EXAMEN DE SECURITE INFORMATIQUE

Référence	ENSEEIHT – 2010-2011
Objet	Partiel de sécurité informatique
Auteur	M. Pierre-Yves BONNETAIN – B&A Consultants

CONTEXTE

La société MoyenneIndustrie (MI dans la suite du document) fabrique et vend des biens de consommation pour le grand public (la nature exacte des produits fabriqués n'a aucune importance). Elle intervient sur un marché à faible marge unitaire (marge réalisée sur chaque produit vendu) et à très forts volumes.

Le système d'informations de MI est tel que décrit par la figure 1. Il est calqué sur l'organisation physique de l'entreprise : le siège social héberge le coeur du système d'informations ; les deux unités de production (Usine1 et Usine2) contiennent des ordinateurs dits « de production », c'est-à-dire permettant de piloter les lignes de production, et des ordinateurs « de gestion », pour le personnel administratif délégué sur le site. Chaque ordinateur « de gestion » est associé à un collaborateur précis et identifié. A l'inverse, les ordinateurs de production peuvent être utilisés par tous les intervenants sur la chaîne de production, afin de régler ou modifier le fonctionnement des machines. : prise de contrôle

DESCRIPTION DU SYSTÈME D'INFORMATIONS

Le coeur du système d'informations de MI est implanté dans les locaux du siège social. On y trouve, sur des sous-réseaux spécifiques, les serveurs de fichiers, les systèmes de sauvegardes et le serveur de messagerie. Parallèlement à ces équipements vitaux, un sous-réseau spécifique est dédié à l'interface avec Internet : relais de messagerie et accès Web.

Le siège social utilise la plage d'adresses IP 10.1.*.*, chaque service (comptabilité, production, ressources humaines) ayant une sous-plage qui lui est propre (10.1.1 pour la comptabilité, 10.1.2 pour la production, 10.1.3 pour les ressources humaines). L'usine 1 utilise la plage d'adresses IP 10.2 (10.2.1 pour les postes de gestion, 10.2.2 pour les postes de production) et l'usine 2 utilise la plage d'adresses 10.3 (10.3.1 pour les postes de gestion, 10.3.2 pour les postes de production).

Tous les postes d'un même sous-réseau sont « remontés » vers un commutateur (switch), lequel est directement connecté au routeur de l'unité en question (siège social, usine 1, usine 2). Il n'existe pas d'autre élément de télécommunication internes. La figure 2 illustre ce point.

Toutes les machines et tous les serveurs utilisent des systèmes d'exploitation fournis par la société Microsoft : Windows XP pour les postes de travail, Windows 2003 Serveur pour les serveurs. Du fait de leur rôle critique pour l'entreprise, les postes de production, dans les deux usines, ne sont pas mis à jour. Les postes de gestion, tant dans les usines qu'au siège social, sont

↳ intégrité

Tournez SVP

automatiquement mis à jour le troisième jeudi du mois. Tous les ordinateurs, à l'exception des postes de production, disposent d'un anti-virus qui est automatiquement mis à jour toutes les quatre heures.

↳ anti-virus anti-spam .

MI dispose d'une unique connexion à Internet dont le point d'arrivée se situe au siège social. L'interconnexion entre le siège et les deux usines repose sur une offre VPN de leur opérateur de télécommunications. Cela signifie que chaque usine est aussi reliée à Internet (connexion ADSL) mais que le routage des paquets passe par des tunnels VPN en direction du siège social. Le routeur du siège social est la porte unique de sortie vers Internet pour toute l'entreprise, et les routeurs des deux unités de production sont configurés pour imposer cela.

Chaque routeur des unités de production est configuré afin de bloquer tout paquet entrant ou sortant s'il ne provient pas ou n'est pas destiné au routeur du siège social. Le seul protocole autorisé à entrer et à sortir d'une unité de production est celui lié au tunnel VPN.

Le routeur du siège social est configuré afin de n'accepter que les transactions entrantes destinées au relais de messagerie et les arrivées des tunnels VPN provenant des unités de production. Toute transaction sortante est autorisée. La navigation vers Internet est libre, le relais de navigation servant uniquement de cache afin d'optimiser la consommation de bande passante sortante.

Non

↳ anti-virus . contrôle de contenu . contrôle des URLs

Un correspondant informatique, sur chaque site de production, gère les postes informatiques, les commutateurs et le routeur.

Les relais doivent journaliser toutes leurs actions

QUESTIONS

Nous supposons qu'il n'existe aucun élément de sécurisation qui ne serait pas décrit précédemment. Si, dans vos analyses et réponses, vous faites des hypothèses quant à ce qui existe ou devrait exister, signalez de façon explicite ces hypothèses.

Afin de simplifier votre travail, nous considèrerons qu'il n'existe pas de contraintes budgétaires pour l'élaboration des solutions.

1. Indiquez les principaux risques que vous identifiez par rapport à l'organisation et au fonctionnement du système d'informations de MI, en signalant ce que vous considérez comme les trois principaux risques. **Justifiez et argumentez** votre analyse.

2. Pour les trois principaux risques identifiés, discutez des mesures de prévention, de détection et/ou de contingentement que vous proposeriez à MI. **Discutez de leurs avantages et inconvénients**.

3. MI veut mettre en place un contrôle et filtrage de la navigation de ses utilisateurs, qui reposera sur le cache actuellement installé au siège social. Qu'est-ce qu'une telle demande va imposer à l'entreprise, sur le plan technique, organisationnel et humain ?

4. Des journalistes ont reçu, par courrier électronique, des documents confidentiels de l'entreprise, rédigés par et pour le comité de direction uniquement. Ces documents sont stockés sur le serveur de fichiers de l'entreprise.

4.1. Quelles investigations (avec leurs éventuelles limites) mèneriez-vous afin d'identifier l'origine de la fuite ?

Journalisation relais de messagerie

4.2. Quelles mesures prendriez-vous pour éviter qu'un tel incident se reproduise dans l'avenir ?

contrôle de contenu → sur des flux sortant

控制文件权限 1) 文件加密 3) 时间期限

2) 权限指定 4) 使用医师

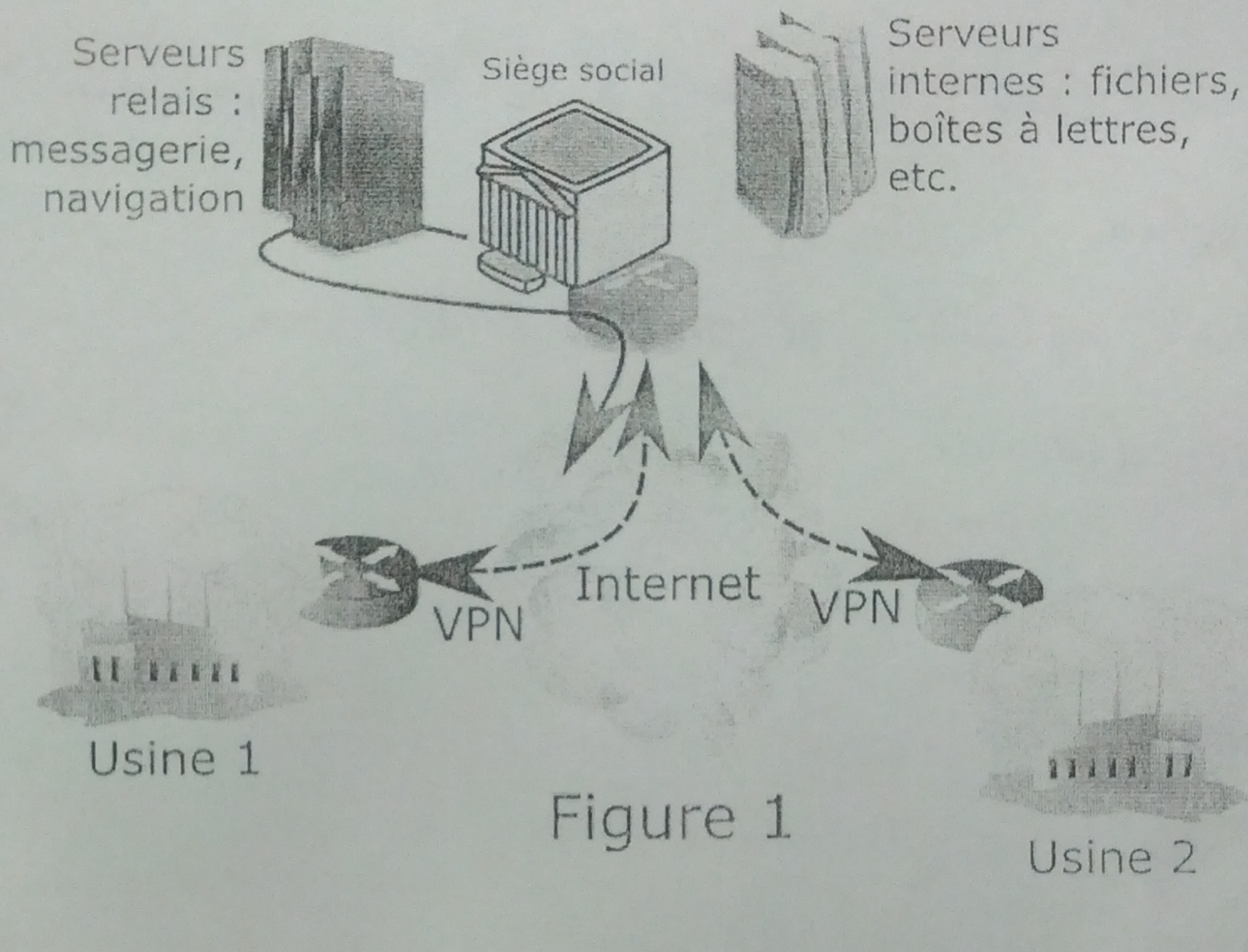

Figure 1

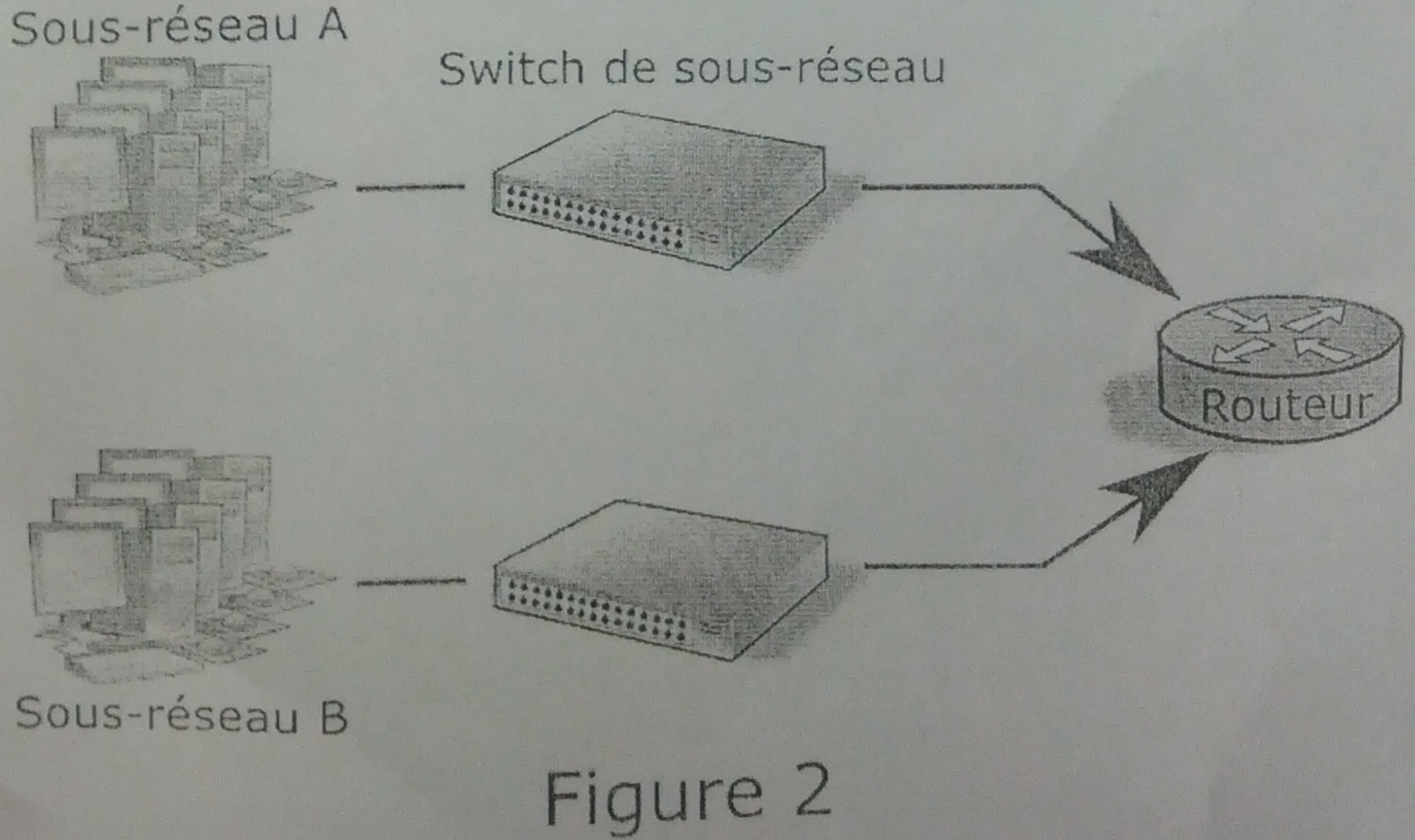

Figure 2