Sécurité des Systèmes d'Information

ALCASAR

Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau

PRÉSENTATION

Projet : ALCASAR	Auteur : Rexy with support of « ALCASAR Team »
Objet : Présentation de la solution	Version : 1.8
Mots clés : portail captif, contrôle d'accès, imputabilité, traçabilité, authentification	Date : Décembre 2009

Table des matières

1 - Introduction

ALCASAR est un portail d'accès Internet libre et gratuit. Il authentifie, contrôle, impute et protège les accès des usagers situés sur un réseau de consultation Internet. En France, ALCASAR permet aux responsables d'un réseau de consultation de répondre aux obligations légales (cf. annexe). ALCASAR s'appuie sur une quinzaine de logiciels libres afin de constituer **un portail captif authentifiant et sécurisé**. Au delà de cet aspect, Alcasar est utilisé par plusieurs centres de formation en tant que démonstrateur de techniques liées à la sécurité des réseau.

Le projet ALCASAR a été initié en 2008 par Richard REY, Franck BOUIJOUX, Pascal LEVANT. Il est indépendant et libre (GPLV3). Il est suivi actuellement par une équipe élargie dont les membres les plus actifs sont Stéphane WEBER, Thierry PELE, Sylvie AUGIZEAU, Stéphane REY, Pascal ROMERO, David Quesada et Fabrice SAVONNI.

Nous remercions tout particulièrement les usagers d'ALCASAR pour le retour d'expérience apporté ainsi que pour les bonnes idées d'évolution qui ne cessent d'alimenter notre imagination (et nos soirées ;-)).

Le site principal d'ALCASAR est situé à l'adresse : www.alcasar.info

Le forum et le suivi du projet sont hébergés sur la plate-forme « ADULLACT » de développement coopératif au service des collectivités, des services de santé, de l'éducation nationale, des associations, de l'état et des services publics : adullact.net/projects/alcasar

Ce document de présentation générale est accompagné des trois documents suivants :

- installation (alcasar-installation)
- exploitation (alcasar-exploitation)
- documentation technique (alcasar-technique -- en cours de finalisation)

2 - Objectifs

2.1 - Authentifier et contrôler les connexions

Alcacar est positionné en coupure entre le réseau de consultation et Internet afin d'en interdire l'accès pour les usagers non authentifiés (identifiant + mot de passe). Il se comporte comme un sas d'accès pour l'ensemble des services Internet.

Le contrôle des connexions implémenté dans ALCASAR permet, par exemple, de définir des usagers et des groupes d'usagers autorisés à se connecter. Pour chaque usager ou groupe d'usagers, il est possible de définir des dates de fin de validité de compte, des créneaux de connexion hebdomadaire ainsi que des durées maximales de connexion par session, journée ou mois. Pour gérer les usagers, ALCASAR s'appuie sur une base interne qui peut être couplée à un annuaire externe de type LDAP ou A.D.

2.2 - Tracer et imputer tout en protégeant la vie privée

ALCASAR permet aux responsables d'organismes de répondre aux exigences des politiques d'accès et d'utilisation des réseaux de consultation Internet. En France, il permet de décliner l'obligation légale de tracer et d'imputer[1] les connexions. Les extraits de la loi française relatifs à cette obligation sont présentés en annexe.

Ces exigences consistent à authentifier les usagers du réseau de consultation désirant utiliser Internet et à produire, pour chacun d'eux, une trace précise de toutes les activités réalisées (consultation, téléchargement, écoute multimédia, courriel, discussion, blog, etc.). ALCASAR produit ces traces sous forme de fichiers pouvant être aisément archivés sur supports externes afin d'être exploitées dans le cadre d'une enquête judiciaire. Dans le cadre de la cybersurveillance[2] et pour répondre aux exigences de la CNIL (cf. annexe), la production de ces traces est associée aux mécanismes suivants afin d'en assurer la non-répudiation et afin de garantir la protection de la vie privée :

- les flux liés à l'authentification des usagers sont chiffrés. Les mots de passe des usagers sont stockés chiffrés dans la base. Les fichiers de trace peuvent être chiffrés. Ces précautions permettent de prévenir l'accusation d'un autre usager ou d'un administrateur d'avoir récupéré, exploité ou modifié des données ;
- la consultation directe des activités Internet nominatives est impossible. En effet, les traces des connexions sont volontairement « éclatées » dans plusieurs fichiers dont les domaines sont séparés (authentifications d'un côté et activités Internet de l'autre). L'imputation des connexions n'est ainsi rendue possible qu'après un travail d'agrégat sur ces fichiers. Ce traveil est réservé aux autorités judiciaires. L'interface graphique de gestion d'ALCASAR ne présente aucune donnée nominative liée aux activités réalisées sur Internet ;
- la protection contre les « oublis » de déconnexion est prise en compte. ALCASAR déconnecte automatiquement les usagers dont l'équipement de consultation ne répond plus (arrêt de système, pannes réseau, etc.). En outre, un module externe permet de déconnecter automatiquement l'usager à la fermeture de sa session.

2.3 - Sécuriser

2.3.1 - le réseau de consultation

ALCASAR intègre un pare-feu spécifiquement paramétré afin de protéger les équipements du réseau de consultation des menaces externes directes. De plus, un module spécifique a été mis en place afin de protéger les usagers authentifiés des tentatives d'un pirate interne cherchant à usurper leurs sessions.

1 Contrairement aux idées reçues, la seule constitution des fichiers de connexion sur des équipements de consultation ne suffit pas à imputer une activité à un usager. L'imputabilité doit permettre de répondre par exemple à la question suivante : quel personnel identifié sous tel identifiant a écrit dans tel groupe de discussion via tel protocole à telle heure et tel jour à partir de tel équipement ?

2 cf. article d'Olivier ITEANU (avocat spécialisé en informatique) « cybersurveillance des salariés en entreprise » publié dans PC-Expert de juin 2008 (P30).

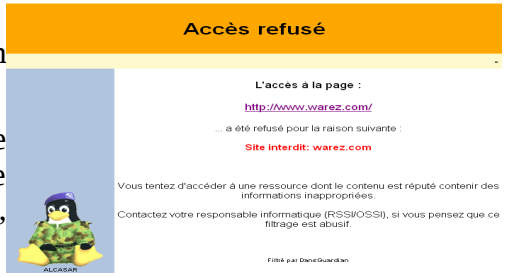
Les mises à jour de sécurité des équipements de consultation (antivirus et rustines/patch) sont rendues possibles et automatisables à travers la déclaration d'une liste de sites pouvant être contactés directement sans authentification préalable.

2.3.2 - le portail

La sécurité du portail a été élaborée comme pour un système bastion devant résister à différents types de menaces :

- utilisation et sécurisation d'un système d'exploitation récent et minimaliste (Mandriva Linux LSB) ;
- protection du portail vis-à-vis d'une attaque interne (durcissement et anticontournement) ;
- les logiciels choisis sont reconnus par la communauté comme des valeurs sûres et éprouvées ;
- possibilité d'effectuer une image complète et « à chaud » du système sur CDROM. Cela permet de le réinstaller rapidement en cas de panne matérielle ;
- concernant l'accès à l'interface de gestion, les précautions suivantes ont été prises en compte : chiffrement des trames, authentification et comptabilité des accès, séparation entre les fonctions d'archivage, de gestion des usagers et d'administration (au moyen de profiles d'administrateurs).

2.3.3 - les usagers



Afin de protéger les usagers authentifiés, ALCASAR met en oeuvre deux dispositifs optionnels de filtrage :

- le premier permet de bloquer l'accès aux sites WEB dont le contenu est jugé répréhensible ou non-conforme (liste noire). Il est entièrement paramétrable (activation, désactivation, ajout ou retrait de site, etc.) ;
- le deuxième permet de bloquer tout trafic autre que le trafic WEB et de n'activer que les services réseau désirés (Web sécurisé « HTTPS », courriel « SMTP/POP », etc.).

Ces deux dispositifs sont optionnels. Ils ont surtout été élaborés pour les organismes susceptibles d'accueillir un jeune public.

3 - Solution proposée

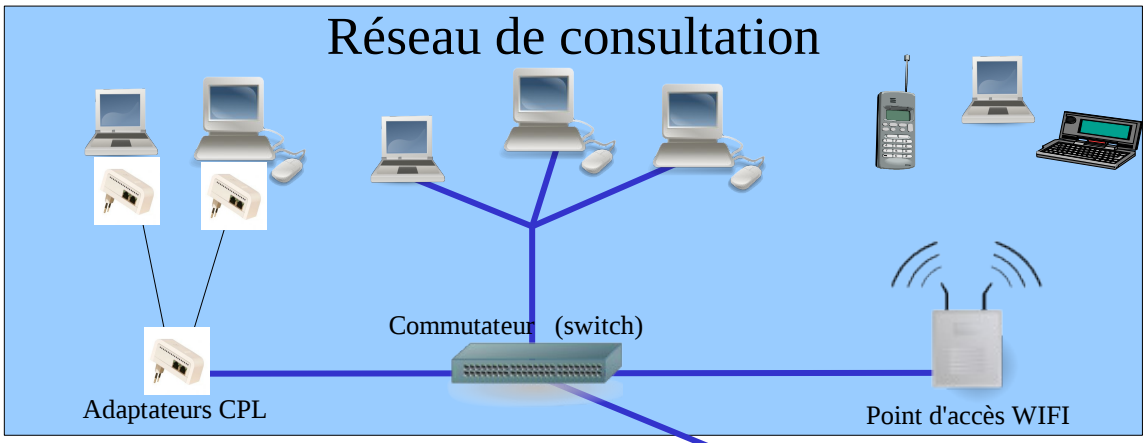
Afin d'être le plus universel possible, ALCASAR n'exploite que des technologies standardisées lui permettant d'être compatible avec tous les réseaux de consultation (LAN filaire, LAN WIFI, LAN CPL, etc.). Ces derniers peuvent intégrer tout type d'équipements (PC fixes, PC portables, assistants personnels, smartphone WIFI, etc.) exploitant tout type de systèmes (Windows, Unix, Linux, Palm-OS, Blackberry, Symbian OS, etc.).

Les équipements du réseau de consultation n'ont pas besoin de logiciel complémentaire pour fonctionner avec ALCASAR.

Le système d'exploitation et les logiciels utilisés par ALCASAR sont protégés par des licences libres ; les développements réalisés spécifiquement se trouvent eux-mêmes sous licence libre.

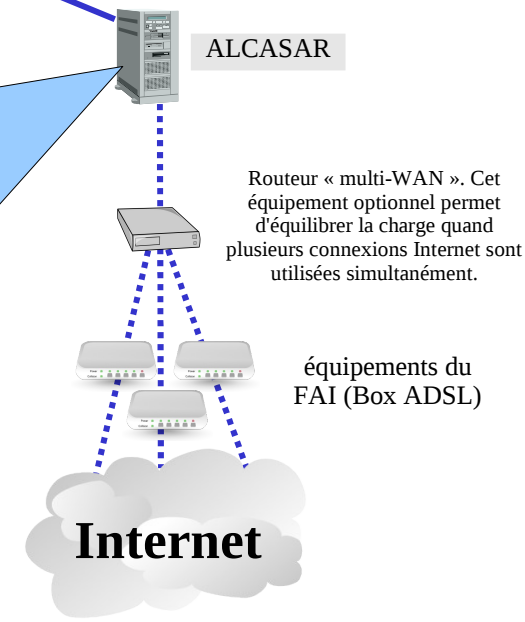
Une procédure d'installation unifiée et automatisée a été élaborée afin de permettre un déploiement rapide par du personnel ayant une connaissance sommaire des techniques utilisées. Toutes les fonctions techniques du portail ont été intégrées dans un seul équipement standard (PC de bureautique). Un centre de gestion sécurisé et graphique permet aux administrateurs ainsi qu'aux OSSI/RSSI d'exploiter simplement les fonctions de leur domaine de responsabilité (archivage, gestion des usagers, visualisation des journaux, définition des sites filtrés, etc.). Lors de la mise en place d'une nouvelle version, une procédure de mise à jour permet de conserver les anciens paramètres du portail.

ALCASAR est totalement indépendant des équipements fournis par le prestataire de service Internet (FAI). Il est bâti autour d'une quinzaine d'éléments constituants ainsi un portail captif authentifiant complet positionné en coupure entre Internet et le réseau de consultation.



Constituant d'Alcasar

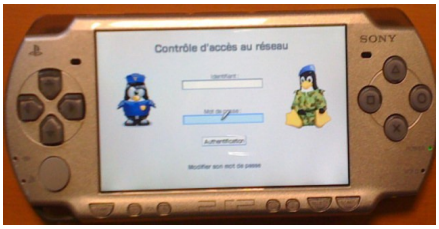
- Un seul PC de type « bureautique » possédant deux cartes réseau
- Système d'exploitation Linux
- Passerelle d'interception
- Serveur DHCP principal et secondaire (ou de secours)
- Serveur Web dédié à l'administration
- Serveur d'authentification
- Serveur de base de données (base des usagers et des groupes)
- Serveur mandataire (proxy)
- Serveur de temps
- Routeur / Parefeu
- Processeur de journalisation
- Processus de clonage à chaud du système
- Système de filtrage de flux et de contenu
- Serveur de connexions distantes sécurisées
- Scripts de déploiement, de mise à jour et de gestion
- Interface graphique d'administration sécurisé :
    - gestion des usagers et des groupes d'usagers
    - gestion du système de filtrage de flux et de contenu
    - archivage des fichiers journaux
    - rapport de statistiques de connexion et de consultation
    - rapport temps réel des journaux du parefeu
    - rapport temps réel d'information système
    - rapport temps réel de l'activité du réseau de consultation



4 - Exploitation

4.1 - pour l'usager

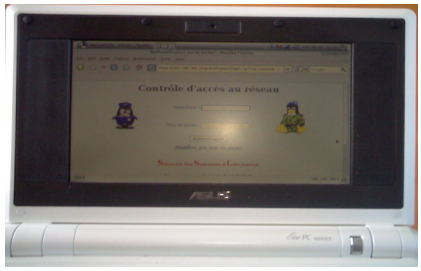
- L'usager peut utiliser n'importe quel équipement connecté sur le réseau de consultation. Au lancement d'un navigateur WEB, une page d'authentification lui est présentée. Cette page contient une information l'informant des fonctions principales du portail. Elle lui permet aussi de modifier son mot de passe :



sur une PSP

sur un assistant « Palm tungsten »

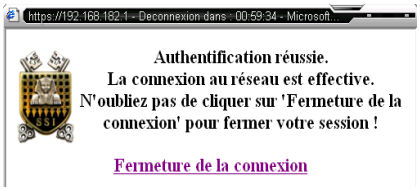
sur un « Iphone »



Sur un EeePC (Linux-ubuntu)

- Une fois l'authentification effectuée, le navigateur affiche la première page de consultation ainsi

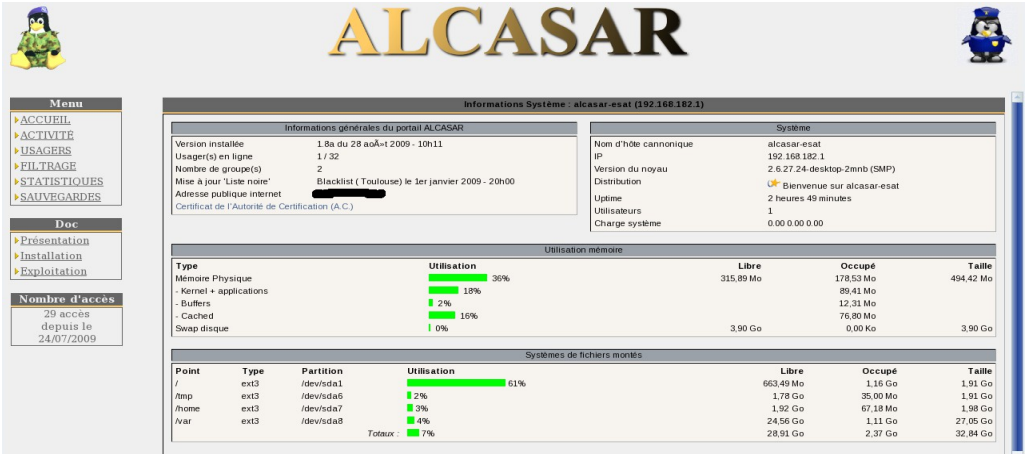
qu'une fenêtre supplémentaire permettant de se déconnecter.



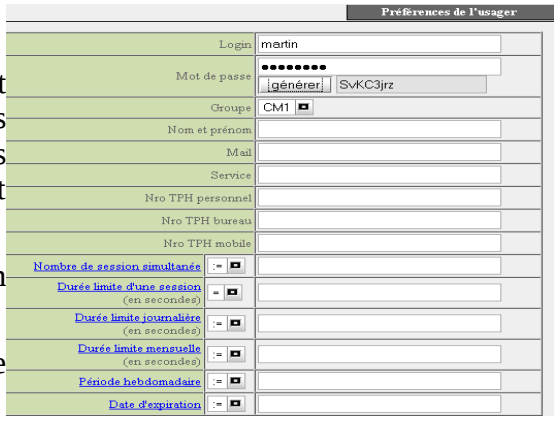
- En fonction de la configuration des postes de consultation, toutes les applications et tous les protocoles réseau sont alors disponibles pour l'usager (ftp, courrier électronique, discussion, P2P, blog, etc.).
- Il est possible d'intégrer dans les marque-pages des navigateurs deux liens permettant de se déconnecter ou de changer son mot de passe.

4.2 - pour les administrateurs

Il est possible, à partir de n'importe quel équipement de consultation, d'accéder de manière authentifiée et chiffrée à l'interface graphique de gestion du portail[3] :



À titre d'exemple, ce centre de gestion permet :

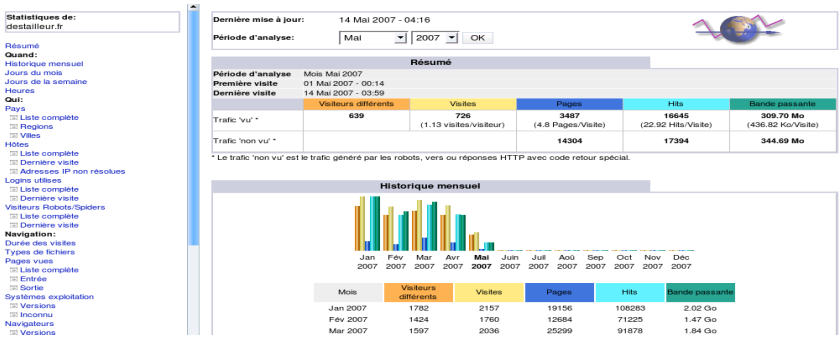


• de gérer les usagers : création, suppression et import d'usagers ou de groupe d'usagers. Modification de leurs attributs (date d'expiration, périodes de connexions autorisées, durées de connexion par session, par journée et par mois, etc.) ;

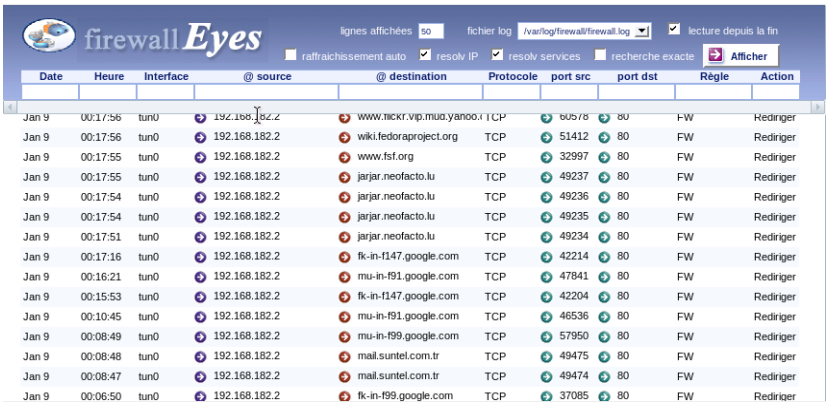
• de modifier le comportement du portail (connexion sur un serveur d'annuaire, configuration du filtrage réseau, etc.) ;

• de consulter les statistiques d'exploitation du réseau de consultation et de la bande passante :

3 Le document « alcasar-exploitation » décrit les possibilités de ce centre de gestion.

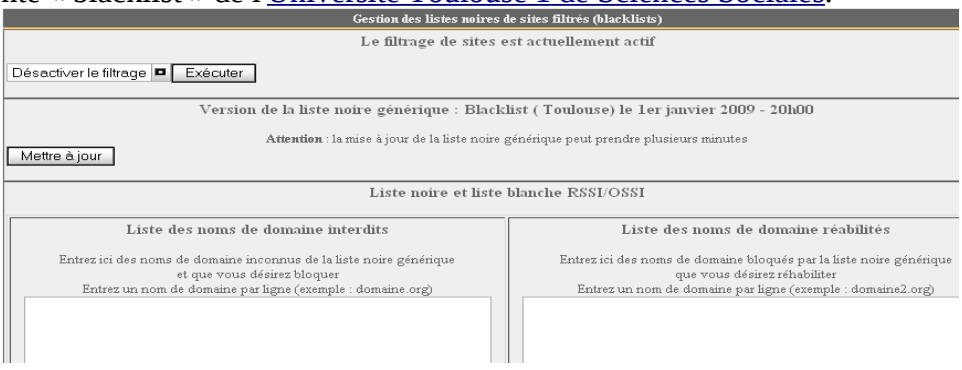


• de consulter les évènements du pare-feu :



• de récupérer pour archivage les fichiers journaux. Ces fichiers contiennent les traces de toutes les connexions, de tous les protocoles et de toutes les adresses consultées. Ils constituent ainsi les preuves de l'activité du réseau de consultation. Ces fichiers peuvent être chiffrés ;

• d'activer, de désactiver, de modifier ou de mettre à jour les listes des sites filtrés (blacklists). ALCASAR intègre l'excellente « blacklist » de l'Université Toulouse 1 de Sciences Sociales.



5 - Annexe - Réglementation française

décret nº 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques - Article 10-13

I- En application du II de l'article L.34-1, les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :
a) les informations permettant d'identifier l'utilisateur,
b) les données relatives aux équipements terminaux de communication utilisés,
c) les caractéristiques techniques, ainsi que la date, l'horaire et la durée de chaque communication,
d) les données relatives aux services complémentaires demandés ou utilisés et leur fournisseur,
e) les données permettant d'identifier le ou les destinataires de la communication.
...
III- La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

NOTA 1 : Une directive européenne est en préparation concernant l'augmentation de la durée de conservation des données de connexion. Suite aux attentats de Londres, 6 chefs d'État de l'UE ont proposé que le conseil européen porte cette durée à trois ans.

NOTA 2 : Selon l'article 10-14 de ce même décret, l'opérateur peut exploiter pendant 3 mois les traces des connexions (exclusivement dans le cadre de la sécurité des réseaux).

NOTA 3 : En France, l'opérateur est responsable de la traçabilité et de l'imputabilité des connexions au niveau de l'adresse publique fournie par contrat. Si un réseau de consultation est déployé à partir de cette adresse, le responsable de ce réseau doit mettre en oeuvre son système de traçabilité et d'imputabilité afin de dégager sa propre responsabilité (cf. ci-dessous).

La loi du 23 janvier 2006 sur la lutte contre le terrorisme

Cette loi précise que sont concernées par cette obligation de traçabilité, « les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit » (CPCE, art. L. 34-1, I, al. 2). Tout manquement à cette obligation expose à une peine de prison d'un an et à 75000 euros d'amende, le quintuple pour les personnes morales.

CNIL

La Cnil et les tribunaux considèrent la cybersurveillance légale quand les trois conditions suivantes sont remplies :

- L'existence de la cybersurveillance doit d'abord avoir été portée à la connaissance des salariés, soit par voie d'affichage soit par note de service. ALCASAR fournit automatiquement cette information sur la page d'authentification lors de chaque connexion ;
- Les représentants du personnel doivent avoir été consultés (pour simple avis) ;
- Elle doit être justifiée (proportionnalité) et limitée à une surveillance de flux (volume de trafic, type de fichiers échangés, filtrage url, etc.) sans accéder aux contenus des courriers électroniques ni aux répertoires identifiés comme « personnel » sur le disque dur du poste de travail du salarié sous peine d'être poursuivi pour violation de correspondance privée. Les traces enregistrées par ALCASAR correspondent à cette exigence.