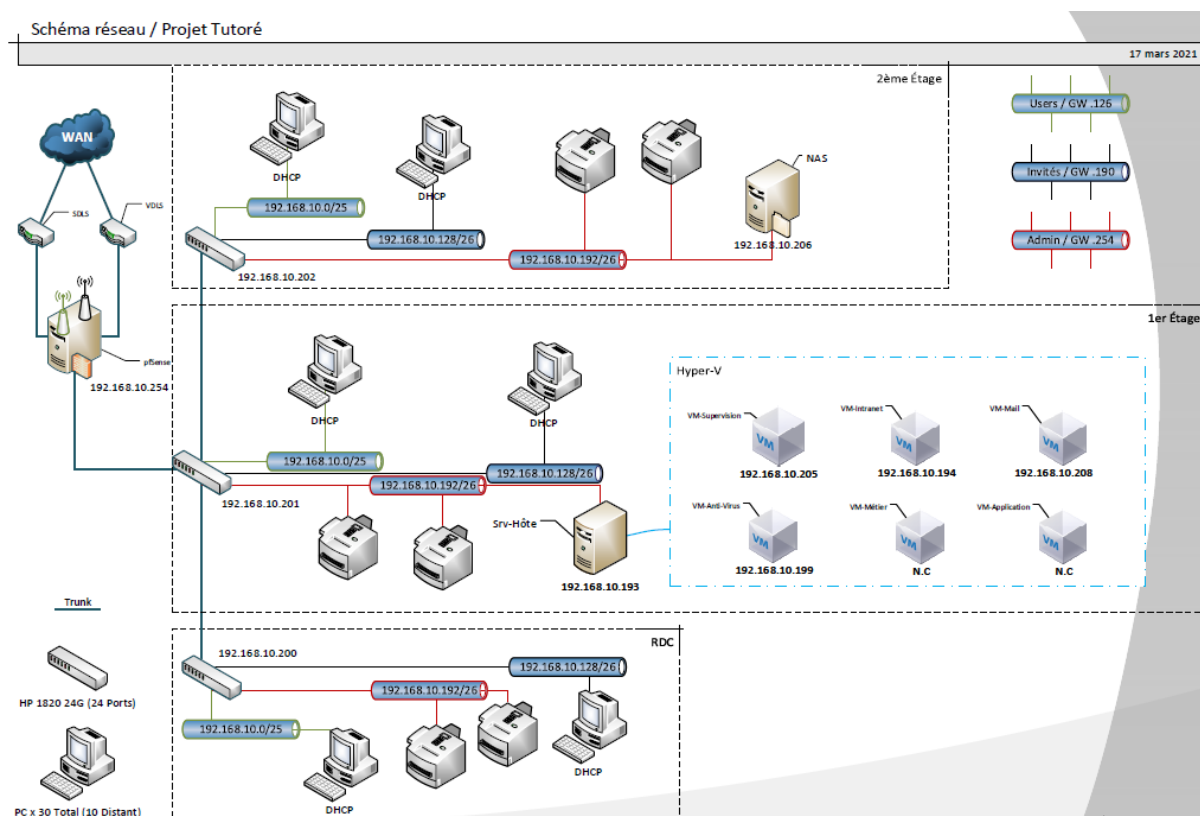
Il apparaît que, suite à un souhait de la Mairie de Signes de ne pas investir dans du matériel neuf, la solution la plus adaptée a été de réutiliser les équipements déjà présents.

Découpage logique/Segmentation :

Nous avons donc choisi de procéder comme suite de manière à pouvoir implémenter une sécurité supplémentaire (sous-réseaux) :

- Sous-réseau **« Utilisateurs »** : 192.168.10.0/25 = 128 emplacements (dédiés aux utilisateurs principaux)
- Sous-réseau **« Invités »** : 192.168.10.128/26 = 64 emplacements disponibles pour les « invités »
- Sous-réseau **« Equipements »** : 192.168.10.192/26 = 64 équipements (EAR : switch – routeur – box – proxy..)

Voici **l'architecture finale** que nous avons proposé au responsable informatique :



Concernant les besoins exprimés par la mairie de Signes, nous avons dressé un tableau exhaustif avec proposition de solutions :

<u>Tâche à réaliser</u>	<u>Solution apportée</u>
<u>Réutilisation de l'ancien serveur pour unité de sauvegarde supplémentaire</u>	Déploiement d'un serveur TRUENAS pour Backup du serveur Windows 2019
<u>Réutiliser le routeur PFSense</u>	Utilisation d'une machine dédiée pour le rôle de Routeur / Proxy / Pare-feu PFSense
<u>Agrégation des 2 liens VDSL/SDL</u>	Réalisation via PFSense
<u>Créer des accès "invité" pour les intervenants extérieurs</u>	Segmentation du réseau & Création d'un VLAN dédié

<u>Blocage/Filtrage des accès sur les réseaux sociaux (sauf postes identifiés)</u>	Configuration du DNS sur le routeur PFSense Identification des machines à autoriser
<u>Activer le WIFI avec deux types d'accès :</u> - Accès Internet - Accès ressources locales + périphériques	Segmentation du réseau Implémentation LDAP du domaine avec Wifi pour authentification
<u>Permettre un accès distant aux ressources locales</u>	Utilisation d'OpenVPN (environ 10 utilisateurs)
<u>Mise en place d'un logiciel de messagerie (gestion des mails interne)</u>	Déploiement d'un serveur de mails SOGO avec SSL

2.2.1.2) Plan de Sauvegardes

La société informatique FUTURZO a réalisé un plan de sauvegardes et l'a proposé au responsable informatique de la mairie de Signes.

Le plan de sauvegardes est disponible en **annexe 6.**

2.2.1.3) PRA

La société informatique FUTURZO a réalisé une Plan de Reprise d'activité et l'a proposé au responsable informatique de la mairie de Signes.

Le plan de Reprise d'Activité est disponible en **annexe 7.**

2.2.2) Partie « Mise en place de la SSI »

L'expertise réseaux étant notre domaine principal, nous n'en sommes pas moins doué concernant le panel de compétences appétent à la Cyberdéfense, nous avons proposé au responsable informatique plusieurs scénarios :

- Proposition de mise en place d'une solution Anti-virus payante, et d'une station blanche payante également (KUB),
- Proposition d'une solution réutilisant les moyens déjà déployés ainsi que des solutions open source.

2.2.1.1) Description de la solution retenue

Après avoir recensé les besoins concernant le sujet 3 dans l'audit préliminaire, nous avons pu tomber d'accord avec le responsable informatique de la mairie de Signes concernant la solution Anti-virus à déployer.

Le reste des tâches étant de notre ressort, nous avons donc pu dresser un tableau de réponses aux besoins exprimés

<u>Tâche à réaliser</u>	<u>Solution apportée</u>
<u>Mise en place d'un PRA</u>	Inexistant - à créer
<u>Mise en place d'une charte informatique</u>	Inexistante - à créer
<u>Solutions anti-virus</u>	Déploiement d'une appliance BitDefender GravityZone
<u>Mise en place d'un contexte SSI</u>	Station blanche pour "SAS" des supports USB
<u>Sensibilisation des utilisateurs</u>	Création d'un panel d'affiches, mesures SSI sensibilization et formation

2.2.2.2) Solution Anti-virus

Projet de solution anti-virus complète : BitDefender GravityZone



Cette solution étant déjà utilisée dans notre entreprise, nous avons donc pris l'initiative de la proposer en détaillant les avantages dans un schéma récapitulatif :



Les multiples raisons citées ci-dessus ont donc joué un rôle prépondérant d'aide à la décision pour le responsable informatique de la mairie de Signes.

Panel des fonctionnalités et rôles :



2.2.2.3) Station Blanche

Projet Station Blanche : GitHub (Open Source)

La configuration de la solution est paramétrable selon la politique de sécurité de la mairie

Elle s'implémente facilement dans un périmètre défini et améliore la sécurisation et la protection des sites.



Elle permet en outre, la sensibilisation et la communication auprès des collaborateurs et prestataires en utilisant l'écran de la station blanche.

De ce fait il peut être utilisé pour faire passer des messages, attirer l'attention et informer sur le domaine de la cybersécurité.

Partie 3 : Déploiement des solutions choisies

3.1) Planning de déploiement

La société informatique a réalisé un planning de déploiement en adéquation avec les disponibilités de la mairie de Signes et l'a proposé au responsable informatique de la mairie de Signes.

Le planning de déploiement est disponible en annexe 8.

3.2) Matrice des flux

Afin de pouvoir garantir la sécurisation des communications et surtout d'éclaircir le responsable informatique dans la gestion des flux entrants/sortants, la société FUTURZO a mis en place une matrice des flux.

Elle permettra au responsable informatique de :

- Mesurer le volume de trafic
- Suivre les performances de ses flux
- Superviser la sécurité du système.

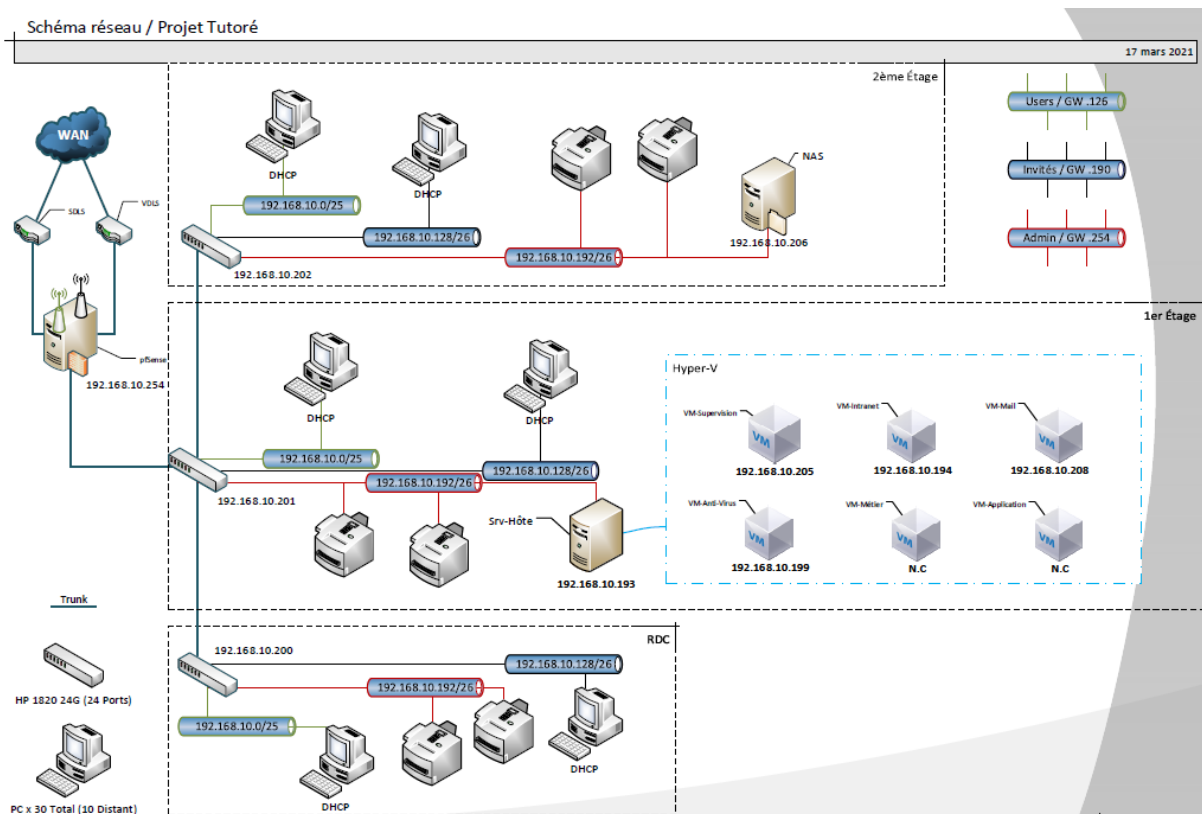
<u>Matrice des flux</u>				
<u>Source</u>	<u>Flux</u>	<u>Destination</u>	<u>Action</u>	<u>Log</u>
<u>LAN</u>	HTTP/HTTPS	WAN	Permit	Oui
<u>LAN</u>	SMTP/POP/IMAP	WAN	Permit	Oui
<u>LAN</u>	Serveur Anti-Virus BitDefender	WAN	Permit	Non
<u>LAN</u>	VPN	WAN	Permit	Non
<u>LAN</u>	Applications métier	WAN	Permit	Oui
<u>WAN</u>	HTTP/HTTPS	LAN	Permit	Oui
<u>WAN</u>	SMTP/POP/IMAP	LAN	Permit	Oui
<u>WAN</u>	Serveur Anti-Virus BitDefender	LAN	Permit	Non
<u>WAN</u>	Applications métier	LAN	Permit	Oui
<u>WAN</u>	VPN	LAN	Permit	Non

3.3) Personnels & Main d'œuvre

Les experts réseaux mandatés pour les travaux globaux sont M. ALBA Julien et M. DE SOUZA Hugo, tous deux diplômés d'une licence en Réseaux & Télécommunications – spécialité Administration Réseaux et Sécurité.

3.4) Architecture & Topologie

En adéquation avec les besoins formulés par le responsable informatique de la mairie de Signes, la topologie mise en œuvre, citée précédemment :



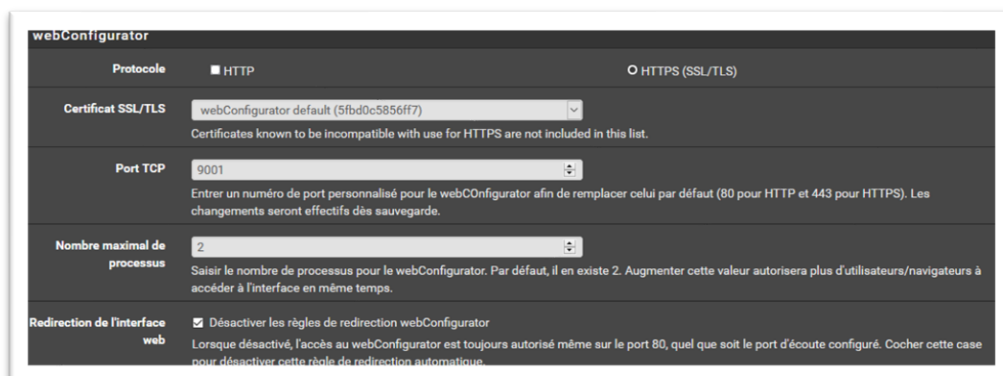
Pour mieux appréhender le fonctionnement du réseau malgré un déploiement physique qui reste assez simple mais dont la configuration repose sur des équipements anciens, la société d'expertise Réseaux FUTURZO a mis en place un schéma sur Cisco Packet Tracer permettant d'en constater le fonctionnement.

La maquette de la topologie Réseaux/systèmes de la mairie de Signes est disponible en [annexe 9](#). (à ouvrir avec [cisco Packet Tracer](#))

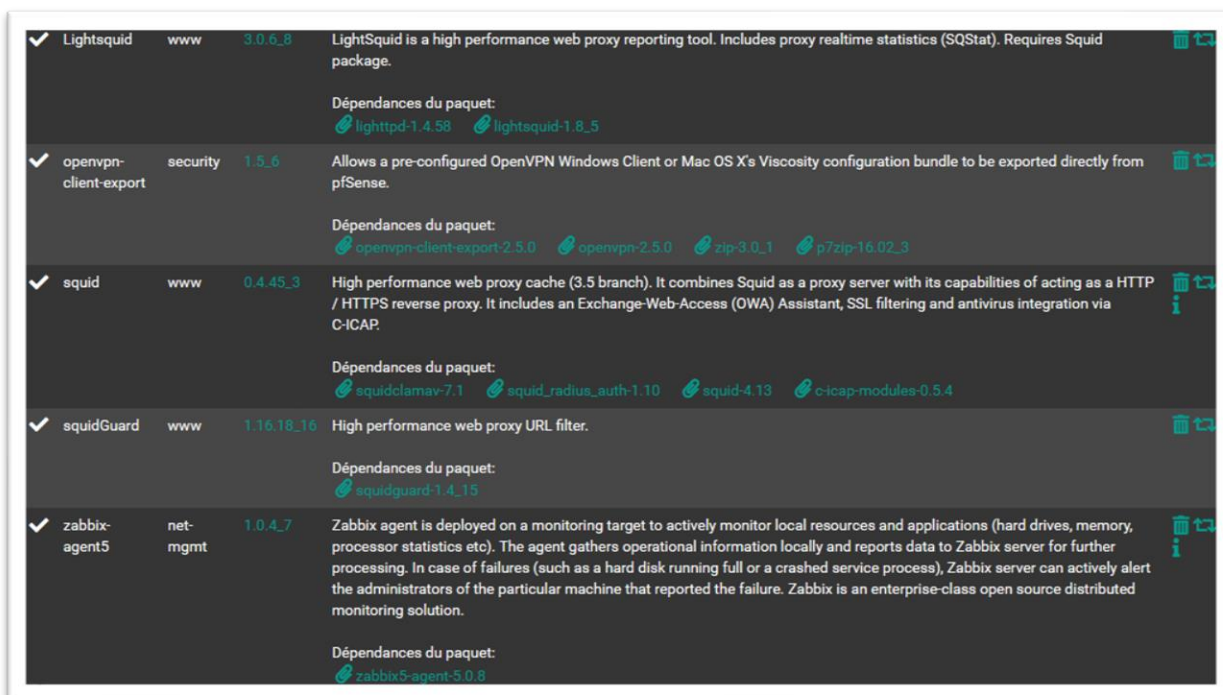
3.5) Déploiement des solutions

3.3.1) Routeur

La reconfiguration du routeur pfSense existant commence par la sécurisation de son accès web, désactivation du protocole HTTP et changement du port HTTPS par défaut en tant que pratique d'hygiène numérique conforme au RGPD et à la charte informatique de la mairie de Signes.



Un certain nombre de packages seront nécessaires à la configuration du routeur notamment Squid qui sera notre serveur proxy et openvpn_export qui nous permettra de fournir un utilitaire de connexion au VPN pour les utilisateurs.



3.3.1.1) Agrégation des liens

La mairie disposant de deux connexions internet souhaite donc réaliser une agrégation de liens afin d'augmenter son débit et de disposer d'une redondance.

Dans un premier temps la configuration des deux interfaces WAN représentant les deux accès internet avec une adresse IP surveillée internet (ici les DNS Google) différentes pour chacune afin de surveiller l'accès web des passerelles.



La création d'un groupe de passerelle avec les deux interfaces configurées ci-dessus toutes deux en « **Niveau 1** » ce qui permet une répartition 50/50 du trafic sur les interfaces.

Le seuil de déclenchement est défini sur « **Membre tombé** », c'est-à-dire si l'une des interfaces ne dispose plus d'Internet ou est déconnectée tout le trafic sera redirigé vers la seconde.

Système / Routage / Groupes de passerelle / Modifier

Modifier l'entrée de groupe de passerelle

Nom de groupe: SDSL_VDSL

Priorité de passerelle

Passerelle	Niveau	Adresse de l'interface	Interface
WAN_DHCP	Niveau 1	Adresse de l'interface	Interface WAN_DHCP Gateway
WAN2_DHCP	Niveau 1	Adresse de l'interface	Interface WAN2_DHCP Gateway

Priorité de liaison: The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.

adresse IP virtuelle: The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.

Seuil de déclenchement: Membre tombé
Quand déclencher l'exclusion d'un membre

Description: Agrégation WAN
Une description peut être saisie ici à des fins de référence administrative (non analysée).

3.3.1.2) Routage et pare-feu

L'idée initiale pour le routage était d'utiliser un des switches de niveau 3 pour effectuer le routage inter-Vlan, mais en nous heurtant à de nombreux problèmes lors de la configuration et des tests notamment avec les ACL nous avons décidé d'utiliser le routeur pfSense a la place.

La configuration commence par la définition des interfaces de VLAN avec leurs tags respectif.





Interfaces / VLANs

Assignations des interfaces Groupes d'interface Sans-fil **VLANs** QinQs PPPs GREs GIFs Ponts LAGGs








Interfaces de réseau local virtuel (« VLAN »)

Interface	Balise VLAN	Priorité	Description	Actions
em1 (lan)	100		VLAN 100 Utilisateurs	
em1 (lan)	200		VLAN 200 Invite	
em1 (lan)	400		VLAN 400 Admin	

Des interfaces « **Ponts** » sont créées pour le VLAN100 et 200 (Utilisateurs et Invités), elles permettent de relier plusieurs interfaces en une et elles seront utiles par la suite lors de la configuration VPN et Wi-Fi.

















Interfaces / Ponts			
Assignations des interfaces	Groupes d'interface	Sans-fil	VLANs
QinQs	PPPs	GREs	GIFs
Ponts	LAGGs		
Interfaces pont			
Interface	Membres	Description	Actions
BRIDGE0	VLAN100, VPN_USER, WIFIUSERS	VLAN100_Bridge	 
BRIDGE1	VLAN200, WIFIINVITES	VLAN200_Bridge	 

Les adresses IP peuvent maintenant être attribuées aux interfaces « **BRIDGEUSERS** », « **BRIDGEINVITES** » et « VLAN400 » en concordance avec le plan d'adressage.

Interfaces				
 WAN	↑	1000baseT <full-duplex>		192.168.84.30
 VLAN400	↑	1000baseT <full-duplex>		192.168.10.254
 WAN2	↑	1000baseT <full-duplex>		192.168.84.142
 WIFIUSERS	running	autoselect mode 11ng <hostap>		n/a
 WIFIINVITES	running	autoselect mode 11ng <hostap>		n/a
 BRIDGEUSERS	↑			192.168.10.126
 BRIDGEINVITES	↑			192.168.10.190

Configuration des règles de pare-feu pour les utilisateurs :

Le protocole HTTPS est bloqué afin de forcer l'utilisation du proxy.

Pare-feu / Règles / BRIDGEUSERS										
Flottant(e)	WAN	VLAN400	WAN2	VLAN100	VLAN200	VPN_USER	WIFIUSERS	WIFIINVITES	BRIDGEUSERS	
BRIDGEINVITES	OpenVPN									
Règles (Faire glisser pour changer l'ordre)										
	États	Protocole	Source	Port	Destination	Port	File Passerelle d'attente	Ordonnancement	Description	Actions
-> Proxy										
	✓ 27 / 8.78 MB	IPv4 TCP	*	*	Ce pare- feu	*	*	aucun		  
Proxy obligatoire pour HTTP/HTTPS										
	✗ 0 / 13 KIB	IPv4 TCP	BRIDGEUSERS net	*	*	443 (HTTPS)	*	aucun	Bridge_Bypass_Block_HTTPS	  
	✗ 0 / 1 KIB	IPv4 TCP	BRIDGEUSERS net	*	*	80 (HTTP)	*	aucun	Proxy_Bypass_Block	  
Allow										
	✓ 3 / 50.42 MB	IPv4 *	BRIDGEUSERS net	*	*	*	*	aucun		  

Configuration des règles de pare-feu pour les invités :

Autorisation du DNS, Proxy et des imprimantes, blocage du trafic à destination des serveurs et utilisateurs.

Pare-feu / Règles / BRIDGEINVITES										
Flottant(e) WAN VLAN400 WAN2 VLAN100 VLAN200 VPN_USER WIFIUSERS WIFIINVITES BRIDGEUSERS										
BRIDGEINVITES OpenVPN										
Règles (Faire glisser pour changer l'ordre)										
	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description Actions
DNS + HTTP/S Proxy										
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 UDP	BRIDGEINVITES net	*	192.168.10.193	53 (DNS)	*	aucun	
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	BRIDGEINVITES net	*	192.168.10.254	3128	*	aucun	Proxy
Imprimantes										
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.120	*	*	aucun	
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.121	*	*	aucun	
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.122	*	*	aucun	
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.123	*	*	aucun	
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.124	*	*	aucun	
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.125	*	*	aucun	
Block										
<input checked="" type="checkbox"/>	✗	0 / 0 B	IPv4 TCP	BRIDGEINVITES net	*	*	80 (HTTP)	*	aucun	
<input checked="" type="checkbox"/>	✗	0 / 0 B	IPv4 TCP	BRIDGEINVITES net	*	*	443 (HTTPS)	*	aucun	
<input checked="" type="checkbox"/>	✗	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	VLAN400 net	*	*	aucun	
<input checked="" type="checkbox"/>	✗	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	BRIDGEUSERS net	*	*	aucun	
Allow										
<input checked="" type="checkbox"/>	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	*	*	*	aucun	

Concernant le routage, aucune règle particulière n'est à créer étant donné que tous les réseaux sont directement connectés au routeur. Le trafic sortant sera géré automatiquement par pfSense avec du NAT automatique.

Pare-feu / NAT / Sortant

Transfert de port 1:1 Sortant NAT

Mode NAT sortant

Mode

- Création automatique de règles NAT sortantes. (IPsec passthrough inclu)
- Création hybride de règles NAT sortantes. (NAT sortant automatique + règles ci-dessous)
- Création manuelle de règles NAT sortantes. (NSA - NAT sortant avancée)
- Désactiver la création de règles NAT sortantes. (Aucune règle NAT sortant)

Enregistrer

Mappages

Interface	Source	Port source	Destination	Port destination	Adresse NAT	Port NAT	Port statique	Description	Actions																																													
<p>Règles automatiques :</p> <table border="1"> <thead> <tr> <th>Interface</th> <th>Source</th> <th>Port source</th> <th>Destination</th> <th>Port destination</th> <th>Adresse NAT</th> <th>Port NAT</th> <th>Port statique</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>✓ WAN</td> <td>127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25</td> <td>*</td> <td>*</td> <td>500</td> <td>WAN address</td> <td>*</td> <td>✓</td> <td>Règle auto-générée pour ISAKMP</td> </tr> <tr> <td>✓ WAN</td> <td>127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25</td> <td>*</td> <td>*</td> <td>*</td> <td>WAN address</td> <td>*</td> <td>✗</td> <td>Règle créée automatiquement</td> </tr> <tr> <td>✓ WAN2</td> <td>127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25</td> <td>*</td> <td>*</td> <td>500</td> <td>WAN2 address</td> <td>*</td> <td>✓</td> <td>Règle auto-générée pour ISAKMP</td> </tr> <tr> <td>✓ WAN2</td> <td>127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25</td> <td>*</td> <td>*</td> <td>*</td> <td>WAN2 address</td> <td>*</td> <td>✗</td> <td>Règle créée automatiquement</td> </tr> </tbody> </table>										Interface	Source	Port source	Destination	Port destination	Adresse NAT	Port NAT	Port statique	Description	✓ WAN	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	500	WAN address	*	✓	Règle auto-générée pour ISAKMP	✓ WAN	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	*	WAN address	*	✗	Règle créée automatiquement	✓ WAN2	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	500	WAN2 address	*	✓	Règle auto-générée pour ISAKMP	✓ WAN2	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	*	WAN2 address	*	✗	Règle créée automatiquement
Interface	Source	Port source	Destination	Port destination	Adresse NAT	Port NAT	Port statique	Description																																														
✓ WAN	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	500	WAN address	*	✓	Règle auto-générée pour ISAKMP																																														
✓ WAN	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	*	WAN address	*	✗	Règle créée automatiquement																																														
✓ WAN2	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	500	WAN2 address	*	✓	Règle auto-générée pour ISAKMP																																														
✓ WAN2	127.0.0.0/8 :: 1/128 192.168.10.192/26 192.168.10.0/25	*	*	*	WAN2 address	*	✗	Règle créée automatiquement																																														

3.3.1.3) Relais DHCP

Le cloisonnement des réseaux nous impose de mettre en place un relais DHCP afin de distribuer des adresses IP approprié sur l'ensemble de l'infrastructure.

Services / Relais DHCP

Configuration de relais DHCP

Activer ☒ Activer le relais DHCP sur l'interface

Interface(s) VLAN400 WAN2 BRIDGEUSERS BRIDGEINVITES

Les interfaces sans adresse IP ne seront pas affichées.

☐ Ajouter l'ID du circuit et l'ID de l'agent aux requêtes
Si cette option est activée, le relais DHCP ajoutera le circuit ID (pfSense numéro de l'interface) et l'ID de l'agent à la requête DHCP.

Serveur de destination 192.168.10.193

Il s'agit de l'adresse IPv4 du serveur auquel les requêtes DHCP sont relayées.

3.3.1.4) Proxy

Comme indiqué précédemment, nous allons utiliser un package de pfSense comme serveur proxy, Squid, sa configuration se fait par la même interface.

Tout d'abord la configuration de la partie HTTP du proxy, il suffit d'indiquer sur quelle interface le serveur doit écouter le trafic.

The screenshot shows the 'Squid General Settings' page. It includes several configuration options:

- Enable Squid Proxy:** A checkbox that is checked. Below it, a red note states: 'Important: If unchecked, ALL Squid services will be disabled and stopped.'
- Keep Settings/Data:** A checkbox that is checked. Below it, a red note states: 'Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.'
- Listen IP Version:** A dropdown menu set to 'IPv4'. Below it, text says: 'Select the IP version Squid will use to select addresses for accepting client connections.'
- CARP Status VIP:** A dropdown menu set to 'aucun'. Below it, text says: 'Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.'
- Proxy Interface(s):** A multi-select dropdown menu with 'WIFIUSERS', 'WIFIINVITES', 'BRIDGEUSERS', and 'BRIDGEINVITES' selected. Below it, text says: 'The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.'
- Outgoing Network Interface:** A dropdown menu set to 'Default (auto)'. Below it, text says: 'The interface the proxy server will use for outgoing connections.'
- Port du mandataire (« proxy »):** A text input field containing '3128'. Below it, text says: 'This is the port the proxy server will listen on. Default: 3128.'
- ICP Port:** An empty text input field. Below it, text says: 'This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.'

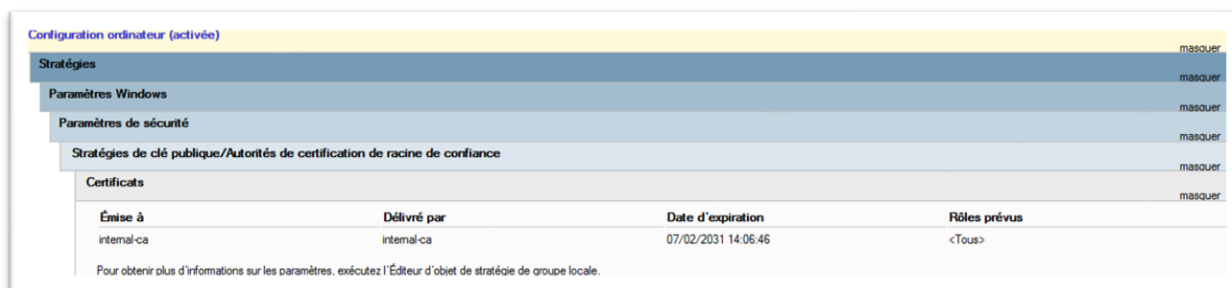
La partie HTTPS nécessite plus de configuration afin être mise en place.

La création d'une autorité de certification et d'un certificat pour permettre au proxy de signer le trafic HTTPS une fois intercepté.

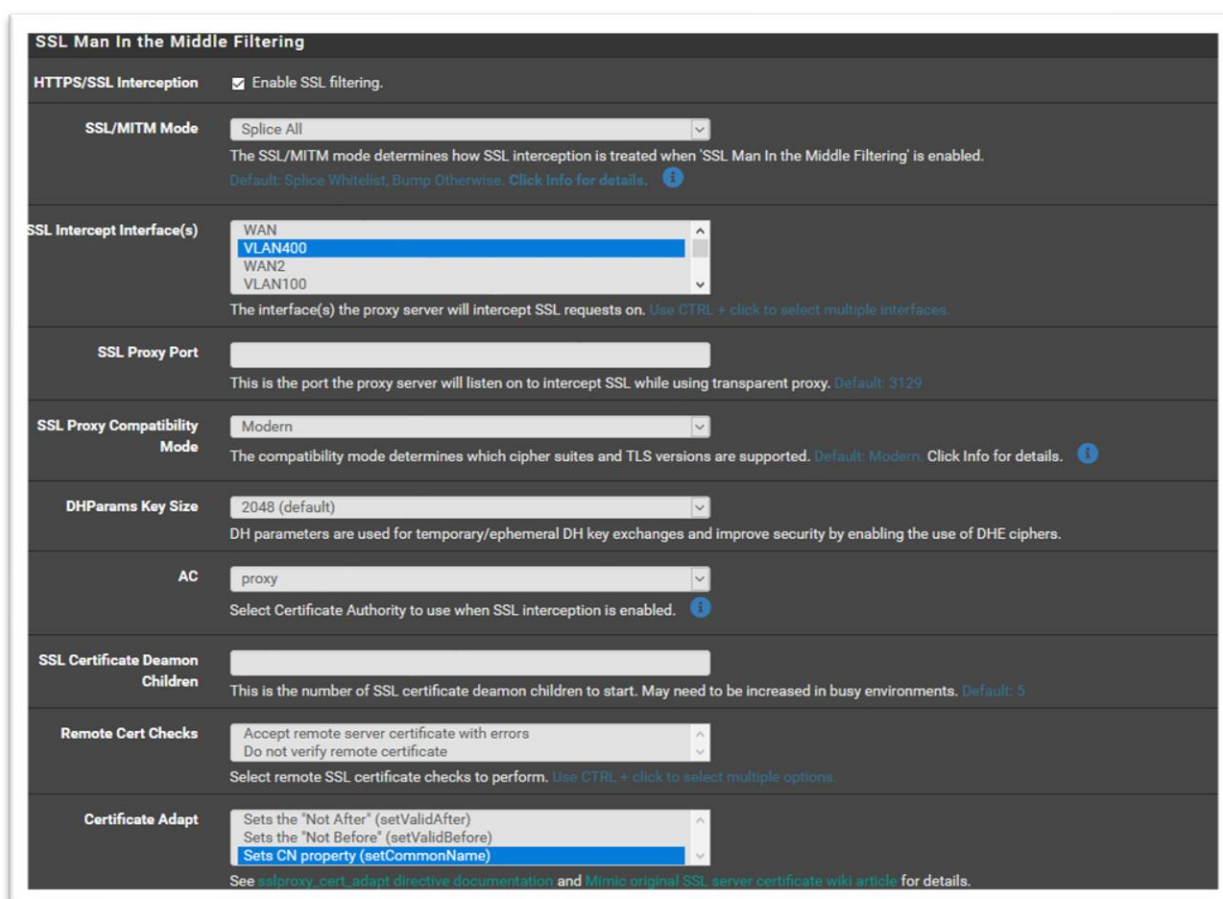
Autorités de certification						
Nom	Interne	Émetteur	Certificats	Nom distinctif	En cours d'utilisation	Actions
proxy	✓	auto-signé	0	ST=Var, OU=Projet, O=UnivTln, L=Toulon, CN=internal-ca, C=FR Valable depuis: Fri, 19 Mar 2021 00:19:51 +0100 Valable jusqu'à: Mon, 17 Mar 2031 00:19:51 +0100		

Certificats				
Nom	Émetteur	Nom distinctif	En cours d'utilisation	Actions
webConfigurator default (5e7808b8f1f8b) Server Certificate CA: No Serveur: Yes	auto-signé	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5e7808b8f1f8b Valable depuis: Mon, 23 Mar 2020 01:54:17 +0100 Valable jusqu'à: Sat, 13 Sep 2025 02:54:17 +0200	webConfigurator	
proxy User Certificate CA: No Serveur: No	proxy	ST=Var, OU=Projet, O=UnivTln, L=Toulon, CN=proxy.domaine.lpr, C=FR Valable depuis: Fri, 19 Mar 2021 00:20:34 +0100 Valable jusqu'à: Mon, 17 Mar 2031 00:20:34 +0100		

Il est nécessaire d'ajouter cette autorité de certification sur les machines clientes via une GPO.



Les configurations préalables terminées, on indique l'AC dans les paramètres du proxy et on active le filtrage SSL.



Afin de faciliter la configuration des clients, les paramètres du proxy sont diffusés via un fichier wpad hébergé directement sur le proxy lui-même (fichier de configuration automatique de proxy).

Voici un extrait du fichier :

```
// If the IP address of the local machine is within a defined
// subnet, send to a specific proxy.
    if (isInNet(myIpAddress(), "192.168.10.192", "255.255.255.192"))
        return "DIRECT";

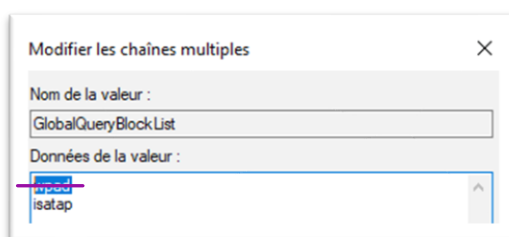
// DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
return "PROXY 192.168.10.254:3128";
```

Ajout de l'option WPAD sur le DHCP ainsi que l'enregistrement DNS correspondant.

 252 WPAD	Standard	http://wpad.domaine.lpr/wpad.dat	Aucun
--	----------	---	-------

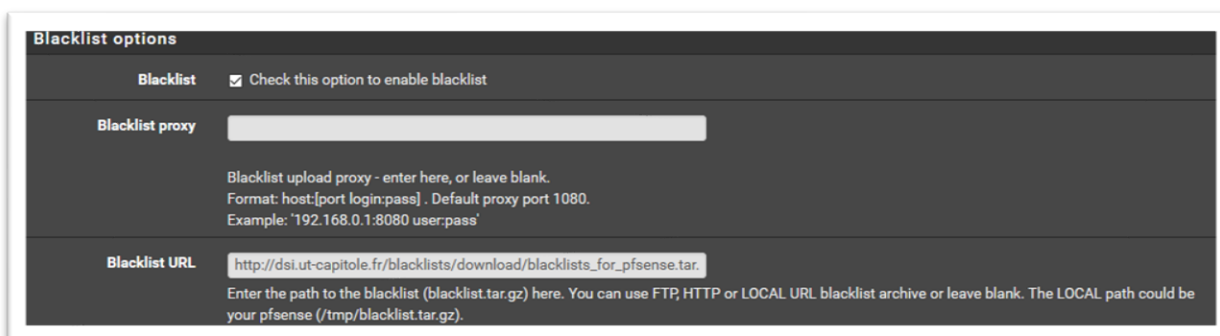
Dans notre cas, le serveur DNS étant un serveur Windows, il faut en plus permettre la réponse WPAD (bloqué par défaut).

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\



3.3.1.5) Filtrage Accès Web

Pour le filtrage via SquidGuard, nous allons utiliser une liste noire mise à disposition par l'Université de Toulouse 1 Capitole, elle est complète et fréquemment mise à jour (18/03/2021).



Blacklist options

Blacklist ☒ Check this option to enable blacklist

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Il est ensuite possible de choisir de bloquer ou non, certaines catégories.

target Categories			
[blk_blacklists_adult]	access	deny	▼
[blk_blacklists_agressif]	access	deny	▼
[blk_blacklists_arjel]	access	—	▼
[blk_blacklists_associations_religieuses]	access	deny	▼
[blk_blacklists_astrology]	access	deny	▼
[blk_blacklists_audio-video]	access	—	▼
[blk_blacklists_bank]	access	—	▼
[blk_blacklists_bitcoin]	access	deny	▼
[blk_blacklists_blog]	access	—	▼
[blk_blacklists_celebrity]	access	—	▼
[blk_blacklists_chat]	access	deny	▼
[blk_blacklists_child]	access	deny	▼
[blk_blacklists_cleaning]	access	—	▼
[blk_blacklists_cooking]	access	—	▼
[blk_blacklists_cryptojacking]	access	deny	▼
[blk_blacklists_dangerous_material]	access	deny	▼
[blk_blacklists_dating]	access	deny	▼

Cette liste noire permet de bloquer un grand nombre d'URL et de domaines, mais cependant, il reste le mot-clé et notamment les recherche d'image qui ne sont pas filtrer.

Une façon de restreindre les recherche l'utilisation de la fonctionnalité « **SafeSearch** » des moteurs de recherche. Elle peut être forcée par l'utilisation de redirection DNS.

	Nom	Type	Données	Horodateur
WS19-1.domaine.lpr	(identique au dossier parent)	Source de nom (SOA)	[2], ws19-1.domaine.lpr, hostmaster.domaine.lpr.	statique
WS19-1.domaine.lpr	(identique au dossier parent)	Serveur de noms (NS)	ws19-1.domaine.lpr.	statique
WS19-1.domaine.lpr	(identique au dossier parent)	Hôte (A)	216.239.38.120	statique

3.3.1.6) VPN

Le télétravail oblige un accès distant via VPN doit être mis en place. La solution OpenVPN directement intégrée à pfSense est privilégiée.

L'accès sera sécurisé par SSL/TLS et une authentification de l'utilisateur avec son compte Active Directory.

The screenshot shows the 'Informations Générales' (General Information) tab for an OpenVPN server configuration. The settings are as follows:

- Désactivé:** A checkbox labeled 'Désactiver ce serveur' (Deactivate this server) is checked. Below it, a note says: 'Définissez cette option pour désactiver ce serveur sans le retirer de la liste.'
- Mode serveur:** A dropdown menu is set to 'Accès à distance (SSL/TLS + Authentification utilisateur)' (Remote access (SSL/TLS + User authentication)).
- Backend pour l'authentification:** A dropdown menu is set to 'Active Directory'. 'Local Database' is also visible in the list.
- Protocole:** A dropdown menu is set to 'UDP on IPv4 only'.
- Mode dispositif:** A dropdown menu is set to 'tap - Layer 2 Tap Mode'. Below it, a note explains: 'Le mode "tun" porte IPv4 et IPv6 (couche OSI 3) et est le mode le plus courant et compatible sur toutes les plates-formes. Le mode "tap" est capable de transporter 802.3 (couche OSI 2.)'
- Interface:** A dropdown menu is set to 'WAN'. Below it, a note says: 'L'interface ou l'adresse IP virtuelle où OpenVPN recevra les connexions des clients'.
- Port local:** A text input field contains '1194'. Below it, a note says: 'Le port utilisé par OpenVPN pour recevoir des connexions client.'
- Description:** A text input field contains 'Vpn_User'. Below it, a note says: 'Une description peut être saisie ici à des fins de référence administrative (non analysée).'

À l'aide des interfaces bridges créés précédemment les utilisateurs connectés au VPN seront directement connecter au réseau comme s'il se trouver sur place.

L'ajout d'une règle dans le pare-feu pour autoriser le trafic entrant sur le port défini pendant la configuration du serveur.

The screenshot shows the 'Pare-feu / Règles / WAN' (Firewall / Rules / WAN) page. The 'WAN' tab is selected. Below the tabs, there is a list of rules. The first rule is highlighted:




Flottant(e)	WAN	VLAN400	WAN2	VLAN100	VLAN200	VPN_USER	WIFIUSERS	WIFIINVITES	BRIDGEUSERS
BRIDGEINVITES	OpenVPN								

Below the tabs, there is a section titled 'Règles (Faire glisser pour changer l'ordre)' (Rules (Drag to change order)). It contains a table with the following data:

États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
✓	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	aucun	Assistant Users OpenVPN	[Icons]

Un auto-installeur pourra être fourni directement aux utilisateurs grâce au package « **openvpn-client-export** » installer au début de la configuration.

3.3.1.7) Wi-Fi

Interfaces sans-fil			
Interface	Mode	Description	Actions
ath1_wlan0	Point d'accès	Wifi-Users	 
ath1_wlan1	Point d'accès	Wifi-Invites	 

Les deux interfaces sans-fil sont configurées et ajoutées à leurs interfaces pont respectif (**BRIDGESUSER et BRIDGESINVITES**).

Le premier réseau wifi destiné à l'invité est laissé ouvert afin de faciliter leurs connexions, ils sont soumis aux mêmes règles que s'ils étaient connectés sur le réseau filaire.

Le réseau wifi utilisateurs quant à lui devra être configuré avec une sécurité de type WPA2-EAP ce qui permettra grâce à un serveur *RADIUS* l'authentification des utilisateurs avec leurs comptes active directory.

Dû à un problème matériel, la partie RADIUS n'a pas pu être mise en place sur la maquette.

3.3.2) Switchs

L'architecture générale des switchs est présentée en [annexe 10](#).

3.3.2.1) VLANs

La création de plusieurs VLANs a été mise en œuvre afin de sécuriser et segmenter le réseau au plus proche des besoins exprimés par le responsable informatique de la mairie de Signes :

- VLAN 100 = **« Utilisateurs »** : 192.168.10.0/25
- VLAN 200 = **« Invités »** : 192.168.10.128/26
- VLAN 300 = **« TRUNK »** : pour créer un canal de communication et échanger les données transmises entre les différents VLANs.
- VLAN 400 = **« Administration - Equipements »** : 192.168.10.192/26

3.3.2.2) Configuration physique des commutateurs

Le matériel ré-utilisé par la société FUTURZO est composée de 3 switchs dont 2 de niveau 3 : commutateurs HP 1910-16G et HP1810-24G.

La configuration en lignes de commandes de ces switchs étant un peu particulière, nous ne parlerons ici que de la configuration par interface web.

3.3.2.2.1) Configuration générique des switchs

La configuration générique des switchs se décompose en plusieurs étapes :

- Réinitialisation du commutateur,
- Configuration de l'adresse IP de management,
- Sécurisation des accès,
- Création de comptes administrateurs nominatifs,
- Mise en place de la journalisation,
- Configuration du NTP.

Voici les paramètres qui sont communs aux 3 commutateurs.

1ère étape : Réinitialisation des switchs

Afin de paramétrer les switchs, il a fallu les réinitialiser.

- Connexion d'un câble en port série,
- Paramétrage de l'utilitaire « **Putty** » comme suit :
 - o Bits par seconde : 38400 ;
 - o Data bits : 8 ;
 - o Parity : None ;
 - o Stop bit : 1 ;
 - o Flow control : None ;
 - o Emulation : VT100.
- « **Initialization** » qui a pour effet d'effacer le fichier de configuration et démarre sur la configuration par défaut du commutateur

```
<HP V1910 Switch>?
User view commands:
  initialize  Delete the startup configuration file and reboot system
  ipsetup     Specify the IP address of the VLAN interface 1
  password    Specify password of local user
  ping        Ping function
  quit        Exit from current command view
  reboot      Reboot system
  summary     Display summary information of the device.
  upgrade     Upgrade the system boot file or the Boot ROM program

<HP V1910 Switch>
```

- Puis « **ipsetup** » : pour paramétrer une adresse IP sur le VLAN1 (défaut) ;

<HP V1910 Switch> ipsetup ip-address 10.0.0.1 255.0.0.0 default-gateway 10.0.0.254

2ème étape : Configuration des switches en Web console

- Sécurisation des accès aux switches : activer le protocole HTTPS et désactiver le http

Security ► Secure Connection

Web Configuration

HTTP Admin Mode	Disabled ▼
HTTPS Admin Mode	Enabled ▼

- Activer le SSH et le SFTP pour pouvoir administrer les switches à distance et télécharger les configurations :

Service	
FTP	<input type="checkbox"/> Enable FTP service
Telnet	<input type="checkbox"/> Enable Telnet service
SSH	<input checked="" type="checkbox"/> Enable SSH service
SFTP	<input checked="" type="checkbox"/> Enable SFTP service
HTTP	<input type="checkbox"/> Enable HTTP service
HTTPS	<input checked="" type="checkbox"/> Enable HTTPS service

- Création de 2 comptes d'administrateurs nominatifs avec droits d'accès étendus :

Select a user and modify the selected user attributes in the fields below

Username	Access Level	Service Type
admin	Management	Web/FTP/Telnet/Terminal
adm_j.alba	Management	Web/FTP/Telnet/Terminal
adm_h.desouza	Management	Web/FTP/Telnet/Terminal

- Mise en place de la journalisation vers le contrôleur de Domaine :

Loghost

☒ IPv4 ☐ IPv6

Loghost IP

Items marked with an asterisk(*) are required

Apply

Please select the loghost IP

Loghost	
Loghost	192.168.10.193

- Configuration du NTP : source = Routeur PfSense

External Reference Source

NTP Server 1	192.168.10.254
--------------	----------------

- Création d'une adresse IP de VLAN (pour le VLAN de Management) :

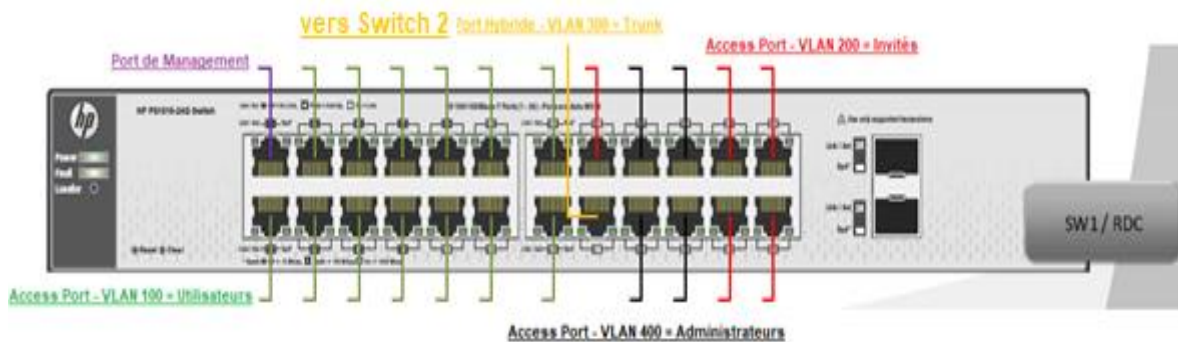
<input type="radio"/> All Address	<input checked="" type="radio"/> IPv4 Address	<input type="radio"/> IPv6 Address	<input type="radio"/> No Address
VLAN ID	IPv4 Address / IPv6 Link Local Address	Admin Status	Method
*1	10.0.0.1/8	Up	Manual

Dans l'optique d'avoir un réseau sécurisé et des interfaces d'administration segmentées, nous recommandons au client changer les adresses IP de Management.

3.3.2.2.2) Switch 1 : RDC

Dénomination du matériel utilisé : Commutateur HP 1820-24G.

Voici la disposition finale du switch1 :



- Création des VLANS :

VLAN	
Create VLAN	<input type="checkbox"/>
Create VLAN ID	<input type="text"/>
Number of VLANs	5

VLAN ID	VLAN Name
1	default
100	Utilisateurs
200	Invités
300	Trunk
400	Management

- Configuration des ports :

- o VLAN 1 = Management – le port d'accès doit être configuré en U (Untagged)

VLAN Tagging																											
VLAN																											
											Tag / Untag / Exclude All																
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
	U	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E

- VLAN 100 = Utilisateurs

VLAN Tagging																											
VLAN																											
100																											
Tag / Untag / Exclude All																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
	E	U	U	U	U	U	U	U	U	U	U	U	U	U	U		E	E	E	E	E	E	E	E	E	E	

- VLAN 200 = Invités

VLANs ▶ Participation / Tagging																											
VLAN Tagging																											
VLAN <div>200</div>																											
<div>U</div> Tag / Untag / Exclude All																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E		U	U	U	U	E	E	E	E	U	U	

- Pas de VLAN 300 sur ce switch, le TRUNK se configure directement en accès sur le port :

Trunks ▶ Trunk Configuration																													
Trunk	Name	Mode	Port Members																										
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
TRK1	<div>TRUNK</div>	<div>Static</div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>

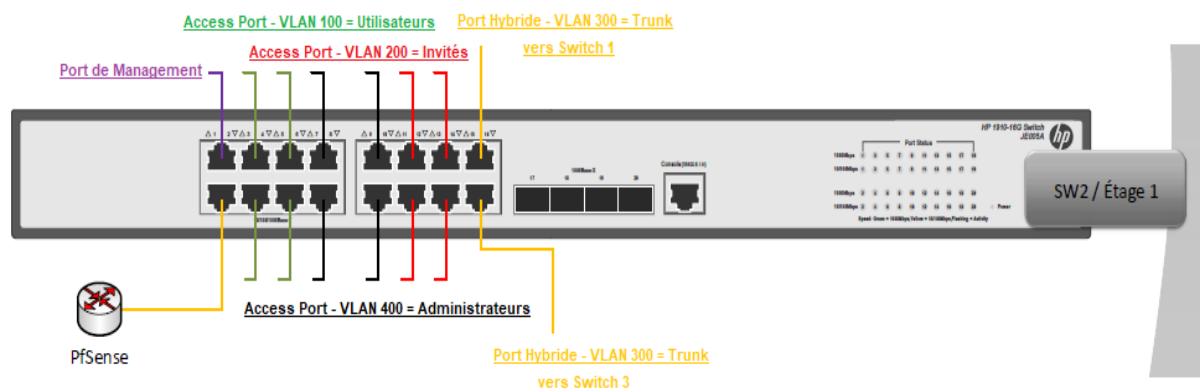
- VLAN 400 = Administrateurs/Equipements

VLAN Tagging																											
VLAN																											
400																											
U Tag / Untag / Exclude All																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E		E	E	E	E	U	U	U	U	E		

3.3.2.2.3) Switch 2 : 1^{er} étage

Dénomination du matériel utilisé : Commutateur HP 1910-16G.

Voici la disposition finale du switch 3 :



- Création des VLANS :

Autre particularité sur les switchs HP 1910-16G : Pour assurer la propagation des VLANS, il faut tagguer les différents VLANS sur le port qui servira au TRUNK.

VLAN Summary

ID	Description	Untagged Membership	Tagged Membership
1	VLAN 0001	GE1/0/1, GE1/0/17-GE1/0/20	
100	Utilisateurs	GE1/0/2-GE1/0/6	GE1/0/15-GE1/0/16
200	Invites	GE1/0/7-GE1/0/10	GE1/0/15-GE1/0/16
300	Trunk		GE1/0/15-GE1/0/16
400	Management	GE1/0/11-GE1/0/14	GE1/0/15-GE1/0/16

- Configuration des ports :

La spécificité des switchs HP 1910-16G est que les ports hybrides ont tendance à faire planter le routage inter-VLANs.

Il a donc été décidé d'attribuer des VLANs aux différents ports (port d'accès = « **UNTAGGED** ») comme prévu puis de passer 2 ports en mode « **TRUNK** » (ports 15 et 16) qui serviront à la desserte des autres VLANS en direction des switch 1 et switch 3.



Port	Untagged Membership	Tagged Membership	Link Type	PVID
GE1/0/1	1		Access	1
GE1/0/3	100		Access	100
GE1/0/5	100		Access	100
GE1/0/7	200		Access	200
GE1/0/9	200		Access	200
GE1/0/11	400		Access	400
GE1/0/13	400		Access	400
GE1/0/15		2-400	Trunk	1
GE1/0/2	400		Access	100
GE1/0/4	100		Access	100
GE1/0/6	100		Access	100
GE1/0/8	200		Access	200
GE1/0/10	200		Access	200
GE1/0/12	400		Access	400
GE1/0/14	400		Access	400
GE1/0/16		2-400	Trunk	1

- Routage inter-VLANs :

La particularité du switch 2 réside dans le fait qu'il fait office de « routeur » pour la desserte réseau des switchs 1 et 3.

Pour cela, il a fallu créer des interfaces de VLAN uniquement sur le switch 2 :

☒ All Address
 ☐ IPv4 Address
 ☐ IPv6 Address
 ☐ No Address

VLAN ID	IPv4 Address / IPv6 Link Local Address	Admin Status	Method
*1	10.0.0.1/8	Up	Manual
100	192.168.10.126/25	Up	Manual
200	192.168.10.190/26	Up	Manual
400	192.168.10.201/26	Up	Manual

Enfin, nous avons créé les routes en direction du routeur PfSense afin de faire transiter les données depuis le LAN local de la mairie :

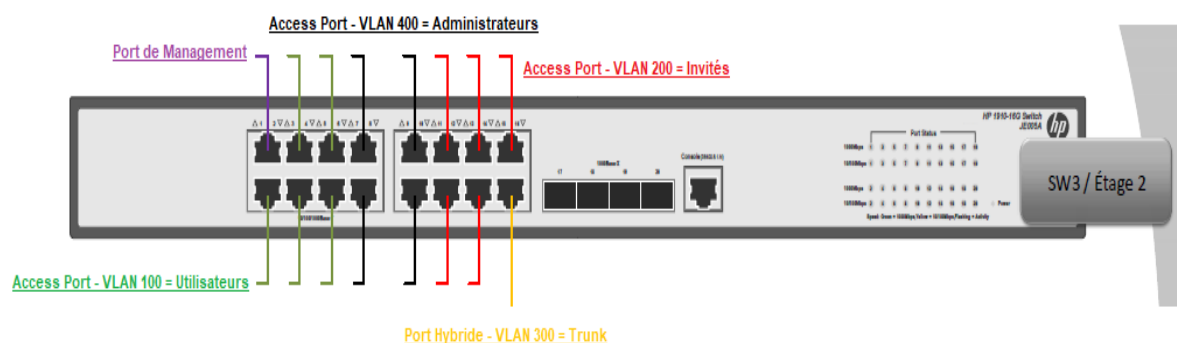
Active route table

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface
0.0.0.0	0.0.0.0	Static	60	192.168.10.254	Vlan-interface100
10.0.0.0	255.0.0.0	Direct	0	10.0.0.1	Vlan-interface1
10.0.0.1	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0
127.0.0.0	255.0.0.0	Direct	0	127.0.0.1	InLoopBack0
127.0.0.1	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0
192.168.10.0	255.255.255.128	Direct	0	192.168.10.126	Vlan-interface100
192.168.10.126	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0
192.168.10.128	255.255.255.192	Direct	0	192.168.10.190	Vlan-interface200
192.168.10.190	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0
192.168.10.192	255.255.255.192	Direct	0	192.168.10.201	Vlan-interface200
192.168.10.201	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0

3.3.2.2.4) Switch 3 : 2^{ème} étage

Dénomination du matériel utilisé : Commutateur HP 1910-16G.

Voici la disposition finale du switch 3 :



- Création des VLANS :

Autre particularité sur les switchs HP 1910-16G : Pour assurer la propagation des VLANS, il faut tagguer les différents VLANS sur le port qui servira au TRUNK.

VLAN Summary

ID	Description	Untagged Membership	Tagged Membership
1	default	GE1/0/1, GE1/0/17-GE1/0/20	
100	Utilisateurs	GE1/0/2-GE1/0/6	GE1/0/16
200	Invites	GE1/0/7-GE1/0/12	GE1/0/16
400	Management	GE1/0/13-GE1/0/15	GE1/0/16

- Configuration des ports :

La spécificité des switchs HP 1910-16G est que les ports hybrides ont tendance à faire planter le routage inter-VLANs.

Il a donc été décidé d'attribuer des VLANs aux différents ports (port d'accès = « **UNTAGGED** ») comme prévu puis de passer 1 seul port en mode « **TRUNK** »



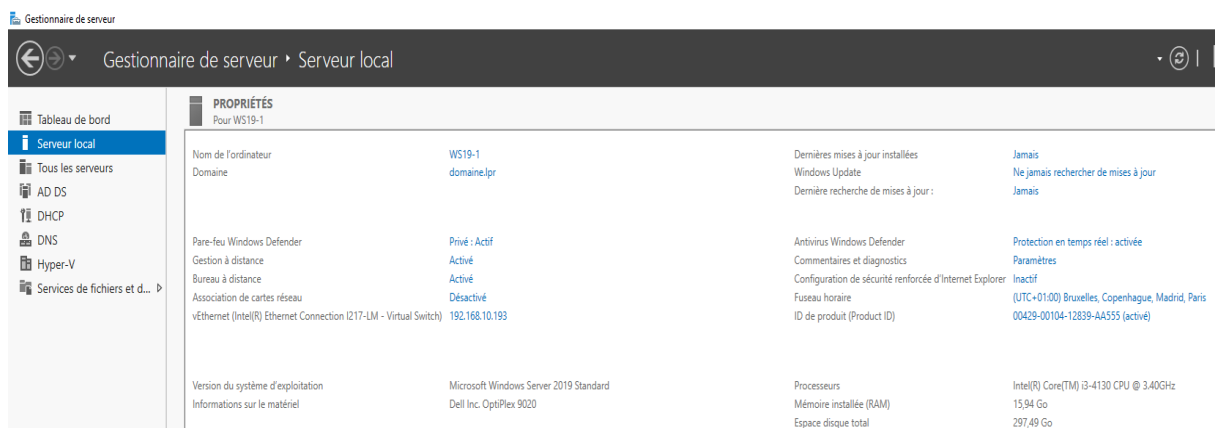
Port	Untagged Membership	Tagged Membership	Link Type	PVID
GE1/0/1	1		Access	1
GE1/0/3	100		Access	100
GE1/0/5	100		Access	100
GE1/0/7	200		Access	200
GE1/0/9	200		Access	200
GE1/0/11	200		Access	200
GE1/0/13	400		Access	400
GE1/0/15	400		Access	400
GE1/0/2	100		Access	100
GE1/0/4	100		Access	100
GE1/0/6	100		Access	100
GE1/0/8	200		Access	200
GE1/0/10	200		Access	200
GE1/0/12	200		Access	200
GE1/0/14	400		Access	400
GE1/0/16		2-400	Trunk	1
GE1/0/17	1		Access	1

3.3.3) Serveurs

3.3.3.1) Serveur Physique

Le serveur physique faisant office de contrôleur de domaine pour la mairie est un serveur Windows 2019 Professionnel.

Voici le résumé des rôles serveurs et fonctionnalités le composant :



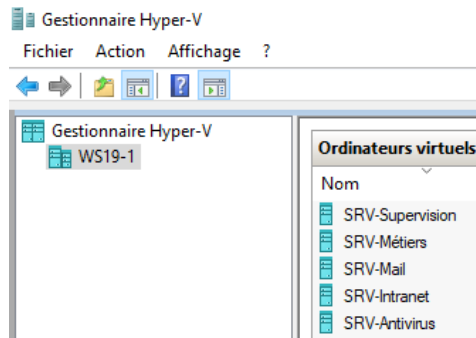
3.3.3.1.1) Contrôleur de Domaine

Le contrôleur de domaine a été nommé « **WS19-1** ». Il a pour adresse IP : 192.168.10.193.

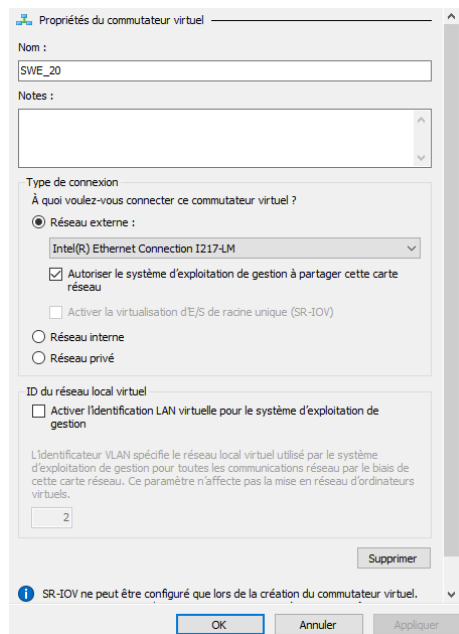
Le domaine créé lors de la maquette se nomme « **domaine.lpr** ». Il ne représente pas le domaine déployé à la mairie de Signes.

3.3.3.1.1.1) Hyper-V

Nous avons utilisé le gestionnaires de machines virtuelles - décrites dans la suite du compte-rendu (Mails, Web, Anti-Virus, Supervision, Métier) - natif de Windows.



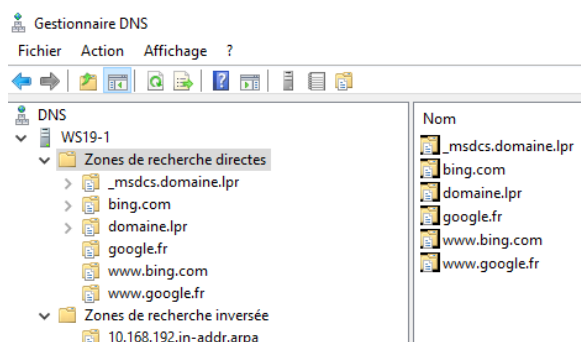
Un **commutateur virtuel** a été utilisé pour pouvoir faire communiquer les différentes VM créées par la suite :



3.3.3.1.1.2) DNS

Service de système de noms de domaine utilisé pour traduire les noms de domaine Internet en adresse IP et les autres enregistrements.

○ Recherche directes :



Les recherches directes suivantes : « **bing.com** », « **www.bing.com** », « **google.fr** » et « **www.google.fr** » ont été ajoutées manuellement afin de permettre le filtrage des accès à un contenu explicite (filtrage détaillé plus haut)

○ Recherches inversées :

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[42], ws19-1.domaine.lpr, ...	statique
(identique au dossier parent)	Serveur de noms (NS)	ws19-1.domaine.lpr.	statique
192.168.10.1	Pointeur (PTR)	Acer-Swift-3.	16/02/2021 16:00:00
192.168.10.126	Pointeur (PTR)	pfsense.domaine.lpr.	statique
192.168.10.129	Pointeur (PTR)	Acer-Swift-3.	02/03/2021 15:00:00
192.168.10.130	Pointeur (PTR)	Acer-Swift-3.	02/03/2021 15:00:00
192.168.10.190	Pointeur (PTR)	pfsense.domaine.lpr.	statique
192.168.10.193	Pointeur (PTR)	WS19-1.domaine.lpr.	statique
192.168.10.194	Pointeur (PTR)	SRV-Intranet.	16/02/2021 17:00:00
192.168.10.195	Pointeur (PTR)	CLIENT2.	02/03/2021 12:00:00
192.168.10.198	Pointeur (PTR)	localhost.localdomain.	02/03/2021 15:00:00
192.168.10.199	Pointeur (PTR)	SRV-Antivirus.	02/03/2021 16:00:00
192.168.10.2	Pointeur (PTR)	CLIENT1.domaine.lpr.	statique
192.168.10.201	Pointeur (PTR)	Switch2.	statique
192.168.10.205	Pointeur (PTR)	zabbix.domaine.lpr.	statique
192.168.10.206	Pointeur (PTR)	truenas.	statique
192.168.10.208	Pointeur (PTR)	mail.domaine.lpr.	statique
192.168.10.254	Pointeur (PTR)	pfsense.domaine.lpr.	statique
192.168.10.3	Pointeur (PTR)	CLIENT2.	02/03/2021 18:00:00
192.168.10.4	Pointeur (PTR)	HUAWEI_P30_Pro-7188ac9...	02/03/2021 18:00:00
192.168.10.5	Pointeur (PTR)	Acer-Swift-3.	02/03/2021 15:00:00

3.3.3.1.1.3) DHCP

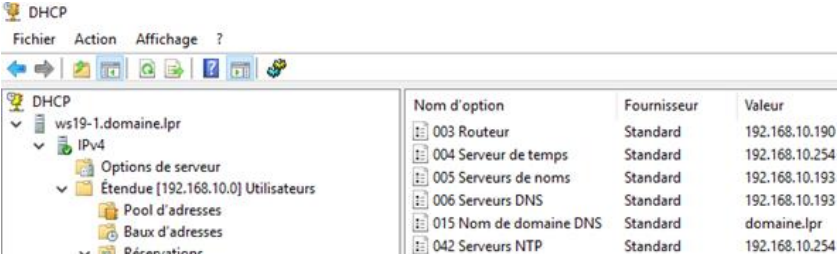
Protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

Le système de bail périodique attribué a été défini à « **infini** » pour des convenances pratiques, il appartient au responsable informatique de la mairie de Signes de modifier ce paramètre s'il souhaite sécuriser les baux DHCP.

- Etendue **« Utilisateurs »** : correspondant à la plage d'adresses IP 192.168.10.0/25
- Etendue **« Invités »** : correspondant à la plage d'adresses IP 192.168.10.128/26
- Etendue **« Equipements »** : correspondant à la plage d'adresses IP 192.168.10.192/26

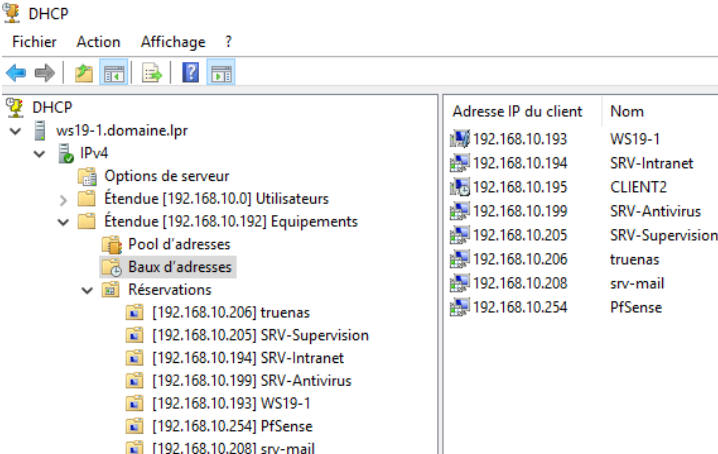
- **Options d'étendues** définies pour paramétrer automatiquement les clients récupérant dynamiquement une adresse IP auprès du serveur DHCP :

- **Routeur :**
 - **192.168.10.126** pour l'étendue « **Utilisateurs** »
 - **192.168.10.190** pour l'étendue « **Invités** »
 - **192.168.10.201** pour l'étendue « **Equipements** »
- **Serveur de Temps :**
 - routeur PfSense = **192.168.10.254**
- **Serveur de noms :**
 - Contrôleur de domaine = **192.168.10.193**
- **Serveur DNS :**
 - Contrôleur de domaine = **192.168.10.193**
- **Nom de domaine DNS :**
 - Contrôleur de domaine = **domaine.lpr**
- **Serveur NTP :**
 - routeur PfSense = **192.168.10.254**



Nom d'option	Fournisseur	Valeur
003 Routeur	Standard	192.168.10.190
004 Serveur de temps	Standard	192.168.10.254
005 Serveurs de noms	Standard	192.168.10.193
006 Serveurs DNS	Standard	192.168.10.193
015 Nom de domaine DNS	Standard	domaine.lpr
042 Serveurs NTP	Standard	192.168.10.254

- **Réservation de baux** effectuée pour l'ensembles des machines du LAN de la mairie :



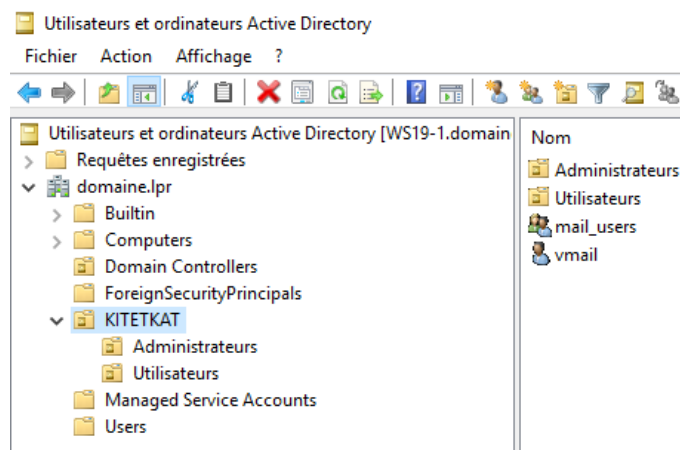
Adresse IP du client	Nom
192.168.10.193	WS19-1
192.168.10.194	SRV-Intranet
192.168.10.195	CLIENT2
192.168.10.199	SRV-Antivirus
192.168.10.205	SRV-Supervision
192.168.10.206	truenas
192.168.10.208	srv-mail
192.168.10.254	PfSense

3.3.3.1.1.4) AD DS

Services de domaine Active Directory consistant à stocker les données d'annuaire et gérer les communications. Active Directory Domain Services ou AD DS s'occupe de la gestion des communications entre utilisateurs, le processus d'ouverture de session, la recherche d'annuaire et l'authentification.

Pour des raisons pratiques, nous avons déployé un AD de test sur la mquette de notre livrable intitulé « **domaine.lpr** ». Le déploiement de l'AD ne faisant pas partie des termes de l'accord passé avec la mairie de Signes, la responsabilité du déploiement de l'AD incombe au responsable informatique.

- Résumé de l'AD de test déployé :



Une UO a été créée « **KITETKAT** » afin de pouvoir paramétrer les GPO ultérieures et 2 sous-UO « **Administrateurs** » et « **Utilisateurs** » afin de pouvoir monter un partage de fichiers qui sera utilisé notamment dans la sauvegarde du serveur de fichiers avec le NAS.

Le Partage « P : » fera office de partage test pour le paramétrage du NAS.

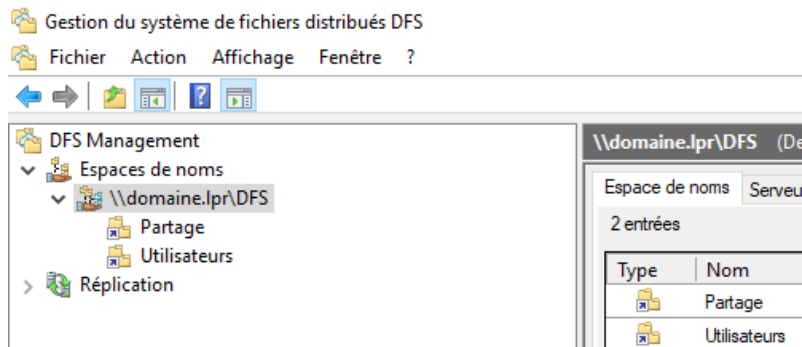
- Quotas des disques en termes de stockage :

Gestion des disques							
Fichier Action Affichage ?							
Volume	Disposition	Type	Système de ...	Statut	Capacité	Espace li...	% libres
(C:)	Simple	De base	NTFS	Sain (Dém...	102,18 Go	24,18 Go	24 %
(Disque 0 partition...	Simple	De base	NTFS	Sain (Parti...	100 Mo	100 Mo	100 %
Partage (P:)	Simple	De base	NTFS	Sain (Parti...	146,48 Go	142,77 Go	97 %
Récupération	Simple	De base	NTFS	Sain (Parti...	499 Mo	70 Mo	14 %
Utilisateurs (E:)	Simple	De base	NTFS	Sain (Parti...	48,83 Go	48,73 Go	100 %

3.3.3.1.1.5) DFS

La technologie Distributed File System de Microsoft, en français « Système de fichiers distribué » est un ensemble de services client et serveur permettant : de fournir une arborescence logique aux données partagées depuis des emplacements différents.

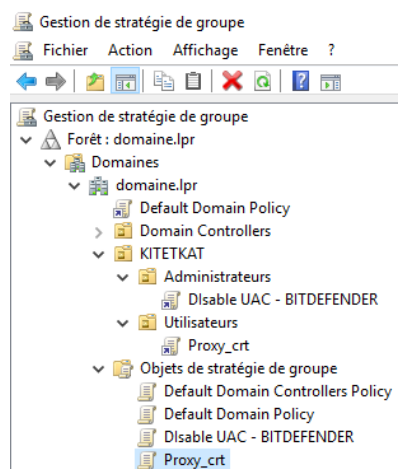
Le rôle est installé et configuré mais non utilisé pour un déploiement avec un serveur redondé à l'avenir.



3.3.3.1.1.6) GPO

Résumé des GPO utilisées :

- Proxy_crt : sert à ajouter une autorité de certification sur les machines clientes via une GPO.
- Disable UAC - BitDefender : sert à désactiver l'élévation de privilèges pour installer l'agent BitDefender sur les postes clients depuis l'appliance GravityZone



3.3.3.1.1.7) Sauvegarde distante

Nous avons créé une tâche planifiée qui va permettre de sauvegarder le Partage de fichiers utilisé par le personnel de la mairie directement sur le NAS distant :

Sauvegarde planifiée
Une sauvegarde planifiée à intervalles réguliers est configurée pour ce serveur.

Paramètres
Éléments de sauvegarde : État du système; Récupération; Partage (P:)
Fichier exclus : Aucun
Option avancée : Sauvegarde de copie VSS
Destination : \\192.168.10.206\administrateur (Partage réseau distant)
Heure de la sauvegarde : Tous les jours 21:00

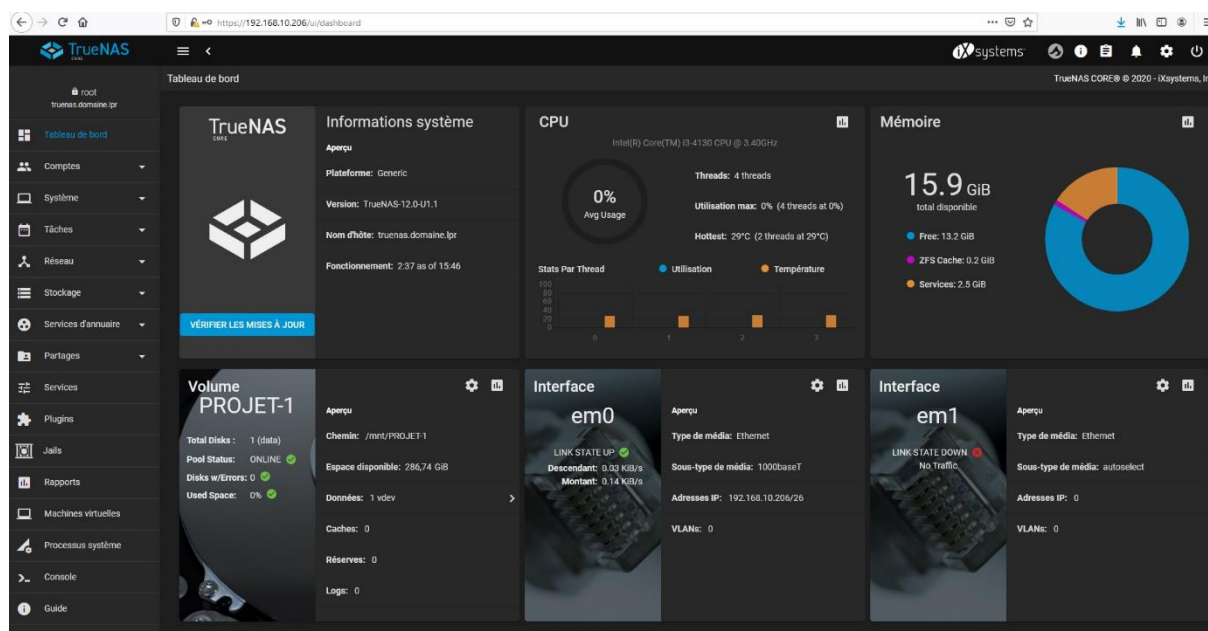
Utilisation de la destination
Nom : \\192.168.10.206\administrateur
Capacité : Aucun détail n'est disponible pour le dossier partagé distant.
Espace utilisé : Aucun détail n'est disponible pour le dossier partagé distant.
Sauvegardes disponibles : Aucun détail n'est disponible pour le dossier partagé distant.
[Afficher les détails](#)
[Actualiser les informations](#)

3.3.3.1.2) Recyclage de l'ancien serveur pour configuration en NAS

TrueNas est un système d'exploitation sous licence libre, basé sur FreeBSD, destiné aux serveurs de stockage en réseau NAS. Il supporte de nombreux protocoles : CIFS, FTP, NFS, rsync, AFP, iSCSI, rapport S.M.A.R.T. l'authentification d'utilisateurs locaux, et RAID Logiciel.

Le choix de ce système d'exploitation a été fait car il possède des avantages indéniables : OpenSource, système de volumes et d'autorisations, répliquions et synchronisations, Instantanés/snapshots.

- Résumé du serveur :



Après avoir installé le serveur (sous sa version brute) puis paramétré la carte réseau en DHCP, le serveur est donc prêt à être configuré.

- **Configuration réseau du serveur :**

Nom de Domaine et Domaine		Annonce de service	
Nom d'hôte truenas	?	<input checked="" type="checkbox"/> NetBIOS-NS	?
Domaine domaine.lpr	?	<input checked="" type="checkbox"/> mDNS	?
Domaines supplémentaires	?	<input checked="" type="checkbox"/> WS-Discovery	?
Serveurs DNS		Passerelle par défaut	
Serveur de noms 1 (DNS) 192.168.10.193	?	Passerelle IPv4 par défaut 192.168.10.254	?
Serveur de noms 2 (DNS)	?	Passerelle IPv6 par défaut	?
Serveur de noms 3 (DNS)	?		
Autres Paramètres			
Proxy HTTP 192.168.10.254		?	
<input type="checkbox"/> Activer la fonction Netwait ?			
Base de données des noms d'hôtes 192.168.10.193		?	

- **Configuration de l'AD (synchronisation) :**

Identifiants du Domaine	
Nom de domaine * DOMAINE.LPR	
<input checked="" type="checkbox"/> Activer (requiert le mot de passe ou le principal Kerberos) ?	
<input type="checkbox"/> Niveau de journalisation ?	<input checked="" type="checkbox"/> Autoriser les mises à jour DNS ?
<input checked="" type="checkbox"/> Autoriser les domaines approuvés ?	<input type="checkbox"/> Désactiver le cache FreeNAS ?
<input checked="" type="checkbox"/> Utiliser le domaine par défaut ?	<input type="checkbox"/> Restreindre PAM ?
Nom du site DOMAINE.LPR	Délai d'attente DNS 10
Realm Kerberos ▼	Winbind NSS Info
Kerberos Principal TRUENAS\$@DOMAINE.LPR	Nom Netbios * truenas
Compte d'ordinateur OU ?	Alias NetBIOS
Délai d'expiration AD 60	?
<input type="button" value="ENREGISTRER"/> <input type="button" value="OPTIONS DE BASE"/> <input type="button" value="MODIFIER IDMAP"/> <input type="button" value="RECONSTRUCTION DU CACHE DU SERVICE D'ANNUAIRE"/>	

- Configuration du LDAP :

A noter que la création d'un utilisateur pour synchroniser le LDAP n'est pas automatique, il faut le faire à la main donc créer 1 utilisateur dans l'AD distant puis renseigner les champs concernant le LDAP sous TrueNas.

- Vérification de la présence des disques : (pour créer les volumes nécessaires au stockage)

Disques			
Opérations par lots (batch)			
<div> <div>MODIFIER LE(S) DISQUE(S)</div> <div>TEST MANUEL</div> </div>			
<input type="checkbox"/>	Nom	Numéro de série	Taille du disque
<input type="checkbox"/>	ada0	S2AW6F7B	465.76 GiB
<input checked="" type="checkbox"/>	ada1	Z3T8E7R3	298.09 GiB
Type de disque: HDD Description: Modèle: ST320DM000-1BD14C Mode de transfert: Auto Vitesse de rotation (RPM): 7200 HDD en veille: ALWAYS ON Gestion avancée de l'alimentation: DISABLED Niveau d'acoustique: DISABLED Activer S.M.A.A.R.T.: true Options supplémentaires S.M.A.R.T.:			

Un petit problème a été constaté sur la plate-forme de test, étant donné qu'il n'y avait qu'un seul disque dédié à l'OS sur le serveur TrueNas, nous avons dû « ouvrir » le capot du serveur afin d'y intégrer un 2^{ème} disque pour stocker les données.

- **Création des utilisateurs :**

Utilisateurs				
Filtre Utilisateurs				
COLONNES				
AJOUTER				
Nom d'utilisateur	UID	Builtin	Nom complet	
Hugo	1001	non	Hugo	>
Julien	1000	non	Julien	>
root	0	oui	root	>

Différents utilisateurs sont en réalité créés dans le cas où il n'y a pas d'AD à synchroniser. Ici, étant donné que l'AD est synchronisé, nous utiliserons le paramètre « Builtin_users » qui correspond aux utilisateurs du domaine distant.

- **Création des volumes :**

3 volumes ont été créés afin de permettre un accès distant à plusieurs capacités de stockage :

- Admin : pour les administrateurs (envoi des confs réseaux des différents EAR)
- Partage : sauvegarde distante du serveur de fichiers
- Utilisateurs : pour les répertoires privés des utilisateurs

Volumes								
PROJET-1 (System Dataset Pool)								
ONLINE ✓ 13 MiB (0%) Utilisé 286.74 GiB Libre								
Nom	Type	Utilisé	Available	Compression	Compression Ratio	Readonly	Dedup	Commentaires
PROJET-1	FILESYSTEM	13.00 MiB	286.74 GiB	lz4	13.67	false	OFF	
Admin	FILESYSTEM	264.00 KiB	286.74 GiB	Hérite (lz4)	1.02	false	OFF	Dataset Administrateurs
PARTAGE	FILESYSTEM	296.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	Dataset Public
administrateur	FILESYSTEM	96.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	
ws19-1_	FILESYSTEM	96.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	
Utilisateurs	FILESYSTEM	456.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	Dataset Utilisateurs
Adel	FILESYSTEM	96.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	Dataset Adel
Hugo	FILESYSTEM	128.00 KiB	286.74 GiB	Hérite (lz4)	1.01	false	OFF	Dataset Hugo

Pour des raisons pratiques, les configurations des autorisations sur les volumes ne seront pas détaillées.

- **Création des instantanés du NAS :**

Une sauvegarde du NAS est faite tous les jours à minuit. Les sauvegardes courent sur 2 semaines (donc 2 semaines de sauvegardes de données au cas où un utilisateur aurait eu un problème avec une erreur de manipulation de données)

The screenshot shows a configuration window for a dataset named 'PROJET-1'. It is divided into two main sections: 'Dataset' and 'Planifier' (Schedule).
In the 'Dataset' section, the name 'PROJET-1' is shown with a dropdown arrow and a help icon. Below it, the 'Récursif' (Recursive) checkbox is checked, and there is an 'Exclure' (Exclude) section which is currently empty.
In the 'Planifier' section, the 'Durée de vie des instantanés' (Retention of snapshots) is set to '2 WEEKS'. The 'Schéma de nommage' (Naming scheme) is 'auto-%Y-%m-%d_%H-%M' with a '00**' input field. The 'Planifier' (Schedule) is set to 'Daily (0 0 * * *) at 00:00 (12:00 AM)'. There are two checked checkboxes: 'Autoriser la prise d'instantanés vides' (Allow taking empty snapshots) and 'Activé' (Enabled).
At the bottom, there are two buttons: 'ENREGISTRER' (Save) in blue and 'ANNULER' (Cancel) in grey.

Dû à un problème de configuration distant, la connexion SSH n'a pas pu être paramétrée.

3.3.3.2) Serveurs Virtuels

Plusieurs machines virtuelles ont donc été nécessaires au déploiement de l'architecture réseaux/système souhaité par la mairie de Signes.

Les mêmes modus operandi ont été utilisé pour installer les serveurs de Supervision, Messagerie et Web, à savoir :

- Un fichier .iso à installer directement sur la VM,
- Le paramétrage de la carte réseau en DHCP,
- La configuration du serveur en interface WEB.

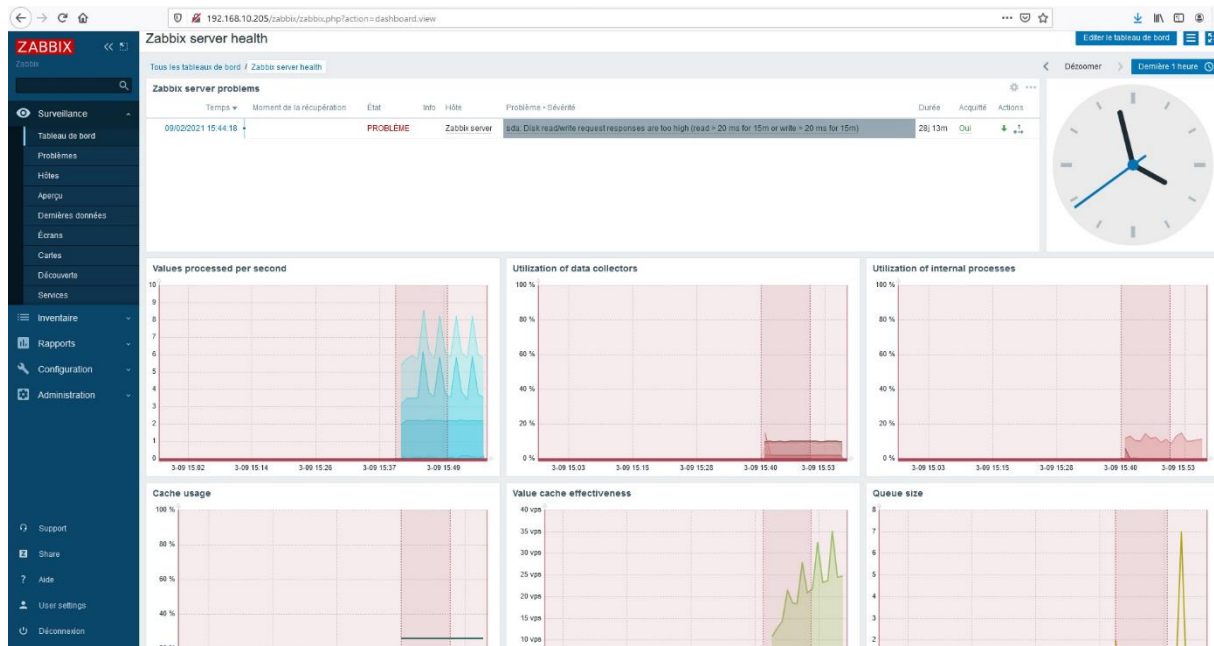
3.3.3.2.1) Serveur de Supervision

Pour implémenter un moyen de supervision sur notre architecture, nous avons choisi Zabbix.

ZABBIX est un logiciel libre permettant de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources.

Le choix de ce système d'exploitation a été fait car il possède des avantages indéniables : OpenSource, vue simplifiée, nombreuses fonctionnalités (paramétrage des hôtes, découverte du réseau, déploiement des agents..)

- **Résumé du serveur :**



- **Création de comptes d'administrateurs nominatifs :**

The screenshot shows the Zabbix user management interface. The left sidebar menu is visible, with 'Administration' selected. The main content area is titled 'Utilisateurs'. At the top, there's a green bar indicating 'Utilisateur ajouté'. Below this, there's a form to add a new user with fields for 'Alias', 'Nom', and 'Nom de famille'. An 'Appliquer' button is at the bottom right of the form. Below the form, there's a table listing existing users:

<input type="checkbox"/>	Alias ▲	Prénom	Nom de famille	Type d'utilisateur	Groupes
<input type="checkbox"/>	Admin	Zabbix	Administrator	Super Administrateur Zabbix	Zabbix administrators
<input type="checkbox"/>	adm_h.desouza			Utilisateur Zabbix	Zabbix administrators
<input type="checkbox"/>	adm_j.alba			Utilisateur Zabbix	Zabbix administrators
<input type="checkbox"/>	guest			Utilisateur Zabbix	Disabled, Guests

At the bottom, there's a status bar showing '0 sélectionné' and buttons for 'Débloquer' and 'Supprimer'.

- Paramétrage des hôtes :

On crée des « **templates** » ou modèles d'administration sur lesquels on sélectionne le type d'OS utilisé, puis Zabbix déploie automatiquement l'agent dessus et la remontée des informations se fait via le protocole SNMP.

Groupes d'hôtes: Templates ✕ Zabbix servers ✕ Discovered hosts ✕ Templates/Network devices ✕ taper ici pour rechercher Sélectionner

IP:

DNS:

Port:

Sévérité: ☐ Non classé ☐ Avertissement ☐ Haut ☐ Information ☐ Moyen ☐ Désastre

Appliquer Réinitialiser

Nom ▲	Interface	Disponibilité	Tags	Problèmes	État
CLIENT2	192.168.10.3: 10050	ZBX SNMP JMX IPMI		6	Activé
PFSense	192.168.10.254: 10050	ZBX SNMP JMX IPMI			Activé
Srv-Backup	192.168.10.206: 10050	ZBX SNMP JMX IPMI		2	Activé
Switch 1	192.168.10.200: 161	ZBX SNMP JMX IPMI			Activé
Switch 2	192.168.10.201: 161	ZBX SNMP JMX IPMI		1	Activé
Switch 3	192.168.10.202: 161	ZBX SNMP JMX IPMI			Activé
WS19-1	192.168.10.193: 10050	ZBX SNMP JMX IPMI		19 1	Activé
Zabbix server	127.0.0.1: 10050	ZBX SNMP JMX IPMI		1	Activé

- Création de la règle de « découverte » du réseau local :

Utilise un système de polling sur la plage d'adresse IP 192.168.10.0/24 pour découvrir les potentiels machines/équipements susceptibles d'être supervisés.

Règle de découverte: Réseau Local ✕ taper ici pour rechercher Sélectionner

Appliquer Réinitialiser

Équipement découvert ▲	Hôte surveillé	Temps de fonctionn
Réseau Local (15 équipements)		
192.168.10.3 (CLIENT2)	CLIENT2	00:02:10
192.168.10.126 (pfsense.domaine.lpr)		7 jours, 00:48:51
192.168.10.190 (pfsense.domaine.lpr)		7 jours, 00:38:21
192.168.10.193 (WS19-1.domaine.lpr)	WS19-1	21 jours, 02:20:19
192.168.10.194 (SRV-Intranet)		20 jours, 23:51:03
192.168.10.195 (CLIENT2)		7 jours, 01:42:20
192.168.10.199 (SRV-Antivirus)		6 jours, 23:40:59
192.168.10.200	Switch 1	6 jours, 23:40:57
192.168.10.201 (Switch2)	Switch 2	27 jours, 21:29:14
192.168.10.202	Switch 3	6 jours, 22:42:41
192.168.10.204 (Acer-Swift-3)		20 jours, 23:50:10
192.168.10.205 (zabbix.domaine.lpr)		27 jours, 21:28:32
192.168.10.206 (truenas)	Srv-Backup	21 jours, 00:47:04
192.168.10.207		20 jours, 23:49:58
192.168.10.254 (pfsense.domaine.lpr)	PFSense	21 jours, 01:40:46

- Exemple d'état de supervision des machines selon plusieurs vues :

o Générale :

<input type="checkbox"/> Nom ▲	Applications	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité	Chiffrement
<input type="checkbox"/> CLIENT2	Applications 22	Éléments 172	Déclencheurs 105	Graphiques 37	Découverte 4	Web 192.168.10.3:10050			Template OS Windows by Zabbix agent (Template Module Windows CPU by Zabbix agent, Template Module Windows filesystems by Zabbix agent, Template Module Windows generic by Zabbix agent, Template Module Windows memory by Zabbix agent, Template Module Windows network by Zabbix agent, Template Module Windows physical disks by Zabbix agent, Template Module Windows services by Zabbix agent, Template Module Zabbix agent)	Activé	20% SNMP JMX PMU	AUCUN
<input type="checkbox"/> PFSense	Applications 11	Éléments 70	Déclencheurs 16	Graphiques 22	Découverte 2	Web 192.168.10.254:10050			Template OS FreeBSD (Template Module Zabbix agent)	Activé	20% SNMP JMX PMU	AUCUN
<input type="checkbox"/> Srv-Backup	Applications 32	Éléments 138	Déclencheurs 95	Graphiques 29	Découverte 3	Web 192.168.10.205:10050			Template OS Linux by Zabbix agent (Template Module Linux block devices by Zabbix agent, Template Module Linux CPU by Zabbix agent, Template Module Linux filesystems by Zabbix agent, Template Module Linux generic by Zabbix agent, Template Module Linux memory by Zabbix agent, Template Module Linux network interfaces by Zabbix agent, Template Module Zabbix agent)	Activé	20% SNMP JMX PMU	AUCUN
<input type="checkbox"/> Switch 1	Applications 9	Éléments 14	Déclencheurs 9	Graphiques 1	Découverte 8	Web 192.168.10.200:161			Template Net HP Enterprise Switch SNMP (Template Module EtherLike-MIB SNMP, Template Module Generic SNMP, Template Module Interfaces SNMP)	Activé	20% SNMP JMX PMU	AUCUN
<input type="checkbox"/> Switch 2	Applications 33	Éléments 236	Déclencheurs 109	Graphiques 25	Découverte 8	Web 192.168.10.201:161			Template Net HP Enterprise Switch SNMP (Template Module EtherLike-MIB SNMP, Template Module Generic SNMP, Template Module Interfaces SNMP)	Activé	20% SNMP JMX PMU	AUCUN
<input type="checkbox"/> Switch 3	Applications 9	Éléments 14	Déclencheurs 9	Graphiques 1	Découverte 8	Web 192.168.10.202:161			Template Net HP Enterprise Switch SNMP (Template Module EtherLike-MIB SNMP, Template Module Generic SNMP, Template Module Interfaces SNMP)	Activé	20% SNMP JMX PMU	AUCUN
<input type="checkbox"/> WS19-1	Applications 22	Éléments 198	Déclencheurs 132	Graphiques 37	Découverte 4	Web 192.168.10.193:10050			Template OS Windows by Zabbix agent (Template Module Windows CPU by Zabbix agent, Template Module Windows filesystems by Zabbix agent, Template Module Windows generic by Zabbix agent, Template Module Windows memory by Zabbix agent, Template Module Windows network by Zabbix agent, Template Module Windows physical disks by Zabbix agent, Template Module Windows services by Zabbix agent, Template Module Zabbix agent)	Activé	20% SNMP JMX PMU	AUCUN
<input type="checkbox"/> Zabbix server	Applications 17	Éléments 127	Déclencheurs 58	Graphiques 25	Découverte 3	Web 127.0.0.1:10050			Template App Zabbix Server, Template OS Linux by Zabbix agent (Template Module Linux block devices by Zabbix agent, Template Module Linux CPU by Zabbix agent, Template Module Linux filesystems by Zabbix agent, Template Module Linux generic by Zabbix agent, Template Module Linux memory by Zabbix agent, Template Module Linux network interfaces by Zabbix agent, Template Module Zabbix agent)	Activé	20% SNMP JMX PMU	AUCUN

o détaillée (sur un hôte en particulier) :

Hôtes

Switch 2 ✕

taper ici pour rechercher

Sélectionner

Afficher les éléments sans donnée ☒

Application

Sélectionner

Afficher les détails ☐

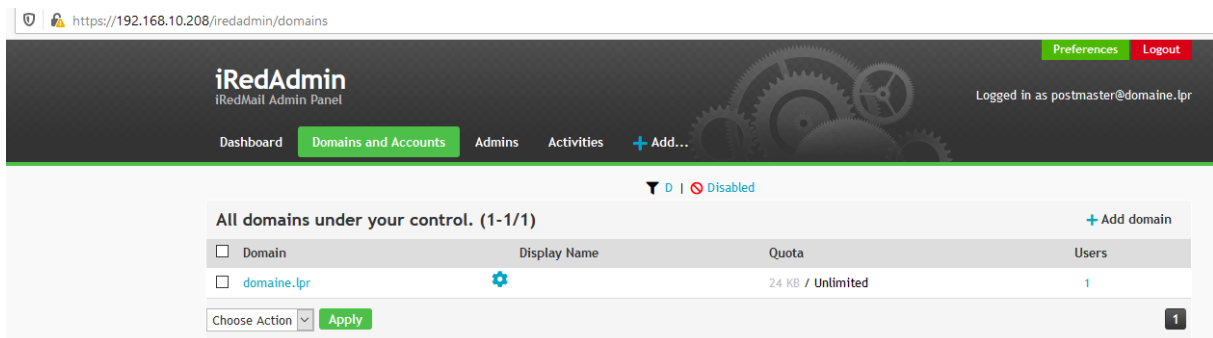
Appliquer
Réinitialiser

3.3.3.2.2) Serveur de Mails

SOGo est un collecticiel (ou **serveur** collaboratif) libre dont l'architecture est axée sur l'extensibilité (en anglais : « scalability ») qui permet son utilisation simultanée par des dizaines de milliers d'utilisateurs.

Le choix de ce système d'exploitation a été fait car il possède des avantages indéniables : OpenSource, boîte mail en version Web pour un accès distant, nombreuses fonctionnalités (redirection de mails, filtres, réponses automatiques...)

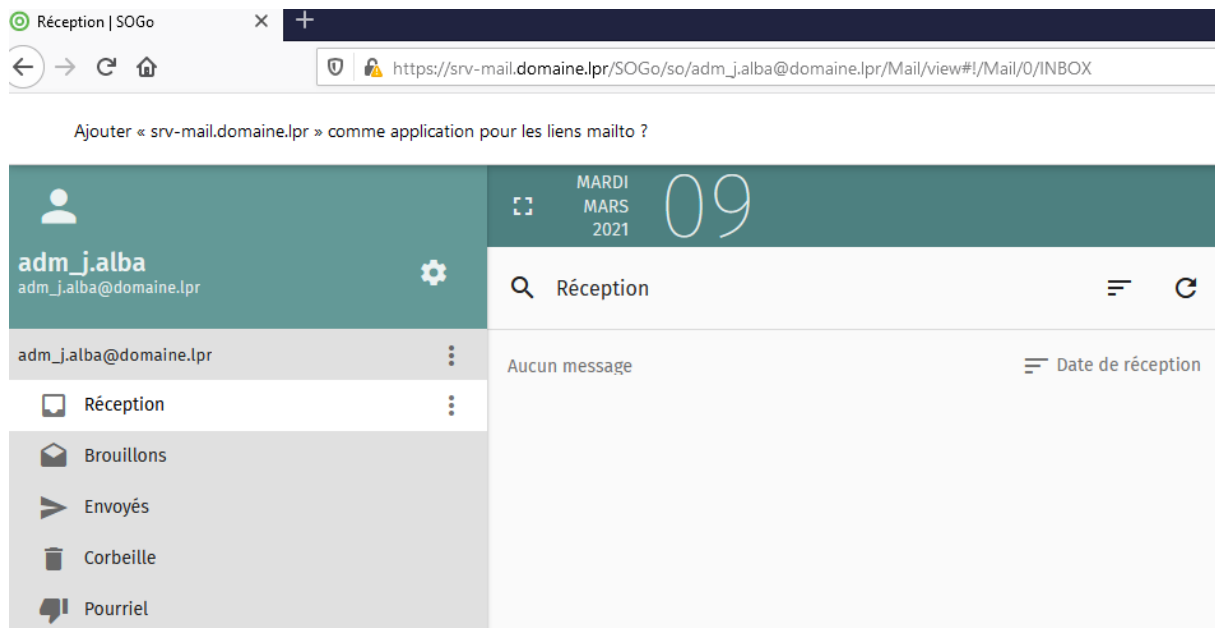
- Paramétrage de la synchronisation avec l'AD :



Une fois l'AD synchronisé avec le serveur de mails, l'utilisation d'une boîte mail en interface « Web » est disponible en utilisant ses login/mdp de connexion du domaine.



- **Résumé de l'interface utilisateur :**



3.3.3.2.3) Serveur Applications Métiers

La machine virtuelle a été créée. Un OS type Windows Serveur 2019 a été installé mais non utilisé car elle ne fait pas l'objet d'un accord avec la mairie pour traiter ce point.

3.3.3.2.4) Serveur Web

Joomla! est un système de gestion de contenu libre. Il est écrit en PHP et utilise une base de données MySQL. Joomla! est sous licence GNU GPL

Le choix de ce système d'exploitation a été fait car il possède des avantages indéniables : OpenSource, nombreuses fonctionnalités (flux RSS, news, version imprimable des pages, blogs, sondages, recherches...)

- **Résumé du serveur :**

Accueil

192.168.10.194

Intranet

Recherche...

Accueil

Comment débuter ?

Joomla

La création d'un site web avec Joomla est simple, le déploiement de ce site exemple vous y aidera. Les quelques principes de base présentés ci-dessous vous guideront dans la compréhension de ce logiciel.

Qu'est-ce qu'un Système de Gestion de Contenu ?

Un système de gestion de contenu (SGC ou CMS de l'anglais Content Management System) est un logiciel qui vous permet de créer et gérer des pages Web facilement, séparant la création des contenus de la gestion technique nécessaire à une diffusion sur le web.

Le contenu rédactionnel est stocké et restitué par une base de données, l'aspect (police, taille, couleur, emplacement, etc.) est géré par un template (habillage du site). Le logiciel Joomla permet d'unir ces deux structures de manière conviviale et de les rendre accessibles au plus grand nombre d'utilisateurs.

Deux interfaces

Un site Joomla est structuré en deux parties distinctes : la partie visible du site appelée «Frontal» de *Frontend* en anglais et, la partie d'administration pure appelée «Administration» de *Administrator*.

Tags populaires

- Joomla

Derniers articles

- Comment débuter ?

Menu utilisateur

- Votre profil
- Créer un article
- Administration
- Paramètres du template
- Paramètres du site

Connexion

Bonjour, Super Utilisateur

Déconnexion

- **Interface d'administration des menus et autres fonctionnalités :**

← → ↺ 🏠 192.168.10.194/administrator/index.php

Système ▾ Utilisateurs ▾ Menus ▾ Contenu ▾ Composants ▾ Extensions ▾ Aide ▾

🏠 Panneau d'administration

Joomla 3.9.25 est disponible : Mettre à jour

1 Mise(s) à jour d'extension disponible(s) Afficher les mises à jour

Joomla! aimerait obtenir votre permission pour recueillir des statistiques de base.

Afin de mieux comprendre les environnements d'installation et d'utilisation finale, il est utile d'envoyer certaines informations concernant le site vers un serveur central contrôlé par Joomla!. Aucune donnée n'est envoyée à partir de Plug-ins => Système - Statistiques Joomla!. [Cliquer ici pour voir les informations qui seront envoyées.](#)

Activer les statistiques Joomla ?

Toujours Une seule fois Jamais

CONTENU

- Ajouter un article
- Articles
- Catégories
- Médias

STRUCTURE

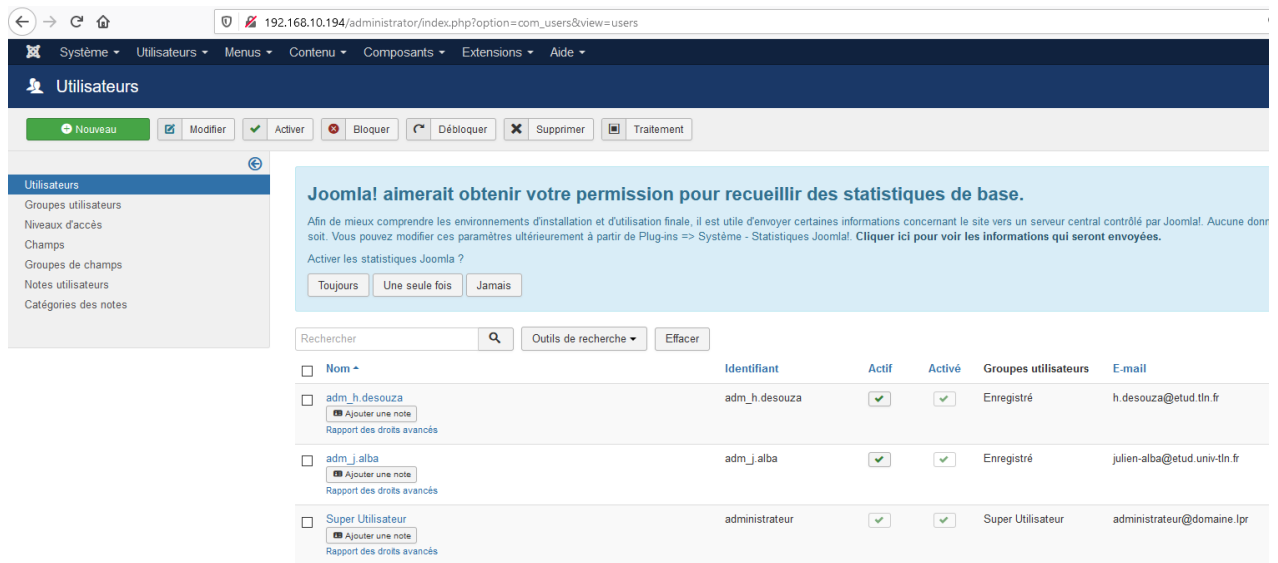
Des messages de post-installation sont disponibles

Des messages de post-installation importants requièrent votre attention.

Cet espace d'information n'apparaît pas lorsque vous avez caché tous les messages.

Consulter les messages

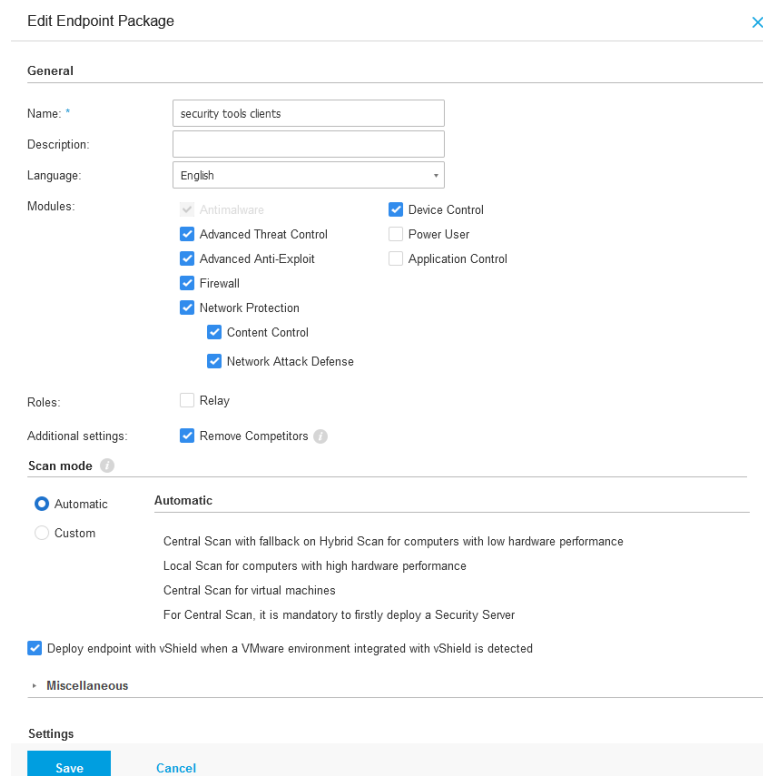
- Création des comptes administrateurs nominatifs :



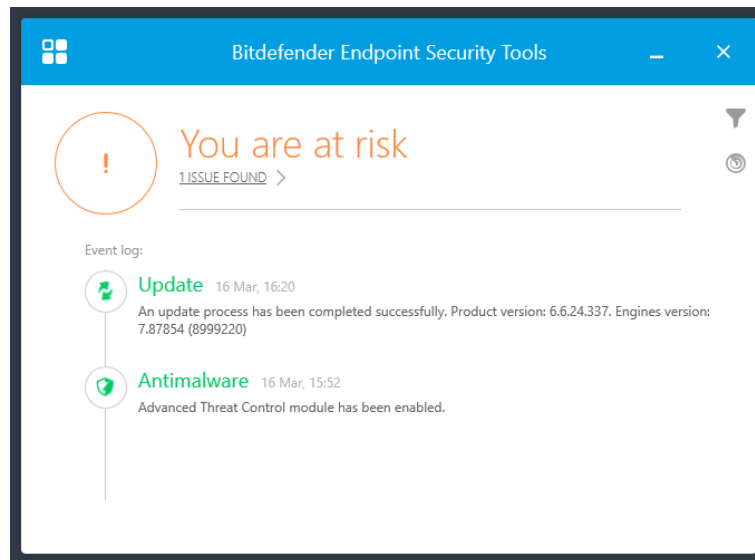
3.3.3.2.5) Serveur Anti-Virus

Le déploiement a consisté en plusieurs étapes :

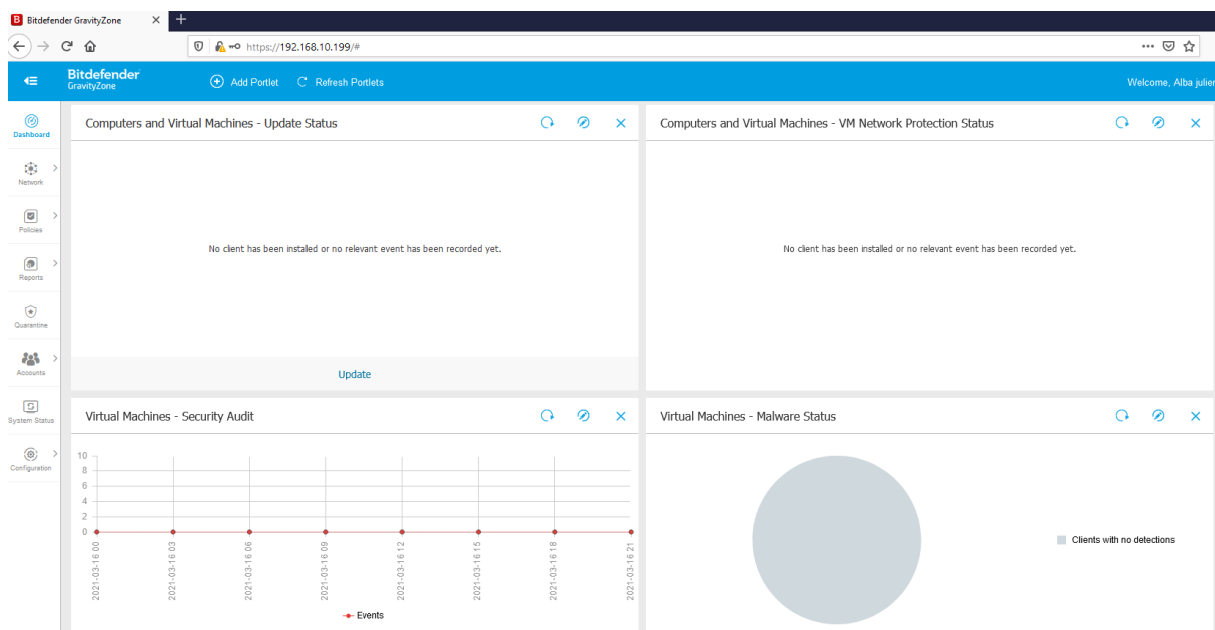
- Création d'une machine virtuelle sous HYPER-V,
- Installation du serveur Anti-Virus,
- Configuration de l'interface Web,
- Création des packages d'installation des agents



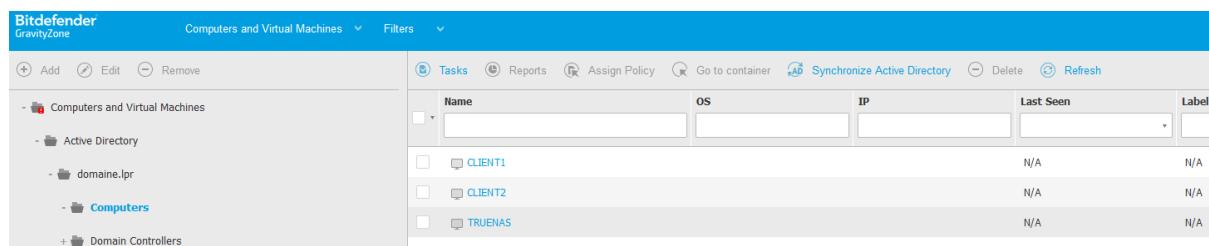
- **Déploiement des agents**



- **Supervision des équipements**



- la remontée des équipements grâce au déploiement des packages sur les clients



- la bonne configuration de synchronisation de l'AD

Bitdefender GravityZone

Mail Server Miscellaneous Proxy Backup **Active Directory** Virtualization Providers

Domains Access permissions

< Back | Edit Active Directory Domain

Credentials:

Domain:* domaine.lpr

User:* Administrateur

Password:* Type the password

Check credentials

Synchronization interval (hours): 1

Domain Controllers

Select a preferred domain controller to use for synchronization. If selecting multiple domain controllers, Gr

	Order
<input checked="" type="checkbox"/> Discovered Domain Controllers	
<input checked="" type="checkbox"/> WS19-1.domaine.lpr	⬆ ⬇

La solution Anti-Virus a été livrée à la mairie de Signes fonctionnelle et opérationnelle. Etant donné que la prise en main du serveur Anti-Virus s'est faite très simplement, il n'a pas été nécessaire de rajouter d'informations supplémentaires.

Dû à des problèmes de remontée des agents sur les équipements distants, la supervision de l'appliance GravityZone est donc faussée.

3.3.4) Machines Physiques

3.3.4.1) Client

Le PC Client mis en place dans l'architecture de test est un PC de configuration identique à celles retrouvées sur les postes de la Mairie de Signes, à savoir équipé de Windows Professionnal 2019.

3.3.4.2) Station Blanche

Conformément aux souhaits formulés par le responsable informatique de la mairie de Signes, le projet de station blanche a été créé sur Github en construisant une image .iso à l'aide d'une Debian 9 stretch et de l'anti-virus ClamAV :

Utilisation de la station blanche :

- Au boot sur la clé USB d'installation, celle-ci sera entièrement automatique jusqu'à l'extinction de la machine. L'installation doit se faire sur une machine connectée à Internet.

Caractéristiques techniques :

- Utilitaire antivirscan réalisant le scan d'une clé usb connectée à la machine
- Utilisation de l'antivirus Clamav, mise à jour des définitions de virus toutes les heures
- **Logs des analyses :** /var/log/antivirscan
- **Fichiers en quarantaine :** /var/lib/antivirscan/quarantine

Partie 4 : Mise en place du contexte de Sécurité

4.1) Protection pro-active

4.1.1) Formation à la CYBERDEFENSE

La société FUTURZO, dont les membres ont suivi une licence professionnelle à l'Université de Toulon, ont été formés à l'aide de modules disponibles sur le site du gouvernement.

C'est une formation en matière de Cyberdéfense idéale en lien avec le souhait de la mairie de Signes qui sera dispensée par les experts réseaux de FUTURZO.

Cette formation est indexée en **annexe 11.**

4.1.2) Fiches-réflexes

La société FUTURZO a élaboré un panel de fiches-réflexe nécessaires à la bonne application d'une hygiène numérique saine au sein de la mairie de Signes.

Ces documents concernent l'ensemble des utilisateurs et seront affichés dans les locaux techniques ainsi que dans les locaux de travail de la mairie.

Ces fiches-réflexes sont indexées en **annexe 12** et **annexe 13.**

4.1.3) Mémento Utilisateur

La société FUTURZO a élaboré un mémento d'utilisation des systèmes d'information en lien avec le souhait de la mairie de Signes.

Ce mémento est indexé en **annexe 14.**

4.1.4) Sensibilisation à la CYBERDEFENSE

La société FUTURZO, dont les membres ont suivi une licence professionnelle à l'Université de Toulon, ont été formés à l'aide de modules disponibles sur le site du gouvernement.

Comme la mairie de Signes désirait une protection pro-active, les experts réseaux, eux-mêmes formés en matière de Cyberdéfense, ont proposé de dispenser une sensibilisation gratuite et idéale en lien avec le souhait de la mairie de Signes.

Cette sensibilisation est indexée en **annexe 15.**

4.2) Protection Active du Réseau et des Systèmes

4.2.1) Solution Anti-virus

Afin de déterminer quelle solution anti-virus serait la plus appropriée pour un déploiement au sein de la mairie de Signes, la société FUTURZO a tout d'abord recensé les souhaits du responsable informatique, à savoir :

- Une solution fiable,
- Administrable à distance,
- Une maintenance relativement facile,
- Un système de supervision des machines surveillées,

Suite à cette discussion, la société FUTURZO a proposé l'appliance GravityZone de BitDefender qu'elle utilisait au sein de son entreprise.

C'est une solution de confiance, sûre et techniquement très accessible du fait de la sobriété de son interface.

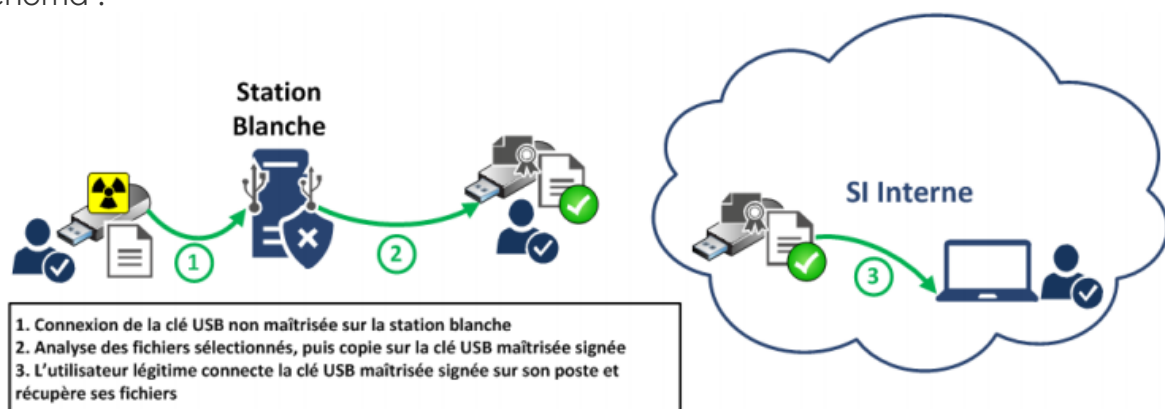
Les mises à jour de l'appliance sont réalisées directement depuis l'interface Web (pas besoin de télécharger des patches de mises à niveau).

4.2.2) Station Blanche

Dans le cadre de la mise en place d'un contexte de la SSI à la mairie de Signes, la société d'expertise FUTURZO a ainsi mis en place une station blanche.

La station, dédiée à l'analyse antimalware des médias amovibles et des données qui y sont stockés, donne des garanties raisonnables quant à l'innocuité du média amovible et des données transférées vers le réseau opérationnel.

C'est une solution d'analyse et de décontamination autonome et c'est pour cela que la solution d'intégration de cette machine a été choisie, comme le montre ce schéma :



Partie 5 : Suivi de la mise en production

5.1) Livraison du produit final

La société FUTURZO s'est engagée à livrer le réseau nouvellement déployé ainsi que le contexte de sécurité associé en bonne et due forme au plus tard le 23/03/2021. Elle conservera l'ensemble des documentations techniques ainsi que son architecture de test (VM).

Les données spécifiques à la mairie de Signes seront conservées durant la durée du contrat de maintenance.

Cela comprendra :

- l'architecture physique,
- l'architecture logique,
- les systèmes déployés,
- les pièces administratives,
- les procédures d'administration, de sauvegarde et de restauration.

Le trousseau de mots de passe liés aux différents équipements et systèmes, disponible en **annexe 16**, (à ouvrir avec l'application « **KeyPass** », logiciel permettant la création, génération et stockage de mots de passe pour différentes utilisations) sera livré également le jour de la présentation du projet ainsi que le « **Master Password** » au responsable informatique de la mairie de Signes.

5.2) Retour d'expérience

La réunion des services qui présentera la nouvelle solution de déploiement réseau/sécurité ainsi que la charte informatique et les dates de formation au personnel communal aura lieu le 23/03/2021 après la présentation du projet final au Marie de Signes.

Julien et Hugo se relaieront pour la formation du personnel en charge de l'administration du réseau.

Les documentations techniques, ainsi que la procédure de désinfection et le complément au plan de reprise d'activité sont remis au responsable informatique

A la fin de la journée, la mairie devra fournir le procès-verbal de livraison conforme de la solution.

Un contrat de maintenance sera proposé à la mairie de Signes à l'issue.

La société FUTURZO s'appuiera au futur de cette expérience afin d' étoffer son « CV » en matière d'expertise et déploiement de réseaux sécurisés.

Cela fera l'objet d'offres de service via un site web et via des plates-formes dédiées à la communication afin d'augmenter sa notoriété et ses clients.

La société FUTURZO aura pris la peine de garantir la qualité des services par 1 mois de maintenance offerte à titre gracieux.

Annexes

SITES/SOURCES :

Partie II. Commutateur HP v1910 (smnet.fr)

GitHub - Crypt-On/Station-blanche: Image pour l'installation d'une station Linux Debian dédiée au scan antivirus de clé USB

<https://www.ssi.gouv.fr/>

<https://docs.netgate.com/pfsense/en/latest/>

<https://docs.iredmail.org/index.html>

<https://docs.microsoft.com/fr-fr/>

TUTORIEL | Chiffrer vos documents avec Veracrypt | CNIL