Gestion du filtrage à l'aide de l'interface EAD2

Introduction

Le pare-feu AMON vous permet d'organiser le filtrage de la navigation web et des accès réseau de la zone pédagogique de votre établissement.
Pour vous faciliter la gestion de ce filtrage, vous avez à disposition une interface web nommée « EAD2 ».
Il faudra vous y authentifier avec le compte « amon2 » et le mot de passe personnalisé diffusés aux établissements.

I. L'authentification

Afin de vous connecter, il vous faudra ouvrir un navigateur comme « Firefox » ou « Internet Explorer » et entrer l'URL composée de la manière suivante : https://10.dept.etab.1:4200
Ensuite, il vous faudra choisir « Authentification Locale », puis le « - Serveur Axxxxxxx(Arne sans le 0)».
Saisissez le « login » « amon2 » et le mot de passe vous ayant été fourni.
Vous observerez le message suivant :« VOUS ÊTES CONNECTÉ(E) EN TANT QUE ADMIN_PEDAGO »

II. Le filtrage

Nous allons d'abord décrire les différentes rubriques présentes dans la « configuration 2 ».

Dans la fenêtre (comme illustré ci-dessus), nous observons les rubriques suivantes :

- Groupe de machine

Permet l'organisation du filtrage par groupe de postes se trouvant dans le réseau pédagogique de l'établissement

- Postes

Permet d'interdire la navigation réseau ou seulement web vers et/ou depuis des machines ou un ensemble de machines

- Visites des sites

Permet d'obtenir des logs sur les sites web visités à partir d'une ip ou d'un utilisateur authentifié.

- Sites

Permet de paramétrer le filtrage des sites web.

- Règles du pare-feu

Permet de configurer le pare-feu en activant des règles globales pour la zone pédagogique

Rectorat de Créteil
Division Informatique
Infrastructures EPLE et Ecoles
09/06/2009

1. Les filtres

Pour mettre en place un filtrage basique, il vous faut configurer la page « Filtres » se trouvant sous « Configuration 2 », puis « Sites ».

Vous observerez les 4 colonnes suivantes :

Colonne 1 : Les différents « Filtres » proposés, qui pour chaque thème correspond une liste de sites maintenues par l'université de Toulouse et pour plus d'informations, nous vous invitons à visiter leur site par ce lien : http://cri.univ-tlse1.fr/blacklists/
Colonne 2 : La politique de filtrage « Défaut », elle s'applique de base pour toutes les machines n'appartenant pas à un groupe.
Colonne 3 et 4 : Les politiques de filtrage « 1 » et « 2 » s'ajoutent à la « Défaut » et sont utilisables pour des groupes de machines
Pour un filtrage basique, dans la colonne « Défaut », cochez simplement les thèmes qui vous semble être interdits d'accès dans votre établissement.

2. Le filtrage syntaxique

Il analyse le contenu des pages sur la base d'une liste de mots interdits. Vous avez les choix suivants :

- de ne pas activer cette analyse
- de ne l'effectuer que sur les entêtes de pages WEB (recommandé)
- de l'effectuer sur la totalité de la page

3. Sites interdits et Sites autorisés

Vous pouvez interdire ou autorisé des sites, même les inscrits dans la liste noire de Toulouse, en tapant l'url dans la zone de saisie et en cochant la politique optionnelle « Défaut ».

4. Extensions

Vous pouvez interdire des extensions de fichiers qui vous semblent dangereuse à télécharger.

5. Type MIME

Un Type MIME est un identifiant de format de données sur internet en deux parties, vous pouvez obtenir des précisions sur le site suivant : http://fr.wikipedia.org/wiki/Type_MIME
Vous pouvez choisir les Type MIME que vous souhaitez interdire.

6. Sites du mode liste blanche

Vous pouvez alimenter une liste exhaustive de sites que vous souhaitez autoriser, le reste des sites web d'internet ne se seront plus accessibles. Cette liste s'utilisera en l'affectant à un groupe de machine.

7. Postes

a. Destinations interdites

Pour interdire la navigation réseau à destination d'adresses Ip internet, hors navigation web (http seulement), il suffit de taper l'adresse IP dans la zone prévue à cet effet.
Exemple :
Syntaxe pour l'adresse Ip d'une machine internet : 69.63.186.30
Syntaxe pour un ensemble du réseau dans lequel se trouve se serveur : 69.63.186.0/24

b. Postes

Pour interdire la navigation web ou réseau d'une machine ou d'un ensemble de machines sur une plage horaire choisie dans la semaine, il suffit de taper l'adresse IP du poste dans la zone prévue à cet effet.

Exemple :
Syntaxe pour 1 poste du réseau pédagogique : 172.16.5.1
Syntaxe pour un ensemble de postes de ce réseau : 172.16.5.0/24

8. Règles du pare-feu

Vous pouvez activer les règles suivantes :

- Interdire l'utilisation des dialogues en direct
  Permet de bloquer les Icq, Yahoo Messenger, MSN, ...
- Interdiction des protocoles de messagerie
  Permet de bloquer les réception de type POP, IMAP et les envois du type SMTP
- Interdiction des forums
- Interdire les connexions FTP
  Permet de bloquer les transferts de fichiers
- Internet restreint
  Permet de bloquer toute la navigation web sauf par le proxy

9. Groupe de machines

a. Présentation

Le pare-feu Amon propose de gérer des groupes de machine par plage d'adresse Ip.

Lors de la création, remplissez un nom pour le groupe de machine (sans accents, ni caractères spéciaux), puis donnez l'Ip de début de plage et Ip de fin de plage, puis choisissez l'interface à laquelle correspondent les ips.

Remarque :
Si il ne vous est pas possible de choisir l'interface de votre groupe lors de sa création, c'est qu'une seule interface du pare-feu est associé à cette zone.
La plage d'adresse du groupe doit être de classe C.
Un trop grand nombre d'ip dans un groupe peut emmener une baisse de performance.

Pour un groupe construit, il est possible de lui appliquer les conditions suivantes:

- De lui interdire l'accès au réseau, ou la navigation web seulement en permanence ou selon des horaires
- De lui associer une politique optionnelle de filtrage web spécifique (défaut, 1 ou 2)

Dans la colonne Interdictions, il est possible de choisir parmi :

- Jamais
- Le web tout le temps (Le groupe de machine est alors interdit d'accès sur les ports : 80« http », 443« https », 3128« dansguardian », 8080« squid »)
- Le web selon des horaires (définir les horaires au préalable)
- Toute activité réseau

Remarque
Sans plage horaire définie au préalable, la navigation web est interdite tout le temps
La modification des plages horaires est dynamique, ainsi si le groupe de machine est interdit de navigation web selon horaires, il est possible de modifier les plages horaires.
Il est aussi possible de copier les horaires depuis un autre groupe de machine.

Le filtrage web permet de spécifier des politiques de filtrages.

Certaines de ces politiques sont fixes (modérateur, interdits, liste blanche), d'autres sont configurables (Défaut, 1 et 2)

b. Exemples

Soit des postes pour la salle des professeurs et le C.D.I. pour lesquels nous désirons créer des groupes :
5 postes pour les professeurs : une plage d'adresse Ip 172.16.5.1 à 172.16.5.5, jamais d'interdictions et la politique de filtrage 1.
10 postes pour le CDI : une plage d'adresse Ip 172.16.10.1 à 172.16.10.10, une interdiction web selon horaires (8h à 13h et 14h à 17h) et la politique de filtrage 2

i. Création des groupes

Choisissez « Groupe de machine », puis « Nouveau groupe de machine ».

Un formulaire de création apparaît :

- Remplissez un nom pour le groupe de machine (sans accents, ni caractères spéciaux), nous choisirons « cdi »
- Donnez l'Ip de début de plage, « 172.16.10.1 »
- Donnez l'Ip de fin de plage, « 172.16.10.10 »
- Choisissez l'interface à laquelle correspondent les ips
- *Validez*

ii. Configuration des horaires

Cliquez sur l'horloge, la gestion des horaires apparaît:

- Choisissez le début et la fin de la plage horaire d'autorisation
- Choisissez les jours d'applications
- Validez

iii. Configuration des interdictions

Cliquez sur le menu déroulant de « interdictions », la liste des interdictions apparaît:

- Choisissez « Le web selon horaires » (l'activation est dynamique)

iv. Configuration des politiques optionnelles

Cliquez sur le menu déroulant de « politique optionnelle », la liste des politiques apparaît:

- Choisissez « 2 » (l'activation est dynamique)

Idem pour la salle des professeurs.

III. Signalement

L'écran se trouvant sous Outils, puis Signalement, vous permet de signaler un site à ajouter ou à supprimer de la liste noire nationale (faux positif).
Vous disposez également d'un lien vers le site Éducnet concernant la navigation internet en cliquant sur « Plus d'information ».