BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS

Option : Solutions d'infrastructure, systèmes et réseaux

U5 – PRODUCTION ET FOURNITURES DE SERVICES INFORMATIQUES

SESSION 2020

_____

Durée : 4 heures
Coefficient : 5

_____

Matériel autorisé :
Aucun matériel ni document est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 16 pages, numérotées de 1/16 à 16/16
(sans compter la page de garde).

CAS DMAT

Le sujet compte 16 pages dont 9 pages de documentation.

Le sujet est constitué de trois dossiers qui peuvent être traités de façon indépendante.

Dossier documentaire

Barème

Dossier A	Intégration et sécurisation du site de Trèves	50 points
Dossier B	Ouverture à l'Allemagne	15 points
Dossier C	Évolution du stockage et de la sécurisation des données	35 points
	Total	100 points

Présentation du contexte

DMat est une société française créée en 2009 par un couple de concepteurs 3D, elle est basée à Metz. Spécialisée dans l'impression et dans la production de matériaux pour imprimantes 3D, elle s'est d'abord développée dans le prototypage de pièces puis a étendu son activité en investissant dans des imprimantes utilisant des matériaux variés comme le cobalt et le titane.

Forte de son expertise en matière d'impression 3D et soucieuse d'élargir son activité, la société s'est diversifiée dans l'impression tout public et propose la conception et/ou l'impression de pièces en filament PLA[1]. Ce matériel étant principalement importé de Chine, les créateurs se sont mis, il y a 5 ans, en relation avec des agriculteurs locaux et ont implanté à Thionville une usine de production de fils pour imprimantes. Forte de son succès, une deuxième unité de production a vu le jour en Allemagne, près de Trèves. Les deux usines sont presque entièrement robotisées. DMat possède également des bureaux au Luxembourg à Esch-sur-Alzette.

La société emploie soixante personnes à temps plein, elle est organisée en services :

- L'administration regroupe tous les services de gestion : ressources humaines, comptabilité, achats. Elle est basée à Metz et à Esch-sur-Alzette au Luxembourg.
- Le département Design, localisé à Metz crée les fichiers 3D et fait les études de matériaux pour les impressions. Ce département utilise des stations de travail puissantes pour le traitement des fichiers 3D avec un stockage dédié.
- Le département Impression est scindé en deux services : « Impression GC » et « Impression PUB ». « Impression GC » opère pour les grands comptes (groupes aéronautiques et automobiles pour lesquels sont créées des pièces uniques en matière rare) tandis que « Impression PUB » est le département qui gère les impressions des particuliers et petites sociétés.

Les deux départements partagent certaines imprimantes mais ils ont des sites *Web* bien distincts ainsi que des espaces de stockage spécifiques.

Le service informatique a un rôle primordial du fait des technologies innovantes utilisées, mais aussi en raison des besoins importants en matière de sécurité. En effet, les prototypes sont la cible de piratage industriel et la société s'engage auprès de ses clients grands comptes à mettre tout en œuvre pour garantir la confidentialité de leurs fichiers et prototypes.

Le service informatique compte 8 personnes : la cheffe de service qui gère l'infrastructure et la sécurité, un responsable système qui s'occupe de tous les serveurs et deux techniciens de maintenance par site.

La DSI n'a plus recours à des intervenants extérieurs et a procédé à votre embauche comme assistant(e) afin de l'aider dans ses différentes missions :

- l'intégration et la sécurisation du nouveau site de production de Trèves en Allemagne ;
- l'ouverture à l'Allemagne et notamment à l'adoption du protocole IPv6 ;
- l'évolution du stockage et de la sécurisation des données.

Vous vous appuierez sur les dossiers documentaires mis à votre disposition.

[1] Le filament PLA est un fil pour imprimante à base de maïs ou de betterave.

Dossier A – Intégration et sécurisation du site de Trèves

Le site de Trèves doit être intégré à l'infrastructure informatique de l'entreprise.
Votre rôle, en tant qu'assistant(e) de la DSI, est de préparer cette intégration en proposant les modifications à apporter aux règles de filtrage des sites et à la configuration du serveur DNS, et en préparant le déploiement des serveurs à l'aide de la solution de gestion de configuration *Ansible* utilisée par DMat.

Mission A.1 – Sécurisation des communications des sites

Le pare-feu MPLS (*MultiProtocol Label Switching*) « PS-RtM », présent sur le site de Metz, permet de sécuriser les communications inter-sites. Néanmoins, la sécurisation des communications doit être également assurée par des règles de filtrage configurées sur les commutateurs de niveau 3 sur le site principal de Metz et sur les routeurs MPLS des sites distants. Le dossier documentaire comporte un extrait des règles du commutateur S3X-M1 que la cheffe de service vous demande d'analyser.

Question A.1.1
Expliquer le rôle des règles N°1 et N°2 et les réseaux locaux virtuels (VLAN) concernés.

Afin d'intégrer le nouveau site, vous devez implémenter des règles de filtrage sur le routeur RtTr de Trèves, la règle par défaut est « bloquer » pour tout le trafic réseau entrant et sortant.

Question A.1.2
Écrire la (ou les) règle(s) permettant d'autoriser les communications SSH vers les serveurs de Trèves depuis les réseaux locaux virtuels (VLAN) DSI de Trèves et de Metz.

Question A.1.3
Écrire la (ou les) règle(s) permettant d'autoriser les communications DNS des réseaux de Trèves vers le serveur DNS de Metz.

Mission A.2 – Proposition d'une solution d'infrastructure

Dans le cadre de l'intégration du site de Trèves, vous devez proposer les modifications à apporter au fichier de zone DNS du site principal de Metz présent dans le dossier documentaire.

Question A.2.1
Ajouter les enregistrements DNS nécessaires afin de prendre en compte le nouveau site de Trèves.

Votre solution est en place sur les serveurs de Metz et Trèves. Vous devez maintenant configurer les postes clients du site de Trèves pour effectuer la résolution DNS.

Question A.2.2
a) Proposer un paramétrage DNS des postes clients qui permette d'assurer la résolution DNS même en cas de panne du serveur DNS local.

b) Proposer une procédure détaillée qui permette de tester ce paramétrage en vous appuyant sur les serveurs connus de l'entreprise qui sont présents sur le site de Metz.

Mission A.3 – Gestion des serveurs avec le logiciel de gestion de configuration *Ansible*

Suite à votre passage dans le service réseau de Metz, vous avez rapidement pris conscience de l'intérêt que présente le logiciel *Ansible* pour la gestion de la configuration des serveurs. Un nouveau responsable informatique du site de Trêve vient d'être recruté, il utilisait principalement des *scripts* et des images disques pour réaliser les tâches de configuration de ses serveurs. Votre mission d'assistant(e) de la DSI est de le convaincre de l'intérêt d'utiliser un outil de gestion de configuration.

Question A.3.1

Citer quatre arguments en faveur de l'utilisation d'un logiciel de gestion de configuration comme *Ansible* pour configurer les serveurs.

L'utilisation du logiciel *Ansible* est décidée, il est maintenant nécessaire de préparer l'intervention pour configurer les serveurs du site de Trèves.

Question A.3.2

Détailler les étapes nécessaires au déploiement de la configuration des serveurs du site de Trèves via le logiciel *Ansible*.

L'ensemble des serveurs est accessible via le protocole SSH sécurisé par clé asymétrique. Cette méthode d'authentification permet notamment d'éviter à tout moment le passage d'un mot de passe sur le réseau. L'administrateur voudrait donc désactiver l'authentification classique (couple login/mot de passe) sur les serveurs des zones *Out* de l'ensemble des sites.

C'est le fichier de configuration SSH (*/etc/ssh/sshd_config*) présent sur chaque serveur qui permet l'authentification par mot de passe via la ligne « PasswordAuthentication yes ». Pour empêcher cette méthode d'authentification, Il est nécessaire de passer cette directive à « no » et de relancer le service SSH.

Question A.3.3

a) Écrire le fichier d'instructions (*playbook*) « *securSSH.yml* » permettant de répondre aux contraintes de sécurité quant au service SSH.

b) Écrire la commande qui exécute le fichier d'instructions (*playbook)*.

Dossier B – Ouverture à l'Allemagne

Suite à l'ouverture du site de Trèves, l'entreprise DMat souhaite développer ses activités avec l'Allemagne, en particulier son site *Web* grand public qui permet à des PME ou des particuliers de demander la réalisation d'impressions 3D.

Le coût des liaisons MPLS est important et la cheffe du service informatique souhaite d'une part diminuer les coûts et d'autre part améliorer les liaisons entre les différents sites. En comparant les différentes offres des fournisseurs d'accès allemands ou luxembourgeois, il remarque qu'il existe des offres plus intéressantes à condition de passer au protocole IPv6 totalement ou partiellement.

L'entreprise étant dans un secteur de pointe, la direction est en général plutôt favorable aux projets innovants tant en matière de robotique que d'informatique. Aussi, la cheffe de service souhaite intégrer le protocole IPv6 dans son infrastructure.

Mission B.1 – Choix d'une solution technique

La cheffe de service vous charge d'effectuer des recherches sur le protocole IPv6 et d'en dégager des éléments de choix pour son projet d'intégration d'IPv6.

Vous devez dans un premier temps analyser l'impact d'un éventuel abandon du protocole IPv4 pour un passage au protocole IPv6 natif au niveau du réseau interne de l'entreprise. On vous fournit en particulier une liste de type de matériels utilisés sur le réseau.

Question B.1.1
Parmi les matériels présents, lister ceux qui doivent être remplacés en expliquant les raisons de ce changement.

Afin de préparer sa présentation auprès de la direction, la cheffe de service vous charge de la préparation d'une note de synthèse sur l'utilisation future du protocole IPv6 pour DMat.

Elle envisage pour le passage au protocole IPv6 :

- soit le passage au protocole IPv6 natif au niveau du réseau interne de l'entreprise et du réseau d'interconnexion des sites (actuellement via des liaisons MPLSv4) ;
- soit uniquement pour le réseau d'interconnexion des sites (MPLSv6) avec la solution *Dual-Stack Lite12*.

Question B.1.2
Présenter trois avantages de la solution *Dual-Stack Lite12* par rapport au protocole IPv6 natif.

Mission B.2 – Proposition d'une solution d'infrastructure

La solution MPLSv6 a été retenue et la cheffe de service a demandé une plage d'adresses IPv6 auprès du RIPE[2]. Cela lui permettra de pouvoir changer d'opérateur, voire d'en avoir plusieurs, et surtout, de ne plus avoir à faire de migration lourde à chaque changement.

Le RIPE lui a fourni l'adresse de réseau 2002:7a7b::/48

Dans un premier temps, seuls les routeurs d'interconnexion MPLSv6 et les serveurs *Web* utiliseront cet adressage IPv6. Le serveur *Web* public www de DMat aura l'adresse : 2002:7a7b:0:1241::1 et le serveur *Web* grand compte de DMat aura l'adresse : 2002:7a7b:0:1243::1.

Afin de préparer la migration, on vous demande de trouver les modifications à apporter au fichier DNS du site de Metz.

Question B.2.1
Écrire les enregistrements à ajouter au fichier DNS afin de prendre en compte l'adressage IPv6.

[2] Le RIPE (Réseaux IP Européens) est responsable des allocations d'adresses IP transfrontalières en Europe

Dossier C – Évolution du stockage et de la sécurisation des données

Mission C.1 – Choix et gestion d'une solution de stockage

La direction envisage d'installer un pôle Design à Esch-sur-Alzette et réfléchit à mettre en place le même type de solution XSan Raid que sur le site de Metz.

Question C.1.1
Présenter deux avantages d'utiliser une solution XSan Raid pour stocker les fichiers de développement 3D plutôt que le stockage sur les stations de travail.

Après avoir étudié les différentes architectures Raid supportées par la baie de stockage XSan, vous avez opté pour le Raid 50. La baie de stockage dispose de 12 disques de 500 Go. L'administrateur se demande quelle configuration choisir entre 3 grappes de 4 disques ou 4 grappes de 3 disques Raid 50.

Question C.1.2
a) Présenter, sous forme d'un tableau comparatif, les caractéristiques des deux configurations envisagées en termes de stockage utile, de tolérance de pannes et de performance.
b) Proposer la solution à mettre en œuvre pour le nouveau pôle Design d'Esch-sur-Alzette en expliquant votre choix.

Mission C.2 – Protection des données pour une mise en conformité avec le RGPD[3]

Le serveur Xsan Raid, comme de nombreux autres serveurs, contiendra des fichiers particulièrement sensibles. Il est essentiel pour DMat de se prémunir contre la perte ou le vol de ces données.

Parmi toutes les mesures visant à assurer une protection effective des données à caractère personnel et sensibles, le RGPD impose la limitation des accès aux seules personnes habilitées au sein de l'organisation. C'est dans ce cadre que la cheffe de service s'intéresse plus particulièrement à la protection des locaux sensibles dont la gestion des accès se fait actuellement grâce à des trousseaux de clés qui donnent accès aux différents locaux et secteurs suivant le niveau d'accréditation des employés.

Un état des lieux, résumé dans le dossier documentaire, a été mené.

Question C.2.1
Indiquer, en argumentant, si la solution actuelle d'accès aux locaux sensibles vous semble être en totale conformité avec la politique de protection des accès aux locaux sensibles de DMat et les exigences du RGPD.

Il a finalement été décidé de renforcer la protection des locaux sensibles. Une solution basée sur la technologie NFC présentée dans le dossier documentaire attire votre attention.

Question C.2.2
Présenter trois avantages d'une solution basée sur la technologie NFC par rapport à la solution actuelle.

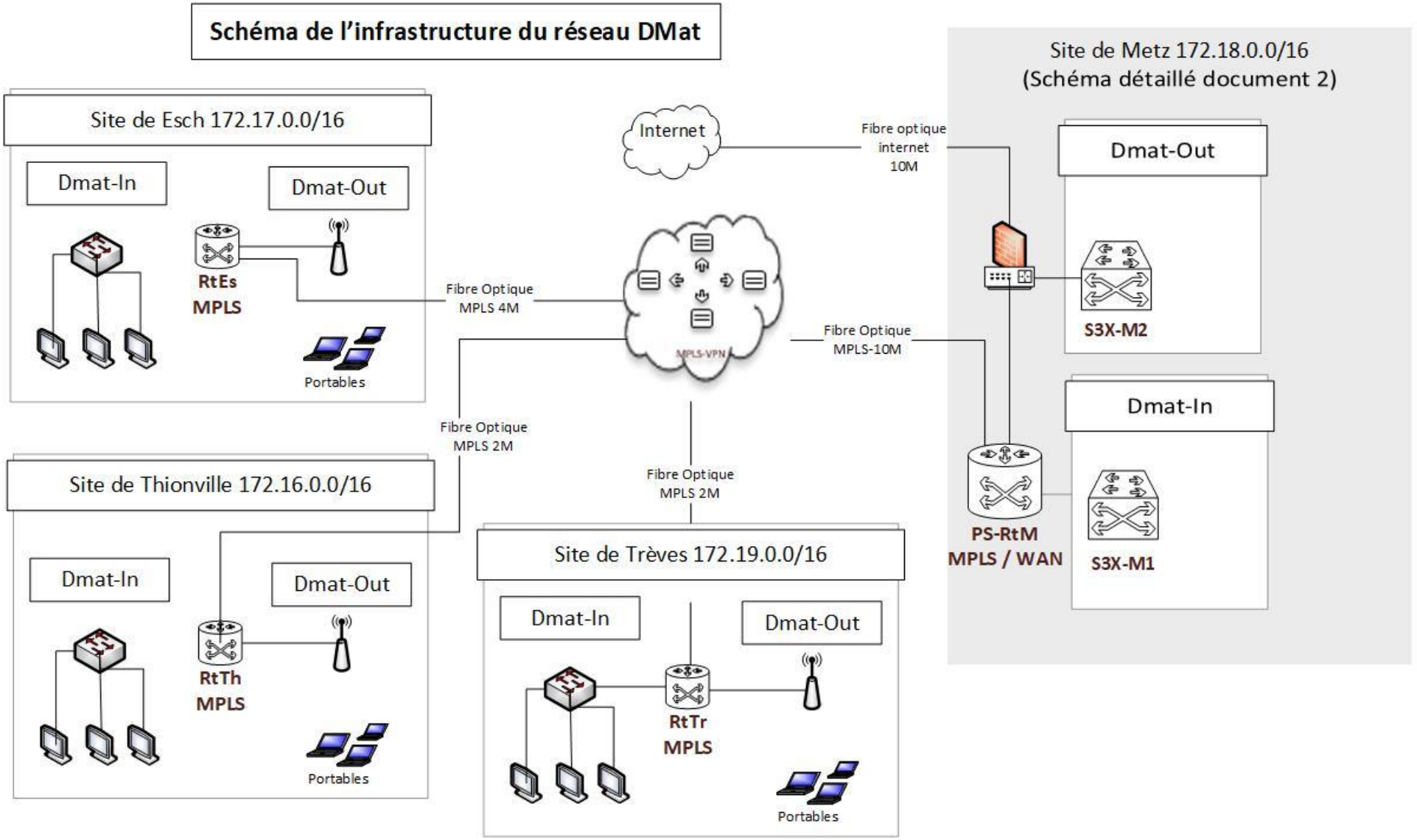
La solution NFC est choisie. Vous êtes en charge de la préparation et de la mise en place de cette solution qui sera implémentée sur chaque site.

Question C.2.3
Pour chaque élément du système de contrôle des habilitations, préciser le local technique dans lequel vous l'installerez. *Justifier votre réponse.*

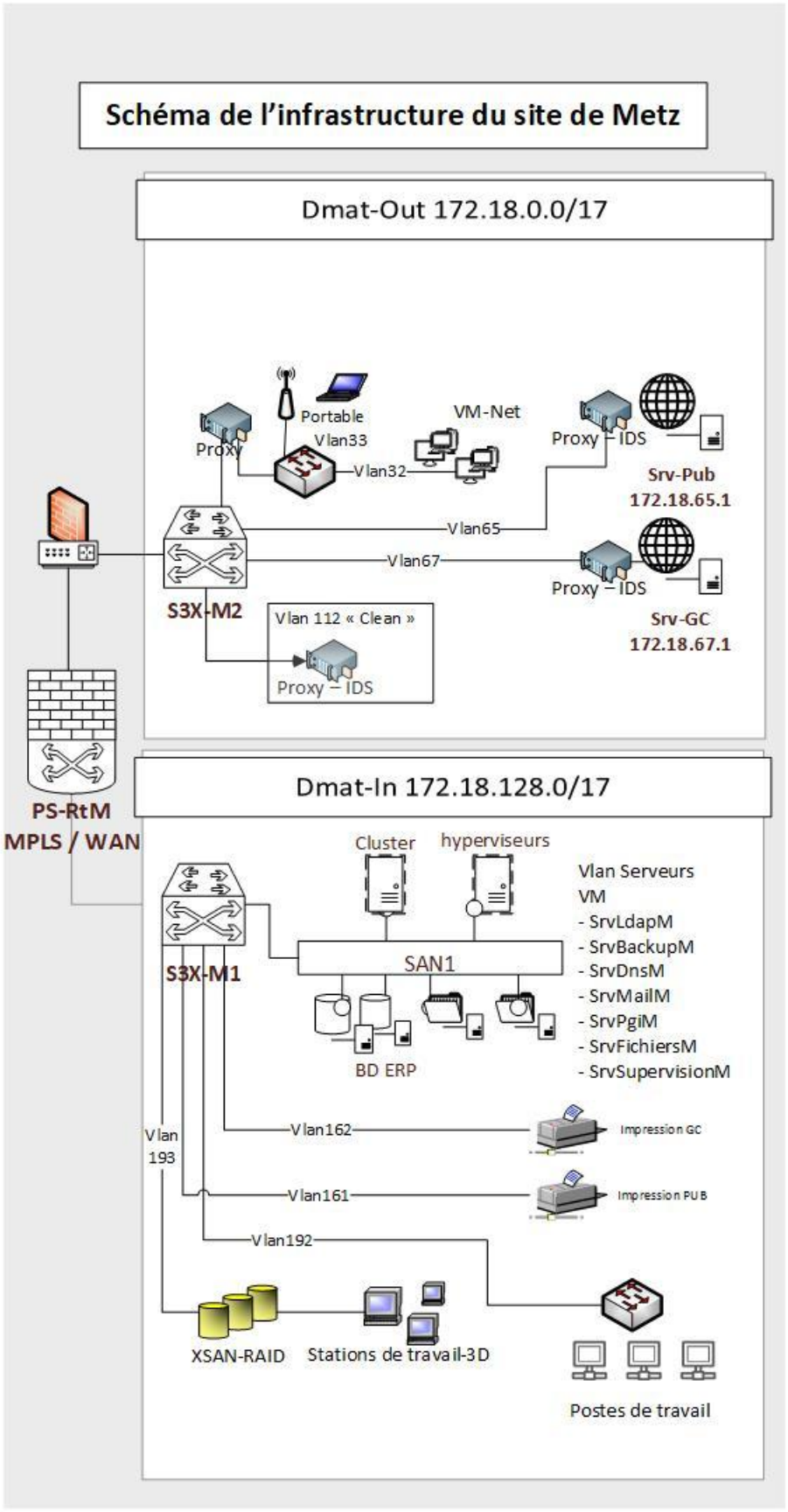
[3] RGPD : règlement général européen relatif à la protection des données personnelles.

DOSSIER DOCUMENTAIRE COMMUN

DOCUMENT 1 : Schéma de l'infrastructure du réseau DMat



DOCUMENT 2 : Schéma de l'infrastructure du site de Metz



DOCUMENT 3 : Plan d'adressage et description de l'infrastructure

Metz	**172.18.0.0/16**		
OUT	172.18.0.0/17		
	Vlan 31	DMZ, DNS	172.18.31.0/24
	Vlan 32	VM-Net	172.18.32.0/24
	Vlan 33	Wifi	172.18.33.0/24
	Vlan 65	Web-Pub	172.18.65.0/24
	Vlan 67	Web-GC	172.18.67.0/24
	Vlan 112	Clean	172.18.112.0/24
IN	172.18.128.0/17		
	Vlan 145	Serveurs	172.18.145.0/24
	Vlan 146	Backup	172.18.146.0/24
	Vlan 147	Administration	172.18.147.0/24
	Vlan 148	Achats	172.18.148.0/24
	Vlan 176	Production	172.18.176.0/24
	Vlan 161	Impression PUB	172.18.161.0/24
	Vlan 162	Impression GC	172.18.162.0/24
	Vlan 192	Postes de travail	172.18.192.0/24
	Vlan 193	Station-3D	172.18.193.0/24
	Vlan 224	DSI	172.18.224.0/24

Thionville	**172.16.0.0/16**		
OUT	172.16.0.0/17		
	Vlan 31	DMZ, DNS	172.16.31.0/24
	Vlan 32	VM-Net	172.16.32.0/24
	Vlan 33	Wifi	172.16.33.0/24
IN	172.16.128.0/17		
	Vlan 145	Serveurs	172.16.145.0/24
	Vlan 147	Administration	172.16.147.0/24
	Vlan 176	Production	172.16.176.0/24
	Vlan 224	DSI	172.16.224.0/24

Esch	**172.17.0.0/16**		
OUT	172.17.0.0/17		
	Vlan 31	DMZ, DNS	172.17.31.0/24
	Vlan 32	VM-Net	172.17.32.0/24
	Vlan 33	Wifi	172.17.33.0/24
IN	172.17.128.0/17		
	Vlan 145	Serveurs	172.17.145.0/24
	Vlan 146	Backup	172.17.146.0/24
	Vlan 147	Administration	172.17.147.0/24
	Vlan 148	Achats	172.17.148.0/24
	Vlan 224	DSI	172.17.224.0/24

Treves	**172.19.0.0/16**		
OUT	172.19.0.0/17		
	Vlan 31	DMZ, DNS	172.19.31.0/24
	Vlan 32	VM-Net	172.19.32.0/24
	Vlan 33	Wifi	172.19.33.0/24
IN	172.19.128.0/17		
	Vlan 145	Serveurs	172.19.145.0/24
	Vlan 147	Administration	172.19.147.0/24
	Vlan 176	Production	172.19.176.0/24
	Vlan 224	DSI	172.19.224.0/24

Tous les sites sont adressés selon le même principe. On trouve le numéro du site sur le deuxième octet et le numéro du réseau local virtuel (VLAN) sur le troisième octet. Par ailleurs, la dernière adresse de chaque sous-réseau (Vlan) est réservée à l'interface du commutateur cœur de réseau du réseau local virtuel Vlan correspondant. Les **serveurs DNS** appartiennent au réseau Vlan 31 de chaque site et prennent la première adresse.

Les différents sites, Metz, Esch-sur-Alzette et Thionville sont reliés par des liaisons MPLS (*MultiProtocol Label Switching*) afin de garantir un haut niveau de sécurité sur les échanges inter-sites. L'infrastructure MPLS définit un réseau privé de bout en bout qui ne transite pas sur internet, ce qui empêche tout tiers d'intercepter les données échangées. Les risques d'intrusions ou de failles de sécurité sont donc moins importants. La solution MPLS est paramétrée par l'opérateur qui supervise et maintient l'ensemble du réseau de l'entreprise. Un pare-feu mutualisé (l'équipement PS-RtM) permet de sécuriser les communications inter-sites.

Tous les équipements sont administrables via les réseaux Vlan DSI de chaque site et depuis celui de Metz.

Chaque site est divisé en deux zones, une zone **IN**, qui représente le réseau interne de l'entreprise, elle-même divisée en réseaux locaux virtuels, et une zone **OUT**, l'équivalent d'une zone démilitarisée (DMZ) découpée en plusieurs parties correspondant à différentes politiques de sécurité. La zone OUT est la zone composée des réseaux Vlan qui communiquent avec internet. Les utilisateurs n'accèdent pas directement depuis leur poste sur internet mais par le biais de machines virtuelles connectées à un réseau dédié (Vlan VM-Net) et protégé par un serveur mandataire - *proxy* -. Tous les éléments (fichiers, courriels) qui doivent entrer sur le réseau interne passent par une zone de décontamination (*reverse proxy*, système de détection d'intrusion, anti-virus, anti-spam).

Chaque service serveur est protégé par un logiciel *reverse-proxy* intégrant un système de détection d'intrusion (IDS) chargé d'analyser tous les flux et fichiers entrants et, le cas échéant, de bloquer les flux et les fichiers suspects.

DOCUMENT 4 : Fichier de la zone DNS dmat.net. (extrait)

1	$TTL 172800			
2	@ IN SOA SrvDnsM.dmat.net. hostmaster.dmat.net. (2018102200 ; serial 21600 ; refresh 3600 ; retry 3600000 ; expire 86400) ; minimum			
3	@	IN	NS	SrvDnsM.dmat.net.
4	@	IN	NS	SrvDnsEs.dmat.net.
5	@	IN	NS	SrvDnsTh.dmat.net.
6		IN	MX 10	SrvMailM.dmat.net.
7		IN	MX 20	SrvMailEs.dmat.net.
8	SrvDnsM	IN	A	172.18.31.1
9	SrvDnsEs	IN	A	172.17.31.1
10	SrvDnsTh	IN	A	172.16.31.1
	; serveur web public Srv-Pub			
11	SrvPubM	IN	A	172.18.65.1
	; serveur web Srv-GC			
12	SrvGCM	IN	A	172.18.67.1
	; Alias pour le serveur public			
13	www	IN	CNAME	SrvPubM.dmat.net.

DOCUMENT 5 : Types d'enregistrement DNS

A	Address	Renvoie une adresse IPv4 pour un nom d'hôte donné.
AAAA	IPv6 Address	Renvoie une adresse IPv6 pour un nom d'hôte donné.
NS	Name Server	Délègue la gestion d'une zone à un serveur de nom faisant autorité.
CNAME	Canonical NAME	Permet de réaliser un alias (un raccourci) d'un hôte vers un autre.
SOA	Start Of Authority	Définit le serveur maitre du domaine.
PTR	Pointer	Réalise l'inverse de l'enregistrement A ou AAAA, renvoie un nom d'hôte (FQDN) pour une adresse IP.
MX	MX record	Définit le nom du serveur de messagerie électronique du domaine.

Documents spécifiques au dossier A

DOCUMENT A1 : Extraits de la table de filtrage du commutateur S3X-M1 de Metz

N° de règle	*Adresse source*	*Port source*	*Adresse dest*	*Port dest*	**Action**
1	172.18.224.0/24	*	172.18.145.0/24	22/TCP(SSH)	Autoriser
2	*	*	172.18.31.1/32	53/UDP(DNS)	Autoriser
…					
Défaut	Toutes	Tous	Toutes	Tous	Refuser

NB : il s'agit de filtrage en mode « stateful », les règles de retour sont donc implicites.

DOCUMENT A2 : Présentation du logiciel Ansible

Pour homogénéiser et faciliter la maintenance de son parc, l'équipe réseau de DMat utilise le logiciel libre *Ansible* qui permet de centraliser la configuration système de machines au sein d'un référentiel unique, puis de déployer cette configuration sur l'ensemble ou une partie du parc informatique. *Ansible* permet le déploiement d'applications à distance, la gestion des services (lancement, arrêt, redémarrage, etc.), la copie ou la génération de fichiers de configuration (*template*), la gestion des paramètres système (interfaces, routes, montage, etc.) et l'interaction avec les principales plateformes des opérateurs de services en ligne (*cloud*).

Ansible gère de multiples systèmes d'exploitation et ne nécessite l'installation d'aucun logiciel ou agent spécifique car il se connecte grâce au protocole SSH via un couple de clés. Sur chaque hôte cible, le service SSH doit être activé et la clé publique du serveur *Ansible* doit être déployée.

DOCUMENT A3 : Intégration des machines dans le dispositif

Étape 1 - Elle consiste à faire figurer sur le serveur *Ansible*, les noms des hôtes (individuellement ou par groupe) qui sont administrés dans le fichier de configuration « */etc/ansible/hosts* » dont voici un extrait simplifié, présenté en colonnes (entre crochets, on trouve les groupes d'hôtes, avec les hôtes concernés en dessous) :

[site_metz] SrvPubM.dmat.net SrvGCM.dmat.net ProxyM.dmat.net SrvMailM.dmat.net SrvDnsM.dmat.net …. [site_esch] ProxyEs.dmat.net SrvMailEs.dmat.net SrvDnsEs.dmat.net ….	[Dmat-Out] SrvPubM.dmat.net SrvGCM.dmat.net ProxyM.dmat.net ProxyEs.dmat.net … [Dmat-In] SrvMailM.dmat.net SrvDnsM.dmat.net SrvMailEs.dmat.net SrvDnsEs.dmat.net ...	[serv_Mail] SrvMailM.dmat.net SrvMailEs.dmat.net … [serv_DNS] SrvDnsM.dmat.net SrvDnsEs.dmat.net …	À noter : • qu'il existe un groupe par défaut « all » qui définit tous les serveurs ; • que de nombreux autres groupes spécifiques ont également été créés.

Étape 2 - Elle consiste à copier la clé publique du serveur *Ansible* sur chaque machine.

DOCUMENT A4 : Fichier d'instructions (playbook) Ansible

Ansible fournit un ensemble de modules permettant d'effectuer les tâches les plus courantes comme installer un paquet, redémarrer un service ou bien modifier un fichier de configuration. Les actions à effectuer peuvent être exécutées individuellement en mode commandes ou bien depuis des fichiers d'instructions YAML (*Yet Another Markup Language*) appelés *playbook.* Ces derniers permettent de configurer une machine et de la faire évoluer ; ils décrivent les tâches que le logiciel *Ansible* doit accomplir sur les machines (installation d'un paquet si celui-ci n'est pas encore installé, copie d'un fichier s'il n'existe pas déjà et configuration de ce dernier avec telle ou telle directive, etc.).

Les fichiers *playbooks* utilisent une syntaxe très simple : on définit les hôtes, les variables éventuelles puis les tâches. Chaque tâche possède un nom et appelle des modules.

De nombreux fichiers *playbooks* pour l'installation d'un serveur de base, l'installation de services spécifiques (baseServers.yml, webServers.yml, dbServers.yml, etc.) ont été rédigés.

Extrait simplifié d'un fichier *playbook* qui initialise les serveurs sur un système Linux *Debian*

--- […] - name: Installation des paquets de base hosts: "{{ nomsHotes }}"	## les documents YAML commencent toujours par « --- » # Description du fichier playbook. # Utilisation du module hosts pour appliquer le playbook aux machines définies par la variable « nomsHotes » (option « -e » lors de l'exécution du playbook). Il est possible d'écrire directement ici un nom ou un groupe de machines plutôt qu'une variable.
tasks: - name: Mise à jour liste paquets et installation apt: update_cache: yes name={{ item }} state= present with_items: - vim - unzip - fail2ban […]	# Définition des tâches. # Description de l'action. # Utilisation du module *apt* pour mettre à jour (update_cache: yes et upgrade: dist) et installer les paquets s'ils ne sont pas déjà installés (state=present) qui sont définis dans la boucle {{ item }}. {{ item }} correspond à une variable qui utilise les valeurs présentes dans la directive with_items. Ici, elle va itérer sur les valeurs permettant d'installer la liste de paquets. À noter que si un seul paquet doit être installé, l'utilisation d'une variable n'est pas nécessaire (name=nom_paquet state=present).
- name: Configuration de fail2ban copy: src: fail2ban.conf dest: /etc/fail2ban/jail.d/defaults-debian.conf […]	# Utilisation du module *copy* qui va copier un fichier source sur les machines.
- name: Configuration de zabbix-agent lineinfile: dest: /etc/zabbix/zabbix_agentd.conf regexp: '^ServerActive=127.0.0.1' line: 'ServerActive=172.18.145.1' regexp: '^Hostname=' line: 'Hostname={{ inventory_hostname }}'	# Utilisation du module *linefile* qui permet de modifier les lignes d'un fichier. # Fichier qui doit être modifié. # Recherche de la ligne qui commence par « ServerActive=127.0.0.1 ». # Modification par ServerActive= adresse IP du serveur de supervision ici 172.18.145.1. # Recherche de la ligne qui commence par « Hostname= » # Modification par Hostname=contenu de la variable « inventory_hostname ». Cette variable contient le nom de la machine sur laquelle s'applique le playbook.
- name: Redémarrage de zabbix-agent service: name: zabbix-agent state: restarted	# Utilisation du module service pour redémarrer zabbix-agent après modification de la configuration.

Exécution d'un fichier *playbook*

Ansible est généralement exécuté en mode *push* : un poste de commande lance le fichier *playbook* sur tout ou partie des machines cibles (décrites dans le fichier d'inventaire */etc/ansible/hosts*) :

ansible-playbook baseServers.yml -e "nomsHotes=serv_DNS"

Ansible va se connecter à tous les hôtes compris dans le groupe « serv_DNS » et jouer les différentes étapes du scénario. Ici serv_DNS est la valeur donnée à la variable nomsHotes déclarée dans le script.

Si le nom d'une machine ou d'un groupe de machines est spécifié directement dans le fichier *playbook* au niveau du module *hosts*, il suffit d'appeler la commande **ansible-playbook baseServers.yml** sans option.

Documents spécifiques au dossier B

DOCUMENT B1 : Protocole et adressage IPv6

L'adresse IPv6 est une adresse IP dans la version 6 du protocole IP (IPv6). Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits (4 octets) pour le protocole IPv4.

Notation d'une adresse IPv6

Une adresse IPv6 est notée en hexadécimal et comporte 16 octets, où les 8 groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points comme dans l'exemple suivant : 2001:0db8:0000:0853:0000:0000:ac1f:8001.

Préfixe IPV6

Le préfixe de routage d'une adresse IPv6 est divisé en un préfixe de réseau et un préfixe de sous-réseau. Ceci est représenté dans la notation CIDR (*Classless Inter-Domain Routing*), c'est-à-dire le routage inter-domaine sans classe. Ainsi, la longueur du préfixe en bits est définie à l'aide du signe slash (*/*).

La notation 2001:0820:9511::/48 correspond par exemple à un sous-réseau avec une adresse de 2001:0820:9511:0000:0000:0000:0000:0000 à 2001:0820:9511:FFFF:FFFF:FFFF:FFFF:FFFF.

Préfixe de routage		Identifiant d'interface (Interface ID)
2001:0620:0000	**:0000**	**:0211:24FF:FE80:C12C**
Préfixe de réseau / Topologie publique	Préfixe sous-réseau / Topologie du site	
48 bits	16 bits	
64 bits		64 bits

En règle générale, le réseau /32 est attribué par le RIR[4] aux fournisseurs d'accès à internet (FAI), qui le divise ensuite en sous-réseaux. Pour les clients, ce sont des réseaux /48 ou /56 qui sont octroyés.

DOCUMENT B2 : Interopérabilité des protocoles IPv4 et IPv6

Les adresses IPv4 et IPv6 ne sont pas compatibles, la communication entre un hôte ne disposant que d'adresses IPv6 et un hôte ne disposant que d'adresses IPv4 constitue donc un problème.

Deux approches sont possibles pour permettre la communication :

- les traducteurs de protocoles au niveau réseau, transport ou applicatif. Si elle peut servir à procurer la connectivité pour un nombre d'hôtes ou d'applications limités, la traduction se heurte à des problèmes d'échelle et de performances ;
- la double pile (*Dual-Stack*) IPv4-IPv6 qui consiste à doter les hôtes IPv4, et les serveurs en particulier, à la fois d'adresses IPv6 et IPv4 afin de communiquer avec les hôtes IPv4 et IPv6.

Dual-Stack Lite12 permet d'interconnecter des réseaux IPv4 à travers un réseau d'opérateurs adoptant le protocole IPv6 natif (*full IPv6*). Le routeur chez le client est connecté à l'opérateur en IPv6 et tout le trafic IPv4 de l'entreprise est encapsulé dans un tunnel IPv6 vers IPv4 (*6to4*).

DOCUMENT B3 : Type de matériel installé dans les sites Dmat

Nombre	Type	Nom	Compatibilité IPv6
4	Point d'accès WiFi	AP-site	Administrable en IPv4 uniquement
1	Passerelle sécurité MPLS	PS-RtM	Compatible pour le trafic IPv6 natif et *Dual-stack Lite 12*
3	Routeur MPLS filiale	Rt-site	Compatible pour le trafic IPv6 natif et *Dual-stack Lite 12*
5	Commutateur multi-couches	S3X-M	Compatible pour le trafic IPv6
10	Commutateur couche 2	S2X-x	Administrable en IPv4 uniquement

[4] RIR : registre internet régional. Pour l'Europe, il s'agit du RIPE (réseaux IP européens).

Documents spécifiques au dossier C

DOCUMENT C1 : Organisation du stockage des fichiers sur le site de Metz

Les fichiers sont au cœur de l'activité de l'entreprise et la direction ne veut pas tomber aux mains d'un rançongiciel (*ransomware*). Aussi, la cheffe de service a cloisonné le stockage des fichiers de l'entreprise et l'accès à internet. Pour naviguer sur internet et lire les courriels, les collaborateurs utilisent des machines virtuelles (VM) sur un réseau Vlan spécifique « VM-Net » (Vlan 32).

Les fichiers 3D, reçus sur ce domaine « public » et qui doivent être utilisés sur le réseau interne, sont transférés sur un serveur de décontamination avant d'être renvoyés sur le domaine interne.

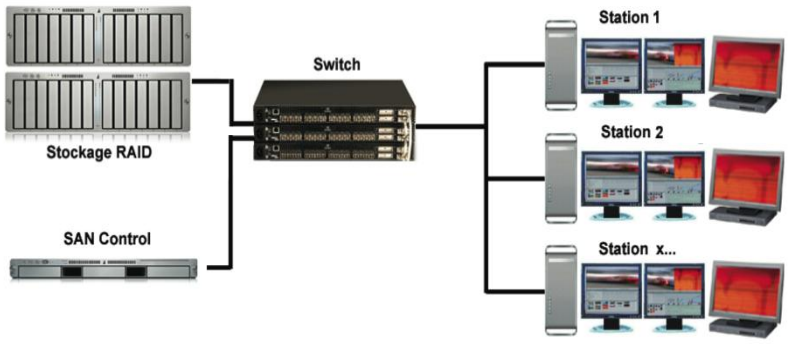
Le stockage des données est réparti en 4 espaces :

- stockage des données de gestion de l'entreprise, base de données du progiciel de gestion intégré (PGI), fichiers internes centralisés sur le réseau de stockage (SAN) de l'entreprise ;
- stockage des fichiers d'impression 3D des clients publics ;
- stockage des fichiers d'impression 3D GC des clients grands comptes ;
- stockage pour les fichiers de développement 3D du service Design (réseau de stockage partagé de type *XSan Raid*).

Chaque concepteur (*designer*) impliqué dans un projet dispose d'un accès simultané aux fichiers de développement 3D, sans jamais avoir à transférer ces données de station en station. Étant donné la taille importante des fichiers 3D, la rapidité est un critère primordial pour que les concepteurs puissent travailler de façon fluide.

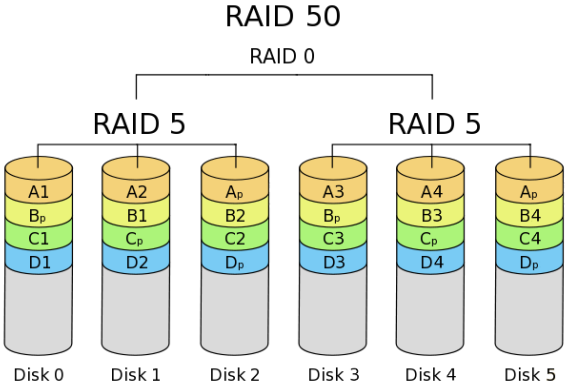
DOCUMENT C2 : XSan Raid

XSan Raid est une solution pour stocker et partager des médias à bande passante élevée. Les différentes architectures Raid supportées (0, 1, 3, 5, 01, 10, 30 & 50) permettent de choisir le compromis rapidité / fiabilité le plus adapté à chaque situation. Le système Raid *Fibre Channel* offre des débits pouvant aller jusqu'à 400 Mo/s.



DOCUMENT C3 : Le Raid 50 (source wikipedia)

Le Raid 50 permet d'obtenir un volume agrégé par bandes basé sur du Raid 5 + 0. Chaque grappe contenant au minimum 3 disques, et un minimum de 2 grappes étant nécessaire, il faut au minimum 6 unités de stockage pour créer un volume Raid 50. Il s'agit d'un des meilleurs compromis lorsque l'on cherche la rapidité sans pour autant vouloir trop dégrader la fiabilité.



DOCUMENT C4 : Protection des accès aux locaux sensibles

Chaque site dispose des locaux sensibles suivants :

Local 1	Stockage des sauvegardes (comprenant des données sensibles).
Local 2	Stockage des données sensibles (serveurs de stockage, serveurs de BDD, PGI, etc.).
Local 3	Cœur de réseau et arrivée des lignes externes.
Local 4	Serveurs applicatifs ne contenant pas de données sensibles.
Local 5	Stations de travail 3D.

Un fichier texte recensant l'ensemble du personnel concerné ainsi que tous les locaux dont l'accès est limité et listant les droits d'accès des utilisateurs est tenu à jour.

Pour être conforme au RGPD, le système doit permettre que seul le personnel dûment habilité soit admis dans les zones à accès restreint selon une plage horaire définie.

Par ailleurs, il doit être possible, lorsqu'un employé quitte l'entreprise, change de service ou est nouvellement affecté dans un service, de réexaminer et mettre à jour rapidement et facilement les permissions d'accès aux zones sécurisées et les supprimer si nécessaire. Dans l'idéal, les dates et l'heure d'accès doivent être consignées.

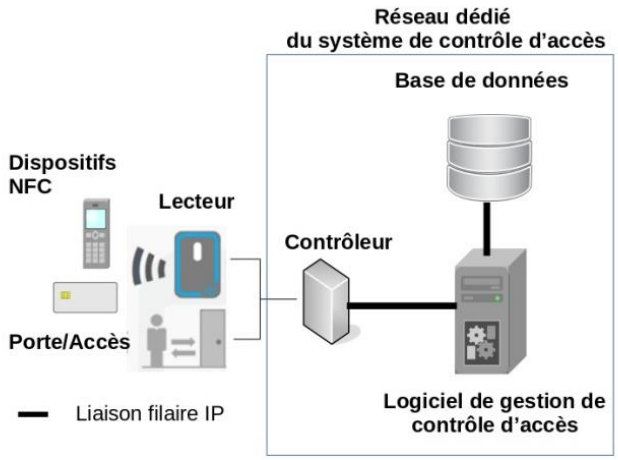
DOCUMENT C5 : Technologie NFC (Near Field Communication)

La technologie NFC ou CCP (communication en champ proche) est une technologie de communication sans fil à courte portée et à haute fréquence, permettant la communication et l'échange d'informations entre deux objets équipés de ce dispositif (un lecteur et un badge par exemple) sur une courte distance (inférieure à 10 cm en général).

L'échange des données est sécurisé car, d'une part, la technologie NFC respecte des normes utilisant des algorithmes de chiffrement et d'authentification et, d'autre part, la courte distance qui sépare les appareils NFC réduit le risque de vol de données.

L'une des particularités des utilisations de cette technologie est d'autoriser différents modes de fonctionnement. Celui qui serait mis en œuvre ici est le mode passif « émulation de carte » : le dispositif (carte à puce, badge, mobile intégrant la technologie NFC ou tout autre objet compatible comme une montre) envoie l'information au périphérique NFC, présent sur un lecteur qui décrypte les informations contenues et les transmet à l'unité de traitement pour comparaison avec la base de données.

Ce dispositif doit être combiné avec une infrastructure complète intégrant des contrôleurs et des lecteurs d'accès, ainsi qu'un logiciel de gestion des habilitations accédant à une base de données permettant notamment de contrôler, de journaliser et d'horodater les accès. Cette infrastructure physique est généralement isolée logiquement du réseau.



L'idée est d'associer à chaque employé un identifiant qui sera présenté à un lecteur via un badge.

Le logiciel de contrôle d'accès définira pour chaque identifiant ses droits d'accès : en l'espèce, il prend la décision (ou pas) d'ouvrir la porte et gère la séquence de commandes associée.

Le contrôleur (positionné dans chaque local) permet d'appliquer la décision provenant du logiciel de gestion des accès.