BTS SIO option SISR

***

PPE 3-1

(Projet Professionnel Encadré)

Construit autour de La Maison Des Ligues (M2L)

MISE EN PLACE D'UN OUTILS DE GESTION DE PARC

ADMINISTRATION RESEAU A DISTANCESECURISEE

***

Suivi par Mohammed KARROUM

Date de distribution : 24 octobre 2014

Date de remise : 24 novembre 2014

Important *: toutes les questions doivent être formulées par écrit (courriel) à l'attention de M KARROUM qui les traitera avec les formateurs*

1. Présentation

La *Maison des Ligues* (La M2L), établissement du Conseil Régionalde Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d'autres structures hébergées. La M2L, comme vous le constaterez dans l'interview avec son responsable, doit fournir les infrastructures matérielles, logistiques et des services à l'ensemble des ligues sportives installées.

Pour assurer le développement du système éducatif sportif de la région Lorraine et des offres aux usagers, le conseil régional et la direction de la M2L ont décidé de développer des services et des capacités d'hébergement pour les ligues sportives.

La M2L comprend plusieurs départements et son organisation lui permet de répondre aux exigences de la région pour assurer l'offre de services et de support technique aux différentes ligues déjà implantées (ou à venir) dans la région.

Administration système (Mohammed Karroum)

Mission 1 : Mise en place d'un serveur de déploiement multi-images

Le parc informatique de la M2L commence à se diversifier au niveau des systèmes d'exploitation client. Si la plupart des machines sont équipés du système Windows 7, certaines ligues souhaitent travailler Windows 8. L'administrateur a déjà mis en place un serveur de déploiement d'images basé sur WDS. Il souhaite à présent y ajouter des outils permettant d'une part d'ajouter des images, des logiciels, des pilotes et d'autre part d'automatiser au maximum les déploiements. Les solutions retenues consisteraient à mettre en œuvre des outils MDT et WAIK.

Mission 2 : Mise en place d'un serveur d'application

Afin de faciliter les ligues et les services de la M2L dans leur installation, l'administrateur envisage de mettre en place un serveur d'application basé sur TSE permettant aux utilisateurs d'accéder et d'utiliser les applications qui y sont installées. Le serveur est hébergé dans le VLAN informatique dans un serveur suffisamment redimensionné, car tous les traitements se font au niveau du serveur. La solution offre plusieurs avantages : côté administration système, cela réduit les coûts d'exploitation, sécurise le serveur et les applications, utiliser les PC clients en tant que clients légers ne nécessitant pas de performance. Côté utilisateurs, ils peuvent accéder à partir du bureau à distance ou depuis une interface WEB, aux applications qui leurs affectées.

La solution peut être enrichie pour la mise en place d'une ferme de serveurs TSE pour assurer une haute disponibilité et la répartition de charge.

Il est donc vital, compte tenu du contexte, d'intégrer ce nouveau service dans l'infrastructure de la M2L.

Mission 3 : Mise en place d'outils de gestions de par cet d'incidents

Le parc informatique de la M2L et des ligues devient de plus en plus important. Il est composé entre autres de matériels, de logiciels, d'imprimantes, d'équipements réseau etc. accumulés tout au long des années. Les machines sont équipées de systèmes d'exploitation divers et des logiciels propriétaires et open source.

Compte tenu de la répartition des services sur plusieurs bâtiments et sur plusieurs étages, des exigences de performance et de réactivité attendues, une gestion manuelle du parc informatique devient rapidement longue et fastidieuse.

Afin d'assurer une meilleure gestion du patrimoine informatique au niveau de la M2L et des ligues qu'elle héberge, l'administrateur de la M2L vous confie la mission d'identifier un outil open source permettant d'inventorier le parc informatique concernant les configurations des ordinateurs. Cette gestion devrait à terme être automatisée pour gagner du temps, et suivre l'évolution du parc, par des remontées automatiques d'inventaires.

L’outil à retenir doit utiliser une interface web et doit être doté d’outils complémentaires pour permettre le déploiement d’agents sur des clients (quel que soit l’organisation du réseau) aussi bien Windows, Mac et Linux.

Outre les fonctions d’inventaire, le gestionnaire de parc à retenir devrait être ouvert, donc couplé à terme avec un autre outil permettant une gestion globale et intuitive de son parc informatique via une interface web, sur les aspects financier, comptable, administratif et technique.

En somme, l’ensemble des outils regroupera : l'inventaire, la gestion des achats et le support client (ou help desk).

- l'inventaire : le logiciel de gestion parc informatique doit scanner automatiquement le réseau de l'entreprise et ses postes pour en repérer l'existant logiciel et matériel ;
- la gestion des achats (gestion des licences) : le logiciel de gestion parc informatique doit être capable d’une gestion comptable et financière du parc à l'utilisateur ;
- le support client : le logiciel de gestion parc informatique offre un module de gestion des incidents.

La prestation attendue doit comprendre un document décrivant la solution technique retenue en en justifiant la pérennité, la cohérence et l’adaptation par rapport aux besoins exprimés, et un document d’implantation.

Administration réseau (Serge Riba)

1 Présentation

La *Maison des Ligues* (La M2L), association agrée du Conseil Régionalde Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d'autres structures hébergées. La M2L, comme vous le constaterez dans l'interview avec son responsable, doit fournir les infrastructures matérielles, logistiques et des services à l'ensemble des ligues sportives installées.

Pour assurer le développement du système éducatif sportif de la région Lorraine et des offres aux usagers, le conseil régional et la direction de la M2L ont décidé de développer des services et des capacités d'hébergement pour les ligues sportives.

L'association M2L possède plusieurs compétences et son organisation lui permet de répondre aux exigences de la région pour assurer l'offre de services et de support technique aux différentes ligues déjà implantées (ou à venir).

1.1 Objet de la prestation

La direction générale de la maison des ligues, se basant sur les recommandations de la commission sécurité de la région Lorraine en matière de sécurité informatique, a décidé d'aligner son système d'information sur ces exigences.

Pour cela, l'administrateur a décidé de refondre son réseau en introduisant tous les outils et composants permettant d'y renforcer la sécurité. Ce projet concerne la sécurisation de l'accès au service Internet, la sécurisation de l'administration à distance du réseau et la mise en place d'un service de haute disponibilité sur les nœuds principaux du réseau.

Mission 1 : Service d'accès sécurisé Internet - DMZ

Soucieux d'améliorer son offre aux associations, les responsables M2L décident de faire évoluer le service d'accès vers l'Internet en améliorantla qualité et la sécurité du traficentre le réseau interne et Internet ceci pour l'ensemble des utilisateurs de M2L.

Le projet s'étend aussi à la mise à disposition du public Internet de services d'accès aux sites WEB des ligues et de téléchargement de documents ou de brochures diverses. Ces serveurs sont accessibles à travers d'une zone commune sécurisée DMZ. Un serveur installé dans la DMZ hébergera ces services.

Un Pare Feu sera configuré sur les interfaces permettant l'accès à Internet et à la DMZ pour règlementer et filtrer les communications.

Mission 2 : Service d'administration à distance sécurisée

Pour pallier à certaines failles de sécurité relative à l'administration à distance des équipements constituant le réseau, l'administrateur a décidé derefondre son outil d'administration à distanceen utilisant un protocole sécurisé empêchant ainsi de possibles prises de contrôle sur les équipements par des utilisateurs non autorisés. L'administrateur décide d'utiliser l'application SSH pour administrer son réseau.

Mission 3 : Service de haute disponibilité

L'association, par l'intermédiaire de son service technique, se doit d'assurer une bonne qualité de service sur sonréseauvis-à-vis des utilisateurs. L'administrateur demande à son service technique de déployer les solutions permettant de sécuriser l'écoulementdu trafic même en cas de panne d'une liaison dans la chaîne de communication.

Cette exigence seraréalisée par l'implantation de matériels et de liens redondants sur les nœuds stratégiques du réseau afin de pallier aux défaillances possibles de ces éléments.

Il vous est demandé de préparer l'installation et la configuration des éléments sur les nœuds suivants :

- Le réseau de commutation des ligues comprendra les commutateurs d'accès et le commutateur de distribution qui seront reliés en boucle permettant ainsi l'introduction de chemins de secours.Les liaisons entre les commutateurs d'accès et le commutateur de distribution seront réalisées en double attachement par agrégation de liens pour pallier aux possibles ruptures de liaisons.
- L'accès Internet à haute disponibilité grâce à la redondance du routeur d'accès FAI. Deux abonnements Internet seront loués au FAI. Un abonnement qui portera tout le trafic en fonctionnement normal, le deuxième assurera la continuité Internet en cas de panne du premier.
- La redondance des services réseau DHCP et DNS

Cahier des charges

Ce cahier des charges fait référence aux données duplan d'adressage IPlivréesdans le PPE2. Pour vos réponses vous utiliserez tous documents, ou autres sources Internet vous permettant d'accéder aux informations utiles et en particulier les documents ***FTA 08 Commandes CLI Cisco*** et ***FT sécurité des données***.

La sécurisation des accès à Internet sera régit par un Pare Feu à l'intérieur duquel seront configurées des règles de contrôle d'accès ACL en respectant les exigences définies dans le tableau **Annexe 1**. Vous devez définir les scripts de configuration des règles ACL à implanter dans le routeur. Le Pare Feu sera implémenté dans le routeur RM2L sur les interfaces appropriées.

L'administration à distance sera réalisée en utilisant le protocole sécurisé SSH qui permet, tout comme le protocole Telnet d'accéder à un équipement à distance en utilisant le réseau.

Le réseau est intégré au domaine ***m2l.fr*** et les paramètres de connexion pour l'administration à distance Telnet et SSH sont décris dans l'annexe 2.

Les paramètres de l'application de sécurisation SSH pour l'administration à distance sont définis dans l'Annexe 2.

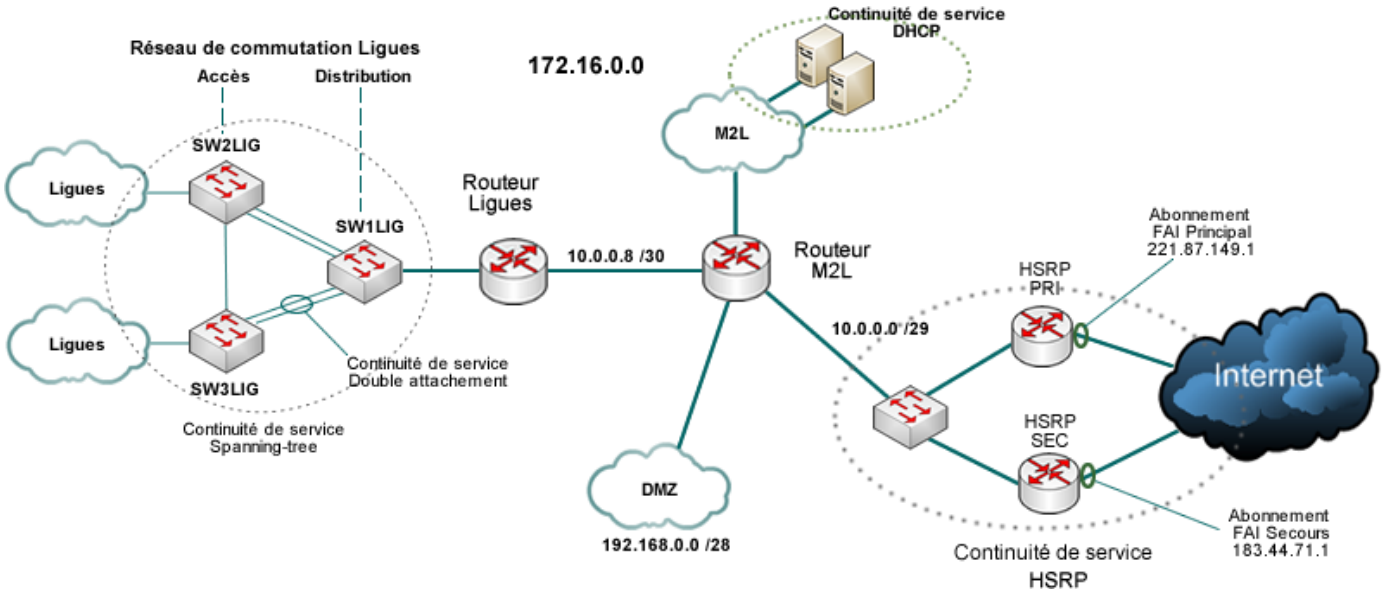
Les services de haute disponibilité sur les nœuds du réseau concernent le réseau de commutation des ligues, le service DHCP et la redondance du réseau d'accès à Internet. Les techniques qui seront employées pour la réalisation de ces projets font appel aux documents de spécification technique ***FTA 08 Commandes CLI Cisco*** et ***FT05 Commutation Ethernet*** ainsi que les documents officiels sur le site des constructeurs.

Les liaisons en double attachement reliant les commutateursd'accès au commutateur de distribution doivent être utilisées pour transporter la totalité du trafic des ligues. Le spanning-tree doit être configuré pour privilégier le trafic sur ces liaisons en phase opérationnelle (la liaison entre SW2LIG et SW3LIG est un secours en cas de défaillance des liaisons principales.

La continuité de service pour l'accès à Internet est réalisée à l'aide de 2 routeurs physiques vus comme un seul routeur virtuel par le routeur M2L, ces 2 routeurs se relaient en cas de panne. Cette fonction sera assurée par le protocole VRRP ou HSRP chez Cisco.

HSRP permet à un routeur de secours de prendre immédiatement le relais de façon transparente dès qu'un problème physique apparaît sur le routeur principal.

Si le routeur, que nous appellerons primaire, devient indisponible le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent une même adresse de passerelle IP et MAC virtuelle.



2 Déroulement de la mission

Dans cette prestation vous devrez produire pour chacune des 3 missions les documents de déploiement des services et le dossier de tests pour la validation du service. Vous réaliserez une maquette mettant en œuvre les différentes fonctionnalités conformément au cahier des charges ci-dessus.

2.1 Modalités de réponse

Vous constituerez le dossier du projet en y incluant le document d'étude et d'analyse des solutions, les documents d'architecture de configuration et de test des éléments de réseau. Vous intègrerez aussi le document de recette contenant les fiches de test en indiquant la couverture de test du réseau. Les Annexes 3 et 4 présentent le format des fiches de test à intégrer au dossier.

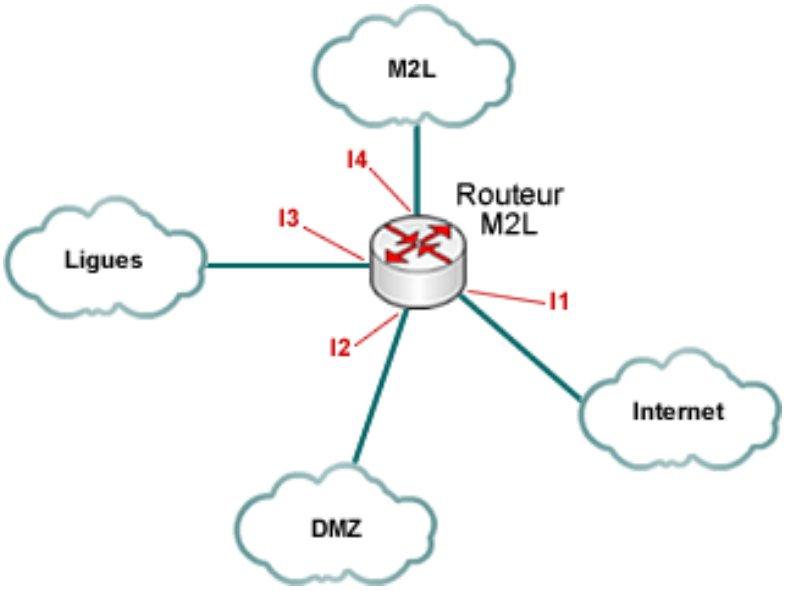
Votre projet sera accompagné d'une maquette qui permettra de présenter et valider la faisabilité technique de ce projet.

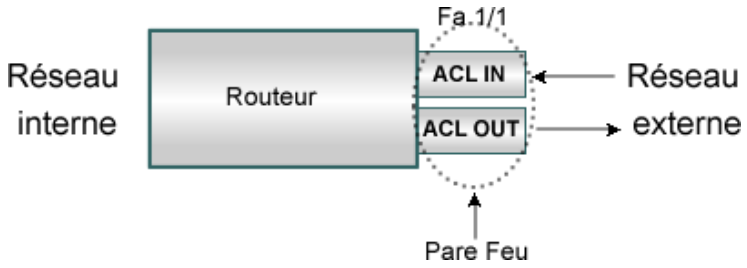
ANNEXE 1 – Définition des règles de sécurité d'accès à Internet

Le Pare Feu doit réaliser le filtrage des flux d'information entre les divers réseaux (internes, externe et DMZ) selon les contraintes décrites ci-dessous :

Contrainte	Interface*	Description
		Les sous réseaux des ligues et M2L ont accès à l'Internet mais il n'est pas possible pour le public Internet d'accéder à un des équipements du réseau interne.
		Les serveurs de téléchargement (FTP) et WEB Extranet (HTTP) de la DMZ sont accessibles à la fois par les sous réseaux des ligues et par le public Internet.
		Les sous réseaux de l'association M2L ne doivent pas accéder au serveur de téléchargement FTP de la DMZ sauf le sous réseau Informatique.
		Seuls les 7 postes du sous réseau Informatique M2L possédant les 7 adresses les plus hautes (dont les 2 postes de l'administrateur réseau) peuvent effectuer les commandes de test ping et tracert vers tous les éléments du réseau des ligues et vers l'Internet.
		Seul le serveur WEB de la DMZ peut effectuer des requêtes vers le serveur de base de données (sur le port 5430) situé dans le sous réseau informatique à l'adresse 172.16.2.57.

* Vous désignerez l'interface sur laquelle ou lesquelles vous placerez le ou les Pare Feu en donnant son libellé. Précisez à quelle adresse IP se réfère la ou les interfaces choisies. Les interfaces seront désignées en suivant le schéma ci-dessous :





Un routeur peut gérer plusieurs Pare Feux simultanément lorsque ceux-ci sont placés sur une ou plusieurs de ses interfaces. Un Pare Feu peut assurer le filtrage du trafic en entrée et/ou en sortie sur une interface et ceci de façon indépendante.

Le filtrage en entrée (IN) permet au routeur de refuser ou d'accepter des paquets dès leur entrée dans le routeur avant le traitement du routage. Le filtrage en sortie contrôle les paquets avant leur envoi sur l'interface.

Un Pare Feu sur le routeur Cisco est aussi appelé Access-List(ACL)et doit répondre aux exigences définies dans la stratégie de sécurité de l'entreprise.

La création et l'installation des règles de filtrage dans un routeur filtrant ou Pare Feu s'effectuent en deux phases :

Syntaxe d'une ACL:

Rx(config)#access-list*N°ID Action Protocole @IPsrcmask @IPdestmask paramètre*

N°ID : 100 à 299 si ACL étendue
Action : permit, deny ou remark
Protocole : IP, ICMP, TCP ou UDP
@IPsrc Mask: adresse IP de poste ou liste d'adresse IP d'où provient le paquet
Si adresse IP de poste, pas de masque et le champ est précédé du paramètre host
Si liste d'adresse IP on donne l'adresse de réseau et on ajoute le masque qui définit la liste des adresses IP
@IPdest Mask: adresse IP de poste ou liste d'adresse IP vers qui est destiné le paquet
Si adresse IP de poste, pas de masque et le champ est précédé du paramètre host
Si liste d'adresse IP on donne l'adresse de réseau et on ajoute le masque qui définit la liste des adresses IP
Paramètre : Prend les valeurs suivantes :
eq (égal) + le protocole application (Ftp, http, SMTP, DHCP…)
ou established si le protocole est TCP
ou echo-reply et/ou unreachable si le protocole est ICMP

On applique ensuite l'ACL sur une interface du routeur :

Rx(config)#*int fa x/y*
Rx(config-if)#*ip access-group ID outou in*

A ce moment, le routeur commence le filtrage des paquets.

ANNEXE 2 – Paramètres de l'application SSH

L'administration à distance utilise l'application SSH en lieu et place de Telnet qui présente des failles de sécurité en particulier une transmission des paquets sans cryptage vers les équipements.

Les paramètres permettant le fonctionnement du protocole SSH vis-à-vis des équipements de réseau sont définis ci-dessous :

- Application SSH
- Version 2
- Taille clé : 512 ou 1024
- Délai de renouvellement des clés (Time out) = 60 sec
- Nombre de tentatives en cas d'échec = 2
- Login : admin - Mot de passe : Btssio2015

ANNEXE 3 - Fiches de test

Nom du Test :

No test	Type scénario	Environnement	Date

Description du test

Résultats attendus

Description technique

Résultats obtenus

ANNEXE 4 - Exemple de fiche de test

Nom du Test : HSRP01

No test	Type scénario	Environnement	Date
01	HSRP	Les 2 abonnements FAI sont simulés par un routeur qui fournit 2 liaisons vers les 2 routeurs HSRP. Une 3ème liaison est créée sur le routeur pour simuler l'Internet.	jj/mm/2014

Description du test

Les routeurs HSRP sont reliés chacun à une interface du routeur du FAI (Fa0/1 pour la liaison principale et Eth 1/0 pour la liaison de secours).
On effectue un ping continu sur l'interface du routeur FAI qui simule l'Internet (Fa0/0). Affichage du Ping sur la console CMD de Windows.
On déconnecte le câble de la liaison principale.

Résultats attendus :

Le Ping donne une réponse correcte tant que la liaison principale est bien raccordée au routeur FAI.
Lorsque le câble est déconnecté, le Ping ne répond plus (délai de la demande dépassé) puis au bout d'un délai de quelques secondes, le Ping affiche à l'écran une réponse correcte.

Description technique :

Placez ici soit un schéma de description des éléments testés et/ou un commentaire de la configuration en test. Cette description doit être claire et précise pour permettre une bonne analyse et un bon diagnostic du test.

Résultat obtenu :

Indiquez ici le résultat et expliquez si ce résultat est différent du résultat attendu.

Economie Management (Aïcha Kannoui)

M2L décide d'étendre son réseau vers l'Internet et les réseaux externes avec accessibilité par l'ensemble des utilisateurs de M2L. Elle envisage, de plus, de sécuriser l'accès aux ressources internes vis-à-vis des intrusions pouvant provenir de l'extérieur afin de les protéger et mieux répondre aux besoins de ces associations.

L'échange d'information sur les réseaux est fondé sur le respect de règles normalisées définies à l'échelle mondiale.
Les protocoles réseau permettent la communication entre systèmes répartis au sein de l'organisation et sur Internet.

Mission

La mise en place du projet d'évolution du réseau (Mission NETCONNECT) nécessite la mobilisation de ressources humaines, technologiques et financières.
Cette mission représente un investissement, qu'il faut pouvoir évaluer puis budgéter afin d'en définir les conditions de financement et d'amortissement.
Ces informations sont importantes pour mesurer les paramètres de qualité de service du projet (retard, dépassement de budget, échec).

Dans cette mission il vous est demandé d'étudier le financement et en particulier de présenter le plan de financement pour les trois années à venir de la mission Netconnect.

Votre mission consiste donc à répondre aux questions suivantes :

- Gestion du projet de système d'information : coût, qualité, délai ;
- Budget d'un projet :
  * coût d'investissement/coût d'exploitation ;
  * caractéristiques des coûts (fixe/variable) ;
  * suivi d'un budget (dépenses).
- Gains qualitatifs : Identification et critères de mesure.
- Risques : identification, nature.

• Coût : quels sont les montants à investir ? Quels sont les coûts induits à prendre en compte ? Quelles sont les sources d'économie et leur montant prévisible ?

• Qualité : Quelle amélioration de la performance visée ? Comment cette amélioration sera mesurée ? Cela justifie t-il les investissements ?

• Service : Quelles sont les accessibilités et qualités de services souhaitées pour les outils (par exemple le portail unique pour les collaborateurs) ? Quelles sont les innovations radicales présentes dans le progiciel ?

• Vitesse : Quelle sera la réactivité aux changements liés aux métiers et aux besoins différents ou nouveaux des employés

Droit (Didier Pasquier)

La M2L, établissement du conseil Régional de Lorraine, met à la disposition de ligues sportive de Lorraine un ensemble de services et en particulier un service informatique sécurisé de stockage de leurs données.

Mission

1) En tant qu'informaticien de la M2L, le directeur de la M2L vous demande de lui présenter un dossier actualisé concernant la qualification juridique de la M2L, l'étendue de sa responsabilité juridique vis-à-vis de ses clients, les ligues. Ce dossier comprendra également un volet concernant les moyens de prévention des risques et de protection devant être mis en place chez M2L, chez ses clients et ses fournisseurs.

2) Le responsable juridique vous demande également un dossier actualisé sur les risques auxquelles sont exposées les données des clients que M2L héberge et les moyens juridiques de protection de ces données.