

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

Caractéristiques du document	
Objet :	Filtrage EAD2
Référence :	Document1
Auteur :	Philippe FERREIRA+Loïc VIOT
Diffusion :	Tous les utilisateurs
N° de version :	1
Date :	13/02/2014
Nombre de page :	16

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.

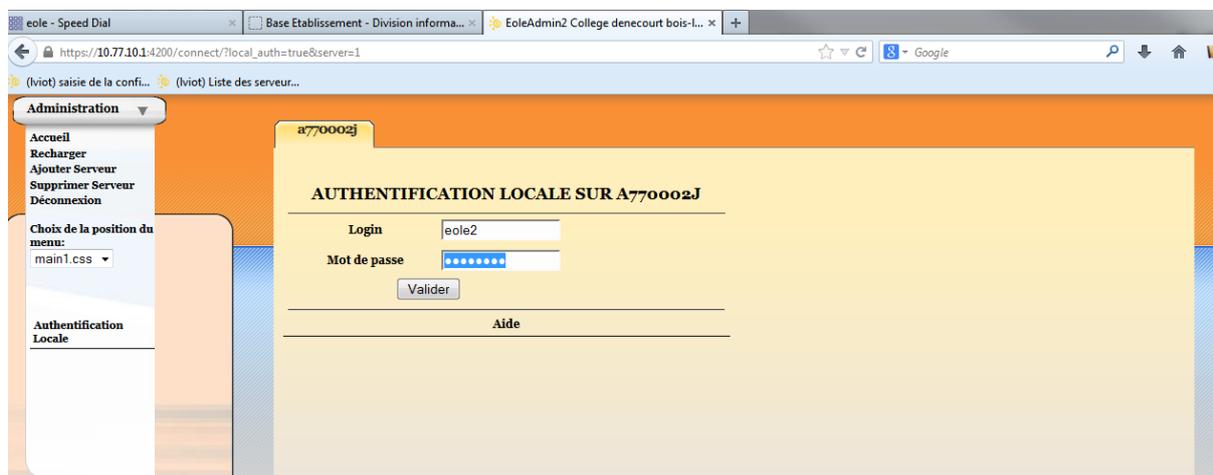
Pour vous faciliter la gestion de ce filtrage, vous avez à disposition une interface web nommée « EAD2 ». Il faudra vous y authentifier avec le compte « eole2 » et le mot de passe personnalisé diffusé aux établissements.

1 L'authentification :

Afin de vous connecter, il vous faudra ouvrir un navigateur comme « Mozilla Firefox » ou « internet explorer » et entrer l'URL composée de la manière suivante : <https://10.dept.etab.1:4200>



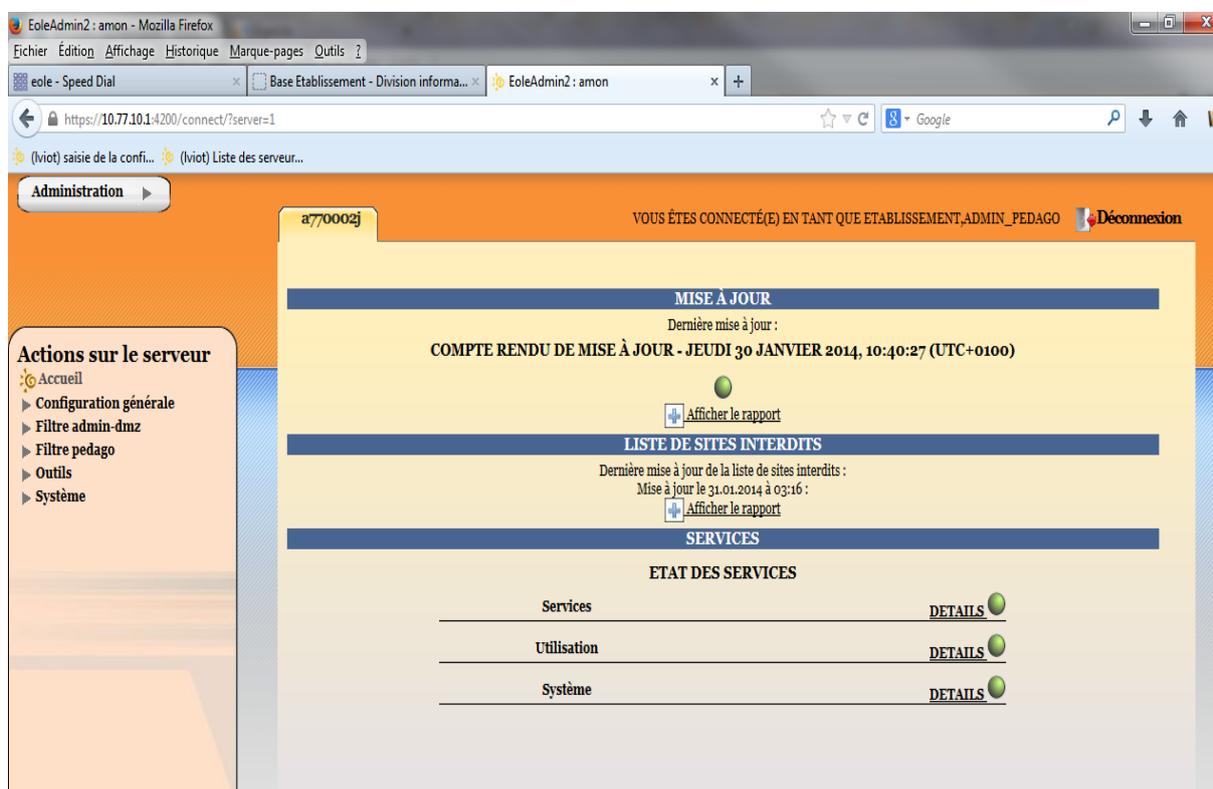
Ensuite il vous faudra choisir « authentification locale » puis cliquer sur le serveur amon en question.



Saisissez le « login » « eole2 » et le mot de passe vous ayant été fourni.

Vous observerez le message suivant :

VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO



2 Le filtrage admin-dmz/pedago

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

Dans la fenetre, nous observons les rubriques suivantes :

2.1 Groupes de machines

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

2.1.1 Présentation

Cliquer sur nouveau groupe de machine

The screenshot shows a web interface for configuring machine groups. At the top, there's a user session bar with the ID 'a770002j' and the text 'VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO'. Below this is a blue header 'GROUPE DE MACHINE' and a green '+ Nouveau groupe de machine' button. A section titled 'LISTE DES GROUPE DE MACHINE' contains a table with five columns: 'Groupes de machine', 'Horaires', 'Interdictions', 'Politique de filtrage', and 'Suppression'. Below the table is a 'CRÉATION DE GROUPE DE MACHINE' form with the following fields: 'nom du groupe', 'début de la plage d'ip', 'fin de la plage d'ip', and 'Interface de la plage' (a dropdown menu currently showing 'admin (eth1)'). A 'Valider' button with a green checkmark is at the bottom of the form.

Lors de la création, remplir un nom pour le groupe lors de sa création (sans accents, ni caracteres spéciaux) puis donner l'IP de debut de plage et l'IP de fin de plage, puis choisir l'interface à laquelle correspondent les IP.

Remarque :

S'il n'est pas possible de choisir l'interface de votre groupe lors de sa création, c'est qu'une seule interface de pare-feu est associée à cette zone. La plage d'adresse du groupe doit être de classe C. Un trop grand nombre d'IPS dans un groupe peut conduire à 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)

2.1.2 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 horaire (8h à 13h et 14h à 17h) et la politique de filtrage 2.

[2.1.2.1 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 fin de plage « 172.16.10.10 »
- Choisissez l'interface à laquelle correspondent les IP.
- Validez

[2.1.2.2 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

[2.1.2.3 Configuration des interdictions](#)

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

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

[2.1.2.4 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.

2.2 Sources et destinations :

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

2.2.1 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 ce serveur :69.63.186.0/24

The screenshot shows a web-based administration interface. At the top, there is a navigation bar with 'Administration' and a user status 'VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO' with a 'Déconnexion' link. The main content area is titled 'INTERDIRE DES DESTINATIONS (FILTRE ADMIN-DMZ)'. On the left, there is a sidebar menu under 'Actions sur le serveur' with options like 'Accueil', 'Configuration générale', 'Filtre admin-dmz', 'Groupe de machine', 'Sources et destinations', 'Visites des sites', 'Sites', 'Règles du pare-feu', 'Filtre pedago', 'Groupe de machine', 'Sources et destinations', 'Visites des sites', 'Sites', 'Règles du pare-feu', 'Outils', and 'Système'. The main area contains a form with a 'Destination à interdire' input field, an 'Interface associée à la source' dropdown menu (set to 'dmz-priv (eth3)'), and an 'Ajouter' button. Below the form, a message states 'Aucune destination n'a été interdite'.

2.2.2 Sources interdites

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

Administration

a770009s VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO Déconnexion

INTERDIRE DES SOURCES (FILTRE ADMIN-DMZ)

Source à interdire

Interface associée à l'adresse
dmz-priv (eth3)

Heure de début 7:00 Heure de fin 19:00

du lundi au dimanche

Niveau de restriction
 Seulement le web
 Toute activité réseau
 interdiction permanente

[✓ Ajouter]

Aucune adresse n'est interdite de web

Aucune adresse n'est interdite de réseau

2.3 Visites des sites

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

The screenshot displays a web interface for monitoring website visits. The page title is 'OBSERVATOIRE DES NAVIGATIONS SUR 'FILTRE PEDAGO'' and it is labeled as an 'OUTIL DE RECHERCHE'. The interface includes a sidebar menu with 'Visites des sites' selected, and a main content area with search filters. The search criteria section includes fields for 'Choix du (des) jour(s)', 'Visite du:' and 'Au:' (date range), 'Critères de recherche' (Hours of visit, IP of visitor, Login of visitor), and a checkbox for 'Seulement les accès refusés'. A 'par page de 10' dropdown and a 'Valider' button are also visible.

Administration ▶

a770009s VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO Déconnexion

OBSERVATOIRE DES NAVIGATIONS SUR 'FILTRE PEDAGO'

OUTIL DE RECHERCHE

Choix du (des) jour(s)

Visite du: Au:

Critères de recherche

Heures de visite Entre: Et:

Ip du visiteur Depuis l'Ip

Login du visiteur Par:

Seulement les accès refusés

par page de 10

[✓ Valider]

2.4 Sites :

Permet de paramétrer le filtrage des sites web.

2.4.1 Les listes

Pour mettre en place un filtrage basique, il vous faut configurer la page « filtres » se trouvant sous « configuration 2 », puis « sites ».

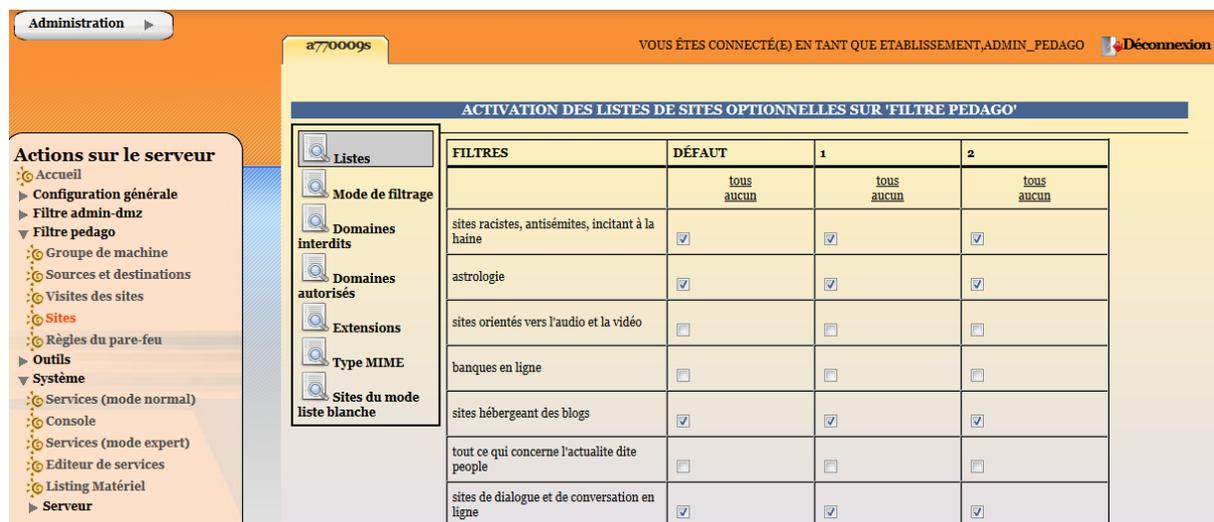
Vous observerez les 4 colonnes suivantes :

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 « default », 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 « default » et sont utilisables pour des groupes de machines.

Pour un filtrage basique, dans la colonne « default », cochez simplement les thèmes qui vous semble être interdits d'accès dans votre établissement.

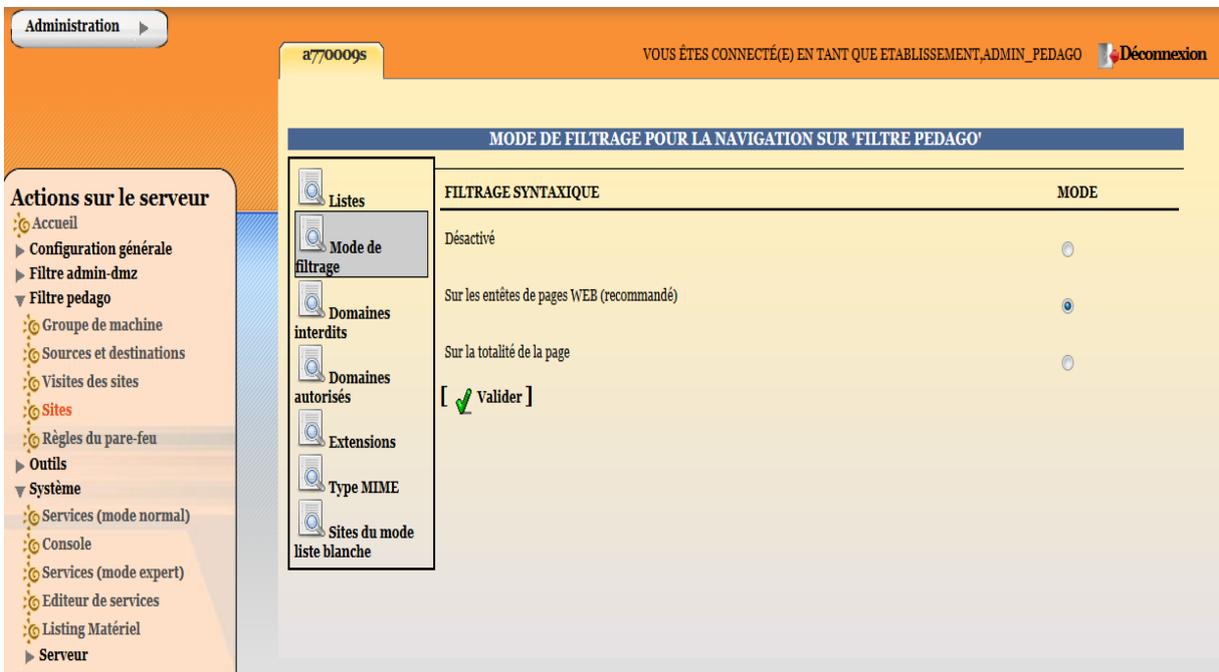


FILTRES	DÉFAUT	1	2
	tous aucun	tous aucun	tous aucun
sites racistes, antisémites, incitant à la haine	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
astrologie	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
sites orientés vers l'audio et la vidéo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
banques en ligne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
sites hébergeant des blogs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
tout ce qui concerne l'actualité dite people	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
sites de dialogue et de conversation en ligne	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

2.4.2 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 les entêtes de pages WEB(recommandé)
- de l'effectuer sur la totalité de la page



Administration

a770009s

VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT_ADMIN_PEDAGO [Déconnexion](#)

MODE DE FILTRAGE POUR LA NAVIGATION SUR 'FILTRE PEDAGO'

FILTRAGE SYNTAXIQUE	MODE
Désactivé	<input type="radio"/>
Sur les entêtes de pages WEB (recommandé)	<input checked="" type="radio"/>
Sur la totalité de la page	<input type="radio"/>

[✓ Valider]

Actions sur le serveur

- Accueil
- Configuration générale
- Filtre admin-dmz
- Filtre pedago
 - Groupe de machine
 - Sources et destinations
 - Visites des sites
 - Sites
 - Règles du pare-feu
- Outils
- Système
 - Services (mode normal)
 - Console
 - Services (mode expert)
 - Editeur de services
 - Listing Matériel
 - Serveur

Listes

Mode de filtrage

Domaines interdits

Domaines autorisés

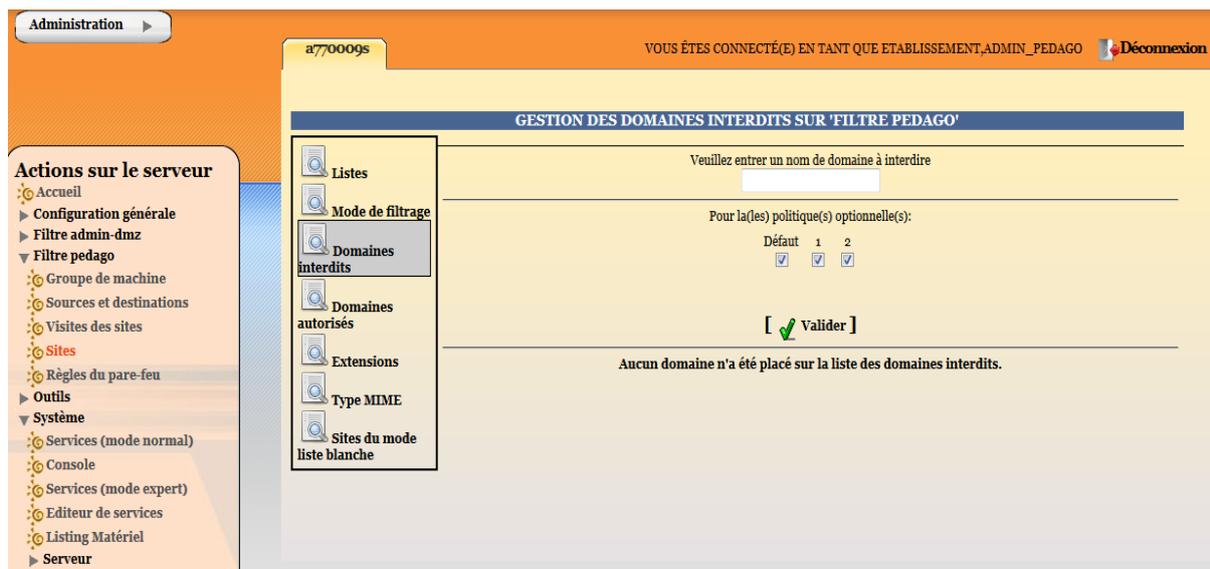
Extensions

Type MIME

Sites du mode liste blanche

2.4.3 Sites interdits et Sites autorisés

-Vous pouvez interdire ou autoriser 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 « default ».



Administration ▶ a770009s VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO Déconnexion

GESTION DES DOMAINES INTERDITS SUR 'FILTRE PEDAGO'

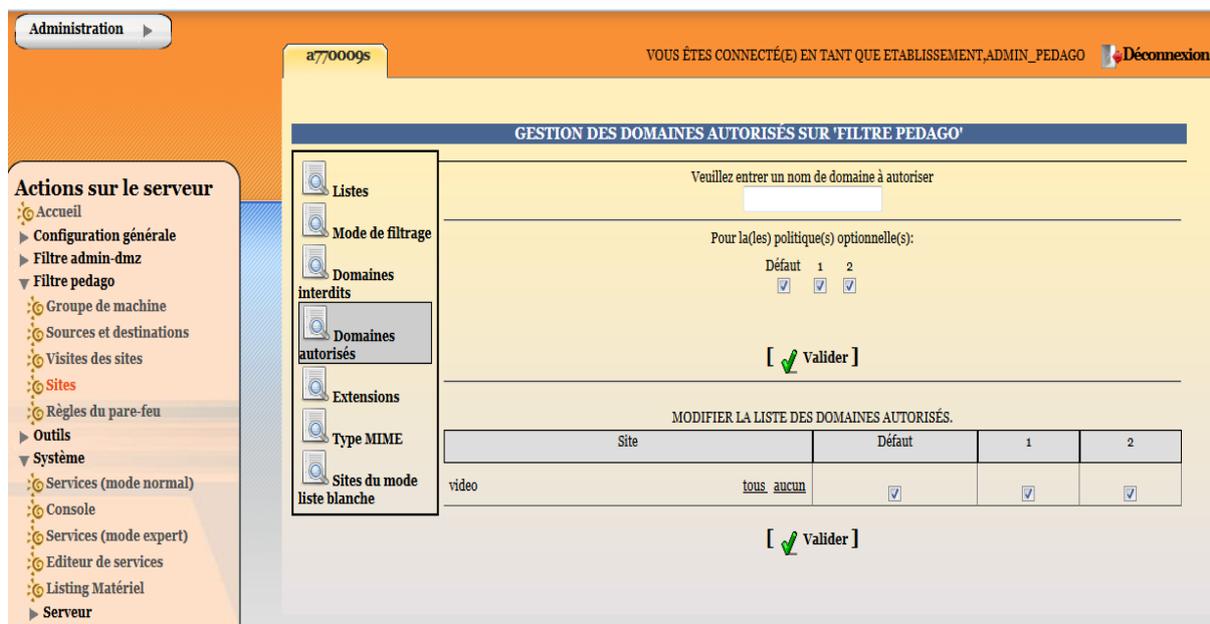
Vous devez entrer un nom de domaine à interdire

Pour la(les) politique(s) optionnelle(s):

Défaut	1	2
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[✓ Valider]

Aucun domaine n'a été placé sur la liste des domaines interdits.



Administration ▶ a770009s VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO Déconnexion

GESTION DES DOMAINES AUTORISÉS SUR 'FILTRE PEDAGO'

Vous devez entrer un nom de domaine à autoriser

Pour la(les) politique(s) optionnelle(s):

Défaut	1	2
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[✓ Valider]

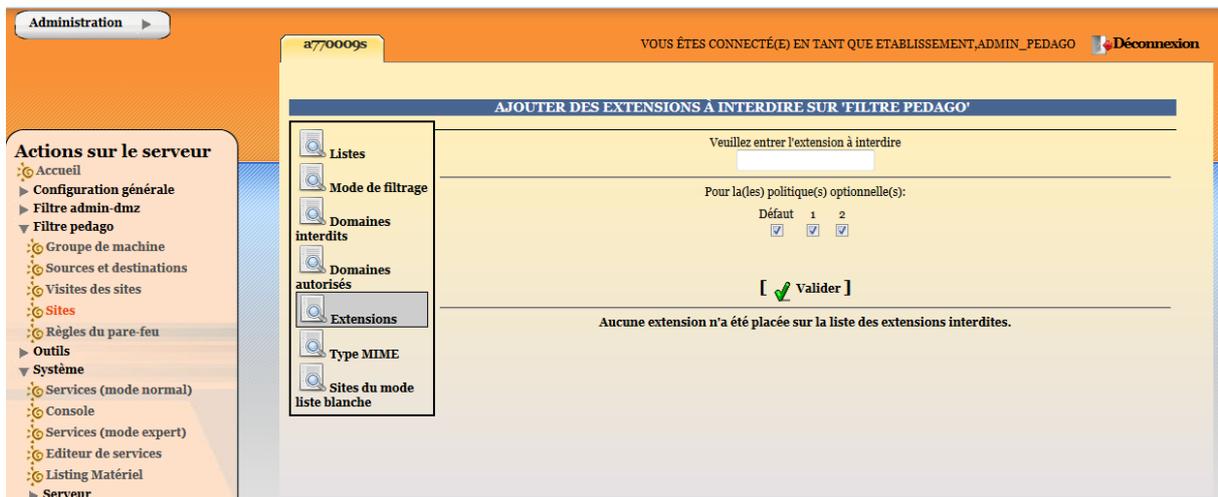
MODIFIER LA LISTE DES DOMAINES AUTORISÉS.

Site	Défaut	1	2
video	tous aucun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[✓ Valider]

2.4.4 Extensions

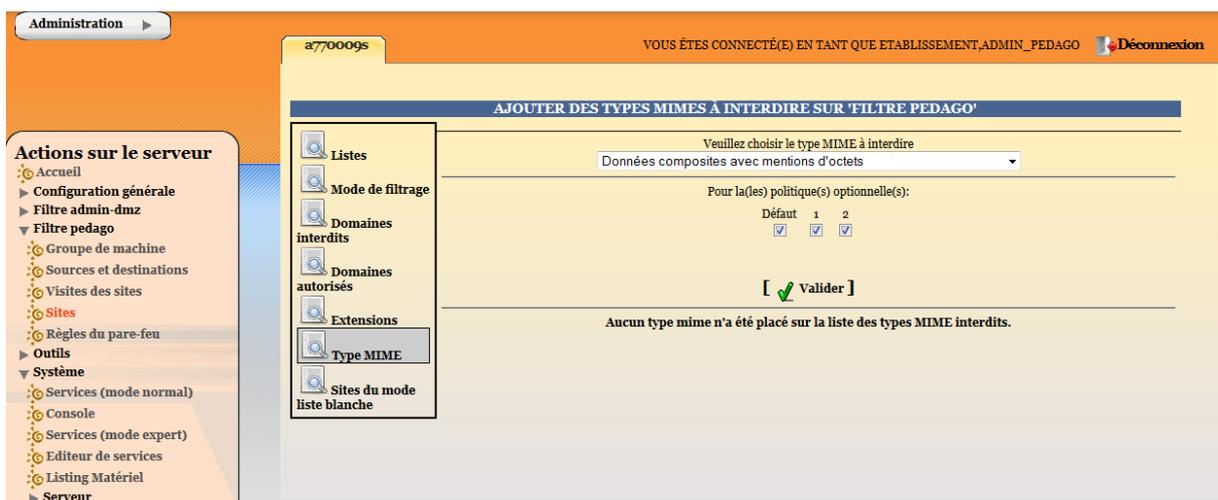
Vous pouvez interdire des extensions de fichiers qui vous semblent dangereuse a télécharger.



2.4.5 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.



2.4.6 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 seront plus accessibles. Cette liste s'utilisera en l'affectant à un groupe de machine.

The screenshot shows a web-based administration interface. At the top, there is a navigation bar with 'Administration' on the left and 'VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT, ADMIN_PEDAGO' with a 'Déconnexion' link on the right. The main content area is titled 'AJOUTER DES SITES POUR LE MODE LISTE BLANCHE SUR 'FILTRE PEDAGO''. On the left, a sidebar menu titled 'Actions sur le serveur' lists various system management options, with 'Sites' highlighted in red. The main area contains a form to 'Ajouter un site au mode liste blanche' with a text input field and a '[✓ Valider]' button. Below this, a section titled 'SITES DU MODE LISTE BLANCHE' contains a text area with the text 'Veuillez sélectionner le(es) site(s) à enlever du mode liste blanche' and a list of URLs: 'http://www.agircontreleharcelementalecole.gouv.fr', 'www.unicef.fr', and 'http://www.youtube.com/'. A '[✕ Supprimer]' button is located below the list. A vertical sidebar on the left of the main content area lists various configuration categories: 'Listes', 'Mode de filtrage', 'Domaines interdits', 'Domaines autorisés', 'Extensions', 'Type MIME', and 'Sites du mode liste blanche', which is currently selected.

2.5 Règles du pare-feu :

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

Vous pouvez activer les règles suivantes :

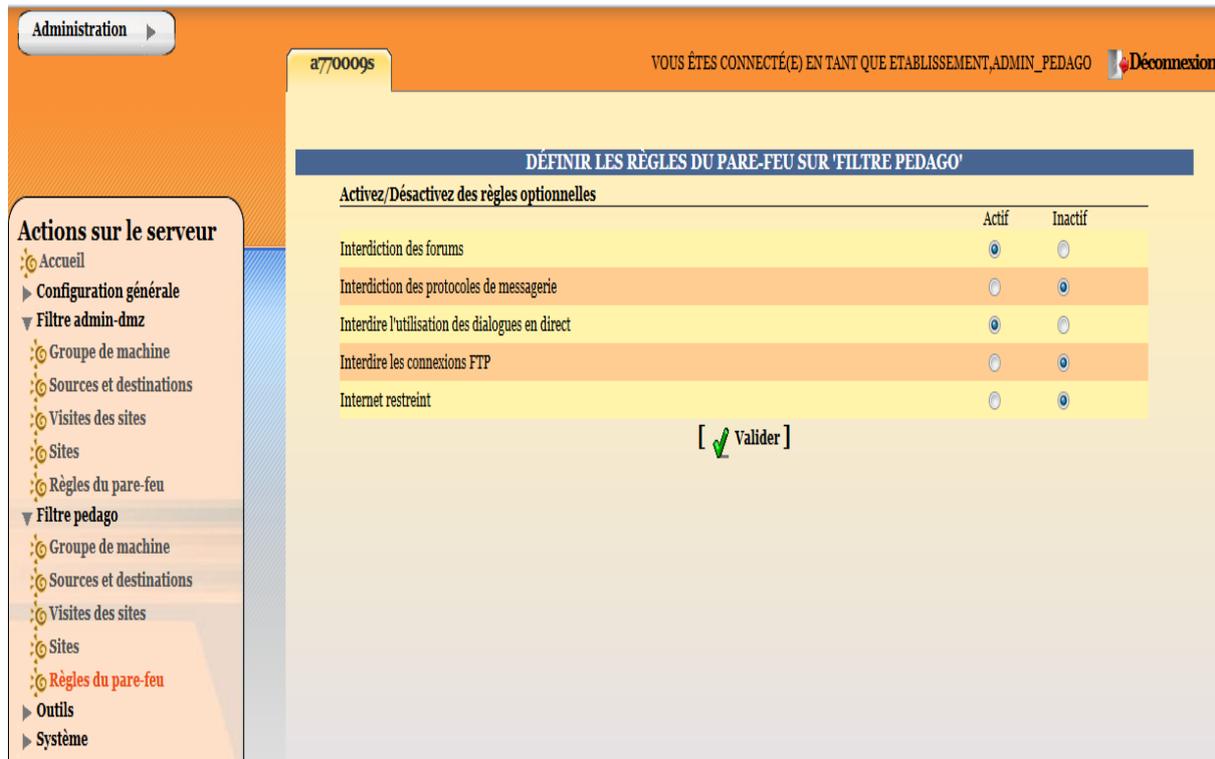
-Interdiction des protocoles de messagerie : Permet de bloquer les réceptions de type POP, IMAP et les envois du type SMTP.

-Interdiction des forums

-Interdire l'utilisation des dialogues en direct : Permet de bloquer les ICQ, Yahoo Messenger, MSN Messenger.

-Interdicte les connexions FTP : Permet de bloquer les transferts de fichiers

-Internet restreint : Permet de bloquer toute la navigation web sauf le proxy.



The screenshot shows a web-based administration interface. At the top, it says 'Administration' and 'a770009s'. The user is logged in as 'ADMIN_PEDAGO'. The main heading is 'DÉFINIR LES RÈGLES DU PARE-FEU SUR 'FILTRE PEDAGO''. Below this, there is a table to 'Activer/Désactiver des règles optionnelles'.

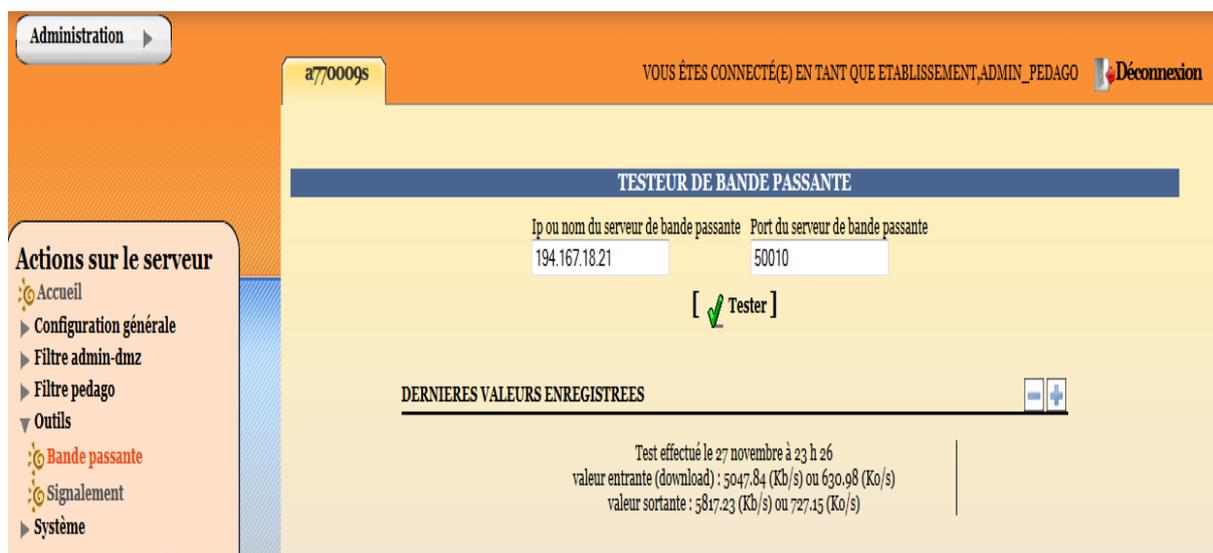
	Actif	Inactif
Interdiction des forums	<input type="radio"/>	<input type="radio"/>
Interdiction des protocoles de messagerie	<input type="radio"/>	<input checked="" type="radio"/>
Interdire l'utilisation des dialogues en direct	<input checked="" type="radio"/>	<input type="radio"/>
Interdire les connexions FTP	<input type="radio"/>	<input checked="" type="radio"/>
Internet restreint	<input type="radio"/>	<input checked="" type="radio"/>

At the bottom of the table, there is a button: [✓ Valider]

3 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 educnet concernant la navigation internet en cliquant sur « plus d'information »



Administration ▶

a770009s VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO Déconnexion

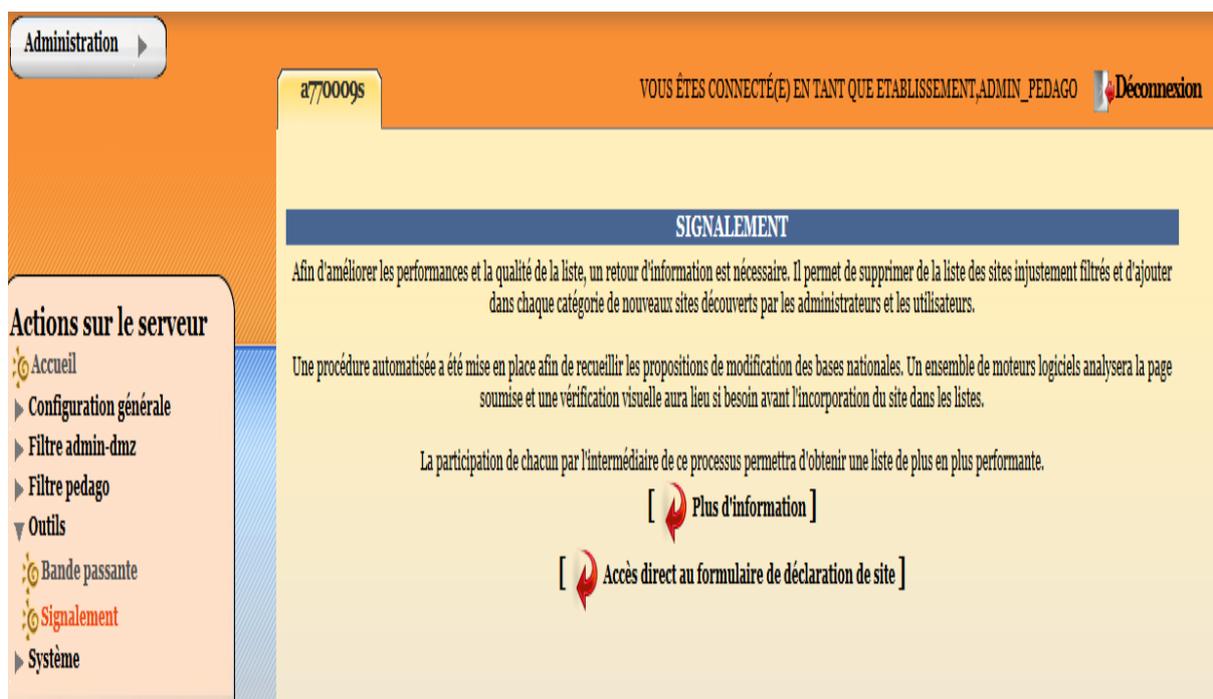
TESTEUR DE BANDE PASSANTE

Ip ou nom du serveur de bande passante	Port du serveur de bande passante
194.167.18.21	50010

[✓ Tester]

DERNIERES VALEURS ENREGISTREES [-] [+]

Test effectué le 27 novembre à 23 h 26
 valeur entrante (download) : 5047,84 (Kb/s) ou 630,98 (Ko/s)
 valeur sortante : 5817,23 (Kb/s) ou 727,15 (Ko/s)



Administration ▶

a770009s VOUS ÊTES CONNECTÉ(E) EN TANT QUE ETABLISSEMENT,ADMIN_PEDAGO Déconnexion

SIGNALEMENT

Afin d'améliorer les performances et la qualité de la liste, un retour d'information est nécessaire. Il permet de supprimer de la liste des sites injustement filtrés et d'ajouter dans chaque catégorie de nouveaux sites découverts par les administrateurs et les utilisateurs.

Une procédure automatisée a été mise en place afin de recueillir les propositions de modification des bases nationales. Un ensemble de moteurs logiciels analysera la page soumise et une vérification visuelle aura lieu si besoin avant l'incorporation du site dans les listes.

La participation de chacun par l'intermédiaire de ce processus permettra d'obtenir une liste de plus en plus performante.

[Plus d'information]

[Accès direct au formulaire de déclaration de site]

4 Validation :



Attention tout changement de parametres doit être validé dans le menu système / console !

Il s'agit de remonter les données locales sur zephir qui est le serveur de configuration centralisée du rectorat.

Il est très important de le faire sous peine de perdre vos données de filtrage

