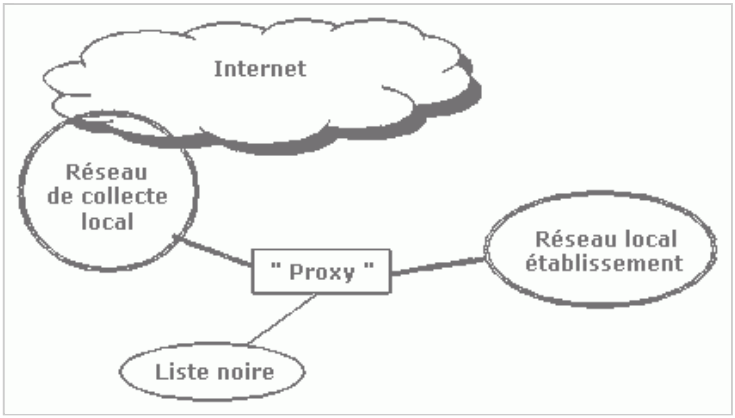
Guide des préconisations techniques pour la protection des mineurs

Architectures proposées et solutions logicielles

Filtrer les contenus avec un serveur mandataire dans un établissement scolaire.

Solution au niveau du serveur mandataire (adaptée à une architecture multiposte ou mutualisée)

Architecture type



Le serveur mandataire est le passage obligé de toute connexion. Il n'y a donc pas de contournement possible, toutes les pages et tous les contenus seront analysés par le dispositif.

Serveurs mandataires disponibles avec dispositif de filtrage intégré

Parmi les serveurs mandataires disponibles, aussi bien dans le domaine du logiciel commercial que dans le domaine du logiciel libre, certains proposent des fonctionnalités de filtrage.

Ces serveurs mandataires permettent d'interdire l'accès à certaines pages web, en redirigeant les requêtes vers une page déterminée. Ils permettent donc de réaliser un contrôle a priori des informations consultées. Ces serveurs sont aussi utilisables pour réaliser le contrôle a posteriori : à partir d'une liste de sites inappropriés, ils permettent d'enregistrer tous les accès à ces sites associés à une identification.

Le logiciel Squidguard

Ce logiciel libre est intégré dans plusieurs projets soutenus par l'éducation nationale : EOLE, SLIS, pingoo, linuxedu, etc. Il s'agit d'un greffon (« plugin ») destiné à Squid qui est un serveur mandataire libre très utilisé. Ce greffon apporte les fonctionnalités de filtrage.

Il permet entre autre fonctionnalités de :

- bloquer l'accès à un ensemble de sites définis par une liste noire pour certaines catégories d'utilisateurs
- rediriger un accès à une page interdite vers une autre page
- limiter l'accès à l'Internet dans le temps en définissant des plages horaires d'accès selon les profils
- autoriser l'accès à un nombre limité de pages web en proposant des fonctionnalités de type liste blanche

Le serveur mandataire Squid permet l'authentification de l'utilisateur.

De plus amples renseignements techniques sont disponibles sur le **site de Fabrice Prigent** à l'Université de Toulouse 1, ou sur le site du logiciel **www.squidguard.org** (en anglais).

Le logiciel Dansguardian

Dansguardian est un logiciel disponible sous une licence libre pour toute utilisation non commerciale.

Il s'agit d'un greffon pour le serveur mandataire Squid, qui apporte des fonctions de filtrage multiples.

En complément des fonctionnalités de SquidGuard et de Squid, il permet de :

- examiner le contenu des pages pour détecter les contenus inappropriés, en analysant les structures de phrases, des éléments de pagination et le vocabulaire type utilisé.
- limiter la quantité de données transmise du réseau interne de l'école vers le serveur de la page web, par exemple pour limiter l'utilisation de pièces jointes dans les courriers électroniques.
  Dansguardian utilise le même format de données que Squidguard pour définir les listes noires. Ces deux logiciels peuvent donc avoir une liste noire commune. Cependant, Dansguardian n'est pas directement intégré dans les projets nationaux.

Les logiciels commerciaux

Des logiciels commerciaux proposant les mêmes types de fonctionnalités sont disponibles. Voici une liste non exhaustive :

- CheckPoint
- Olfeo (**www.olfeo.com**)
- WebSense (**www.websense.com**)

Les listes disponibles

Les listes noires permettent de définir un ensemble de sites interdits par l'intermédiaire de domaines interdits, d'URL interdites, de fichiers interdits et de motifs généraux dans les adresses internet. On peut par exemple imaginer que dans ces listes noires seront présentes les adresses de sites pornographiques, de sites racistes, etc. Ces listes noires peuvent aussi fournir des motifs génériques indiquant des sites à proscrire : par exemple, on peut interdire les fichiers de jeux, des fichiers exécutables, etc.

Différents niveaux de listes noires sont à prévoir, afin de pouvoir adapter le filtrage aux situations pédagogiques :

Les sites illégaux ne pourront pas être consultés, quel que soit le profil de l'utilisateur ou la situation pédagogique. Les sites inappropriés sont définis relativement à une tranche d'âge, une situation pédagogique, un profil d'utilisateurs, etc.

Les listes noires permettent de créer un Internet où tout est autorisé sauf la consultation de quelques sites. On garde donc la possibilité de naviguer librement d'un site à un autre, tout en restreignant les risques d'accéder à un site inapproprié. La spécificité de l'Internet reste conservée. Cependant, une liste noire ne peut jamais être exhaustive : le nombre de sites disponibles sur l'Internet augmente de jour en jour, il n'est pas possible de prendre en compte la totalité des sites. Une liste noire répertorie un maximum de sites, et non la totalité. La participation de chacun, par l'intermédiaire de la remontée d'informations, permet de compléter cette liste et d'augmenter les performances des listes noires.

Les listes blanches permettent d'autoriser des sites. Ce type de liste peut être utile dans le cadre d'un travail en autonomie complète, sans contrôle de l'enseignant. Dans ce cas la recherche d'informations se rapproche d'une recherche dans une documentation.

Une liste « noire » est téléchargeable sur demande au **CTICE** de l'académie. Cette liste est une liste au format texte pur, adaptable facilement à un ensemble de format, dont le format des listes SquidGuard. Les procédures d'utilisation sont détaillées dans cette rubrique. Des procédures automatisées de mise à jour des listes sont mises en place afin de pouvoir prendre en compte rapidement les ajouts et suppressions proposés par les équipes locales.

Installation et configuration

Le logiciel Squidguard est intégré dans les solutions suivantes :

- SLIS (**slis.ac-grenoble.fr**)
- EOLE (**eole.orion.education.fr/**)
- Pingoo (**www.pingoo.org**)
- AbulEdu (**www.abuledu.org**).

Des instructions d'installation sont disponibles sur les sites de chacun de ces projets. En particulier, ces projets permettent d'automatiser la mise à jour de la liste « noire » utilisée. On est alors sûr d'utiliser la dernière version de la liste noire disponible.

Annuaire et identification

Les projets globaux SLIS, EOLE, Pingoo proposent la gestion de comptes utilisateurs par l'intermédiaire d'un annuaire LDAP. Ce dernier est installé automatiquement, à partir de la base de données de l'établissement, et permet d'assurer l'identification de l'utilisateur lors de la navigation sur l'Internet par l'intermédiaire du serveur mandataire.

Cette identification de l'utilisateur peut être conservée dans les traces relatives aux connexions.

Informations à conserver

Afin de pouvoir gérer d'éventuels incidents et de pouvoir perfectionner les listes noires disponibles, il est indispensable de conserver les informations de connexions (« logs ») des usagers.

La durée de conservation doit être suffisante pour permettre de traiter un incident découvert tardivement (cette durée est actuellement de 1 an). La conservation de ces informations peut être réalisée de différentes manières : une conservation locale ou une conservation extérieure à l'établissement.

Les traces devront être analysées régulièrement, afin de garantir l'efficacité du dispositif de filtrage. Les informations extraites de ces fichiers, par exemple lors d'incident ou d'accès à des contenus inappropriés seront transmises, via la chaîne de remontée des incidents, au RSSI qui est le référent unique en matière de sécurité et de filtrage au niveau académique.

Les traces pourront être analysées à l'aide de programmes de type scripts, afin de systématiser et d'améliorer l'efficacité de cette analyse. Des scripts d'analyse peuvent par exemple être trouvés sur la page http://cri.univ-tlse1.fr/documentations/cache/squidguard.html, afin de détecter les pages inappropriées non filtrées par la liste noire.

Solution sur le poste client (adaptée à une architecture mono-poste)

Les petites structures, en particulier les petites écoles ne possèdent parfois qu'un seul poste relié directement à l'Internet, sans réseau local interne à l'école ou à l'établissement.

Dans ce cas précis, la solution du serveur mandataire n'est peut-être pas la mieux adaptée, notamment pour des raisons de moyens. L'utilisation d'un logiciel de filtrage sur le poste client, au niveau du poste unique, semble plus pertinente, bien que moins performante :

- des sites illégaux
- des sites inappropriés
- autres sites

Mis à jour le 31 octobre 2012

Partager cet article