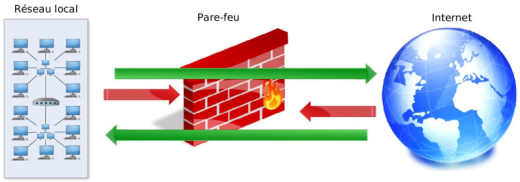
Utilisation de la passerelle AMON



Patrick Dumas, Cédric Frayssinet, Philippe Paccaud, Raphaël Brocq

Novembre 2017
1.2

Table des matières

I - Gestion du filtrage internet - Serveur AMON **3**

II - Comment se connecter sur l'AMON **5**

III - Les fonctions de base du serveur AMON **6**

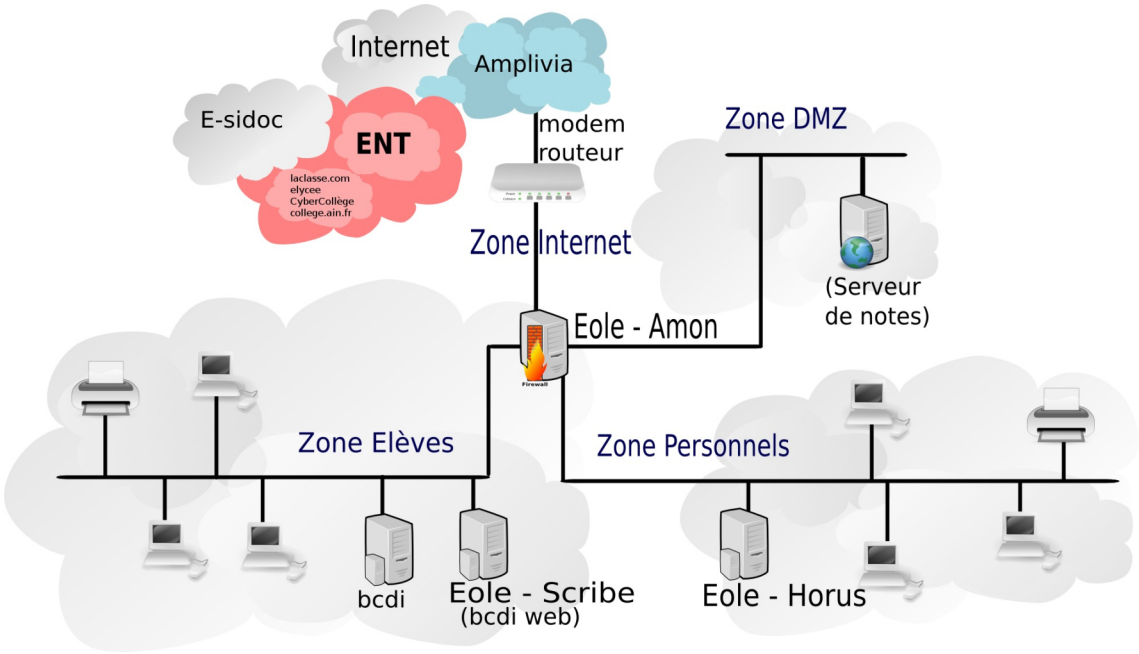
IV - Fonctions avancées du serveur AMON **10**

V - AMON : Sauvegarde de la configuration **13**

Gestion du filtrage internet - Serveur AMON

Généralités

Dans l'académie de Lyon, le schéma réseau d'un établissement scolaire montre le rôle central du serveur de filtrage AMON :



Le DHCP est assuré par le serveur de fichiers Scribe et le filtrage web par le serveur Amon.

Ce même serveur assure aussi le filtrage de la zone “Personnels”.

Fonctionnalités

- Il protège le réseau interne des attaques externes
- Il protège la zone Personnels contre les attaques de la zone Elèves
- Il enregistre toutes les connexions (qui ? quand ? où ?)
- Il sert de proxy-cache ce qui permet d'accélérer les connexions internet
- Il filtre l'accès à Internet grâce à une liste noire nationale
- Il résout les adresses IP en nom de machines (serveur DNS)

...

Remarque

Nous ne nous intéressons là qu'au filtrage web de la zone "élèves"

Conseil

Sur le plan décisionnel et juridique, le chef d'établissement est responsable et décideur dans son établissement et l'accès au réseau informatique se fait sous sa responsabilité.

Le ou les référents numériques de l'établissement peuvent organiser périodiquement une réunion pour l'informer des demandes des enseignants en matière de déblocage de sites web et lui apporter des éléments pour aider à la prise de décision.

Remarque

Tous les serveurs AMON (collèges, lycées) de l'académie sont supervisés par la DSI du Rectorat

II Comment se connecter sur l'AMON

Connexion et authentification

La configuration du pare-feu Amon se fait par le biais d'une interface web d'administration EAD[EAD] qui propose :

- Des actions générales sur le serveur (redémarrage de services...)
- La configuration des filtres web appliqués lors de la navigation sur internet (DansGuardian)
- La gestion des connexions internet par groupe de machines.
- La gestion du pare-feu (horaires, IPs interdites...).
- L'observation des logs (notamment les accès refusés)

L'accès à l'interface EAD est possible avec 2 logins, dont 1 seul nous intéresse (l'autre étant réservé à l'administration de l'établissement). Il nous permettra de paramétrer le filtrage de la zone Élèves.

⚠ *Attention*

- UNE seule station, avec une IP fixe, de la zone Élèves est autorisée à se connecter à l'EAD de l'Amon. Pour connaître l'IP à utiliser il faut consulter le *cahier des charges académique*.
- Pour savoir comment fixer une IP fixe sur un poste et sans utiliser le DHCP, cette FAQ *Comment fixer une IP fixe sur Windows 7 ?* est à disposition.

Il n'y a pas de service d'authentification SSO[SSO] sur un Amon. On se connecte donc via le menu "Authentification locale".

L'identifiant à utiliser est "eole2" sur un AMON en version 2.3 et supérieure.

Le mot de passe est à obtenir auprès de la *plateforme d'assistance*

Une fois connecté, plusieurs informations sont disponibles :

- Dernière mise à jour du serveur
- Dernière mise à jour de la liste noire de l'Université de Toulouse
- État des différents services

Les fonctions de base du serveur AMON

III

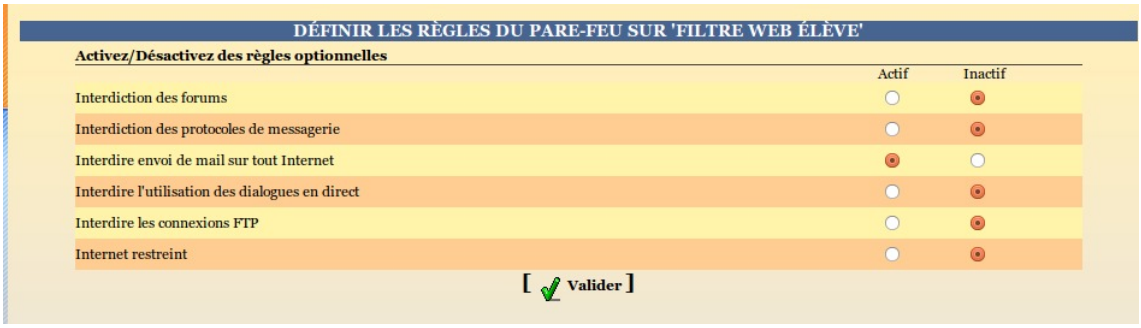
Menu général

Le référent numérique en charge du réseau pédagogique pourra ainsi pour la zone Elèves et seulement pour celle-ci :

- créer des interdictions réseau ou web pour l'ensemble des utilisateurs et/ou pour des groupes machines ou des machines
- activer des filtres Web

Les règles du pare-feu :

Rien de spécial à en dire. Un paramétrage non contraignant est défini au niveau académique. Nous n'avons pas à y toucher.



Le menu "Sites"

C'est là que se feront la plupart des interventions

"listes"

Apparaissent sur 4 colonnes (defaut, 1, 2 et 3) un classement des sites en 36 grands domaines.

Les PC de l'établissement sont tous, à l'origine, soumis au filtrage "defaut".

Les 3 autres colonnes n'ont une utilité que si des groupes de machines sont définis.

Lorsque la case est cochée, tous les sites classés dans le domaine concerné sont interdits.

ACTIVATION DES LISTES DE SITES OPTIONNELLES SUR 'FILTRE WEB ÉLÈVE'

- **Listes**
- **Mode de filtrage**
- **Domaines interdits**
- **Domaines autorisés**
- **Extensions**
- **Type MIME**
- **Sites du mode liste blanche**

FILTRES	DÉFAUT	1	2	3
	tous aucun	tous aucun	tous aucun	tous aucun
sites racistes, antisémites, incitant à la haine	☑	☑	☐	☐
astrologie	☑	☑	☐	☐
sites orientés vers l'audio et la vidéo	☐	☐	☐	☐
banques en ligne	☑	☐	☐	☐
sites hébergeant des blogs	☑	☐	☐	☐
tout ce qui concerne l'actualite dite people	☑	☑	☐	☐
sites de dialogue et de conversation en ligne	☑	☐	☐	☐
sites décrivant des moyens de créer du matériel dangereux (explosif, poison, etc)	☑	☑	☐	☐
sites de rencontres	☑	☑	☐	☐
sites de rencontres	☑	☑	☐	☐
drogue	☑	☑	☐	☐
sites hébergeant des contenus (video, images, son)	☐	☐	☐	☐
informations financières, bourses	☑	☑	☐	☐
forums	☑	☐	☐	☐
sites de jeux en ligne, casino, etc	☑	☑	☐	☐
sites de jeux en ligne, ou de distribution de jeux	☑	☑	☐	☐
sites de piratage et d'agressions informatiques	☑	☑	☐	☐
sites qui injectent des malwares	☑	☑	☐	☐
tout ce qui est lié à l'univers des mangas et de la bande dessinée	☑	☐	☐	☐
sites de marketing très spéciaux	☑	☑	☐	☐
sites qui contiennent des portions adultes	☑	☑	☐	☐
sites pour les mobiles (sonneries, etc)	☑	☐	☐	☐

sites de phishing, de piéges bancaires ou autres	☑	☑	☐	☐
bandeaux publicitaires	☑	☑	☐	☐
sites de radio sur Internet	☐	☐	☐	☐
sites qui ont changé de propriétaire et donc de contenu	☑	☐	☐	☐
sites permettant la prise de contrôle à distance	☑	☐	☐	☐
sectes	☑	☑	☐	☐
sites de vente et d'achat en ligne	☑	☑	☐	☐
sites de réseaux sociaux	☑	☐	☐	☐
sports	☑	☐	☐	☐

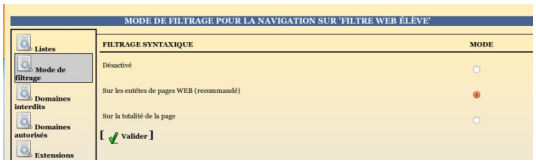
sports	☑	☐	☐	☐
utilisation de proxy distants	☑	☐	☐	☐
proxy spécifiques	☑	☐	☐	☐
sites qui expliquent comme tricher aux examens	☑	☐	☐	☐
sites de logiciels pirates	☑	☑	☐	☐
webmail que l'on trouve sur internet (hotmail, webmail.univ-tlse1.fr, etc)	☐	☐	☐	☐

[✓ **Valider**]

Conseil

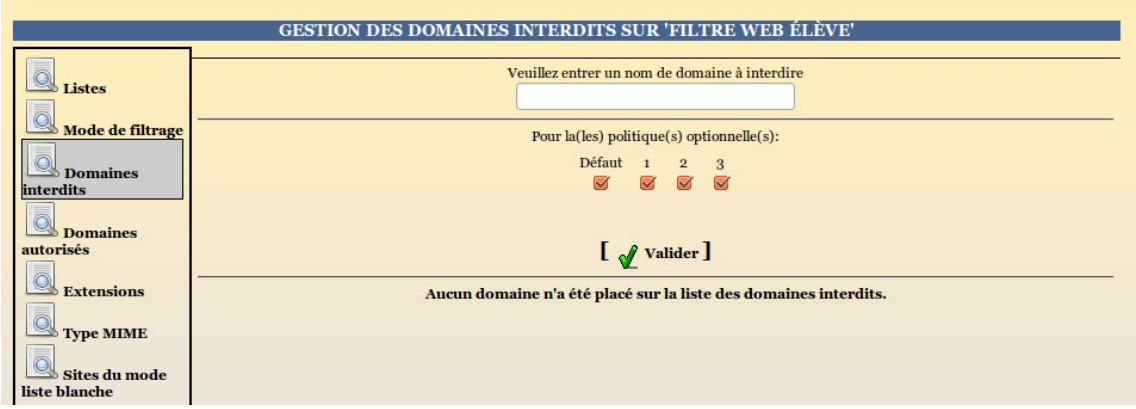
Il vaut mieux partir d'un filtrage dur que l'on va assouplir au fil des demandes. Les copies d'écran proposées ci-dessus dans la colonne "defaut" constituent une base raisonnable.

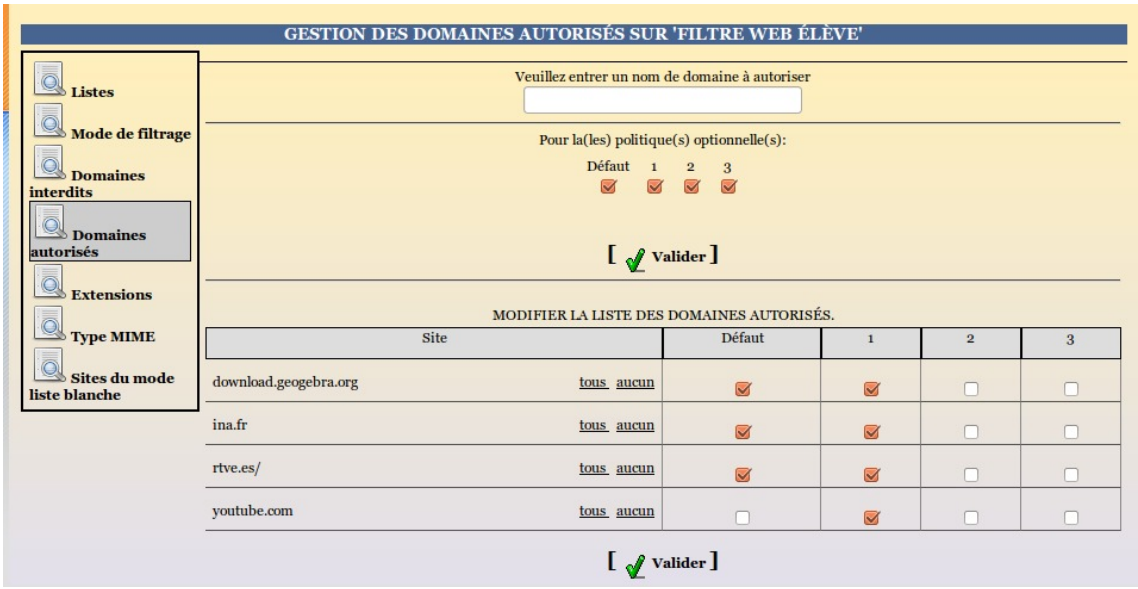
Mode de filtrage :
au choix de l'utilisateur !



Domaines interdits ou autorisés :

Une fois que les cases ont été cochées, suivant la politique générale décidée dans l'établissement en ce qui concerne le filtrage, on peut assouplir cette politique au cas par cas et au fur et à mesure des demandes des enseignants.


GESTION DES DOMAINES INTERDITS SUR 'FILTRE WEB ÉLÈVE'
Listes
Mode de filtrage
Domaines interdits
Domaines autorisés
Extensions
Type MIME
Sites du mode liste blanche
Veuillez entrer un nom de domaine à interdire
Pour la(les) politique(s) optionnelle(s):
Défaut 1 2 3
[Valider]
Aucun domaine n'a été placé sur la liste des domaines interdits.


GESTION DES DOMAINES AUTORISÉS SUR 'FILTRE WEB ÉLÈVE'
Listes
Mode de filtrage
Domaines interdits
Domaines autorisés
Extensions
Type MIME
Sites du mode liste blanche
Veuillez entrer un nom de domaine à autoriser
Pour la(les) politique(s) optionnelle(s):
Défaut 1 2 3
[Valider]
MODIFIER LA LISTE DES DOMAINES AUTORISÉS.
Site
Défaut
1
2
3
download.geogebra.org tous aucun
ina.fr tous aucun
rtve.es/ tous aucun
youtube.com tous aucun
[Valider]

Fonctions avancées du serveur AMON

IV

1. Les groupes de machines

Il est possible de définir une politique de filtrage à quelques machines particulières à partir de leurs adresses IP

En s'aidant éventuellement du *cahier des charges académique*, il faut pour cela tout d'abord choisir une plage d'adresses pour le groupe envisagé.

Adressage IP :

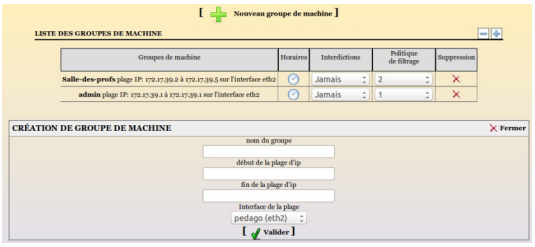
Actuellement nos établissements sont, pour la plupart, en DHCP (adressage dynamique), leur adresse est donc soumise à changement. Si l'on veut affecter un filtrage particulier, il faut donc "figer" l'adresse IP

- Sur un scribe à partir de la version 2.3 :
  Dans l'EAD du Scribe, on utilise le menu "DHCP statique" qui permet de faire de la réservation d'IP.
  Cela permet d'attribuer toujours la même adresse IP à une adresse MAC. Ainsi, les opérations sont simplifiées :

  - choisir les adresses IP dans la plage réservée à cet effet (consulter *l'ancien* ou le *nouveau* plan d'adressage du cahier des charges)
  - tenir à jour un plan d'adressage propre à votre établissement (dans un tableur et mis à disposition dans le perso de l'admin)
  - fixer l'IP depuis le menu DHCP Statique du Scribe.

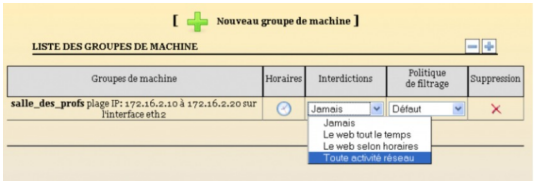
- Sur un scribe en version 2.2 :
  - Il faut définir les adresses IP à la main. Vous pouvez utiliser cette FAQ : *comment fixer une IP fixe sur Windows 7 ?*
  - Tenir à jour un plan d'adressage propre à votre établissement (dans un tableur et mis à disposition dans le perso de l'admin)

Création du groupe de machines via l'EAD du serveur AMON



- Cliquer sur « +Nouveau groupe de machines »
- Renseigner le nom du groupe (choisi explicitement)
- Renseigner la plage IP (début et fin) (indiquer la même ip pour cibler une seule station)
- Choisir pedago (eth2)
- Valider, le groupe apparaîtra dans la liste.

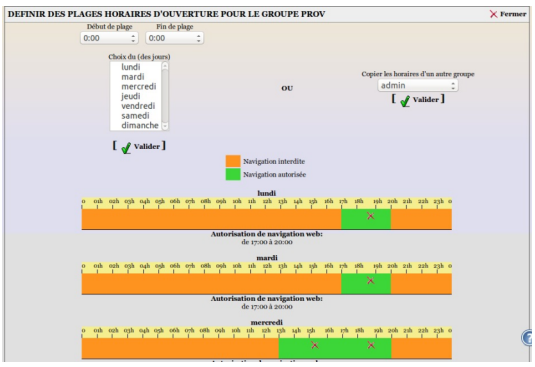
Les interdictions



- “Jamais” : Le groupe de machines n'est soumis à aucune restriction.
- “Le web tout le temps” : Le groupe de machines n'a plus accès à l'internet.
- “Le web selon horaires” : Le groupe de machines ne peut accéder à l'internet que sur une plage horaire définie. (voir définition des plages horaires ci-après)
- “Toute activité réseau” : le groupe de machines n'a plus accès aux ressources réseaux (! !)

Le web selon horaires

Après avoir choisi « le web selon horaires » , il faut cliquer sur l'icône représentant une horloge dans la colonne « horaires ».



- Définir les horaires de début et de fin d'accès au web
- Choisir le/les jours
- Cliquer sur « valider »
- Il est possible de réutiliser ce réglage pour un autre groupe de machines en le choisissant dans « Copier les horaires d'un autre groupe »
- Il est possible de définir plusieurs tranches horaires par jour pour peu qu'elles ne se chevauchent pas. (exemple : 8h00 → 12h00, 13h30 → 17h30).

Politique de filtrage

Une politique optionnelle (type de filtrage) est attribuée à un groupe de machines.

- “Défaut” : il s'agit du filtrage par défaut défini par et pour l'ensemble de l'établissement.
- “Modérateur” : Lorsqu'un site interdit est consulté, un lien est proposé pour outrepasser cette interdiction. Cela peut être utile par exemple pour la salle des professeurs.
- “Interdits” : L'utilisateur ne peut pas naviguer (utile lorsque l'on fait de l' authentification utilisateur).
- “Mode liste blanche” : la navigation n'est possible que sur les sites renseignés dans la liste blanche.
- “1,2,3” : ce sont des politiques de filtrage entièrement personnalisables par l'établissement.

2. Des cas particuliers

"Extensions" et "type MIME"

On peut interdire l'accès et le téléchargement à des fichiers d'un type précis, par exemple des ".exe" ou ".zip".

"site du mode liste blanche"

Si ce mode a été choisi comme politique de filtrage pour un groupe de machines, c'est ici qu'il faut venir lister les seuls sites autorisés.

AMON : Sauvegarde de la configuration

V

Dans l'EAD de l'AMON, il est possible d'appliquer nombre de règles de filtrage.

Malheureusement, il est possible que ces règles disparaissent.

Afin de récupérer en cas de problèmes les règles appliquées, il est possible de les sauvegarder sur le serveur de supervision Zéphyr du Rectorat.

Méthode : Comment sauvegarder sa configuration sur le serveur Zéphyr ?

Cependant, il n'est pas possible de redescendre une configuration sauvegardée sur le serveur Zéphyr depuis l'EAD.

Il faudra s'adresser à la DSI-Reseau, qui elle seule peut y accéder, à contacter le Guichet Unique Académique soit :

- par téléphone au 04.72.80.64.88,
- par mail à *assistance@ac-lyon.fr*,
- par le *portail ARENA* .