

Proxy, cache et filtrage web sur un module Amon

EOLE 2.5



(documentation en brouillon)



EOLE 2.5



(documentation en brouillon)

Version : révision : Avril 2016

Date : création : Mai 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Copyright : Documentation sous licence Creative Commons by-sa - EOLE
(<http://eole.orion.education.fr>)

Licence : Cette documentation, rédigée par le Pôle national de compétences Logiciels Libres, est mise à disposition selon les termes de la licence :

Creative Commons Attribution - Partage dans les Mêmes Conditions 3.0 France (CC BY-SA 3.0 FR) : <http://creativecommons.org/licenses/by-sa/3.0/fr/>.

Vous êtes libres :

- de **reproduire, distribuer et communiquer** cette création au public ;
- de **modifier** cette création.

Selon les conditions suivantes :

- **Attribution** : vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre) ;
- **Partage des Conditions Initiales à l'Identique** : si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

À chaque réutilisation ou distribution de cette création, vous devez faire apparaître clairement au public les conditions contractuelles de sa mise à disposition. La meilleure manière de les indiquer est un lien vers cette page web.

Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits sur cette œuvre.

Rien dans ce contrat ne diminue ou ne restreint le droit moral de l'auteur ou des auteurs.

Cette documentation est basée sur une réalisation du Pôle national de compétences Logiciels Libres. Les documents d'origines sont disponibles sur le site.

EOLE est un projet libre (Licence GPL).

Il est développé par le Pôle national de compétences Logiciels Libres du ministère de l'Éducation nationale, rattaché à la Direction des Systèmes d'Information de l'académie de Dijon (DSI).

Pour toute information concernant ce projet vous pouvez nous joindre :

- Par courrier électronique : eole@ac-dijon.fr
- Par FAX : 03-80-44-88-10
- Par courrier : EOLE-DSI - 2G, rue du Général Delaborde - 21000 DIJON
- Le site du Pôle national de compétences Logiciels Libres : <http://eole.orion.education.fr>

Table des matières

| | |
|--|----|
| Chapitre 1 - eole-proxy | 5 |
| Chapitre 2 - Configuration du proxy et du filtrage web | 6 |
| 1. Onglet Proxy authentifié : 5 méthodes d'authentification | 6 |
| 2. Onglets Proxy authentifié 2 : Double authentification | 9 |
| 3. Onglet Dansguardian : Configuration du filtrage web | 10 |
| 4. Onglet Squid : Configuration du proxy | 14 |
| 5. Onglet Proxy parent : Chaînage du proxy | 15 |
| 6. Exemples de configuration | 18 |
| Chapitre 3 - Filtrage web | 20 |
| 1. Filtrage par utilisateur | 20 |
| 2. Filtrage par machine ou par groupe de machine | 21 |
| 3. Interdire l'accès à un sous-réseau depuis une interface | 26 |
| 4. Interdire ou restreindre l'activité d'un sous-réseau | 28 |
| 5. Bases de filtres optionnels | 30 |
| 6. Filtrage syntaxique | 32 |
| 7. Interdire et autoriser des domaines | 33 |
| 8. Interdire des extensions et des types MIME | 35 |
| 9. Politique liste blanche | 37 |
| Chapitre 4 - Exceptions sur la source ou la destination | 38 |
| Chapitre 5 - Observatoire des navigations | 40 |
| Chapitre 6 - Outil d'analyse de logs LightSquid | 42 |
| Chapitre 7 - Authentification NTLM/SMB - NTLM/KERBEROS hors domaine | 46 |
| Chapitre 8 - Configurer la découverte automatique du proxy avec WPAD | 48 |
| Chapitre 9 - Proxy non configuré dans le navigateur : redirection ou page d'information | 51 |
| Chapitre 10 - Paramétrage des postes client | 56 |
| 1. Authentification NTLM/SMB - NTLM/KERBEROS hors domaine | 56 |
| 2. Configurer la découverte automatique du proxy avec WPAD | 57 |
| 3. Proxy non configuré dans le navigateur : redirection ou page d'information | 59 |
| 4. Synthèse des paramètres proxy à utiliser pour les postes client | 64 |
| Glossaire | 66 |

Chapitre 1

eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les services suivants :

- Squid : proxy cache ;
- Dansguardian : filtrage web ;
- Lightsquid : analyseur de logs ;
- smb, nmb, winbind, krb5 : authentification NTLM/KERBEROS.

<http://www.squid-cache.org/>

<http://dansguardian.org/>

<http://lightsquid.sourceforge.net/>

Historique

A la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté pour être installé sur n'importe quel module EOLE, y compris en **mode une carte**.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `proxy (id=20)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.



En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_proxy_link`).

Remarques

Afin d'assurer l'authentification en mode NTLM/KERBEROS, ce paquet fournit des configurations Samba incompatibles avec celles d'`eole-fichier`.

Si l'on souhaite installer `eole-proxy` et `eole-fichier` sur un même serveur, il est impératif qu'ils soient déclarés dans des conteneurs différents. Leur cohabitation est impossible en *mode non conteneur*.

Chapitre 2

Configuration du proxy et du filtrage web

1. Onglet Proxy authentifié : 5 méthodes d'authentification

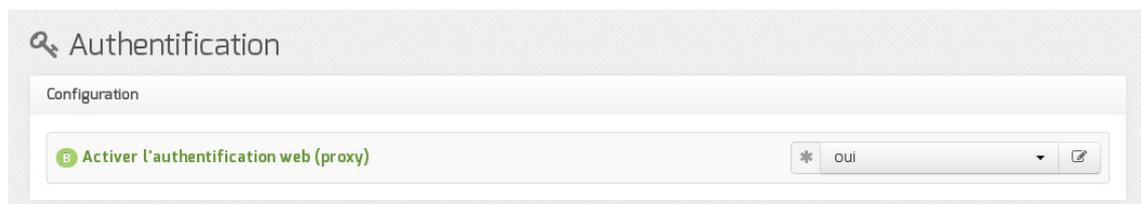
EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

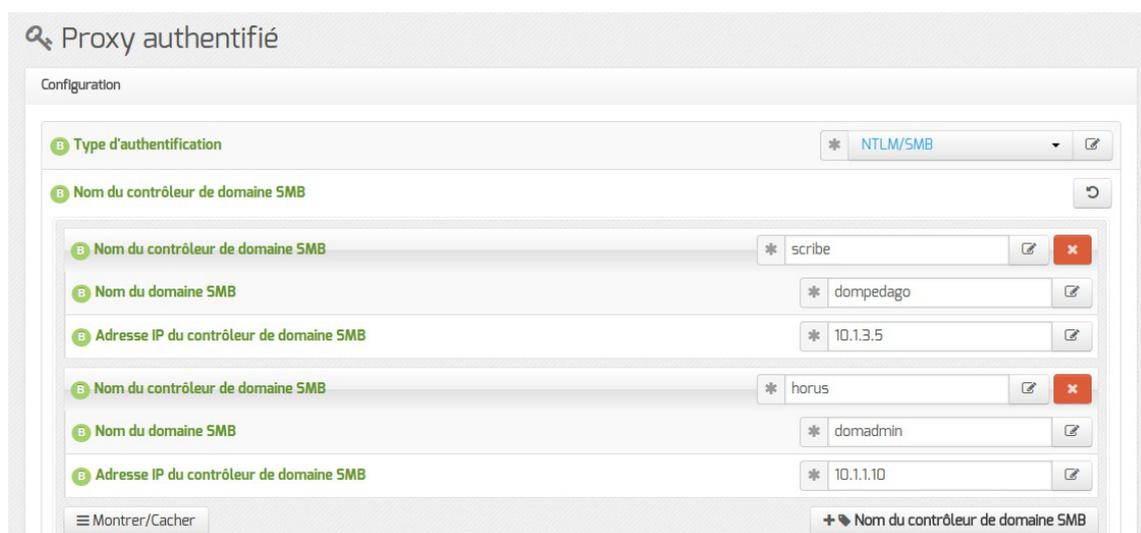
Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet **Authentification** : Activer l'authentification web (proxy).



Cinq méthodes d'authentification sont alors disponibles dans l'onglet **Proxy authentifié**.

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba.



Il est possible de configurer plusieurs contrôleurs de domaine dans le cadre de l'authentification NTLM/SMB.

C'est la configuration à choisir si vous disposez d'un serveur pédagogique Scribe et/ou d'un serveur

administratif Horus.

La syntaxe pour utiliser le proxy authentifié avec une machine hors domaine est `domaine\login` mais elle ne fonctionne pas avec toutes les versions de navigateurs.

L'authentification NTLM/SMB nécessite l'application de la clé de registre suivante sur les clients Windows Vista et Windows Seven :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
```

```
"LMCompatibilityLevel"=dword:00000001
```

Pour plus d'informations, consulter : <http://technet.microsoft.com/en-us/library/cc960646>

Authentification NTLM/KERBEROS

| Configuration | |
|--|-----------------|
| Type d'authentification | * NTLM/KERBEROS |
| Nom du contrôleur de domaine KERBEROS | * srv2k3r2 |
| Nom du domaine KERBEROS (fqdn) | * domaine.lan |
| Nom du domaine Windows | * domaine |
| Adresse IP du contrôleur de domaine KERBEROS | * 10.1.2.73 |

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory. Cette méthode d'authentification fonctionne avec les versions Windows 2000, 2003 et 2008 mais ne fonctionne pas avec Windows NT4.

Elle nécessite l'intégration du serveur hébergeant le proxy authentifiant au domaine.

L'intégration se fait au moment de l'instanciation si l'authentification web est activée et que le type d'authentification NTLM/KERBEROS est configurée.

Si la configuration est faite après l'instanciation il est possible de la relancer à tout moment à l'aide du script `enregistrement_domaine.sh`.

Authentification LDAP

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type OpenLDAP.

The screenshot shows the 'Proxy authentifié' configuration window. Under the 'Configuration' tab, there are three fields:

- Type d'authentification**: Set to 'Ldap'.
- Adresse du premier serveur LDAP**: Set to '10.1.1.10'.
- Suffixe racine de l'annuaire LDAP (base DN)**: Set to 'o=gouv,c=fr'.

Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification LDAP (Active Directory)

The screenshot shows the 'Proxy authentifié' configuration window with the 'Type d'authentification' set to 'Ldap (Active Directory)'. The configuration fields are:

- Type d'authentification**: 'Ldap (Active Directory)'.
- Adresse IP du serveur LDAP (Active Directory)**: '10.1.2.73'.
- Suffixe racine de l'annuaire LDAP (base DN Active Directory)**: 'DC=domaine,DC=lan'.
- Nom du compte nécessaire pour l'interrogation LDAP (Active Directory)**: 'Administrateur'.
- Mot de passe du compte nécessaire pour l'interrogation LDAP (Active Directory)**: 'P@sswOrd'.

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory. Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local

The screenshot shows the 'Proxy authentifié' configuration window with the 'Type d'authentification' set to 'Fichier local'.

Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux. Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

Pour cette authentification, le fichier utilisé par défaut est : `/etc/squid3/users`

Il doit être au format `htpasswd` et il peut être peuplé en utilisant la commande suivante :

```
htpasswd -c /etc/squid3/users <compte>
```

⚠ En mode conteneur (module AmonEcole par exemple), le fichier `/etc/squid3/users` se trouve dans le conteneur `proxy`.

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors eth0 si plusieurs interfaces sont configurées), il est possible d'activer/désactiver l'authentification proxy.

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau eth2, il faut aller dans l'onglet **Interface-2** et répondre **non** à la question Activer l'authentification sur cette interface (s'applique aussi aux VLAN).

2. Onglets Proxy authentifié 2 : Double authentification

Par double authentification, nous entendons la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Configuration pas à pas

1. Activation de la deuxième instance de Squid dans l'onglet **Authentification** :

Activer une deuxième instance de Squid

2. Configuration du type d'authentification dans l'onglet **Proxy authentifié 2** :

Proxy authentifié 2

Configuration

Type d'authentification

Adresse du premier serveur LDAP

Adresse du second serveur LDAP (si le 1er ne répond pas)

Suffixe racine de l'annuaire LDAP (base DN)

Notes techniques

Les fichiers de logs spécifiques au second type d'authentifications sont les suivants :

- `/var/log/rsyslog/local/squid/squid2.info.log`
- `/var/log/rsyslog/local/dansguardian/dansguardian2.info.log`

Dans l'état actuel, ces logs ne sont pas consultables au travers de l'interface EAD et seule la première configuration proxy est distribuée par WPAD (voir partie dédiée).

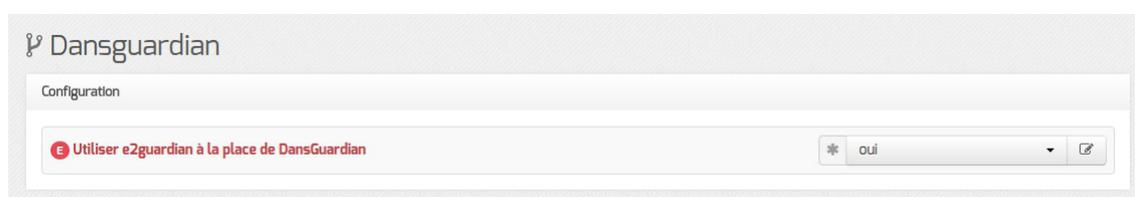
3. Onglet Dansguardian : Configuration du filtrage web

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour Filtre Web à appliquer à cette interface dans la configuration de l'interface (onglets : Interface-1 , Interface-2 , ...).

Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage.

Le module Amon intègre le logiciel libre e2guardian^[p.66]. Pour réaliser le filtrage il est donc possible de choisir entre le logiciel DansGuardian et le logiciel e2guardian.



Paramètres de configuration pour DansGuardian

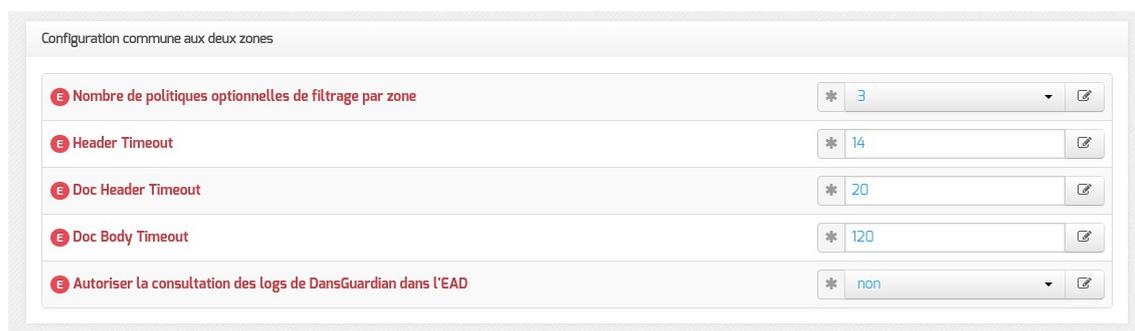
Les variables permettant d'affiner la configuration sont communes aux deux logiciels.

Le paramétrage par défaut de DansGuardian (logiciel utilisé pour le filtrage web) convient à un établissement de taille moyenne sans modification particulière.

Il peut être néanmoins intéressant de modifier ce paramétrage pour satisfaire les besoins de l'établissement (notamment dans le cas où le serveur ne peut plus répondre aux requêtes, la fenêtre d'authentification apparaît de façon intempestive, ...).

Sur un petit établissement, il sera possible d'économiser des ressources.

Sur un gros établissement, il pourra répondre à un plus grand nombre de requêtes.



Paramètres de configuration pour DansGuardian

Un certain nombre de paramétrages sont proposés pour contrôler les ressources de DansGuardian.



Il est possible d'affecter une politique spécifique aux machines du foyer (politique plus laxiste) et une autre aux machines du CDI (politique moins permissive).

Politiques de filtrage optionnelles

Une politique de filtrage correspond à un ensemble d'autorisations ou interdictions d'accès à des sites, suivants différents critères.

Il existe par défaut 4 politiques obligatoires :

- une politique de filtrage par défaut ;
- une politique « modérateur »(permet d'outrepasser les interdictions) ;
- une politique « interdits » (permet d'interdire toute navigation) ;
- une politique « liste blanche » (navigation limitée aux sites de cette même liste).

Seule la politique de filtrage par défaut est modifiable via l'EAD.

En plus de ces politiques, il est possible d'ajouter de 1 à 4 autres politiques de filtrage optionnelles (il y en a 3 par défaut).

Ces politiques de filtrage optionnelles seront alors paramétrables dans l'EAD.

Pour modifier le nombre de politiques de filtrage par zone, il faut utiliser le paramètre :

Nombre de politiques optionnelles par zone.

La valeur 0 revient à n'utiliser que les 4 politiques par défaut proposées ci-dessus.

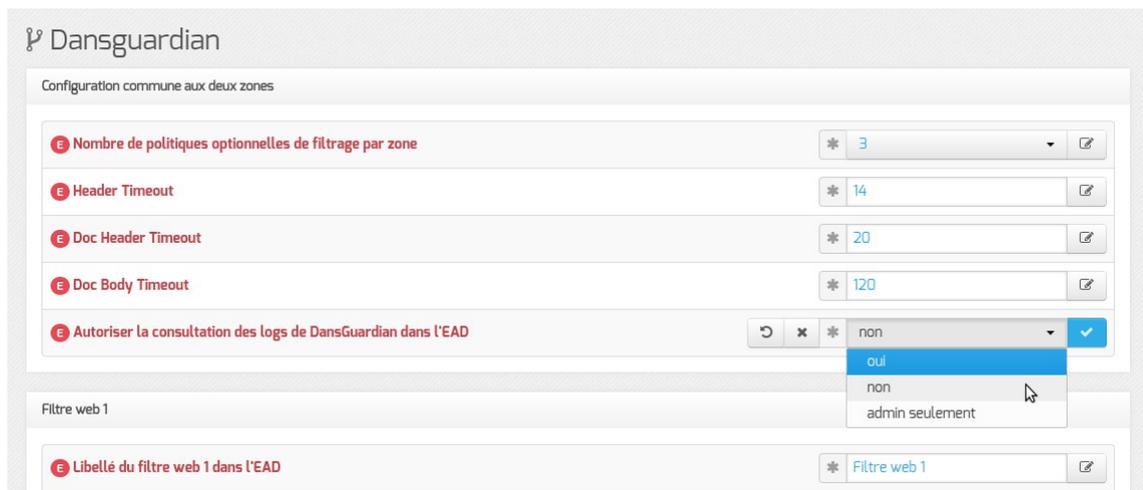
L'ajout de politiques optionnelles (valeur 1,2,3,4) permet d'ajouter des filtres supplémentaires, associables à des groupes de machines ou des logins utilisateur.



Plus vous définissez de politiques, plus DansGuardian utilisera de ressources.
Adaptez le nombre de politiques activées en fonction de vos besoins.

L'observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage Dansguardian.



Paramétrage de l'accès à la consultation des logs

La question Autoriser la consultation des logs de Dansguardian dans l'EAD propose plusieurs options :

- oui : accès autorisé pour les utilisateurs EAD possédant les actions navigation visit admin et/ou navigation visit pedago (configuration proposée sur Amon-2.2)

- `non` : accès interdit pour tout le monde, personne ne voit le lien `Visites des sites` (configuration par défaut sur Amon-2.3)
- `admin_seulement` : accès autorisé uniquement pour le rôle `admin`.



La consultation des visites de site se fait au travers de l'EAD, menu : `Filtre web X/visites des sites`.

Paramétrage de DansGuardian

Le logiciel DansGuardian offre de nombreuses options de configuration.

| Paramètre | Valeur |
|--|--------------|
| Libellé du filtre web 1 dans l'EAD | Filtre web 1 |
| Nombre maximum de processus | 80 |
| Nombre minimum de processus | 8 |
| Nombre minimum de processus en attente | 4 |
| Nombre maximum de processus en attente | 32 |
| Nombre de processus démarré s'il en manque | 6 |
| Durée de vie maximum d'un processus avant de se terminer | 500 |
| Répertoire de cache | /tmp |
| Taille maximum de fichier conservé en mémoire | 5000 |
| Taille maximum de fichier conservé sur le disque | 5000 |

Plusieurs sont paramétrables dans l'interface de configuration du module.

Seule l'expérience «à tâtons»^[p.67] permet de définir les valeurs adéquates à votre installation.

L'objectif est d'utiliser le plus de mémoire possible sans que le serveur n'utilise la partition d'échange (swap^[p.68]).



La commande `top` en console permet d'observer l'évolution de l'utilisation de la partition d'échange de façon dynamique.

Nombre maximum de processus

Le nombre maximum de processus disponibles pour traiter les nouvelles connexions.

La valeur doit être comprise entre 60 et 1018.

Nombre minimum de processus

Le nombre de processus minimal pour traiter les nouvelles connexions.

Nombre minimum de processus en attente

Le nombre minimum de processus prêts à recevoir de nouvelles connexions.

Nombre maximum de processus en attente

Le nombre maximum de processus attendant de nouvelles connexions.

Nombre de processus démarré s'il en manque

Le nombre minimum de processus disponibles lorsqu'ils viennent à manquer.

Durée de vie maximum d'un processus avant de se terminer

Les processus enfants, comme tout processus, peuvent succomber à des variables parasites. Ce paramètre définit l'âge maximal de connexions qu'un processus enfant traite avant de quitter. La valeur par défaut est de traiter 500 demandes de connexion avant de quitter.

Augmenter ce paramètre peut aider à soulager les problèmes de performance liés à la rotation des processus, mais peut créer un problème de performance si un processus s'emballé pour une raison quelconque.

Sur les grands sites vous pourriez vouloir essayer de passer cette valeur à 10000.

Répertoire de cache

Permet de choisir le chemin du répertoire de cache, par défaut `/tmp`.

La taille maximum de fichier conservé en mémoire

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

C'est la taille maximale des fichiers en kibibytes^[p.67] que DansGuardian va télécharger et mettre en cache dans la RAM. Après que cette limite soit atteinte, DansGuardian met en cache sur le disque.

Cette valeur doit être inférieure ou égale à la valeur de `La taille maximum de fichier conservé sur le disque`.

Utiliser la valeur 0 permet de définir le même réglage que `La taille maximum de fichier conservé sur le disque`.

La taille maximum de fichier conservé sur le disque

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

C'est la taille maximale des fichiers en kibibytes^[p.67] que DansGuardian va télécharger de sorte qu'ils soient vérifiés par l'anti-virus.

Cette valeur doit être supérieure ou égale `La taille maximum de fichier conservé en mémoire`.

Désactivation du filtrage web

Dans certaines configurations (utilisation d'un proxy académique, ...), il peut s'avérer utile de désactiver complètement le filtrage web.

Cela est possible en allant dans l'interface de configuration du module en mode expert et en répondant `non` à la question de l'onglet `Services`, `Activer le filtrage sur le proxy`.



Dans cette configuration, le proxy Squid écoute sur le **port 3128** en lieu et place du logiciel de filtrage DansGuardian.

Adresse électronique à utiliser en cas de réclamation

Lorsque la consultation d'une page est refusée à l'utilisateur, une page d'erreur affichant les détails de l'interdiction apparaît.

Celle-ci propose également une adresse électronique à utiliser pour signaler les interdictions injustifiées. Cette adresse se configure par l'intermédiaire de la variable `Adresse courriel du cachemaster` disponible dans l'onglet `Messagerie`.

Voir aussi...

Observatoire des navigations [p.40]

4. Onglet Squid : Configuration du proxy

Le service proxy Squid n'étant pas désactivable, l'onglet `Squid` est toujours accessible en mode expert.

L'onglet expert `Squid` permet de modifier et de fixer une sélection des principaux paramètres du fichier de configuration : `/etc/squid3/squid.conf`.

Les paramètres de ce fichier de configuration se retrouvent explicitement dans le nom des variables Creole (mode Debug de l'interface de configuration du module).

The screenshot shows the 'Squid' configuration page in the Creole interface. It features a list of configuration options, each with a red 'E' icon, a text input field, and a 'fix' icon (a square with a pencil). The options and their current values are:

- `Générer les statistiques Squid automatiquement`: non
- `Port d'écoute du CGI LightSquid`: 8062
- `Méthode d'anonymisation des rapports LightSquid`: aucune
- `Port d'écoute HTTPS de Squid`: (empty)
- `"SSL_ports" supplémentaire`: Pas de valeur
- `"Safe_ports" supplémentaire`: Pas de valeur
- `Nombre de processus associées au module d'authentification basique`: 20
- `Nombre de processus associées au module d'authentification NTLM`: 20
- `Activer les exceptions de cache père de type regexp`: non
- `Port d'écoute pour les requêtes ICP`: 3130
- `Port d'écoute pour les requêtes HTCP`: 4827

Vue de l'onglet Squid de l'interface de configuration du module

Les options `Générer les statistiques Squid automatiquement`, `Port d'écoute du CGI LightSquid` et `Méthode d'anonymisation des rapports LightSquid` servent à configurer l'outil d'analyse de logs LightSquid permettant d'afficher sous forme de pages web l'utilisation du proxy. Sa configuration fait l'objet d'une section dédiée.

L'option `Port d'écoute HTTP de Squid` est par défaut fixée au port `8080` et n'est à modifier que si le filtrage web a été désactivé.

Il est possible de paramétrer Squid pour qu'il écoute les requêtes HTTPS des clients. Ceci est particulièrement utile dans les situations où vous utilisez Squid comme accélérateur des requêtes.

Il faut alors saisir le numéro de port choisi dans le champ `Port d'écoute HTTPS de Squid`.

Par défaut, un certain nombre de ports SSL sont paramétrés et considérés comme sûrs quand ils sont des ports sortants : 443, 563, 631, 4000-5000, 8070, 8090, 8443, 8753 et 7070. Il est possible d'en ajouter autant que vous voulez dans le champ `"SSL ports" supplémentaire`.

Par défaut, un certain nombre de ports sont définis et autorisés aux utilisateurs : 80, 21, 443, 563, 70, 210, 631 et 1025-65535. Il est possible d'en ajouter autant que vous voulez dans le champ `"Safe ports" supplémentaire`.



L'onglet expert Squid permet de modifier et de fixer un nombre conséquent de paramètres optionnels du fichier de configuration : `/etc/squid3/squid.conf`.

Pour plus d'informations sur la modification de ces paramètres, vous pouvez consulter :

- les exemples de configuration dans le fichier de documentation de Squid : `/usr/share/doc/squid3-common/squid.conf.documented.gz`
- la documentation en ligne des différents paramètres : <http://www.squid-cache.org/Doc/config/>

Voir aussi...

Onglet Dansguardian : Configuration du filtrage web ^[p.10]

Outil d'analyse de logs LightSquid ^[p.42]

5. Onglet Proxy parent : Chaînage du proxy

L'onglet expert `Proxy parent` permet de déclarer un ou plusieurs serveurs proxy à utiliser en amont de celui activé sur le module EOLE.

Cette fonctionnalité est à utiliser dans le cas de la mise en place d'un proxy centralisé au niveau d'une académie ou d'un groupe d'établissements.

The screenshot shows the 'Proxy parent' configuration interface. It is divided into three main sections:

- Proxy parent global:** A toggle switch for 'Utiliser un proxy web parent global' is set to 'non'.
- Proxy parent par zone:** A toggle switch for 'Utiliser un proxy web parent par zone' is set to 'non'.
- Coopération des caches:** A toggle switch for 'Activer la coopération des cache' is set to 'non'.

Vue de l'onglet Proxy-pere de l'interface de configuration du module

Si plusieurs proxy parents sont déclarés, un mécanisme de type round-robin^[p.68] est utilisé afin de répartir la charge sur les différents serveurs.



Les proxy déclarés ici ne seront pas utilisés par le serveur lui-même.

La déclaration d'un proxy à utiliser par le module EOLE s'effectue dans l'onglet **Général** en passant la variable : Utiliser un serveur mandataire (proxy) pour accéder à Internet à oui.

Proxy parent global

Le ou les proxy parents peuvent être déclarés de façon globale en passant la variable Utiliser un proxy web parent global à oui.

The screenshot shows the 'Proxy parent global' configuration interface with the following details:

- The toggle for 'Utiliser un proxy web parent global' is set to 'oui'.
- Below this, there is a section for 'Adresse du proxy web parent' containing a list of configurations:

| Paramètre | Valeur |
|--------------------------------------|------------------|
| Adresse du proxy web parent | proxy.ac-test.fr |
| Port du serveur proxy web parent | 3128 |
| Port ICP du serveur proxy web parent | 3130 |
| Option du proxy web parent | no-query |

At the bottom of the list, there is a 'Montrer/Cacher' button and a '+ Adresse du proxy web parent' button to add more entries.

Vue de l'onglet Proxy-pere de l'interface de configuration du module

Proxy parent par zone

Pour des besoins spécifiques, des proxy parents peuvent être déclarés pour des zones DNS particulières en passant la variable Utiliser un proxy web parent par zone à oui.

Les zones DNS de destination peuvent être :

- soit renseignées directement dans la variable Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent si la Méthode d'utilisation de la zone accessible via ce serveur web parent est DNS;
- soit renseignées dans un fichier texte dont le chemin est à indiquer dans la variable Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent si la Méthode d'utilisation de la zone accessible via ce serveur web parent est nom fichier;

Vue de l'onglet Proxy-pere de l'interface de configuration du module



Pour que ces sous-domaines soient également pris en compte, le nom DNS du domaine doit impérativement être précédé d'un point.

Il est possible de renseigner directement plusieurs zones DNS en les séparant par des espaces, exemple : .domain1 .domain2 .domain3.

Coopération des caches

Si on a plusieurs proxy cache, il peut être intéressant de les faire collaborer pour partager le cache. Cela se fait via le mécanisme de proxy sibling^[p.68].

Vue de l'onglet Proxy-pere de l'interface de configuration du module

6. Exemples de configuration

Soit un établissement avec deux sous-réseaux (admin sur eth1 et pédago sur eth2) :

Authentifier et ne pas différencier la politique (comportement par défaut)

- dans l'interface de configuration du module, dans l'onglet **Services** : choisissez **Activer l'authentification du proxy** ;
- vos deux interfaces seront associés au même filtrage web : **1** ;
- il ne vous reste alors qu'à configurer l'authentification (NTLM/SMB, NTLM/KERBEROS ou LDAP) dans l'onglet **Authentification** .

Authentifier l'interface pédagogique et pas l'interface administrative

- dans l'interface de configuration :
dans l'onglet **Services** : **Activer l'authentification du proxy** ;
dans l'onglet **interface-1** :
 - **Activer l'authentification sur cette interface (s'applique aux vlans) : non** ;
 - **Filtre Web à appliquer à cette interface : 1** ;
 dans l'onglet **interface-2** :
 - **Activer l'authentification sur cette interface (s'applique aux vlans) : oui** ;
 - **Filtre Web à appliquer à cette interface : 2** ;
- il ne vous reste alors qu'à configurer l'authentification (NTLM/SMB, NTLM/KERBEROS ou LDAP) dans l'onglet **Authentification**.

Authentifier et utiliser deux politiques différentes

- dans l'interface de configuration :
dans l'onglet **Services** : **Activer l'authentification du proxy** ;
dans l'onglet **interface-1** :
 - **Filtre Web à appliquer à cette interface : 1** ;
 - **Activer l'authentification sur cette interface (s'applique aux vlans) : oui** ;
 dans l'onglet **interface-2** :
 - **Filtre Web à appliquer à cette interface : 2** ;

- Activer l'authentification sur cette interface (s'applique aux vlans) : oui ;
- il ne vous reste alors qu'à configurer l'authentification (NTLM/SMB, NTLM/KERBEROS ou LDAP) dans l'onglet **Authentification**.

Chapitre 3

Filtrage web

Avec le filtrage web, il est possible :

- de configurer la manière dont le filtrage s'effectue ;
- d'associer une politique de filtrage (interdits, modérateurs, liste blanche...) à des utilisateurs (seulement si l'authentification est activée durant la phase de configuration) ;
- d'associer une politique de filtre (interdits, modérateurs, liste blanche...) à des machines.

Cette configuration s'effectue :

- par zone de configuration ;
- de manière plus fine, par politique de filtrage ;
- de façon prioritaire sur les machines puis sur les utilisateurs.

1. Filtrage par utilisateur

Si l'authentification a été activée sur la zone durant la phase de configuration, il est possible de définir, pour l'utilisateur, une des politiques de filtrage suivante :

- modérateurs (lorsqu'un site est interdit, un lien lui est proposé pour outrepasser l'interdiction) ;
- interdits (aucune navigation web n'est possible pour cet utilisateur) ;
- mode liste blanche (seul les sites de la liste blanche sont autorisés) ;
- politiques optionnelles personnalisées.

Placer un professeur sur la liste des modérateurs pour la zone de filtre web 1

Il est parfois intéressant de voir un site interdit, qui, parfois, empêche l'accès à un contenu pédagogique. En définissant un professeur comme modérateur, on lui permet d'outrepasser l'interdiction de navigation et, le cas échéant, le placer sur la liste des sites autorisés.

Dans **Filtre web 1 / Utilisateurs** :

- entrer le nom de l'utilisateur ;
- valider ;
- choisir **Modérateur** dans la liste.



Configurer des politiques de filtrage pour un utilisateur sur la zone de filtre web 2

Ces informations sont stockées dans :

```
/var/lib/blacklists/dansguardian<num_instance>/common/filtergroupslis
```

Sur AmonEcole, ces fichiers sont dans le conteneur **reseau**.



Si le menu **Utilisateurs** n'apparaît pas, c'est que la zone n'est pas authentifiée.

2. Filtrage par machine ou par groupe de machine

Présentation

Le module Amon propose de gérer des groupes de machine par plage d'adresse IP.

En ajoutant une référence à ce groupe, il est possible :

- de lui interdire l'accès au réseau ;
- de lui interdire la navigation web seulement ;
- de lui autoriser la navigation web selon des horaires ;
- de lui associer une politique de filtrage web spécifique.



Les informations liées aux groupes de machine sont stockées dans :

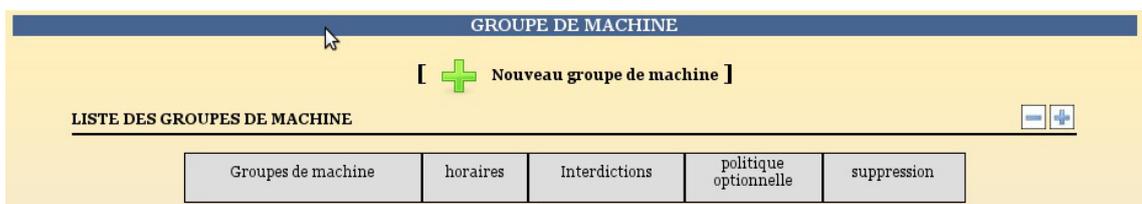
```
/usr/share/ead2/backend/tmp/ipset_group<num_instance>.txt
```

Les éventuelles plages horaires associées sont dans :

```
/usr/share/ead2/backend/tmp/ipset_schedules<num_instance>.pickle
```

Créer un groupe de machine

Pour configurer un groupe de machine de la zone 1, aller dans **Filtre web 1 / Groupe de machine**.



Interface de gestion de groupe de machine

Cliquer sur **Nouveau groupe de machine** et un formulaire de création apparaît.

CRÉATION DE GROUPE DE MACHINE
✖ Fermer

nom du groupe

début de la plage d'ip

fin de la plage d'ip

[✓ Valider]

Formulaire de création

Remplir :

- nom pour le groupe de machine (sans accents ni caractères spéciaux) ;
- donner l'adresse IP de début de plage ;
- donner l'adresse IP de fin de plage ;
- si plusieurs interfaces réseau sont associés à cette zone, il vous demandera le nom de l'interface ;
- valider.

Le groupe de machine est dans la liste et peut être géré.

GRUPE DE MACHINE

[+ Nouveau groupe de machine]

LISTE DES GROUPE DE MACHINE
[-] [+]

| Groupes de machine | horaires | Interdictions | politique optionnelle | suppression |
|---|----------|---------------|-----------------------|-------------|
| bibliotheque plage IP: 192.168.230.10 à 192.168.230.20 sur l'interface eth1 | | Jamais ▾ | Défaut ▾ | ✖ |

Le groupe de machine est ajouté



S'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'adresses dans un groupe peut entraîner une baisse de performance.

Limiter l'accès réseau

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

- jamais ;
- le web tout le temps ;
- le web selon des horaires (à définir au préalable) ;
- toute activité réseau.

Interdire le groupe de navigation web

Dans la colonne **Interdictions**, choisir **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)

Si vous désirez faire une interdiction de navigation selon des horaires, il faut :

- configurer des horaires ;
- appliquer l'interdiction.

Configuration des horaires

Dans la colonne **Interdictions**, choisir **Le web selon horaires**.

Cliquer sur l'horloge, la gestion des horaires apparaît.

The screenshot displays the configuration interface for the 'secretariat' machine group. At the top, there is a button to add a new machine group. Below is a table listing machine groups with columns for 'horaires', 'Interdictions', 'politique optionnelle', and 'suppression'. The 'secretariat' group is highlighted, showing its IP range and the selected policy 'Le web selon'. A configuration window is open for defining time slots for the 'secretariat' group. It includes fields for 'Début de plage' and 'Fin de plage' (both set to 0:00), a dropdown for 'Choix du (des jours)' (showing 'lundi', 'mardi', 'mercredi', 'jeudi', 'vendredi', 'samedi', 'dimanche'), and a 'Copier les horaires d'un autre groupe' option. A legend indicates that orange represents 'Navigation interdite' and green represents 'Navigation autorisée'. The interface shows orange bars for 'Navigation interdite' on Monday, Tuesday, and Wednesday.

Gestionnaire d'horaires pour les groupes de machine

- choisir la plage horaire d'autorisation ;
- choisir les jours d'applications ;
- valider.

GRUPE DE MACHINE

+ **Nouveau groupe de machine**

LISTE DES GROUPES DE MACHINE
[-] [+]

| Groupes de machine | horaires | Interdictions | politique optionnelle | suppression |
|--|----------|---------------|-----------------------|-------------|
| secretariat plage IP: 10.21.11.15 à 10.21.11.18 sur l'interface eth1 | | Jamais | Défaut | ✗ |

DEFINIR DES PLAGES HORAIRES D'OUVERTURE POUR LE GROUPE SECRETARIAT
✗ Fermer

Début de plage

Fin de plage

Choix du (des jours)

lundi
 mardi
 mercredi
 jeudi
 vendredi
 samedi
 dimanche

Validation

OU

Copier les horaires d'un autre groupe

Validation

Validation

Navigation interdite
 Navigation autorisée

lundi

o01h02h03h04h05h06h07h08h09h10h11h12h13h14h15h16h17h18h19h20h21h22h23ho

Autorisation de navigation web:
de 8:00 à 12:00

mardi

o01h02h03h04h05h06h07h08h09h10h11h12h13h14h15h16h17h18h19h20h21h22h23ho

Autorisation de navigation web:
de 8:00 à 12:00

mercredi

Les plages horaires définies s'affichent (la croix permet de supprimer la plage).

GRUPE DE MACHINE

[+ Nouveau groupe de machine]

LISTE DES GROUPES DE MACHINE [-] [+]

| Groupes de machine | horaires | Interdictions | politique optionnelle | suppression |
|--|----------|---------------|-----------------------|-------------|
| secretariat plage IP: 10.21.11.15 à 10.21.11.18 sur l'interface eth1 | | Jamais | Défaut | ✖ |

DEFINIR DES PLAGES HORAIRES D'OUVERTURE POUR LE GROUPE SECRETARIAT ✖ Fermer

Début de plage: 0:00 Fin de plage: 0:00

Choix du (des) jours:

OU

Copier les horaires d'un autre groupe:

■ Navigation interdite
■ Navigation autorisée

lundi

o 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h o

■ 00h-07h ■ 08h-12h ■ 13h-18h ■ 19h-23h

Autorisation de navigation web:
 de 8:00 à 12:00
 de 13:30 à 18:30

mardi

o 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h o

■ 00h-07h ■ 08h-12h ■ 13h-18h ■ 19h-23h

Autorisation de navigation web:
 de 8:00 à 12:00
 de 13:30 à 18:30

Affichage des plages horaires



Sans plage horaire définie, la navigation web est interdite tout le temps

La modification des plages horaires est dynamique.

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.

- choisir le groupe dans la liste ;
- valider.



Interdire l'accès au réseau

Pour interdire tout accès réseau à notre groupe de machine, dans la colonne **Interdictions**, choisir **Toute activité réseau**.

Spécifier une politique de filtrage

Il est possible d'associer une politique de filtrage au groupe de machine. Pour cela choisir la politique dans la colonne **politique optionnelle**.

Certaines politiques de filtrage sont fixes :

- modérateur ;
- interdit ;

- mode liste blanche.

D'autres sont configurables :

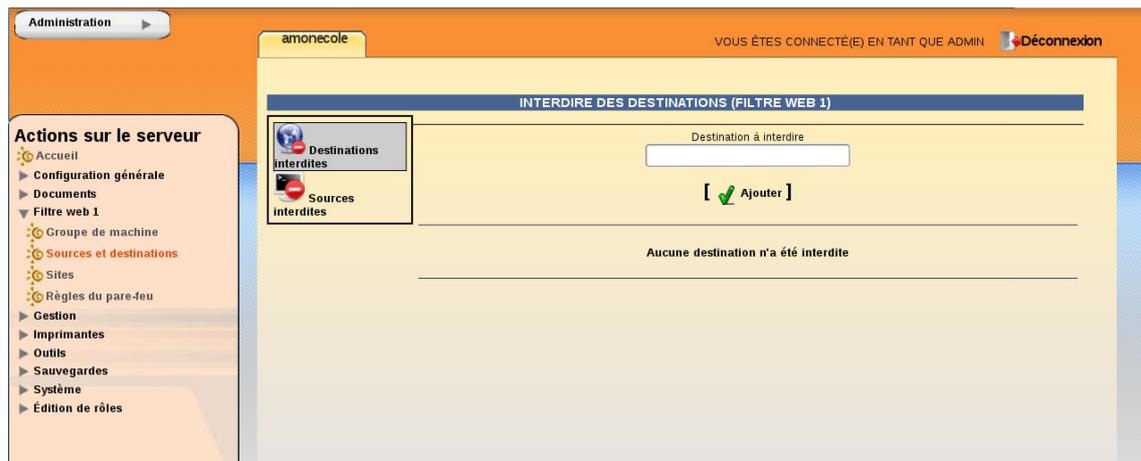
- Défaut ;
- 1 ;
- 2 ;
- 3 ;
- 4.

Supprimer un groupe de machine

Pour supprimer un groupe de machine, cliquez sur la croix en face de votre groupe de machine.

3. Interdire l'accès à un sous-réseau depuis une interface

Dans l'EAD il est possible d'interdire l'accès à un sous-réseau depuis une interface.



Vue d'ensemble pour l'ajout d'une destination à interdire

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut **Filtre web 1**. Puis sélectionner **Sources et destinations** et enfin **Destinations interdites**.

Pour interdire une destination il faut :

- définir le sous-réseau (ou le poste) de destination ;
- choisir l'interface source depuis laquelle interdire l'accès (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné).

Nommage des filtres dans la configuration du filtrage web

► Configuration du filtrage web (cf. Onglet Dansguardian : Configuration du filtrage web) [p.10]

Interdire l'accès au sous-réseau 10.121.11.0/255.255.255.0 depuis l'interface admin (eth1)

Ajout d'une destination à interdire

Soit l'interface eth1 sur la zone de filtre web 1.

- Saisir `10.121.11.0/255.255.255.0` dans **Destinations à interdire** ;
- Choisir `admin (eth1)` dans la liste **Interface associée à l'adresse** ;
- Cliquer sur **Ajouter**.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des destinations interdites. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut **Filtre web 1**. Puis sélectionner **Sources et destinations** et enfin **Destinations interdites**.

Suppression d'une destination interdite

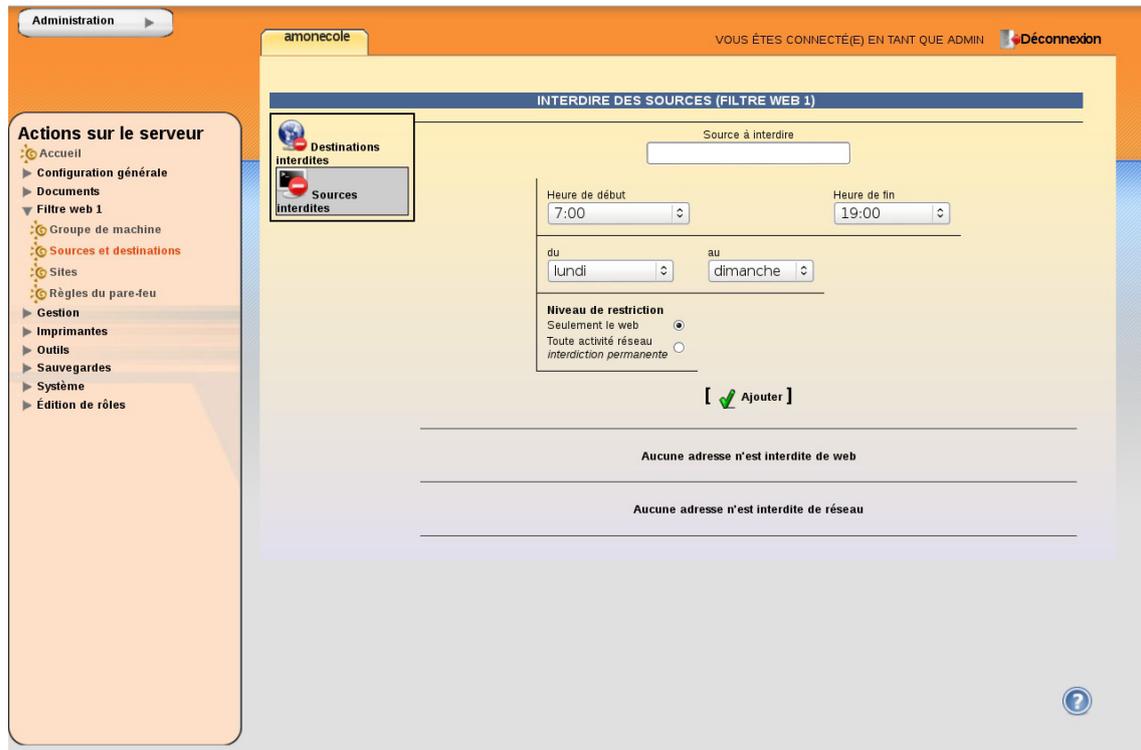
- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur **Supprimer**.

Les destinations interdites sont écrites dans :

```
/usr/share/ead2/backend/tmp/dest_interdites<num_instance>.txt
```

4. Interdire ou restreindre l'activité d'un sous-réseau

Dans l'EAD il est possible d'interdire l'accès web en fonctions de plages horaires ou d'interdire l'activité à tout un sous-réseau .



Vue d'ensemble pour l'ajout d'une source à interdire

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut **Filtre web 1** . Puis sélectionner **Sources et destinations** et enfin **Sources interdites** .

Les paramètres à saisir sont :

- la Source à interdire : le sous-réseau (ou poste) sur lequel les restrictions doivent être appliquées ;
- l'Interface associée à l'adresse (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné) ;
- les plages horaires et journalières de la restriction (restriction web uniquement) ;
- le Niveau de restriction : web ou réseau.

Nommage des filtres dans la configuration du filtrage web

Configuration du filtrage web (cf. Onglet Dansguardian : Configuration du filtrage web) [p.10]

Interdire l'accès web depuis le sous-réseau 10.21.11.0/255.255.255.0 provenant de l'interface eth1 tous les jours entre minuit et 6 heures du matin

Ajout d'une source à interdire

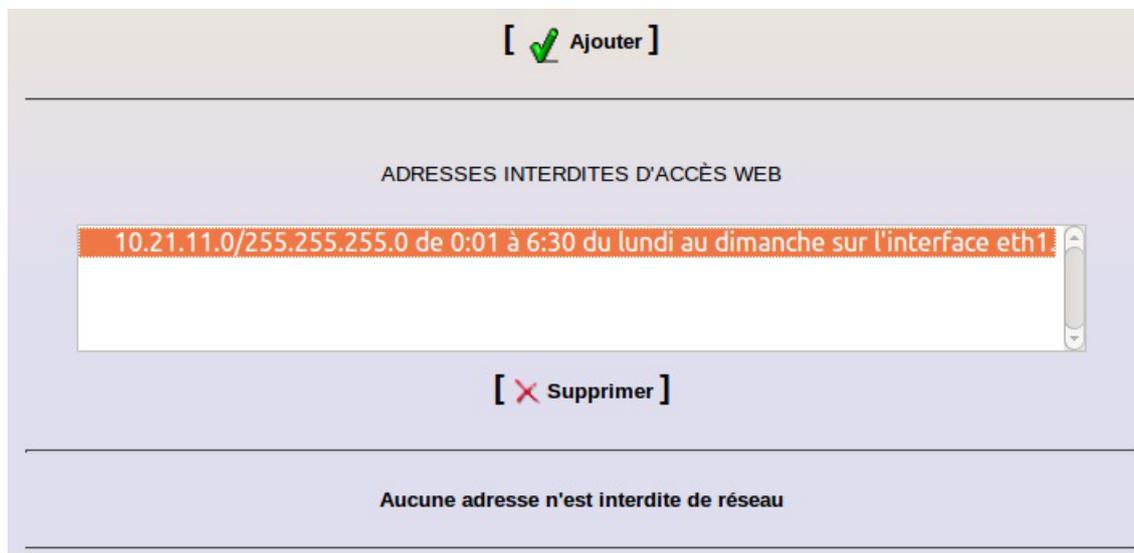
Soit l'interface eth1 sur la zone de filtre web 1 :

- Saisir `10.121.11.0/255.255.255.0` dans `Source à interdire` ;
- Choisir `admin (eth1)` dans la liste `Interface associée à l'adresse` ;
- Sélectionner `0:01` comme heure de début et `06:30` comme heure de fin ;
- Sélectionner les jours : du lundi au dimanche ;
- Choisir `Seulement le web` comme `Niveau de restriction` ;
- Cliquer sur `Ajouter`.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des postes interdits de navigation web. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Sources interdites`.



Suppression d'une source interdite

- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur .



Les sources interdites d'accès web sont écrites dans :

`/usr/share/ead2/backend/tmp/horaire_ip<num_instance>.txt`

Les sources interdites d'accès réseau sont écrites dans :

`/usr/share/ead2/backend/tmp/poste_all<num_instance>.txt`

5. Bases de filtres optionnels

Les bases de filtres proposées sur le module Amon sont des copies de celles gérées par l'université de Toulouse 1 Capitole : <http://cri.univ-tlse1.fr/blacklists> [<http://cri.univ-tlse1.fr/blacklists/>].



L'université de Toulouse 1 Capitole diffuse depuis de nombreuses années une liste noire d'URLs, gérée par Fabrice Prigent afin de permettre un meilleur contrôle de l'utilisation d'Internet.

Les bases, publiées sous licence d'utilisation Creative Commons by-sa 4.0 [<http://creativecommons.org/licenses/by-sa/4.0/deed.fr>], sont largement utilisées par les écoles et sont également intégrées dans un grand nombre d'outils libres ou commerciaux, en complément d'autres listes.

Les bases sont mises à jour 2 à 3 fois par semaine en fonction des disponibilités du mainteneur, elles peuvent être enrichies grâce à un formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Ces bases de filtres proposent des catégories avec des listes de domaines et d'URL triés par catégories.

Les sites référencés dans les catégories `adult` et `redirector` sont interdits d'office.

Les autres bases de filtres sont activables depuis l'interface EAD.

L'activation se fait :

- par filtre web ;
- par politique de filtrage.

La mise à jour des bases de filtres est lancée automatiquement toutes les nuits

Un rapport de mise à jour est disponible sur la page d'accueil de l'EAD.

LISTE DE SITES INTERDITS

Dernière mise à jour de la liste de sites interdits :
 Mise à jour le 16.11.2012 à 02:38 :

[+ Afficher le rapport](#)

Rapport de mise à jour des bases de filtres

➤ **Pour activer la catégorie "agressif" sur toute la zone de configuration 1**

Dans **Filtre 1 / Sites / Filtres** :

- cocher les quatre cases (pour les quatre politiques de filtrage de la zone 1) ;
- valider.

ACTIVATION DES FILTRES FACULTATIFS SUR LA ZONE DE CONFIGURATION 1

| | FILTRES | DÉFAUT | 1 | 2 | 3 |
|-------------------------------------|------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | tous aucun | tous aucun | tous aucun | tous aucun |
| <input checked="" type="checkbox"/> | contenus agressifs (xenophobie...) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | audio/video | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | téléphones mobiles, sonneries | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | radios en ligne | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | drogue | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | mail et chat | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | webmail les plus connus | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | jeux de hasard et d'argent | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | jeux en ligne | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | hacking (piratage) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | phishing | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | warez (piratage) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | triche aux examens | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | bandeaux publicitaires | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | divers (humour...) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | utilisation de proxy distants | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | proxy spécifiques | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

[✓ valider]

Activation de filtres optionnels

➤ Pour activer une catégorie seulement pour une politique de filtrage^[p.67], seule la case correspondant à la politique doit être cochée.

ACTIVATION DES FILTRES FACULTATIFS SUR LA ZONE DE CONFIGURATION 1

| FILTRES | DÉFAUT | 1 | 2 | 3 |
|------------------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|
| | tous aucun | tous aucun | tous aucun | tous aucun |
| contenus agressifs (xenophobie...) | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| audio/video | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| téléphones mobiles, sonneries | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| radios en ligne | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| drogue | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| mail et chat | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| webmail les plus connus | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| jeux de hasard et d'argent | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| jeux en ligne | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| hacking (piratage) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| phishing | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| warez (piratage) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| triche aux examens | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| bandeaux publicitaires | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| divers (humour...) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| utilisation de proxy distants | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| proxy spécifiques | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

[Validier]

Restreindre l'activation d'un filtre à une politique

La commande suivante permet de forcer la mise à jour les bases de filtrages :

```
/usr/share/eole/Maj-blacklist.sh
```

La liste des bases de filtres d'interdiction gérées sur le module EOLE est fournie par le fichier : `/usr/share/ead2/backend/config/filtres-opt`.

La modification des filtres optionnels activés impactent les fichiers suivants :

- `/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedsitelist`
- `/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedurllist`

Sur le module *AmonEcole*, ces fichiers sont dans le conteneur **reseau**.

6. Filtrage syntaxique

Configuration du filtrage syntaxique

Le module Amon filtre dynamiquement les pages web grâce au filtrage syntaxique^[p.67].

Ce système de pondération par mot clef se base sur le fichier `/var/lib/blacklists/meta/weighted` qui est mis à jour toutes les nuits, à partir des données gracieusement gérées et mises à disposition par l'académie de Rouen.

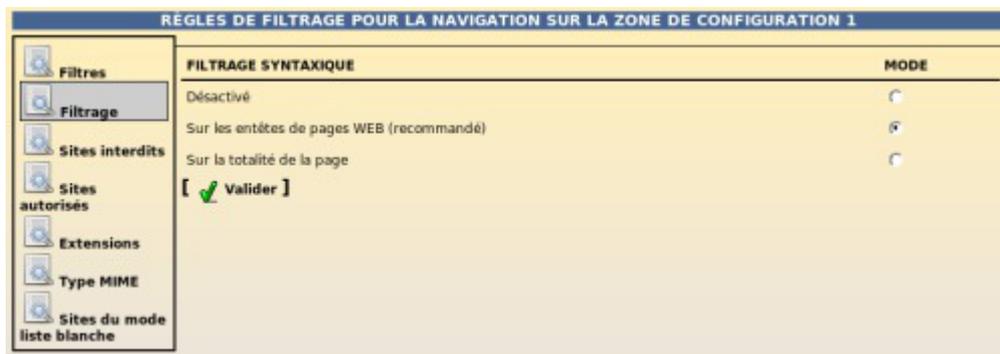
Dans l'EAD, le filtrage syntaxique peut être :

- sur les balises méta^[p.66] (par défaut) ;

- sur la page entière ;
- désactivé.

Il est possible de régler ce filtrage pour chaque zone de configuration.

Pour modifier la configuration, aller dans **Filtre web 1 / Filtrage**.



Configuration du mode de filtrage web pour la zone de configuration 1

Le mode de filtrage syntaxique choisi est enregistré dans le fichier :

```
/var/lib/eole/config/filtrage-contenu<num_instance>
```

Mode "safe search" dans les moteurs de recherche

Le proxy utilise un système de réécriture des *URL* afin que le mode "safe search" des principaux moteurs de recherche et sites d'hébergement de vidéos soit activé automatiquement.

<http://www.google.com/support/websearch/bin/answer.py?answer=510>

Certaines fonctionnalités de recherche avancée ont également été désactivées afin de limiter la charge du serveur.

Filtrage PICS

Le filtrage PICS (<http://www.w3.org/PICS>) ne s'active automatique que si le filtrage syntaxique est configuré sur la page entière.

7. Interdire et autoriser des domaines

Interdire des domaines et des URL

Il est possible de compléter la liste de sites interdits (liste noire^[p.67]) en ajoutant des domaines ou des URL sur la liste personnalisée de domaines interdits.

Cette liste est applicable :

- a une zone entière ;
- de manière plus fine sur une seule politique de filtrage.

Le formulaire qui permet d'interdire des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, **Filtre web 1** par défaut puis **Sites / Domaines interdits**.

Nommage des filtres dans la configuration du filtrage web : Configuration du filtrage web (cf. Onglet Dansguardian : Configuration du filtrage web) ^[p.10]

GESTION DES DOMAINES INTERDITS SUR 'FILTRE WEB 1'

Veuillez entrer un nom de domaine à interdire

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

| | | | |
|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Défaut | 1 | 2 | 3 |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

[Valider]

MODIFIER LA LISTE DES DOMAINES INTERDITS.

| Site | Défaut | 1 | 2 | 3 |
|---------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| www.black1.fr | tous <u>aucun</u> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| www.black2.fr | tous <u>aucun</u> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

[Valider]

Interdiction de domaines pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines interdits sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/domains`

Sur un module AmonEcole, ces fichiers sont dans le conteneur `reseau`.

Personnalisations académiques

Des listes de domaines et d'URL peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/var/lib/blacklists/dansguardian<num_instance>/common/domains_acad`
- `/var/lib/blacklists/dansguardian<num_instance>/common/urls_acad`

Il est possible de signaler des domaines à interdire qui amélioreront les performances et la qualité des bases nationales de domaines interdits.

Pour cela, aller dans **Outils / Signalements**.

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]

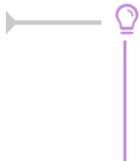
[Accès direct au formulaire de déclaration de site]

Vue du formulaire de signalement

Une procédure automatisée a été mise en place afin de recueillir les propositions de domaine à interdire dans les bases nationales.

Un ensemble de moteurs logiciels analysera l'URL soumise et une vérification visuelle aura lieu si besoin avant l'incorporation du domaine dans les listes de domaines interdits.

La participation de chacun à ce processus permet d'améliorer les bases nationales et leur performance et ce afin que chacun puisse en bénéficier.



Il est également possible de faire un signalement directement auprès de l'université de Toulouse 1 Capitole grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Autoriser des domaines et des URL

Il est possible de forcer l'autorisation de domaines ou d'URL (liste blanche^[p.67]) en les ajoutant à la liste des domaines autorisés.

Cette liste de domaines s'applique :

- sur une zone de filtre web portant le nom du filtre choisi dans l'interface de configuration du module ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans **Filtre web 1 / Sites / Sites autorisés**

Le formulaire qui permet d'autoriser des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, **Filtre web 1** par défaut puis **Sites / Domaines autorisés**.

GESTION DES DOMAINES AUTORISÉS SUR 'FILTRE WEB 1'

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 |
|---------------|--|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| www.white1.fr | tous aucun | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| www.white2.fr | tous aucun | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

[Valider]

Autorisation de sites pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines autorisés sont écrits dans :

```
/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/whites
```

Sur le module AmonEcole, ces fichiers sont dans le conteneur `reseau`.

8. Interdire des extensions et des types MIME

Interdire des extensions

Il est possible d'interdire des extensions, ainsi si l'URL de navigation pointe vers un fichier portant cette extension, l'accès sera interdit.

Cette interdiction s'applique :

- sur une zone de configuration ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans **Filtre web 1 / Sites / Extensions** .

| MODIFIER LA LISTE DES EXTENSIONS INTERDITES | | | | | |
|---|------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| extensions | | Défaut | 1 | 2 | 3 |
| .ext1 | TOUS_AUCUN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| .ext2 | TOUS_AUCUN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Interdiction d'extensions pour les quatre politiques de la zone de configuration 1

Les extensions interdites sont écrites dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/extensions`

Sur AmonEcole, ces fichiers sont dans le conteneur reseau .

Interdire des types MIME

Il est possible d'interdire des types MIME^[p.68]. Cette interdiction fonctionne comme celle des extensions.

Cette interdiction s'applique :

- sur une zone de configuration ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans **Filtre web 1 / Sites / type MIME** .

| MODIFIER LA LISTE DES TYPES MIME INTERDITS. | | | | | |
|---|------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| types MIME | | Défaut | 1 | 2 | 3 |
| Données composites avec mentions d'octets | TOUS_AUCUN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Données composites choix | TOUS_AUCUN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Interdiction de types MIME pour les quatre politiques de la zone de configuration 1

Les types MIME interdits sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/types_mime`

Sur AmonEcole, ces fichiers sont dans le conteneur reseau .

9. Politique liste blanche

Le politique liste blanche^[p.67] permet de restreindre la navigation web à une liste de sites.

Le principe est "tout est interdit sauf".

Restreindre la navigation au site Wikipédia pour les utilisateurs en mode liste blanche de la zone nommée par défaut "Filtre web 2"

Dans Filtre web 2 / Sites / Sites du mode liste blanche

- ajouter un domaine avec ou sans sous-domaine (exemple fr.wikipedia.org) dans le champ Ajouter un site au mode liste blanche ;
- cliquer sur le bouton Valider.

Les utilisateurs et les postes ayant pour politique de filtrage "mode liste blanche" ne pourront naviguer que sur le site ajouté à la liste blanche (exemple Wikipédia).

Ajout d'un site dans la liste blanche

Supprimer un site de la liste blanche

- sélectionner le site dans la liste déroulante SITES DU MODE LISTE BLANCHE ;
- cliquer sur la bouton Valider.

Suppression d'un site dans la liste blanche

Les sites de la liste blanche sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/site_liste_blanche`

Sur un module AmonEcole, ces fichiers sont dans le conteneur reseau.

Chapitre 4

Exceptions sur la source ou la destination

Par défaut, tous les accès à des sites nécessitent une authentification (si elle est active) et toutes les machines du réseau doivent s'identifier. Mais certains systèmes ou logiciels doivent pouvoir se mettre à jour de façon transparente.

Par ailleurs, le proxy conserve une version des pages téléchargées en cache pour limiter la consommation réseau. Ce comportement n'est pas adapté à tous les sites.

Pour les sites comportant des données sensibles, il est nécessaire de s'assurer que des données relatives à la navigation sur ce domaine ne soient pas placées dans le cache du serveur.

Certaines machines peuvent également avoir besoin de naviguer avec des données provenant directement du site consulté.

Certains postes clients ou serveurs du réseau ont besoin d'effectuer des mises à jour automatiquement, les sites de mise à jour doivent être accessibles sans authentification.

Certaines machines peuvent également avoir besoin de naviguer sans être authentifiées.

Pour cela, il existe deux mécanismes :

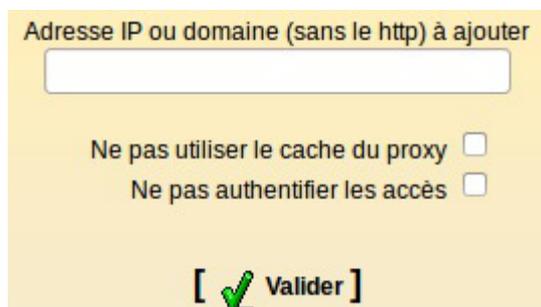
- ne pas utiliser de cache ou d'authentification pour certains sites (destination) ;
- ne pas utiliser de cache ou d'authentification pour certaines machines locales (source).

Pour paramétrer les destinations et les sources qui n'utiliseront pas le cache ou l'authentification lors de la navigation il faut se rendre dans **Configuration générale** puis **Cache et Authentification** de l'interface EAD du module.

Cache et authentification de la destination

Dans **Configuration générale** / **Cache et Authentification** / **Destinations** :

- entrer l'adresse IP ou le nom du domaine ;
- cocher authentification et/ou cache ;
- valider.



Adresse IP ou domaine (sans le http) à ajouter

Ne pas utiliser le cache du proxy

Ne pas authentifier les accès

[ Valider]

Ajout d'une destination à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

| Destination | Cache | Authentification |
|-------------|-------|------------------|
| 10.121.58.5 | ✗ | ✗ |
| ac-dijon.fr | ✗ | ✗ |
| scribe | | ✗ |

Listes des destinations à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Cache et authentification de la source

Dans Configuration Générale / Cache et Authentification / Sources :

- entrer l'adresse IP ou réseau
- cocher authentification et/ou cache ;
- valider.

Machine ou réseau source à ajouter

Ne pas utiliser le cache du proxy

Ne pas authentifier les accès

[✓ Valider]

Ajout d'une source à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

| Source | Cache | Authentification |
|---------------|-------|------------------|
| 10.121.58.5 | ✗ | ✗ |
| 10.21.58.10 | ✗ | ✗ |
| 172.16.0.0/24 | | ✗ |
| 172.16.0.6 | ✗ | ✗ |

Listes des sources à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Personnalisations académiques

Des listes de sites et d'adresses académiques peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/etc/squid3/domaines_noauth_acad` : liste de destinations à ne pas authentifier ;
- `/etc/squid3/domaines_nocache_acad` : liste de destinations pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/src_noauth_acad` : liste de sources à ne pas authentifier ;
- `/etc/squid3/src_nocache_acad` : liste de sources pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/domaines_nopeerproxy` : liste de destinations pour lesquelles on n'utilise pas le proxy père.

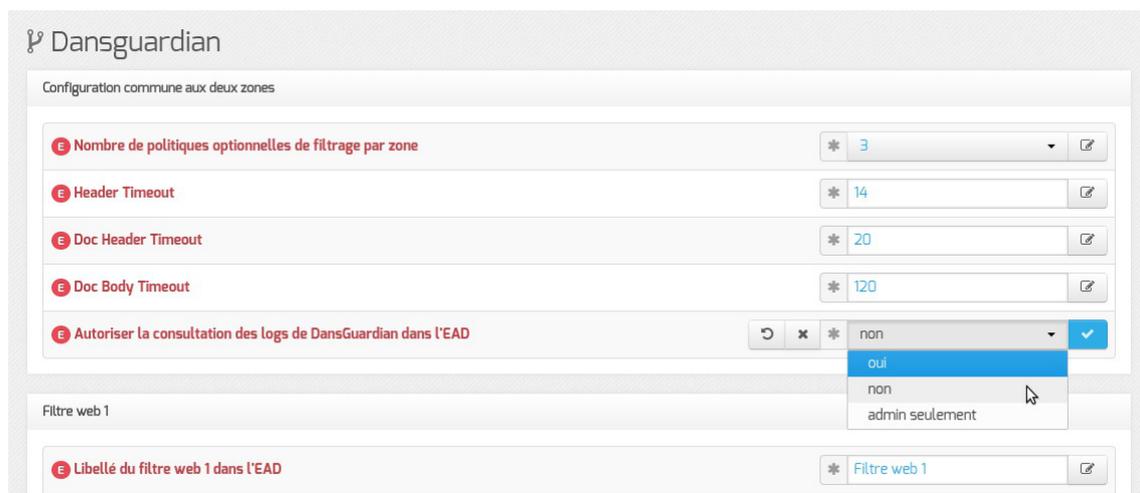
Chapitre 5

Observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage Dansguardian.

Configuration

L'accès à cet outil se paramètre dans l'interface de configuration du module, dans l'onglet expert : **Dansguardian**.



Paramétrage de l'accès à la consultation des logs

La question **Autoriser la consultation des logs de Dansguardian dans l'EAD** propose plusieurs options :

- **oui** : accès autorisé pour les utilisateurs EAD possédant les actions `navigation_visit_admin` et/ou `navigation_visit_pedago` (configuration proposée sur Amon-2.2)
- **non** : accès interdit pour tout le monde, personne ne voit le lien **Visites des sites** (configuration par défaut sur Amon-2.3)
- **admin seulement** : accès autorisé uniquement pour le rôle `admin`.

Consultation

La consultation des visites de site se fait au travers de l'EAD, menu : **Filtre web X/visites des sites**.

Actions sur le serveur

- Accueil
- Configuration générale
- Filtre web proxy 1
- ▼ Filtre web proxy 2
- Groupe de machine
- Sources et destinations
- Visites des sites
- Sites
- Règles du pare-feu
- Outils
- Système
- Édition de rôles

OBSERVATOIRE DES NAVIGATIONS SUR 'FILTRE WEB PROXY 2'

OUTIL DE RECHERCHE = +

[< précédent] [suivant >]

| DATE | LOGIN | URL | IP |
|---------------------|-------|-----------------------------|--------------|
| 2012.10.12 15:21:41 | - | exch-eu.atdmt.com | 172.16.0.202 |
| 2012.10.12 15:21:41 | - | a.rad.msn.com | 172.16.0.202 |
| 2012.10.12 15:21:43 | - | leparc.ac-dijon.fr:443 | 172.16.0.39 |
| 2012.10.12 15:21:43 | - | rad.msn.com | 172.16.0.202 |
| 2012.10.12 15:21:43 | - | a.rad.msn.com | 172.16.0.202 |
| 2012.10.12 15:21:44 | - | m.adnxs.com | 172.16.0.202 |
| 2012.10.12 15:21:44 | - | cm.g.doubleclick.net | 172.16.0.202 |
| 2012.10.12 15:21:44 | - | view.atdmt.com | 172.16.0.202 |
| 2012.10.12 15:21:44 | - | distributif.espace-plus.net | 172.16.0.202 |
| 2012.10.12 15:21:44 | - | by174w.bay174.mail.live.com | 172.16.0.202 |

Les noms des menus (ici : Filtre web proxy 2) sont modifiables dans l'interface de configuration du module (variables `dansguardian_ead_filtre1` et `dansguardian_ead_filtre2`).

Chapitre 6

Outil d'analyse de logs LightSquid

LightSquid est un analyseur de logs pour le proxy/cache Squid^[p.68].

Les statistiques générées manuellement ou automatiquement par cet outil sont consultables dans l'interface EAD.

<http://lightsquid.sourceforge.net/>

Configuration

LightSquid se paramètre dans l'interface de configuration du module, dans l'onglet expert **Squid**. Pour activer les statistiques il faut passer la variable Générer les statistiques Squid automatiquement à oui. Le port par défaut est 8062.



Paramétrage de Lightsquid

La génération des statistiques proxy peut se faire de manière automatique (toutes les nuits) ou manuellement, en exécutant la commande suivante :

```
/usr/share/lightsquid/lightparser.pl
```

La méthode d'anonymisation des statistiques générées est également paramétrable :

- aucune : aucune anonymisation ;
- par IP : n'affiche que les adresses IP ;
- anonyme : entièrement anonyme (remplace par un tiret).

Techniquement, LightSquid fonctionne en mode *cgi* sur un port local (8062 par défaut).

Cela entraîne certaines limitations :

- la ré-authentification nécessaire en mode "pam" ;
- l'accès aux statistiques est impossible depuis un frontend EAD distant.

Consultation

La consultation des statistiques LightSquid se fait au travers de l'EAD, dans le menu **Outils / Statistiques proxy**.

STATISTIQUES SQUID

Les statistiques sont générées une fois par jour.
Pensez à lancer le script /usr/share/lightsquid/lightparser.pl en root sur le serveur.

Accéder aux statistiques

Pour afficher les statistiques il faut cliquer sur le lien [Accéder aux statistiques](#). La navigation se fait dans une nouvelle fenêtre qui demande une authentification. Par défaut, ces statistiques ne sont accessibles que pour le rôle [admin](#), un clic sur le bouton [Connexion](#) sans mot de passe permet de passer à la demande d'authentification pour le compte [root](#).

Une fois connecté la vue initiale propose de naviguer dans les statistiques par date (année, jour, mois), par groupe, par quota dépassé.

Squid rapport d'accès utilisateur Période de travail: Oct 2012

| Calendar | | | | | | | | | | | |
|----------|----|----|----|----|----|----|----|----|----|----|----|
| 2012 | | | | | | | | | | | |
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 |

| Top Sites | Total | Groupe |
|-----------------------|-----------------------|-----------------------|
| ANNEE | ANNEE | ANNEE |
| MOIS | MOIS | MOIS |

| Date | Groupe Utilisateurs | Quota Dépassé | Octets | Moyenne | Hit % |
|-----------------------------|---------------------|---------------|--------|---------|--------------|
| 11 Oct 2012 | grp | 4 | 0 | 6.0 M | 1.5 M 1.27% |
| 10 Oct 2012 | grp | 30 | 8 | 313.0 M | 10.4 M 8.47% |
| 09 Oct 2012 | grp | 81 | 15 | 587.4 M | 7.3 M 3.10% |
| 08 Oct 2012 | grp | 66 | 18 | 702.7 M | 10.6 M 3.48% |
| 07 Oct 2012 | grp | 5 | 1 | 30.0 M | 6.0 M 0.95% |
| 06 Oct 2012 | grp | 4 | 1 | 27.4 M | 6.8 M 1.21% |
| 05 Oct 2012 | grp | 79 | 33 | 5.7 G | 73.4 M 1.92% |
| 04 Oct 2012 | grp | 95 | 50 | 5.9 G | 63.9 M 3.00% |
| 03 Oct 2012 | grp | 51 | 11 | 561.1 M | 11.0 M 1.83% |
| 02 Oct 2012 | grp | 51 | 21 | 1.9 G | 38.4 M 7.52% |
| 01 Oct 2012 | grp | 50 | 22 | 1.7 G | 34.1 M 4.60% |
| Total/Moyenne: | | 46 | 16 | 17.4 G | 24.0 M 3.40% |

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

Consultation au travers de l'EAD

Dans la vue journalière, si la méthode d'anonymisation choisie est par IP, LightSquid n'affiche que les adresses IP utilisées lors de la navigation. Il affiche également le nombre de connexions et le nombre d'octets utilisés. Il est possible d'afficher un rapport sur le top des sites visités et le top des gros fichiers téléchargés dans la journée. Il est possible de repasser à des statistiques journalières par IP.

Squid rapport d'accès utilisateurDate: **02 Jun 2014 (Rafraichir :: 04:00 :: 2 Jun 2014)**[Top Sites](#) Rapport[Gros Fichiers](#) Rapport

| # | Temps | Utilisateur | Real Name | Connexion(s) | Octets | % | Groupe |
|---|-------|------------------------------|-----------|--------------|---------|-------|-------------------|
| 1 | | 172.16.0.6 | ? | 1 211 | 20.8 M | 96.3% | ? |
| 2 | | 172.16.0.129 | ? | 23 | 222 384 | 0.9% | ? |
| 3 | | 172.16.0.126 | ? | 12 | 164 134 | 0.7% | ? |
| 4 | | 172.16.0.134 | ? | 10 | 130 837 | 0.5% | ? |
| 5 | | 172.16.0.128 | ? | 7 | 116 574 | 0.5% | ? |
| 6 | | 10.21.58.10 | ? | 80 | 36 720 | 0.1% | ? |
| 7 | | 172.16.0.135 | ? | 4 | 19 206 | 0.0% | ? |

Vue journalière des statistiques

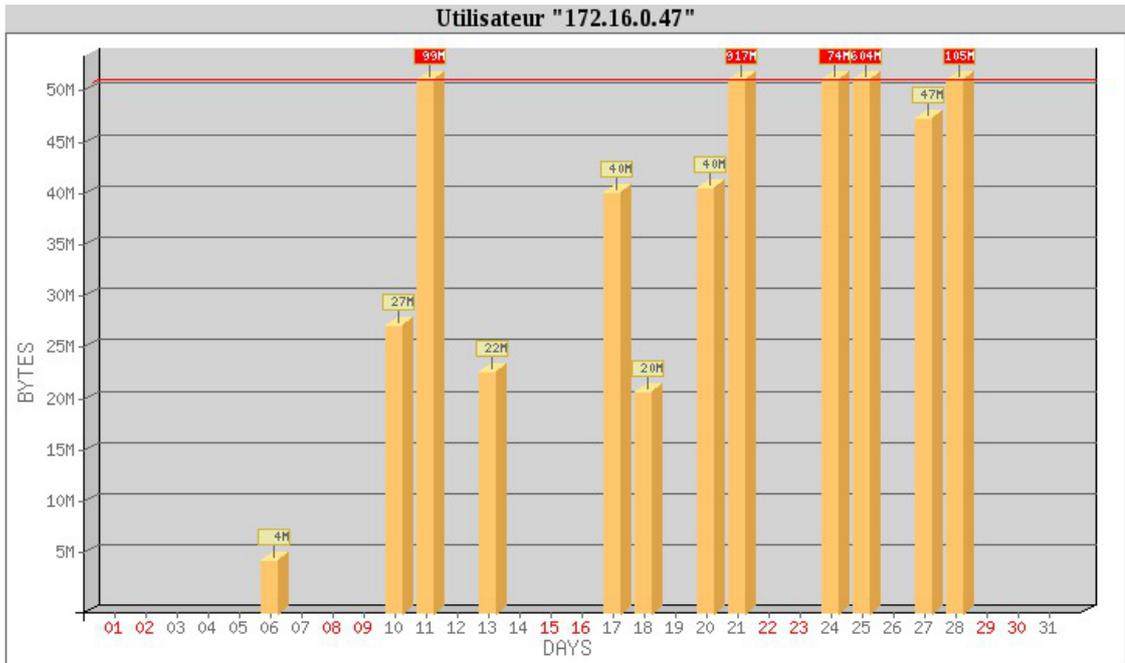
Dans la vue des statistiques journalières par IP, toutes les adresses visitées par l'utilisateur s'affichent avec le nombre de connexions et les octets consommés.

Squid rapport d'accès utilisateurUtilisateur: **172.16.0.6 (?)**Groupe: **?**Date: **02 Jun 2014**[User download "Big Files"](#)

| Total | | 20.8 M | | | |
|--------------|---|---------------|---------------|--------|-------|
| # | Site(s) Accédé(s) | Connexion(s) | Octets | Somme | % |
| 1 | osce106-ilspn25-p.activeupdate.trendmicro.com | 28 | 19.6 M | 19.6 M | 94.3% |
| 2 | osce106-ilspn25wr-p.activeupdate.trendmicro.com | 16 | 869 227 | 20.5 M | 3.9% |
| 3 | 92.51.156.70 | 1 | 152 340 194 | 20.8 M | 1.5% |
| 4 | cyberlib.crdp-poitiers.org:443 | 14 | 25 142 | 20.8 M | 0.1% |
| 5 | ctldl.windowsupdate.com | 1 | 337 | 20.8 M | 0.0% |
| Total | | | 20.8 M | | |

Vue journalière par IP des statistiques

Dans la vue par mois, un clic sur la consommation total des Octets donne un classement de la consommation d'octets par adresse IP. Dans le tableau affiché, un graphe mensuel de la consommation d'octets par adresse IP est disponible.



Graphe mensuel de la consommation d'octets pour une adresse IP

Chapitre 7

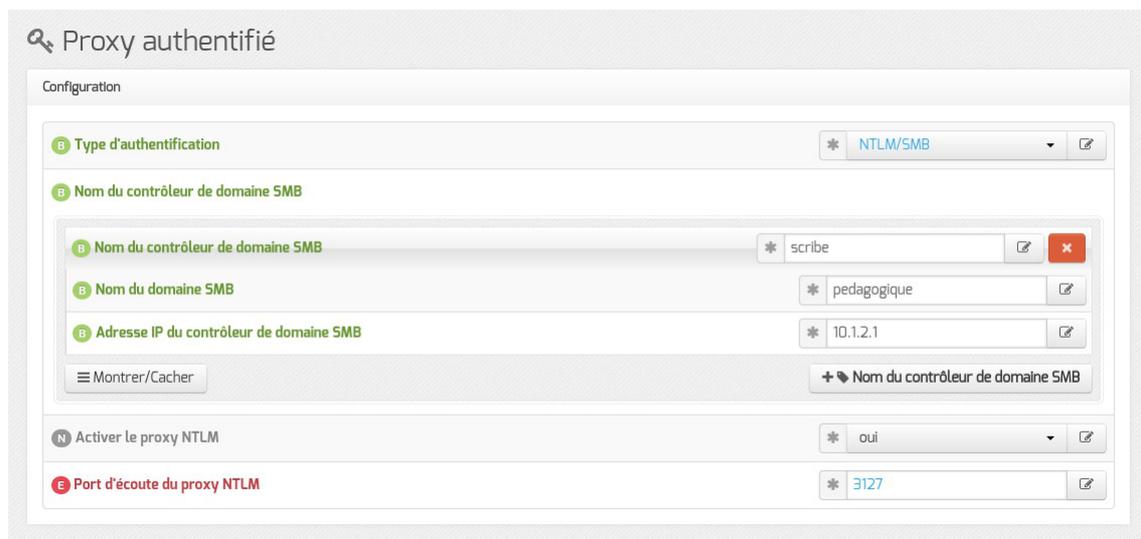
Authentification NTLM/SMB - NTLM/KERBEROS hors domaine

L'authentification NTLM^[p.67] pour des postes hors domaine est facilité par l'utilisation du proxy Cntlm^[p.66].

Installation et activation

Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.

L'activation du service se fait dans l'interface de configuration du module dans l'onglet **Proxy authentifié**. Cet onglet n'est disponible que si l'authentification web a été, elle-même, activée dans l'onglet **Authentification**.



Vue de l'onglet Proxy authentifié dans l'interface de configuration du module

Il faut choisir le type d'authentification sur le proxy NTLM/SMB ou NTLM/KERBEROS.

Ensuite il faut passer la variable Activer le proxy NTLM à oui.

Par défaut, le port de Cntlm est le 3127 mais sa valeur peut être modifiée par le biais de la variable experte intitulée : Port d'écoute du proxy NTLM.

L'activation du service est effective après une reconfiguration du serveur avec la commande :

```
# reconfigure
```



Attention, si l'authentification de type NTLM/SMB est choisie, c'est le premier domaine spécifié qui sera utilisé par Cntlm.

Configuration des clients hors domaine

L'authentification proxy NTLM/SMB et NTLM/KERBEROS nécessite une configuration particulière des postes clients Windows.

Par défaut, il est nécessaire, par exemple, de modifier la base de registre sur le poste Windows Seven.

Mais dans le cas de l'utilisation de Cntlm aucun changement n'est requis dans la base de registre pour les postes hors domaine.

Les postes nomades (hors domaine) doivent utiliser le port [3127](#) pour passer par Cntlm.

Configuration des clients du domaine

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Il est donc nécessaire de configurer correctement les postes du domaine avec, par exemple, ESU^[p.66].

Les postes intégrés au domaine doivent donc utiliser le port [3128](#) pour passer par le proxy .



Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm ([3127](#) par défaut).

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD ^[p.48]

Onglet Proxy authentifié : 5 méthodes d'authentification

Chapitre 8

Configurer la découverte automatique du proxy avec WPAD

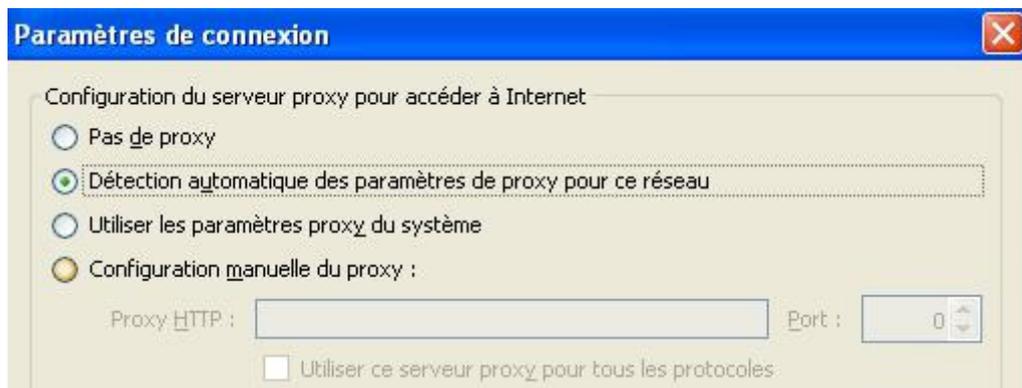
WPAD^[p.68] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essaiera de télécharger le fichier : `wpad.<domaine_local>/wpad.dat` ou le fichier `proxy.pac`.

Dans le cadre d'EOLE, c'est le service Nginx^[p.67] qui se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

⚠ WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-reverseproxy` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.

💡 La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

Dans le cas de l'activation du proxy Cntlm^[p.66] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

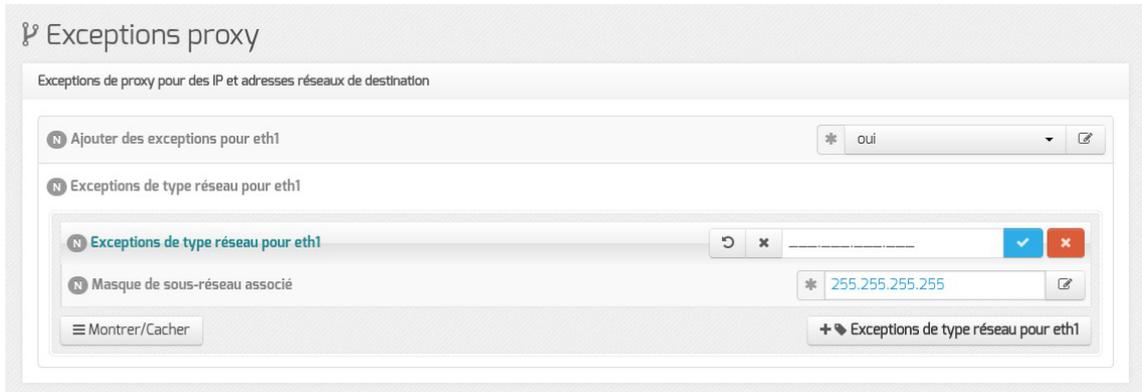
Configuration côté serveur

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des

exclusions dans la configuration automatique du proxy.

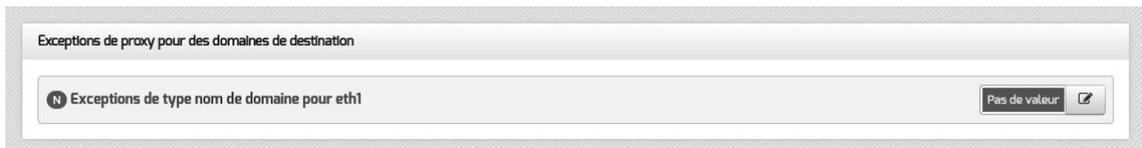
Il est possible de faire des exceptions sur :

- une adresse IP ou une plage d'adresses IP (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour l'adresse IP ;



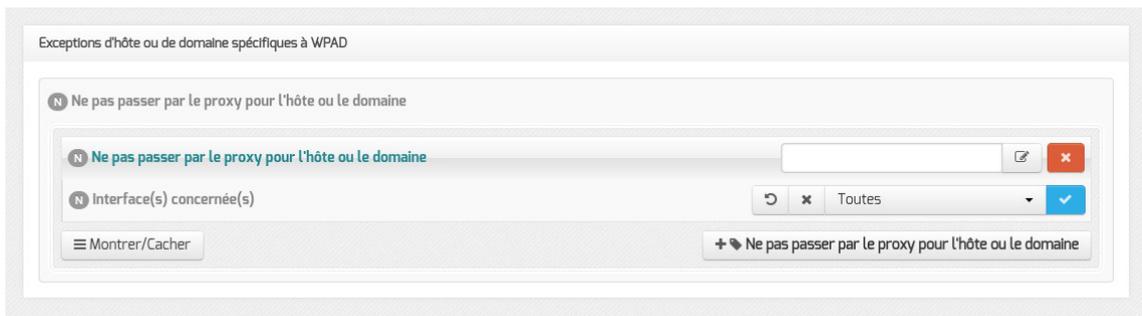
Le bouton Exceptions de type réseau pour eth-n permet d'ajouter plusieurs exceptions sur une même interface.

- un domaine (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour le domaine ;



Il est possible d'ajouter plusieurs exceptions sur une même interface.

- un nom d'hôte (l'exception se fera sur le nom d'hôte et sur le nom d'hôte complet) : Ne pas passer par le proxy pour l'hôte ou le domaine.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton + Ne pas passer par le proxy pour l'hôte ou le domaine permet d'ajouter plusieurs exceptions sur une même interface.



Si le champ Ne pas passer par le proxy pour l'hôte ou le domaine a comme valeur www.ac-monacad.fr, le fichier WPAD.dat généré contiendra la ligne localHostOrDomainIs(host, "www.ac-monacad.fr") qui permet d'exclure simplement des URLs.



Compléments sur Ne pas passer par le proxy pour le domaine (dnsDomainIs) :

<http://findproxyforurl.com/netscape-documentation/#dnsDomainIs>

Compléments sur Ne pas passer par le proxy pour l'hôte ou le domaine (localHostOrDomainIs) :

<http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs>

Chapitre 9

Proxy non configuré dans le navigateur : redirection ou page d'information

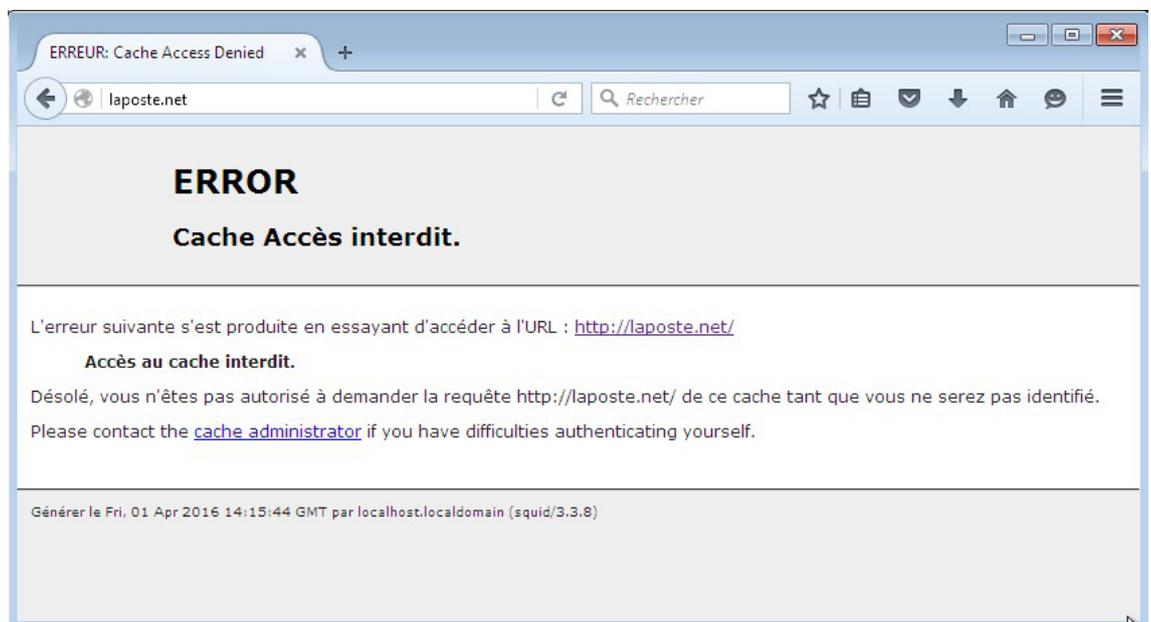
Redirection transparente HTTP sur Amon

Sur le module Amon, les flux HTTP provenant des réseaux internes sont redirigés vers le proxy.

⚠ La redirection transparente ne fonctionne pas avec le protocole HTTPS car il s'agit d'un mode connecté qui ne supporte pas ce genre de manipulation sur les paquets. La redirection est faite uniquement pour obliger les postes à utiliser le proxy.

⚠ La redirection transparente n'est pas mise en place sur le module AmonEcole et ses variantes.

⚠ Si l'authentification du proxy est activée sur l'interface, la redirection fonctionnera mais pas l'authentification et l'utilisateur obtiendra une page d'erreur explicite provenant du logiciel Squid.



Page d'erreur renvoyée par Squid en cas d'erreur d'authentification

En mode expert, les variables `Exceptions de type nom de domaine pour eth1 (proxy_bypass_domain eth1)` et `Exceptions de type nom de domaine pour eth2 (proxy_bypass_domain eth2)` apparaissent dans l'onglet `Exceptions proxy` de l'interface de configuration du module. Elles permettent d'ajouter des exclusions dans la configuration automatique du

proxy.

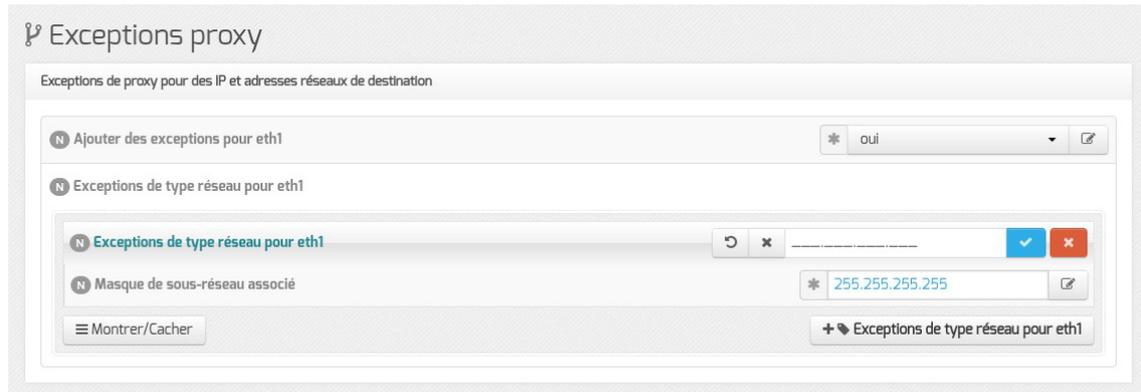
Elles permettent de saisir des adresses de destination pour lesquelles il est possible de ne pas passer par le proxy.



De par ses spécificités, ces variables ne sont pas disponibles sur le module AmonEcole+.

Il est possible de faire des exceptions sur :

- une adresse IP ou une plage d'adresses IP (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour l'adresse IP ;



Le bouton Exceptions de type réseau pour eth1 permet d'ajouter plusieurs exceptions sur une même interface.

- un domaine (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour le domaine ;



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Page d'information renvoyée par Nginx

Sur les modules Amon et AmonEcole, la configuration du logiciel Nginx a été adaptée afin de détecter le cas où le navigateur du client n'a pas été configuré correctement et lui renvoyer un message d'erreur suffisamment explicite.



Page d'erreur renvoyée par Nginx en cas de proxy non configuré



La page d'erreur affichée dans le navigateur peut être personnalisée.

Personnaliser la page renvoyée par Nginx à l'aide d'un patch

La page d'erreur affichée dans le navigateur est un template Creole : `/usr/share/eole/creole/distrib/nginx.no_proxy.html`

Il est possible de le modifier de façon pérenne en utilisant un patch pour Creole.

Il faut copier le template d'origine dans le répertoire `/usr/share/eole/creole/modif/`

```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html /usr/share/eole/creole/modif/nginx.no_proxy.html
```

Il faut éditer, modifier et enregistrer le fichier copié

```
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
```

Puis il faut générer le patch à l'aide de la commande `gen_patch`

```
root@amon:~# gen_patch
```

Le fichier contenant les différences est créé dans le répertoire `/usr/share/eole/creole/patch/`



Les changements prennent effet après la reconfiguration du serveur à l'aide de la commande `reconfigure`

```
root@amon:~# reconfigure
```

La page servie par Nginx contient les modifications :

```
root@amon:~# vim /var/www/index.html
```



```
1 root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html /usr/share/eole/creole/modif/nginx.no_proxy.html
2 root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
3 [...]
```

```

4 root@amon:~# gen_patch
5
6 ** Génération des patches à partir de modif **
7
8 Génération du patch nginx.no_proxy.html.patch
9
10 ** Fin de la génération des patch **
11
12 root@amon:~# ls /usr/share/eole/creole/patch/
13 nginx.no_proxy.html.patch variante
14 root@amon:~# reconfigure
15 [...]
16 root@amon:~# vim /var/www/index.html

```

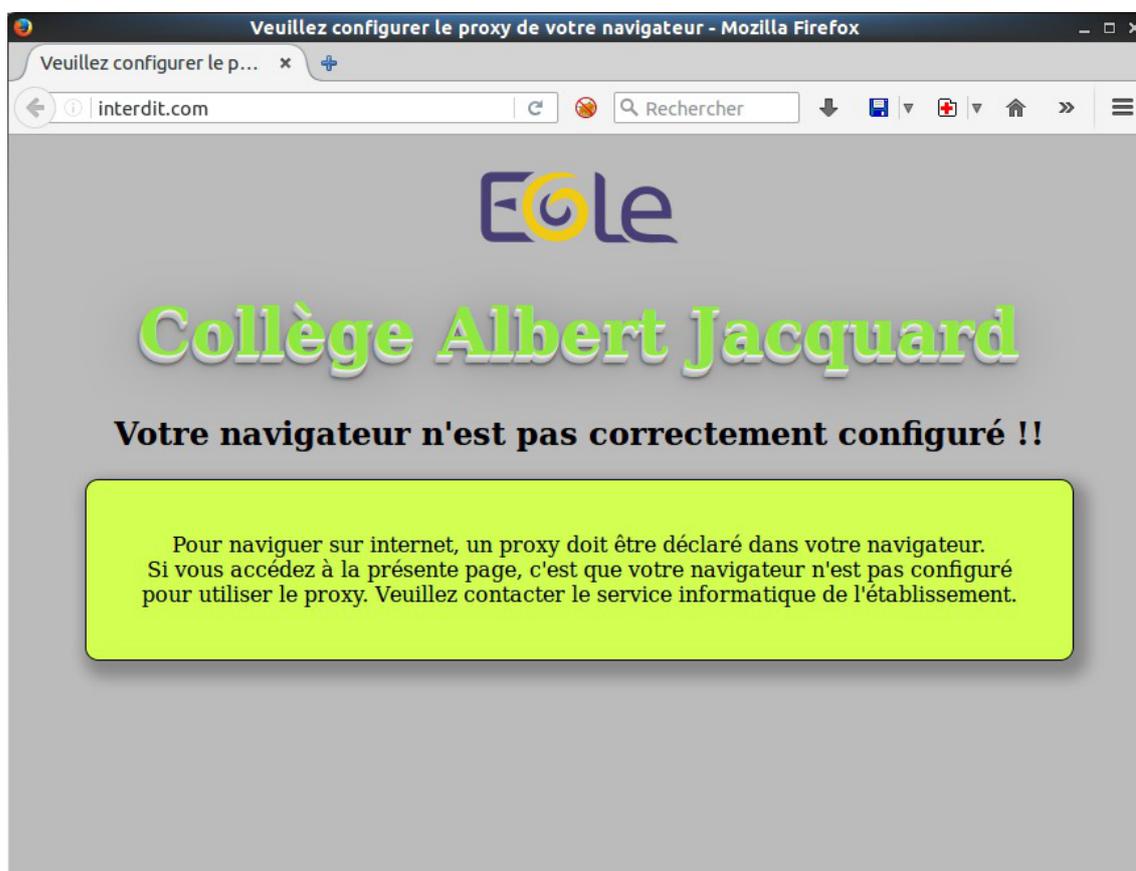
Il est possible d'appeler des variables Creole comme par exemple `%%libelle_etab` et aussi d'ajouter des images en les ajoutant par exemple dans un dossier `/img` dans `/var/www/`.

```

1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
2 <html>
3   <META http-equiv="Content-Type" content="text/html; charset=utf-8;">
4   <head>
5 <title>Veuillez configurer le proxy de votre navigateur</title>
6 <style>
7 .main {
8     background:#bbbbbb;
9     text-align:center;
10 }
11 h1 {
12     /* text-shadow: 0px 0px 7px rgba(0, 0, 0, 0.75);*/
13     color: #91e842;
14     font-size: 50px;
15     text-align:center;
16     text-shadow: 0 1px 0 #eee,
17                 0 2px 0 #e5e5e5,
18                 -1px 3px 0 #C8C8C8,
19                 -1px 4px 0 #C1C1C1,
20                 -2px 5px 0 #B9B9B9,
21                 -2px 6px 0 #B2B2B2,
22                 -2px 7px 2px rgba(0,0,0, 0.6),
23                 -2px 7px 8px rgba(0,0,0, 0.2),
24                 -2px 7px 45px rgba(0,0,0, 0.4);
25 }
26 .message {
27     top:25%;
28     text-align:center;
29     margin-left: 50px;
30     margin-right: 50px;
31
32     padding: 40px;
33     background: #d2ff52;
34     border: 1px solid #000000;
35
36     border-radius: 10px;
37     -moz-border-radius: 10px;
38     -webkit-border-radius: 10px;
39
40     box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);

```

```
41     -moz-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
42     -webkit-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
43 }
44 </style>
45 </head>
46 <body class='main'>
47 
48 <h1>%libelle_etab</h1>
49 <h2>Votre navigateur n'est pas correctement configuré !!</h2>
50 <div class="message">Pour naviguer sur internet, un proxy doit être
    déclaré dans votre navigateur.<br />
51 Si vous accédez à la présente page, c'est que votre navigateur n'est pas
    configuré pour utiliser le proxy. Veuillez contacter le service informatique
    de l'établissement.</div>
52 </body>
53 </html>
54
```



Page d'erreur renvoyée par Nginx en cas de proxy non configuré

Chapitre 10

Paramétrage des postes client

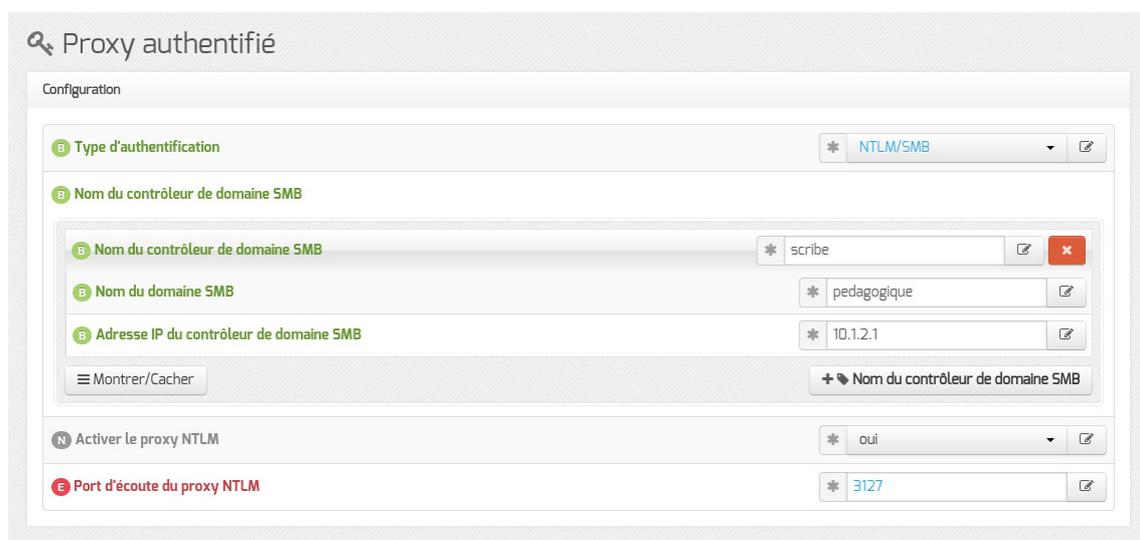
1. Authentification NTLM/SMB - NTLM/KERBEROS hors domaine

L'authentification NTLM^[p.67] pour des postes hors domaine est facilité par l'utilisation du proxy Cntlm^[p.66].

Installation et activation

Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.

L'activation du service se fait dans l'interface de configuration du module dans l'onglet **Proxy authentifié**. Cet onglet n'est disponible que si l'authentification web a été, elle-même, activée dans l'onglet **Authentification**.



Vue de l'onglet Proxy authentifié dans l'interface de configuration du module

Il faut choisir le type d'authentification sur le proxy NTLM/SMB ou NTLM/KERBEROS.

Ensuite il faut passer la variable Activer le proxy NTLM à oui.

Par défaut, le port de Cntlm est le 3127 mais sa valeur peut être modifiée par le biais de la variable experte intitulée : Port d'écoute du proxy NTLM.

L'activation du service est effective après une reconfiguration du serveur avec la commande :

```
# reconfigure
```



Attention, si l'authentification de type NTLM/SMB est choisie, c'est le premier domaine spécifié qui sera utilisé par Cntlm.

Configuration des clients hors domaine

L'authentification proxy NTLM/SMB et NTLM/KERBEROS nécessite une configuration particulière des postes clients Windows.

Par défaut, il est nécessaire, par exemple, de modifier la base de registre sur le poste Windows Seven.

Mais dans le cas de l'utilisation de Cntlm aucun changement n'est requis dans la base de registre pour les postes hors domaine.

Les postes nomades (hors domaine) doivent utiliser le port [3127](#) pour passer par Cntlm.

Configuration des clients du domaine

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Il est donc nécessaire de configurer correctement les postes du domaine avec, par exemple, ESU^[p.66].

Les postes intégrés au domaine doivent donc utiliser le port [3128](#) pour passer par le proxy .

— Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm ([3127](#) par défaut).

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD ^[p.48]

]

Onglet Proxy authentifié : 5 méthodes d'authentification

2. Configurer la découverte automatique du proxy avec WPAD

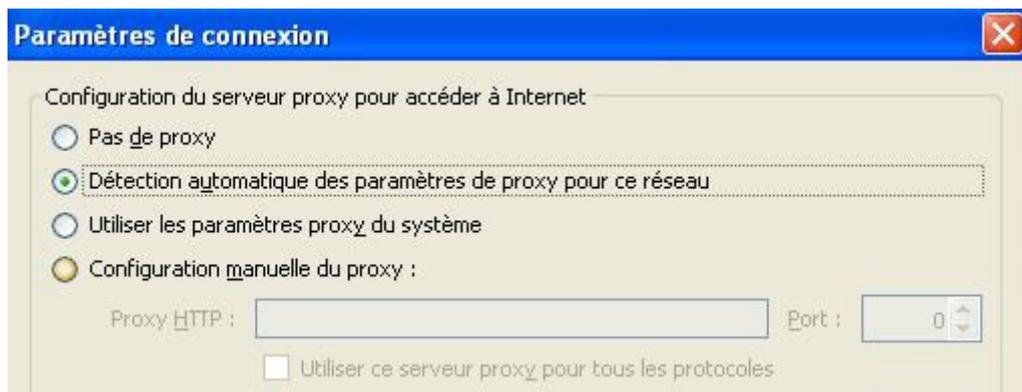
WPAD^[p.68] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essaiera de télécharger le fichier : [wpad.<domaine local>/wpad.dat](#) ou le fichier [proxy.pac](#) .

Dans le cadre d'EOLE, c'est le service Nginx^[p.67] qui se charge de distribuer les fichiers [wpad.dat](#) adaptés à chacun des sous-réseaux.

— WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet [eole-reverseproxy](#) mais n'est fonctionnel que si le paquet [eole-proxy](#) est installé.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.



La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

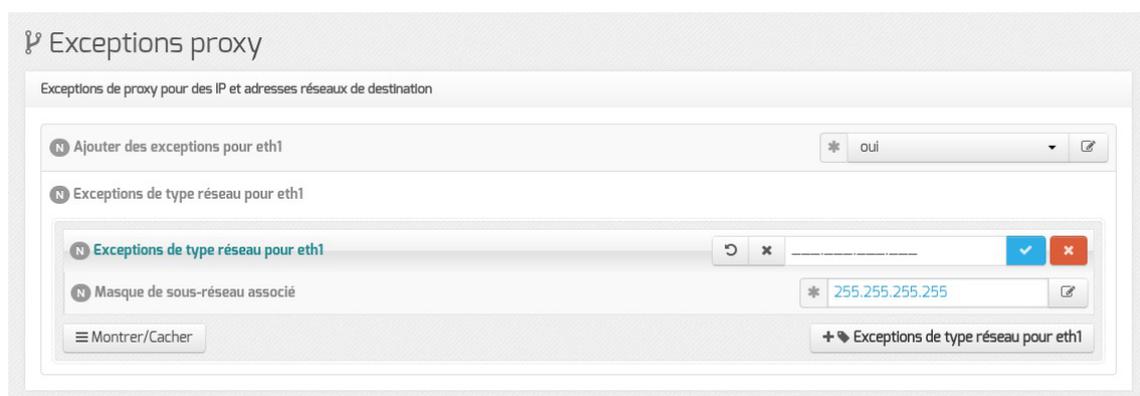
Dans le cas de l'activation du proxy Cntlm^[p.66] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

Configuration côté serveur

Dans l'onglet **Exceptions proxy** de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de faire des exceptions sur :

- une adresse IP ou une plage d'adresses IP (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour l'adresse IP ;



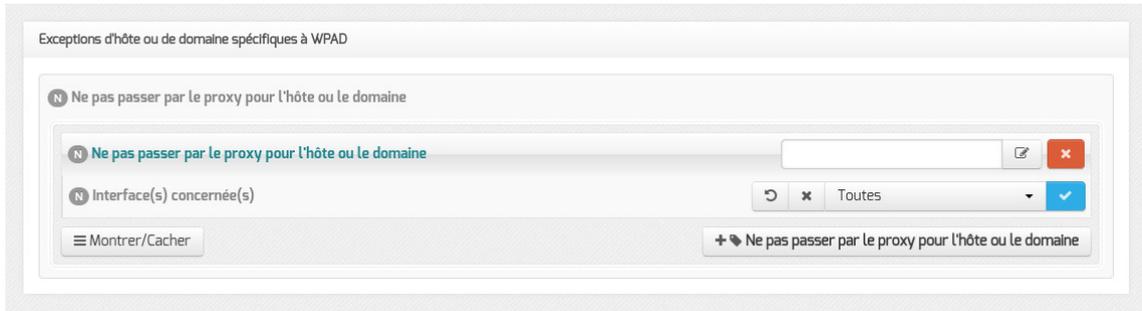
Le bouton **Exceptions de type réseau pour eth-n** permet d'ajouter plusieurs exceptions sur une même interface.

- un domaine (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour le domaine ;



Il est possible d'ajouter plusieurs exceptions sur une même interface.

- un nom d'hôte (l'exception se fera sur le nom d'hôte et sur le nom d'hôte complet) : Ne pas passer par le proxy pour l'hôte ou le domaine.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton + Ne pas passer par le proxy pour l'hôte ou le domaine permet d'ajouter plusieurs exceptions sur une même interface.



Si le champ Ne pas passer par le proxy pour l'hôte ou le domaine a comme valeur www.ac-monacad.fr, le fichier WPAD.dat généré contiendra la ligne `localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.



Compléments sur Ne pas passer par le proxy pour le domaine (dnsDomains) :

<http://findproxyforurl.com/netscape-documentation/#dnsDomains>

Compléments sur Ne pas passer par le proxy pour l'hôte ou le domaine (localHostOrDomains) :

<http://findproxyforurl.com/netscape-documentation/#localHostOrDomains>

3. Proxy non configuré dans le navigateur : redirection ou page d'information

Redirection transparente HTTP sur Amon

Sur le module Amon, les flux HTTP provenant des réseaux internes sont redirigés vers le proxy.



La redirection transparente ne fonctionne pas avec le protocole HTTPS car il s'agit d'un mode

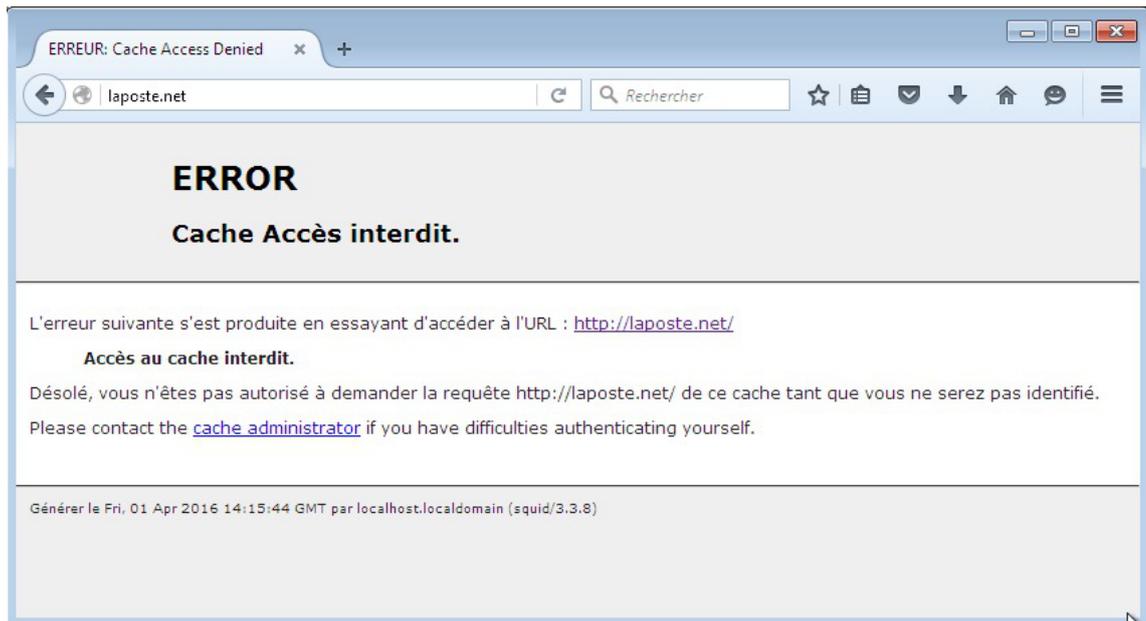
connecté qui ne supporte pas ce genre de manipulation sur les paquets. La redirection est faite uniquement pour obliger les postes à utiliser le proxy.



La redirection transparente n'est pas mise en place sur le module AmonEcole et ses variantes.



Si l'authentification du proxy est activée sur l'interface, la redirection fonctionnera mais pas l'authentification et l'utilisateur obtiendra une page d'erreur explicite provenant du logiciel Squid.



Page d'erreur renvoyée par Squid en cas d'erreur d'authentification

En mode expert, les variables Exceptions de type nom de domaine pour eth1 (proxy bypass domain eth1) et Exceptions de type nom de domaine pour eth2 (proxy bypass domain eth2) apparaissent dans l'onglet Exceptions proxy de l'interface de configuration du module. Elles permettent d'ajouter des exclusions dans la configuration automatique du proxy.

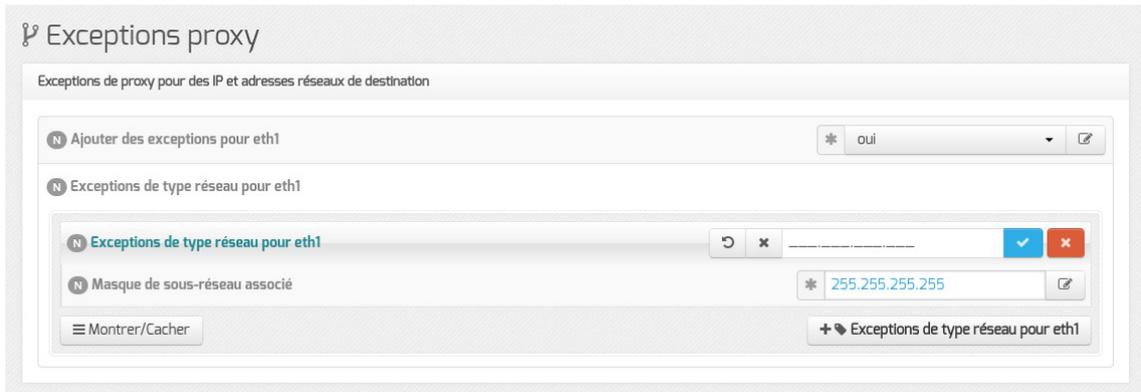
Elles permettent de saisir des adresses de destination pour lesquelles il est possible de ne pas passer par le proxy.



De par ses spécificités, ces variables ne sont pas disponibles sur le module AmonEcole+.

Il est possible de faire des exceptions sur :

- une adresse IP ou une plage d'adresses IP (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour l'adresse IP ;



Le bouton **Exceptions de type réseau pour eth-n** permet d'ajouter plusieurs exceptions sur une même interface.

- un domaine (exception commune à ERA et à WPAD) : Ne pas passer par le proxy pour le domaine ;



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Page d'information renvoyée par Nginx

Sur les modules Amon et AmonEcole, la configuration du logiciel Nginx a été adaptée afin de détecter le cas où le navigateur du client n'a pas été configuré correctement et lui renvoyer un message d'erreur suffisamment explicite.



Page d'erreur renvoyée par Nginx en cas de proxy non configuré



La page d'erreur affichée dans le navigateur peut être personnalisée.

Personnaliser la page renvoyée par Nginx à l'aide d'un patch

La page d'erreur affichée dans le navigateur est un template Creole :
`/usr/share/eole/creole/distrib/nginx.no_proxy.html`

Il est possible de le modifier de façon pérenne en utilisant un patch pour Creole.

Il faut copier le template d'origine dans le répertoire `/usr/share/eole/creole/modif/`

```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html
/usr/share/eole/creole/modif/nginx.no_proxy.html
```

Il faut éditer, modifier et enregistrer le fichier copié

```
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
```

Puis il faut générer le patch à l'aide de la commande `gen_patch`

```
root@amon:~# gen_patch
```

Le fichier contenant les différences est créé dans le répertoire `/usr/share/eole/creole/patch/`



Les changements prennent effet après la reconfiguration du serveur à l'aide de la commande `reconfigure`

```
root@amon:~# reconfigure
```

La page servie par Nginx contient les modifications :

```
root@amon:~# vim /var/www/index.html
```



```
1 root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html
  /usr/share/eole/creole/modif/nginx.no_proxy.html
2 root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
3 [...]
4 root@amon:~# gen_patch
5
6 ** Génération des patches à partir de modif **
7
8 Génération du patch nginx.no_proxy.html.patch
9
10 ** Fin de la génération des patch **
11
12 root@amon:~# ls /usr/share/eole/creole/patch/
13 nginx.no_proxy.html.patch variante
14 root@amon:~# reconfigure
15 [...]
16 root@amon:~# vim /var/www/index.html
```

Il est possible d'appeler des variables Creole comme par exemple `%%libelle_etab` et aussi d'ajouter des images en les ajoutant par exemple dans un dossier `/img` dans `/var/www/`.

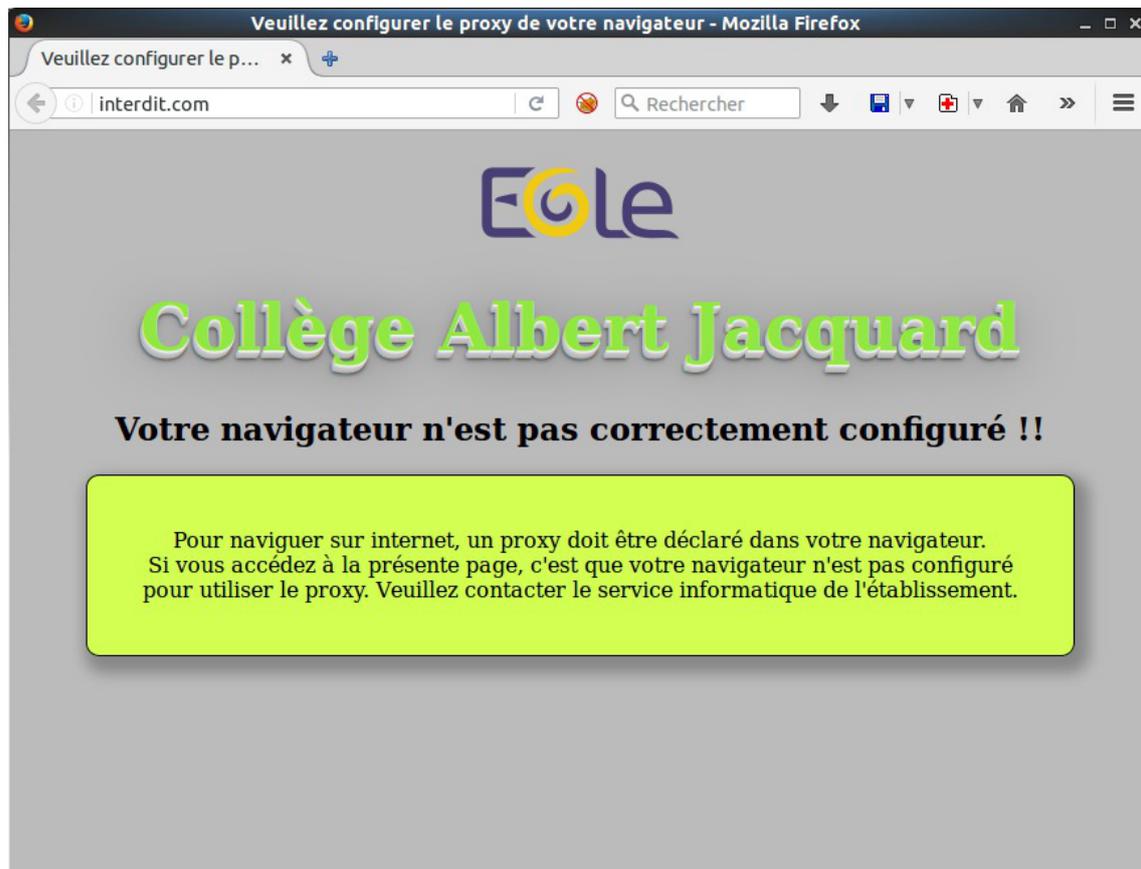


```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
2 <html>
3   <META http-equiv="Content-Type" content="text/html; charset=utf-8;">
4   <head>
5 <title>Veuillez configurer le proxy de votre navigateur</title>
```

```

6 <style>
7 .main {
8     background:#bbbbbb;
9     text-align:center;
10 }
11 h1 {
12     /* text-shadow: 0px 0px 7px rgba(0, 0, 0, 0.75);*/
13     color: #91e842;
14     font-size: 50px;
15     text-align:center;
16     text-shadow: 0 1px 0 #eee,
17                 0 2px 0 #e5e5e5,
18                 -1px 3px 0 #C8C8C8,
19                 -1px 4px 0 #C1C1C1,
20                 -2px 5px 0 #B9B9B9,
21                 -2px 6px 0 #B2B2B2,
22                 -2px 7px 2px rgba(0,0,0, 0.6),
23                 -2px 7px 8px rgba(0,0,0, 0.2),
24                 -2px 7px 45px rgba(0,0,0, 0.4);
25 }
26 .message {
27     top:25%;
28     text-align:center;
29     margin-left: 50px;
30     margin-right: 50px;
31
32     padding: 40px;
33     background: #d2ff52;
34     border: 1px solid #000000;
35
36     border-radius: 10px;
37     -moz-border-radius: 10px;
38     -webkit-border-radius: 10px;
39
40     box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
41     -moz-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
42     -webkit-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
43 }
44 </style>
45 </head>
46 <body class='main'>
47 
48 <h1>%%libelle_etab</h1>
49 <h2>Votre navigateur n'est pas correctement configuré !!</h2>
50 <div class="message">Pour naviguer sur internet, un proxy doit être
déclaré dans votre navigateur.<br />
51 Si vous accédez à la présente page, c'est que votre navigateur n'est pas
configuré pour utiliser le proxy. Veuillez contacter le service informatique
de l'établissement.</div>
52 </body>
53 </html>
54

```



Page d'erreur renvoyée par Nginx en cas de proxy non configuré

4. Synthèse des paramètres proxy à utiliser pour les postes client

Module Amon standard

Sur une installation standard du module Amon, l'adresse du proxy sera l'adresse du serveur Amon sur le réseau. Le port sera celui de DansGuardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau administratif : `adresse_ip_eth1:3128`
- proxy sur le réseau pédagogique : `adresse_ip_eth2:3128`
- proxy sur la DMZ : `adresse_ip_eth3:3128`

Module AmonEcole et ses variantes

Sur une installation standard des modules AmonEcole/AmonHorus, l'adresse du proxy sera l'adresse IP réservée pour le proxy sur le réseau. Le port sera celui de DansGuardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3128`

On notera que, comme sur un module Amon standard, la passerelle est l'adresse du module Amon sur le réseau (`adresse_ip_eth1`). Mais par contre pour le DNS, il faut utiliser la même adresse IP que celle du proxy.

Double authentification

Si la double authentification est configurée, le port à utiliser pour le second proxy sera celui de la troisième configuration DansGuardian (variable `dansguardian_port3` : 3129 par défaut), soit :

- proxy2 sur le réseau eth1 Amon : `adresse_ip_eth1:3129`
- proxy2 sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3129`

Proxy NTLM

Si l'authentification NTLM pour des postes hors domaine est configurée :

- les postes intégrés au domaine doivent continuer à utiliser le port de DansGuardian (3128 par défaut) ;
- les postes nomades (hors domaine) doivent utiliser le port défini par la variable `cntlm_port` (3127 par défaut) pour passer par Cntlm.

Filtrage web désactivé

Si le filtrage web est désactivé, le proxy Squid écoute sur le port 3128 en lieu et place du logiciel de filtrage DansGuardian.

En cas de double authentification, le second proxy répondra sur le port 3129.

Glossaire

| | |
|--|---|
| Balise méta | Information sur la nature et le contenu d'une page web, ajoutée dans l'en-tête de la page HTML. |
| Cntlm | <p>Cntlm proxy d'authentification NTLM rapide écrit en C.</p> <p>Il s'intercale entre le poste client et le proxy. Il oblige l'utilisateur à renseigner son identifiant/mot de passe dans une fenêtre surgissante (popup).</p> <p>Il ouvre une socket en écoute et gère la transmission de chaque requête au proxy parent. Si une connexion au proxy parent est créée à nouveau et authentifiée, la connexion précédente est mise en cache et est réutilisée pour une plus grande efficacité. Cntlm intègre également la redirection transparente de port TCP/IP. Il existe de nombreuses fonctions avancées telles que le support de NTLMv2, la protection de mot de passe, le hachage de mot de passe, etc. Il est peu gourmand en terme de ressources.</p> <p>http://cntlm.sourceforge.net/</p> |
| e2guardian | <p>e2guardian est un fork de DansGuardian. La dernière version stable de DansGuardian est sortie depuis un très long moment (2009) et plus récemment, suite au désengagement du créateur originel Daniel Barron, le projet a été migré sur la plateforme sourceforge et repris en main par un nouveau mainteneur. DansGuardian devait devenir un projet plus communautaire mais après diverses versions alpha le projet n'a pas réellement repris vie.</p> <p>Depuis 2012 le travail a repris pour incorporer toutes les évolutions et corrections proposées par de nombreux contributeurs et le logiciel est publié sous le nom de e2guardian.</p> <p>http://e2guardian.org</p> |
| ESU <i>= Environnements Sécurisés des Utilisateurs</i> | <p>Environnement Sécurisé des Utilisateurs (ESU) est un projet initialement développé par Olivier Adams du CRDP de Bretagne qui est maintenant publié par EOLE et distribué sous licence CeCILL. Cet outil permet aux administrateurs de réseaux en établissement scolaire de définir (très simplement) les fonctions laissées disponibles aux utilisateurs des postes informatiques.</p> <p>ESU propose de nombreuses fonctions :</p> <ul style="list-style-type: none"> • limitation des accès aux paramètres de Windows (panneau de configuration...) ; • définition par salle ou par poste des lecteurs réseaux, icônes du bureau, menu démarrer et limitation des fonctions ; • configuration des imprimantes partagées sur les postes ; • configuration des navigateurs (Internet Explorer et Mozilla |

| | |
|--|--|
| | <p>Firefox) ;</p> <ul style="list-style-type: none"> éditeur de règles permettant de rajouter autant de règles que vous le souhaitez. |
| Filtrage syntaxique | <p>Système de pondération détectant des mots interdits dans une page et lui assignant un score en fonction de la gravité et du nombre de mots détectés. Le proxy bloquera les pages dont le score dépasse un certain seuil.</p> |
| L'expérience à tâtons | <p>Ne pouvant établir avec certitude qui de l'équipe a introduit ce type d'expérience dans la documentation du module Amon en version 2.2, l'équipe dans son intégralité revendique la paternité du concept.</p> |
| Liste blanche | <p>Une liste blanche est une liste d'adresse web autorisées par le proxy.</p> |
| Liste noire | <p>Une liste noire est un document rassemblant les noms d'entités concrètes ou virtuelles jugés indésirables.</p> <p>Dans le contexte informatique une liste noire est une liste d'adresses web indésirables qui seront bloquées par le proxy.</p> |
| Nginx = <i>Engine-x</i> | <p>Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse. Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Donc au lieu d'exploiter une architecture parallèle et un multiplexage temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps. Le traitement de chaque requête est découpé en de nombreuses tâches plus petites ce qui permet de réaliser un multiplexage efficace entre les connexions.</p> <p>Pour tirer parti des ordinateurs multiprocesseurs, le serveur permet de démarrer plusieurs processus. Ce choix d'architecture se traduit par des performances très élevées, une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs Web classiques, tels qu'Apache.</p> |
| NTLM = <i>NT Lan Manager</i> | <p>NTLM est un protocole d'identification utilisé dans diverses implémentations des protocoles réseau Microsoft. Il est aussi utilisé partout dans les systèmes de Microsoft comme un mécanisme d'authentification unique SSO.</p> |
| Politique de filtrage | <p>Une politique de filtrage permet de définir une suite d'autorisation et d'interdiction dans les accès web.</p> |
| Préfixe binaire | <p>Les préfixes binaires (kibi-, mébi-, gibi-, tébi-, pébi- et exbi-) sont souvent utilisés lorsqu'on a affaire à de grandes quantités d'octets. Ils sont dérivés, tout en étant différents, des préfixes du système international (kilo-, méga-, giga- et ainsi de suite). La raison d'être de ces préfixes binaires est d'éviter la confusion de valeur avec les préfixes du système international.</p> |

| | |
|--|---|
| | http://fr.wikipedia.org/wiki/Préfixe_binaire |
| Proxy sibling <i>= proxy frère</i> | <p>Hiérarchiquement, un cache interrogé peut être un de niveau supérieur (parent) ou de niveau égal (frère ou sibling).</p> <p>Les serveurs parents sont d'ordinaire plus proches du serveur hébergeant l'objet recherché que les serveurs fils. Si un serveur fils ne peut trouver l'objet, la requête est en général relayée vers un serveur de cache parent qui va rapporter, mémoriser (mettre en cache) et finalement transmettre la requête au demandeur.</p> <p>Les serveurs frères (siblings) sont des serveurs de cache d'un niveau hiérarchique égal, dont le but est de répartir la charge.</p> <p>http://fr.wikipedia.org/wiki/Internet_Cache_Protocol</p> |
| Round-robin <i>= tourniquet</i> | <p>Round-robin (RR) est un algorithme d'ordonnement courant dans les systèmes d'exploitation. Ce dernier attribue des tranches de temps à chaque processus en proportion égale, sans accorder de priorité aux processus.</p> <p>Source Wikipédia :</p> <p>http://fr.wikipedia.org/wiki/Round-robin_(informatique)</p> |
| Squid | <p>Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites.</p> |
| Swap <i>= Verbe échanger</i> | <p>En informatique le swap sert à étendre la mémoire utilisable par un système d'exploitation, par un fichier d'échange ou une partition dédiée ; c'est aussi une instruction de certains processeurs et une fonction de certains langages de programmation qui permet l'échange de deux variables.</p> |
| Type MIME | <p>Un type MIME est une information permettant de connaître le format d'un document sans se baser sur l'extension.</p> |
| WPAD <i>= Web Proxy Autodiscovery Protocol</i> | <p>WPAD définit la façon selon laquelle un navigateur web se connecte à Internet. Ce protocole permet au navigateur d'utiliser automatiquement le proxy approprié à l'URL demandée. WPAD laisse le navigateur découvrir l'emplacement du fichier PAC grâce aux services DHCP et DNS.</p> <p>Un fichier PAC est un fichier texte en JavaScript, qui contient entre autres la fonction FindProxyForURL(url, host).</p> <p>Cette fonction possède deux arguments associés :</p> <ul style="list-style-type: none"> • URL : l'URL de l'objet • HOST : le nom de domaine dérivé de l'URL |