PROJET

WOOD2019.

CONCEPTION D'UNE INFRASTRUCTURE RÉSEAU ET SYSTÈME

M. Arthur MOREAU

M. Thomas SICAUD

M. Pierre-Axel JIMENES

LOT 2.

SOMMAIRE.

Tables des illustrations.

Tables des tableaux.

1. Introduction.

Ce document fait suite au lot 1 qui consistait à rédiger un cahier des charges. Il se concentre principalement sur la rédaction de la proposition de la solution. Il sera conçu pour répondre aux besoins exprimés par l'entreprise dans ses objectifs de refonte du système d'information système et réseau.

La première phase du projet vise à la formalisation de la réponse aux besoins.

Par conséquent, le groupe WOOD a décidé d'adresser un appel d'offres aux professionnels pouvant mettre en forme la demande.

À partir de maintenant, nous deviendrons le nouvel acteur à la maitrise d'œuvre de ce projet. Pour ce faire, nous avons créé une entreprise fictive nommée : « VALORANT CORP. ». Une entreprise experte dans la conception d'infrastructure systèmes et réseaux pour répondre aux besoins de l'épreuve.

2. Présentation de l'entreprise.

2.1 L'entreprise « VALORANT Corp »

Fondée à Angoulême en 2019 et bénéficiant déjà d'un chiffre d'affaires atteignant 4,143,326 €, « VALORANT Corp » est une entreprise experte dans la mise en œuvre d'infrastructure informatique système et réseau.

La société met en place des infrastructures modernes et sécurisées pour les entreprises. Elle accompagne également les professionnels dans la maintenance des infrastructures mises en place. L'entreprise peut suivre un projet du début jusqu'à la fin, c'est-à-dire de la rédaction du cahier des charges jusqu'à la mise en place d'une infrastructure informatique.

2.2 Les partenaires.

2.3 Contexte du projet.

Le groupe WOOD se trouve ralenti dans sa progression par un manque de clarté et de précision sur les projets informatiques. Depuis le renouvellement du parc informatique effectué en 2010, aucun projet de modernisation du système informatique n'a été mis en place.

Le groupe connaît actuellement une forte croissance de son chiffre d'affaires ; en conséquence le besoin d'expansion se fait ressentir. Pour la mener à bien, l'entreprise va mettre un point d'honneur crucial sur la modernisation de son système d'information.

L'entreprise avance dans l'optique d'apporter des corrections et de faire évoluer son système d'information afin de répondre aux objectifs stratégiques mis en place par la direction du groupe. Malheureusement, l'obsolescence du système actuel ne permet plus de faire face à l'accroissement des demandes.

Les points énumérés et détaillés ci-dessous ont un impact négatif sur le système d'information du groupe.

- Le vieillissement de l'infrastructure informatique peut provoquer des perturbations qui nécessitent une intervention des prestataires de service.
- La non-sauvegarde entraîne une perte répétée de données (fichiers et documents).
- Le manque de mise à jour des postes clients ainsi que des serveurs rend le système d'information de l'entreprise vulnérable aux attaques informatiques.
- Le manque de contrats de maintenance et les non-compétences internes conduisent à des facturations répétées des prestataires informatiques.
- Le groupe ne s'est pas concentré sur son logiciel antivirus et n'a pas de stratégie de prévention en réponse aux virus et aux attaques. Le site de Lille a été touché par plusieurs attaques virales type « Ransomware ». Le serveur de fichiers et 120 postes clients sur divers sites ont été touchés par ces attaques informatiques ce qui a causé 5 jours d'interruption sur le site.
- Le groupe ne gère aucune autorisation de partage sur le système de fichiers ce qui laisse un accès total à tous les utilisateurs.
- Le groupe n'a pas adopté de stratégie de responsabilité écologique pour son système d'information.
- L'obsolescence du système actuel ne permet plus de faire face aux flux de commande, entraînant une perte financière pour l'entreprise.

Pour donner suite à l'étude effectuée en amont par l'entreprise, le groupe fait ressortir les points suivants :

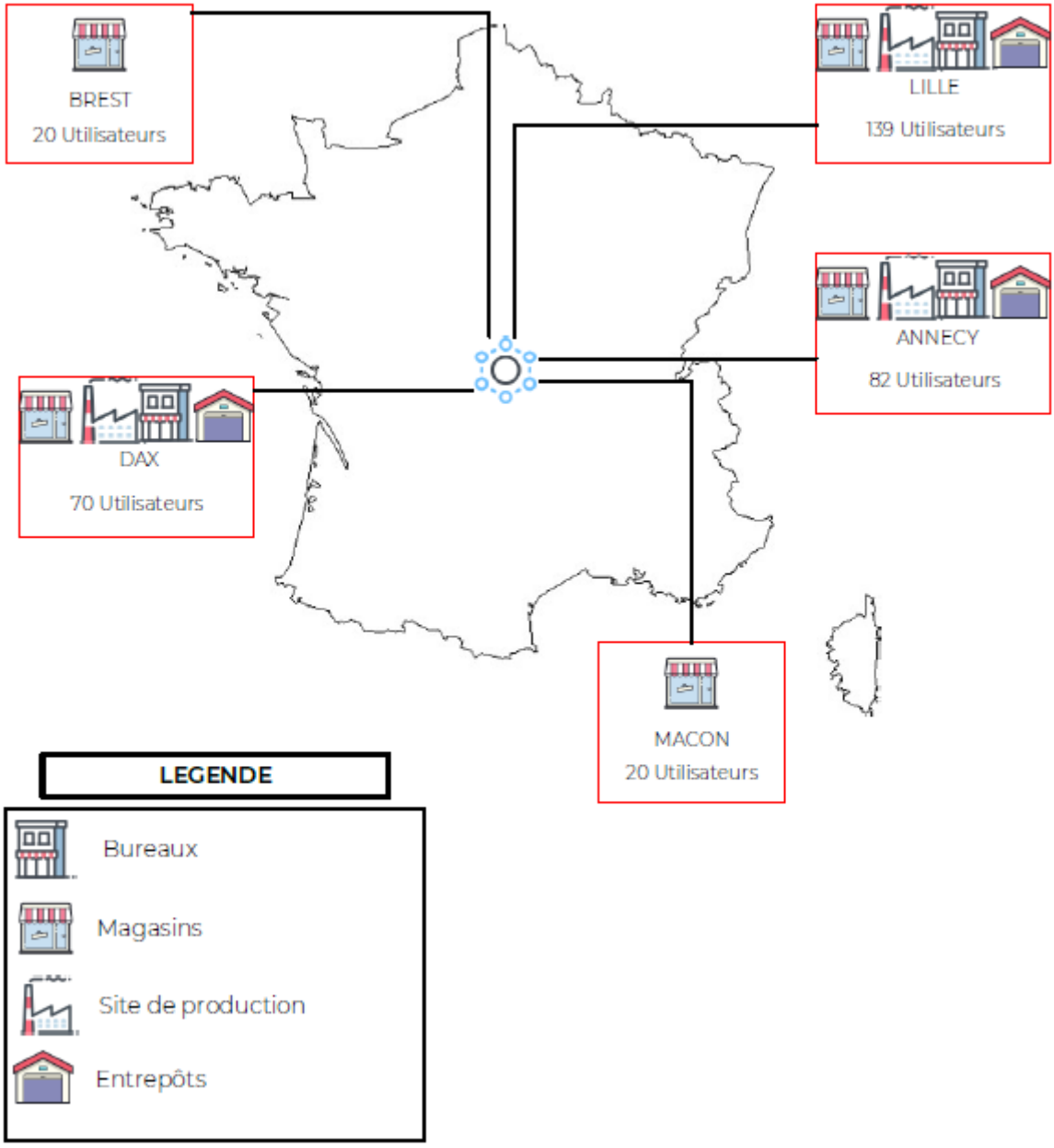
POINTS	CONSEQUENCES
Parc informatique veillissant	Pannes récurentes sur les systèmes informatique. Intervention de prestataire externe.
Sauvegarde non-opérationnel	Restauration des fichiers utilisateurs inexistance. PCA / PRA inexistant. Pertes de données.
Aucune mises à jours des postes clients et des serveurs	Vulnérabilité pour tous le système informatique
Aucun de contrat de maintenance	Facturation supplémentaire
Aucun antivirus mis en place dans la société	Pertes de données. Coûts pour la désinfection des PC et des Serveurs lors des attaques.
Aucun gestion des droits sur les serveurs de fichier.	Tous les utilisateurs disposes ont accès à tous les services.
Vieillisement du matériels informatique.	Basse performance du réseaux. Pannes intermittentes.

Les besoins fonctionnels ont été définis ci-dessous :

	Critère d'échange	Utilisation	Installation	Maintenance	Transport & Stockage
FP1 : Le système permet aux Internes l'échange de données	7				
FP2 : Le système permet aux Externes l'échange de données	7				
FP3 : Le système permet au Service Informatique de gérer l'accès aux données	7				
FP4 : Le système permet au Service Informatique de sécuriser les données	7				
FC1/FC14 : Le système ne doit pas interrompre la production	7/6				
FC2 : Le système doit être administrable par le Service Informatique	5				
FC3 : Le système doit résister à son environnement	2				
FC4 : Le système doit respecter les normes	3				
FC5/FC11 : Le système ne doit pas gêner les Internes	3/4				
FC6/FC12 : Le système ne doit pas gêner les Externes	3/4				
FC7 : Le système doit respecter les normes	3				
FC8 : Le système doit transférer les données	7				
FC9 : Le système doit réutiliser les données	6				
FC10 : Le système doit s'installer dans son environnement	4				
FC13 : Le système doit être administrable par les prestataires	1				
FC15 : Le système doit être acheminé dans son environnement	6				
FC16 : Le système doit sécuriser les données.	1				

3. Récapitulatif de l'existant.

3.1 Les sites et leurs interconnexions.



3.2 Inventaire des postes clients.

Le groupe WOOD a inventorié ses parcs informatiques, soit un total de 193 parc répartis sur les différents sites.

SITES.	PC FIXES.	PORTABLES.	STATIONS DE TRAVAIL.	MONITEURS.
· LILLE	33 - DELL OPTIPLEX 3010	65 - 14" DELL LATITUDE E5430		33 - DELL P170S
· DAX	11 - DELL OPTIPLEX 3010	20 - 14" DELL LATITUDE E5430	3 - DELL PRECISION T5500	3 - DELL ULTRASHARP U2410
· ANNECY	11 - DELL OPTIPLEX 3010	25 - 14" DELL LATITUDE E5430	15 - DELL PRECISION T5500	15 - DELL ULTRASHARP U2410
· BREST	5 - DELL OPTIPLEX 3010			5 - DELL P170S
· MACON	5 - DELL OPTIPLEX 3010			5 - DELL P170S

NOMBRE TOTAL DE POSTES	193

Configuration des postes clients :

	PC FIXES.	PORTABLES.	STATIONS DE TRAVAIL.
· PROCESSEURS	CORE I5 - 3470 3,20 GHz	CORE I5 - 3470 2,50 GHz	Xeon 65620 QuadCore 2,40 GHz
· MÉMOIRE RAM	4 Go	4 Go	6 Go
· CAPACITE DE STOCKAGE	500 Go - HDD	500 Go - HDD	2 To - HDD

3.3 Inventaire des serveurs.

SITES	SERVEURS	ROLES	SYSTÈME D'EXPLOITATION
LILLE	1 Serveur DELL POWEREDGE T310	Active Directory, Serveur DNS, Serveur d'impression.	Windows Server 2008
	1 Serveur DELL POWEREDGE T310	Serveur de messagerie	Linux Mandrake 6.1
	1 Serveur DELL POWEREDGE T310	Stockages de fichiers	Windows Server 2008
DAX	1 Serveur DELL POWEREDGE T310	Active Directory, Serveur DNS, Serveur d'impression.	Windows Server 2008
	1 Serveur DELL POWEREDGE T310	Stockages de fichiers	Windows Server 2008
	1 Serveur DELL POWEREDGE T310	Stockages de fichiers	Windows Server 2008
ANNECY	1 Serveur DELL POWEREDGE T310	Active Directory, Serveur DNS, Serveur d'impression.	Windows Server 2008
	1 Nas NETGEAR READYNAS ULTRA	Stockages de fichiers	

Configuration des serveurs :

	SERVEUR DELL POWEREDGE T310	NAS NETGEAR READYNAS ULTRA
· PROCESSEURS	Intel Xeon X3450	Intel Atom
· MÉMOIRE RAM	8 Go	1Go DDR3
· CAPACITE DE STOCKAGE	5x500Go en raid 5	2x500Go en raid 1

3.4 La charte de nommage.

Pour les besoins d'identification mais également pour faciliter les interventions lors d'incidents sur le parc, nous proposons de mettre en place une charte de nommage qui permettra l'identification du matériel en fonction des lieux et caractéristiques définis par la charte.

Charte de nomage serveurs				
Exemple :	16ASPAD02			
Département	Batiment	erveur physique / virtu	Service / fonction	Identifiant
00	X	XX	XX	0
16	A	SP	AD	2
Charente	Batiment A	Serveur Physique	Active Directory	numéro 02

Translation	
Serveur Physique / Virtuel	
SV	Serveur Virtuel
SP	Serveur physique
HV	Hyperviseur
Service / Fonction	
AD	Active directory
HV	Hyperviseur
ST	Stockage
DN	DNS
ML	MAIL

Charte de nomage PC				
Exemple:	16APCDG002			
Département	Batiment	Format	Fonction	Identifiant
00	X	XX	XX	000
16	A	PC	DG	002
Charente	Batiment A	PC fixe	Directeur Général	numéro 002

Translation	
Format	
PC	PC fixe
PT	Portable

Fonction	
DG	Directeur Général
DR	Direction des ressources
DC	Direction Commerciale
DP	Direction de production
RH	REssources Humaines
SC	Service Compta
SJ	Service Juridique
SA	Service Administratif
SI	Service Informatique
BP	Buisiness Unit Particulier
BC	Business Unit Collectivités
BM	Buisiness Unit M Modulaire
MA	Magasin
PP	Production Particuliers
PC	Prodcution Collectivités
PM	Production M Modulaire
IP	Installation Particuliers
IC	Installation Collectivités
IM	Installatim M Modulaire

Charte de nomage Actifs réseaux / système

Exemple : 59ASWC03

Département	Batiment	Matériel	Particularité	Identifiant
00	X	XX	X	00
16	A	Sw	C	03
Charente	Batiment A	Switch	Coeur réseau	numéro 03

Translation :

Ville	Département
Lille	59
Brest	29
Macon	71
Dax	40
Annecy	74

Matériel	
Switch	SW
Borne wifi	Wi
FireWall	FW
Imprimantes	IM

Particularité	
Coeur de réseau	C
Distribution	D
Commutation	A

3.5 L'adressage IP.

Site de Lille.

Site Lille						
	VLAN	TYPES	NOMBRE UTILISATEURS	PLAGES ADRESSES	MASQUES	NOMBRE ADRESSES
LILLE Plage totale 10.59.0.0/17	10	CLIENTS	139	de 10.59.10.1 à 10.59.10.254 / 24	255.255.255.0	254
	20	WIFI INVITE	30	de 10.59.20.1 à 10.59.20.30 / 27	255.255.255.224	30
	30	VOIP	75	de 10.59.30.1 à 10.59.30.126 /24	255.255.255.0	254
	40	SERVEUR	17	de 10.59.40.1 à 10.59.40.255 /24	255.255.255.0	254
	50	MANAGEMENT	52	de 10.59.50.1 à 10.59.50.62 /26	255.255.255.192	92
	60	DMZ	6	de 10.59.60.01 à 10.59.60.14/28	255.255.255.240	14

Site d'Annecy.

Site Annecy						
Ville et réseau	VLAN	TYPES	NOMBRE UTILISATEURS	PLAGES ADRESSES	MASQUES	NOMBRE ADRESSES
ANNECY Plage totale 10.59.0.0/17	10	CLIENTS	147	de 10.74.10.1 à 10.74.10.254 / 24	255.255.255.0	254
	20	WIFI INVITE	30	de 10.74.20.1 à 10.74.20.30 / 27	255.255.255.224	30
	30	VOIP	57	de 10.74.30.1 à 10.74.30.126 /25	255.255.255.128	126
	40	SERVEUR	10	de 10.74.40.1 à 10.74.40.255 /24	255.255.255.0	254
	50	MANAGEMENT	37	de 10.74.50.1 à 10.74.50.62 /26	255.255.255.192	62
	60	DMZ	6	de 10.74.60.1 à 10.74.60.14 /28	255.255.255.240	14

Site de Dax.

Site Dax						
Ville et réseau	VLAN	TYPES	NOMBRE UTILISATEURS	PLAGES D'ADRESSES	MASQUES	NOMBRE ADRESSES
DAX Plage totale 10.49.0.0/17	10	CLIENT	72	10.40.10.1 - 10.40.10.126/25	255.255.255.128	126
	20	WIFI INVITE	30	10.40.20.1 - 10.40.20.30/27	255.255.255.224	30
	30	VOIP	31	10.40.30.1 - 10.40.30.62/24	255.255.255.0	254
	40	SERVEUR	2	10.40.40.1 - 10.40.40.2/30	255.255.255.252	2
	50	MANAGEMENT	25	10.40.50.1 - 10.40.50.30/27	255.255.255.224	30

Site de Mâcon.

Site Macon						
Ville et réseau	VLAN	TYPES	NOMBRE UTILISATEURS	PLAGES D'ADRESSES	MASQUES	NOMBRE ADRESSES
MACON Plage totale 10.71.0.0/17	10	CLIENT	7	10.71.10.1 - 10.71.10.14/28	255.255.255.240	14
	20	WIFI GUEST	6	10.71.20.1 - 10.71.20.06/29	255.255.255.248	6
	30	VOIP	8	10.71.30.1 - 10.71.30.14/28	255.255.255.240	14
	40	SERVEUR	2	10.71.40.1 - 10.71.40.2/30	255.255.255.252	2
	50	MANAGEMENT	9	10.71.50.1 - 10.71.50.14/28	255.255.255.240	14

Site de Brest.

Site Brest						
Ville et réseau	VLAN	TYPES	NOMBRE UTILISATEURS	PLAGES D'ADRESSES	MASQUES	NOMBRE ADRESSES
BREST Plage totale 10.29.0.0/17	10	CLIENT	7	10.29.10.1 - 10.29.10.14/28	255.255.255.240	14
	20	WIFI GUEST	6	10.29.20.1 - 10.29.20.6/29	255.255.255.248	6
	30	VOIP	8	10.29.30.1 - 10.29.30.14/28	255.255.255.240	14
	40	SERVEUR	2	10.29.40.1 - 10.29.40.2/30	255.255.255.252	2
	50	MANAGEMENT	9	10.29.50.1 - 10.29.50.14/28	255.255.255.240	14

4. Solution WAN – Réseau étendu de l'entreprise.

Le WAN ou réseau étendu permet de connecter des machines au réseau local de l'entreprise « LAN » (Local Area Networks) sur une longue distance. Le WAN est utilisé pour connecter plusieurs sites entre eux.

Son fonctionnement est basé sur la technologie de liaison point à point, qui comprend la connexion entre un opérateur type SFR, BOUYGES, ORANGE et le réseau d'un client via des lignes louées. (Fil de cuivre, fibre optique). Cependant, cela nécessite également la présence de routeurs qui déterminent le meilleur itinéraire pour permettre de joindre le réseau.

Le WAN accorde aux entreprises la possibilité de centraliser ou d'externaliser leur infrastructure informatique plutôt que d'héberger des serveurs sur chaque site professionnel. Il leur permet également de maintenir une position importante dans la stratégie informatique. Par une amélioration des performances des applications métiers ainsi qu'une réduction des temps d'arrêt, il entraîne une augmentation de la productivité.

4.1 La connectivité de l'entreprise.

L'entreprise WOOD évolue et les besoins de connexion augmentent en conséquence. La numérisation des activités implique une grande réactivité et questionne quant à l'évaluation des besoins et des attentes.

En vue des évolutions de l'entreprise, il est nécessaire d'examiner les flux disponibles pour évaluer les besoins des débits.

Le partage de fichiers en entreprise.

Les échanges sont plus faciles que jamais. Il est possible de faire des envois de fichier de toute part ; que ce soit par courrier électronique, en téléchargeant des documents depuis un stockage qui se trouve sur le cloud ou bien en récupérant depuis un serveur FTP des informations clients internes à l'entreprise. Il est nécessaire que le débit soit cohérent vis-à-vis des besoins de chaque agent de l'entreprise. Chaque téléchargement ou envoi de fichier entraîne une augmentation des besoins en débit internet.

L’utilisation de la bande passante par le cloud.

Il nous semble que le premier exemple à prendre pour parler du Cloud et permettre une collaboration entre les différentes équipes dans l’entreprise est Microsoft 365. Il est important de noter que quel que soit l’action entreprise, celle-ci nécessite forcément une connexion internet pour interagir avec le Cloud.

L’utilisation de la vidéoconférence.

La vidéoconférence est une des activités les plus gourmandes car elle demande d’envoyer un flux important pour une qualité correcte d’envoi mais également pour la réception. Cela implique donc une bonne connexion internet, d’autant plus si plusieurs collaborateurs utilisent cette technologie régulièrement.

Les mises à jour logiciels.

Trop souvent oubliées, les mises à jour logiciel sont pourtant capitales. Dans une société connectée et en perpétuelle évolution, les développeurs mettent régulièrement leurs logiciels et applications à jour pour y inclure de nouvelles fonctions ou bien pour y apporter des corrections. Il est nécessaire de prendre en compte la récurrence de ces mises à jour logiciel au sein des entreprises. Le système d’exploitation fait des mises à jour régulièrement pour garantir une grande stabilité du système.

4.2 Étude de flux

Afin d'être le plus précis possible dans le choix de nos liaisons WAN ainsi que dans le choix de notre débit pour nos réseaux LAN, il est important de bien en définir les besoins.

Pour ce faire nous avons procédé à une étude des flux consommés par les différents services utilisés au sein de l'entreprise WOOD.

Flux	Services	Frequence	Volume
Messagerie	IMAP4/MAPI/SMTP	Elevé	Elevé
	ActiveSync	Bas	Bas
Téléphonie	SIP pour la voix	Elevé	Elevé
	SIP pour la vidéo	Bas	Elevé
Internet	HTTP	Elevé	Elevé
	HTTPS	Elevé	Elevé
	FTP	Elevé	Elevé
Réplication AD	RPC (Remote procedure call)	Quotidienne	Bas
Administration	SSH	Moyen	Moyen
	RDP	Elevé	Moyen
Supervision	SNMP	Elevé	Moyen
ERP	HTTPS	Elevé	Elevé
VPN	IPsec	Bas	Moyen
Données partagées	DFS	Quotidienne	Elevé
Déploiement	WDS/MDT	Bas	Bas
Mise à jour	WSUS	Moyen	Bas
Sauvegarde	VEEAM B&R	Quotidienne	Moyen
Helpdesk	GLPI	Quotidienne	Bas

4.3 Les offres des opérateurs :

Les opérateurs pour la connexion principale des sites :

1. **SFR Business : Connect Sécurisé : Accès Internet Fibre Très Haut Débit sécurisée**

   Nous avons choisi le produit SFR Business Connect Sécurisé pour fournir une connexion en fibre optique sur les sites de Lille, Annecy et Dax.

L'offre :

Solution d'accès Internet Fibre Optique Entreprise FTTO (Fiber To The Office), jusqu'à 1Gb/s symétrique, qui inclut la protection contre les Cyber Menaces grâce à un pare-feu de dernière génération, d'un anti-malware, et également d'une solution Anti DDoS intégrée.

Garantie de Temps de Rétablissement : GTR

L'offre bénéficie d'une Garantie de Temps de Rétablissement de 4h, du lundi au vendredi de 8h à 18h, incluse, ainsi qu'un lien de secours sur le réseau de SFR Business ou sur un réseau tiers : en cas de défection de l'accès principal.

Prix :

Le prix est de 390€ HT/mois soumis à un engagement minimum de 36 mois.

2. **SFR Business : Connect SDSL**

   Nous avons choisi le produit SFR Business Connect SDSL pour fournir une connexion secondaire en SDSL pour les sites de Brest et Mâcon.

L'offre :

Un débit symétrique de Connect SDSL 100% garanti, jusqu'à 8Mb/s.

Garantie de Temps de Rétablissement : GTR

L'offre bénéficie d'une Garantie de Temps de Rétablissement de 4h, du lundi au vendredi de 8h à 18h, incluse, ainsi qu'un lien de secours sur le réseau de SFR Business ou sur un réseau tiers : en cas de défection de l'accès principal.

Prix :

Le prix est de 150€ HT/mois.

Les opérateurs pour la connexion secondaire des sites :

1. **Orange Open Pro SDSL**

Afin de fournir une connexion secondaire en SDSL pour la totalité des sites, nous avons choisi l'offre Orange Open Pro SDSL.

L'offre :

Internet avec un débit Ethernet jusqu'à 100 Mbps en descendant et 300 Mbps en montant.

Garantie de Temps de Rétablissement : GTR

L'offre bénéficie d'une Garantie de Temps de Rétablissement de 8h, du lundi au vendredi de 8h à 18h, incluse.

Prix :

Le prix est de 69€ HT/mois avec engagement de 24mois.

2. SFR Business Box 4G+ Illimité

Nous avons choisi une box 4G+ de SFR Business, afin de pouvoir fournir une connexion de secours en 4G en cas de panne des connexions filaires sur le site de Lille.

L'offre :

Accès internet 4G/4G+ pouvant atteindre 220 Mbps.

Garantie de Temps de Rétablissement : GTR

L'offre bénéficie d'une Garantie de Temps de Rétablissement de 8h, du lundi au vendredi de 8h à 18h, incluse.

Prix :

Le prix est de 109€ HT/mois avec engagement de 24 mois.

4.4 Présentation de la solution XG Firewall

La solution choisie par l'équipe s'articule principalement autour du constructeur SOPHOS. Grâce à leurs modèles XG Firewall et RED, ils vont permettre une protection et un contrôle du réseau non négligeable pour les entreprises.

Déploiement de la solution

SOPHOS propose 4 types des déploiements possibles :

- Un déploiement matériel. Les appareils SOPHOS XG sont livrés et prêts à l'emploi.
- Un déploiement logiciel installé sur du matériel d'entreprise (nécessite d'être compatible INTEL)
- Un déploiement à l'aide d'une machine virtuel. Il est compatible VMware, Citrix, MS Hyper V et KVM.
- Un déploiement dans le cloud. Le pare-feu XG peut être déployé dans le cloud sur Azure et également AWS.

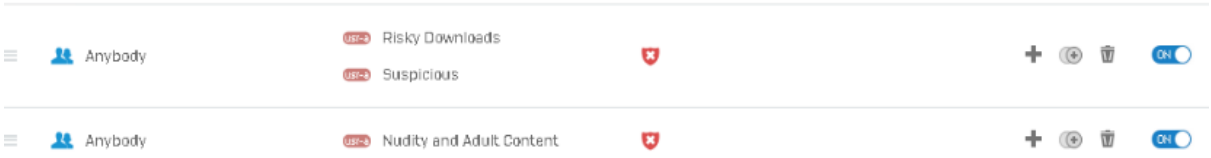
Quelque soit la façon dont la solution sera déployée et peu importe la forme choisie, il utilisera le même logiciel et fournira la même fonctionnalité.

Protection WEB

Le pare-feu SOPHOS XG a vocation à protéger en analysant le trafic HTTP et HTTPS à la recherche de contenu indésirable ou de logiciel malveillant.

Le filtrage web XG fournit des filtres prédéfinis qui bloquent automatiquement l'accès aux sites web catégorisé comme :

- Les sites de hasard
- Les sites pornographiques



On trouvera également une option contre le phishing qui empêche les utilisateurs d'être redirigés vers des sites contrefaits ou compromis.

Safe Search est une fonction de Google Search qui agit comme un système automatisé pour le filtrage de la pornographie et des contenus potentiellement offensants.

La fonction de protection du Web est personnalisable, par exemple en limitant le quota de navigation et l'accès des utilisateurs. Le temps permet de contrôler ce à quoi les utilisateurs peuvent avoir accès et à quel moment. Il est possible de restreindre les utilisateurs afin qu'ils ne puissent accéder qu'à des sites web qui sont essentiels à l'entreprise, ou encore d'imposer une restriction dans la politique web pour bloquer l'accès aux réseaux sociaux par exemple.

Protection COURRIEL

La protection du courrier électronique empêche les fuites de données à l'extérieur de l'organisation par email. Il est possible de créer des listes de contrôle des données (CCL).

Les CCLs sont basées sur des listes communes de contrôle financier et de contrôle de données. On peut retrouver dans ces listes communes des données personnelles, des numéros de carte de crédit ou même des adresses électroniques.

Lorsque le pare-feu XG trouve une correspondance pour les informations spécifiées, il applique une action spécifique.

La confiance 0 (Zéro Trust)

Zero Trust est un modèle de sécurité qui repose sur le principe qu'aucun utilisateur n'est totalement digne de confiance sur un réseau, et qu'on ne devrait pas permettre à des utilisateurs d'accéder à des ressources avant d'avoir vérifié leur légitimité et leur autorisation. Ce modèle met en place un « accès basé sur des droits minimums », permettant ainsi de restreindre l'accès des utilisateurs ou groupes d'utilisateurs uniquement aux ressources dont ils ont besoin et rien de plus.

À l'origine, le Zero Trust a été créé en réponse à l'augmentation exponentielle du nombre de travailleurs mobiles et distants, à la tendance du BYOD (Bring Your Own Device) et à la croissance rapide des services cloud. Si ces tendances ont été bénéfiques aux utilisateurs et ont apporté plus de flexibilité aux équipes informatiques, elles ont également réduit la capacité des entreprises à contrôler et à sécuriser l'accès aux données et aux ressources du réseau. Avec Zero Trust, les entreprises reprennent les rênes et renforcent leur sécurité, dans un contexte où le périmètre du réseau est en train de disparaître.

Les avantages du Zero Trust

La mise en place d'un modèle comme celui-ci permet de protéger les applications privées et les ressources du réseau, tout en réduisant considérablement les risques de comportements internes malveillants et de comptes compromis.

Cette solution offre les avantages suivants :

- Sécurisation efficace des accès des utilisateurs à distance.
- Protection des données sensibles et de la propriété intellectuelle
- Garantie d'une authentification robuste
- Mise en place d'une gouvernance efficace à l'accès aux ressources
- Réduction du potentiel de vulnérabilité.

4.5 Application au sein de notre système

Interconnexion des sites :

Afin d'interconnecter les différents sites du groupe WOOD, nous utiliserons des boîtiers SOPHOS SD-RED qui offrent une appliance gérée de façon centrale, couplés à un UTM central SOPHOS XG 230 Rev.2 ce qui va nous permettre de relier en toute sécurité les différents sites du groupe WOOD, tout en assurant un accès sécurisé à internet.

Les appliances SOPHOS SD-RED :

Dans notre schéma réseau, les appliances SOPHOS SD-RED seront installées sur les sites distants de Dax, Brest, Mâcon et Annecy. Les appliances seront gérées de façon centralisée par l'UTM Sophos installée sur le site de Lille.

L'appliance SOPHOS SD-RED (Remote Ethernet Device) est une solution réseau, conçue pour être simple à déployer. Son objectif premier est de fournir un tunnel sécurisé à partir de son emplacement principal jusqu'à un firewall SOPHOS UTM.

Les appliances SOPHOS SD-RED ne disposent pas d'interface utilisateur, elles sont conçues pour être entièrement configurées et gérées à partir d'un Sophos UTM.

Les fonctionnalités principales des appliances SD-RED :

Déploiement instantané de la protection :

Sophos SD-RED facilite l'extension du réseau sécurisé à d'autres sites. Il ne nécessite aucune compétence technique sur le site distant : il suffit de saisir l'identifiant de l'appareil dans la console XG Firewall puis de l'expédier. Dès que l'appareil est branché et connecté à Internet, il entre en contact avec le pare-feu et établit une connexion sécurisée via un tunnel VPN dédié. C'est aussi simple que cela.

Configuration souple :

Configurez les appareils SD-RED de manière que tout le trafic provenant du site distant soit acheminé vers le pare-feu, en contrôlant le DHCP et d'autres éléments du réseau distant. Il sera aussi possible de choisir d'acheminer uniquement le trafic entre les différents bureaux du réseau via le SD-RED, tout en assurant à distance un accès direct à Internet.

Chiffrement sécurisé, gestion centralisée :

Toutes les données transitant entre le SD-RED et le pare-feu Sophos sont chiffrées selon la norme AES-256, ce qui garantit une connexion sécurisée, inviolable et à l'épreuve du piratage. Grâce à la gestion centralisée de nos dernières séries XG, la protection est totalement transparente sur l'ensemble du réseau distribué et peut être personnalisée ou répliquée pour répondre à besoins spécifiques.

SD-WAN synchronisé,

Lorsqu'il est administré par XG Firewall, le SD-WAN synchronisé permet de bénéficier de la puissance de la Sécurité synchronisée et de l'intégration de XG Firewall avec Sophos Intercept X pour optimiser la sélection du chemin WAN pour les applications professionnelles importantes avec une fiabilité de 100 %.

Connectivité Wi-Fi et WAN souple :

En option, ajoutez un module Wi-Fi-5 ou 3G/4G pour fournir une connectivité aux clients sans fil ou pour utiliser des connexions Internet 3G/4G**.**

SD-WAN Remote Ethernet Devices:

Sophos SD-RED permet d'étendre la sécurité du réseau vers d'autres sites de manière simple et économique. Il n'exige aucune expertise sur le site distant : il suffit de saisir l'identifiant du boîtier SD-RED dans la console XG Firewall et de valider. Une fois branché et connecté à Internet, notre service le connecte automatiquement au pare-feu et établit une connexion sécurisée via un tunnel VPN dédié.

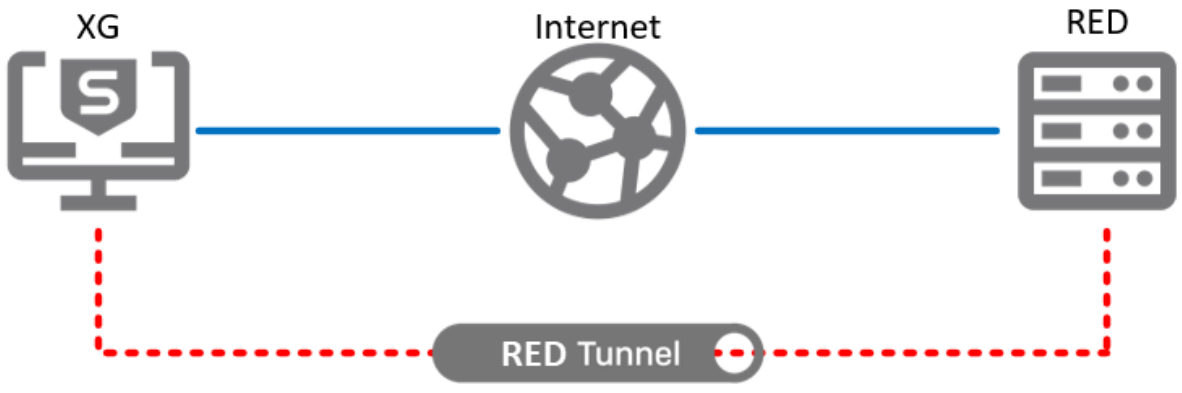
Les plus :

- Service automatique qui permet le déploiement par du personnel non spécialisé
- Sécuriser la connectivité du VPN avec XG Firewall de n'importe où
- Options de routage sélectif pour tout accès VPN et WAN local
- Chiffrement pour entreprise
- Les SD-RED répondent à une variété de besoins en matière de sites distants et de bande passante, et peuvent être complétés par une connectivité Wi-Fi ou 3G/4G à l'aide de modules optionnels ou en ajoutant des points d'accès de la série APX.

La solution SD-WAN permet de remplacer les connexions MPLS onéreuses par des connexions SD-WAN moins coûteuses. Le XG firewall intègre les fonctionnalités nécessaires pour activer et protéger la connectivité SD-WAN et pour atteindre les objectifs de continuité.

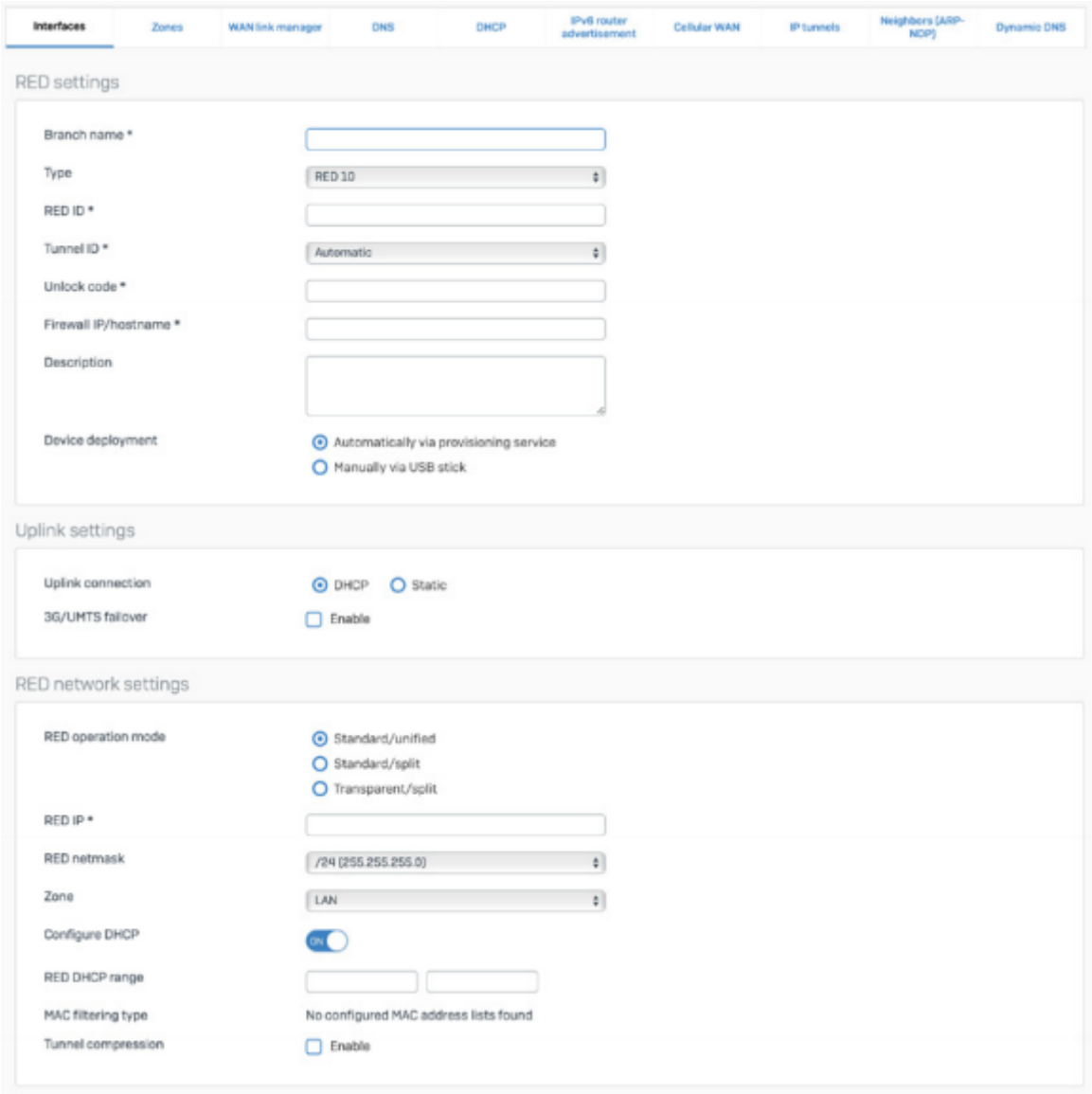
Le mode de fonctionnement :

RED peut fonctionner dans plusieurs modes. Ces scénarios font référence à deux appareils Sophos différents. L'un est l'appareil RED, qui se trouve à distance. L'autre est le Sophos XG Firewall avec lequel le RED établit un tunnel. Les deux ont une connexion à Internet, comme le montre la figure.



Le mode de déploiement :

Déployer des périphériques SD-RED n'a jamais été aussi simple : notez tout simplement le numéro de série du boîtier dans le pare-feu XG Firewall et expédiez-le au site destinataire. Une fois reçue par le site distant, l'installation n'exige aucune connaissance technique : le boîtier se connecte automatiquement au service d'approvisionnement Cloud pour établir un tunnel sécurisé avec XG Firewall.

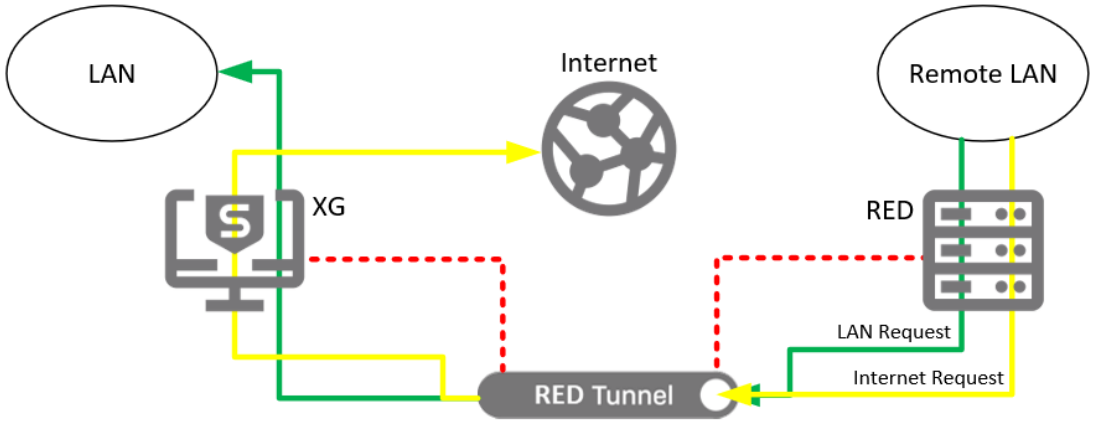


Au moment du déploiement d'un périphérique SOPHOS SD-RED, nous avons le choix parmi trois options de déploiement différentes :

- « Standard/Unified »
- « Standard/Split »
- « Transparent/Split »

Le mode « Standard/Unified » :

Standard / Unified est le mode couramment utilisé. Dans ce mode, nous nous attendons à ce que le réseau distant soit entièrement géré par le Sophos XG Firewall, via le SD-RED. Le DHCP peut être proposé pour le LAN distant par le pare-feu Sophos XG, et le SD-RED peut être le seul appareil connectant le LAN à Internet.



Le schéma illustre le flux de données dans ce mode de fonctionnement. Tout le trafic provenant du LAN distant passe par le tunnel RED, qu'il se dirige vers le LAN local ou Internet. Cela permet au Sophos XG Firewall d'autoriser ou de refuser les demandes de la même manière que pour le trafic provenant du LAN local.

Le trafic entre les réseaux locaux et distants peut être bloqué ou autorisé à l'aide de règles de pare-feu. Le trafic Web peut être filtré à l'aide du module de sécurité Web et des applications telles que Skype ou BitTorrent peuvent être contrôlées pour les utilisateurs LAN distants, tout comme elles peuvent l'être pour les utilisateurs LAN. Cela offre le plus haut niveau de sécurité et de gestion pour les réseaux distants.

Son principal inconvénient est l'augmentation des besoins en bande passante qu'il peut entraîner sur la liaison Internet du Sophos XG Firewall. Étant donné que tout le trafic Internet provenant du LAN distant utilise également la bande passante Internet du Sophos XG Firewall, la bande passante du Sophos XG Firewall doit être suffisamment grande pour répondre aux demandes de ses utilisateurs locaux et de tous les utilisateurs RED distants.

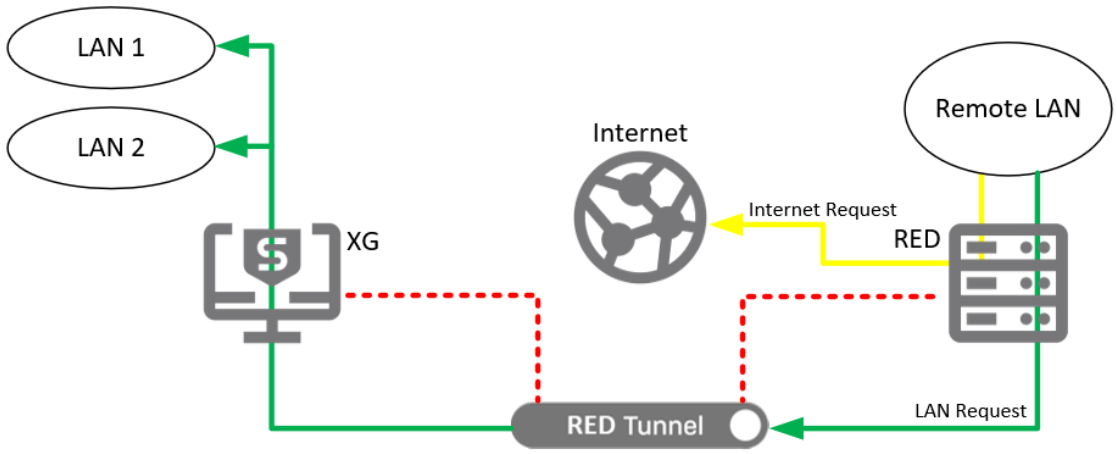
Le mode « Standard/Split » :

Le mode Standard / Split est physiquement similaire à Standard / Unified.

Nous nous attendons à ce que le réseau distant soit géré par le pare-feu Sophos XG et puisse fournir un DHCP au LAN distant. Le SD-RED étant le seul appareil entre le LAN et Internet, seul le trafic pour les réseaux sélectionnés est envoyé via le tunnel. Tout autre trafic est envoyé directement par la connexion Internet locale.

Le SD-RED masque le trafic sortant pour atteindre son adresse IP publique. Cette fonctionnalité minimise l'utilisation de la bande passante sur le tunnel et allège les exigences de bande passante sur le pare-feu Sophos XG, mais elle réduit également considérablement la gérabilité du réseau distant.

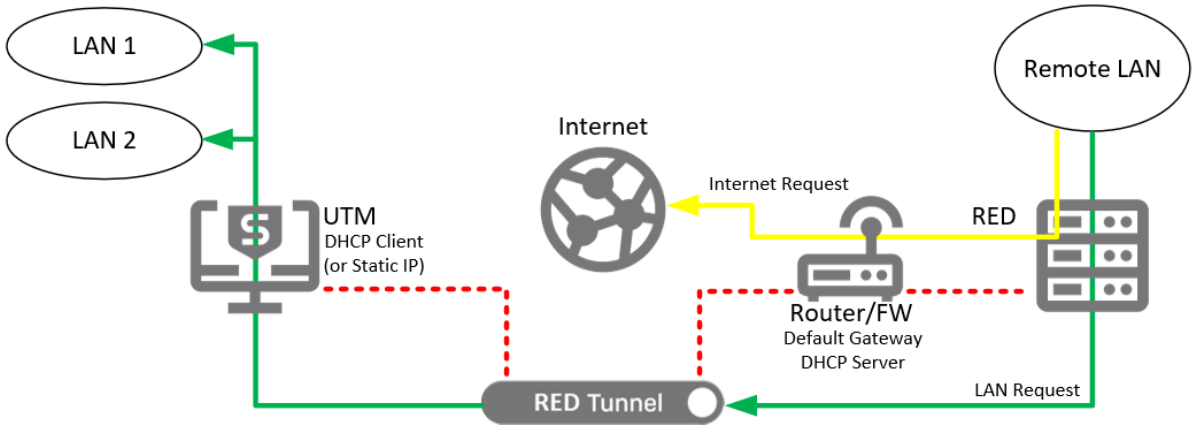
Le trafic vers ou depuis Internet ne peut pas être filtré ou protégé contre les menaces. La sécurité ne peut être appliquée qu'entre les réseaux locaux distants et locaux.



Le mode « Transparent/Split » :

Dans ce mode, le pare-feu Sophos XG n'est pas censé gérer le réseau distant. Il est connecté au LAN distant et à la passerelle du LAN distant et s'attend à recevoir une adresse sur le LAN distant via DHCP.

Semblable à l'option Standard / Split, seul le trafic destiné à certains réseaux parcourt le tunnel. Dans ce cas, le RED n'agit pas comme une passerelle, mais est en relation avec la passerelle et peut rediriger de manière transparente les paquets dans le tunnel.



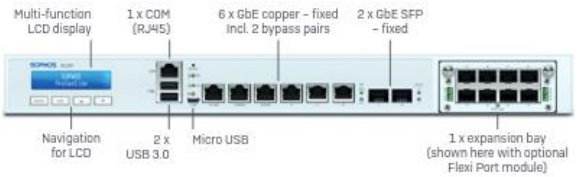
Cette option ne nécessite aucune reconfiguration du réseau distant et ne permet aucune gestion du LAN distant. Il assure la sécurité entre le LAN distant et tous les sous-réseaux locaux accessibles via le tunnel.

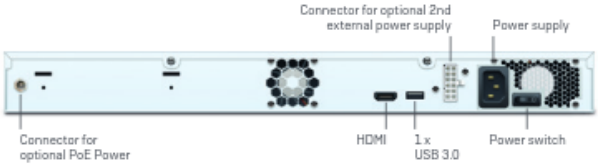
4.6 Le choix de notre matériel.

SOPHOS XG230 Rev.2

Comme expliqué ci-dessus, nous interconnecterons le site de l'entreprise via un UTM central. Nous avons choisi le modèle SOPHOS XG 230 Rev.2 qui peut être monté en rack.

Afin de garder une grande disponibilité, nous mettrons en place un système de redondance avec un cluster composé de deux appliances.

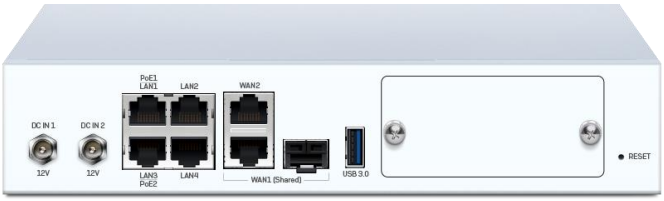




SOPHOS SD-RED60

Nous connecterons les sites distants Brest, Mâcon, Annecy et Dax entre eux via les appliances SOPHOS SD-RED60 (Remote Ethernet Device). Ces appliances qui seront installés sur ces 4 sites seront monitoré grâce à l'UTM central SOPHOS que nous aurons installé sur le site principal de Lille.

Grâce aux abonnements de protection, les sites distants reliés via l'appliance SD-RED60 seront entièrement protégés pour le courrier, le web et le réseau.



4.7 Interconnexion des sites

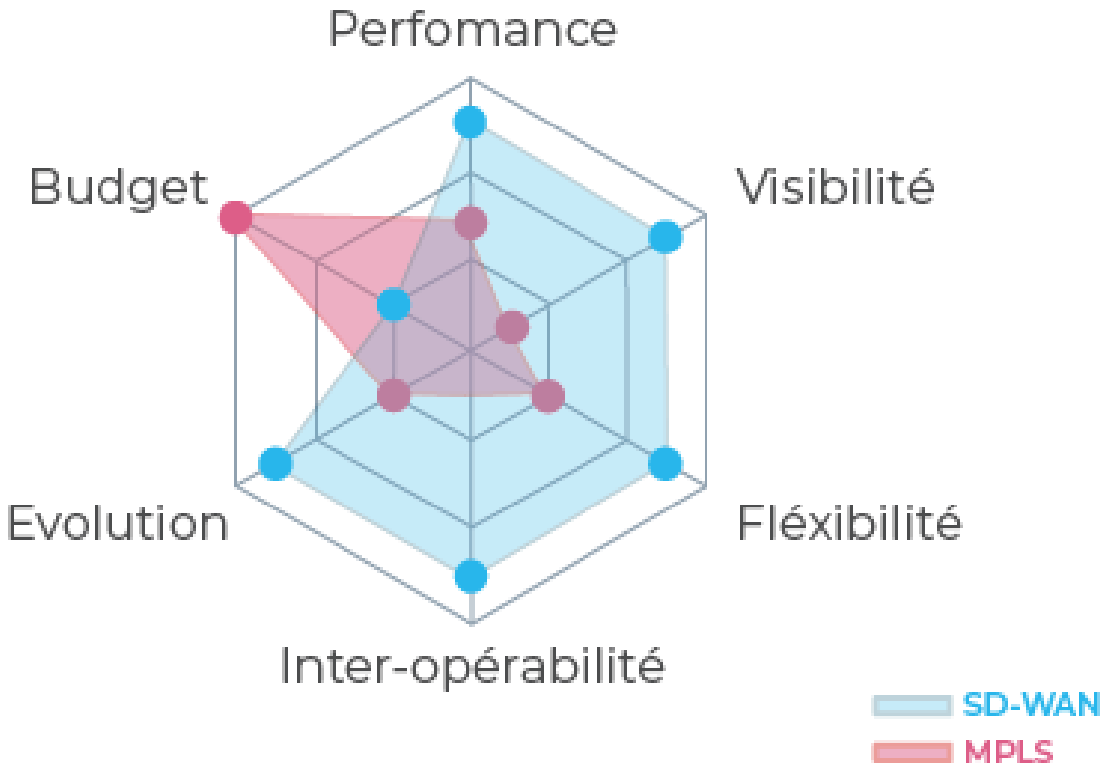
SD-WAN ou MPLS ?

- MPLS ou Multi Protocol Label Switching consiste à « tagger » les paquets IP. Ce principe, massivement appliqué aux entreprises françaises notamment, entre 2002 et 2005, a révolutionné la notion de Réseau Privé Etendu. Elle permet, à la fois une gestion centralisée et simplifiée du réseau chez l'opérateur MPLS, la mise en place de classes de services et une sécurité théoriquement plus élevée qu'IPsec en centralisant les accès à Internet de toutes les entreprises en cœur de réseau de l'opérateur MPLS.
  L'avantage majeur du MPLS est la qualité de service au sens de la QOS et la gestion centralisée, opérée par l'opérateur MPLS. L'inconvénient est la dépendance totale à l'offre de services de l'opérateur télécom choisi ou bien à l'infrastructure, parfois fragile, de l'opérateur virtuel qui doit maintenir ses centres de données et ses troncs de collectes avec les opérateurs télécoms qu'il a choisi pour rendre ses services.

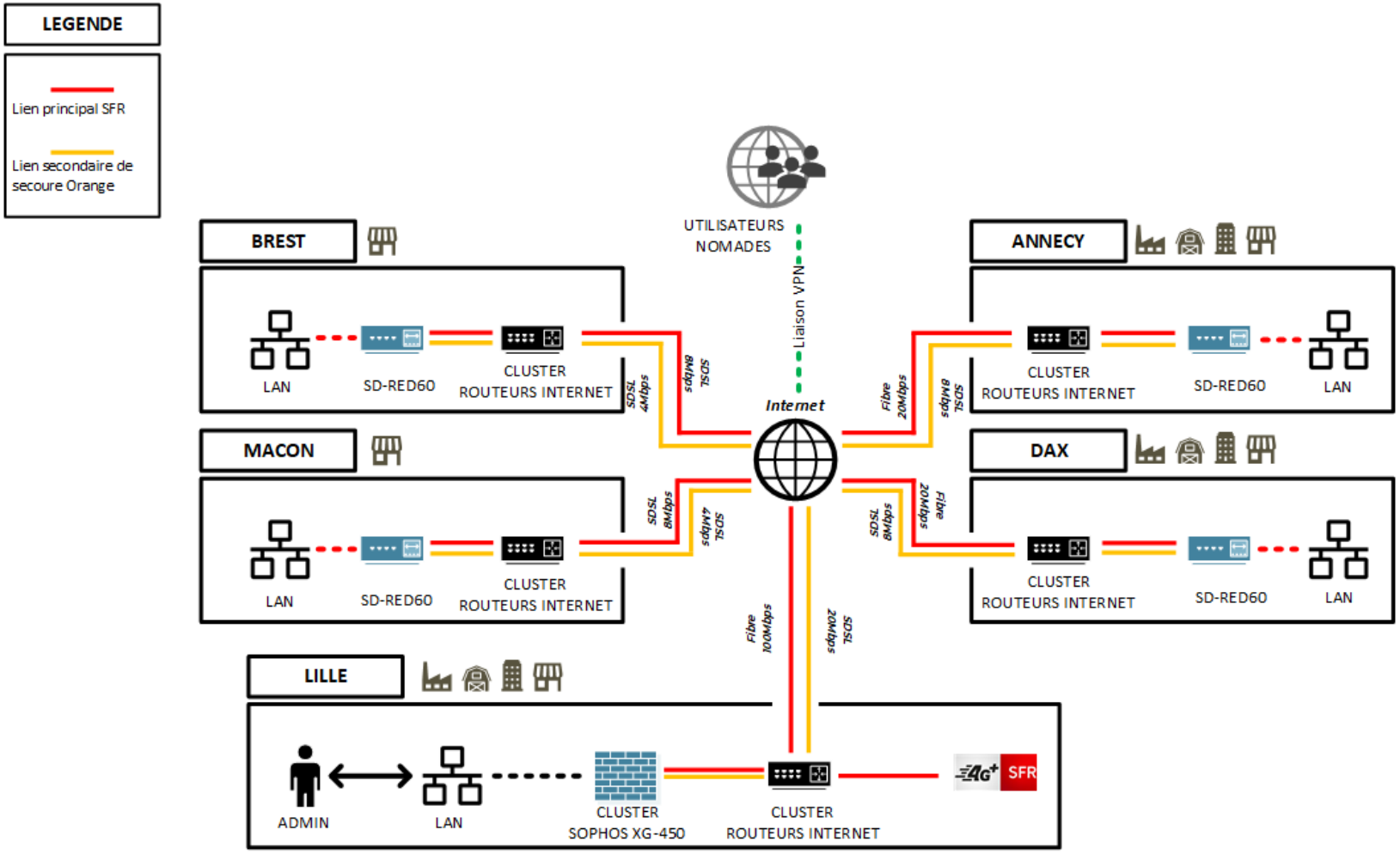
- Le SD-WAN permet d'appréhender son réseau d'entreprise d'une façon résolument moderne. La direction informatique de l'entreprise et/ou l'opérateur SD-WAN peuvent piloter le réseau de l'entreprise au travers d'un portail web sécurisé. C'est une façon de retrouver la liberté apportée par IPsec, la qualité de service du MPLS, mais surtout d'accéder à de nouveaux services :
  - Étendre son réseau d'entreprise à n'importe quel Cloud Provider dans le monde
  - Étendre son réseau d'entreprise à n'importe quel hébergeur (au travers d'une VM)
  - Créer/modifier/supprimer un accès distant à son réseau SD-WAN>
  - Moduler sa COS/QOS, « à sa façon », et sans limites
  - Pouvoir intégrer n'importe quel accès à Internet, de n'importe quel opérateur télécom, de n'importe quelle technologie (filaire ou sans fil) à son réseau privé SD-WAN, sans concessions sur la sécurité

  En bref, le SD-WAN est la meilleure réponse aux exigences des entreprises d'aujourd'hui :

  - Sécurité => Sécurité logique – cybercriminalité
  - Disponibilité => Zéro coupure
  - Performance => Toujours plus de débit
  - Flexibilité => Adaptabilité aux nouveaux environnements informatiques (Cloud)


Perfomance
Budget
Visibilité
Evolution
Fléxibilité
Inter-opérabilité
SD-WAN
MPLS

4.8 Schéma d'interconnexion des sites



4.9 Connexions à distance (Utilisateurs nomades)

Certains utilisateurs ont besoin de se connecter à distance au réseau de l'entreprise. Ces utilisateurs peuvent être ce qu'on qualifie d'utilisateurs nomades, possédant un pc portable ou un smartphone, et se déplaçant régulièrement en dehors de la société, tout en nécessitant un accès au réseau.

Les collaborateurs en situation de télétravail ont également besoin d'un accès à distance aux ressources de l'entreprise. En effet, la crise du COVID-19 nous a démontré l'intérêt et la nécessité absolue pour les entreprises en 2020 de disposer d'une solution de connexion à distance sécurisée pour permettre aux salariés de continuer de travailler depuis leur domicile.

Pour répondre à ces différents besoins, nous allons mettre en place une connexion sécurisée VPN SSL.

4.10 Choix de la solution

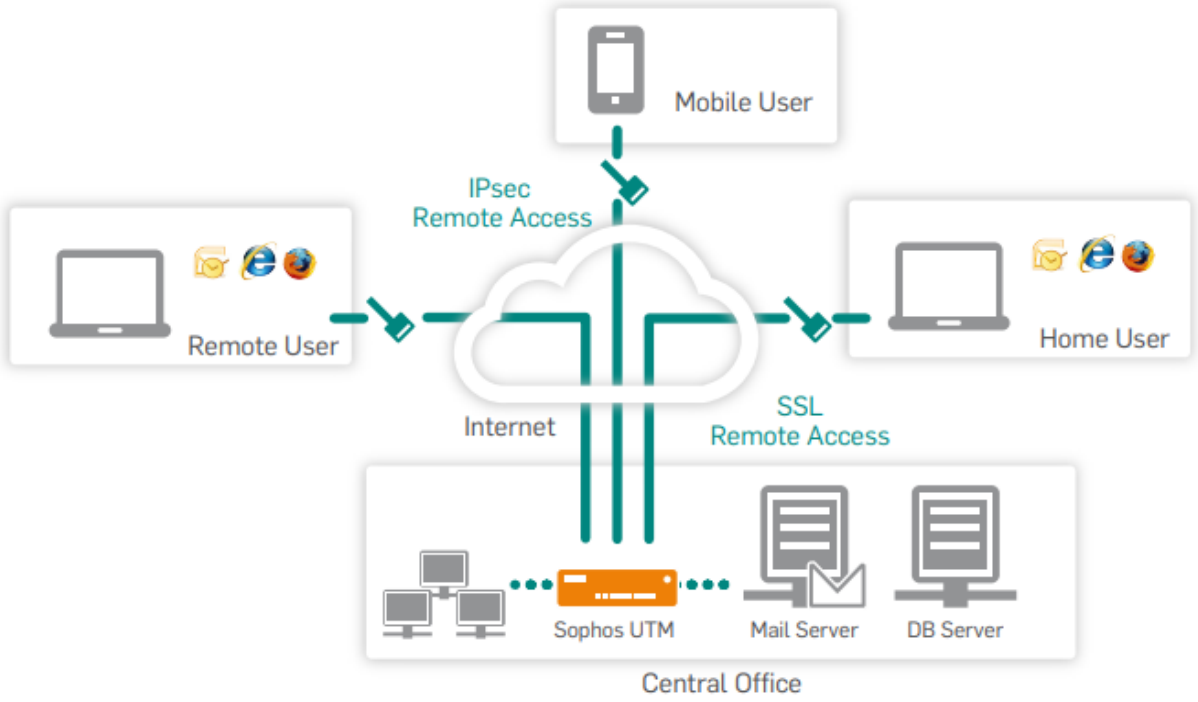
Différentes solutions de connexions à distance existent. Une des plus courantes est le VPN SSL. Le protocole SSL (Secure Socket Layer) offre une sécurité entre le navigateur des utilisateurs à distance et les serveurs de l'entreprise. Avec une solution VPN SSL, les utilisateurs pourront accéder à leurs e-mails, aux applications de l'entreprise ainsi qu'à l'intranet de celle-ci. Les solutions VPN SSL permettent également une personnalisation de l'accès aux ressources, dépendant du niveau de sécurité du poste de l'utilisateur, ou de ses niveaux d'accès.

Dans le cadre de la société Wood et de notre projet, nous avons décidé d'utiliser le client VPN Sophos.

4.11 Sophos SSL Client

Le client SSL Sophos est fourni gratuitement avec toute Appliance Sophos UTM sous abonnement UTM Network Protection.
Possédant des firewalls Sophos, nous allons donc partir sur cette solution intégrée.
La sécurité de ce client est éprouvée, et son client dédié possède un faible impact sur les performances du poste de l'utilisateur.
Il fonctionne à travers les pare-feux et fournit un accès transparent à toutes les ressources de la société.

Après une simple configuration au niveau du firewall Sophos, et après installation par l'utilisateur ou le service informatique du client sur le poste utilisateur, l'utilisateur pourra se connecter aux ressources de l'entreprise en utilisant son identifiant habituel ou un identifiant différent.
La solution est très modulable et accorde une configuration assez poussée des ressources disponibles aux utilisateurs.



Voici le schéma de fonctionnement de la solution VPN Sophos. Les utilisateurs nomades se connectent aux ressources de l'entreprise en passant par internet.

4.12 Comparaison entre l'ADSL, le SDSL et la fibre optique.

Description	ADSL	SDSL	FIBRE OPTIQUE
Débit descendant	20 Mbps (max)	Symétrique 500k à 4M en 1 ou 2p 4M à 8M en 2 ou 4p >=8M en 4p	Symétrique 6M à 200M+
Débit ascendant	1 Mbps (max)		
Débit garanti	Non	Débit max à 95%	Garantis 100%
Taille de l'entreprise	<5	5 à 100	10 à x0000
Garantie de Temps sur Rétablissement	Non	GTR 4h	GTR 4h
Usage	Non critique	Critique	Critique
Agrégation / Failover	Pas recommandé	Oui	Oui

5. Solution LAN – Réseau interne de l'entreprise

5.1 Rappel de l'existant.

Pour donner suite à l'étude des documents et divers éléments du cahier des charges du groupe WOOD, nous pouvons établir les observations suivantes liées à l'existant :

SITES	CABLAGE FILAIRE	CABLAGE FO	PRISES RESEAUX		COMMUTATEURS	
			TYPE	NBRE	TYPE	NBRE
LILLE	U-UTP CAT3	Multimode 100Mb/s	RJ45 CAT3	162	Netgear L2 24P 100 Mb/s	9
ANNECY	U-UTP CAT3	Multimode 100Mb/s	RJ45 CAT3	68	Netgear L2 24P 100 Mb/s	5
DAX	U-UTP CAT3	Multimode 100Mb/s	RJ45 CAT3	82	Netgear L2 24P 100 Mb/s	6
BREST	U-UTP CAT3	Multimode 100Mb/s	RJ45 CAT3	6	Netgear L2 24P 100 Mb/s	1
MACON	U-UTP CAT3	Multimode 100Mb/s	RJ45 CAT3	6	Netgear L2 24P 100 Mb/s	1

Figure 1 - Tableau récapitulatif de l'existant LAN

Nous constatons que sur l'ensemble des sites, les liaisons réseau ne permettent pas une intégration de matériel de commutation récents. Le matériel réseau de l'entreprise ne possède plus de garantie constructeur.

5.2 Rappel du besoin.

Le groupe Wood a décidé de faire évoluer son système d'information afin de répondre aux objectifs stratégiques établis par la direction de l'entreprise.

L'obsolescence du système ne permet plus de faire face à l'accroissement des commandes, ce qui engendre des pertes financières.

L'absence de contrats de maintenance et de compétences internes entraîne des facturations à chaque intervention de prestataire et des frais liés aux changements de matériel.

Les équipements de câblage et de commutation obsolètes rendent les performances du réseau imprévisibles et provoquent sa congestion.

Nous répondons au problème en proposant une nouvelle architecture réseau, capable de répondre aux besoins actuels du groupe WOOD tout en respectant les meilleures pratiques actuelles en matière de sécurité et d'intégration.

5.3 La topologie réseau.

La couche agrégée cœur de réseau, distribution ou 2/3.

Le nombre d'utilisateurs du groupe WOOD ne justifiant pas l'installation de 3 couches, les couches de cœur de réseau et de distribution peuvent être fusionnées en une seule couche dans l'optique de faire des économies et de simplifier l'architecture réseau.

La couche agrégée (cœur/distribution) s'effectuera à l'aide des commutateurs **FS S5850-32S2Q** avec 30 modules SFP + 10 Gb/s. Ils seront installés en doublon afin d'apporter de la haute disponibilité grâce à deux modules d'alimentation redondants.

La couche d'accès s'effectuera à l'aide des commutateurs **FS S3400-48T4SP.**

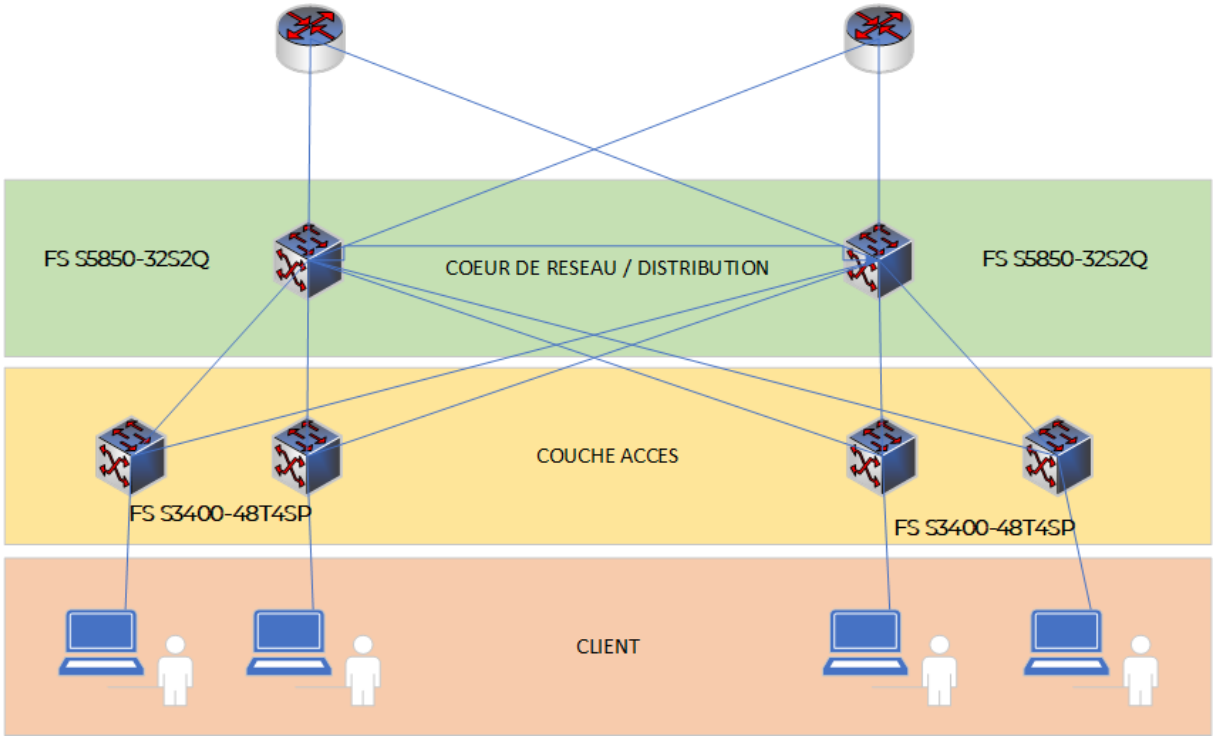


Figure 2 - Topologie 2/3

Implémentation du réseau sur les sites.

Lille
Lille est le site principal du groupe WOOD. Nous recommandons d'implémenter un modèle de topologie 2/3.

Annecy
Annecy est le site secondaire du groupe WOOD. Nous recommandons d'implémenter un modèle de topologie 2/3.

Dax
Dax est un site de production et également le plus petit site en termes d'utilisateurs. Le site de Dax hébergera quelques serveurs servant à la réplication des données. Nous recommandons d'implémenter un modèle de topologie 2/3.

Brest
Le magasin de Brest étant un petit site, nous recommandons d'installer un commutateur derrière le pare-feu RED60.

Mâcon
Le magasin de Mâcon étant un petit site, nous recommandons d'installer un commutateur derrière le pare-feu RED60.

5.4 Les VLANs

Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique.

Les VLANs présentent les intérêts suivants :

- Améliorer la gestion des flux.
- Optimiser la bande passante.
- Séparer les flux.
- Renforcer la sécurité.

Un réseau local virtuel est un regroupement virtuel d'au moins deux périphériques. Le fait que les périphériques soient isolés des autres permet de contenir le périphérique au sein du vlan concerné sans utiliser de routeur.

On retrouve trois types de VLAN ;

VLAN niveau 1 :

Un VLAN de niveau 1 (VLAN par port) définit un réseau virtuel en fonction des ports sur un commutateur.

Une configuration de VLAN de niveau 1 demande de faire la configuration de manière manuelle.

VLAN niveau 2 :

Un VLAN de niveau 3 (VLAN par MAC) définit un réseau virtuel en fonction des adresses MAC des périphériques connectés au commutateur.

Ce type de VLAN est beaucoup plus souple que le VLAN de niveau 1. Il est indépendant de la location du périphérique connecté.

VLAN niveau 3 :

Un vlan de niveau 3 (VLAN par sous-réseau) définit un réseau virtuel en fonction du sous-réseau selon l'adresse IP source.

Ce type de solution offre une grande flexibilité pour changer automatiquement la configuration du commutateur lorsque le poste de travail est déplacé. En contrepartie, lorsque les informations contenues dans le paquet doivent être analysées plus finement, une légère dégradation des performances peut se faire sentir.

5.5 Les avantages du VLAN

La mise en place de VLAN dans l'infrastructure permet :

- La gestion et la modification du réseau avec une plus grande flexibilité ; en effet toute la structure système peut être modifiée avec le paramétrage des commutateurs.
- Un gain en sécurité, car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Une réduction de la diffusion du trafic sur le réseau.

5.6 Implémentation des VLANs

Nous proposons l'implémentation des VLANs de niveau 1.

Description des VLANs :

Figure 3 - Description des VLANs

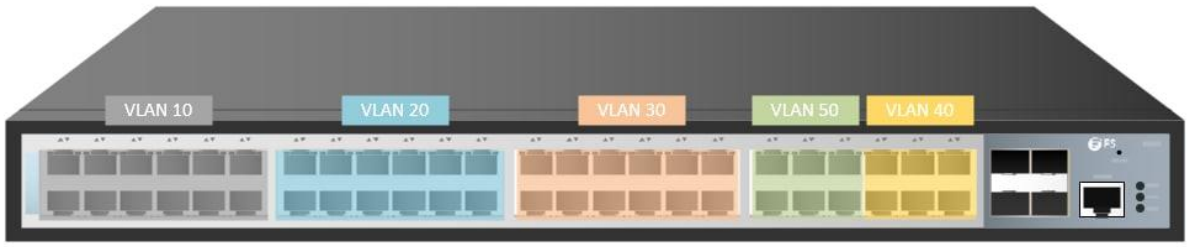


Figure 4 - Exemple d'implémentation des vlans sur un switch

5.7 Le choix des cœurs de réseau

Le choix des cœurs de réseau est un facteur crucial, car ils fournissent la liaison par laquelle tous les équipements se connectent.

Nous proposons des cœurs de réseau FS S5850-32S2Q :

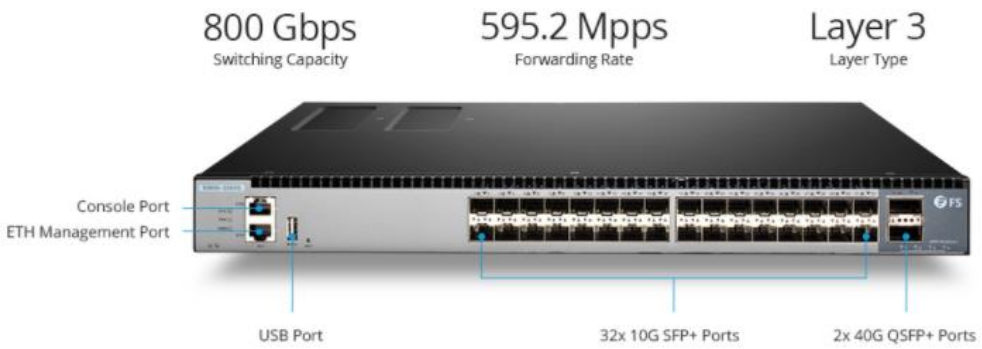


Figure 5 - Cœur de réseau FS S5852-32S2Q

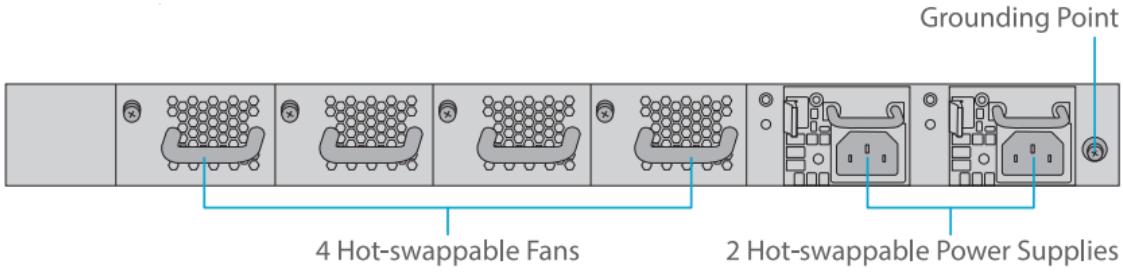


Figure 6 - Cœur de réseau FS 5850-32S2Q #2

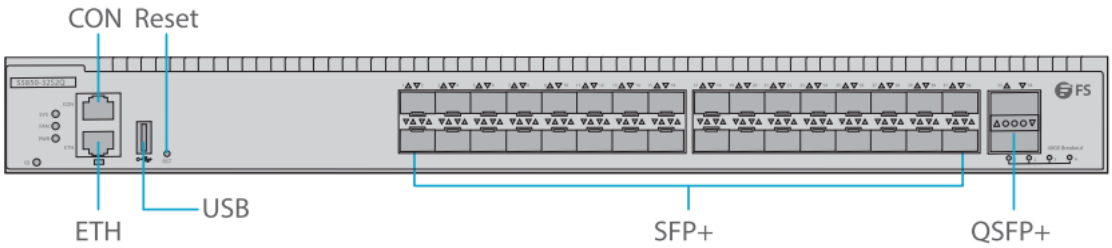


Figure 7 - Cœur de réseau FS 5850-32S2Q #3

Module SFP

Les distances étant inférieures à 10km et le connecteur support de la fibre multimode OM4, nous utiliserons des modules SFP-10GLR-31 pour la fibre 10Gb. Ce sont des connecteurs au standard LC full duplex.

Ces cœurs de réseau de couche 3 prennent en charge le routage statique et dynamique, les listes de contrôles d'accès, le SNMP, le protocole IPv6 avec 32 ports SFP + 10G, 2 ports SQFP+ 40G tout ça dans une plateforme 1U.

Le cœur de réseau FS S5850-32S2Q offre 800Gbps de connectivité de couche 2 et couche 3 aux réseaux. Il offre également les options suivantes :

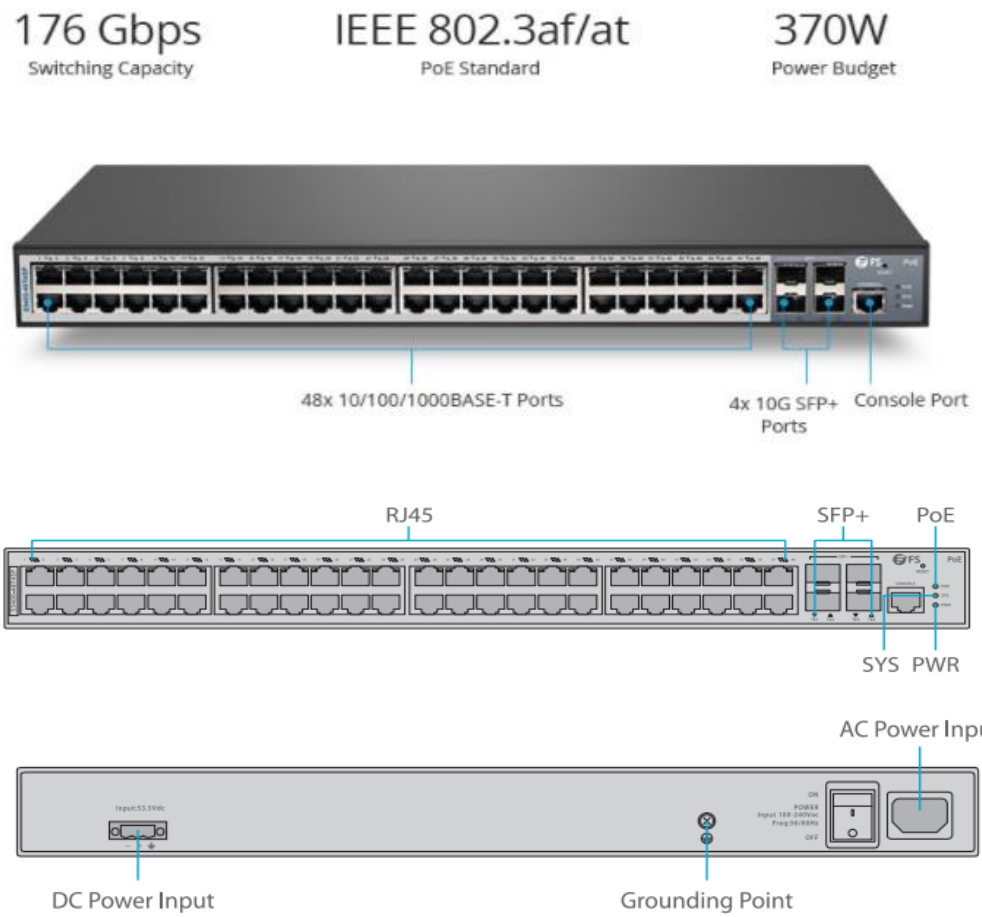
- MLAG : Pour Multi-Chassis Link Aggregation ; c'est la capacité de deux ou plusieurs commutateurs à agir comme un seul lors de la formation de groupement de liens pour améliorer la fiabilité des liaisons du réseau
    - Plusieurs avantages :
        - Répartit le trafic de manière égale sur chacun des commutateurs
        - Permet d'augmenter la largeur de la bande en regroupant simplement davantage de liens dans le LAG
        - Offre la possibilité de mettre à niveau un commutateur à la fois sans affecter les autres appareils
        - Augmente la capacité de port en toute simplicité en ajoutant un autre commutateur
- Haute fiabilité : Il prend en charge les modules d'alimentation interchangeables à chaud avec redondance 1+1 et les ventilateurs redondants N+1.
- Technologie de surveillance de l'environnement en temps réel pour détecter la température de l'équipement mais également pour connaître l'état des ventilateurs et de l'alimentation.
- Prise en charge de LACP /ECMP /VRRP /VARP /STP /RSTP /MSTP /SmartLink /BFD /ERPS /LoardBalancing

Le commutateur S5852-32S2Q est doté d'une double alimentation redondante 1+1, de 3+1 ventilateurs pour la circulation d'air de l'avant à l'arrière et peut fonctionner avec un ventilateur en panne.

5.8 Le choix des commutateurs

Nous proposons des commutateurs FS S3400-48T4SP

Le choix des commutateurs est un facteur important, car ils fournissent toute la couche d'accès des utilisateurs.



Ces commutateurs de couche 3 prennent en charge le routage statique et dynamique, les listes de contrôles d'accès, le SNMP, le protocole IPv6 et le PoE. En revanche, ils ne possèdent pas de modules d'alimentations redondants, mais ils comportent un port supplémentaire RPS à l'alimentation standard interne permettant une redondance électrique en utilisant une alimentation extérieure. Support de nombreux modes de gestion tels que le CLI, Telnet, SSH, SSL, SNMP, gestion web.

5.9 Emplacement des Datacenter

Les datacenters doivent suivre des recommandations afin d'atténuer les risques liés à la sécurité. Il est nécessaire de d'abord vérifier si l'emplacement actuel respecte plusieurs points.

Les locaux techniques choisis respecteront aux mieux les bonnes pratiques données par CLUSIF.

Nous retrouverons un premier datacenter dans les locaux principaux de Lille ainsi qu'un second pour une redondance dans l'atelier. Les salles seront aménagées pour une intégration totale sur système.

Nous retrouverons une troisième et quatrième salle serveur à DAX pour assurer une autonomie totale du site en cas de coupure.

Et enfin, une cinquième et sixième salle serveur à Annecy, également à visée d'assurer une autonomie totale du site en cas de coupure.

5.10 Câblage interbâtiment

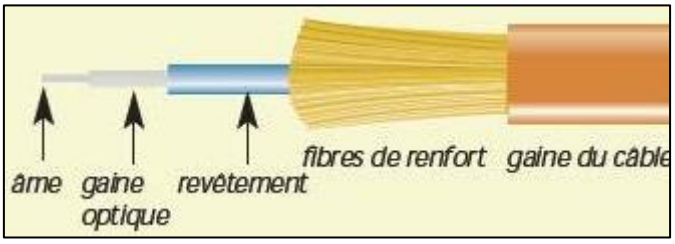
Actuellement les bâtiments à Lille, Annecy et Brest sont interconnectés avec de la fibre d'ancienne génération. Elle ne permet pas un débit suffisant. C'est pour cela que nous décidons de réutiliser les passages de câble afin de refaire une installation neuve de fibre optique.

La Fibre Optique.

La fibre optique est un fil de verre entouré d'une gaine réfléchissante. Sa propriété principale est de servir de « tuyau » par lequel fait circuler la lumière. Elle permet le transport de données informatiques.

Composition d'une fibre optique :

Un câble fibre est composé d'une âme, d'une gaine optique, d'un revêtement, de fibres de renfort et d'une gaine de câble.



Âme

Support physique qui transporte les signaux optiques entre une source de lumière et un équipement récepteur. L'âme est constituée d'un fil continu de verre ou de plastique, caractérisé par son diamètre externe dont la taille est exprimée en micromètres (µm). Plus l'âme est épaisse, plus elle peut transporter de lumière. Tous les câbles de fibre optique sont calibrés en fonction du diamètre de leur âme. Les trois calibres de fibre multimode les plus courants sont 50 µm, 62,5 µm et 100 µm.

Gaine optique

Fine couche qui entoure l'âme de la fibre et qui sert de barrière pour retenir les ondes lumineuses et provoquer la réfraction. Elle permet aux données de circuler sur toute la longueur du segment de fibre.

Revêtement

Couche de plastique qui entoure l'âme et sa gaine, destinée à renforcer l'âme, à absorber les chocs et à offrir une protection supplémentaire contre les courbures excessives du câble. L'épaisseur des revêtements est exprimée en micromètres (µm) et peut aller de 250 à 900 µm.

Fibres de renfort

Ils aident à protéger l'âme contre l'écrasement et les tensions excessives lors de l'installation. Il peut s'agir de fibres de Kevlar® de fils renforcés, de tubes remplis de gel, etc.

Gaine du câble

Couche extérieure standard de n'importe quel câble.

Type de fibre optique

Nous retrouvons deux types de fibres optiques utilisées :

Fibre Monomode (OS) : Elle n'autorise qu'une seule longueur d'onde, son cœur est plus petit, elle accorde une bande passante et un débit de données plus élevé sur de plus longues distances. Le coût de la monomode est élevé. Son utilisation est orientée réseau longue distance et réseau opérateur.

Fibre Multimode (OM) : Elle autorise plusieurs longueurs d'onde, son cœur est plus grand, la bande passante et le débit sont limités et les distances autorisées sont plus courtes. Le coût de la multimode est plus abordable. Son utilisation est orientée réseau d'entreprise.

Pour mettre en place un réseau 10 Gbits/s en coordination avec le matériel réseau implémenté dans l'infrastructure. Le changement des fibres optiques devient nécessaire.

Distances admissibles par type de fibre optique :

PROTOCOLES	DEBITS	OM1	OM2	OM3	OM4
100 BASE-FX	100 Mb/s	5 000 m	5 000 m	5 000 m	5 000 m
1000 BASE-SX	1 Gb/s	275 m	550 m	1 000m	1 100 m
1000 BASE-LX	1 Gb/s	550 m	550 m	550 m	600 m
10 GBASE-SR	10 Gb/s	33 m	82 m	300 m	550 m
10 GBASE-LX4	10 Gb/s	300 m	300 m	300 m	300 m
10 GBASE-LRM	10 Gb/s	220 m	220 m	220 m	220 m
40GBASE-SR4	40 Gb/s	-	-	100 m	125 m
100GBASE-SR10	40 à 100 Gb/s	-	-	100 m	125 m

Figure 8 - Distances admissibles par type de fibre optique

Nous aurons besoin de faire passer des connexions 10 Gbps entre les bâtiments sur des distances d'environ 100 mètres. La technologie utilisée sera de la fibre optique OM4 multimode pour des raisons d'évolution ; cette fibre est capable d'avoir des débits jusqu'à 100 Gb/s sur une distance de 125m.

Câblage fibre optique

Comme vu précédemment, nous avons décidé d'utiliser de la fibre optique OM4. Nous aurions pu proposer un câblage en liaisons cuivrées en catégorie 6A pouvant supporter ce débit, mais la fibre optique dispose d'un débit de transmission plus élevé et n'est pas sensible à certaines perturbations comme l'orage ou des appareils électriques comme pourraient l'être les liaisons cuivrées.

Plan de passage des fibres optiques à Lille :

Figure 9 - Plan de passage des fibres optiques à Lille

Tableau longueurs de fibre optique		
Du	Vers	Longueur
Bureau	Atelier	70 m
Bureau	Stock	90 m
Bureau	Magasin	120 m
Atelier	Stock	15 m
Atelier	Magasin	150 m

Plan de passage des fibres optiques à Annecy :

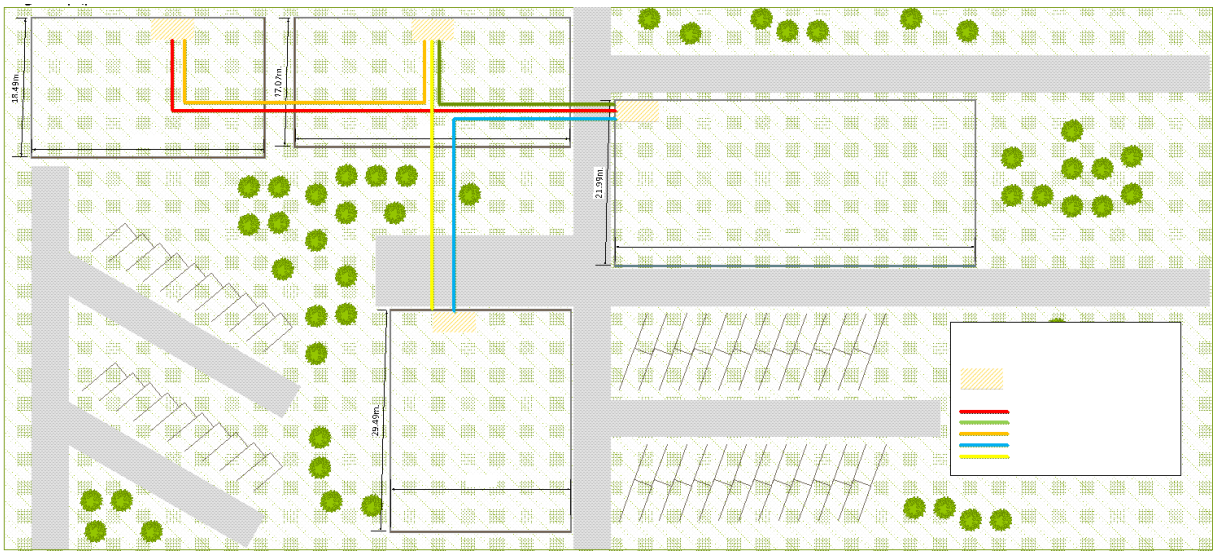


Figure 10 - Plan de passage des fibres optiques à Annecy

Tableau longueurs de fibre optique		
Du	Vers	Longueur
Bureau	Atelier	50 m
Bureau	Stock	55 m
Bureau	Magasin	70 m
Atelier	Stock	60 m
Atelier	Magasin	90 m

Plan de passage des fibres optiques DAX

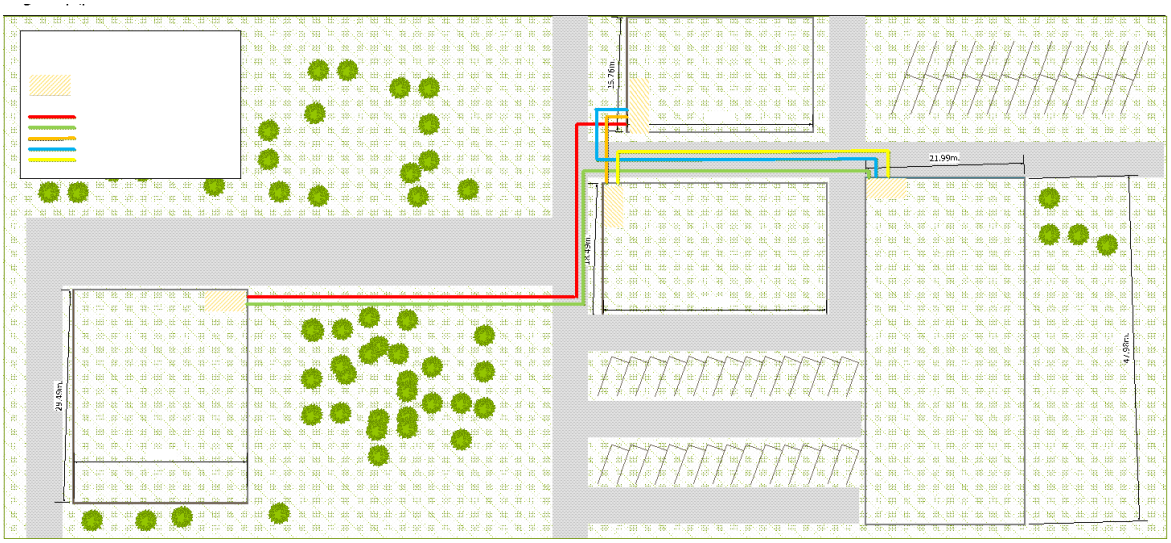


Figure 11 - Plan de passage des fibres optiques à Dax

Tableau longueurs de fibre optique		
Du	Vers	Longueur
Bureau	Atelier	60 m
Bureau	Stock	80 m
Bureau	Magasin	25 m
Atelier	Stock	120 m
Atelier	Magasin	50 m

Architecture d'interconnexion

Nous avons choisi d'utiliser une architecture Hub and Spoke avec double liaison et un unique point de sortie qui permet de garantir une haute disponibilité comme l'avait émis le groupe Wood.

Aucune tranchée n'est à prévoir, ni même de construction quelconque pour la mise en place de ce système. Nous allons utiliser les fourreaux et gaines déjà existantes.

5.11 Câblage des bâtiments

Les équipements de câblage et de commutation obsolètes rendent les performances du réseau imprévisibles et provoquent une congestion du réseau. C'est pour cela que nous proposons un remplacement de toutes les liaisons cuivrées sur l'ensemble des bâtiments des sites. Ce remplacement permettra de mettre à neuf toutes les liaisons et de garantir un réseau gigabit.

Les travaux seront réalisés par une entreprise spécialisée dans le câblage des réseaux qui garantira une expertise du câblage ainsi que la mise en place de toutes les dernières normes en vigueur.

La catégorie du câble

La catégorie du câble détermine la fréquence du signal diffusé et donc la vitesse théorique des câbles.

Récapitulatif des types de câbles Ethernet		
Type	Débit théorique pour 10m	Débit théorique pour 100m
CAT5	100 Mbps	100 Mbps
CAT5E	1Gbps	100 Mbps
CAT6	1Gbps	1Gbps
CAT6A	10Gbps	10Gbps
CAT7	10Gbps	10Gbps

Figure 12 - Récapitulatif des types de câbles Ethernet

Le blindage

On retrouve 3 grandes catégories de câblage :

Récapitulatif des types de blindage	
Type	Description
F/UTP	Blindage assuré par une feuille d'aluminium située entre la gaine et les 4 paires torsadées.
U/FTP	Ce sont les paires torsadées qui sont blindées avec une feuille d'aluminium, ce qui est plus efficace qu'un simple écrantage.
S/FTP	Chaque paire est entourée d'un blindage en aluminium et l'ensemble des quatre paires d'une tresse métalique

Figure 13 - Récapitulatif des types de blindage

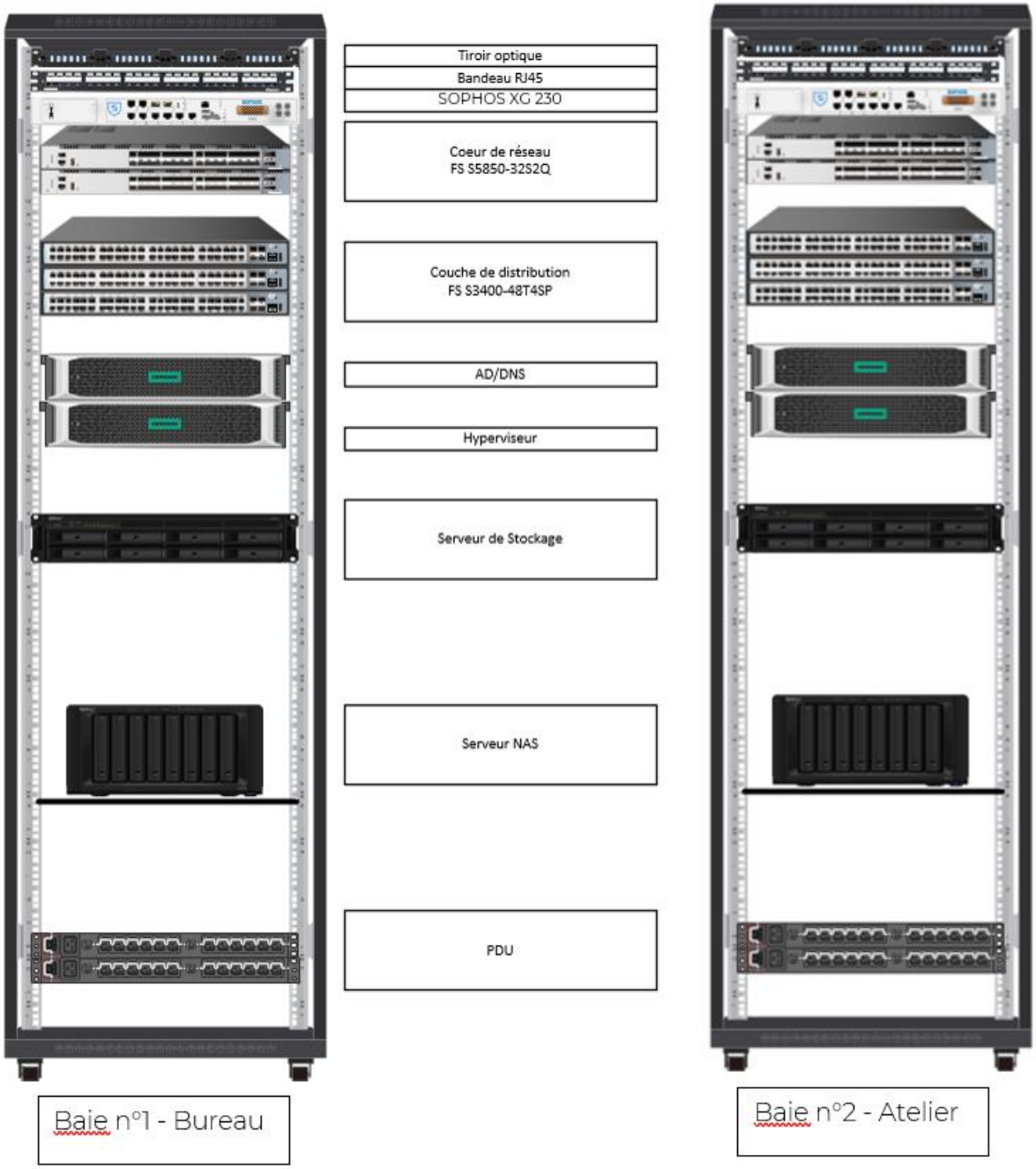
Quelle catégorie de câble choisir ?

Nous retiendrons des câbles CAT6 U/FTP. Ces câbles offrent un bon rapport qualité / prix blindage.

5.12 Les Baies informatiques

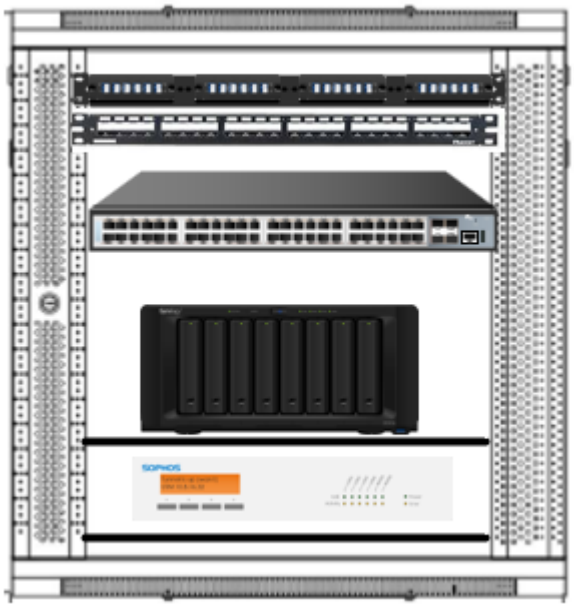
Nous proposons l'intégration de baies informatique 48U une située dans un bâtiment « bureau » et l'autre dans le bâtiment « atelier ». La première baie aura tous les équipements réseau et serveurs et la seconde sera identique à la première.

Nous proposons une baie de la marque FS Séries GR800. Une solution de baie distincte et robuste qui prend en charge et protège les serveurs montés en rack, les équipements de stockage et de réseau dans les centres de données multi locataires et d'entreprise, les salles informatiques et les installations réseau.



Pour les sites qui disposent de moins d'équipement système et réseau, nous proposons un coffret mural FS Série GW600 12U.

Conçue avec une excellente gestion des câbles, un accès facile par le haut et le bas et un système de rail de montage entièrement réglable, la baie de brassage de montage mural est extrêmement polyvalente pour une large gamme d'applications. Elle est idéale comme mini-salle de télécommunication ou pour les points de distribution et de consolidation de réseaux distants dans des espaces ouverts non protégés tels que des entrepôts, des magasins et des écoles.



Tiroir optique

Bandeau RJ45

Couche de distribution
FS S3400-48T4SP

Serveur NAS

RED 60

Voici un récapitulatif des baies sur les sites

Lille	
Baie 42U	Baie 12U
Bureau	Magasin
Atelier	Stocks

Annecy	
Baie 42U	Baie 12U
Bureau	Magasin
Atelier	Stocks

Dax	
Baie 42U	Baie 12U
Bureau	Magasin
	Stocks
	Atelier

Macon
Baie 12U
Magasin

Brest
Baie 12U
Magasin

Figure 14 - Récapitulatif des baies par site

5.13 Onduleurs

Définitions

Il est nécessaire de disposer d'un courant électrique exempt de tout défaut et perturbation, et disposant d'une fréquence et d'une tension constantes. Dans les faits, les lignes électriques sont très souvent victimes d'instabilités, et peuvent être victimes de coupures de courant, baisse ou hausse de tension, etc...

Dans une démarche de haute disponibilité et de continuité d'activité, il est ainsi nécessaire de nous protéger de ces impondérables à l'aide d'onduleurs.

Un onduleur va lisser le courant électrique afin de délivrer à notre infrastructure un courant propre exempt de défauts. Les onduleurs que nous avons sélectionnés sont également équipés de batteries, pour ainsi fournir du courant pendant une courte durée (15 minutes, le temps de couper les différents périphériques et de se préparer à adopter une solution électrique de secours).

Choix des onduleurs

Pour sélectionner nos onduleurs, nous avons calculé la consommation estimée de chacune de nos Baies. Voici la consommation estimée pour le site de Lille :

Baie N°1			Baie N°2		
Modèle	Conso(W)	Nombre	Modèle	Conso(W)	Nombre
Switch S5850-32S2Q	150	2	Switch S5850-32S2Q	150	2
Serveur HPE DL380	500	1	Serveur HPE DL380	500	1
Petit serveur pour l'AD	500	1	Petit serveur pour l'AD	500	1
Switch S3400-48T4SP	400	3	Switch S3400-48T4SP	400	1
Serveur de sauvegarde	60	1	Serveur de sauvegarde	60	1
NAS	67	1	NAS	67	1
Total		2627	Total		1767
Cos phi		0,66	Cos phi		0,66
Va		3980	Va		2677

Tableau 1 - Consommation électrique des baies principales de Lille

À la vue de cette consommation, ces 2 baies seront équipées d'un onduleur chacune.

L'onduleur sélectionné est le suivant :

Eaton 9PX 3000W RT3U French Hotswap with 1 EBM

- On line double conversion
- Écran LCD
- Batteries remplaçables à chaud
- By-Pass automatique et manuel
- Mesure de la consommation d'énergie

Cet onduleur nous permettra d'avoir une autonomie de 20 minutes en cas de coupure, et fonctionnera à seulement 87% de sa capacité maximum.

Concernant nos petites baies d'accès, voici la solution sélectionnée :

Entrepôt		
Modèle	Conso(W)	Nombre
Switch S3400-48T4SP	400	1
Total		400
Cos phi		0,66
Va		606

Tableau 2 - Consommation électrique de l'entrepôt de Lille

Eaton 9PX 2200W RT3U French Hotswap

- On line double conversion
- Écran LCD
- Batteries remplaçables à chaud
- By-Pass automatique et manuel
- Mesure de la consommation d'énergie

Cet onduleur permettra à ces baies réseau d'avoir une autonomie de 29 minutes.

Tous ces onduleurs disposent de prises françaises avec terre, et ont un rendement normal de 93% (ou 98% en mode haut-rendement.)

Au total, voici la quantité d'onduleurs nécessaire :

Modèle	Nombre	Prix	Prix total
Eaton 9PX 3000W RT3U	3	2 684€	8 052€
Eaton 9PX 2200W RT3U	9	2 109€	18 981€
Total			27 033€

Tableau 3 - Tableau récapitulatif de nos onduleurs

Nous aurons un onduleur 3000W dans chacune de nos baies disposant de serveurs, et un onduleur 2200W dans chacune de nos baies réseau. Ainsi, nous garantissons une autonomie minimum de 20 minutes en cas de coupure électrique et un courant propre pour l'intégralité de notre infrastructure réseau et serveur.

À l'aide du logiciel d'Eaton, installé sur nos serveurs, il serait possible d'éteindre proprement les machines ondulées si une coupure venait à se prolonger. Avec le second logiciel d'Eaton, il est possible d'avoir une gestion centralisée gratuite jusqu'à 10 onduleurs. Étant donné que nous en avons 12, le choix est pris de prendre une License Silver à 1 705,59€.

6. Réseau Wi-Fi de la société Wood.

6.1 Communications sans fil

Les communications sans fil sont des communications réseau ou au moins un des terminaux ne dispose pas de liaison filaire. L'intérêt de ce genre de communications réside dans le gain de mobilité ainsi que dans la facilité d'installation.

Il existe différentes catégories de communications sans fil.

- Réseaux étendus sans fil (WWAN) : LTE, 4G, 5G …
- Réseaux métropolitains sans fil (WMAN) wiMAX
- Réseaux locaux sans fil (WLAN) Wi-Fi
- Réseaux personnels sans fil (WPAN) Bluetooth

Nous allons nous concentrer sur un réseau local sans fil (WLAN) : Le Wi-Fi.

Le Wi-Fi, ce sont différents protocoles de communications sans fil régis par des normes du groupe IEEE 802.11.

Grâce au Wi-Fi, on peut faire communiquer des ordinateurs portables, ordinateurs, smartphones, et objets connectés sur un rayon de plusieurs dizaines de mètres en intérieur, dans un réseau local sans fil haut débit.

6.2 Avantages et inconvénients du WiFi

Comme toute communication sans fil, le Wi-Fi possède des avantages et des inconvénients. Les avantages du Wi-Fi sont les suivants :

- **Simplicité d'installation** : Un réseau Wi-Fi est simple et rapide à installer. Il n'y a pas besoin de tirer des câbles, de creuser des tranchées, etc. On peut donc installer des bornes Wi-Fi à des endroits où l'on ne pourrait pas installer des câbles habituellement, et on peut également déplacer temporairement une borne pour couvrir une zone provisoirement.
- **Coût** : Même si les bornes et contrôleurs Wi-Fi ont un certain coût, ils restent inférieurs au prix d'un réseau filaire sur le long terme en raison de la flexibilité d'utilisation et de l'absence de câbles.
- **Mobilité :** Le principal avantage du réseau Wi-Fi. Les utilisateurs peuvent se connecter au réseau Wi-Fi sans se brancher physiquement et rester connectés tout en se déplaçant au sein de la société. Ils peuvent donc accéder aux données et applications du réseau entreprises en toute mobilité.
- **Compatibilité avec les réseaux locaux filaires**

Naturellement, le Wi-Fi possède également certains inconvénients :

- Problématiques des ondes radio : En effet, le Wi-Fi utilisant des ondes radio, toutes les problématiques propres aux ondes radio s'appliquent également.
- Sécurité : En effet, un réseau Wi-Fi pose certains problèmes de sécurité, il est donc nécessaire que ce dernier possède une sécurité adaptée.
- Interférences : Le réseau Wi-Fi est très fragile aux interférences.
- Moins de bande passante que sur un réseau câblé.

6.3 Les différents protocoles

Il existe différents protocoles Wi-Fi. Chaque nouveau protocole a pour objectif d'augmenter les taux de transfert et la portée du signal.

Protocole	Date	Fréquence	Taux de transfert réel	Taux de transfert Max	Portée (en intérieur)	Portée (en extérieur)
802.11	1997	2,4-2,5 GHz	1 Mbit/s	2 Mbit/s	inconnue	inconnue
802.11a	1999	5,15-5,35/5,47-5,725/5,725-5,875 GHz	25 Mbit/s	54 Mbit/s	25 m	75 m
802.11b	1999	2,4-2,5 GHz	6,5 Mbit/s	11 Mbit/s	35 m	100 m
802.11g	2003	2,4-2,5 GHz	25 Mbit/s	54 Mbit/s	25 m	75 m
802.11n	2009	2,4 GHz ou 5 GHz	200 Mbit/s	450 Mbit/s	50 m	125 m
802.11ac	janvier 2014	5 GHz	433 Mbit/s	1300 Mbit/s	20 m	50 m

Dans le cadre de notre projet, on se concentrera sur le protocole 802.11n, protocole le plus viable pour une utilisation professionnelle. (Pour le taux de transfert et la portée en intérieur.) En effet, il faut à la fois être capable de fournir un débit suffisant pour l'utilisateur, et être capable de couvrir convenablement les locaux de la société avec le minimum de bornes possible.

6.4 Notre architecture WiFi

Nous allons opter pour une architecture Wi-Fi courante, structurée et éprouvée : des bornes Wi-Fi, avec un contrôleur Wi-Fi central, aussi appelé : Architecture Wi-Fi centralisée. Dans une architecture centralisée, ce sera le contrôleur central qui prendra en charge l'administration et la configuration de nos bornes d'accès Wi-Fi.

Cette configuration précise permet une haute fiabilité, une tolérance à la panne plus élevée, plus de fonctionnalités, et une meilleure sécurité, puisque la configuration est localisée sur le contrôleur.

L'intégralité des paramétrages réseau et de sécurité sont réalisés et stockés dans le contrôleur central qui les diffusera à l'ensemble de nos points d'accès.

6.5 Notre solution

2 marques de points d'accès Wi-Fi ont attiré notre attention : Ubiquiti, et Sophos.

Avantages Sophos	Inconvénients Sophos	Avantages Ubiquiti	Inconvénients Ubiquiti
Intégration à l'environnement sophos	Moins bonne couverture par rapport à un modèle équivalent chez Ubiquiti	Prix faible (69€)	Marque moins éprouvée
Possibilité d'utiliser notre Firewall comme contrôleur Wi-Fi	Prix élevé (170€)	Excellente couverture /portée	Nécessite un contrôleur Wi-Fi pour avoir une architecture centralisée
Bon signal à courte portée (Cf schéma ci-dessous, l'atténuation de signal de 10db arrive plus loin que sur les bornes ubiquiti		Le choix de points d'accès Ubiquiti permettrait d'en utiliser moins pour avoir la même couverture qu'avec des AP Sophos (entre 3 et 5 bornes de moins)	

Tableau 4 - Avantage et inconvénient Sophos et Ubiquiti

Les 2 solutions possèdent chacune leurs avantages, mais l'avantage principal reste le prix moins élevé des bornes Ubiquiti. En effet, sur une trentaine de points d'accès, la différence de prix permet même de justifier l'achat du contrôleur Wi-Fi nécessaire à la solution centralisée Ubiquiti. Sur l'image suivante, nous pouvons constater la différence de couverture Wi-Fi entre une borne Sophos APX 120, et une borne Ubiquiti UAP AC LITE.

Figure 15 - Comparaisons de couverture Wi-Fi entre une Borne Sophos et une borne Ubiquiti

Pour construire notre réseau Wi-Fi, nous allons donc utiliser des points d'accès Wi-Fi de la marque Ubiquiti.

Les points d'accès seront des UAP-AC-LITE :

- Taille compacte
- Adapté à l'usage intérieur
- Alimentation 24V Passive PoE
- Portée annoncée de 122m
- Débit attendu en 2.4Ghz : 300 Mbps
- Débit attendu en 5Ghz : 867 Mbps

Pour notre contrôleur central, nous allons utiliser un UAS-XG de chez Ubiquiti

Grâce aux performances de ce contrôleur, et avec l'assistance du logiciel propriétaire Unifi, nous pourrons contrôler l'intégralité de nos points d'accès.

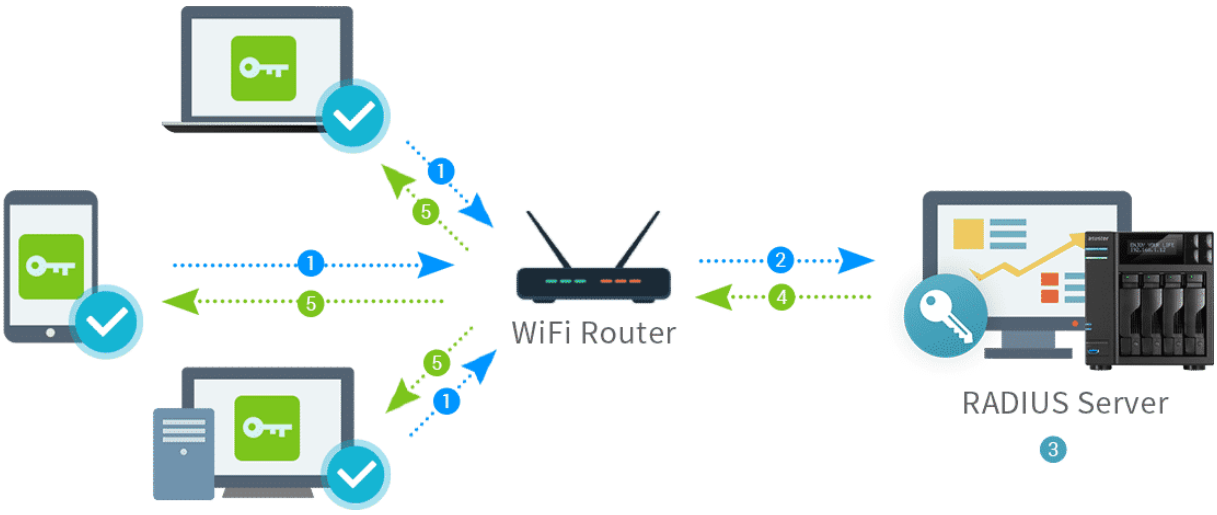
- Intel Xeon @2.4Ghz / 2.7Ghz
- 16Go DDR4-SDRAM
- Disque dur de 8000 Go
- SSD de 120 Go
- Interfaces 10 Gigabit Ethernet
- Rack 1 U

Les points d'accès seront tous connectés et alimentés en Ethernet. Ils seront dans un VLAN dédié aux points d'accès, et pourront accéder au contrôleur central.

6.6 Gestion des authentifications

Afin d'avoir une infrastructure cohérente et simple d'utilisation pour les utilisateurs, nous allons mettre en place un serveur Radius.

Remote Authentication Dial-In User Service (Radius) est un protocole de type client-serveur qui permet de centraliser les demandes d'authentification provenant d'équipement réseau (dans notre cas, les bornes Wi-Fi). Radius va centraliser les demandes et interroger un service d'annuaire de type LDAP.

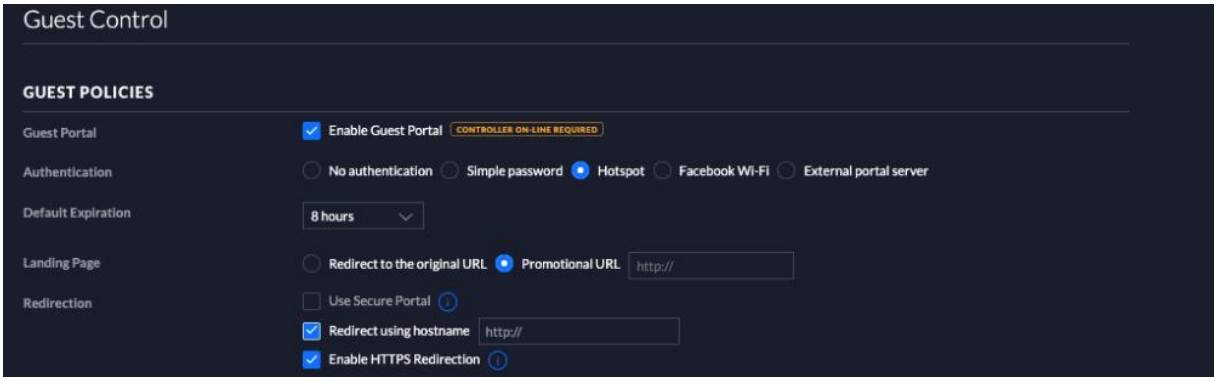


En somme, le serveur Radius va authentifier les utilisateurs sur le réseau Wi-Fi, en comparant leur identité avec notre annuaire LDAP. Radius ayant également une fonction « Accounting », il enregistrera la date, l'heure et l'adresse MAC du client, afin de constituer des logs de connexions au réseau.

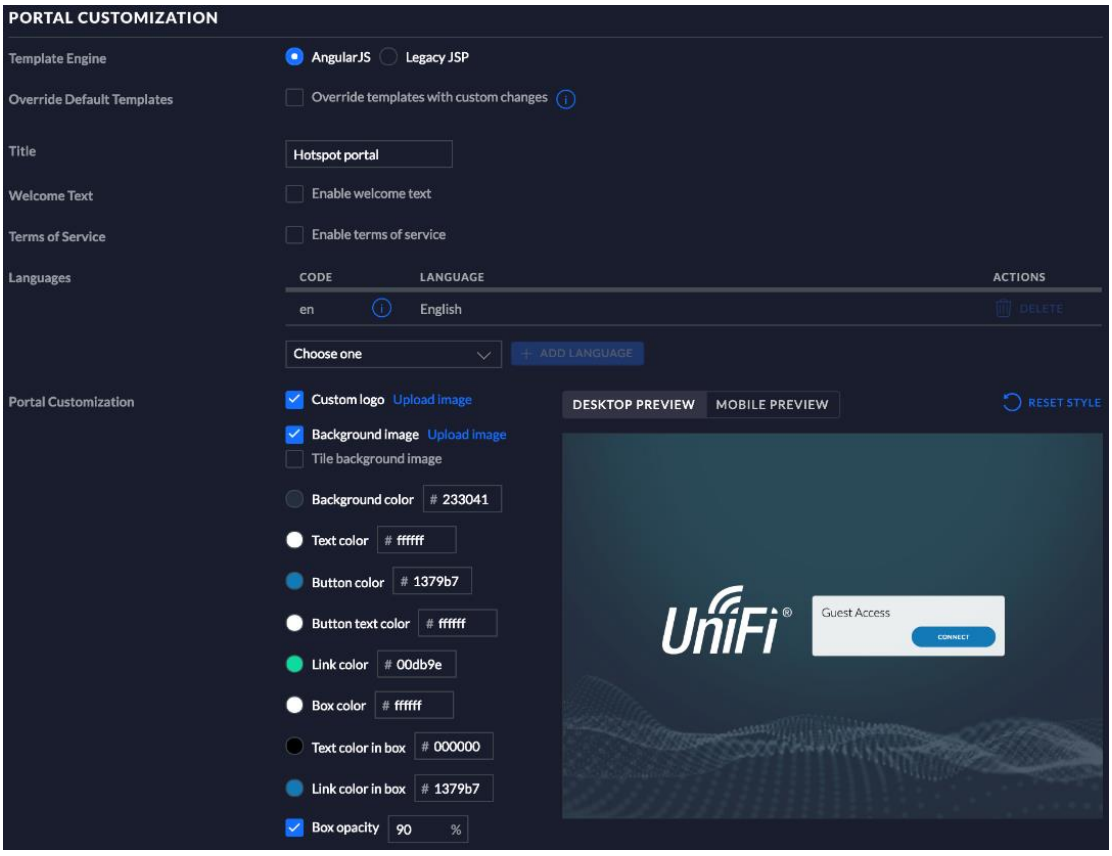
Notre solution Unifi étant compatible avec Radius, nous pourrons autoriser le serveur sur notre contrôleur central, et administrer la sécurité de notre réseau. Ainsi, les utilisateurs qui sont connectés sur leurs postes pourront se connecter de manière quasi transparente au réseau wifi (ils auront simplement besoin de se connecter au réseau Wi-Fi de manière classique.) Sur notre réseau Wi-Fi, relié aux ressources de l'entreprise, il sera nécessaire d'être authentifié par Radius.

6.7 Réseau Wi-Fi invité : Wi-Fi Guest

Nous allons mettre à disposition des invités de la société un réseau Wi-Fi Guest séparé du réseau Wi-Fi standard. Ce réseau Wi-Fi Guest sera sur un VLAN séparé ou seul l'accès à internet, via un portail, sera disponible. Pour ce faire, nous allons utiliser la solution proposée par UniFi.

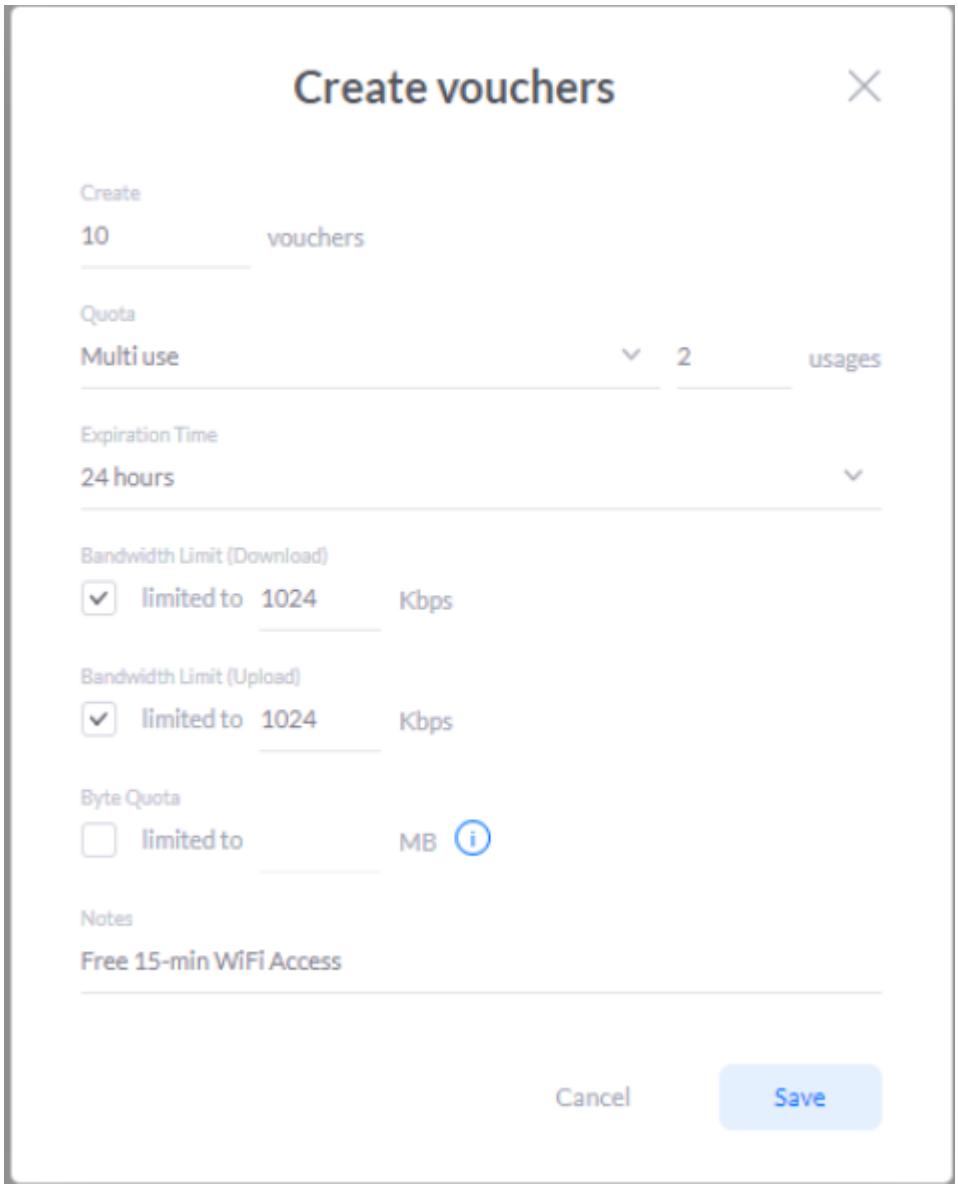


En activant la fonctionnalité Hotspot du portail invité, les utilisateurs seront invités à s'identifier avant de pouvoir accéder au réseau invité.



La page d'accueil présentée aux visiteurs est personnalisable, et permet de mettre un logo et une image de fond individualisée, afin de correspondre à la charte graphique de la société Wood.

En activant la gestion de l'identification par « Voucher » il sera possible de créer des coupons de connexion afin d'autoriser chaque utilisateur UN à UN, afin de s'assurer de qui utilise notre réseau public.



Il est possible de limiter la bande passante, le quota de données, de lui donner une limite de durée.

Conformément aux réglementations nationales et européennes, les logs de connexions seront conservés et authentifiés.

6.8 Couverture Wi-Fi des locaux

Pour positionner nos bornes Wi-Fi, nous avons utilisé Ekahau, un logiciel de cartographie du Wi-Fi. Grâce à cet outil, nous avons pu concevoir les cartes de couverture Wi-Fi suivantes, et positionner nos bornes Wi-Fi aux meilleurs endroits afin d'en avoir le moins possible tout en assurant la meilleure couverture possible.

Sur la carte suivante, on peut voir le positionnement de nos points d'accès Wi-Fi dans le bâtiment administratif de Lille. Plus la zone est verte, plus la couverture et le débit sont optimaux.

Par ailleurs, pour chaque magasin du groupe Wood, un point d'accès sera déployé.

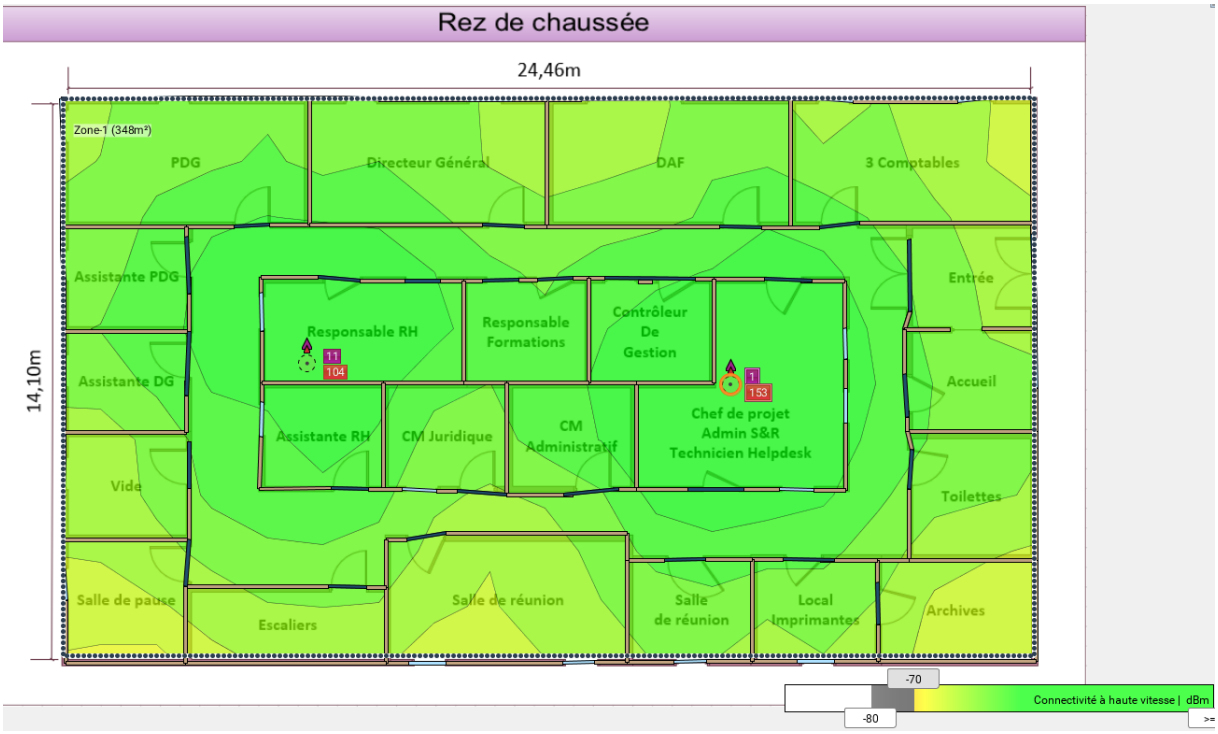


Figure 16 - Cartographie Wi-Fi du Rez du Chaussée de bâtiment administratif de Lille

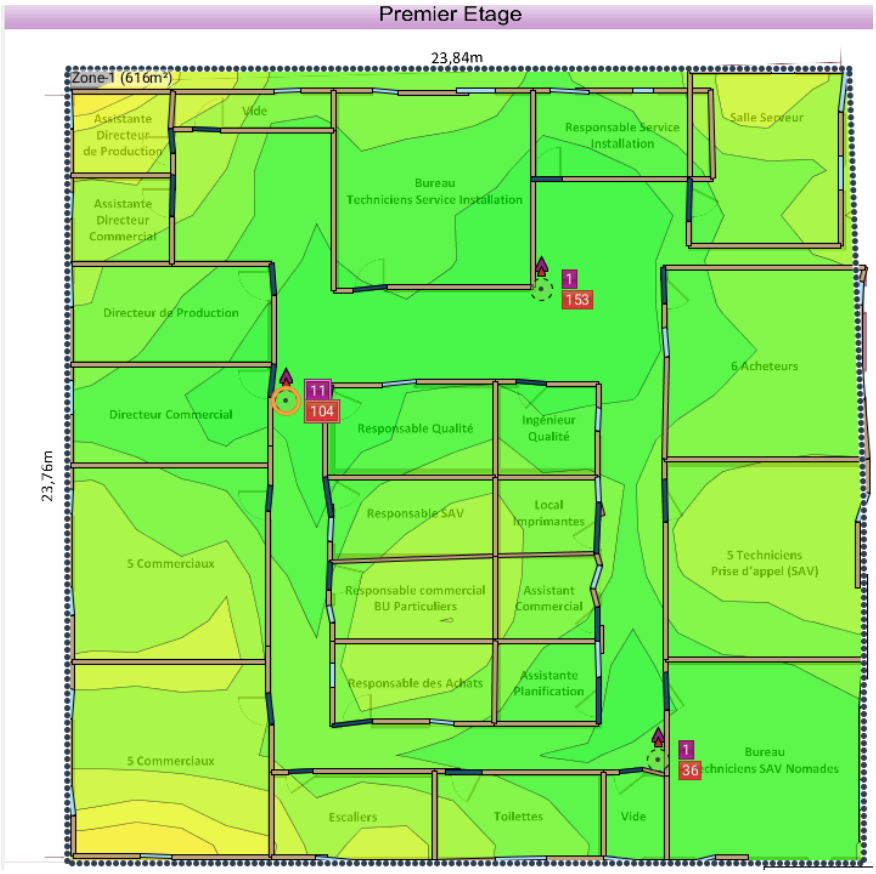


Figure 17 - Cartographie Wi-Fi du Premier étage du bâtiment administratif de Lille

Dans le bâtiment administratif de Lille, il y aura donc besoin de 5 points d'accès Wi-Fi.

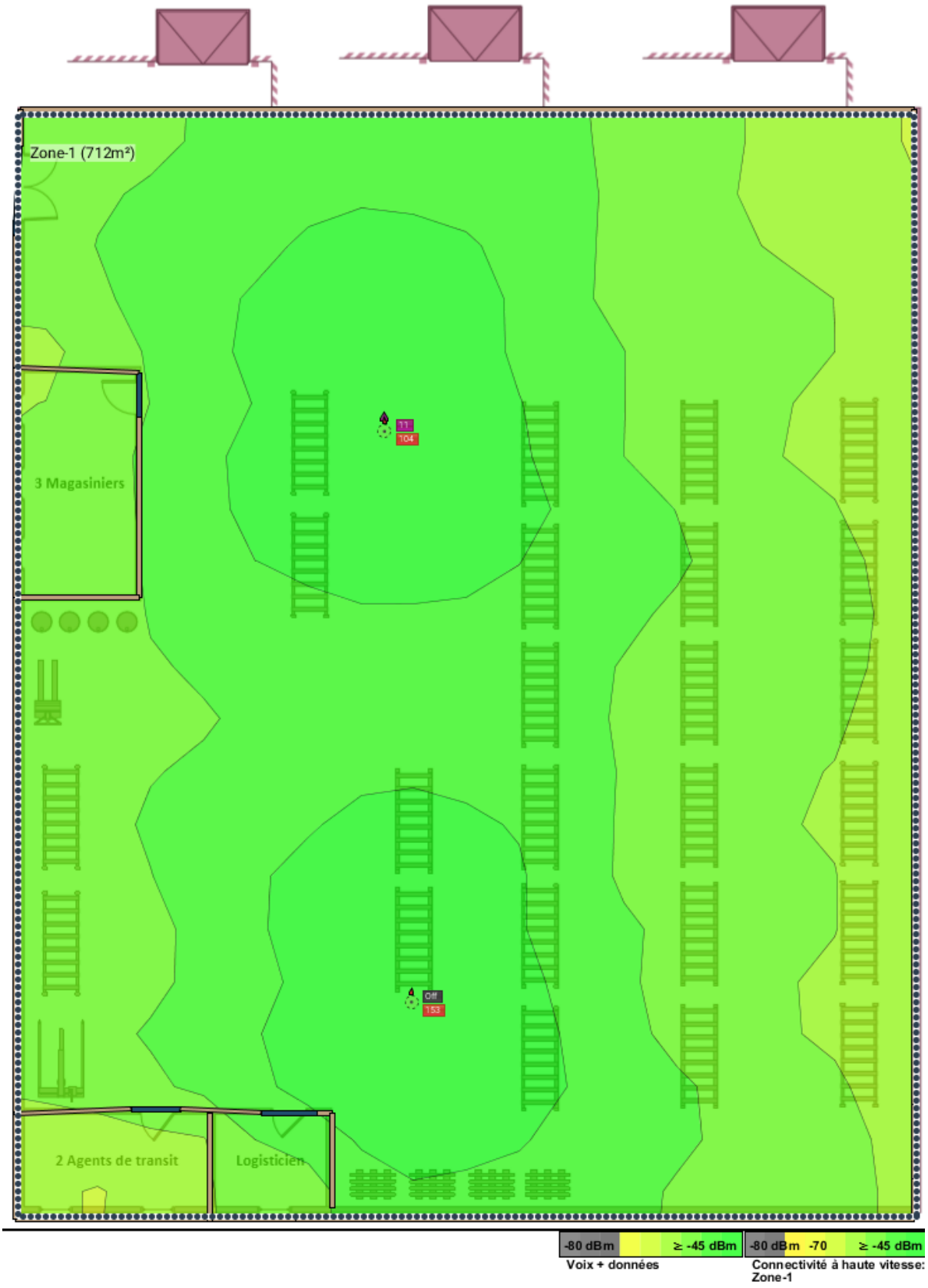


Figure 18 - Cartographie Wi-Fi de l'entrepôt de Lille

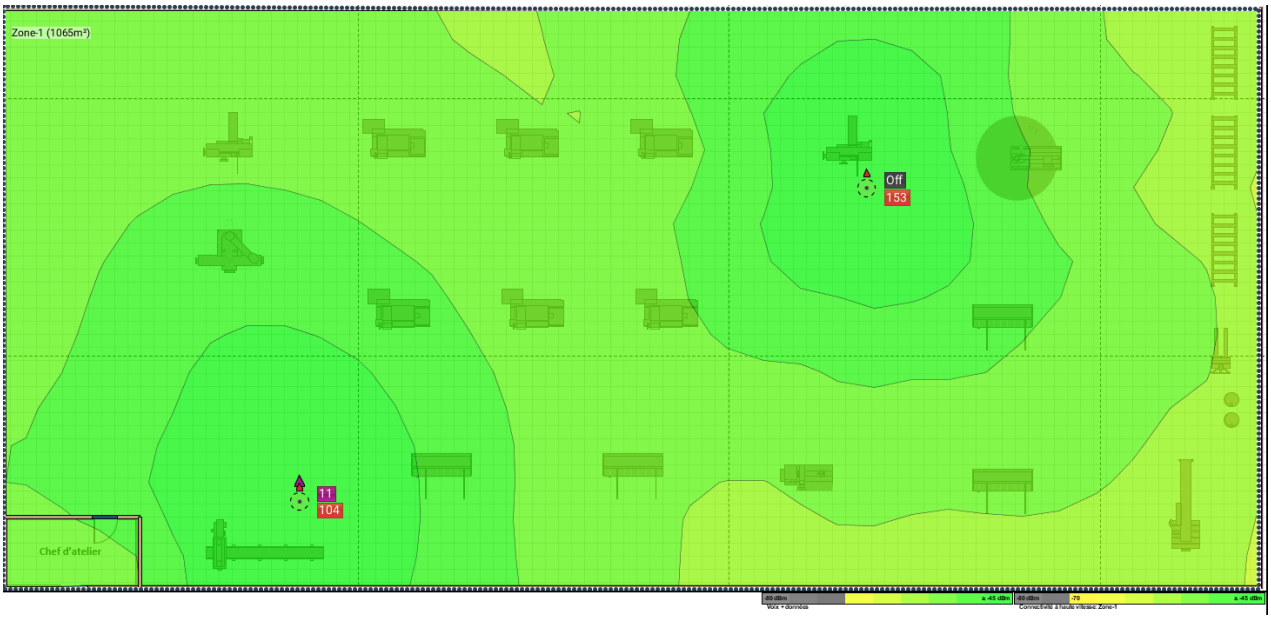


Figure 19 - Cartographie WiFi de l'atelier de Lille

Au total, pour l'entrepôt et l'atelier de Lille, il faudra 4 points d'accès. Il a été décidé d'intégrer le Wi-Fi dans tous les entrepôts et ateliers de Lille, Dax et Annecy à des fins de mobilités et pour l'utilisation de terminaux sans fils.

Pour le site de Lille, on totalise donc 9 points d'accès.

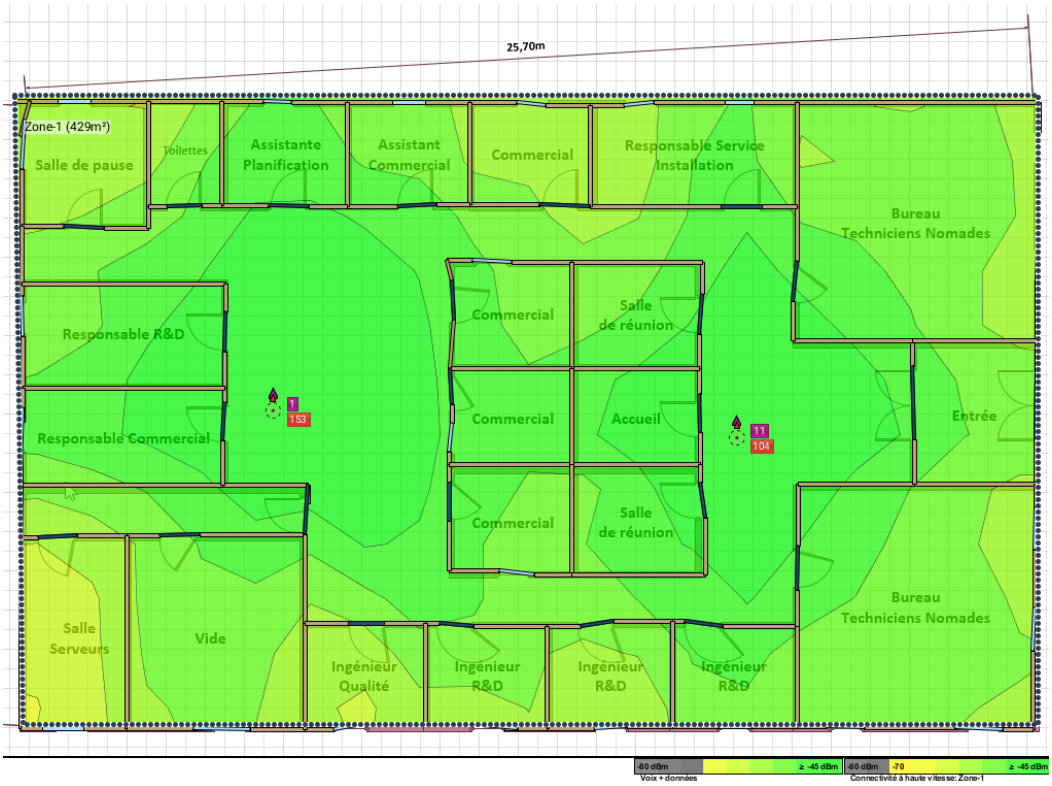


Figure 20 - Cartographie WiFi des bureaux de Dax

Il faudra 2 points d'accès pour couvrir les bureaux de Dax.

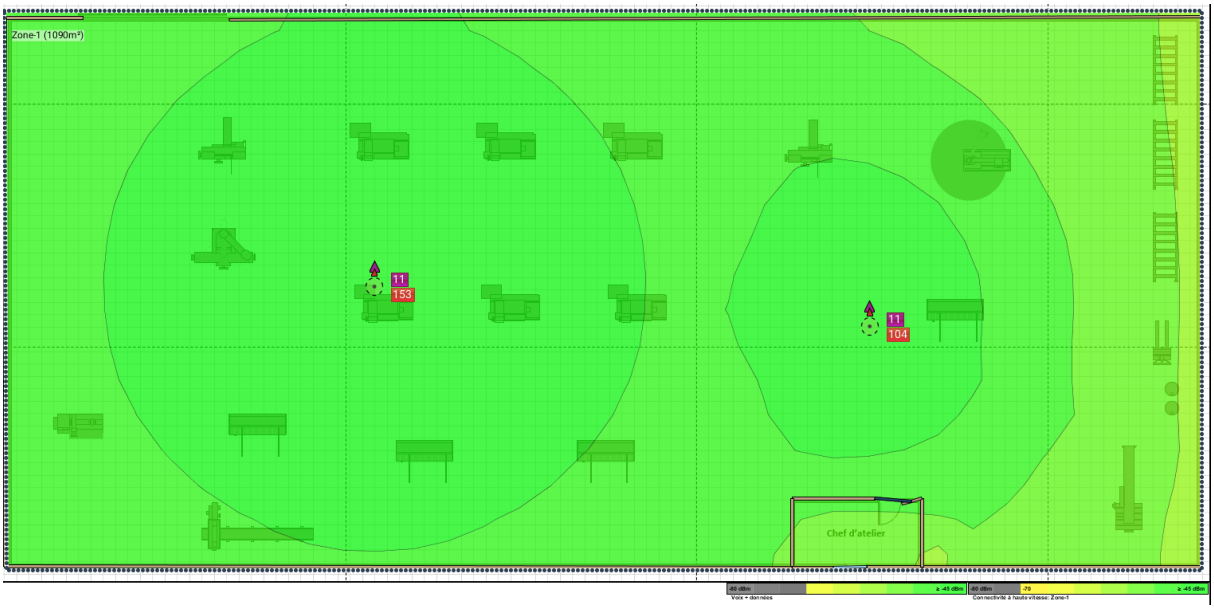


Figure 21 - Cartographie WiFi de l'atelier de Dax

Figure 22 - Cartographie Wi-Fi de l'entrepôt de Dax

Nous utiliserons 4 points d'accès pour l'entrepôt et l'atelier de Dax, pour un total de 6 points d'accès pour le site.

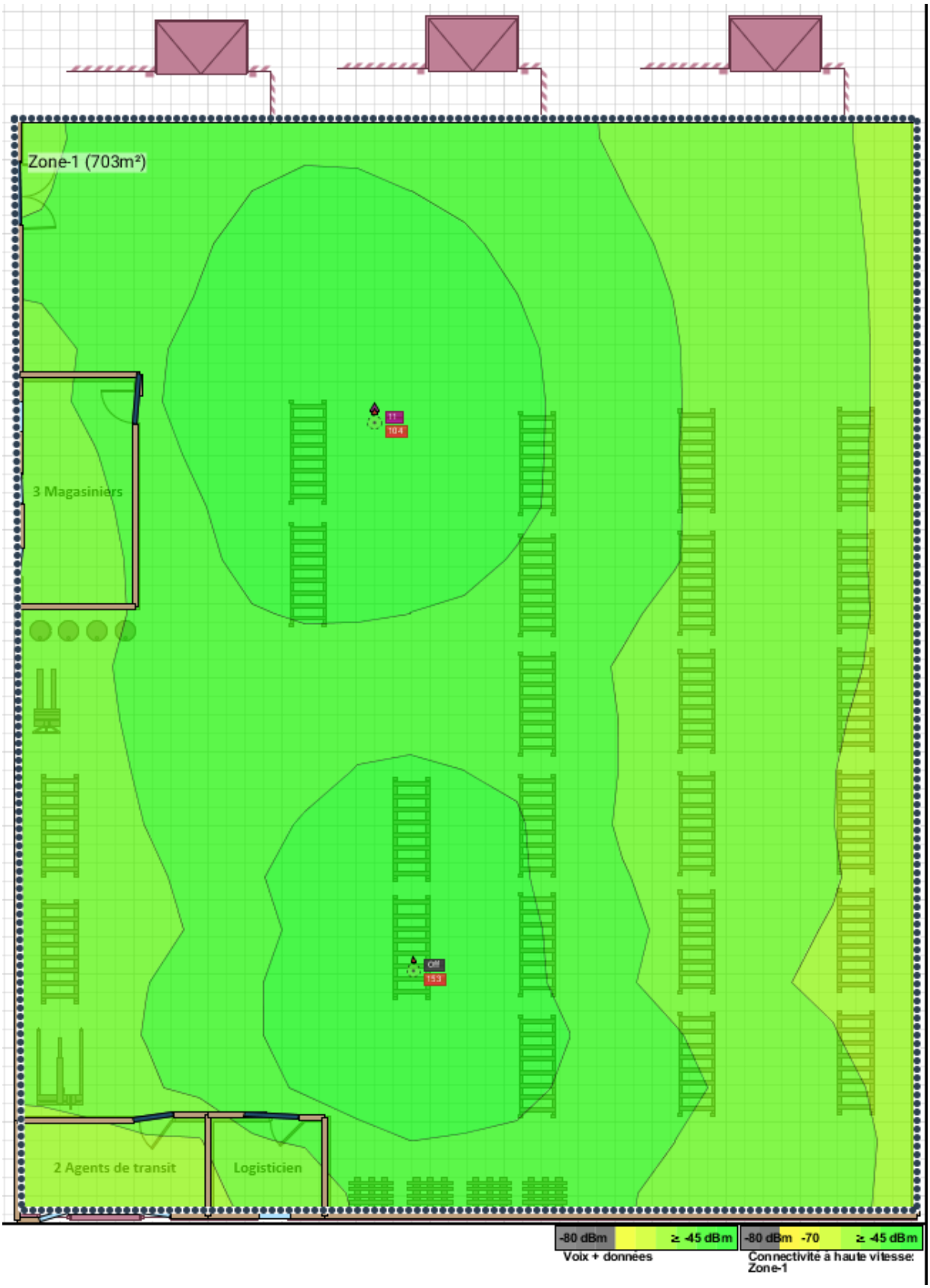


Figure 23 - Cartographie Wi-Fi de l'entrepôt d'Annecy

Figure 24 - Cartographie Wi-Fi des bureaux d'Annecy

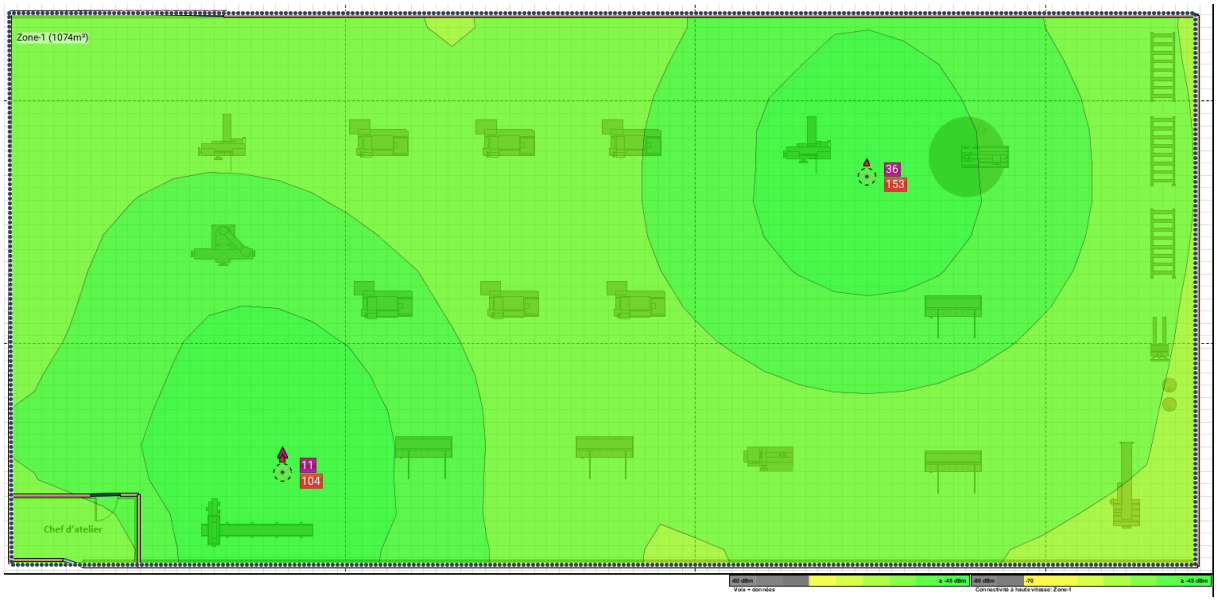


Figure 25 - Cartographie Wi-Fi de l'atelier d'Annecy

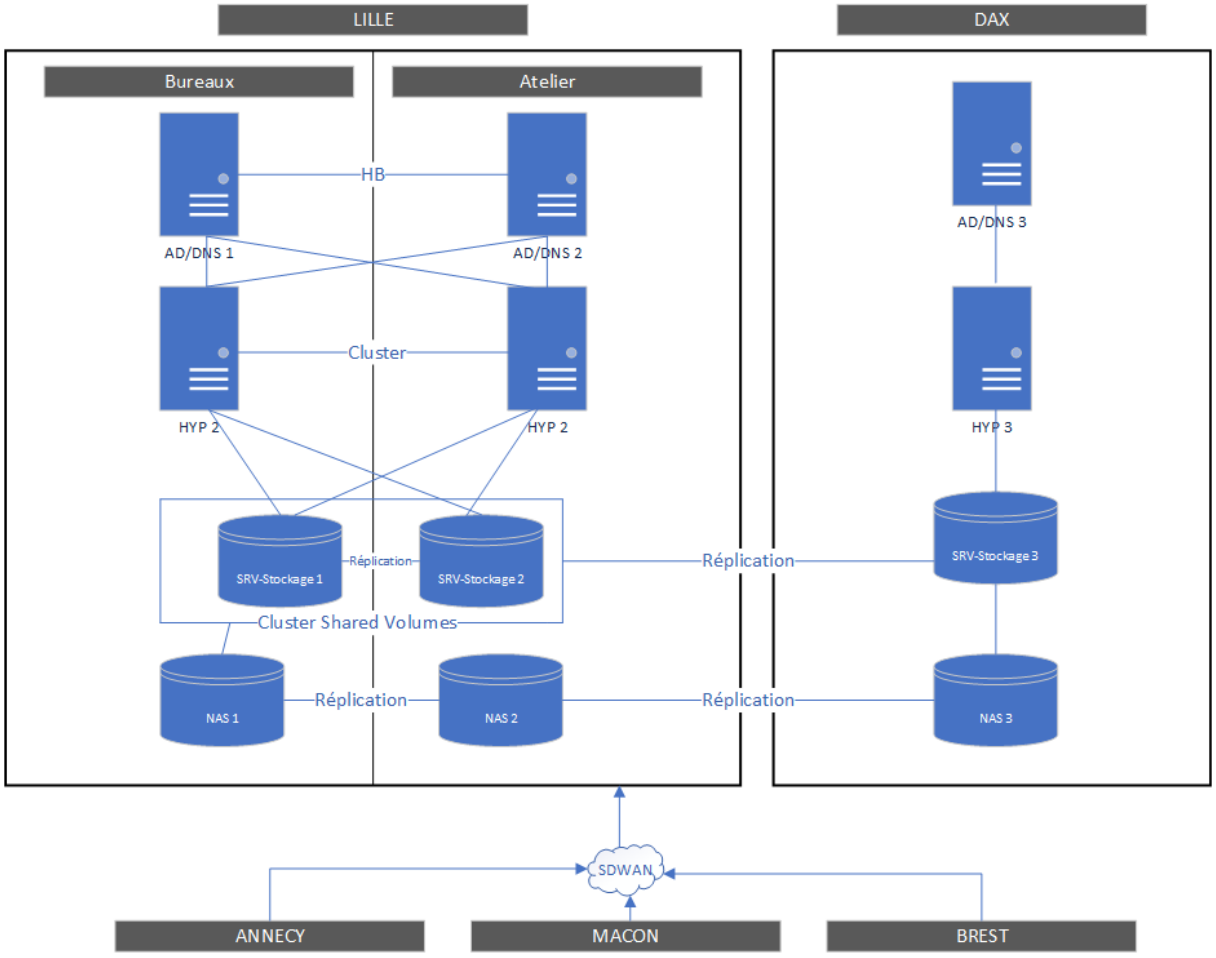
Au total sur le site d'Annecy, 6 points d'accès seront nécessaires.

Lille	9 points d'accès
Dax	6 points d'accès
Annecy	6 points d'accès
Magasins	5 points d'accès (1 par magasin)
Secours	5 points d'accès
TOTAL	31 points d'accès

Chaque point d'accès coûtant 69,39€ HT on totalise donc un budget total de **2151,09€ HT**

7. Architecture Système.

7.1 Schéma fonctionnel de l'infrastructure



Pour résumer ce schéma, nous aurons sur le site principal, Lille :

- 2 serveurs physiques avec un heartbeat pour l'AD et le DNS en réplication avec DAX
- 2 hyperviseurs physiques en cluster
- 2 serveurs de stockage en réplication avec DAX
- 2 NAS en réplication avec DAX

Et sur le site de Dax :

- 1 serveur physique répliqua pour l'AD et le DNS
- 1 hyperviseur physique
- 1 serveur de stockage
- 1 NAS

7.2 Détails des rôles et services de nos hyperviseurs

Les rôles et services de nos hyperviseurs HYP1, HYP2 et HYP3 seront :

- 1 serveur d'impression
- 1 serveur WDS (déploiement) et WSUS (mise à jour)
- 1 serveur de fichier (DFS)
- 1 serveur de sauvegarde (VEEAM)
- 1 serveur GLPI / PRTG
- 1 serveur antivirus
- 1 serveur DHCP

7.3 Virtualisation

La virtualisation permet d'héberger plusieurs systèmes d'exploitation sur un seul serveur physique. Elle permet des économies financières, car l'achat d'une machine pouvant héberger plusieurs VM coûte généralement moins cher que l'achat de 10 serveurs physiques.

Elle offre également la possibilité de centraliser la partie matérielle en un seul point, créant certes un plus grand risque si le matériel venait à défaillir, mais minimisant les chances de défaillances globales étant donné qu'il y a moins de matériel sur le parc de serveurs.

La virtualisation permet enfin de s'orienter vers une architecture dite de Haute Disponibilité ; une telle architecture permet de complètement nullifier le risque d'arrêt des services lors d'un incident matériel.

Choix d'une solution de virtualisation

Nous devons choisir une solution de virtualisation pour l'infrastructure système de la société Wood.
Nous avons réalisé un tableau comparatif de solution afin de déterminer quel était le meilleur hyperviseur dans notre situation.

Critères	Coefficient	Hyper-V	VMWare	Proxmox
Prix	2	3	1	5
Configuration requise	1	3	2	4
Temps nécessaire pour sauvegarde et restauration	3	4	4	2
Haute disponibilité des données	4	4	4	4
Facilité d'utilisation	3	4	3	3
Facilité d'installation	3	4	3	4
Support technique disponible	2	3	4	1
Facilité d'administration	2	4	4	4
Ressources disponibles en ligne	2	3	4	2
Efficacité pour virtualiser Windows Server	3	4	3	2
Optimisation des ressources	3	4	4	3
Total		3,75	3,65	3,07

Tableau 5 - Tableau comparatif de solution de virtualisation

Nous avons comparé les hyperviseurs Hyper-V, VMWare et Proxmox, et avons choisi Hyper-V.

Hyper-V est une solution de virtualisation de Microsoft intégrée directement dans Windows Server. C'est le meilleur hyperviseur du marché pour virtualiser des systèmes d'exploitation Windows par sa capacité à mutualiser les ressources.

Infrastructure de Virtualisation

Lille :

- 2 Hyperviseurs physiques avec Windows Server et Hyper-V
- NAS assurant la sauvegarde des VM et du serveur de fichier
- Serveur de stockage sur lequel les VM seront stockés et avec le serveur de fichier

Dax :

- Hyperviseur physique avec Windows server et Hyper-V de secours (pour le Plan de reprise d'activité)
- NAS récupérant la sauvegarde du NAS de Lille
- Serveur de stockage recevant les données du serveur de stockage de Lille. Ce serveur de stockage permettra une reprise d'activité en cas de perte du site de Lille

Haute Disponibilité :

La haute disponibilité fait partie intégrante de notre plan de continuité d'activité. Cela consiste à assurer une continuité de service pour nos machines virtuelles en réalisant un « Cluster » d'Hyper-V. En effet, en utilisant deux hyperviseurs physiques et en les connectant en cluster de basculement, si l'un des deux hyperviseurs venait à tomber, il y aurait alors un basculement automatique vers le second.

Pour mettre en place le cluster de basculement, il y a quelques prérequis :

- Disposer d'un Active Directory
- Installer le rôle Hyper-V sur nos hyperviseurs
- Dans notre cas, connecter les 2 hyperviseurs à notre espace de stockage réservé aux machines virtuelles.
- Connecter les deux hyperviseurs entre eux sur un réseau qui leur sera propre. (Heartbeat)
- Disposer d'un nombre impair de Nœuds dans le cluster, ou alors disposer d'un témoin pour le quorum

Afin de respecter le quorum, nous utiliserons l'hyperviseur de Dax comme témoin. Ainsi, nous aurons un nombre impair de votes afin que, dans le cas où l'un de nos 2 hyperviseurs de Lille tombe, l'autre puisse reprendre la charge de travail avec le nombre de votes nécessaires.

Plan de reprise d'activité

Nous avons un plan de reprise d'activité pour permettre un fonctionnement en mode dégradé si les serveurs de Lille venaient à tomber. En effet, chaque nuit, les données de Lille seront transférées sur l'infrastructure de Dax. Ainsi, si on venait à perdre le site de Lille, l'hyperviseur de Dax reprendrait le flambeau et ferait tourner les machines virtuelles avec des données anciennes d'une journée tout au plus, avec des performances réduites.
Le serveur de stockage ne pourra pas non plus excéder un jour de retard.

7.4 Le DNS

Le DNS pour Domain Name System est obligatoire pour le fonctionnement d'AD DS. Un serveur DNS externe au serveur AD DS peut être utilisé (Windows ou Linux). Cependant, il est possible d'installer le rôle DNS dans le même temps qu'un Domain Controller. Cela permet à AD DS d'être directement intégré au DNS sans configuration supplémentaire.

Pour faciliter la recherche d'un site donné sur Internet, le système de noms de domaine (DNS) a été inventé. Le DNS permet d'associer un nom compréhensible à une adresse IP. On associe donc une adresse logique, le nom de domaine, à une adresse physique ; l'adresse IP.

Le nom de domaine et l'adresse IP sont uniques. Le DNS permet au message d'atteindre son destinataire et non quelqu'un d'autre possédant un nom de domaine similaire. Il vous permet également de taper « https://www.google.com » sans avoir à saisir une longue adresse IP et d'accéder au site web approprié.

Résolution DNS

Lorsqu'un internaute saisit une adresse dans son navigateur, c'est donc un serveur DNS qui traduit cette adresse humainement compréhensible, en une adresse IP, compréhensible par les ordinateurs et les réseaux.

On appelle cela la « résolution DNS ».

Ce temps est d'autant plus faible que le serveur est performant : CPU (processeur), accès disque, et RAM (mémoire) doivent être correctement dimensionnés.

L'architecture logique du DNS est calquée sur la structure hiérarchique des noms de domaine.

Le DNS d'un niveau hiérarchique donné « délègue » au niveau inférieur le soin de traiter le sous-domaine suivant, jusqu'au dernier niveau qui, lui, connaît l'adresse IP correspondant au nom de domaine demandé.

Enregistrement DNS

Les enregistrements DNS associent un domaine à un service Web.

Il existe plusieurs types d'enregistrements DNS, mais dans la plupart des cas, seuls 4 ou 5 types d'enregistrements DNS sont utilisés :

- **Un enregistrement** : Utilisé pour faire pointer un domaine ou un sous-domaine vers une adresse IPv4. C'est la règle utilisée pour faire pointer un domaine comme exemple.com vers le serveur web où se trouve le site web exemple.com. (Note : Si un serveur web utilise une adresse IPv6 plutôt qu'une adresse IPv4, alors un enregistrement de type AAAA est utilisé plutôt qu'un enregistrement de type A).
- **Enregistrements CNAME** : Permettent d'associer un sous-domaine au domaine primaire ou canonique. Ce type de règle est couramment utilisé pour associer un sous-domaine www au domaine primaire, tel que www.exemple.com avec exemple.com.
- **Enregistrements MX** : Utilisés pour associer un domaine à un service de messagerie. C'est le type de règle utilisée si l'on souhaite que le mail par exemple.com soit livré à un service de messagerie spécifique tel que Gmail.
- **Enregistrements TXT** : Permettent d'associer n'importe quel texte arbitraire à un domaine. Le plus souvent, les enregistrements TXT sont utilisés pour associer des enregistrements SPF à un domaine afin d'améliorer la délivrabilité du courrier électronique et de protéger des spammeurs qui utilisent le nom de domaine à mauvais escient lorsqu'ils envoient du spam. Jetez un coup d'œil à notre blog détaillé sur l'authentification par courriel et sur les raisons de son importance.

7.5 L’Active Directory

Créé par Microsoft, Active Directory est un annuaire au sens informatique et technique chargé de répertorier tout ce qui touche au réseau comme le nom des utilisateurs, des imprimantes, des serveurs, des dossiers partagés, etc. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.

Il est possible d'interroger l'annuaire pour obtenir une liste des objets possédant des attributs, en formulant par exemple une requête du type : " Trouver toutes les imprimantes couleur de l'étage 2 ".

Au niveau sémantique, Active Directory est un annuaire LDAP, tout comme l'annuaire d'Exchange 5.5.

Actuellement dans l’entreprise WOOD, nous ne retrouvons pas de gestion centralisée (chaque site gère son propre domaine).

Nous allons donc mettre en place une nouvelle FORET dans un environnement Active Directory afin de créer le domaine WOOD.

Grâce à la technologie SD-WAN mise en place, nous pourrons interconnecter chaque site facilement.

Réplication de l'Active Directory

La réplication d'Active Directory est la méthode de transfert et de mise à jour des objets Active Directory d'un contrôleur de domaine à un autre.

Les connexions entre les contrôleurs de domaine sont établies en fonction de leur emplacement dans une forêt et un site. Chaque site d'Active Directory contient un ou plusieurs sous-réseaux, qui identifient la plage des adresses IP associées à ce site. En établissant une correspondance entre l'adresse IP d'un contrôleur de domaine et un sous-réseau, Active Directory identifie quels contrôleurs de domaine se trouvent dans quel site. Des connexions sont configurées entre les différents sites pour garantir que les objets Active Directory soient répliqués d'un site à l'autre.

La réplication principale se nomme « Réplication à maîtres multiples », cela consiste à garantir que chaque contrôleur de domaine peut recevoir des mises à jour pour les objets sur lesquels il fait autorité. Cela assure une tolérance aux défaillances dans un environnement Active Directory.

Pour réduire les risques de conflit, certaines modifications ne doivent pas être réalisées sur deux contrôleurs de domaines différents.

Voici les 5 rôles FSMO qui peuvent réaliser ces modifications :

- Maître d'attribution des noms de domaine

Le maître d'opération qui détient ce rôle est unique au sein de la forêt, et il est le seul autorisé à distribuer des noms de domaine aux contrôleurs de domaine lors de la création d'un nouveau domaine.

- Contrôleur de schéma

Le schéma désigne la structure de l'annuaire Active Directory ; c'est donc un élément critique au sein de l'environnement Active Directory. Cela implique l'exclusivité au sein de la forêt de ce maître d'opération, qui sera le seul – contrôleur de domaine – à pouvoir initier des changements au niveau de la structure de l'annuaire (schéma).

- Maître RID

Le RID (Relative Identifier) est un identifiant relatif unique au sein de chaque SID (Security Identifier), ceci afin d'être sûr d'avoir un SID unique pour chaque objet de l'annuaire. Étant constitué d'une partie commune qui correspond au domaine, le RID est essentiel pour rendre unique chaque SID. C'est là que le maître RID intervient.

- Maître d'infrastructure

Unique au sein d'un domaine, le contrôleur de domaine qui dispose du rôle de Maître d'infrastructure a pour objectif de gérer les références entre plusieurs objets.

Arrêtons-nous sur un exemple pour mieux comprendre ce que cela implique. Imaginons qu'un utilisateur d'un domaine A soit ajouté au sein d'un groupe du domaine B. Le contrôleur de domaine « Maître d'infrastructure » deviendra responsable de cette référence et devra s'assurer de la réplication de cette information sur tous les contrôleurs de domaine du domaine.

- Émulateur PDC

L'émulateur PDC (Primary Domain Controller) est unique au sein d'un domaine et se doit d'assurer cinq missions principales :

  - Modification des stratégies de groupe du domaine (éviter les conflits et les écrasements)
  - Synchroniser les horloges sur tous les contrôleurs de domaine (heure et date)
  - Gérer le verrouillage des comptes
  - Changer les mots de passe
  - Assure la compatibilité avec les contrôleurs de domaine Windows NT

Toutes ces partitions sont répliquées sur chaque contrôleur de domaine. La réplication intersites par défaut se fait toutes les 5 minutes.

Aussi, il existe un vérificateur de cohérence, KCC (Knowledge Consistency Checker) qui est présent sur les contrôleurs de domaine.

Dans notre infrastructure nous retrouvons deux contrôleurs de domaine sur le site principal de Lille en réplication dans un bâtiment différent, ainsi qu'une réplication sur un contrôleur de domaine à Dax.

Cette réplication mise en place entre contrôleurs de domaine apporte un haut niveau de tolérance de panne. Si jamais un contrôleur de domaine venait à subir une défaillance, son partenaire de réplication possédant également une copie de l'Active Directory pourrait prendre le relai.

7.6 Les Unités d'Organisation (OU)

Le réel objectif d'une OU, ce pourquoi elles ont été créées, est de déléguer les tâches d'administration et les droits sur les objets d'Active Directory. Les Organization Unit sont des conteneurs administratifs. Elles contiennent des objets ayant les mêmes besoins administratifs.

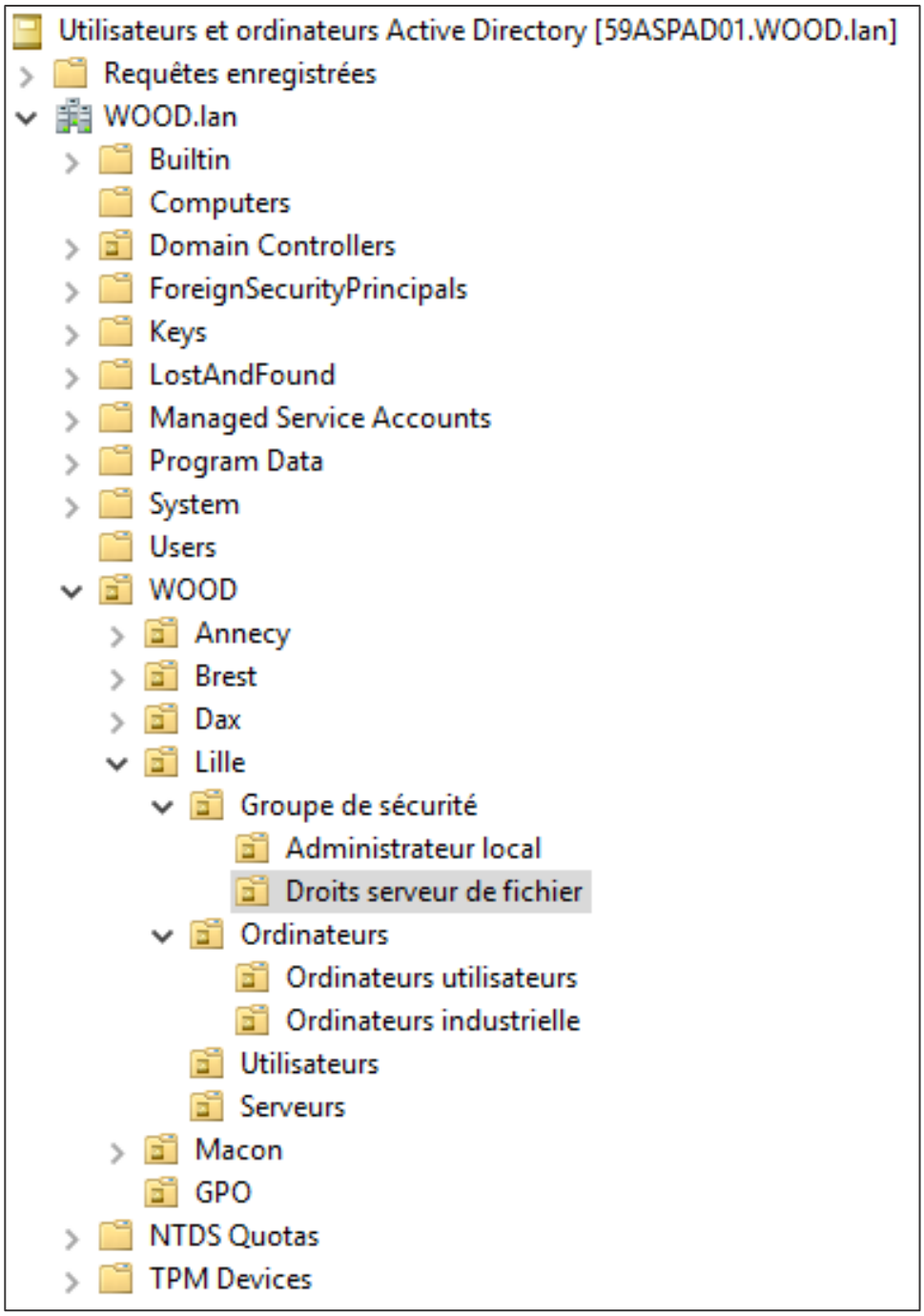
Elles ne présentent donc aucune similitude avec un classement par services ou autre. Les groupes sont faits pour cela, pas les Organization Unit. Les objets qui seront administrés de la même manière devront être placés dans la même Organization Unit indépendamment du service et des besoins d'affichage. On n'utilise pas les Organization Unit pour classer les utilisateurs.

Pour notre arborescence du domaine WOOD, nous proposons :

- Une OU principale **WOOD**
    - Une sous OU pour chaque site
        - Une sous OU pour les **Groupes de sécurité**
            - Une sous OU pour les **Administrateurs locaux**
            - Une sous OU pour les **Droits serveurs de fichier**
        - Une sous OU pour les **Ordinateurs**
            - Une sous OU pour les **Ordinateurs utilisateurs**
            - Une sous OU pour les **Ordinateurs industriels**
        - Une sous OU pour les **Utilisateurs**
        - Une sous OU pour les **Serveurs**
    - Une sous OU pour les **GPO**

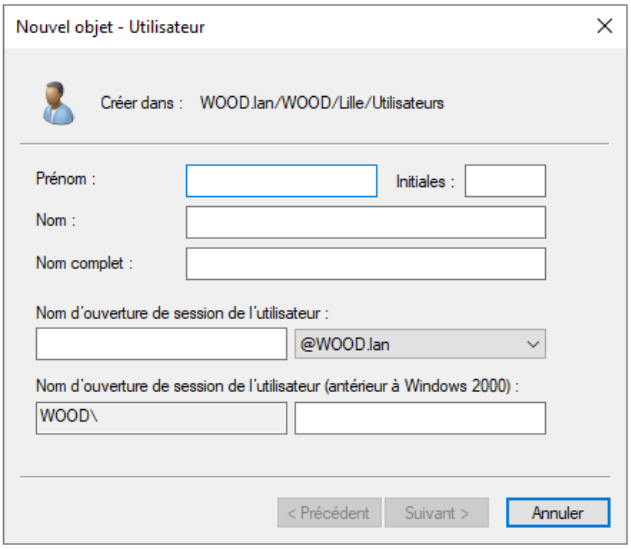
Chaque site aura la même arborescence.

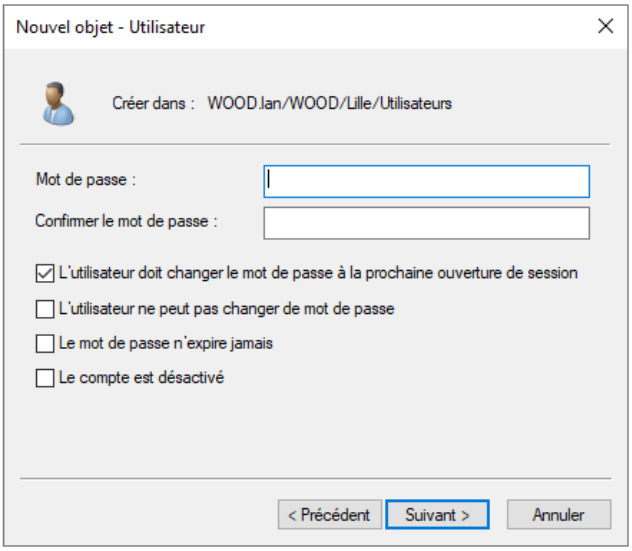
Exemple :


Utilisateurs et ordinateurs Active Directory [59ASPAD01.WOOD.lan]
Requêtes enregistrées
WOOD.lan
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
System
Users
WOOD
Annecy
Brest
Dax
Lille
Groupe de sécurité
Administrateur local
Droits serveur de fichier
Ordinateurs
Ordinateurs utilisateurs
Ordinateurs industrielle
Utilisateurs
Serveurs
Macon
GPO
NTDS Quotas
TPM Devices

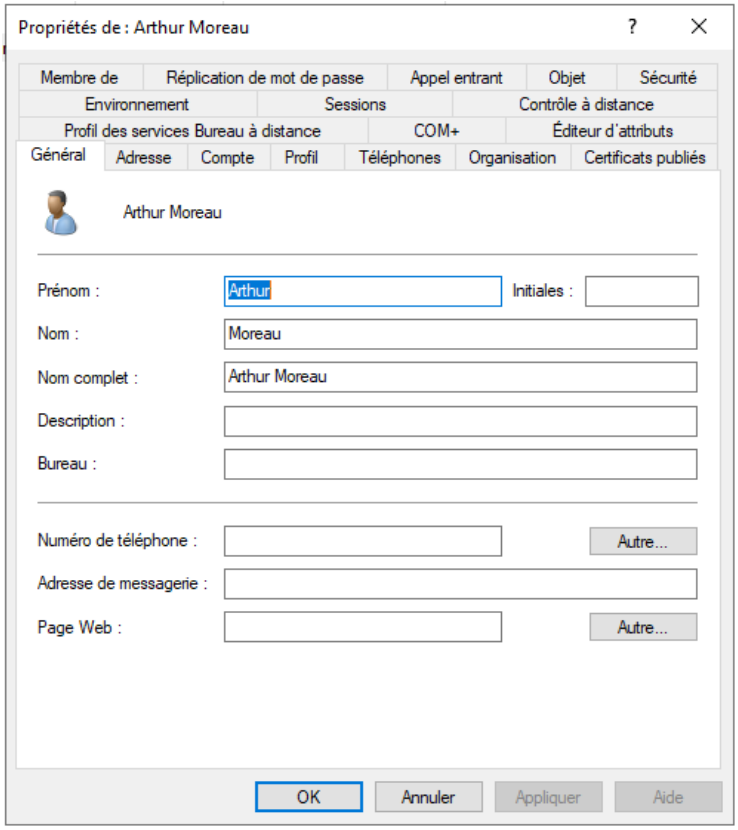
7.7 Les Utilisateurs

La gestion des utilisateurs se fait directement à partir de l'Active Directory.



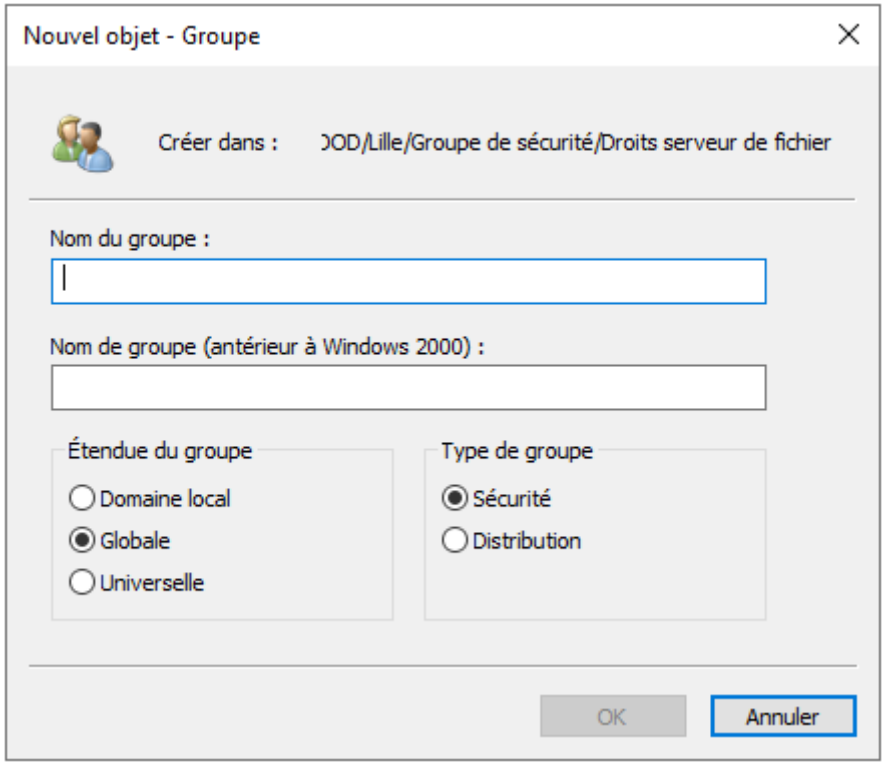


Une fois l'utilisateur créé, nous avons accès à plusieurs paramètres :



- Nom et prénom
- Adresse, service, description
- Groupe de sécurité
- Mot de passe
- ...

7.8 Les Groupes



Deux types de groupes sont disponibles :

- Les groupes de sécurité ;

Ce sont les plus utilisés et ceux qui seront manipulés le plus souvent. Ils permettent d'utiliser les groupes pour gérer les autorisations d'accès aux ressources.

Par exemple, dans le cas d'un partage sur lequel on souhaite accorder des autorisations d'accès, on pourra utiliser un « groupe de sécurité » pour donner des autorisations à tous les membres de ce groupe.

En résumé, ces groupes sont utilisés pour le contrôle d'accès, ce qui implique que chaque groupe de ce type dispose d'un identifiant de sécurité « SID ».

- Les groupes de distribution,

L'objectif de ce type de groupe n'est pas de contrôler les accès, mais plutôt d'élaborer des listes de distribution. Par exemple, créer une liste de distribution d'adresses e-mail en ajoutant des contacts.

De ce fait, ces groupes sont utilisés principalement par des applications de messagerie, comme Microsoft Exchange.

Comme il n'y a pas de notion de sécurité, ce type de groupe ne dispose pas d'identifiant de sécurité « SID ».

Et nous retrouvons aussi 3 types d'étendue :

- Domaine local :

Un groupe qui dispose d'une étendue « domaine local » peut être utilisé uniquement dans le domaine dans lequel il est créé. Avec ce type d'étendue, le groupe reste local au domaine où il est créé.

Cependant, les membres d'un groupe à étendue locale peuvent être bien sûr des utilisateurs, mais aussi d'autres groupes à étendues locales, globales ou universelles. Cette possibilité offre là encore une flexibilité dans l'administration.

Il peut être défini pour contrôler l'accès aux ressources uniquement au niveau du domaine local.

- Globale :

Un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base. Ainsi, si un « domaine A » approuve via une relation un « domaine B », alors un groupe global créé dans le « domaine A » pourra être utilisé dans le « domaine B ».

Un groupe global pourra contenir d'autres objets du domaine, et être utilisé pour contrôler l'accès aux ressources sur le domaine local et tous les domaines approuvés.

- Universelle :

Un groupe disposant de l'étendue « universelle » a une portée maximale puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt.

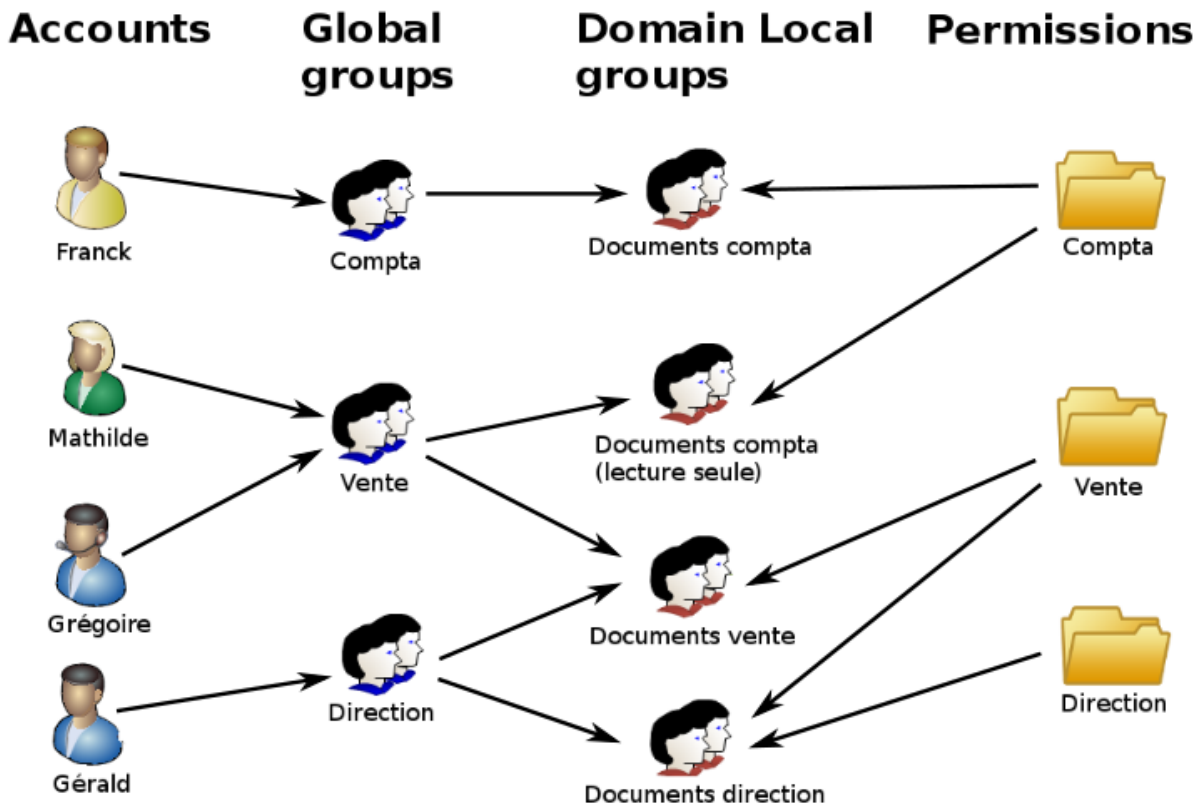
Un groupe universel peut contenir des groupes et objets provenant de n'importe quel domaine de la forêt. De la même manière, il est possible de l'utiliser pour définir l'accès aux ressources sur tous les domaines de la forêt.

Ainsi, avec ce type d'étendue on pourra consolider plusieurs groupes qui doivent avoir une portée maximale sur l'ensemble du système.

Dans le cas de la société WOOD, nous utiliserons des groupes de sécurité pour les accès DFS.

Nous mettrons en place la méthode recommandée par Microsoft : AGDLP (Account, Global group, Domain Local group, Permission).

Cette méthode consiste à affecter des utilisateurs (**Account**), dans des groupes globaux (**Global**), ajouter ces groupes globaux dans des groupes de domaine local (**Domain Local**) et pour terminer, attribuer aux groupes de domaine local des permissions NTFS sur les ressources (**Permissions**), les permissions NTFS étant les autorisations attribuées sur un objet dossier ou fichier.



7.9 Les GPO : Gestion des stratégies de groupe

Une stratégie de groupe est un ensemble d'outils intégrés à Windows Server qui permet au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à l'application de politiques.

Chaque stratégie dispose de ses propres paramètres, définis par l'administrateur système, et qui seront appliqués ensuite à des postes de travail, des serveurs ou des utilisateurs.

Il existe deux types de GPO :

- Les GPO Utilisateur : Les règles de ces GPO vont être appliquées dès l'identification de l'utilisateur (ouverture de sa session), et elles nécessitent dans certains cas, selon les opérations effectuées, d'être administrateurs de leur machine.
- Les GPO Ordinateur : Ces GPO vont s'appliquer au moment du démarrage de la machine et ne nécessitent, par la présente, aucune authentification d'administrateur (les opérations s'effectuant en compte système).

En plus de cela, on peut définir une GPO avec deux types de déploiement différents :

- Elles peuvent être publiées : dans ce cas, l'installation d'un programme ne se fera pas automatiquement, mais sera directement disponible dans les programmes et fonctionnalités du Panneau de configuration.
- Elles peuvent être attribuées : ici, les programmes seront installés automatiquement, sans que l'utilisateur le lance manuellement.

Nous allons créer plusieurs GPO, en voici quelque exemple :

- Mise en place d'une veille automatique au bout de 10 minutes
- Définir le serveur de mise à jour
- Modification du panneau de configuration
- Déploiement de logiciels
- Stratégie de mot de passe
    - Durée de vie minimum et maximum : 1/90 jours
    - Longueur minimum : 8
    - Historique de mots de passe : 6
    - Seuil de verrouillage de compte : 5
    - Durée de verrouillage du compte : 30 minutes

7.10 DHCP

DHCP ou Dynamic Host Configuration Protocol, est utilisé dans le processus d'attribution d'adresses IP aux périphériques. Plutôt que de demander aux administrateurs réseau d'attribuer manuellement les adresses IP à tous les périphériques réseau, il gère et automatise les configurations de manière centralisée.

Composants du DHCP

Pour utiliser le DHCP, il est important d'en comprendre tous les composants. Voici leur liste :

- Serveur DHCP : appareil en réseau exécutant le service DHCP qui contient les adresses IP et les informations de configuration associées.
- Client DHCP : le point de terminaison qui reçoit les informations de configuration d'un serveur DHCP.
- Pool d'adresses IP : plage d'adresses disponibles pour les clients DHCP. (*cf page 17*)

Site Lille						
	VLAN	TYPES	NOMBRE UTILISATEURS	PLAGES ADRESSES	MASQUES	NOMBRE ADRESSES
LILLE Plage totale 10.59.0.0/17	10	CLIENTS	139	de 10.59.10.1 à 10.59.10.254 / 24	255.255.255.0	254
	20	WIFI INVITE	30	de 10.59.20.1 à 10.59.20.30 / 27	255.255.255.224	30
	30	VOIP	75	de 10.59.30.1 à 10.59.30.126 /24	255.255.255.0	254
	40	SERVEUR	17	de 10.59.40.1 à 10.59.40.255 /24	255.255.255.0	254
	50	MANAGEMENT	52	de 10.59.50.1 à 10.59.50.62 /26	255.255.255.192	92
	60	DMZ	6	de 10.59.60.01 à 10.59.60.14/28	255.255.255.240	14

- Sous-réseau : les réseaux IP peuvent être partitionnés en segments appelés sous-réseaux. Ces sous-réseaux aident à garder les réseaux gérables.
- Location : la durée pendant laquelle un client DHCP détient les informations d'adresse IP.
- Relais DHCP : routeur ou hôte, il reçoit les messages clients diffusés sur ce réseau, puis les transmet à un serveur configuré.

7.11 Gestion et partage des données

Le DFS

Présentation

Accessible dans un environnement Microsoft sous Windows Server de son acronyme DFS qui signifie Distributed File System c'est-à-dire Système de fichiers distribués.

Ce système de fichier hiérarchisé permet de structurer les fichiers partagés sur différents serveurs du réseau de façon logique. Il permet de référencer un ensemble de partages qu'il faudra rendre accessibles de manière uniforme puis, de centraliser l'ensemble des espaces disponibles sur cet ensemble de partages.

Avec le DFS, l'utilisateur final ne visualise pas le nom du serveur sur lequel il accède pour lire les données ; c'est totalement transparent. L'intérêt étant que, dans le dans le cas où le serveur viendrait à changer à cause d'une panne ou pour cause d'évolution, le chemin d'accès restera le même.

Derrière un même chemin d'accès DFS peuvent se cacher plusieurs serveurs, contenant les mêmes données, avec une synchronisation entre ces serveurs grâce à DFSR (DFS Replication). Cette approche est très intéressante pour proposer de la haute disponibilité de données et de la répartition de charge.

Bien sûr, il est possible d'utiliser un chemin pour un serveur (1 pour 1), où chaque serveur hébergera des données différentes.

Lorsque l'on parle de DFS, trois termes sont importants à retenir et comprendre : Racine DFS, dossier et cible.

- **Racine DFS** : Point d'entrée principal d'un système DFS, la racine DFS contient le chemin d'accès aux différentes liaisons DFS qui lui sont associées. Il existe deux types de racines DFS, mais nous verrons cela en détail dans une autre partie.
- **Dossier** : Le dossier sera le nom du partage affiché côté client et dans la configuration du serveur, une liaison sera effectuée entre ce dossier DFS et la cible DFS afin de faire un lien entre les deux éléments. Certains dossiers n'utilisent pas de cible, uniquement dans le but de hiérarchiser les espaces de noms DFS. Les dossiers sont également appelés « Liaison DFS ».
- **Cible** : Serveur sur lequel sont situées les données, la cible représente le chemin d'accès vers le dossier partagé situé sur ce serveur.

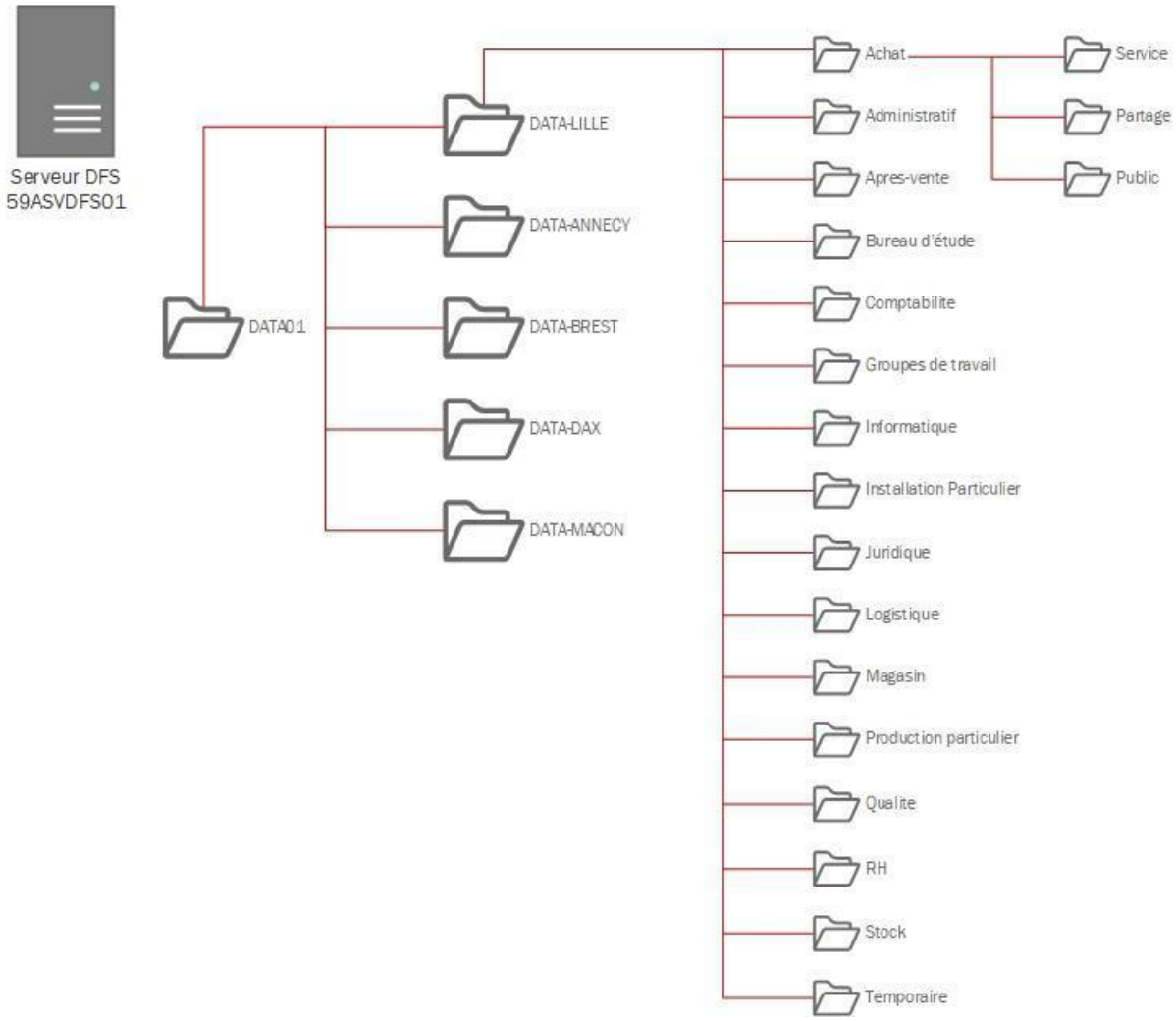
Ces 3 éléments sont essentiels à la mise en place d'une infrastructure DFS.

Les avantages

L'utilisation du DFS en entreprise présente plusieurs avantages non négligeables :

- Simplifier l'administration : si une cible DFS tombe, la liaison DFS peut être déplacée vers un autre serveur contenant une copie des données en changeant le dossier cible sur le serveur DFS. Du côté utilisateur, cela sera totalement transparent, car le nom ne changera pas.
- Le client DFS est intégré à Windows ce qui ne nécessite pas d'installation supplémentaire sur les postes clients
- Un nom unique permet d'accéder à toutes les ressources, il n'est pas nécessaire de mapper une lettre sur chaque ressource
- Fonction de mise en cache afin d'améliorer les performances
- Le DFS prend en compte les ACL situées au niveau du système de fichiers
- Remplacement d'un serveur simplifié, car l'espace de noms utilisés côté client n'est pas affecté
- Équilibrage de charge (si plusieurs ciblent par dossier DFS)
- Tolérance aux pannes (si plusieurs ciblent par dossier DFS)
- Évolution : Un espace disque supplémentaire peut être ajouté si l'espace disque actuel ne suffit plus

L’infrastructure de l’entreprise WOOD

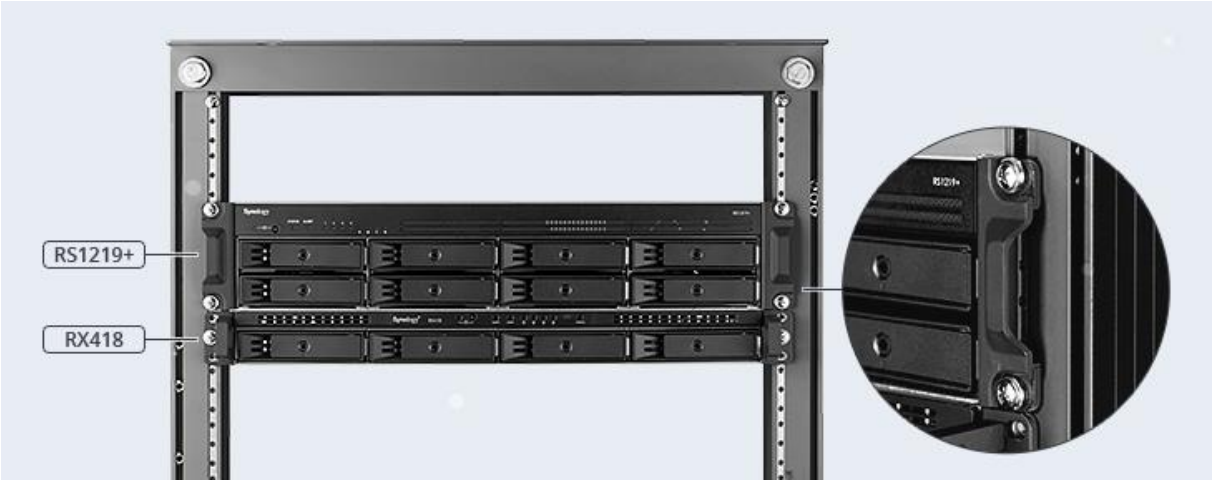


8. Gestion du stockage

8.1 Stockage des machines virtuelles

Tous les Datacenter de la société WOOD (Lille Bureau, Lille Atelier et Dax) bénéficieront de serveur NAS Synology. Nous avons choisi les modèles RS1219+ PCI Carte Réseau 10G. Ses NAS permettront le stockage des machines virtuelles.

Le RS1219+ prend en charge jusqu'à 12 disques lorsqu'il est raccordé à une unité d'expansion RX418. Comme les RS1219+ et RX418 ne font que 30 cm de profondeur, ils s'adaptent parfaitement dans un montage rack.

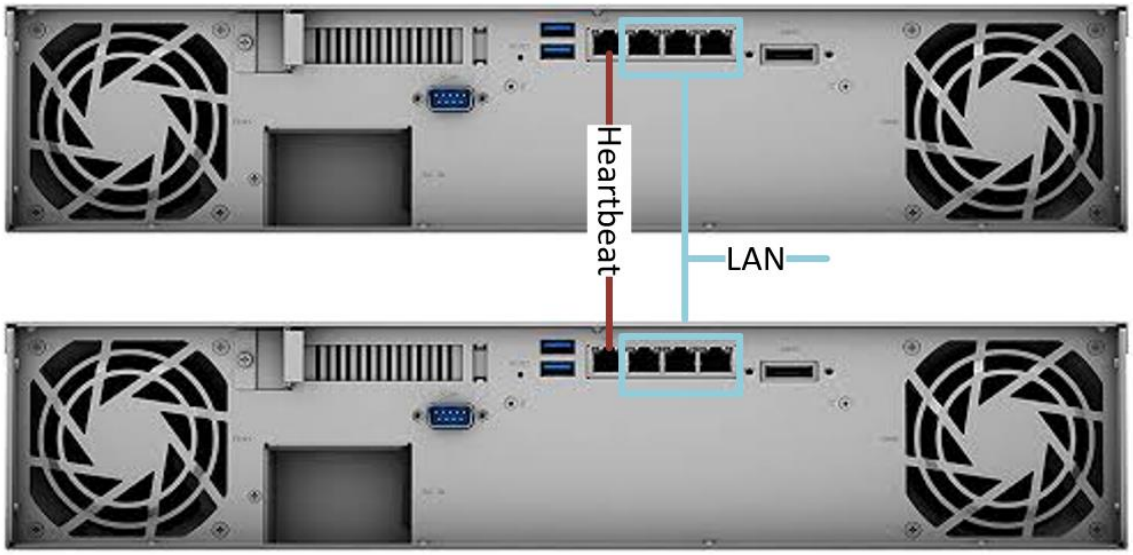


Le stockage iSCSI de Synology prend en charge la plupart des solutions de virtualisation afin d'améliorer l'efficacité au travail avec une interface de gestion simple.

La technologie SHA (Synology High Avability) sera configurée afin de mettre les deux serveurs en cluster. Cette solution permettra une haute disponibilité pour assurer les fonctionnements des services.

SHA permet d'associer les deux serveurs NAS dans un cluster de haute disponibilité. Cela assure des services de stockage avec une disponibilité maximisée du système.

Les serveurs NAS RS1219+ seront équipés d'une carte d'extension 10G pour permettre aux serveurs, un plein potentiel avec la mise en place du réseau. Il est également équipé de 4 ports Ethernet 1Gb/s. Ils serviront à la mise en place du cluster NAS grâce au Heatbeat.



On retrouve 8 emplacements de disques :

- 5 baies seront remplies par : **WD Gold Enterprise Class SATA Hard Drive de 4To.**

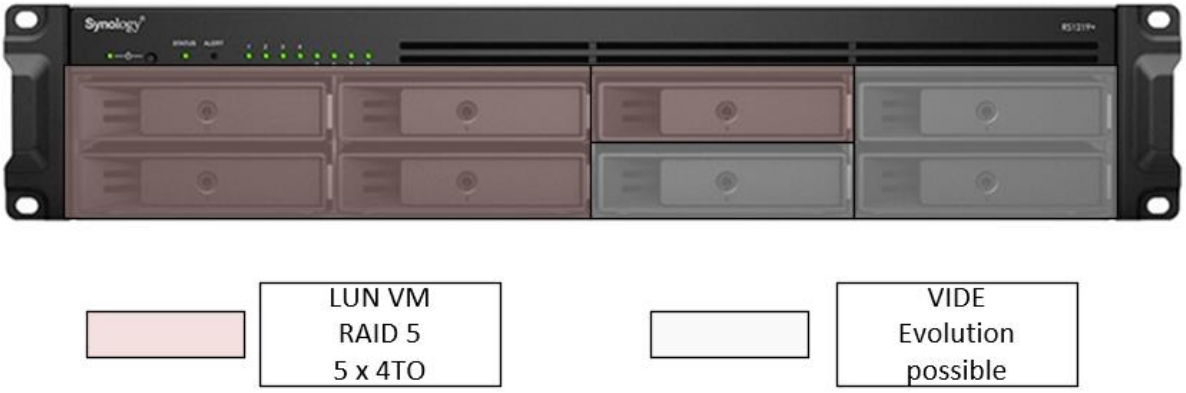


Figure 26 - Serveur de stockage

8.2 Stockage des sauvegardes

Nous proposons un NAS Synology DS1819+ qui permettra de faire les sauvegardes des machines virtuelles et également des données utilisateurs. Notre choix s'est dirigé vers Synology pour associer performance, fiabilité et rationalisation des coûts.

Le NAS sera accompagné de 3 disques de 10To pour permettre la création d'un LUN de sauvegarde en RAID 5.

On retrouvera ce genre d'équipement à Lille dans les deux salles serveur, mais également à Dax.

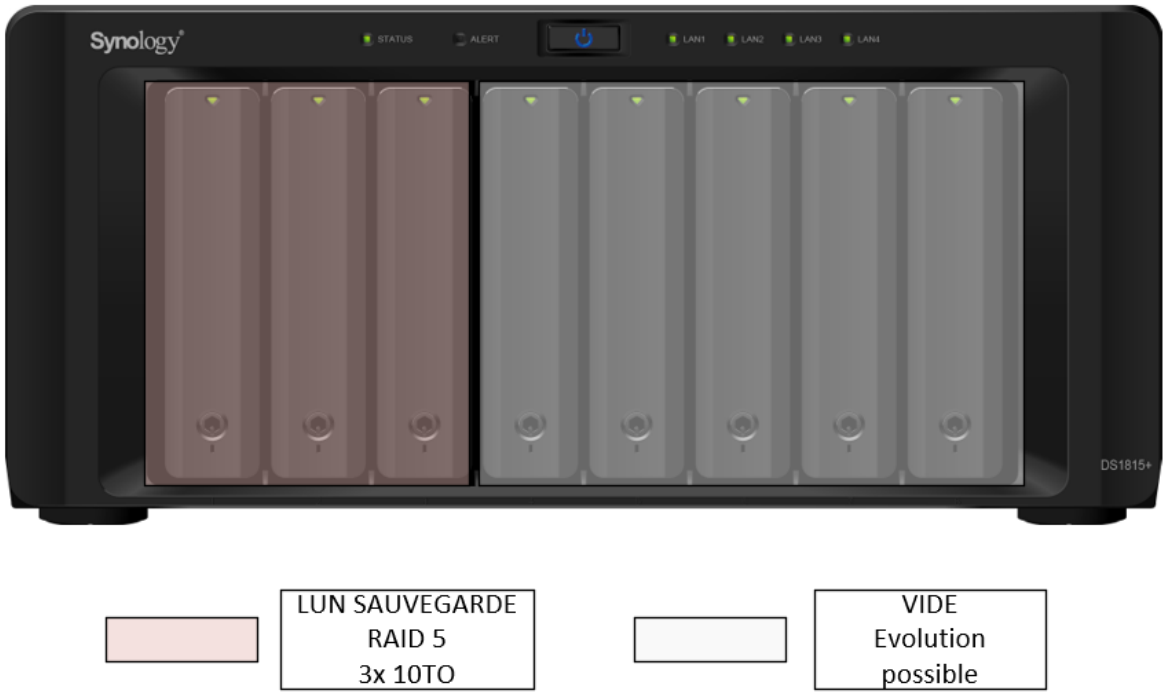


Figure 27 - NAS DS1819+

8.3 Stockage des magasins

Nous proposons également de mettre en place des NAS DS1819+ dans les magasins, pour offrir au magasin une plus grande autonomie et la possibilité de gérer leurs stockages. En effet, cela pourra permettre, dans le futur, la mise en place de vidéo surveillance pour enregistrer directement sur le NAS.

Le NAS sera accompagné de 3 disques de 4To bien sûr, avec un RAID 5.

	LUN SAUVEGARDE RAID 5 3x 4TO		VIDE Evolution possible

9. La téléphonie.

9.1 Existant téléphonie

Dans le tableau ci-dessous, nous avons déterminé le nombre de lignes téléphoniques au sein de l'entreprise WOOD et ainsi estimé le coût annuel.

Afin de déterminer le coût annuel, nous avons pris en compte deux facteurs :

- Prix d'une ligne analogique mensuel : 15€/mois
- Nombre d'utilisateurs ayant un téléphone.

	Utilisateurs	**Détails téléphone**
TOTALE DIRECTION	4 utilisateurs	4 Fixes
TOTAL RH	14 utilisateurs	14 Fixes
TOTALE PROD	175 utilisateurs	18 Fixes
TOTAL DC	138 utilisateurs	138 Mobiles

Total :	**331 utilisateurs**	**174 téléphones totaux**

Nombre de téléphones existant :	174
Coût mensuel 15€ :	2 610 €
Coût annuel :	31 320 €

Nous pouvons voir que le coût annuel de tous les téléphones est de 31 320 €, ce qui n'inclut pas les contrats de maintenance et les divers changements de téléphone dû aux différentes pannes.

La solution actuelle de téléphonie a un coût important pour l'entreprise et ce pour une technologie vouée à disparaître.

Nous préconisons l'évolution de la solution téléphonie en proposant de passer sur une technologie VoIP, qui sera de faibles coûts avec un retour sur investissement de quelques mois.

9.2 La voix sur IP

Définition :

VoIP est un acronyme qui signifie Voice Over Internet Protocol, ou en d'autres termes, la transmission de la voix via Internet. C'est une technologie qui permet de délivrer des communications vocales ou multimédias (vidéo par exemple) via le réseau Internet (IP).

Les avantages d'un système VoIP pour une entreprise :

Les sociétés qui choisissent un système VoIP au lieu d'un standard téléphonique classique (sur réseau câblé) bénéficient de multiples avantages, dont notamment la réduction des factures téléphoniques, une plus grande mobilité, ainsi qu'une plus grande productivité.

Le principe de fonctionnement :

Dans la communication par VoIP, la voix est traitée de la même manière que les autres données numériques transmises via le réseau Internet. Elle est d'abord captée par le microphone sous forme d'un signal analogique, puis envoyé via le réseau Internet. Ce signal analogique doit être converti en un signal numérique, puis il est ensuite comprimé par un codec.

La voix est alors numérisée puis regroupée en paquets de données numériques, prêtes à être transportées par le réseau via le protocole IP.

Les protocoles dits de « signalisation » :

Les principaux protocoles utilisés pour l'établissement des connexions en voix sur IP sont :

- H.323 ;
- IAX (Asterisk) ;
- Jingle ;
- MGCP ;
- SCCP (propriétaire Cisco Systems) ;
- SIP ;
- UA/NOE (propriétaire Alcatel-Lucent) ;
- UNISTIM (propriétaire Nortel).

Ce sont des normes dont les spécifications doivent être respectées par les appareils de téléphonie sur IP pour assurer l'interopérabilité.

Les deux protocoles les plus utilisés actuellement dans les solutions VoIP présentes sur le marché sont le H.323 et le SIP.

- **Protocole H.323 :**

Plus qu'un protocole, H.323 ressemble davantage à une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

Les messages de signalisation sont ceux que l'on envoie pour demander d'être mis en relation avec une autre personne, qui indiquent que la ligne est occupée, que le téléphone sonne… Cela comprend aussi les messages que l'on envoie pour signaler que tel téléphone est connecté au réseau et peut être joint de telle manière.

- **Protocole SIP,**

Session Initiation Protocol (dont l'abréviation est SIP) est un protocole de la couche applicative du modèle OSI (et non de la couche session comme son nom pourrait le laisser croire), conçu pour établir, modifier et terminer des sessions multimédias.

Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de médias utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol).

SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange. Cependant le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audios et vidéos. SIP remplace progressivement H.323.

- **Comparaison entre H.323 et SIP :**

	H.323	SIP
Avantages	Maturité du protocole	Simple à mettre en place
Coût	Élevé	Faible
Protocole de transport	TCP	TCP ou UDP
Complexité	Élevé	Faible
Nombre d'échange pour établir la connexion	6 - 7 échanges	1 - 5 échanges

Les protocoles dits de « transport de la voix » :

Le transport de la voix sur IP est relativement complexe. La première étape est la numérisation du signal analogique capté par le microphone. Selon le protocole utilisé pour transporter le signal numérique, une étape complémentaire d'encodage peut être nécessaire, notamment pour compresser les signaux. Ensuite, les informations sont découpées en trames pouvant circuler sur un réseau informatique.

Divers protocoles peuvent alors être utilisés pour acheminer les informations aux destinataires. Ainsi le protocole RTCP est utilisé pour contrôler le transport des paquets RTP.

- **Protocole RTP,**

Le protocole RTP (Real-time Transport) assure la gestion des flux multimédia en mode UDP, il permet aussi la transmission en temps réel des données audio et vidéo sur des réseaux IP et il est utilisé pour les appels téléphoniques simples, les audio ou les visioconférences.

Le Protocole RTP permet l'identification de type de l'information transportée, l'ajout des numéros de séquence des donnés émise ainsi le contrôle l'arrivée des paquets à la destination.

- **Protocole RTCP,**

Le protocole de contrôle (RTCP : Real Time Control Protocol) assure la bonne qualité de service des communications RTP, il permet l'envoi d'un rapport sur la qualité de service, l'identification et le contrôle de la session.

Les codecs de la VoIP :

La voix est ce qui permet aux humains d'échanger de l'information, de communiquer, et de faire passer des émotions. Il s'agit d'un phénomène physique complexe. Lorsque l'on parle, nous produisons un ensemble de son possédant des niveaux de fréquences différents (grave, médium, aigüe…).

La voix captée par le microphone du combiné fournit un signal analogique. Pour l'envoyer sur un réseau TCP/IP (numérique), il va falloir convertir ce signal analogique en un signal numérique en format PCM (Pulse Code Modulation), par exemple à 64 kb/s.

Une fois convertie, la voix, ainsi numérisée, doit être compressée grâce à un codec (Codeur/Décodeur) pour l'insérer dans un paquet IP. Le codage doit offrir la meilleure qualité de voix possible, pour un débit le plus faible possible et un temps de compression le plus court possible.

Il existe plusieurs techniques de codage, chacune étant mesurée de façon totalement subjective par une masse de population prise au hasard. Elle doit noter chaque codage par un chiffre de 1 à 5 (1 = insuffisant - 5 = excellent). Cette technique s'appelle le MOS.

Les principaux codecs sont :

- G.711 → MOS : 4.1
- G.723.1 → MOS : 3.9
- G726 → MOS : 3.85
- G.729 → MOS : 3.92

9.3 La téléphonie sur IP

Définition :

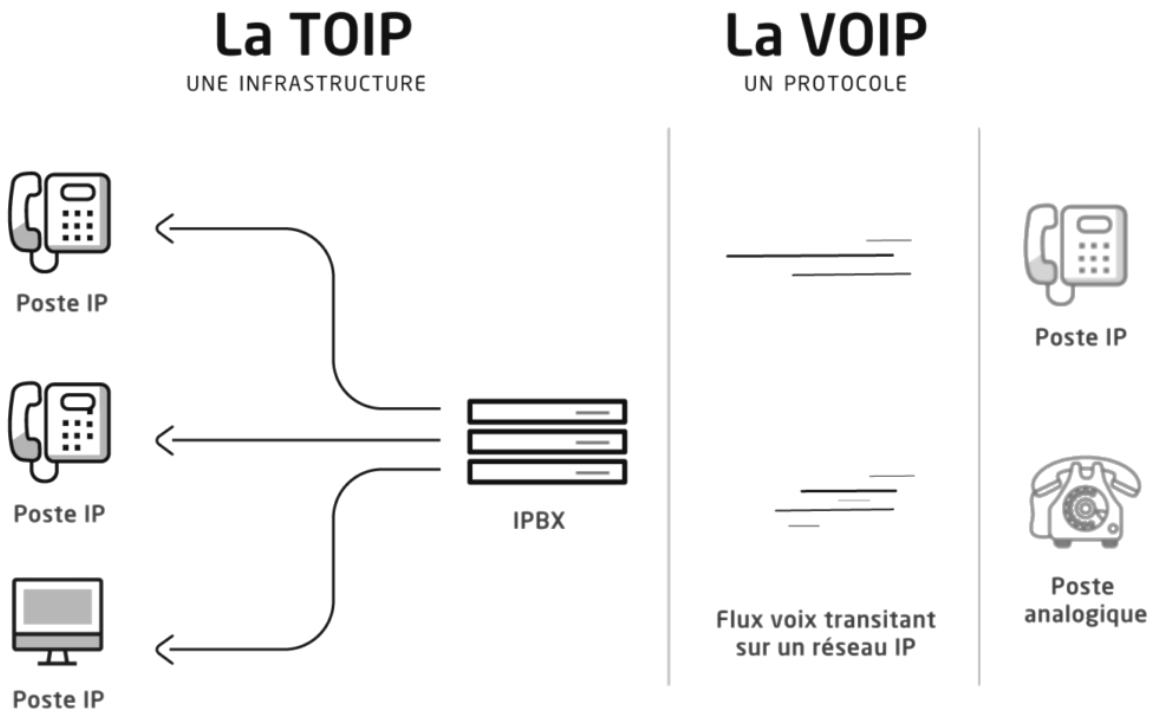
La TOIP signifie que tout le système de téléphonie de l'entreprise fonctionne en IP depuis le téléphone. Concrètement, ce n'est pas que la voix qui va transiter en IP sur les réseaux opérateurs, mais avant tout le système de téléphonie qui va fonctionner sur le protocole IP grâce à un IPBX. Les téléphones vont donc être branchés directement sur le réseau informatique de l'entreprise en fonctionnant sur le même protocole, le même langage donc, que l'informatique.

Les avantages d'un système ToIP pour une entreprise :

Lorsqu'un centre d'appel ToIP vient remplacer un standard téléphonique classique en entreprise, les fonctions de ce dernier continuent à être remplies. La ToIP va toutefois bien au-delà en initialisant et gérant l'intégralité des communications téléphoniques de la structure. Les professionnels sont de plus en mesure de profiter de fonctionnalités autrefois réservées aux grandes entreprises comme le serveur vocal interactif accueillant les appels extérieurs ou les messages vocaux arrivant directement sur la boîte mail. De façon concrète, les utilisateurs se servent d'un softphone compatible SIP (protocole des logiciels VoIP) ou d'un terminal ToIP pour profiter du réseau téléphonique de l'organisation.

9.4 VoIP et ToIP

Pour simplifier à son paroxysme la comparaison, disons que la VOIP coûte moins que la TOIP. En effet, la VOIP est un protocole sur lequel il est possible de basculer en mettant en place un convertisseur. Mais d'un point de vue fonctionnement, ce changement sera tout à fait transparent sans aucun apport matériel. En revanche, la TOIP étant une infrastructure, l'investissement est plus conséquent : IPBX (qui peut être hébergé dans le cloud avec une solution Centrex), postes IP, routeurs, etc.



9.5 La migration du système

Considérant que l'infrastructure de télécommunications de l'entreprise comprend des équipements de divers fabricants, nous aurons besoin de méthodes fiables pour intégrer et optimiser l'infrastructure réseau.

Actuellement, l'entreprise est équipée de réseau physique distinct pour la donnée et la voix. Chaque site possède son propre réseau local (LAN). L'entreprise WOOD est équipée d'un réseau étendu (WAN) sur lequel transitent les protocoles IP qui sont utilisés pour échanger des données informatiques.

Nous préparerons le réseau informatique de l'entreprise WOOD pour qu'ils puissent recevoir la téléphonie IP du côté du réseau local (LAN) et recevoir la voix sur IP du côté du réseau étendu (WAN).

Nous aurons donc une seule infrastructure commune de données, de voix et de vidéoconférence.

L'entreprise bénéficiera d'une architecture de communication fiable, qui réduira les frais mensuels.

9.6 Mise en place de la VoIP dans l'entreprise

La téléphonie avec Microsoft Office 365

Le système téléphonique de Microsoft Office 365 active le contrôle d'appel et les fonctionnalités PBX dans le Cloud avec Microsoft teams et Skype entreprise online.

Grâce au système téléphonique, les utilisateurs peuvent utiliser teams ou Skype entreprise Online pour passer et recevoir des appels, transférer des appels, activer ou désactiver les appels.

Pour passer et recevoir des appels, les utilisateurs du système téléphonique peuvent utiliser leurs appareils mobiles, un casque avec un ordinateur portable ou un PC, ou l'un des nombreux téléphones IP compatibles avec teams et Skype entreprise online. Les administrateurs de système téléphonique peuvent gérer les options d'appel et les paramètres à partir de la même console utilisée pour la messagerie, la collaboration, etc.

Les appels entre les utilisateurs sont gérés en interne au sein du système téléphonique et ne sont jamais dirigés vers le réseau téléphonique public commuté (RTC). Cela concerne également les appels entre les utilisateurs de l'entreprise qui se trouvent dans des zones géographiques différentes, et cela présente l'avantage non négligeable de supprimer les coûts liés à la grande distance de ces appels internes.

Le Réseau Téléphonique Commuté (RTC)

Pour les appels hors de l'entreprise, Microsoft fournit plusieurs options pour connecter le système téléphonique au réseau téléphonique public commuté (RTC).

Le système téléphonique peut être connecté au RTC de l'une des deux manières suivantes :

- Acheter un forfait d'appels Microsoft (national ou national et international). Le forfait d'appel Microsoft est une solution tout-en-un cloud avec Microsoft comme opérateur PSTN.
- Utiliser l'infrastructure de téléphonie existante pour une connectivité PSTN locale.

Les services téléphoniques Microsoft Office 365

- **Standards automatiques** : les standards automatiques peuvent être utilisés pour créer un système de menus qui permet aux appelants externes et internes de se déplacer dans le système pour localiser et transférer des appels vers des utilisateurs ou services de l'entreprise.

- **Files d'attente d'appels** : les messages d'accueil de la file d'attente peuvent être utilisés lorsque quelqu'un appelle un numéro de l'entreprise. Ces messages d'accueil incluent la possibilité de mettre automatiquement les appels en attente et celle de rechercher le prochain agent d'appel disponible pour gérer l'appel tandis que les appelants écoutent de la musique durant l'attente. Il est possible de créer des files d'attente d'appels uniques ou multiples.

- **Boîte vocale** : lorsque l'entreprise dispose d'une licence de système téléphonique pour un utilisateur, celui-ci est en mesure d'obtenir la boîte vocale laissée par les appelants. Le message vocal Cloud est configuré automatiquement et approvisionné pour les utilisateurs lorsqu'il est attribué une licence de système téléphonique et un numéro de téléphone.

Le service Cloud PBX

Comme son nom l'indique, cette fonctionnalité propose le remplacement de l'IPBX traditionnel par un PBX dans le cloud.

C'est donc un équipement qui permet de distribuer et gérer des numéros de téléphone pour les collaborateurs. Possibilité de gérer les SDA, le nombre de canaux…

Tout comme dans un schéma traditionnel, les communications internes sont gratuites et toutes les personnes ne disposent pas forcément d'une ligne directe.

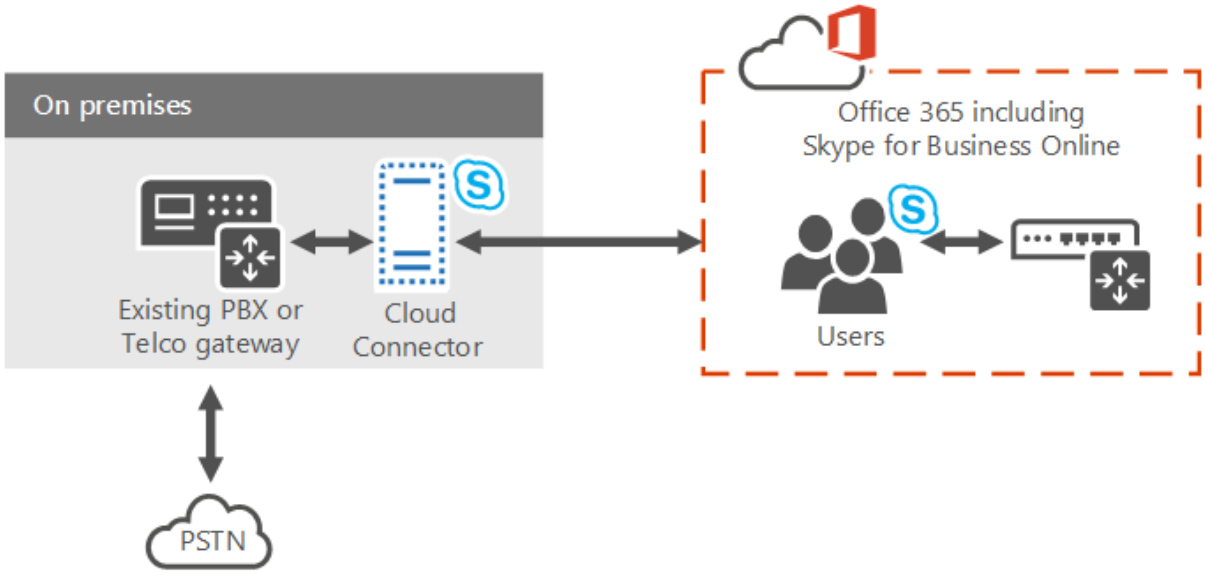


Figure 28 - Schéma Cloud PBX

Pour l'entreprise WOOD nous choisirons le Cloud PBX de chez 3CX, compatible avec nos licences Microsoft Office 365 E5.

Le tarif annuel pour 140 utilisateurs à l'année est de 1954€. Cette solution est extensible.

9.7 Mise en place de la ToIP dans l'entreprise

Licence Office 365 Entreprise E5

Afin de mettre en place la solution ToIP dans l'entreprise WOOD, nous avons choisi de prendre un abonnement à l'offre Office 365 Entreprise E5.

La licence Office 365 Entreprise E5 est la version la plus complète, et elle intègre des services avancés de gestion des communications vocales avec le module Skype Entreprise Online.

Cette version permet :

- La gestion de réunions en ligne
- Un système de visioconférence
- Un système d'audioconférence

9.8 Le choix du matériel téléphonique

Le système audioconférence :

Yealink - CP960 Skype for business

- Téléphone de conférence IP DECT
- Écran LCD 5" haute visibilité avec clavier tactile
- Trois microphones HD Voice, Full Duplex 360° jusqu'à 6m
- Connexion USB, Bluetooth, Wifi pour PC et smartphone
- Permets l'enregistrement des appels
- Optimisé Skype for Business

Le système IP Phone :

Yealink T46S Skype For Business:

- Téléphone de bureau
- POE, autoalimenté
- Grand écran LCD couleur : 4.3"
- Son Optima HD Voice Yealink
- Ports Ethernet Gigabit et port USB 2.0 intégré
- Wifi via WF40 et Bluetooth via BT40
- Version optimisée Skype For Business

Le système de téléphone mobile :

Nous équiperons chaque utilisateur devant disposer d'un téléphone mobile d'une licence Office 365 E5 afin qu'il puisse disposer des fonctionnalités de Skype Enterprise sur son propre smartphone.

On appelle ça le BYOD (Bring Your Own Device) : l'employeur autorise ses salariés à utiliser leurs équipements privés pour remplir leurs missions professionnelles. Cette option présente un avantage certain : disposer d'un matériel qui correspond à son utilisateur et dont il maîtrise l'usage de A à Z.

9.9 Mobile Device Management

Définition

Cette technologie est apparue dans les années 2000 dans le but d'assurer la gestion des terminaux d'appareils mobiles. Actuellement, le système est utilisé pour la gestion des flottes avec les Smartphones, les tablettes et parfois même les ordinateurs portables. En clair, ce système concerne tous les appareils ayant une forme mobile.

Le Mobile Device Management a pour rôle principal d'assurer que les flottes de la société soient à la fois harmonisées et sécurisées. Il doit permettre aux entreprises d'avoir un meilleur contrôle de chacune de leurs dépenses télécoms.

Comment fonctionne le MDM ?

Le MDM est avant toute chose un logiciel dit Firmware. Il est essentiellement utilisé pour gérer le système d'exploitation des appareils portables. Il va ainsi servir à installer les mises à jour sur des téléphones et tablettes à distance. Véritable outil de suivi, il permet également de faire les inventaires des appareils utilisés, la consultation des différentes communications, etc.

Puisque chaque appareil constitue un terminal, tous les appareils vont constituer ensemble un parc de terminaux. Un monitoring est de ce fait indispensable. La solution MDM peut assurer ce suivi ; elle permet un remote controle ou un contrôle à distance pour dépanner les utilisateurs de ces mobiles surtout dans le cas où ceux-ci sont bloqués.

Le Mobile Device Management est généralement divisé en deux grandes catégories. Les systèmes les plus traditionnels sont installés de manière on premise, c'est-à-dire au sein même de l'entreprise. La deuxième catégorie fonctionne via un système sur internet basé sur des solutions dans le cloud.

La sécurité

Puisque cette solution MDM est très puissante et permet un suivi à distance des communications et activités sur un appareil mobile, elle permet également de sauvegarder et de restaurer les comptes d'utilisateurs. Elle donne ainsi accès à l'offre, aux emails et aux différents comptes Internet disponibles sur l'appareil.

Le Mobile Device Management conserve également les données relatives à ces comptes, car celles-ci sont logiquement enregistrées sur les serveurs de l'entreprise et peuvent à tout moment être transférées sur un autre mobile. Le plus grand avantage avec cette technologie c'est qu'elle permet une sécurisation efficace des données personnelles et professionnelles.

En effet, dans le cas d'une perte ou piratage de l'appareil par exemple, le système MDM permet de supprimer tous les fichiers et data sur le mobile avant qu'ils soient

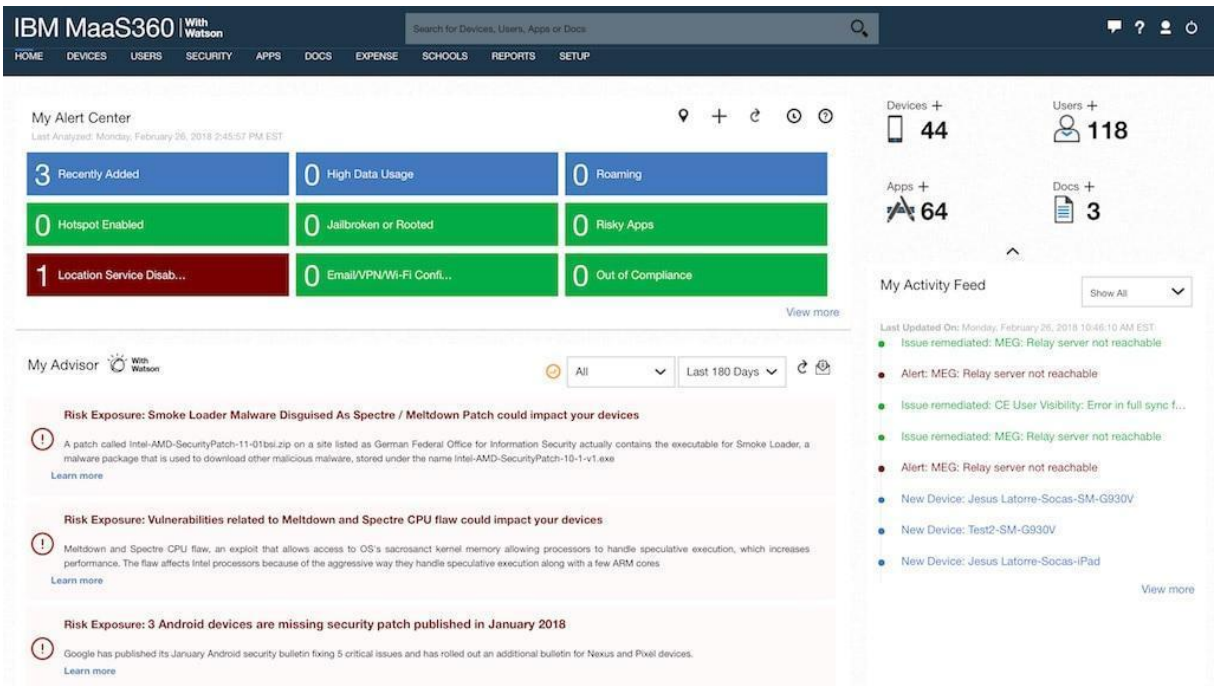
corrompus. Une de ses multiples missions est notamment d'installer des logiciels à travers le réseau OTA. Il diagnostique chaque terminal, fournit des informations sur la performance de celui-ci et surtout gère les applications et le roaming dans d'autres régions et pays.

Notre solution de MDM

IBM MaaS360

Principales fonctionnalités :

- Gestion de MaaS360 Apple iOS et de macOS
- Gestion de Google Android dans MaaS360
- Gestion de Microsoft Windows dans MaaS360
- MaaS360 Container App
- MaaS360 Advisor
- Moteur de recommandation de politiques de MaaS360
- MaaS360 Business Dashboards for Apps
- MaaS360 Laptop Patch and Update Management
- MaaS360 Identity Management
- MaaS360 Mobile Threat Management
- MaaS360 Mobile App Security
- TeamViewer Remote Support for MaaS360



10. La sauvegarde.

10.1 La sauvegarde de données

Pourquoi la sauvegarde en entreprise ?

Une entreprise subissant un revers telle qu'une attaque informatique va se trouver en grande difficulté pour redémarrer son activité. Les conséquences peuvent être désastreuses et variées :

- La société peut voir son image affectée par la situation
- Les équipes peuvent se désorganiser et donc perdre en productivité
- La société peut subir des pertes financières

La sauvegarde permet à une société de restaurer ses données.

Il faut distinguer deux types de sinistres : les sinistres mineurs, localisés, et les sinistres majeurs qui impactent l'ensemble des infrastructures informatiques de l'entreprise. Parmi les sinistres mineurs, on peut citer les pannes de disques durs, les fausses manipulations ou encore les virus. Dans tous les cas, cela se traduit par la perte d'un ou plusieurs fichiers.

Afin d'en limiter les conséquences, il est indispensable de disposer d'une solution de sauvegarde qui permet une restauration granulaire ; c'est- à-dire qui permet de parcourir et choisir les fichiers avant de les restaurer, et non après avoir restauré l'intégralité des données sauvegardées.

Enfin, la fonction rétention permet de figer les sauvegardes de données dans le temps. Entre le moment où un fichier a été corrompu et le moment où l'on s'en aperçoit, il peut s'être écoulé des jours voire des semaines. La rétention permettra de retrouver la version du fichier qui n'avait pas encore été corrompue à l'époque de sa sauvegarde.

Explication de la sauvegarde de données

La sauvegarde des données peut répondre aux problèmes de récupération de données supprimées, tels que :

- La restauration d'une base de données à un instant donnée.
- La restauration de données et de fichiers utilisateurs.
- La restauration de boîte mail

La solution de sauvegarde doit définir spécifiquement la fréquence de sauvegarde (ponctuelle, quotidienne, hebdomadaire ...) des fichiers et dossiers sélectionnés. La sauvegarde peut être configurée pour envoyer automatiquement les données cryptées vers un site externe sécurisé. Les données de sauvegarde perdues lors de la panne du serveur peuvent être restaurées afin que les utilisateurs puissent récupérer toutes leurs informations numériques.

Il est également possible de sauvegarder des machines virtuelles, leurs configurations et leurs données. Des solutions telles que Veeam Cloud Connect offrent également la possibilité d'externaliser les sauvegardes de machines virtuelles vers un environnement (serveurs de la société), ce qui permet d'avoir une sécurité supplémentaire. L'idée est de doubler la protection des données hébergées sur les machines virtuelles et la disponibilité des services implémentés sur les machines virtuelles en créant une copie placée dans un environnement distant. Ainsi, en cas d'événement indésirable, le retour à la normale des machines virtuelles peut être effectué rapidement sans interrompre l'accès au service d'hébergement.

Explication de la réplication de données

La réplication de données, elle, répond à une problématique de perte de service.

Lors d'une interruption de service (site web, serveur de messagerie, plateforme collaborative d'entreprise, etc.) il va être possible d'opérer un basculement des applicatifs touchés vers un autre serveur ou un autre site d'hébergement donné, géographiquement éloigné du site primaire.

On différencie d'ailleurs les réplications synchrones et asynchrones pour des utilisations différentes

Dans quels cas procède-t-on à une réplication synchrone ?

- Un cluster de base de données avec des données importantes, voire critiques pour l'entreprise.
- Une réplication de base de données Exchange pour remonter un serveur de mail sur un autre serveur.
- Une réplication sur de multiples disques durs.

Dans quels cas procède-t-on à une réplication asynchrone ?

- Un cluster de base de données avec des données d'importance faible à moyenne.
- Réplication de fichiers entre plusieurs sites.
- Réplication d'annuaire (Active Directory par exemple).

10.2 Le plan de sauvegarde

Définition :

Lors de la mise en place du système de sauvegarde, nous définirons une méthode. Elle dépend essentiellement des besoins de restauration de l'entreprise. En fonction de la fréquence et de la méthode choisie, la stratégie de l'entreprise déterminera la capacité de stockage requise pour les sauvegardes.

- **La méthode choisie :** complète, différentielle et incrémentielle
- **La fréquence de sauvegarde :** journalière, hebdomadaire et mensuelle
- **La fréquence de modification des fichiers**

Les systèmes de sauvegarde permettent d'appliquer plusieurs méthodes :

- **Sauvegarde complète :** Sauvegarder tous les fichiers et dossiers, toute la partition ou tout le disque.
- **Sauvegarde différentielle :** Sauvegarder des données modifiées ou nouvellement ajoutées sur la base de la dernière sauvegarde complète.
- **Sauvegarde incrémentielle :** Sauvegarder uniquement les données modifiées ou ajoutées depuis la dernière sauvegarde qui peut être une sauvegarde complète ou une sauvegarde incrémentielle.

Afin de garantir la sécurité des données numériques de l'entreprise, nous mettrons en place une stratégie de sauvegarde simple et efficace, la règle 3-2-1.

Notre choix est d'effectuer une sauvegarde complète hebdomadaire et une sauvegarde incrémentielle quotidienne.

La règle du 3-2-1 :

3 copies d'un même fichier

Pour garantir des données numériques, il est de rigueur de disposer à minima de 3 copies : celle utilisée au quotidien et deux sauvegardes. Pourquoi ? Parce qu'il n'y a rien de plus risqué que de croire qu'un dispositif de sauvegarde ne rencontrera pas un problème en même temps que le stockage original.

Il est également pertinent d'effectuer des sauvegardes régulièrement plutôt qu'une fois par mois ou par semaine.

Certains outils permettent de générer des copies régulières ou des « instantanés » (snapshots) toutes les heures, tous les jours, etc. sans impacter les performances et tout en assurant une « rotation des versions » pour ne garder que les essentielles et ainsi revenir en arrière quand c'est nécessaire, avec une bonne granularité.

Ces sauvegardes (locales et distantes) doivent être régulièrement vérifiées, ce qui garantit qu'elles fonctionnent et qu'elles pourront permettre de récupérer les données en cas de problème.

Autre erreur commune : considérer que le fait de disposer d'une redondance de type RAID compte comme une copie supplémentaire. Le RAID n'est pas une solution de sauvegarde en tant que telle mais une protection contre la défaillance d'une unité de stockage avec ses propres limites, permettant de s'assurer de la disponibilité des données.

2 supports différents

C'est là que la notion de support entre en compte : rien ne sert d'avoir des sauvegardes multiples si elles sont toutes stockées sur le même appareil car si celui-ci vient à défaillir, elles seront toutes perdues.

Ce second support peut être un NAS ou un périphérique de stockage externe par exemple. Dans l'idéal, il est indépendant de la machine utilisée au quotidien et/ou par laquelle se fait l'accès aux données à sauvegarder. Là encore, cette précaution d'usage évitera d'importants désagréments si la machine en question vient à être piratée ou rencontre un problème.

1 sauvegarde « hors site »

Si de plus en plus d'utilisateurs disposent d'un NAS où ils sauvegardent leurs données, nombreux sont ceux qui pensent que c'est une solution à tous les problèmes... mais ce n'est pas le cas. En cas d'incendie, de vol ou d'inondation par exemple, celui-ci sera inexploitable, tout comme le reste des machines. D'où l'importance d'une sauvegarde hors site.

Cela peut être un NAS dans un second bureau ou même un service en ligne. Dans tous ces cas, il est primordial de protéger les données en les chiffrant tant dans le transport (HTTPS/TLS) qu'avant de les envoyer à un serveur distant.

L'importance de la gestion des versions

Outre ces grands principes, d'autres points sont à connaître. Le premier est qu'une solution de synchronisation n'est pas à proprement dit une sauvegarde. Si une donnée est supprimée localement, elle le sera aussi sur le serveur distant. Il faut donc veiller dans ce cas à utiliser un service proposant du versioning, permettant de revenir en arrière en cas de problème.

Cela participera notamment à lutter contre une autre menace : les rançongiciels (ransomwares). Une attaque qui vise à chiffrer des fichiers avec un mot de passe que son utilisateur ne connaît pas. Pour le récupérer, il devra payer une rançon (d'où son nom), le tout se propageant à travers une machine infectée ayant accès aux données stockées sur le réseau local ou en ligne. Chiffrées, celles synchronisées ou sauvegardées après l'attaque le seront aussi.

Là aussi, la nécessité de disposer de sauvegardes qui ne seront pas affectées, conservées hors-ligne et/ou disposant d'une gestion des versions permettant de revenir à une version enregistrée avant l'attaque est incontestable.

10.3 Mise en place de la solution de sauvegarde

Veeam Backup & Replication

Veeam Backup est bien plus qu'un logiciel de sauvegarde. Il permet une récupération rapide, souple et efficace d'applications et de données virtualisées.

Elle tire parti de la virtualisation, du stockage et des technologies du cloud pour atteindre des objectifs de temps de restauration, et donc des délais de reprise imbattables.

Les 10 avantages les plus déterminants :

AVANTAGES	VEEAM BACKUP & REPLICATION	OUTILS DE SAUVEGARDE TRADITIONNELLE
Sans agents	✓	–
Réplication avancée intégrée	✓	–
Instant VM Recovery	Breveté	–
Instant File-Level Recovery	Tout SE et tout système de fichiers	Windows, éventuellement Linux
Restauration instantanée d'objets applicatifs	Toute application et tout système de fichiers	Certaines applications seulement
Vérification automatisée de la restauration	Breveté	–
Compression et déduplication côté source intégrées	✓	–
Acheminement simple des sauvegardes hors site	✓	–
Indépendant du stockage	✓	–
Facilité de déploiement et de configuration	15 minutes pour l'autoconfiguration	Plusieurs semaines de déploiement coûteux

Fonctionnalités clés de Veeam Backup & Replication

- Création de **sauvegardes** de machines virtuelles en mode « image » pour une meilleure cohérence avec les sauvegardes d'applications.

- **Accélération WAN intégré** : Externalisation des sauvegardes jusqu'à 50 fois plus rapide grâce à l'utilisation d'une mise en cache ainsi qu'une compression des données. Ceci permet également de minimiser l'utilisation de la bande passante.

- **Réplication avancée** : Sauvegarde et réplication 2-en-1, une copie de la VM prête à être démarrée. Récupération basée sur le cloud grâce aux fournisseurs affiliés à Veeam.

- **Instant VM Recovery** : Exécution directe de la machine virtuelle à partir de la sauvegarde. Réduction du RTO, minimisation du temps d'indisponibilité.

- **Veeam Explorers** : Restauration avancée avec Active Directory, Exchange, Sharepoint ou encore SQL Server. Permet par exemple la restauration d'objet AD (OU, User, Groupe, ...) ou encore de GPO.

- **SureBackup / SureReplica** : Vérifier la récupérabilité de chaque sauvegarde de chaque machine virtuelle, en permanence.

- **ON-Demand Sandbox** : Permets de simuler l'environnement de production pour tester de nouvelles mises à jour et fonctionnalités et de vérifier la sécurité.

- **Veeam One** : meilleure gestion des SLA et des temps d'arrêt grâce à une supervision, un reporting et des alertes d'administration en temps réel.

- **Veeam Intelligent Diagnostics** : Gestion proactive des alertes et des erreurs connues grâce à des résolutions automatiques ou une autonomie de l'utilisateur.

- **Veeam Availability Orchestrator** : permet d'orchestrer automatiquement des actions récurrentes. Ceci permet également d'orchestrer un PRA grâce à une multitude de scénarios envisageable afin de gagner en rapidité.

Le licensing

Veeam utilise un licensing spécifique.

Le modèle VUL (Veeam Universal Licence) est un modèle par abonnement qui s'utilise de manière universelle. Les licences VUL sont vendues pour une durée déterminée : un à cinq ans.

Elles s'utilisent de façon interchangeable pour un vaste choix de produits Veeam et de types de workload (dénomination utilisée par Veeam).

Le terme workload désigne indifféremment une VM, un serveur physique, une application d'entreprise, une VM dans le cloud ou un partage de fichiers. Comme les licences du modèle VUL sont portables, les clients peuvent les utiliser pour protéger tous les types de workload dont ils ont besoin. Ils les achètent par 10 au minimum pour protéger leurs différents workloads.

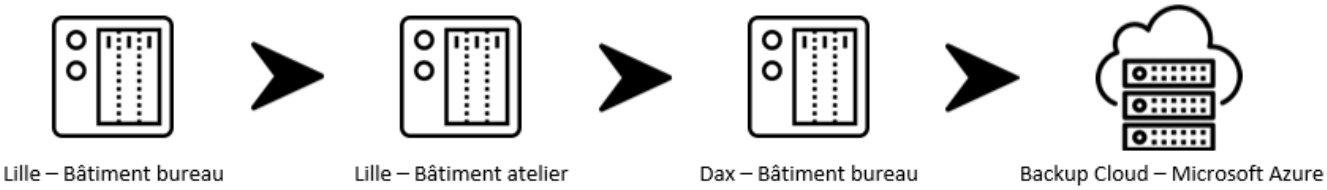
Veeam propose également un licensing plus commun, VIL (Veeam Instance Licence) qui est le licensing par socket. Il s'agit alors d'une licence par sockets CPU, donc, si un serveur dispose de deux processeurs il faudra alors deux licences.

La différence ?

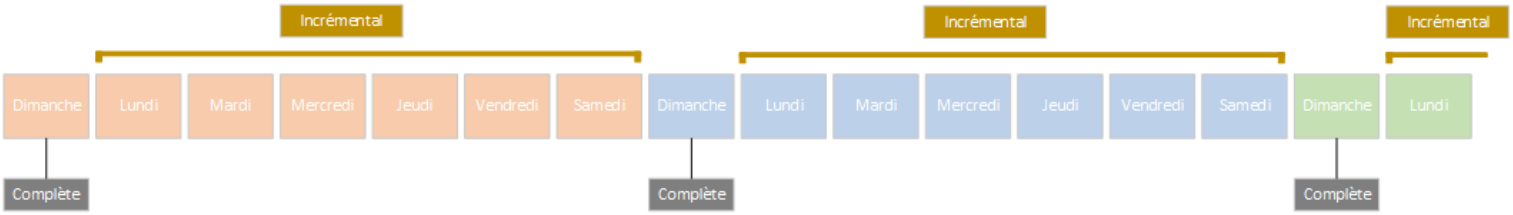
Le modèle VUL est une configuration plus simple, portable et facile à utiliser que son prédécesseur, le modèle de licences par instance de Veeam (VIL). Avec ce modèle, le client achète un ensemble de licences dans une version unique comprenant toutes les fonctionnalités, ce qui évite les calculs complexes de nombre de licences. Une licence VUL protège un workload.

Les sauvegardes :

Une première sauvegarde est effectuée à Lille dans le bâtiment bureau, une seconde sauvegarde est elle aussi effectuée à Lille dans le bâtiment atelier sur le NAS. Une fois celle-ci terminée, une sauvegarde à Dax dans le bâtiment bureau s'enclenche. Quand toutes les sauvegardes sont terminées, une sauvegarde dans le backup cloud Microsoft Azure s'effectue.



Plan de sauvegarde :



Nous avons choisi :

- Une sauvegarde complète tous les lundis : toutes les machines virtuelles et l'Active Directory seront sauvegardées.
- Une sauvegarde incrémentielle tous les jours : seules les modifications apportées sont sauvegardées et ajoutées à la sauvegarde complète.

Afin d'assurer une récupération précoce en cas de problème majeur, nous avons choisi une période de rétention de 2 semaines. Les sauvegardes complètes de plus de 2 semaines seront remplacées par de nouvelles sauvegardes complètes.

11. Gestion de parc informatique.

11.1 Définitions

Le parc informatique englobe l'intégralité des ressources logicielles et matérielles au sein du système informatique. Cela comprend :

- Les postes de travail : Unités centrales, claviers, souris, écrans, PC portables, terminaux légers.
- Les serveurs
- Les actifs réseau
- Les smartphones, tablettes et autres appareils mobiles
- Les périphériques : Imprimantes, scanners, et autres périphériques métier
- L'intégralité des logiciels, applications, et licences
- Les données sur les postes et le réseau
- Les services en Cloud

Gestion du parc informatique :

- Faire un inventaire, recenser, localiser les éléments du parc.
- Sécuriser le parc informatique
- Assurer la maintenance et le dépannage
- Assister à l'organisation du système informatique
- Stockage et affichage de procédures

Pour répondre à notre besoin de gestion du parc informatique, nous allons comparer 2 solutions de « HelpDesk » : GestSup et GLPI.

11.2 GestSup

Gestsup est un logiciel de gestion de support 100% web et gratuit sous licences GPL v3, il permet la gestion de tickets et d'équipements, c'est-à-dire qu'il donne la possibilité de posséder un système de support pour les utilisateurs du système d'information, facile d'accès, et d'utilisation, ainsi qu'un suivi des pannes matérielles.

Fonctions clés :

- Support utilisateur : Interface simplifiée pour les utilisateurs, création de ticket par mail ou via l'interface web. Gestion des tickets déjà ouverts pour les utilisateurs
- Authentification SSO
- Possibilité de créer manuellement un inventaire des équipements.
- Mise en service rapide
- Synchronisation avec l'active directory
- Statistiques de résolutions de tickets

Prérequis utilisateurs :

- Google Chrome recommandé pour les utilisateurs, résolution minimale de 1440x900

Prérequis serveur :

- Une application de virtualisation compatible VMware ou VirtualBox
- Linux Debian
- Apache 2.4X
- Base de données MySQL 5.5x minimum, ou MariaDB 10.0.1.X
- PhP 5.6 minimum
- 4GB de mémoire vive minimum

Prérequis réseau :

- Autorisation du port 21 depuis le serveur web vers « ftp.gestsup.fr » pour les mises à jour FTP
- Autorisation du 25 ou 465 ou 567 depuis le serveur web vers internet pour l'envoi de mail SMTP
- Autorisation du port 143 ou 110 ou 993 depuis le serveur web vers internet pour la réception des mails en IMAP et/ou en POP
- Autorisation du port 80 depuis le serveur web vers internet

11.3 GLPI

GLPI est une solution open source pour gérer et administrer son parc informatique. On y accède depuis une application WEB pour gérer l'ensemble des problématiques d'un parc informatique : Gestion de l'inventaire, des composants matériels / logiciels, gestion des tickets utilisateurs, gestion des contrats.

Fonctions clés :

- Solution gratuite
- Optimisation des ressources matérielles et humaines
- Gestion des licences logiciels et des contrats
- Gestion des utilisateurs et de leurs tickets
- Compatibilité avec OCS Inventory ou Fusion Inventory pour avoir un inventaire automatique des assets.
- Possibilité d'y intégrer du télé déploiement.

Prérequis :

- Serveur Web Apache 2
- PHP 5.3 ou supérieur
- JSON, Mysql
- HTML, CSS
- Aucun prérequis concernant les postes utilisateurs.

11.4 Choix de la solution

Matrice de choix de la solution :

		Coefficient	GestSup	GLPI	Commentaires
Critères	Transparence pour les utilisateurs	2	4	4	Les 2 solutions seront transparentes pour l'utilisateur
	Facilité d'installation	1	4	3	GLPI sera légèrement plus compliqué à installer
	Facilité de maintenance	2	2	2	Les 2 solutions seront sur une distribution Debian
	L'utilisateur peut créer un ticket	4	4	4	
	Les techniciens peuvent gérer les demandes d'interventions	4	4	4	
	Gestion de contrats	3	0	4	Il n'y a pas de gestion de contrats sur GestSup
	Gestion des garanties	4	4	4	
	Inventaire automatique	4	0	4	GestSup ne possède pas de fonctionnalité d'inventaire automatisé
	Base de connaissances	1	4	4	
	Statistiques sur les tickets	2	4	3	GestSup possède légèrement plus de statistiques sur les tickets
	Coût de l'application	4	0	4	GestSup est une solution payante
	Temps dédié à l'application	4	1	3	Même si GLPI nécessitera probablement un peu plus de maintenance, le temps gagné grâce à l'inventaire automatique le compense largement
Total			2,3	3,7	

Tableau 6 - Matrice de choix de la solution de gestion de parc

Après cette étude comparative des solutions, nous avons décidé d'opter pour **GLPI** avec **Fusion Inventory**.

11.5 Présentation de GLPI

GLPI va nous permettre de disposer d'une vue d'ensemble du parc Informatique. En installant Fusion Inventory sur l'intégralité des postes, nous disposerons d'une remontée automatique d'informations sur les machines composant notre parc. On pourra ainsi disposer d'informations sur les versions des applications, les composants informatiques, et les versions de Windows, et tout cela sur un seul et unique outil.

Name	Status	Version	License	Installation date	Software category	Valid license
Acrobat Reader	Sub Retour SAV 4	6.0			Computing	Yes
Acrobat Reader		7.0			Computing	Yes
Acrobat Reader		7.04			Computing	Yes
InkScape	Sub En attente d' 2	0.4	license '0 - serial 0 (type ' 0)		Antivirus > s-category '0	Yes
InkScape		0.4			Antivirus > s-category '0	Yes
Microsoft Office	Sub En stock 0	2003			Antivirus > s-category '0	Yes
Microsoft Office		95			Antivirus > s-category '0	Yes

Figure 29 - Exemple d'informations obtenues pour un poste

Sur la figure ci-dessus, on peut voir un exemple des informations que l'on obtient lorsqu'on va dans la catégorie Logiciel d'un poste remonté par fusion inventory. Ces informations permettent de cibler les postes sur lesquels une mise à jour aurait eu du mal à s'effectuer.

On peut également consulter l'espace disque utilisé pour chaque poste.

Volumes							
Name	Partition	Mount point	File system	Global size	Free size	Free percentage	Encryption
disk '1	/dev/disk1	/mnt/disk1	ext	533.35 Gio	82.16 Gio	15 %	
disk '2	/dev/disk2	/mnt/disk2	ext2	301.25 Gio	12.6 Gio	4 %	
disk '3	/dev/disk3	/mnt/disk3	FAT	974.02 Gio	674.61 Gio	69 %	
disk '4	/dev/disk4	/mnt/disk4	FAT	567.25 Gio	122.72 Gio	22 %	
Name	Partition	Mount point	File system	Global size	Free size	Free percentage	Encryption

Figure 30 - Espace disque utilisée pour un poste

Il est important de préciser qu'il est également possible de faire des recherches d'ordinateur assez précises grâce à l'outil de recherche intégré. Il est même possible de faire une recherche par logiciel. Ainsi on pourra cibler instantanément

les postes où le logiciel ne s'est pas installé, ou sur lesquels le logiciel n'est pas à jour.

GLPI est également une solution de Ticketing. Les utilisateurs peuvent se connecter à l'outil et créer un ticket pour demander de l'assistance.

Pour chaque ticket, l'utilisateur pourra préciser la nature de son problème et l'équipement impacté.

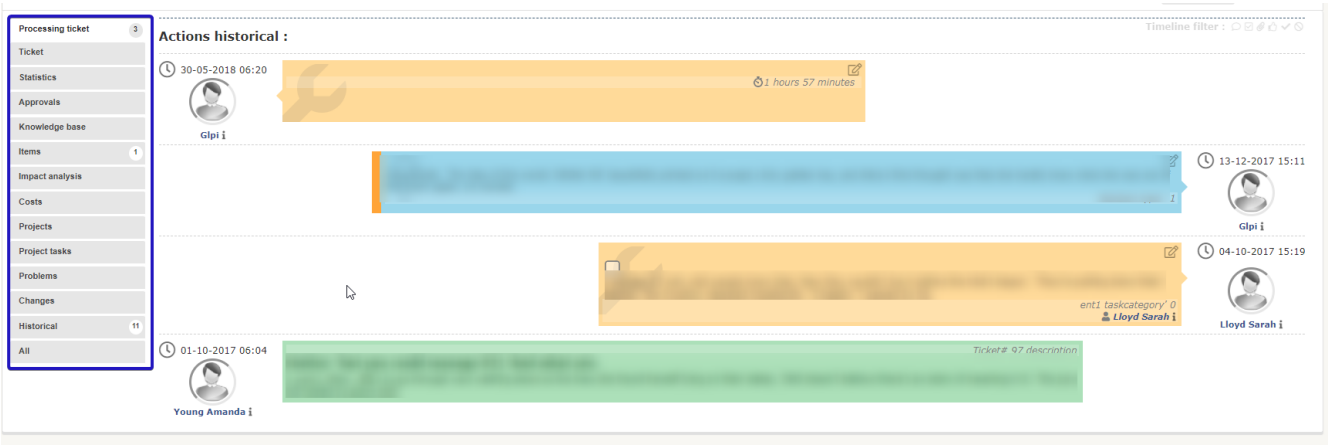


Figure 31 - Exemple de conversation avec un technicien

Ensuite, lorsqu'un technicien prendra en charge le ticket, il pourra engager une discussion avec l'utilisateur afin de résoudre le problème. Une fois le problème résolu, des statistiques seront créées pour le technicien et le responsable informatique sur le temps de résolution et le technicien affecté. Le technicien pourra également remplir la base de connaissance pour documenter le problème.

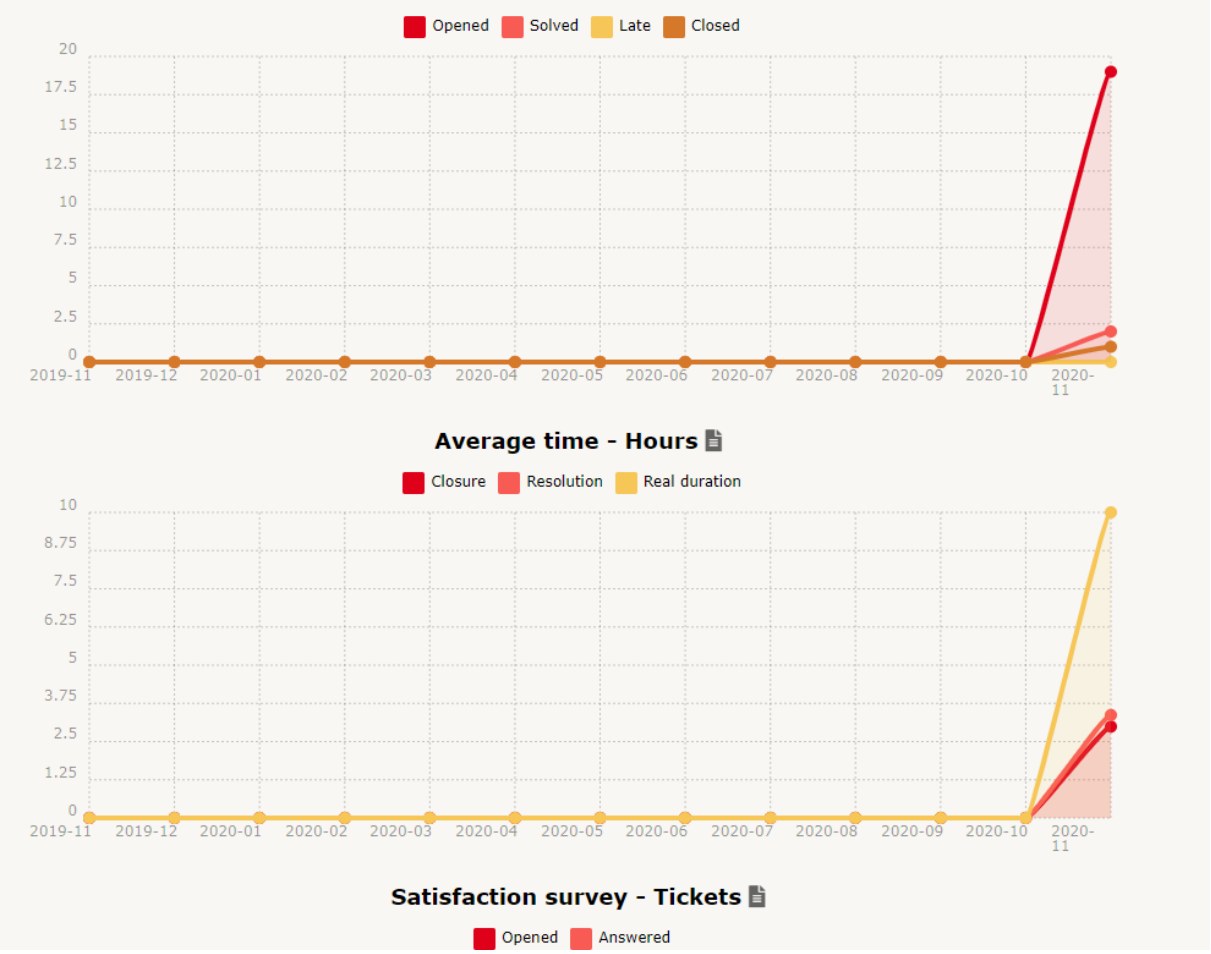


Figure 32 - Statistiques sur les tickets

Ces statistiques permettront au responsable informatique de se justifier auprès de ses supérieurs et de faire valoir une meilleure assistance / prestation.

Toujours dans l'optique de soutenir le service informatique, GLPI permet de gérer et inventorier tous les contrats et garanties du parc informatique, ainsi que les licences, afin d'avoir une vue centralisée.

Enfin, GLPI possède également une base de connaissance, dans laquelle il faudra renseigner toutes les méthodes utilisées pour résoudre les problèmes.

Il faudra relier GLPI à l'active directory afin que les utilisateurs ne rencontrent pas de difficultés à se connecter et configurer les comptes utilisateurs du service informatique afin qu'ils puissent disposer d'un compte technicien pour voir et traiter les tickets.

12. Supervision du parc informatique.

12.1 Définitions

La supervision d'un parc informatique consiste à obtenir des informations sur l'état des ressources du parc informatique. La supervision peut être déclinée en 3 domaines :

Supervision applicative :

- Possibilité d'obtenir des informations sur la disponibilité d'une application, le nombre de sessions ouvertes, et les performances d'une application

Supervision réseau :

- Disponibilité d'un équipement physique
- Interrogation des sondes d'un équipement
- Création d'alertes en cas d'interruption de service
- Disponibilité, charge et état des onduleurs
- Disponibilité, état des consommables des imprimantes
- Disponibilité et interrogation des sondes des commutateurs, routeurs et serveurs.

Supervision système :

- Disponibilité des serveurs
- Utilisation du CPU
- Utilisation de la mémoire vive
- Saturation des disques durs

Dans tous ces cas de figure, il sera possible de réaliser un envoi d'alertes automatiques, pour notifier les services compétents d'une perte de service. Il est également possible de créer une cartographie de l'ensemble du parc informatique avec les principales sondes / équipements, et de créer des rapports d'activités.

La supervision a un rôle très important en matière de prévention et pour la correction de problèmes. Elle permet de déceler des problèmes naissants (Manque de ressources, instabilité d'un lien) ou de réagir le plus rapidement possible à un problème réel. (Perte d'un commutateur / routeur)

Les outils de supervision utilisent différents protocoles et technologies, en voici quelques-unes utilisées :

- Windows performance Counters
- Requêtes http
- SSH
- PING
- Requête SQL
- Protocole SNMP

12.2 Comparatif de solution :

Il existe plusieurs solutions de supervision et monitoring sur le marché. Certaines sont dites libres/open source, d'autres sont des solutions de SaaS (Software as a Service) et d'autres sont des applications payantes.

Les 2 solutions que nous allons comparer sont Nagios XI et PRTG. Ces 2 solutions étant relativement similaires, nous allons nous focaliser sur les points importants.

Nagios XI,

Nagios XI est une version améliorée, payante, et disposant d'un support à destination des professionnels de Nagios core. C'est une solution qui se veut plus intuitive, et avec une interface web lisible.

Prérequis matériel :

Monitored Nodes / Hosts	Monitored Services	Hard Drive Space	CPU Cores	RAM
50	250	40 GB	1 – 2	1 – 4 GB
100	500	80 GB	2 – 4	4 – 8 GB
> 500	> 2500	>120 GB	> 4	> 8 GB

Figure 33 - Hardware requirements de Nagios XI

Nagios fonctionne par Nodes pour le tarif de ses licences. Un nœud pour Nagios est n'importe quel objet qui possède une adresse IP, et que l'on souhaite monitorer.

Il faut donc estimer le nombre d'hôtes que l'on souhaite surveiller. En considérant les équipements suivants :

- Commutateur
- Routeur
- Serveur physique
- Onduleur
- Firewall

On compte une cinquantaine d'hôtes à surveiller, et ce sans compter les machines virtuelles. En incluant celles-ci, il faudra opter pour une licence avec au moins 100 nœuds.

Tarification :

	Prix à l'achat	**Prix à l'année**
Licence 100 nœuds	1995$ / 1709€	
Support téléphonique		2995$ / 2565€
Support tickets		1495$ / 1280€
Total sur 3 ans	1995$ / 1709€	13470$ / 11539€

Tableau 7 - Récapitulatif des frais de License Nagios XI

Cela fait donc un total de 13248€ sur 3 ans pour l'achat de Nagios XI avec un support téléphonique (10 appels) et support par tickets (10 tickets)

PRTG,

PRTG est un outil puissant qui grâce à des trames SNMP va analyser et suivre l'état du réseau local, ainsi que de différents hôtes. L'outil dispose d'une interface web simple et efficace.

Prérequis matériel :

Capteurs par serveur central	Licence	Hardware du serveur central	Espace disque (Conservation des données pendant 1 an)	Comptes Utilisateur	Sondes à distance	Virtualisation	PRTG Cluster
Jusqu'à 1,000 capteurs (~ 100 appareils)	PRTG 1000	2 cœurs de processeur, 3 GB RAM	250 GB	< 30	< 30	✓	✓
1,000 - 2,500 capteurs (~ 250 appareils)	PRTG 2500	3 cœurs de processeur, 5 GB RAM	500 GB	< 30	< 30	✓	✓
2,500 - 5,000 capteurs (~ 500 appareils)	PRTG 5000	5 cœurs de processeur, 8 GB RAM	1 TB	< 20	< 30	✓	!
5,000 - 10,000 capteurs (~ 1000 appareils)	PRTG XL1	8 cœurs de processeur, 16 GB RAM	2 TB	< 10	< 30	✓*	!
Plus de 10,000 capteurs	PRTG Enterprise	Veuillez configurer des serveurs PRTG additionnels et contacter notre équipe d'ingénieurs avant-vente.					

Figure 34 - Prérequis matériel de PRTG

PRTG fonctionne par capteurs pour ses licences. Comptant en moyenne 10 capteurs par hôte, cela implique, si l'on se réfère à l'estimation faite précédemment, qu'il faudra viser la licence 1000 capteurs (100 appareils)

	Prix à l'achat	**Prix à l'année**
Licence 1000 capteurs	2350€	
Support en ligne et mise à jour		587,5€ après la première année
Total sur 3 ans	2350€	1175€

Tableau 8 - Récapitulatif des frais de License PRTG

Cela fait un total de 3525€ sur 3 ans d'utilisation. Le renouvellement de la maintenance et du support de PRTG (Mise à jour toutes les 6 à 8 semaines et support en ligne) coûte 25% du prix d'achat de licence par an après la première année.

12.3 Choix de la solution

Matrice de choix de la solution :

Critères	Coefficien	Nagios XI	PRTG	Commentaires
Prix	3	3	3	Les 2 solutions ont un prix initial relativement proche
Coût additionnel du support	2	1	4	Le support de Nagios XI est très couteux
Configuration requise	2	2	3	PRTG nécessite une configuration plus légère
Support technique disponible	2	4	3	PRTG possède moins de ressources disponibles en ligne que Nagios
Estimation du TCO	3	3	4	PRTG semble posséder un coût total de possession plus faible que Nagios grace à sa facilité d'installation et d'administration
Facilité d'installation	2	2	3	Il est plus simple de configurer un nouvel environnement sur PRTG
Facilité d'administration	3	3	4	PRTG possède une interface claire et précise
Environnement d'installation	2	2	3	PRTG peux s'installer sur Windows Server
Reporting	3	4	4	Les 2 solutions ont des fonctionnalités très proches
Eléments monitorés	3	4	4	Les 2 solutions ont des fonctionnalités très proches
Frais de mise en service	1	4	4	Les 2 solutions n'ont pas de frais de mise en service supplémentaires
Total		2,96	3,58	

Tableau 9 - Matrice de choix solution de supervision

Nous avons donc pris la décision d'utiliser la solution PRTG Network Monitor.

12.4 La supervision avec PRTG

PRTG va nous permettre de superviser le bon fonctionnement de l'infrastructure système et réseau de l'entreprise WOOD afin d'être avertis suffisamment tôt pour agir en amont des problèmes.

Notre supervision :

- Supervision des switches
- Supervision des routeurs
- Supervision des points d'accès et contrôleur Wi-Fi
- Supervision des hyperviseurs
- Supervision des machines virtuelles
- Supervision des sauvegardes
- Supervision des onduleurs
- Supervision des firewalls
- Supervision des températures

12.5 Les capteurs

Les « capteurs » sont les éléments de supervision de base de PRTG. Un capteur surveille généralement une valeur mesurée dans le réseau, par exemple le trafic d'un port de commutateur, la charge du processeur d'un serveur, l'espace libre d'un lecteur de disque. Il faut compter en moyenne de 5 à 10 capteurs par appareil ou bien un capteur par port de commutateur.

Il existe plusieurs capteurs dans PRTG, utilisant la technologie SNMP, WMI ou encore SSH.

Le capteur SNMP :

SNMP signifie Simple Network Management Protocol (traduire protocole simple de gestion de réseau). Il s'agit d'un protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau.

Initialement, le SNMP ne permettait pas aux gestionnaires de communiquer entre eux et aux agents d'envoyer des messages avec accusé de réception. D'autre part, de nombreuses applications n'étaient que partiellement supportées au début du protocole malgré l'ambition d'être un standard ouvert. C'est pourquoi les correctifs du protocole apparus au cours des années suivantes ont principalement visé à intégrer des mécanismes correspondants dans le Simple Network Management Protocol. Une autre aspiration essentielle du groupe de travail IETF responsable du protocole a été, dès le début, d'accroître la sécurité du processus de gestion. On

peut observer ce résultat dans la troisième version. Cette étape d'optimisation du protocole SNMP ainsi que d'autres étapes sont présentées de façon un peu plus détaillée dans la description suivante des différentes versions SNMPv1, SNMPv2 et SNMPv3.

SNMPv1

En tant que première version du protocole de gestion de réseau, la version SNMPv1 pose les bases du modèle gestionnaires/agents et les bases de la communication entre le poste de gestion et les différents agents. Le Simple Network Management Protocol y est décrit comme un protocole simple agissant au niveau de l'application et pouvant s'appuyer sur l'UDP (User Datagram Protocol) et l'Internet Protocol (IP), mais aussi sur des protocoles réseau comparables tels que le DDP AppleTalks (Datagram Delivery Protocol) ou Internet Packet Exchange (IPX). Le seul mécanisme de sécurité intégré est alors l'échange d'un nom de communauté envoyé avec les requêtes correspondantes.

SNMPv2

L'un des problèmes majeurs de la première version du protocole SNMP réside dans le fait que le nom de communauté qui assure la sécurité n'est transmis qu'en texte clair. C'est la raison pour laquelle les développeurs se sont rapidement penchés sur une nouvelle variante appelée Secure SNMP, dans laquelle cette chaîne serait transmise sous une forme cryptée. Toutefois, cette version n'a jamais été publiée, car elle a été directement remplacée par la version SNMPv2. D'autres améliorations ont été apportées à la version initiale du protocole : un traitement des erreurs optimisé, la possibilité d'une communication de manager à manager ainsi que des commandes SET plus performantes. Le principal avantage comparé à la version SNMPv1 réside toutefois dans l'implémentation des nouveaux types de messages GETBULK (pour l'interrogation de plusieurs données dans une même requête) et INFORM (pour les accusés de réception des réponses des agents).

SNMPv3

Après la première étape, de moindre ampleur, franchie avec la deuxième version du protocole, l'IETF s'est pleinement consacrée à la sécurité dans la version SNMPv3 et a remplacé le nom de communauté par un nom d'utilisateur et un mot de passe. D'autre part, et contrairement aux versions antérieures, la troisième version du protocole inclut des fonctionnalités permettant de crypter la transmission des paquets SNMP.

12.6 Présentation de l'outil :

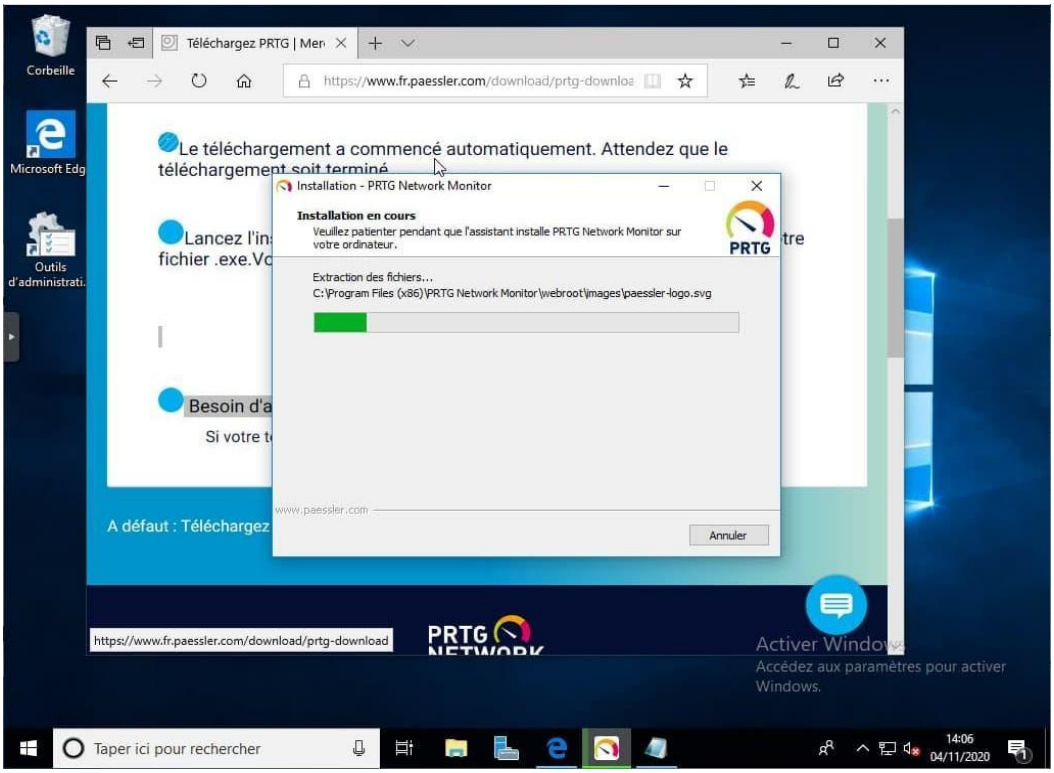


Figure 35 - Installation PRTG #1

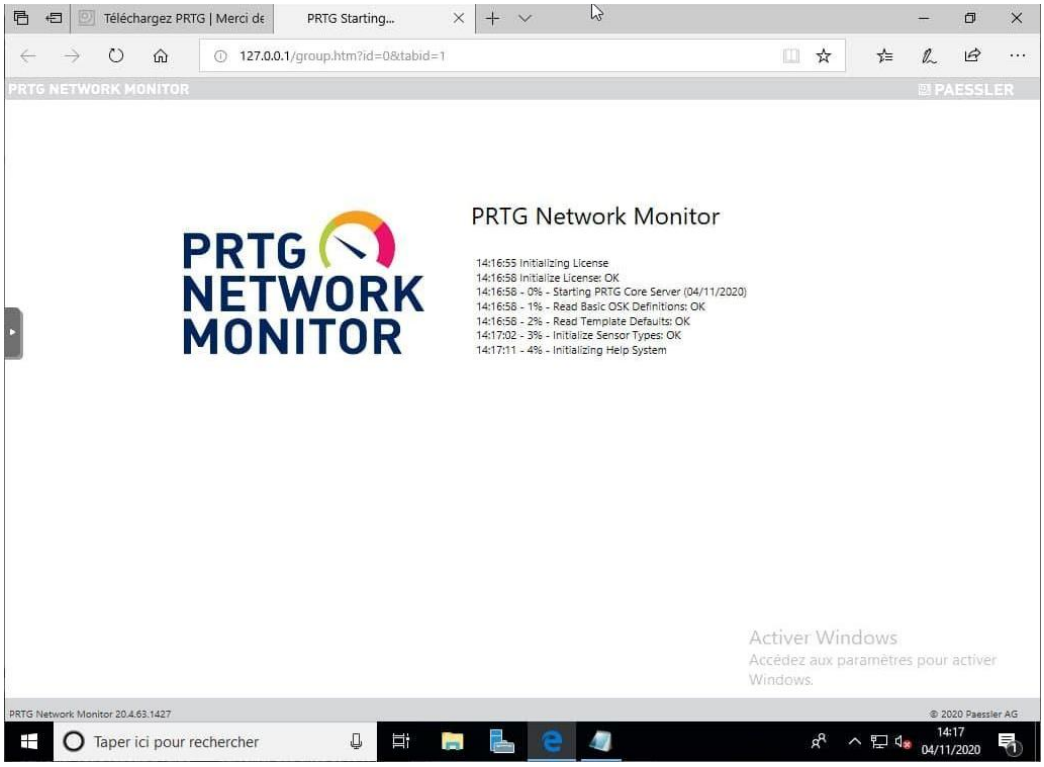


Figure 36 - Installation PRTG #2

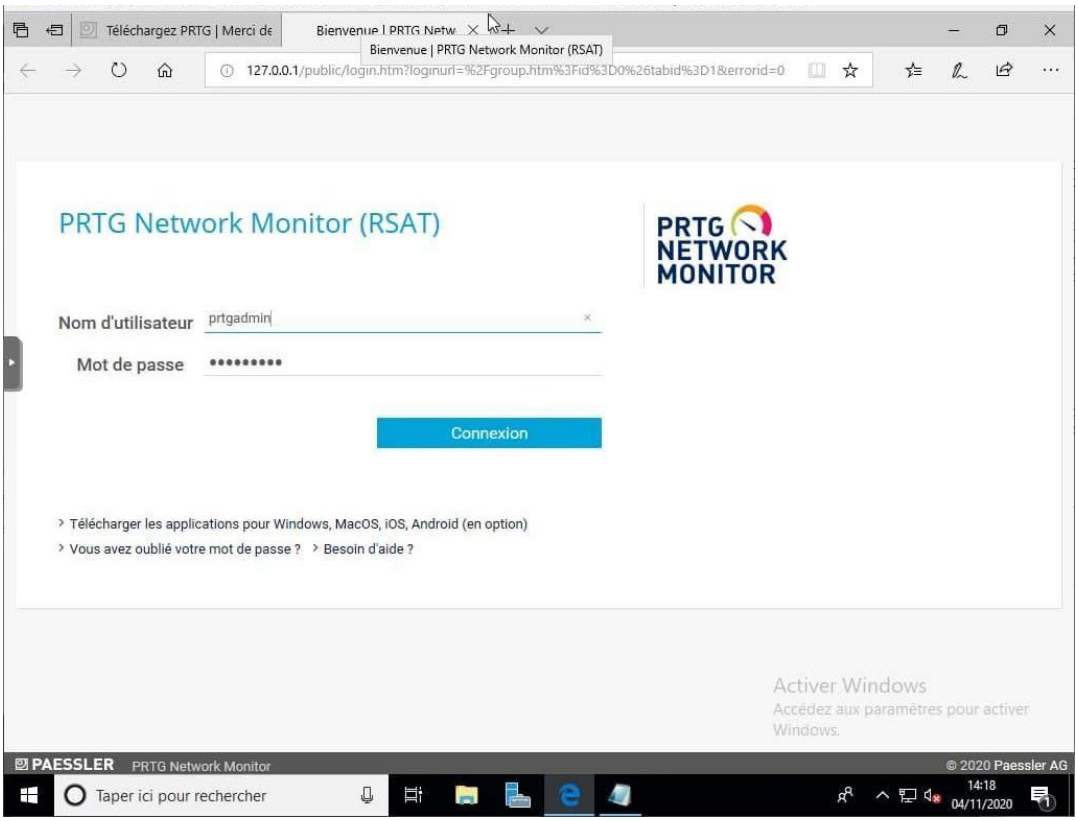


Figure 37 - Installation PRTG #3

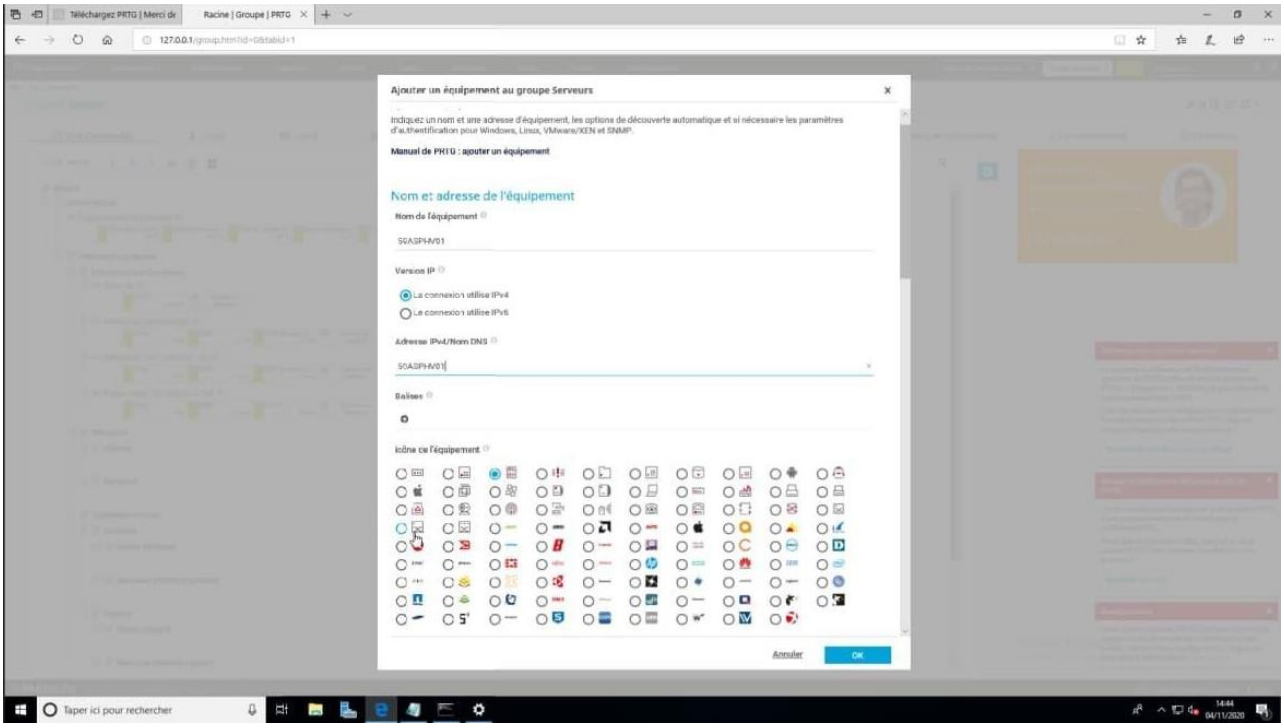


Figure 38 - Ajout d'un équipement

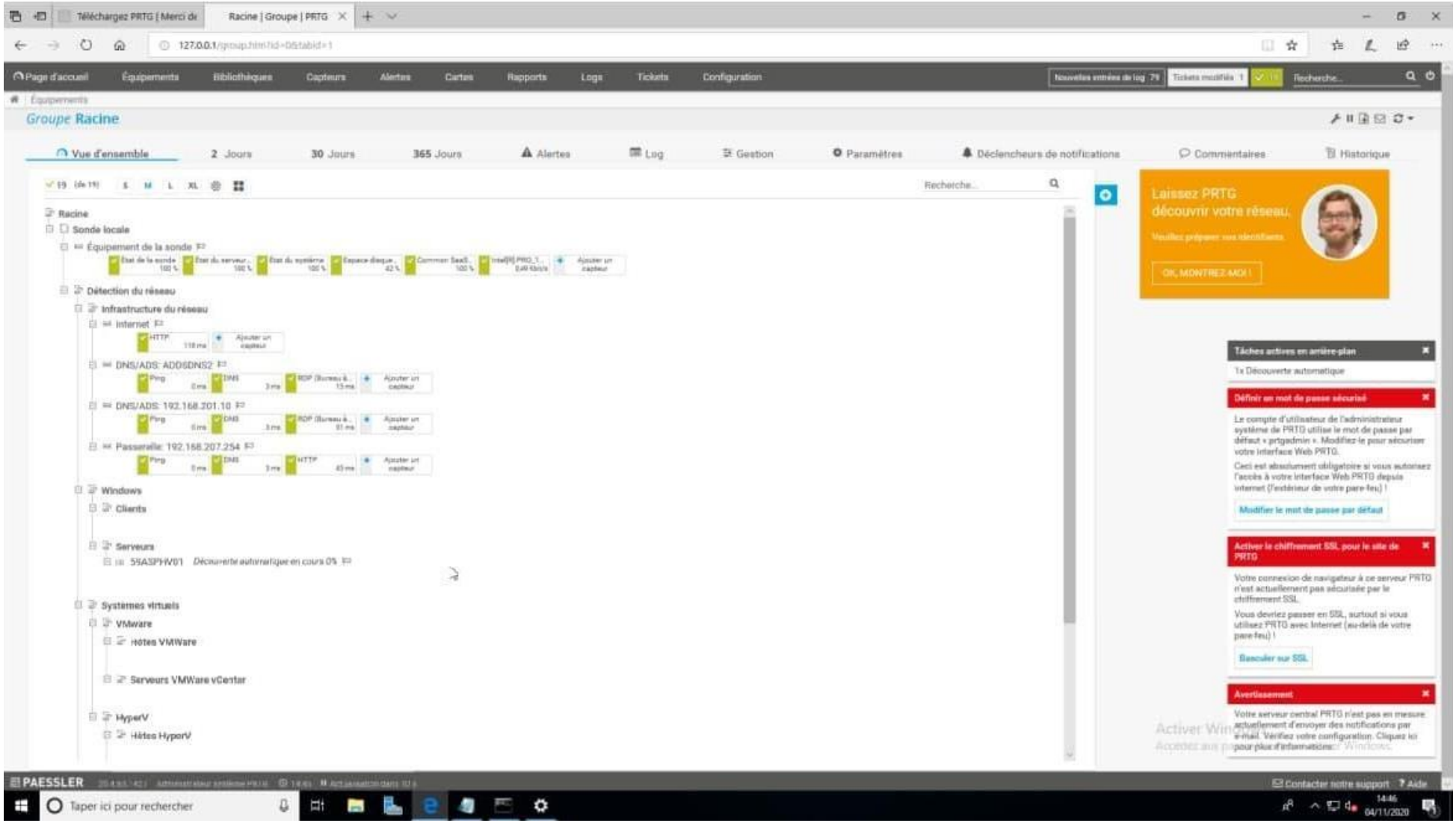


Figure 39 - Vue d'ensemble PRTG

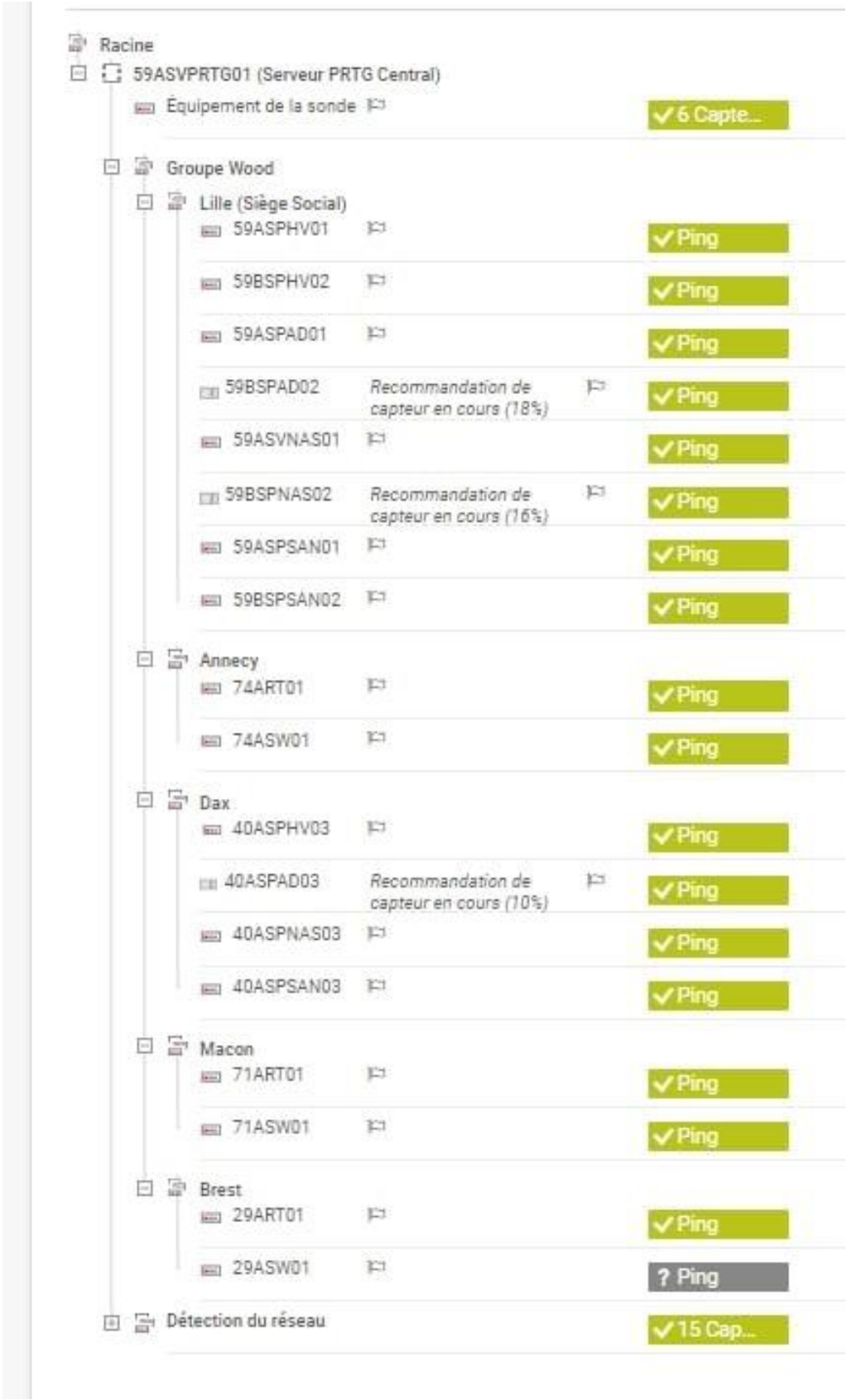


Figure 40 - Monitoring d'équipements

13. Solution Antivirale.

13.1 Définitions

Une solution antivirale protège le système d'information des différentes menaces. (Cheval de Troie, spywares, adwares, bot, miners, ransomwares ...) Pour y arriver, une solution antivirale complète déploiera plusieurs protections : Pare-Feu, Analyse comportementale, protection sur internet, analyse de code, détection de malwares. Certaines protections peuvent même lutter contre le phishing sur internet. (Hameçonnage)

Dans la pratique, un antivirus classique se comportera ainsi :

- Protection passive / active, qui analysera tous les nouveaux fichiers du système.
- Scanner qui recherche les logiciels malveillants à la demande
- Mise à jour régulière de la base de données antivirale (Signatures des différents virus)

Ce type d'antivirus est installé sur tous les ordinateurs du système informatique, et se lance avec une haute priorité dès le démarrage du système.

Si un antivirus détecte un virus grâce à sa signature, il mettra automatiquement en quarantaine le fichier infecté. L'utilisateur et le monitoring central seront alertés, et il sera alors possible de nettoyer les fichiers infectés, de supprimer les fichiers infectés, ou de les laisser en quarantaine.

Les antivirus peuvent également détecter un virus par l'analyse heuristique qui consiste à vérifier si un programme est vérolé ou non en simulant l'exécution dudit programme, en analysant son code et en utilisant des paternes récurrents ; il est ainsi possible de détecter de nouveaux virus inconnus jusqu'à présent.

13.2 Notre solution

Nous avons sélectionné Sophos Endpoint Security and Control comme solution d'antivirus au sein de notre système.

Sophos Endpoint Security and Control est une suite intégrée de logiciels de sécurité de Sophos :

Sophos Anti-Virus : Sophos Anti-Virus peut détecter et supprimer les virus, chevaux de Troie, vers et logiciels espions ainsi que les logiciels publicitaires et autres applications potentiellement nuisibles. Leur technologie HIPS (Host Intrusion Prevention System) protège l'ordinateur contre l'intrusion de fichiers suspects et les rootkits.

Sophos Behavior Monitoring : utilise la technologie HIPS pour assurer une protection continue des ordinateurs contre les menaces, même celles qui ne sont pas identifiées, et contre les comportements suspects.

Sophos Live Protection : Mise à jour rapide des bases de données antivirales, améliore la détection des nouveaux malwares.

Sophos Web Protection : Protection Web supplémentaire en empêchant l'accès aux emplacements réputés pour héberger des malwares. Possède une base de données en ligne de sites malveillants. Il surveille également les fichiers téléchargés.

Sophos Application Control : bloque les applications non autorisées par l'administrateur du système.

Sophos Device Control : Gestion des périphériques externes non autorisés.

Sophos Client Firewall : Protection anti-vers / chevaux de Troie / spywares.

Sophos AutoUpdate : Service de mise à jour automatique avec une gestion automatique de la bande passante.

13.3 Fonctionnement

Pour un fonctionnement optimal, notre infrastructure antivirale sera composée comme telle :

- Logiciel antivirus Protection Sophos sur tous les postes de notre système d'information, afin de protéger les ordinateurs des différents dangers.
- Machine virtuelle avec Sophos Enterprise console, qui permettra d'administrer la sécurité antivirale de notre parc.

Grâce au logiciel central Sophos Enterprise console, nous serons avertis à la moindre alerte de sécurité. En effet, les logiciels de protection Sophos installés sur les postes utilisateurs remonteront les différentes alertes et leur état de sécurité actuel.

Il est important de préciser qu'une bonne solution antivirale n'est pas suffisante pour assurer une sécurité à 100% du parc informatique. Ainsi, il faudra organiser des formations de sensibilisation à la sécurité informatique pour les utilisateurs et les guider dans l'apprentissage des réflexes importants.

14. Solution de déploiement.

Windows Deployment Service (WDS) est un rôle disponible sur toutes les versions de Windows Server 2003R2 (anciennement appelé Remote Installation Service RIS). Le service va alors assurer 2 fonctions : le déploiement des images WIM pour les systèmes d'exploitation Windows et également la fourniture d'images de démarrage via le PXE pour l'initialisation des processus d'installation.

Microsoft Deployment Toolkit est un outil conçu par Microsoft pour obtenir un système autonome de déploiement d'images Windows sur un parc informatique. L'intérêt est de pouvoir créer un système d'exploitation personnalisé. Pour un bon fonctionnement, il faudra prévoir d'installer le service WDS.

WDS est un service qui assure 2 fonctions majeures, le déploiement des images WIN pour les systèmes d'exploitation Windows et la fourniture d'images de démarrage (via le PXE) pour l'initialisation des processus d'installation.

C'est là que MDT est très utilisé ; avec son interface et les outils à disposition, il est possible de gérer l'ordre des étapes des installations à effectuer. Il peut également exécuter des logiciels, des scripts après l'installation de l'os pour terminer la configuration, changer des paramètres de personnalisation, etc.

MDT / WDS

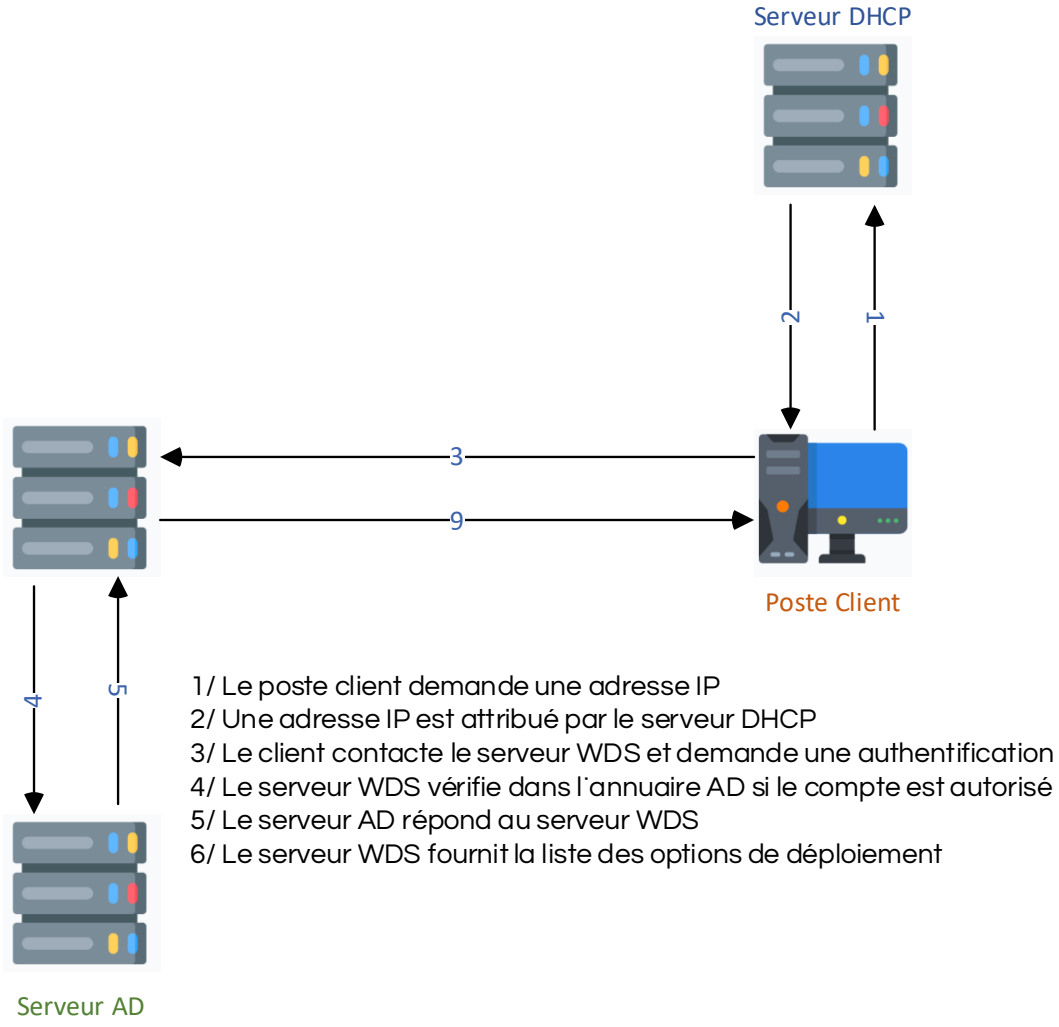
14.1 Windows Deployment Services (WDS)

WDS est le rôle qu'il est possible d'attribuer à n'importe quelle version de Windows Server à partir de Windows Server 2008, anciennement appelé Remote Installation Service.

WDS a pour rôle de déployer des systèmes utilisant la technologie PXE.

PXE étant l'acronyme de Pre-boot eXecution Environment et qui permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur.

Nous allons procéder à la mise en place d'un serveur WDS (Windows Deployment Services), présent sur les versions de Windows Server 2008 et supérieures. Nous allons également installer sur ce serveur MDT 2013 (Microsoft Deployment Toolkit) qui fonctionne en complément de WDS.



1/ Le poste client demande une adresse IP
2/ Une adresse IP est attribué par le serveur DHCP
3/ Le client contacte le serveur WDS et demande une authentification
4/ Le serveur WDS vérifie dans l'annuaire AD si le compte est autorisé
5/ Le serveur AD répond au serveur WDS
6/ Le serveur WDS fournit la liste des options de déploiement

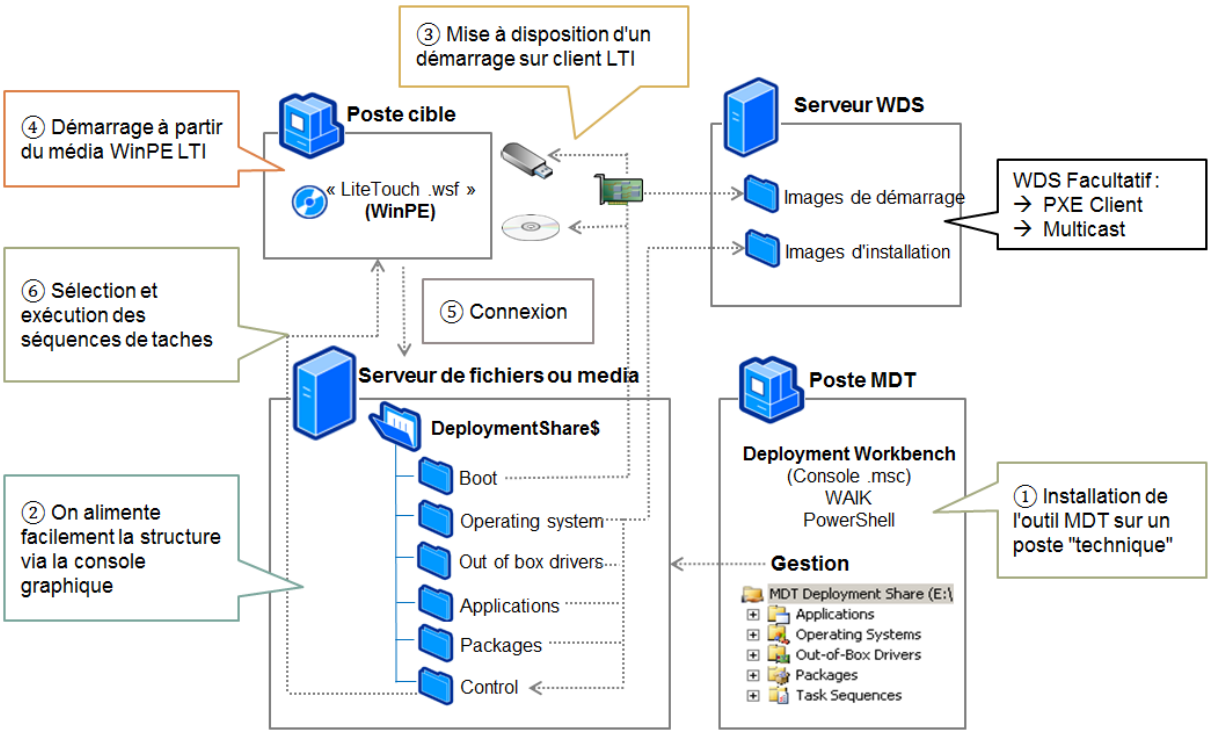
14.2 Microsoft Deployment Toolkit (MDT)

MDT est un outil d'automatisation de la fabrication et de l'installation des systèmes Windows. Il fonctionne en complément de WDS et permet de réduire le temps de déploiement et d'uniformisation des images Windows. Il offre également la possibilité d'incorporer l'installation des logiciels sans qu'aucune action de l'utilisateur ne soit requise.

Microsoft Deployment Toolkit (MDT) 2013

14.3 Architecture de déploiement WDS MDT

Un schéma explicatif d'un déploiement d'images avec les outils WDS et MDT :



14.4 Images Windows 10

Nous mettrons une image en place pour permettre à tous les ordinateurs de la société d'avoir la même version OS, mais aussi les mêmes applications avec la même version. Cela contribuera à une homogénéisation du parc informatique complet, et cela permettra au technicien de résoudre les potentiels problèmes plus rapidement.

Les logiciels qui sont présents systématiquement sur chaque poste utilisateur seront installés par défaut sur l'image. Quant aux autres logiciels spécifiques à certains services, les techniciens auront le choix lors de la phase de prédéploiement de choisir lesquels installer en fonction du service.

Durant la phase de prédéploiement, l'OU sera préremplie pour intégrer directement l'ordinateur dans l'AD. Le technicien devra par la suite déplacer l'objet dans la bonne OU.

15. Gestion des mises à jour avec WSUS.

15.1 Définitions

Windows Server Update Services est un service distribuant les mises à jour pour les systèmes d'exploitation Windows et les autres applications Microsoft au sein d'un parc informatique.

15.2 Fonctionnement

WSUS prend la forme d'un rôle pour Windows Server, afin qu'il devienne un serveur de mises à jour local (Un Relais pour les mises à jour).

WSUS se chargera de télécharger et stocker l'ensemble des mises à jour disponibles auprès des serveurs Windows Update de Microsoft et permettra de contrôler toutes les mises à jour manuellement avant de les déployer sur le parc.

Cela aura pour effet de minimiser l'impact des mises à jour Windows sur la bande passante ; en effet, par défaut, chaque ordinateur sous Windows fait ses mises à jour en passant par internet. En déployant un WSUS, lui seul téléchargera les paquets de mise à jour, en 1 seul exemplaire, et les redistribuera aux différents postes de la société.

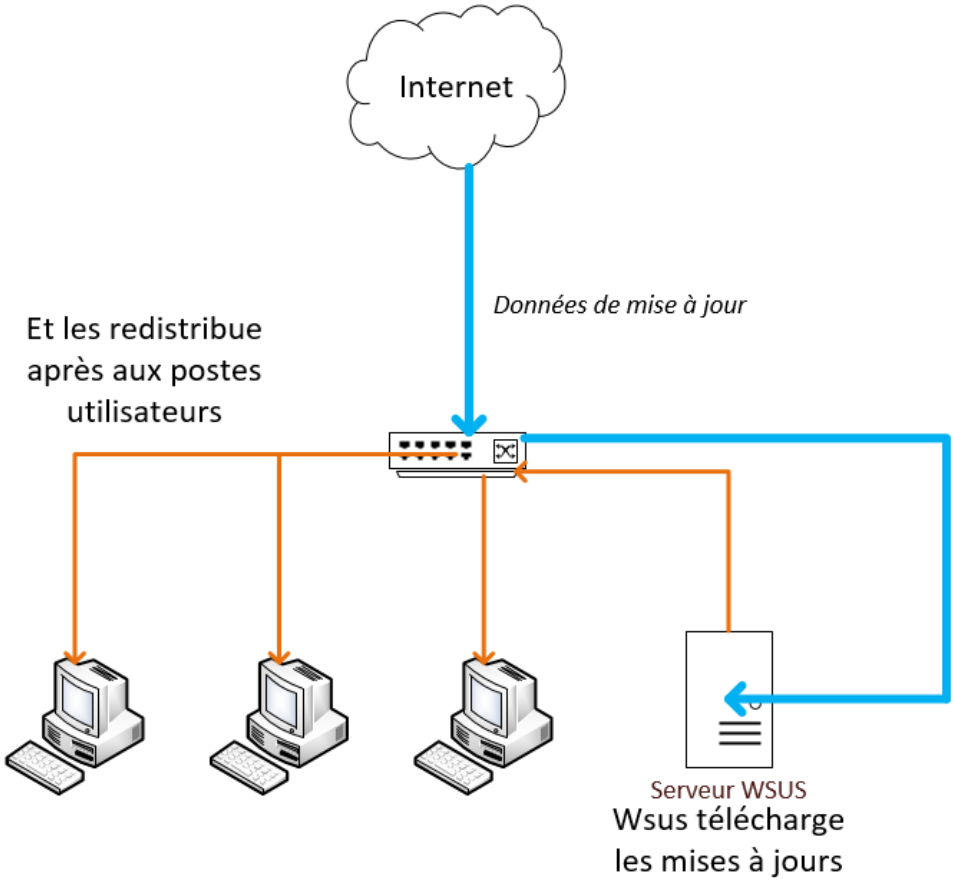


Figure 41 - Fonctionnement de WSUS

Nous installerons et configurerons donc une machine virtuelle Windows Server équipée du rôle WSUS pour assurer les mises à jour Windows du parc informatique. Initialement, nous vérifierons manuellement chacune des mises à jour critique afin de nous assurer du bon fonctionnement des postes après celle-ci. Une potentielle amélioration future pourrait être d'envisager l'automatisation de la vérification des mises à jour Windows.

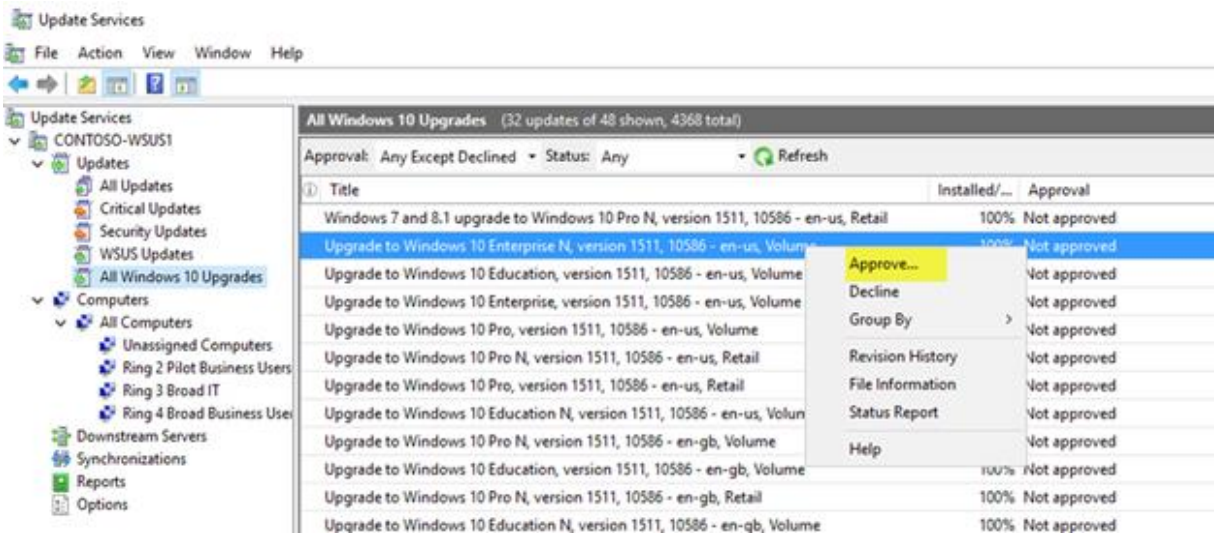


Figure 42 - Approbation des mises à jour système

16. Messagerie.

16.1 Exchange Online

Puisque notre choix s'oriente vers l'offre Office 365 de Microsoft, nous aurons accès avec l'abonnement au service de messagerie Exchange Online.

Exchange Online est le serveur de messagerie en ligne et Outlook le client de messagerie permettant de s'y connecter.

Les Atouts de Microsoft Exchange

- Une messagerie personnalisable et professionnelle

Microsoft Exchange Online offre la possibilité d'échanger avec des destinataires grâce notamment à des emails personnalisés. Il est l'outil le plus adapté pour la gestion de ses mails professionnels. Il permet de communiquer avec son nom de domaine ou créer des signatures personnalisées.

- Une messagerie collaborative

Exchange Online (et Outlook) répond à ces besoins qui ne cessent d'augmenter grâce à ses services reliés comme le partage de calendriers, la planification et délégation de tâches, la centralisation des contacts, l'utilisation de dossiers partagés...

- Un accès nomade

Exchange Online répond aux besoins de plus en plus importants de mobilité des collaborateurs. Exchange, via les services Office 365 donneront accès aux boîtes aux lettres électroniques à n'importe quel endroit, n'importe quand et depuis n'importe quel appareil (PC, tablette, smartphone...) grâce à la synchronisation en direct des services 365. Par exemple, si un utilisateur perd son téléphone, il pourra supprimer ses données personnelles et professionnelles à distance.

- Un stockage adapté et évolutif

La capacité de stockage de base est de 50Go par usager. Cette capacité de stockage peut paraître conséquente, mais elle a un avantage certain qui est d'éviter les archives et d'offrir la possibilité de revoir en ligne un large historique de mails. Il faut considérer le fait que certains abonnés se servent de la messagerie pro Outlook depuis plus de 20 ans. On peut alors comprendre que la synchronisation des archives avec l'espace de stockage de Microsoft Office 365 est un plus pour la pérennité des données. Il est possible de provisionner 100 GO par utilisateur voir plus.

- Une sécurité accrue

Les services de Microsoft sont réputés pour leur grande fiabilité en matière de sécurité. Le tri drastique des courriers indésirables, le dispositif de mise en quarantaine de certains mails ainsi que la personnalisation des filtres de sécurité accordent une certaine sérénité quant à la réception de mails « malveillants ».

- Une boîte aux lettres « intelligente »

La gestion de la boîte mail est personnalisable notamment grâce à la création de dossiers et sous-dossiers pour une meilleure organisation. L'outil de recherche est lui aussi très efficace, il permet d'obtenir de meilleurs résultats et plus rapidement.

Les services Exchange sont reliés avec les différents services accessibles dans les abonnements Office 365… les échanges sur Skype Pro sont enregistrés dans un dossier dédié.

- Un calendrier performant

Le calendrier propose des options de planification de rendez-vous et de réunions. Mais il permet aussi de « capturer » des évènements depuis sa boîte mail comme des réservations d'avion et d'hôtel…

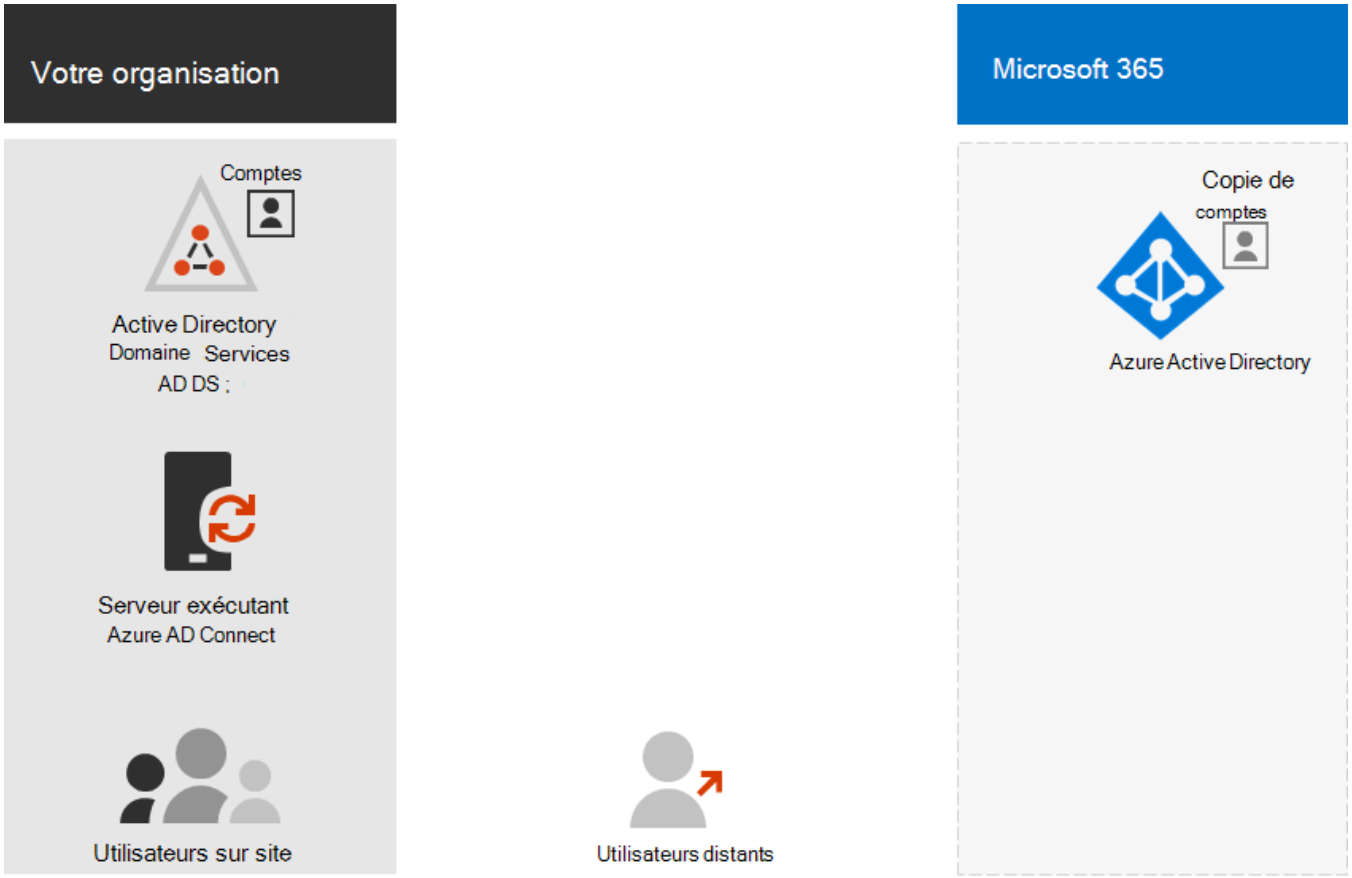
- Un calendrier partagé (ou non)

L'utilisateur est en mesure de gérer simplement les autorisations d'accès au calendrier. Grâce à cet outil collaboratif, il pourra vérifier la disponibilité de ses collaborateurs pour la planification d'un événement ou encore réserver un équipement ou une salle de réunion. Un assistant ou un collaborateur pourra également co-éditer le calendrier…

Il est aussi possible d'identifier des rendez-vous personnels ou privés dans ce calendrier. L'identification de ce type d'événements sera grisée vis-à-vis des autres collaborateurs. Ils n'auront donc pas accès aux détails de ces rendez-vous personnels ou privés.

16.2 Connexion au domaine Active Directory

Avec un domaine Active Directory (AD DS) sur site, nous pouvons synchroniser les comptes d'utilisateur, groupes et contacts AD DS avec le client Azure AD de l'abonnement Microsoft 365. Il s'agit de l'identité hybride pour Microsoft 365.



Azure AD Connect s'exécute sur un serveur local et synchronise nos services de domaine Active Directory avec le client Azure AD. En plus de la synchronisation d'annuaires, nous pouvons également spécifier les options d'authentification suivantes :

- Synchronisation de hachage de mot de passe (hachage)

Azure AD effectue l'authentification proprement dite.

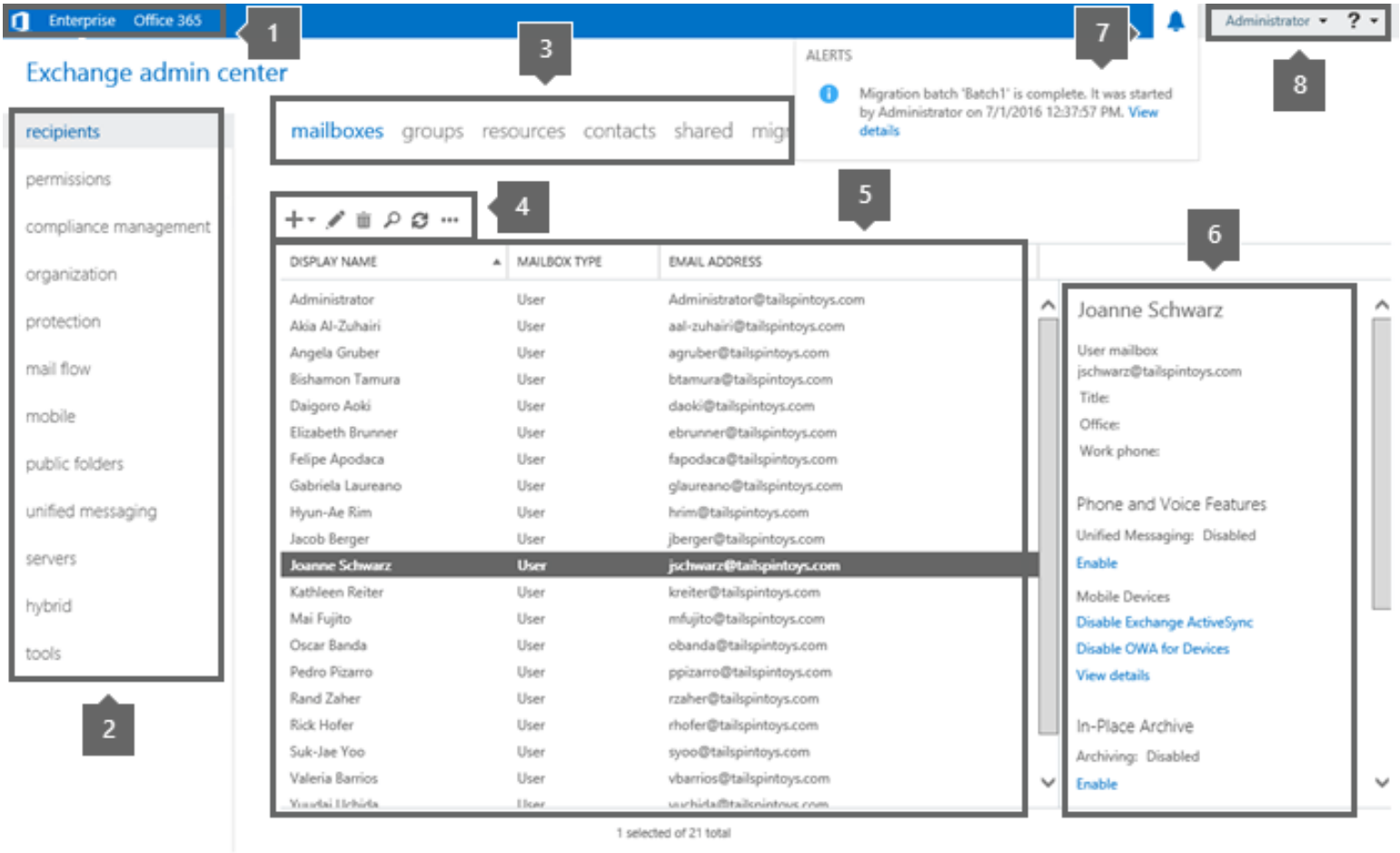
- Authentification directe (PTA)

Les services AD DS d'Azure AD effectuent l'authentification.

- Authentification fédérée

Azure AD fait référence à l'ordinateur client qui demande l'authentification à un autre fournisseur d'identité.

16.3 Centre d'administration Exchange Online



1. Navigation intersites
2. Volet des fonctionnalités
3. Onglets
4. Barre d'outils
5. Affichage liste
6. Volet d'informations
7. Notifications
8. Vignette de l'utilisateur en cours et Aide

17. Impression.

17.1 Pourquoi mettre en place une politique d’impression ?

Aujourd'hui, les entreprises recherchent des solutions professionnelles qui leur permettent de travailler plus intelligemment. Quel que soit leur niveau d'avancement dans l'adoption d'une stratégie de gestion de l'impression et de numérisation, elles peuvent réduire leurs coûts et améliorer la productivité de leur parc d’impression, mais aussi renforcer la sécurité documentaire.

Une gestion centralisée du parc d’impression entraîne une réduction des coûts pouvant atteindre 30 %, le renforcement de la sécurité des documents et l’amélioration de la productivité. De plus, le fait de s’authentifier permet à l’utilisateur de récupérer ses propres impressions sur n’importe quel multifonction du parc selon des règles qui lui ont été attribuées (Noir & Blanc uniquement, en recto/verso, agrafé par exemple). L’administrateur de la solution lui retrouve l’activité globale et détaillée du parc d’impression et peut générer des rapports d’audit factuels.

Réduction des coûts d’impression

Combien d’impressions, de copies et de numérisations sont réalisées et quel est leur coût ? Toutes les activités d’impression, de copie et de numérisation peuvent être suivies en temps réel par utilisateur, groupe d’utilisateurs, projet ou centre de coût, ce qui facilite la création d’historiques complets.

Par exemple, un budget individuel peut être alloué à chacun, ce qui simplifie la maîtrise des coûts d’impression, de copie, de numérisation. Les budgets alloués aux utilisateurs ou aux groupes d’utilisateurs peuvent aussi être redéfinis ou plafonnés automatiquement à des intervalles donnés.

Amélioration de la productivité

Les salariés utilisent-ils les systèmes d'impression multifonctions de manière efficace et productive ? C'est le cas, en s'assurant notamment que les documents sont capturés avec précision et distribués automatiquement dans des destinations prédéfinies autorisées. La capture précise de documents et les fonctionnalités de traitement robustes rendent également la recherche et la récupération de documents plus rapides et plus faciles. Le transfert des documents peut aussi être automatisé vers des bibliothèques de documents Microsoft SharePoint, ce qui aide les salariés à communiquer et à collaborer entre eux, ainsi qu'avec des clients, des partenaires et des fournisseurs.

En outre, l'impression sécurisée à partir de n'importe quel périphérique mobile est un prérequis pour permettre aux employés d'imprimer des documents sur le multifonction au bout du couloir ou au bout du monde.

Optimisation de la sécurité documentaire

81%* des décideurs informatiques se déclarent préoccupés par la sécurité documentaire et 61%* disent avoir subi une fuite de données en lien avec des documents imprimés. Qui imprime ou numérise des documents ? De quels documents s'agit-il ? Les tâches sont-elles sécurisées ? L'authentification des utilisateurs par badge, code, ou login/mot de passe pour libérer les impressions renforce la notion de confidentialité d'un document et permet d'éliminer les impressions oubliées sur le copieur.

En s'appuyant sur un fournisseur de Managed Print Services, les entreprises peuvent améliorer la gestion des impressions et la capture documentaire.

17.2 Les objectifs de la politique d'impression

Lorsque l'on fait réaliser un audit de son parc d'imprimantes et photocopieurs, l'objectif premier est de réduire les coûts d'impression et de faire des économies d'encre. Mais cela peut également être élargi à l'efficacité des flux de documents numérisés et à la gestion électronique des documents (GED).

Un audit sur l'ensemble d'un parc d'imprimantes et photocopieurs permet d'identifier puis d'actionner différents leviers d'économie. Cela offre plusieurs avantages pour optimiser les coûts d'impression et pour tirer efficacement parti de la transformation digitale.

L'usage d'appareils multifonctions (photocopieurs/imprimante/fax) peut aussi amener sa pierre à l'édifice dans la politique d'impression et faciliter une réduction des coûts :

- **Flexibilité** accrue pour l'utilisateur : un utilisateur peut déclencher un travail d'impression à partir de n'importe quel périphérique souhaité dans l'entreprise.
- **Services** mieux gérés : garantit les bons périphériques au bon endroit pour répondre aux besoins des utilisateurs avec la possibilité de fournir à tout moment des rapports d'utilisation détaillés. Les services d'impression peuvent fournir à chaque département, sur demande, au début de chaque nouveau mois, un rapport sur leur utilisation du mois précédent.
- **Durabilité** – les appareils d'impression multifonctions sont des dispositifs écoénergétiques qui réduisent l'empreinte carbone de l'entreprise. De plus, les tâches ne sont imprimées que lorsque l'utilisateur le décide. Ainsi, en cas d'erreur ou de modification, le papier n'est pas gaspillé.
- **Économique** – les imprimantes ou photocopieurs multifonctions sont plus rentables et les fournitures et les services de maintenance sont inclus dans le programme. La maximisation de l'utilisation de ces périphériques permet de tirer parti de ces accords pour obtenir une tarification au volume qui peut réduire davantage les coûts d'impression dans l'entreprise.
- **Confidentialité** – les travaux d'impression ne sont effectués que lorsque l'utilisateur les publie. Ainsi, les documents confidentiels ne sont pas oubliés et laissés sur des imprimantes ouvertes.

17.3 Le choix de la solution

Nous avons choisi de remplacer intégralement le parc d'impression de l'entreprise WOOD. Après une étude, nous avons décidé d'équiper chaque étage des bâtiments principaux de photocopieurs multifonction et de fournir à chaque directeur ou responsable ainsi que leur assistant(e) une imprimante multifonction par bureau.

	Lille	Annecy	Dax
Photocopieur multifonction (étage)	2	1	1
Imprimante multifonction (directeur/assistant)	19	6	5

Nous avons pour cela choisi de faire confiance à **Konica Minolta** afin de répondre aux besoins de l'entreprise en ce qui concerne la politique d'impression à mettre en place.

Un contrat de location de 5 ans, fixant un prix à la page, incluant le matériel, les consommables et la maintenance, sera mis en place.

La location d'un photocopieur est une solution plus onéreuse, mais qui permet de renouveler régulièrement son matériel, et de profiter d'un service de maintenance pendant toute la durée du contrat de location. Par ailleurs, le loyer est fixé à l'avance, ce qui permet d'éviter les mauvaises surprises.

En cas de panne, des techniciens agréés interviendront sur site sous 24 heures.

17.4 Le choix du matériel

Photocopieur multifonction - bizhub C250i

- 25/25 ppm en couleur et noir et blanc
- Formats papier : A6-SRA3, formats sur mesure et format de bannière jusqu'à 1,2 mètre de longueur
- Écran tactile couleur de 10,1 pouces en forme de tablette avec support multi-touch et interface utilisateur redessinée pour une utilisation intuitive et une facilité d'utilisation.
- Impact réduit sur l'environnement grâce à une technologie de pointe avec une consommation d'énergie réduite et compétitive - économie d'énergie et d'argent
- Sécurité maximale des données grâce à diverses fonctionnalités de sécurité, dont le moteur antivirus Bitdefender, qui réduit le risque de perte de données et préserve la confidentialité des données.

Imprimante multifonction - bizhub C3300i

- 33/33 ppm en couleur et noir et blanc
- Formats papier : A6-A4, dimensions spéciales
- Écran tactile couleur de 7 pouces en forme de tablette avec support multi-touch et interface utilisateur redessinée pour une utilisation intuitive et une facilité d'utilisation.
- Impact réduit sur l'environnement grâce à une technologie de pointe avec une consommation d'énergie réduite et compétitive - économie d'énergie et d'argent
- La plus haute sécurité des données, dotées de diverses fonctionnalités de sécurité, réduit le risque de perte de données et préserve la confidentialité des données.

18. Postes utilisateurs.

18.1 Introduction

Le parc d'ordinateurs existant étant plutôt ancien, nous avons décidé de remplacer l'intégralité des ordinateurs de la société Wood.

Cette décision coûteuse permettra de repartir sur une base saine au sein d'un parc homogène et jouissant de bonnes performances pour faire tourner des systèmes d'exploitations et applications toujours plus gourmandes.

À des fins de mobilité, la quasi-intégralité des postes seront des PC portables. Ainsi, les salariés pourront se déplacer librement au sein de la société avec leur ordinateur, ou exercer en télétravail si la situation sanitaire l'exige. Les seules personnes disposant d'un ordinateur fixe seront les utilisateurs nécessitant une station de travail beaucoup plus puissante.

Tous les postes utilisateurs seront équipés d'un SSD. Posséder un SSD est devenu un prérequis extrêmement important en 2020. Cela permet d'accélérer de façon non négligeable la vitesse du système d'exploitation. Il est également important de préciser que cela permet d'éviter la rencontre de problèmes lors du déplacement d'un ordinateur en fonctionnement.

18.2 Ordinateurs portables

Pour les ordinateurs portables, nous allons opter pour des Lenovo ThinkBook 15-IIL - 15,6 pouces

Configuration :

- Taille d'écran 15''
- Système d'exploitation Windows 10 Pro
- Processeur Intel Core i5 1035G1
- Mémoire vive 8 Go ram
- Carte graphique Intel UHD Graphics
- Stockage principal SSD 256 Go
- Poids 1 - 2Kg

Cet ordinateur portable a le mérite de proposer une configuration solide et un SSD, et ce pour un poids suffisamment léger pour être mobile.

Nous allons en acheter 175 pour les utilisateurs, au prix unitaire de 729€.

Tous les utilisateurs équipés d'un PC portable disposeront d'un écran externe 24 pouces de chez Lenovo :

Lenovo ThinkVision S24e-10 - écran LED - Full HD (1080p), au prix de 99,80€.

18.3 Stations de travail

Les utilisateurs des bureaux d'études / ingénieurs disposeront de stations de travail avec des processeurs plus puissants, et avec 32 Go de ram.

Ils disposeront également d'un écran 27 pouces de chez Lenovo.

- Processeur Core i7
- Stockage 512 Go SSD
- RAM / Taille installée 32 Go ram
- Système d'exploitation Windows 10 Pro
- Châssis Tour
- Type de disque SSD
- Lecteur de carte Carte mémoire SD

Les stations de travail sont plus onéreuses, mais néanmoins nécessaires pour certains utilisateurs qui utilisent des logiciels 3D complexes.

18.4 Total

Modèle	Quantité	Prix HT	Reduction	Total/an	Total
Lenovo ThinkBook 15-IIL - 15.6" - Core i5 1035G1 - 8 Go RAM - 256 Go SSD	175	729,00 €	20%		102 060,00 €
Lenovo ThinkStation P330 (2nd Gen) - tour - Core i7 9700 3 GHz - 32 Go - SSD 512 Go	18	1 210,59 €	20%		17 432,50 €
Lenovo ThinkVision S24e-10 - écran LED - Full HD (1080p)	175	99,80 €	10%		15 718,50 €
Lenovo ThinkVision T27i-10 - écran LED - Full HD (1080p)	18	200,00 €	10%		3 240,00 €

Tableau 10 - Budget total postes utilisateur

Ce qui fait un total de **138 450€** pour l'intégralité des postes utilisateurs et écrans.

19. Plan de continuité d’activité et plan de reprise d’activité.

19.1 Définition et explication

Plan de continuité d’activité : PCA

Qu’est-ce qu’un plan de continuité d’activité ?

Il s’agit de l’ensemble des mesures visant à assurer, selon divers scénarios de crise (y compris face à des chocs extrêmes), le maintien des prestations de service essentielles à l’entreprise. Un plan de continuité d’activité comprend l’analyse des risques, afin de pouvoir anticiper plusieurs scénarios : il peut s’agir d’un problème IT, d’une attaque de violation des données, d’une catastrophe naturelle sur un site, d’un incendie …

Quel est l’objectif d’un Plan de Continuité d’Activité (PCA) ?

Un travail de recherche et de prévention est à effectuer en amont afin d’établir des stratégies permettant de réagir efficacement à un scénario de catastrophe, à une alerte ou à une panne logicielle par exemple. Le plan de continuité d’activité (PCA) a un rôle de prévention et d’anticipation pour affronter un danger ou un risque opérationnel. Il renforce la résilience de l'entreprise. Il servira à coordonner les différentes actions à entreprendre, à réagir rapidement en rassemblant les bonnes personnes.

Plan de reprise d’activité : PRA

Qu'est-ce que le plan de reprise d’activité ?

Un Plan de Reprise d'Activité (PRA) permet d'assurer, dans le cas d'une crise majeure, la reconstruction de son infrastructure informatique et la remise en route des applications nécessaires à l'activité de l'entreprise. Il existe plusieurs niveaux de capacités de reprise qui sont à définir en accord avec les besoins de l'entreprise et ses moyens financiers.

À quoi sert le PRA ?

En cas d'incident ou de sinistre, le PRA garantit l'activité par un plan de sauvegarde et de remise en route et réduit les conséquences financières. Il est essentiel pour une entreprise d'atténuer l'impact des catastrophes pour sauver l'activité, mais aussi pour conforter l'image de fiabilité auprès des partenaires et clients. L’objectif est de concevoir une parade pour chaque menace potentielle.

19.2 Nos solutions

Plan de continuité d'activité :

Solution haute disponibilité des serveurs :

Nous proposons de mettre en place un premier serveur à Lille dans le bâtiment bureau, puis un second dans le bâtiment atelier.

Cela permettra plusieurs choses :

- Une répartition de charge entre les deux salles serveur
- Une redondance en cas de coupure d'une des deux salles

Redondance des switches cœur de réseau

Nous proposons de mettre en place un premier cœur de réseau à Lille dans le bâtiment bureau, puis un second dans le bâtiment atelier.

Cela permettra plusieurs choses :

- Une répartition de charge entre les deux cœurs de réseau
- Une redondance en cas de coupure d'une des deux salles

Liens WAN redondé

Nous proposons de disposer de plusieurs fournisseurs d'accès internet, afin de garantir plusieurs choses :

Site	Lien principal	Lien secondaire #1	Lien secondaire #2
Lille	Fibre SFR Business	Fibre Orange Open Pro	4G+ SFR Business
Annecy	Fibre SFR Business	Fibre Orange Open Pro	
Dax	Fibre SFR Business	Fibre Orange Open Pro	
Brest	SDSL SFR Business	Fibre Orange Open Pro	
Macon	SDSL SFR Business	Fibre Orange Open Pro	

Tableau 11 - Répartition des opérateurs internet par sites

Continuité électrique

Nous proposons d'installer un onduleur sur chaque baie informatique et réseau.

Pour la totalité de l'infrastructure, cela correspond à un minimum de 20 minutes d'autonomie en cas de coupure électrique.

Il y aura également un courant propre exempt de tout défaut et perturbation. Le logiciel d'Eaton propose une coupure automatique des serveurs dans les cas où la coupure de courant serait plus longue que prévu.

Plan de reprise d'activité :

Architecture miroir à Dax (cœur réseau, serveur, sauvegarde)

Nous disposons d'un hyperviseur, d'un serveur de stockage, d'un NAS de sauvegarde et d'un cœur de réseau de secours à Dax.

Cette infrastructure dormante permettra en cas de sinistre informatique à Lille sur les deux salles redondantes de redémarrer la production et de revenir à un état antérieur fonctionnel à J-1.

Système de sauvegarde (deux sites différent et Cloud)

Nos sauvegardes respectent la règle des 3-2-1 et permettent de revenir à un état antérieur en cas de panne.

Nous avons 3 sauvegardes sur NAS : 2 à Lille, 1 à Dax.

Nous avons 2 sauvegardes sur 2 médias différents, 1 sur disque et 1 dans le cloud.

La règle voudrait une externalisation de la sauvegarde du site principal. Dans notre cas, nous avons 2 sauvegardes externalisées, 1 dans le cloud et 1 à Dax.

Procédure de reprise d'activité

Des procédures normées vont être rédigées afin de contrer tout problème et situation imprévue. Ces procédures contiendront notamment l'intégralité des actions à réaliser de manière simple et claire. Elles intègreront le plan global de reprise d'activité de la société WOOD.

20. Conclusion.

Pour conclure, notre mission était de répondre à un appel d'offres de la société WOOD afin de leur proposer une solution technique sur l'infrastructure système et réseau dans l'objectif d'une refonte complète de leur SI.

Le travail fourni dans ce document répond au cahier des charges fonctionnel fourni par la société WOOD, dans le respect des délais, coûts, exigences et qualité.