OPTENET WEB FILTER Server 5.27.05 Windows/Linux/Solaris/Aix/MacOS

Manuel de l'utilisateur

Rév. 28.06.2006

TABLE DES MATIÈRES

1. INTRODUCTION

OPTENET est un système de filtrage qui permet d'optimiser les ressources Internet de l'entreprise et le temps passé à son utilisation. En l'installant sur le Server permettant la connexion à votre réseau, vous pourrez filtrer les sites Internet que vous considérez inadéquats et contrôler les accès de vos usagers.

Pour pouvoir réaliser cette fonction de filtrage, OPTENET Server doit toujours travailler avec un proxy. Le proxy garantit que toutes les demandes de sites du réseau passent par ce dernier, OPTENET Server n'ayant plus qu'à s'accoupler au proxy pour filtrer tout le réseau. Si le réseau à filtrer possède des ordinateurs dont les demandes de sites ne passent pas par le proxy, ces demandes ne pourront pas être filtrées. Le processus par lequel OPTENET communique avec le proxy se fait en installant une extension (qu´on appellera à partir de ce moment ***plugin***) dans ce proxy ou en configurant le ICAP si ce proxy est doté de ce protocole. Lorsqu'un utilisateur essayer d'accéder à un site, ce dernier demande la page au proxy. En arrivant au proxy, la demande est saisie par le ***plugin*** d'OPTENET Server qui décide si elle doit être autorisée ou pas.

Pour prendre une telle décision, le service d'OPTENET Server se base sur un ensemble de règles qui définit l'administrateur selon les critères suivants :

Site demandé (URL, type de fichier ou type de contenu)
Utilisateur de la demande (nom et adresse IP)
Moment de la demande (jour de la semaine et heure)
Type de fichiers (musique, vidéo, exécutables)
Il permet également de définir manuellement les listes d'URL dont il est possible d'autoriser ou de bloquer l'accès.

Si l'ensemble des règles établit que le site demandé doit être autorisé, le site est alors affiché sur le navigateur de l'utilisateur. Au contraire, si la demande est refusée, l'utilisateur reçoit un message qui lui fait part du blocage. Ce blocage est à son tour consigné pour un contrôle ultérieur de l'usage du réseau.

La principale caractéristique d'OPTENET Server consiste au classement des contenus du système. Grâce à la combinaison d'une base de données d'URL préalablement triés et d'un moteur d'analyse multilingue de contenus, OPTENET Server est capable de trier les sites en plusieurs catégories pouvant être combinées pour définir les règles de filtrage.

OPTENET Server 5.20 peut fonctionner également comme un Server ICAP s'intégrant avec toute sorte d'appliances ou caches qui supportent ce protocole (en s´installant sur les plate-formes Windows, Linux, Solaris et Aix). Il peut également être installé avec le proxy SQUID 2.5 sur les plate-formes Linux, Solaris et Aix ou avec Microsoft ISA Server et Microsoft Proxy Server, ou enfin avec le proxy OPTENET sur les plate-formes Windows. Sa technologie leader en sélection et filtrage d'accès à Internet va permettre un contrôle maximum de l'utilisation d'Internet pour l'ensemble des postes connectés au réseau.

Pour gérer l'accès à Internet, OPTENET dispose de quatre niveaux de filtrage :

- Filtrage en fonction de **l'analyse multilingue sémantique du texte** qui apparaît dans la page web. OPTENET analyse chaque page **lors de leur téléchargement** d'Internet, ce qui permet d'obtenir un niveau de sécurité accru.

- Filtrage basé sur des **listes prédéfinies** contenant des adresses classées manuellement par des spécialistes.
- Filtrage basé sur une **analyse d'URL**.
- Filtrage basé sur des **listes prédéfinies par l'administrateur**.

De plus, OPTENET Server possède les caractéristiques suivantes :

- Mise à jour automatique des listes.
- Personnalisation des listes prédéfinies.
- Administration via WWW multilingue (anglais, français, espagnol, Italien et Portugais).

2. NOUVELLES CARACTERISTIQUES DE LA VERSION 5.27

Voici les nouvelles caractéristiques et améliorations de la version 5.27 par rapport à son prédécesseur, la version 5.25 :

- Catégories ajoutées : guides et kiosques, Art et culture, infos, juridiques, banques et établissements financiers, blogs, payer pour naviguer, logos/sonneries, code malin, DNS Services, télécommunications.
- Possibilité de fonctionner avec ICAP et ISA sur LDAP lorsqu'est utilisé un nom d'utilisateur différent de "**Distinguished name**"
- Filtrage du protocole Skype (lorsqu'intégré avec ICAP)
- Identification d'utilisateurs à l'aide de certificats numériques en cas d'utilisation d'authentification LDAP.
- Possibilité de consulter depuis l'administration du Web les catégories auxquelles appartient une adresse URL déterminée.
- Possibilité d'appliquer des règles de filtrage aux demandes qui n'appartiennent à aucune des catégories supportées par l'outil de filtrage.

3. INSTALLATION

Le présent chapitre décrit l'installation d'OPTENET et la configuration requise du système Windows, Linux ou Solaris où va être installé OPTENET.

3.1. Configuration du système

3.1.1. Sous Windows

- Microsoft Windows 98 / Me / NT / 2000 / XP / 2003.
- OPTENET recommande l´installation avec Windows Server (NT / 2000 / 2003) dû à une plus grande stabilité avec ces derniers. De plus dans ces systèmes le logiciel s´installe comme un service pouvant être démarré ou arrêté avec plus de facilité.
  Dernier Service Pack de Windows recommandé.
- L'équipement dépend du nombre d'utilisateur mais l'utilisation d'une unité centrale d'au moins 266Mhz avec 128 Mo de RAM est recommandée.

3.1.2. Sous Linux

- Kernel Linux 2.4.0 ou ultérieur.
- Glibc 2.0.7 ou ultérieur, en raison de la prise en charge des threads.
- Service portmap, nécessaire à la communication RPC. (si installé pour fonctionner avec SQUID)
- Red Hat Linux 7.0 ou ultérieur recommandé.
- L'équipement minimum dépend du nombre d'utilisateurs, mais l'utilisation d'une unité centrale d'au moins 266 MHz avec 128 Mo de RAM est recommandée.

3.1.3. Sous Solaris

- Solaris 2.6 ou ultérieur.
- Service rpcbind nécessaire pour la communication RPC (si installé pour fonctionner avec SQUID).
- L'équipement dépend du nombre d'utilisateurs mais l'utilisation d'une Sun UltraSPARC d'au moins 200 Mhz et 128 Mo de RAM est recommandée.

3.1.4. Sous AIX

- AIX 4.3
- Service portmap pour la communication RPC.
- L'équipement dépend du nombre d'utilisateurs mais l'utilisation d'un PowerPC d'au moins 200 MHz et 128 Mbytes de mémoire RAM est recommandée.
- GNU tar et gzip pour décompresser les archives.
- Librairie runtime de gcc 3.2.1 pour AIX.

3.1.5. Sous Mac OS X

- Mac OS X 10.3.3 ou ultérieur.

- Service portmap pour la communication RPC (déjà inclus dans Mac OS X)
- L'équipement dépend du nombre d'utilisateurs mais l'utilisation d'un processeur G4 et de 256 Mo de mémoire RAM est recommandée.

3.2. Installation

Pour pouvoir réaliser cette fonction de filtrage, OPTENET Server doit toujours travailler avec un proxy. Le proxy centralise l´accès à l´Internet de tous les utilisateurs qui l´utilisent, ainsi OPTENET Server n'a plus qu'à se coupler au Server pour filtrer tout le réseau. Si le réseau à filtrer possède des ordinateurs dont les demandes de sites ne passent pas par le proxy, ces demandes ne pourront pas être filtrées.

OPTENET Server permet d'installer son propre Proxy dans des environnements Windows, idéal pour desservir des réseaux de plus de 200 utilisateurs.
Dans les environnements Unix (Linux, Solaris, Aix, MacOS), est distribué le Proxy SQUID capable de desservir des réseaux de moyenne et grande taille.

De plus, à l'issue de l'installation d'OPTENET Server, il est possible d'installer OPTENET Reporter, outil permettant d'élaborer des rapports d'utilisation d'Internet.

3.2.1. Sous Windows

Pour installer OPTENET Server sur votre Server, exécuter le programme OPTENET-5.27.XX-2.03.XX.exe (ou version ultérieure). Par défaut l'assistant d´installation démarre dans la langue de votre système d'exploitation, et s'il ne s´agit pas de l´une des 3 langues disponibles le système, il démarrera en anglais.

Ce programme inclut OPTENET Server et OPTENET Reporter. A l'issue de l'installation d'OPTENET Server, il est possible d'installer OPTENET Reporter.

Ce programme peut être utilisé pour installer uniquement l'un des deux produits. Pour plus de renseignements sur OPTENET Reporter (installation, configuration…), consultez le manuel correspondant.

Vous trouverez ci-dessous le détail du processus d'installation d'OPTENET Server uniquement.

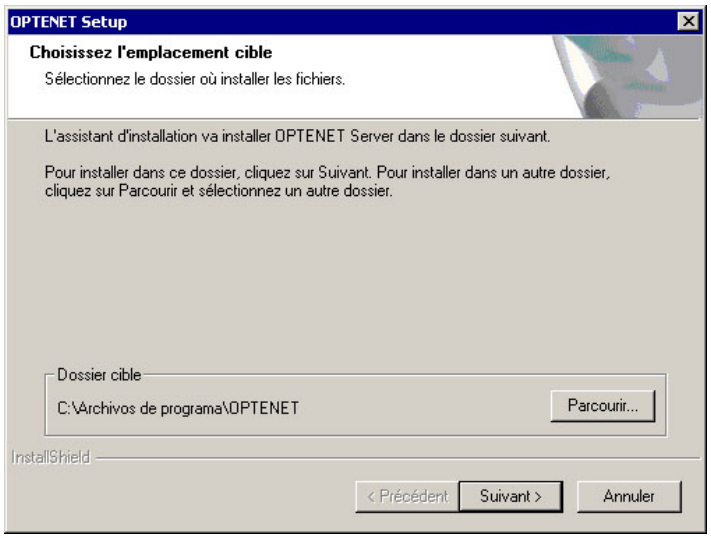
Vous trouverez ci-dessous une fenêtre où il vous est demandé si cous souhaitez installer OPTENET Server. Répondez par oui.

Ensuite, vous devrez sélectionner le type d'installation souhaité :

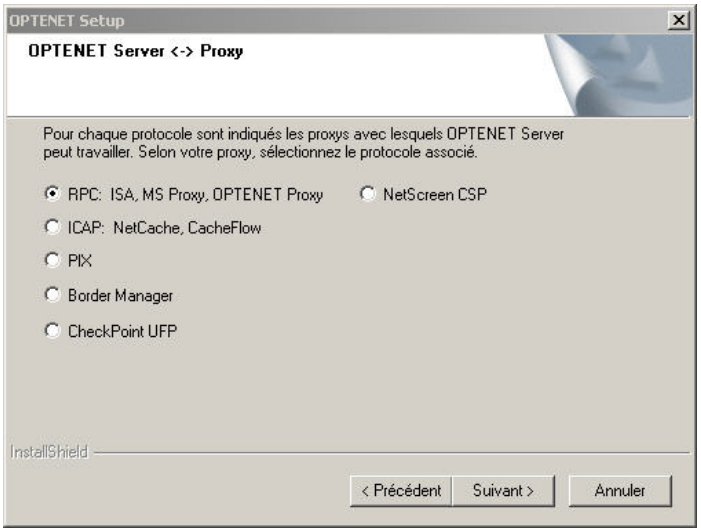
- Version Démo : Installation avec licence temporaire. C'est l'installation par défaut et il n'est pas nécessaire de saisir un quelconque numéro de licence. La limite dans le temps s'active à partir du moment de l'installation et non à partir du téléchargement. Cette licence Démo sera valide pendant 30 jours.
- Version payante : Installation indéfinie. Choisissez cette option et veuillez ensuite saisir votre code de licence valide.

Si vous désirez une installation indéfinie mais ne disposez pas encore de votre code de licence, veuillez l'installer en mode "démo", du fait qu'à tout moment vous pourrez saisir le code de licence à partir de l'administration d'OPTENET Server.

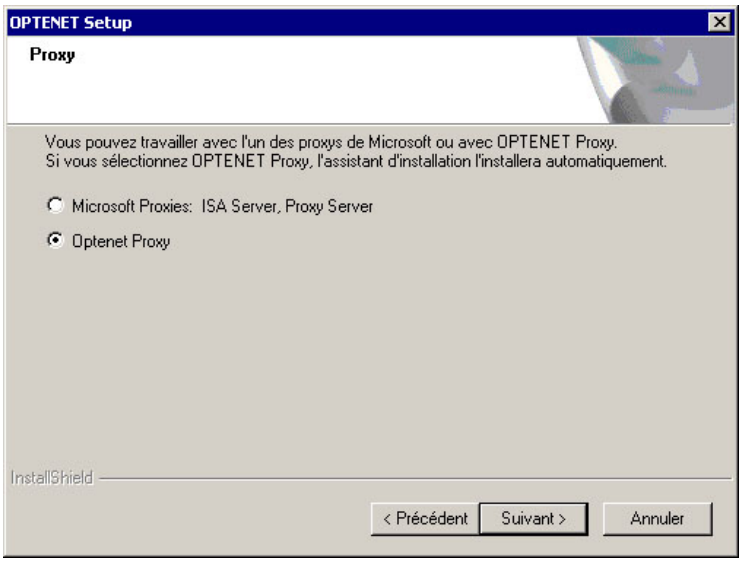
Ensuite il vous sera demandé le répertoire d'installation du logicie. Le répertoire : C:\Program Files\OPTENET est utilisé par défaut mais vous pouvez en choisir un autre. Si le répertoire choisi n'existe pas, le programme d'installation le créera.



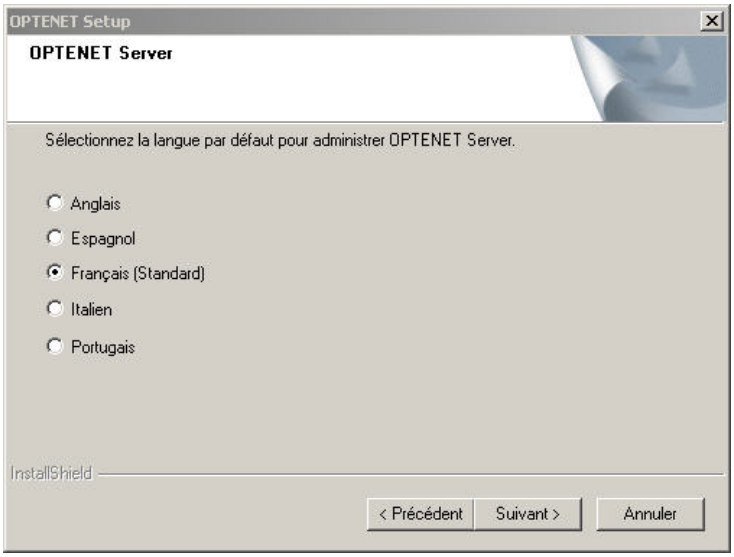
En pressant la touche Next vous pourrez sélectionner le protocole de communication par le biais duquel OPTENET Server communiquera avec le proxy. Pour chaque protocole seront indiqués les proxys avec lesquels l´on peut travailler.



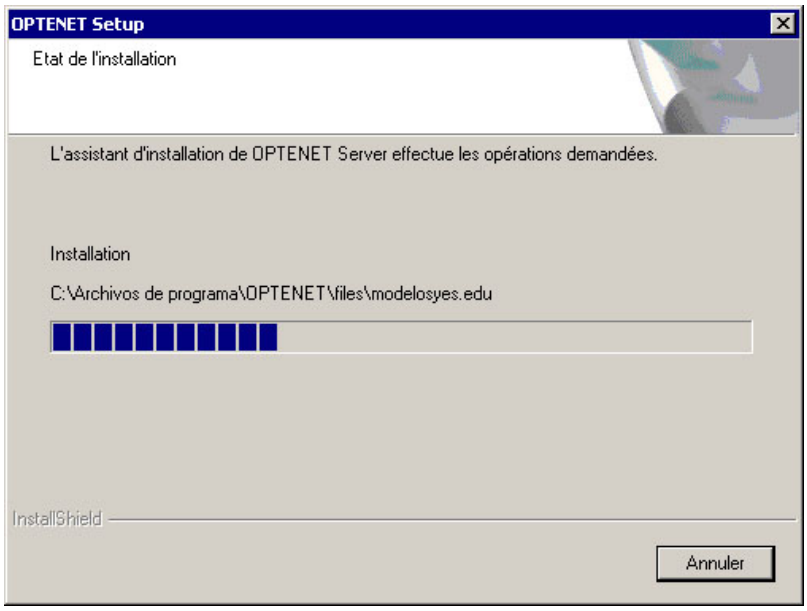
Si vous avez choisis RPC dans la fenêtre antérieur alors vous pouvez configurer OPTENET Server pour qu´il travaille avec un proxy Microsoft (ISA Server, MS Proxy Server) ou avec OPTENET Proxy.



Ensuite vous devez choisir la langue par défaut d'OPTENET Server (Administration web, Outil de rapports, logs,...)..



En pressant la touche Suivant le programme d´installation va installer tous les éléments d'OPTENET Server et configurer le Server pour qu´il exécute OPTENET Server lors du prochain redémarrage du Server (voir la figure suivante).



En dernier lieu le programme d´installation vous demandera si vous souhaitez installer OPTENET Reporter. Si vous ne souhaitez pas l'installer, il vous demandera de redémarrer l´ordinateur. Il est obligatoire de redémarrer le système pour que OPTENET fonctionne bien.

Groupe de programmes.

OPTENET Server crée un nouveau groupe de programmes avec les éléments suivants :

- **Contribution:** si vous choisissez cet élément vous pourrez envoyer à OPTENET des pages d´Internet pour lesquelles vous pensez que l´accès devrait être interdit.
- **Désinstaller OPTENET Server:** cet élément désinstalle OPTENET Server de votre ordinateur.
- **Administration:** si vous choisissez cet élément une page internet s´ouvrira et se connectera à l´administration WWW d'OPTENET Server.
- **Home OPTENET:** cet élément ouvre le site Internet http://www.optenet.com
- **Manuel d'utilisateur:** Cet élément vous permettra d'accéder à la dernière version en ligne du manuel d'OPTENET Server.

BASE DE REGISTRE de Windows

Pour le bon fonctionnement d'OPTENET Server, le processus d'installation réalise une série de modifications des registres Windows.

Pour conserver les paramètres essentiels d'OPTENET Server le programme d'installation ajoute des clefs dans la base de registre:
HKEY LOCAL MACHINE\SOFTWARE\OPTENET\OPTENET Server\

CheckData Si OPTENET Server est installé avec un Proxy Server ou ISA Server de Microsoft, et s'il y a un antivirus qui fonctionne comme un plugin ISAPI de ces mêmes

proxys, il faudra mettre à jour cette clef avec la valeur FALSE. Dans toutes autres circonstances (valeur par défaut) cette clef indiquera la valeur TRUE.
DownloadContent Flag qui indique à OPTENET Server s'il doit demander le contenu lorsqu'il est intégré avec PIX, Border Manager et CheckPoint. Par défaut « TRUE », c'est-à-dire qu'il demande le contenu.
FilterServer Server où est exécuté le service d'OPTENET Server et auquel le plugin d'OPTENET Server doit envoyer les données. La valeur par défaut est 127.0.0.1 (machine locale).
IcapClients Identifie le nombre de clients icap au moment de communiquer avec un Server ICAP (NetCache, BlueCoat). Par défaut 1.
IcapPort Port d´écoute du Server ICAP le port par défaut est le 1344
IcapServices Indique le nombre de services ICAP qu'OPTENET utilise. Sa valeur par défaut est 2. OPTENET calcule en fonction de IcapClients, le nombre de threads (connections) que le Server ICAP doit lancer.
InstallDir Répertoire de l'installation d'OPTENET Server.
Language Identificateur de la langue d'OPTENET Server et que vous avez sélectionné lors du processus d'installation. (eng, esp, fra, ita, por)
ManagerPort Port d'écoute de l'Administration WWW d'OPTENET Server. Le port par défaut est le 10237.
Mode Mode de communication entre OPTENET Server et le proxy (RPC, ICAP, PIX, UFP, BM, OPT.
Proxy Identificateur du proxy auquel est intégré OPTENET Server (ICA, PIX, BMA, OPT, MSP, UFP).
RemoveDomain Flag qui indique à OPTENET Server comment identifier les utilisateurs et les groupes. A l'aide de son nom (« TRUE » par défaut) ou avec le nom du domaine devant (« FALSE », c'est-à-dire nomdomaine/nomutilisateur)
Version Identifie la version d'OPTENET Server qui est actuellement installée.
SendIpUser indique à Optenet s'il doit envoyer, comme paramètres de la page de stop, l'IP et l'utilisateur qui ont été bloquées. Sa valeur par défaut est « FALSE »
LogServerPort Port d'écoute d'OPTENET Server pour les demandes de logs effectuées par OPTENET Reporter. Le port par défaut est 10239.
LogServerClients Nombre de threads que lancera OPTENET Server pour répondre aux demandes de logs effectuées par OPTENET Reporter. Par défaut, 5.
WebserverThreads Nombre de fils lancés par OPTENET Server pour répondre aux demandes de l'administration. Il sera de 50, par défaut.
BindIpLocal Adresse ip locale (interface de réseau) permettant à OPTENET Server d'écouter. Par défaut, il s'agit de 0.0.0.0 (toutes les interfaces de réseau). Ce paramètre s'avère utile en présence de diverses interfaces de réseau et nous ne souhaitons pas qu'OPTENET Server soit en mesure d'écouter par le biais de toutes ces adresses.
Discardheaders En-têtes que le plug-in d'OPTENET Servet pour ISA doit ignorer. Il convient d'ajouter l'en-tête 'X-Actual-URL' au cas où le trafic de RealPlayer passerait par Microsoft ISA. En cas d'ajout de plus d'un en-tête, ils doivent être séparés par des virgules.

Pour conserver les paramètres élémentaires d'OPTENET Proxy, le processus d'installation ajoute la clé HKEY LOCAL MACHINE\SOFTWARE\OPTENET\OPTENET Proxy
InstallDir Répertoire d'installation d'OPTENET Server.

Données du système

Pour qu'OPTENET Server, OPTENET Reporter et OPTENET Proxy puissent être exécutés comme un service Windows, utiliser l'observateur d'événements et être

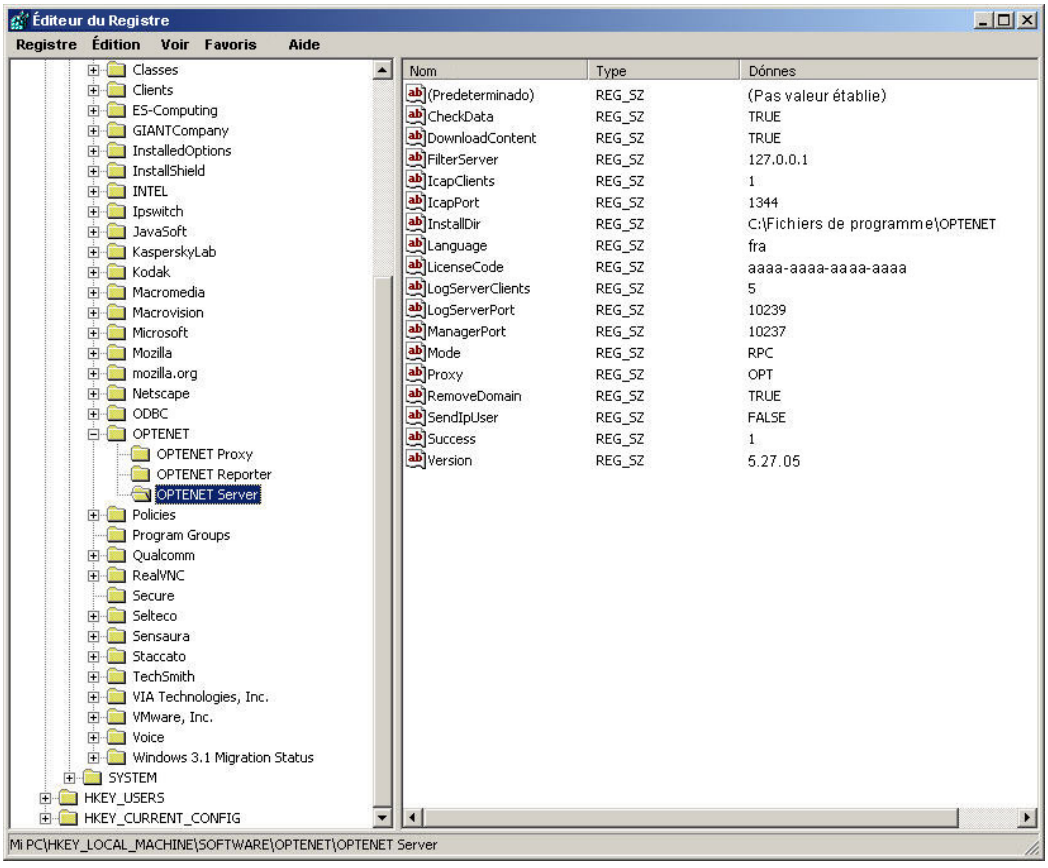
désinstallé, le processus d'installation d'OPTENET ajoute une série de clefs parmi les données du système qui sont stockées dans la base de registres Windows:

- HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\OPTENET
Les données nécessaires pour qu'OPTENET Server puisse être exécuté comme un service. Dans Windows 98 et WindowsMe cette entrée dans le répertoire ne s´ajoute pas car il n´y a pas de service.

- HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\OPTENET Proxy
Les données nécessaires pour qu'OPTENET Proxy puisse être exécuté comme un service. Dans Windows 98 et WindowsMe cette entrée dans le répertoire ne s´ajoute pas car il n´y a pas de service.

- HKEY LOCAL MACHINE\SYSTEM\Current ControlSet\Services\ Eventlog\Application\OPTENET
Les données nécessaires pour qu'OPTENET Server puisse utiliser l'Observateur d'événements pour signaler ses problèmes.

- **HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current Version\ Uninstall\OPTENET Server**
Les données nécessaires pour qu'OPTENET Server puisse être désinstallé correctement.



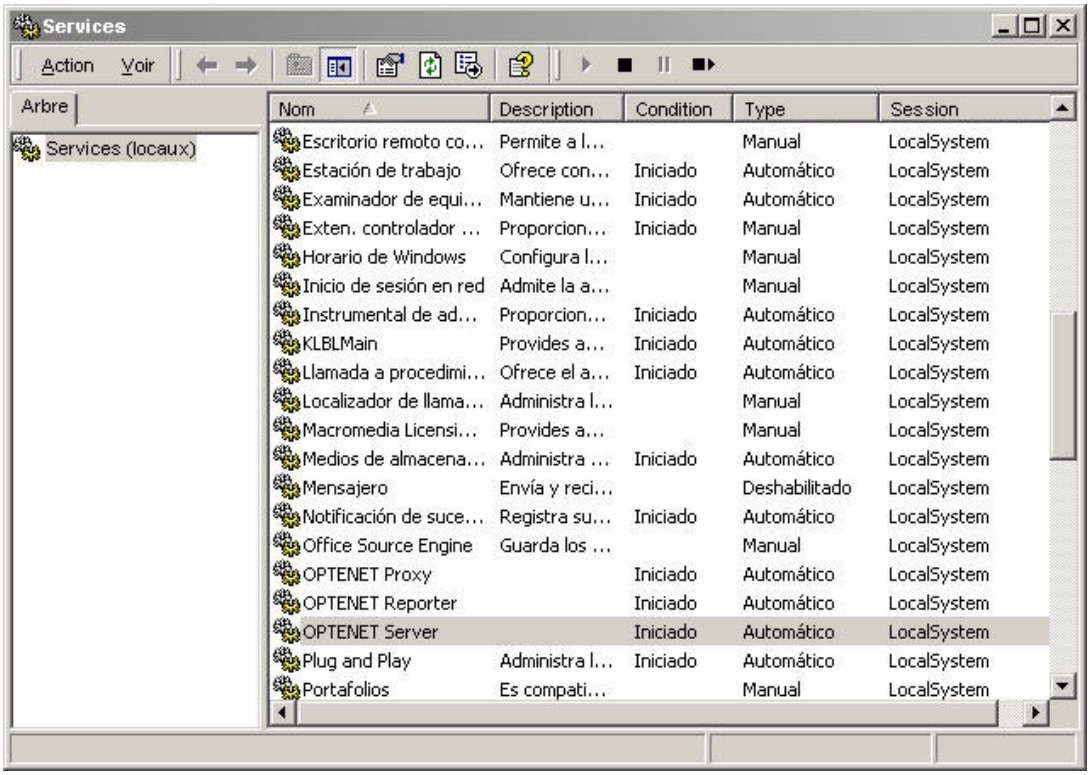
ÉLÉMENTS D'OPTENET Server

Les éléments installés par OPTENET Server se divisent en deux parties principales: L'une se charge de la capture des demandes Internet et l'autre gère le filtrage de ces demandes.

Le premier élément dépend du proxy utilisé. Ce thème est détaillé dans les paragraphes suivants.

Le deuxième élément d'OPTENET Server est un service/procédure de Windows qui analyse les demandes reçues du plugin d'OPTENET Server, installé avec le proxy ou relié avec le protocole ICAP, et décide si ces demandes doivent être autorisées ou non. Dans le cas où il s´agit d´un Server (NT, XP, 2000, 2003) vous pouvez voir s'il a été installé correctement dans les services de Windows.

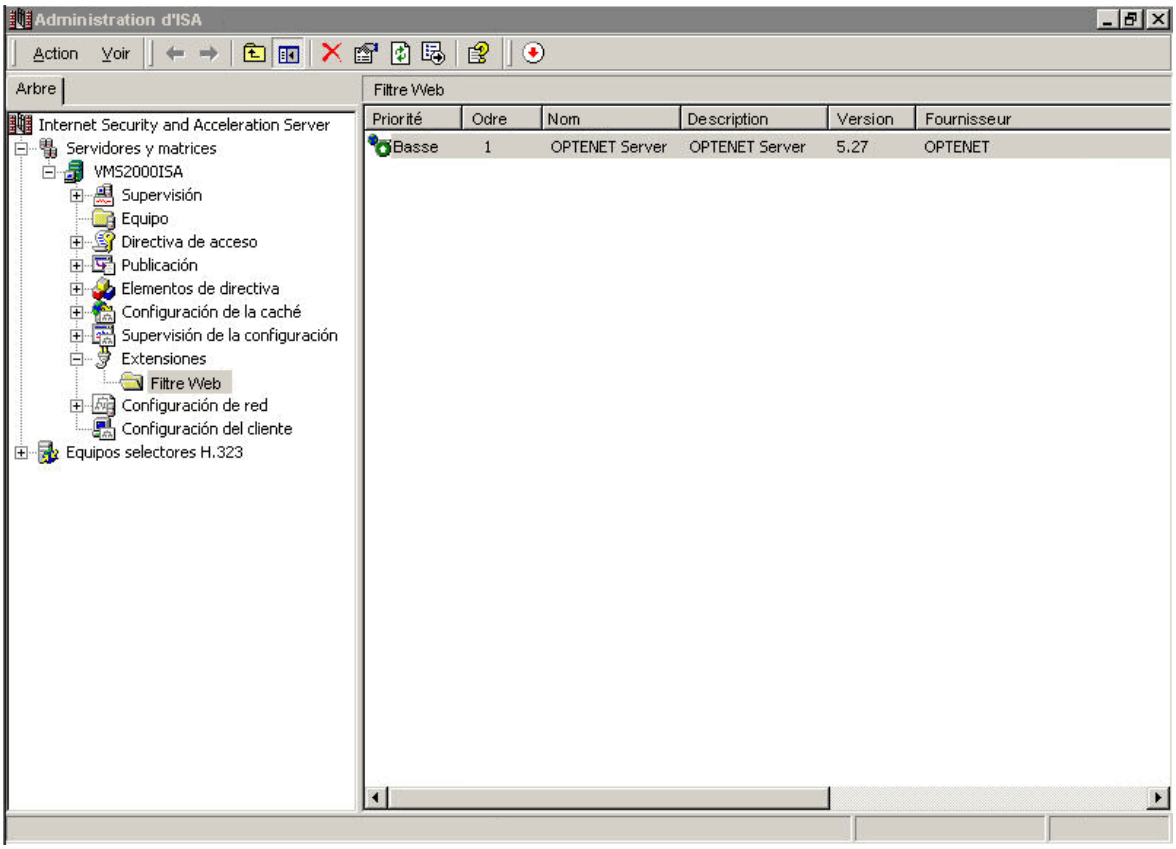
Vous pouvez procéder à la même vérification avec OPTENET Reporter ou OPTENET Proxy.



3.2.1.1. Intégration avec Microsoft ISA-Server

L'élément chargé de la capture de demandes est appelé OPTENET **plugin**, comme il a déjà été mentionné dans l'introduction. Il s'agit d'un filtre Web qui est ajouté à Microsoft ISA Server. Vous pouvez voir s'il a été installé correctement dans Administration du Server ISA.

Si vous intégrez OPTENET Server avec Microsoft ISA 2004, veuillez consulter l’Annexe 8 Configuration de Microsoft ISA 2004 une fois le processus d’installation d’OPTENET Server terminé.



Microsoft Web Proxy

Microsoft Web Proxy est le proxy qui est installé avec Microsoft ISA Server. C'est un service Windows que l'on peut contrôler au moyen de l'administration de services de Windows. OPTENET Server travaille en étroite relation avec Microsoft Web Proxy : il ne peut filtrer que les demandes qui y passent.

Par conséquent, si vous avez installé Microsoft ISA Server mais que vous n'utilisez pas Microsoft Web Proxy, OPTENET Server ne réalisera aucun type de filtrage. Pour que les ordinateurs utilisent Microsoft Web Proxy, il faut normalement configurer les navigateurs à cet effet. Vous pouvez **consulter la documentation de Microsoft ISA Server** pour établir **un navigateur comme client de Microsoft Web Proxy.**

Si vous ne désirez pas configurer les navigateurs pour l'usage de Microsoft Web Proxy mais que vous utilisez Microsoft ISA Server comme Server de sécurité ou Server SecureNat de votre réseau, vous pouvez **enchaîner** le Server de sécurité et le Server Secure Nat Microsoft Web Proxy au moyen du filtre redirecteur de HTTP. De cette façon, les demandes web passeront par Microsoft Web Proxy et pourront être filtrées par OPTENET Server. Vous pouvez **consulter la documentation de Microsoft ISA Server** pour obtenir plus d'information sur cette fonctionnalité.

COMMUNICATION ENTRE Microsoft Web Proxy ET OPTENET Server

Pour pouvoir filtrer les demandes qui passent par Microsoft Web Proxy, OPTENET Server ajoute un filtre web à Microsoft ISA Server. Ce filtre Web consiste en un plugin de Microsoft Web Proxy qui se charge de capturer les données des demandes qui passent par lui et de les envoyer au service de filtrage d'OPTENET Server. **Les données capturées sont les suivantes:**

- L'**adresse IP** de l'ordinateur d'où procède la demande.
- L'**utilisateur** qui réalise la demande (seulement si Microsoft Web Proxy réalise une authentification).
- L'**URL** de la page demandée.
- **Le contenu du site demandé**.

Avec ces données, le service d'OPTENET Server vérifie les règles de filtrage configurées et décide si la demande doit être autorisée ou pas. En fonction du résultat, il informe le plugin s'il doit laisser la demande s'effectuer par voie normale ou au contraire la bloquer. En cas de blocage, le service d'OPTENET Server indique au plugin le message de blocage à montrer au lieu du site demandé.

La communication entre le plugin et le service d'OPTENET Server est réalisée au moyen d'appels de procédure distants (RPC). Il est nécessaire que le service RPC soit démarré.

3.2.1.2. Intégration avec Microsoft Proxy Server

Pour le fonctionnement correct d'OPTENET Server avec Microsoft Proxy Server il est important d´installer Proxy Server en suivant les indications recommandées par Microsoft.

1. Installer Microsoft Windows NT 4.0 Service Pack 3 (Ne pas le remplacer par Windows NT 4.0 Service Pack 4 ou version postérieure).
2. Installer Microsoft Internet Explorer 4.01 Service Pack 2 sans l´interface Active Desktop.
   NOTE : Windows NT Option Pack contient Internet Explorer 4.01 Service Pack 1 néanmoins nous recommandons d´installer Internet Explorer 4.01 Service Pack 2 (Ne pas le remplacer par Internet Explorer 5.0 ou versions postérieures).
3. Installer Microsoft Windows NT 4.0 Option Pack.
4. Installer Microsoft Proxy Server 2.0
5. Installer Microsoft Windows NT 4.0 Service Pack 4 ou Service Pack 5 (ne pas installer les actualisations Y2K car celles-ci sont déjà installées par MDAC 2.1 Service Pack 2).
6. (En option) Installer Microsoft Internet Explorer 5.
7. Installer MDAC 2.1.2.4202.3 connu aussi sous MDAC 2.1 Service Pack 2.
8. Installer Microsoft Windows NT 4.0 Service Pack 6a ou versions postérieures.

   NOTE : même lorsque vous installez la dernière version de Windows NT Service Pack dans l´étape 5, il faut réinstaller le dernier Service Pack car l´installation de Windows NT Option Pack remplace les DLL qui sont installés par le Service Pack.
9. Installer Proxy 2.0 Service Pack 1.

3.2.1.3. Intégration avec proxy ICAP (modo ICAP)

Une fois OPTENET installé, vous devrez configurer ces caches ou appliances pour qu'ils utilisent le Server ICAP d'OPTENET comme système de filtrage (Voir le paragraphe 3.5).

3.2.1.4. Sans proxy supplémentaire (mode Stand-Alone)

L'élément installé pour la saisie de demandes dans la version stand-alone est ce que l'on appelle OPTENET Proxy. OPTENET Proxy est un proxy simple distribué par OPTENET qui est lancé au démarrage du système d'exploitation. Ceci permet l'usage du filtre

OPTENET sans accessoire supplémentaire. Les données capturées par OPTENET Proxy sont les mêmes que celles mentionnés pour le Microsoft Web Proxy. Le OPTENET Proxy n'a pas besoin d'un plugin particulier et il communique directement avec le filtre OPTENET via les appels de procédure distants (RPC).

Il faut tenir compte du fait que le filtre ne peut réaliser le filtrage que si les demandes HTTP sont reconduites dans le proxy. Pour cela, il faut inscrire explicitement le proxy dans la configuration des navigateurs.

Vous pouvez consulter l´annexe 4 pour savoir comment configurer OPTENET Proxy.

3.2.1.5. Informations spécifiques à Windows 98 et WindowsME

Comme sur Windows 98 et WindowsME le concept services est différent, OPTENET Server, OPTENET Proxy et OPTENET Reporter sont installés comme des processus habituels et sont lancés automatiquement en démarrant le système d'exploitation.

3.2.2. Sous Linux, Solaris et AIX

Sous Linux et Solaris, la distribution d'OPTENET compte les fichiers suivants:

- optenet-5.27.XX-2.03.XX.tgz – Fichier du logiciel d'OPTENET Server et OPTENET Reporter pour les systèmes Linux et AIX ou optenet-5.27.XX-2.03.XX.tar.Z pour le système Solaris.
- install.sh – Script d'installation.
- OPTENETManual.pdf – Manuel de l'utilisateur.
- OptenetDCAgent2.00.xx.zip – Fichier du logiciel à installer sur votre Server Windows, si l'authentification des utilisateurs auprès d'un domaine NT est utilisée.

install.sh est un shell script ; vous pouvez donc l'ouvrir et le modifier selon vos besoins. Concrètement, pendant l'installation, install.sh crée un utilisateur auquel va appartenir le logiciel OPTENET. Par défaut, cet utilisateur s'appelle optenet ; vous avez toutefois la possibilité d'éditer install.sh et de le renommer. Vous pouvez également modifier le répertoire racine de l'utilisateur, c'est-à-dire le répertoire d'installation d'OPTENET (par défaut, /usr/local/optenet). L'utilisateur est créé sans mot de passe, mais vous pouvez lui en assigner un au moyen de la commande passwd. Il se passe la même chose si vous décider également d'installer OPTENET Reporter. Par défaut, l'utilisateur reporter sera créé avec son répertoire d'installation (/usr/local/reporter).
Après la création de l'utilisateur, le script d'installation décompresse le fichier optenet-5.27.tgz dans le répertoire d'installation et personnalise les scripts d'OPTENET.
Pendant le processus d'installation, le programme d'installation vous demandera si vous souhaitez qu'OPTENET fonctionne comme Server ICAP pour être intégré avec Appliances qui supportent ce protocole, ou bien pour être intégré avec Border Manager de Novell ou bien avec Cisco PIX Firewall ou qui s'intègre avec le SQUID qui est fourni avec. De même, si vous possédez le code de licence correspondant au produit, l'installateur vous permettra d'enregistrer ce code.

3.2.2.1. Installation d'OPTENET comme Server ICAP (mode ICAP)

L'option ICAP doit être choisie quand OPTENET va être installé dans un réseau qui a déjà des caches ou des appliances (par exemple machines Netcache ou BlueCoat) qui supportent le protocole ICAP 1.0. Dans ce cas, les scripts de démarrage d'OPTENET seront créés de sorte qu'OPTENET démarre son Server ICAP en attendant de recevoir les demandes de filtrage qui y passent. Une fois OPTENET installé, il faudra configurer ces caches ou appliances pour qu'ils utilisent le Server ICAP d'OPTENET comme système de filtrage. (Voir paragraphe 3.5)

3.2.2.2. Installation d'OPTENET avec SQUID (mode SQUID)

L'option SQUID installe avec OPTENET une version du proxy SQUID modifiée afin qu'il communique avec OPTENET via RPC (Remote Procedure Call) à chaque demande de connexion à Internet. Dans ce cas, les scripts de démarrage d'OPTENET sont modifiés pour qu'ils démarrent simultanément avec OPTENET et SQUID. Bien que SQUID entende des demandes par défaut dans le port 8080, vous pouvez changer ce port en éditant le fichier squid/etc/squid.conf du répertoire d'installation et en modifiant la valeur http_port. Le fichier squid/etc/squid.conf permet de configurer de nombreux aspects du fonctionnement de SQUID. Nous vous recommandons de lire attentivement et de l'adapter à vos besoins. Après avoir démarré OPTENET, il faudra configurer les navigateurs de votre réseau pour qu'ils utilisent SQUID comme proxy et réaliser ainsi le filtrage.
Avec l'installation sur le mode SQUID par défaut, ce dernier ne reconnaît pas d'utilisateurs. Pour configurer Squid avec l'option d'identification d'utilisateurs, il faudra éditer le fichier squid/etc/squid.conf, décommenter le tag auth_param avec l'authentification correspondante, ajouter une entrée dans l'ACL (access control list) et autoriser cette entrée dans l'accès. Par exemple si l´on veut activer le modèle d´authentification de base basé sur un fichier texte avec les utilisateurs et ses données il faudra ajouter les lignes suivantes au fichier de configuration:

```
auth_param basic program /usr/local/optenet/squid/libexec/ncsa_auth /usr/local/optenet/squid/etc/passwd
auth_param basic children 5
auth_param basic realm OPTENET Server
auth_param basic credentialsttl 2 hours

acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Dès lors, chaque utilisateur qui désire accéder à Internet par le proxy devra indiquer la première fois son identification (utilisateur-mot de passe) pour pouvoir naviguer. Cet utilisateur pourra être utilisé par la suite pour former des règles avec OPTENET. Par défaut, il n'y a aucun utilisateur défini. Nous pouvons créer des utilisateurs en utilisant le script de perl situé dans le répertoire tools/adduser.pl dans le répertoire d'installation de la sorte:

```
perl adduser.pl utilisateur password fichier_password
```

Par exemple:

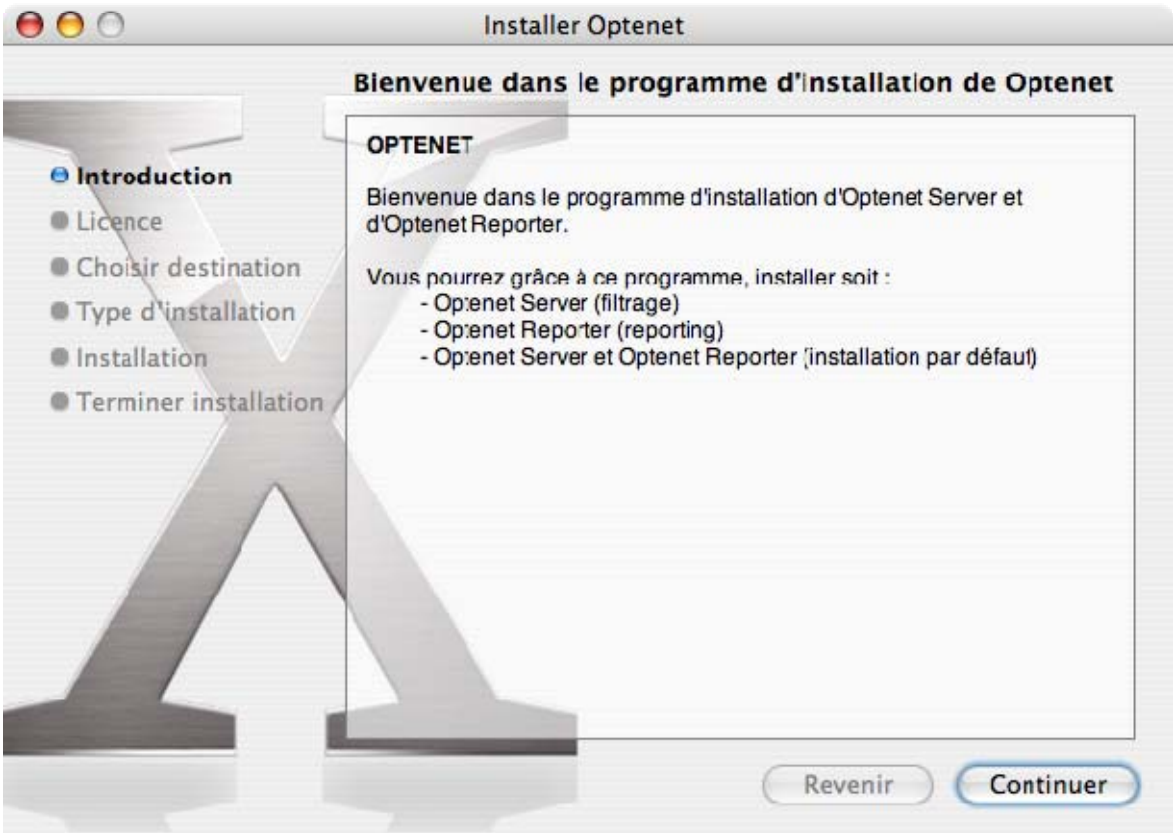
```
# perl adduser.pl louis password_luis ../squid/etc/passwd
```

3.2.3. Sous Mac OS X

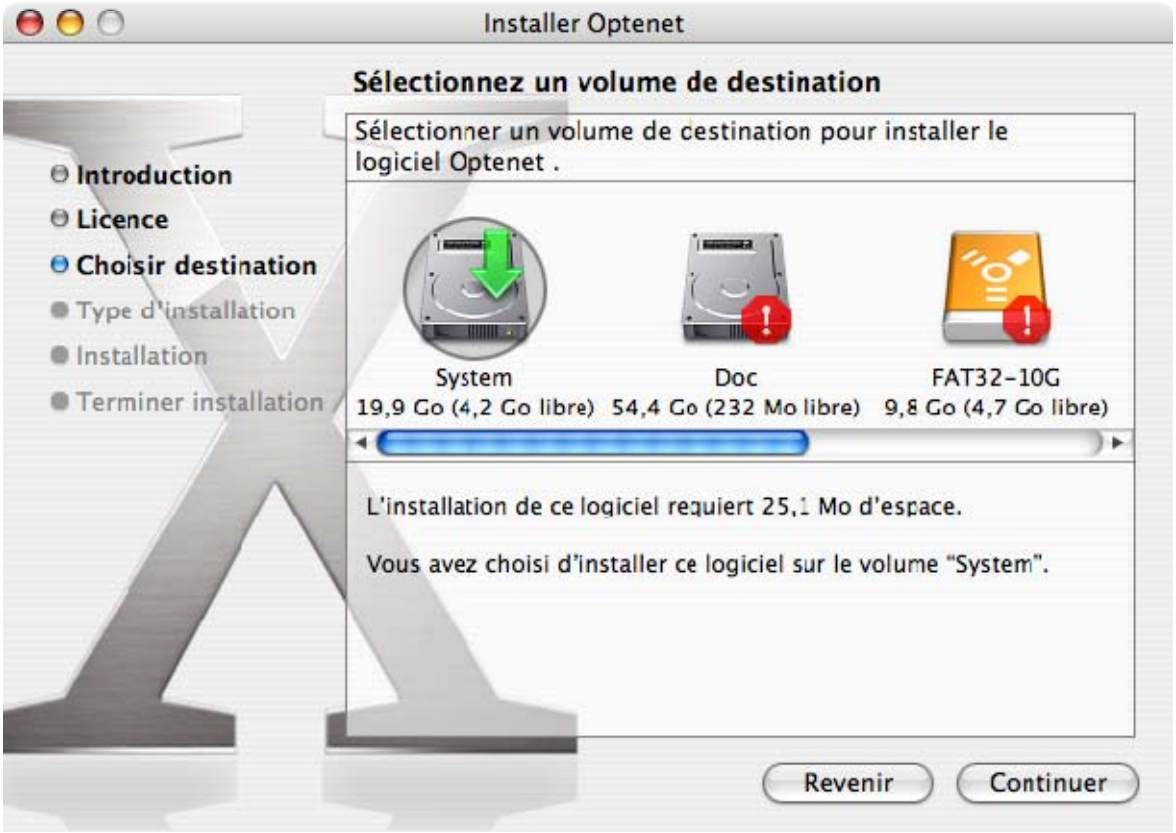
Sous Mac OS X, la distribution d'OPTENET compte les fichiers suivants:

- optenet-5.21.dmg
- OPTENETManual.pdf – Manuel de l'utilisateur.
- OptenetDCAgent2.00.xx.zip – Fichier du logiciel à installer sur votre Server Windows, si l'authentification des utilisateurs auprès d'un domaine NT est utilisée.

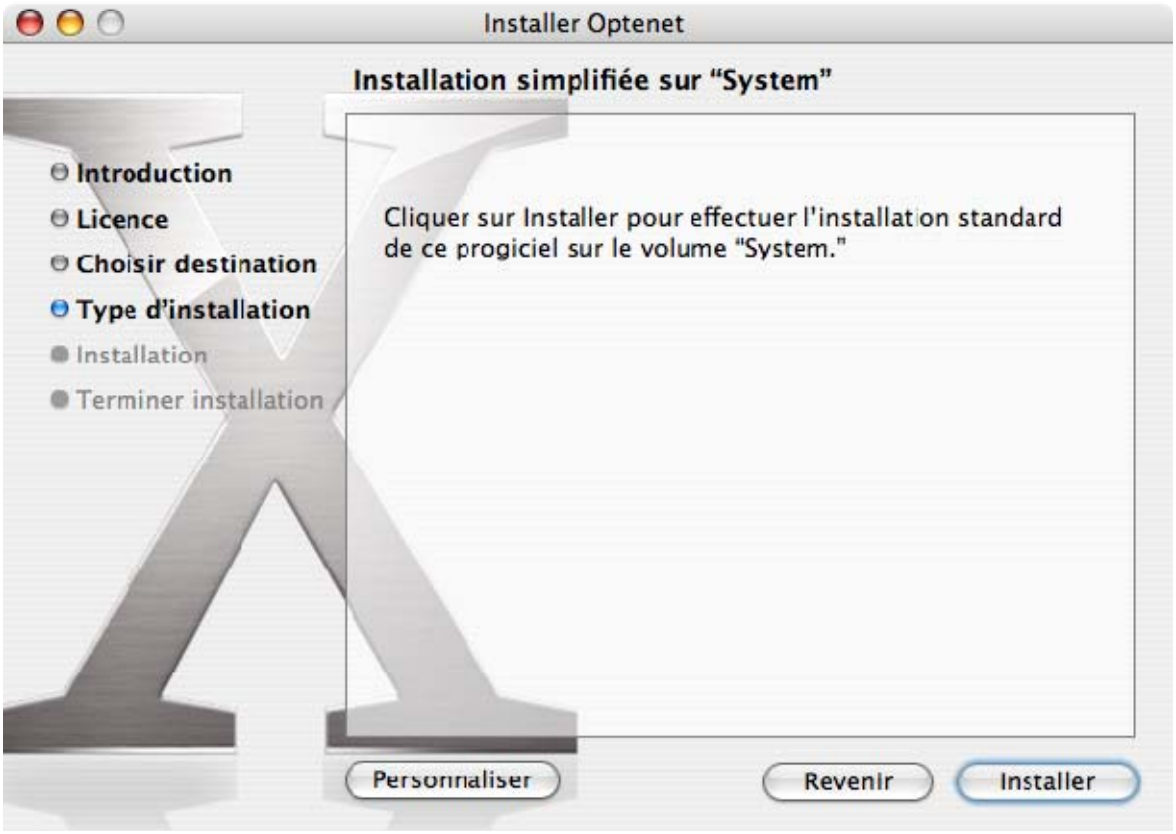
Pour installer OPTENET Server sur votre Server, double-cliquez sur optenet-5.21.dmg. Vous verrez ensuite un nouveau volume dans le Finder. Double-cliquez alors sur Optenet.mpkg pour lancer la procédure d'installation. Par défaut l'assistant d'installation démarre dans la langue de votre système d'exploitation, et s'il ne s'agit pas de l'une des 3 langues disponibles, il démarrera en anglais.
Vous verrez alors la fenêtre d'accueil du logiciel d'installation. Cliquez sur Continuer pour voir les conditions générales d'utilisation.



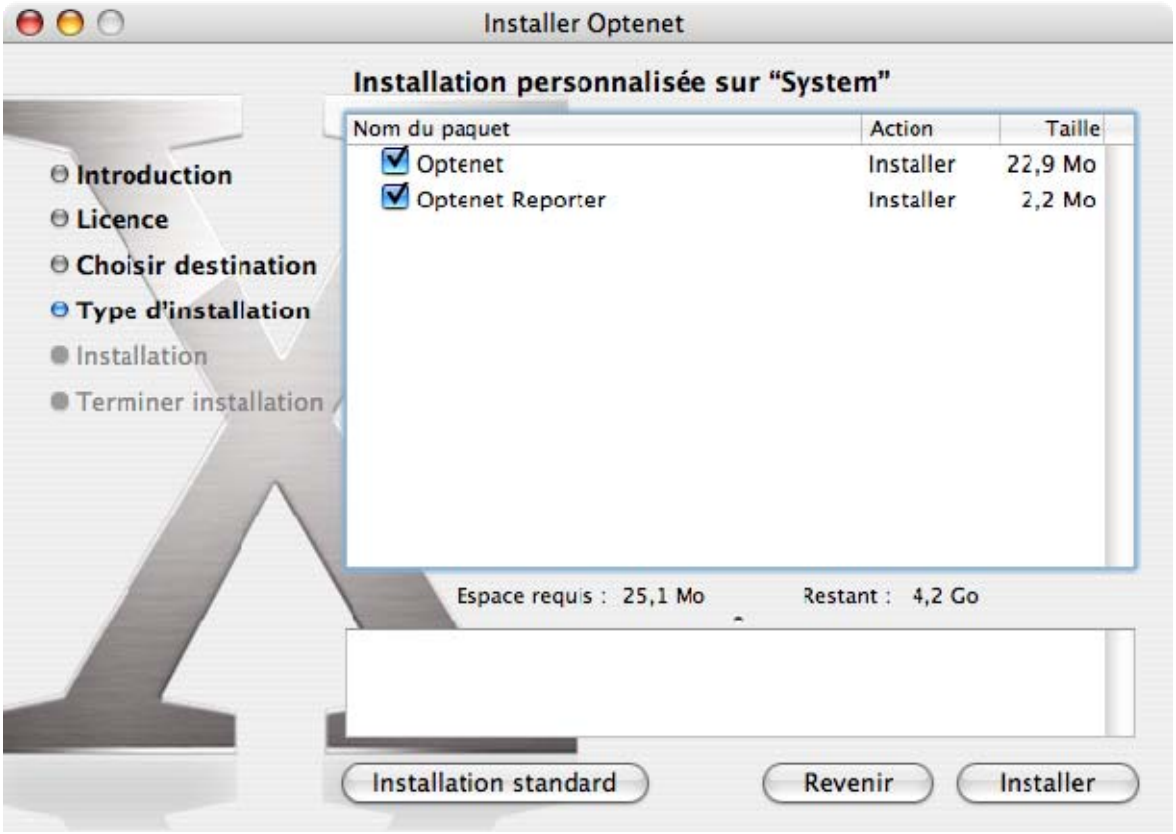
Vous pouvez alors imprimer ou enregistrer les conditions générales d'utilisation. En cliquant sur Continuer, Il vous sera demandé si vous acceptez ou refusez ces conditions d'utilisation.

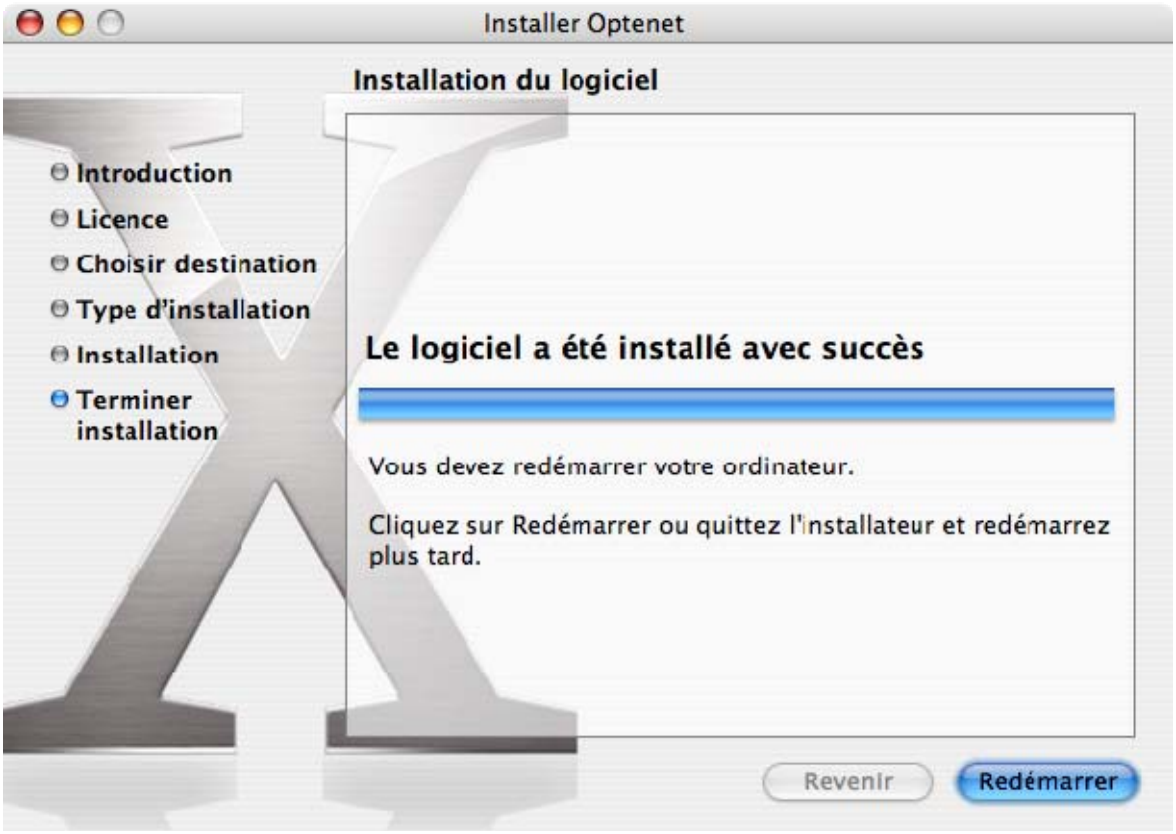


Vous devez ensuite choisir le volume de destination. OPTENET doit être installé sur le volume du système d'exploitation, ce volume est indiqué par un flèche verte.



Par la suite, vous pouvez lancer l'installation d'OPTENET Server et OPTENET Reporter en cliquant sur le bouton Installer. Si vous ne voulez installer que l'un des composants, cliquez sur le bouton Personnaliser et sélectionnez le composant choisi.





L'installation du logiciel s'exécute. OPTENET et son proxy Squid se lancent automatiquement au démarrage du système.

3.2.4. Système de fichiers installés par OPTENET

OPTENET Server installe les fichiers et les répertoires suivants à partir du répertoire d'installation:

manager.html Site HTML qui redirige à l'administration http d'OPTENET Server.
optenet.html Site HTML qui redirige au site Internetde la société OPTENET.

- Répertoire **bin:** où sont placés les DLL et exécutables d'OPENET Server.
optenet.exe L'exécutable du service d'OPTENET Server en Linux.
Optenet_service.exe l´exécutable du service OPTENET Server en Windows NT, Windows 2000, Windows XP et Windows 2003.
Optenet process.exe l´exécutable du service OPTENET Server en Windows 98 et WindowsME.
messages.dll La DLL avec les messages des évènements d'OPTENET Server. Seulement sous Windows.
metabase.dll DLL avec des fonctions auxiliaires pour l'installation et la désinstallation d'OPTENET Server. Seulement sous Windows.

- Répertoire **etc:** Fichiers de configuration d'OPTENET Server.
***.conf** Fichiers de configuration d'OPTENET Server. Ces fichiers ne doivent pas être modifiés. La configuration doit être réalisée exclusivement au travers de l´administration WWW d'OPTENET.

- Répertoire **files:** avec les bases de données d'URL et les analyseurs d'OPTENET Server.

***useryes.edu** Fichiers avec les URL appartenant aux catégories. Ce sont des fichiers de texte simple qui peuvent être modifiés pour ajouter, changer ou éliminer des URL manuellement.

***usernot.edu** Fichiers avec les URL n'appartenant pas aux catégories. Ce sont des fichiers de texte plat qui peuvent être modifiés pour ajouter, changer ou éliminer des URL manuellement. Avec les fichiers *useryes.edu ils forment la base de données locale d'URL. Au début ils n'existeront pas puis ils seront créés au fur et à mesure que des URL seront ajoutées.

list.crp Fichier crypté et compressés avec l'ensemble de listes générales d'URL classés. Dans le cas de la corruption d'un des fichiers *.edu il est décompressé pour récupérer les données. Ce fichier apparaît à partir du 2ème jour.

Listxxxx.crp Fichier pour l'actualisation de la base de données générale d'URL et analyseurs d'OPTENET Server. C'est un fichier compressé qui n'apparaît que lors du processus de rechargement manuel de listes complètes car il est éliminé après la mise à jour.

categoryuserex.edu: Fichier avec la description des catégories ajoutées par l'administrateur.

- Répertoire **logs:** emplacement où par défaut sont gardés les logs générés par OPTENET Server.

updates.log Fichier avec les résultats des mises à jour automatiques réalisées par OPTENET Server.

requestYYYYMMDD.log Fichier avec toutes les demandes et blocages HTTP réalisées avec OPTENET Server qui correspondent au jour DD du mois MM de l'année YYYY. Par exemple, request20040422.log contient les demandes et les blocages qu'OPTENET a réalisé le 22 avril 2004.

cluster.log Fichier avec informations relatives à la gestion en clusters.

actions.log Fichier qui garde l'enregistrement d'actions sur l'administration.

- Répertoire **manager:** contient les fichiers nécessaires pour les pages HTML utilisées par l'administration WWW d'OPTENET Server.

index.html Page par défaut de l'administration WWW d'OPTENET Server. Il redirectionne à l'administration WWW.

- - Répertoire **esp:** contient les pages de l'administration WWW d'OPTENET Server en espagnol.
- - Répertoire **eng:** contient les pages de l'administration WWW d'OPTENET Server en anglais.
- - Répertoire **fra:** contient les pages de l'administration WWW d'OPTENET Server en français.
- - Répertoire **deu:** contient les pages de l'administration WWW d'OPTENET Server en allemand.
- - Répertoire **ita:** contient les pages de l'administration WWW d'OPTENET Server en italien.
- - Répertoire **por:** contient les pages de l'administration WWW d'OPTENET Server en portugais.
- - Répertoire **eus:** contient les pages de l'administration WWW d'OPTENET Server en basque.

- - Répertoire **cgi-bin:** contient le code JavaScript utilisé par l'administration WWW d'OPTENET Server.

- - Répertoire **listclusters :** il contient l'exécutable pour la gestion en cluster.
- - Répertoire **stop :** emplacement où est stockée la page de stop locale. Il doit y avoir autant de dossiers que de langues.

- Répertoire **tools** contient des outils d'OPTENET Server
logrotate.bat Outil pour la rotation de fichiers journaux d'OPTENET Server. Seulement en système Linux et Solaris.

optenetcli (cli.conf) Application pour administrer OPTENET par lignes de commandes.
backup.bat Outil pour faciliter les copies de sécurité d'OPTENETServer.
restore.bat Outil pour restaurer les copies de sécurité réalisées au moyen de l'outil backup.bat.
OptenetSnmp (snmp.conf) : Exécutable de l'agent SNMP d'OPTENET Server. Seulement sous Linux.
stunnellauncher Exécutable pour administrer le filtre de forme sécurisée, https. Seulement sous Linux.
adduser.pl Script qui ajoute un utilisateur pour l'authentification NCSA avec Squid. Seulement avec proxy Squid et systèmes Linux.
addplugin.vbs Script qui ajoute le plugin d'OPTENET Server à Microsoft ISA Server. Seulement sous Windows pour ISA Server ou Proxy Server.
delplugin.vbs Script qui efface le plugin d'OPTENET Server de Microsoft ISA Server. Seulement sous Windows pour ISA Server ou Proxy Server.

Outre les fichiers qui sont installés dans le répertoire d'installation, OPTENET Server installe aussi:

un fichier dans le répertoire d'installation de Microsoft ISA Server (par défaut C:\Program Files\Microsoft ISA Server). Ce fichier s'appelle **optenet.dll** et c'est la DLL qui réalise les fonctions de ***plugin*** de capture de données d'OPTENET Server.

3.3. Démarrage et arrêt

3.3.1. Sous Windows

3.3.1.1. Début et arrêt du filtre sous Windows NT, XP, 2000 et 2003

La partie principale d'OPTENET Server consiste en un service de filtrage. Ce service peut être administré à partir des services de Windows comme tout autre service, il peut être démarré, arrêté, on peut établir son type de démarrage, etc..

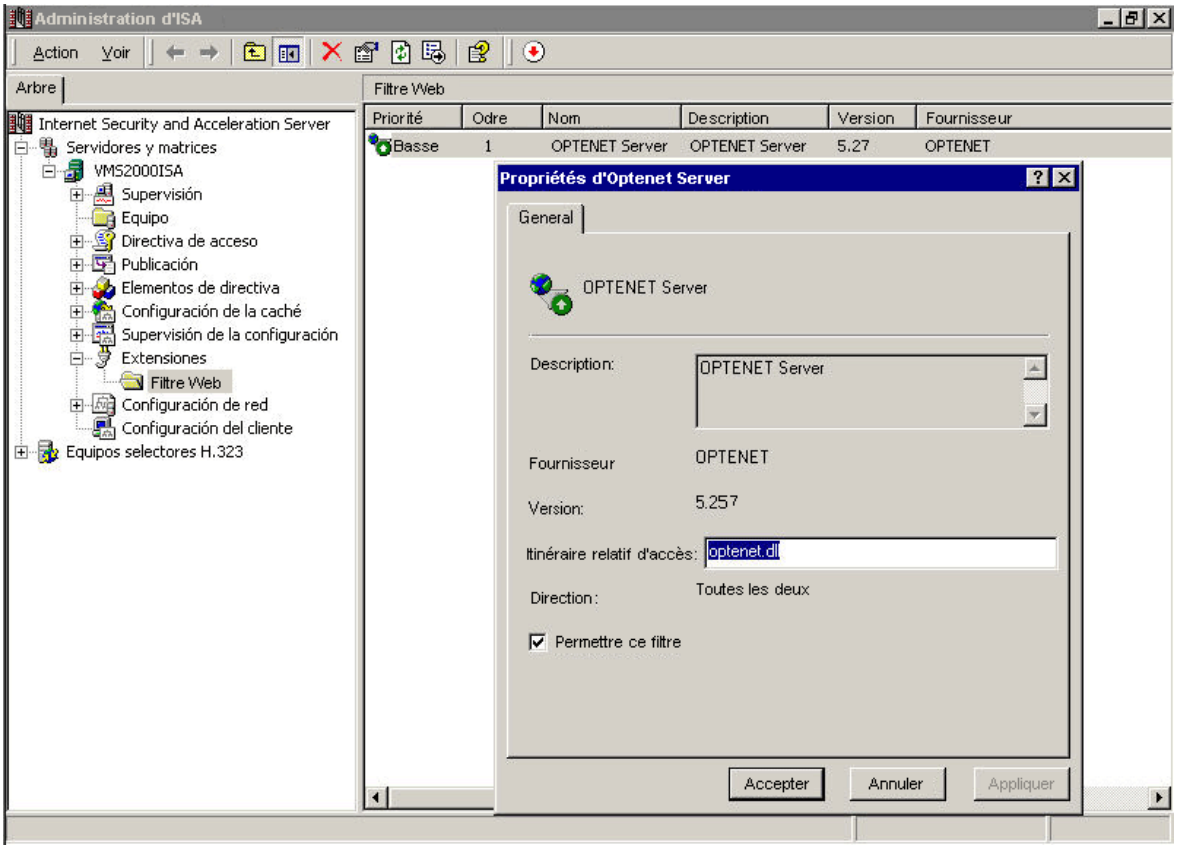
Ledémarrage du service d'OPTENET Server requiert un certain temps (environ 3 secondes) pendant lequel l'unité centrale du Server est utilisée à presque 100% : les bases de données des URL sont chargées ainsi que les moteurs d'analyse en mémoire, le processus d'actualisation automatique est lancé ainsi que l'administration http d'OPTENET Server. En cas de problèmes, OPTENET Server écrit un message dans l'Observateur d'événements du Server.

3.3.1.2. Début et arrêt sous Windows 98

Comme sous Windows 98 le concept de services de système est différent ; les deux parties , le proxy OPTENET et Optenet Server, sont installés comme processus habituels. Ils sont lancés en démarrant le système d'exploitation. (Voir paragraphe 3.2.1.1)

3.3.1.3. Le plugin pour Microsoft ISA Server

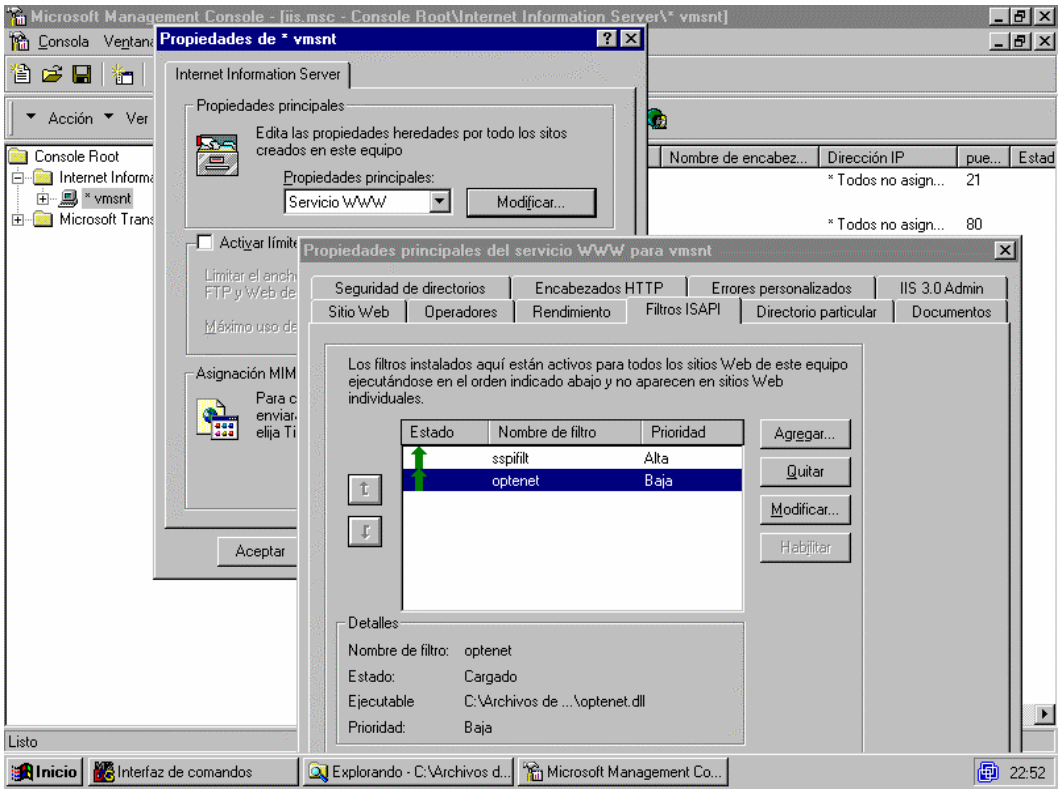
L'autre partie d'OPTENET Server, le plugin pour la saisie de données, est un filtre Web de Microsoft ISA Server et il peut être contrôlé à partir de l'administration du Server ISA. Tout comme tout autre filtre web, il peut être activé ou désactivé selon les besoins (voir Figure ci dessous). Il pourra être démarré ou
arrêté au moyen du service Microsoft Web Proxy.



Les deux parties d'OPTENET Server sont indépendantes et peuvent être démarrées ou arrêtées séparément mais pour que le filtrage puisse avoir lieu les deux parties doivent être en marche simultanément.

3.3.1.4. Le plugin pour Microsoft Proxy Server

L´autre partie de'Optenet Server, le plugin pour la capture de données, s´agit d´un filtre ISAPI installé dans votre Server web où est installé Proxy Server. Celui ci peut être contrôler à partir de la console d´administration de votre Proxy Server. Tout comme tout autre filtre ISAPI, il peut être activé ou désactivé selon vos besoins (voir la figure suivante).



Les deux parties d'Optenet Server sont indépendantes l´une de l´autre et peuvent être activé ou désactivé séparément mais pour que le filtrage puisse avoir lieu les deux doivent fonctionner ensemble.

3.3.1.5. OPTENET Proxy

Dans la version stand-alone, OPTENET proxy est intégré, traitant les demandes HTTP et HTTPS au lieu de Microsoft ISA Server. Il est visible par une icône de la barre d'outils. S'il faut utiliser un proxy supplémentaire en cascade, il faut introduire son adresse IP et le port dans la fenêtre « configuration » de l'icône. Notez que pour un usage normal sans proxy supplémentaire, il n'est pas nécessaire d'ajouter de type de configuration dans ce paragraphe. Consulter l´annexe 4 si vous désirez savoir plus sur comment configurer ce proxy.

3.3.2. Sous Linux, Solaris et AIX

Pour démarrer OPTENET, entrez dans le système en utilisant le nouvel utilisateur créé et exécutez le script filterinit. Ce script admet les paramètres start, stop et restart.
Pour démarrer le filtre, vous devez exécuter :

```
# ./filterinit start
```

Pour l'arrêter, exécutez:

```
# ./filterinit stop
```

Vous pouvez également le redémarrer en exécutant:

```
# ./filterinit restart
```

Si vous rencontrez des problèmes lors de l'installation, vous pouvez bénéficier d'un support technique en écrivant à support@optenet.com

3.3.3. Sous Mac OS X

Pour démarrer OPTENET, entrez dans le système via l'utilitaire terminal. Vous devez être en administrateur et taper la commande suivante:

```
# sudo su – optenet
```

Entrez votre mot de passe. Ce script admet les paramètres start, stop et restart.
Pour démarrer le filtre, vous devez exécuter:

```
# ./filterinit start
```

Pour l'arrêter, exécutez:

```
# ./filterinit stop
```

Vous pouvez également le redémarrer en exécutant:

```
# ./filterinit restart
```

Si vous rencontrez des problèmes lors de l'installation, vous pouvez bénéficier d'un support technique en écrivant à info@optenet.com

3.4. Démarrage et arrêts automatiques en fonction du système

3.4.1. Sous Windows:

Avec la configuration par défaut après l'installation, le démarrage et l'arrêt se réalisent automatiquement avec le système. Pour ne pas qu'il démarre avec le système, il faut aller à l'outil du système "Outils d'administration" et dans la section"Services", il faut modifier le "Type de démarrage" du service "OPTENET Server" comme "Manuel".

3.4.2. Sous Linux

Dans la configuration par défaut après l'installation, le démarrage et l´arrêt d'OPTENET se réalise automatiquement avec le système. Pour établir OPTENET en tant que service sur le Server de manière manuel afin qu'il démarre et s'arrête automatiquement à chaque démarrage ou arrêt du système, connectez-vous comme utilisateur racine et suivez les étapes ci-après:

Sur les systèmes Linux disposant de l'outil chkconfig (Red Hat):

```
# cp /usr/local/optenet/optenet/tools/optenet /etc/rc.d/init.d
# chkconfig --add optenet
```

Vous pouvez vérifier la correcte installation d'OPTENET en tant que service à l'aide de la commande:

```
#chkconfig –list
```

Sur les systèmes Linux qui ne disposent pas de l'outil chkconfig:

```
# cp /usr/local/optenet/optenet/tools/optenet /etc/init.d
# cp -s /etc/init.d/optenet /etc/rc.d/rc3.d/S99optenet
# cp -s /etc/init.d/optenet /etc/rc.d/rc3.d/K99optenet
```

3.4.3. Sous Solaris

Dans la configuration par défaut après installation le démarrage et l´arrêt d'OPTENET se réalise automatiquement avec le système. Pour établir OPTENET en tant que service sur le Server de manière manuel afin qu'il démarre et s'arrête automatiquement à chaque démarrage ou arrêt du système, connectez-vous comme utilisateur racine et suivez les étapes ci-après:

```
# cp /usr/local/optenet/tools/optenet /etc/init.d
# link /etc/init.d/optenet /etc/rc2.d/S99optenet
# link /etc/init.d/optenet /etc/rc2.d/K99optene
```

3.4.4. Sous AIX:

Dans la configuration par défaut après installation le démarrage et l´arrêt d'OPTENET se réalise automatiquement avec le système. Pour établir OPTENET en tant que service sur

le Server de manière manuel afin qu'il démarre et s'arrête automatiquement à chaque démarrage ou arrêt du système, connectez-vous comme utilisateur racine et suivez les étapes ci-après:

```
# cp /usr/local/optenet/tools/optenet /etc/rc.optenet
# nkitab ¨optenet :2 :once:/etc/rc.optenet. start¨
```

3.4.5. Sous Mac OS X:

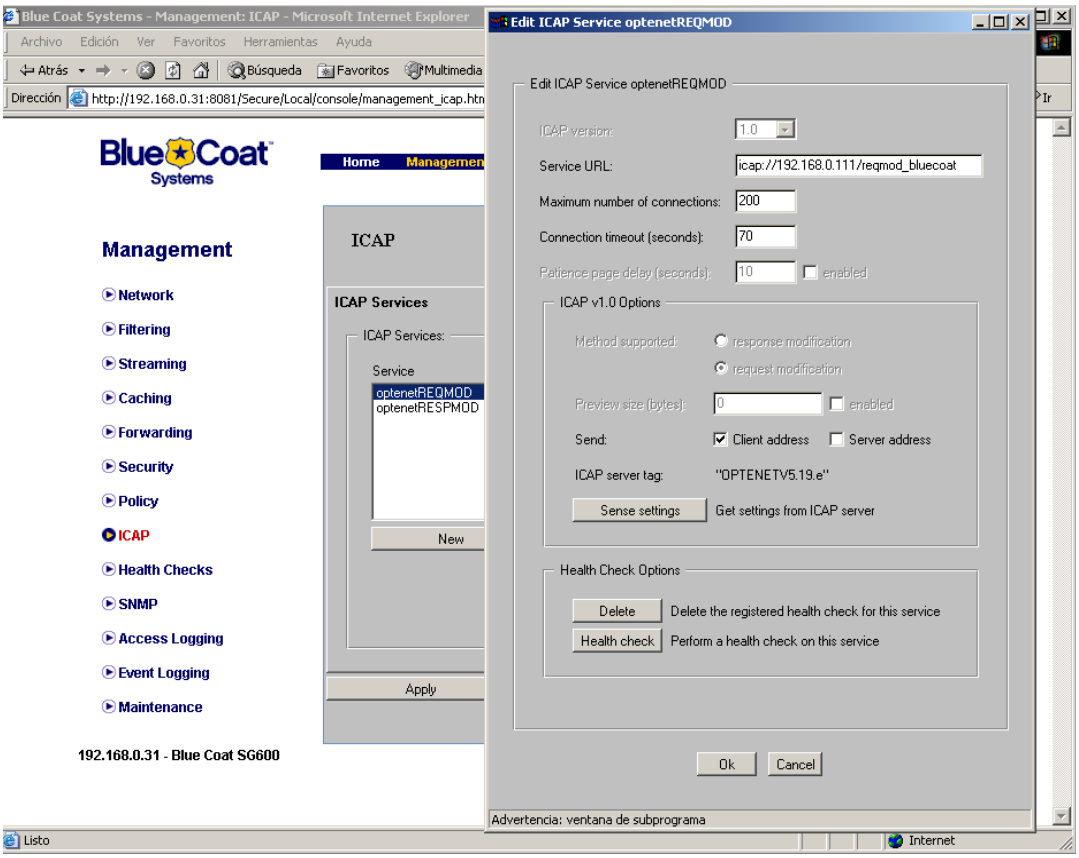
Dans la configuration par défaut après installation le démarrage et l´arrêt d'OPTENET se réalise automatiquement avec le système. Mac OS X démarre automatiquement OPTENET grâce au script « Optenet » qui est placé dans /Library/StartupItems/Optenet.

3.5. Configuration d'une Appliance BlueCoat pour qu'il utilise OPTENET comme système de filtrage (ICAP)

Pour qu'OPTENET puisse communiquer au moyen du protocole ICAP avec son Appliance de BlueCoat, ce dernier doit être muni du système d'exploitation Security Gateway 2.1.06 ou ultérieur. Il est décrit ci-après la manière de configurer un Appliance de BlueCoat (avant CacheFlow) pour qu'il utilise OPTENET comme système de filtrage. Pour cela, procéder comme suit:

3.5.1. Créer un service de modification de demande (REQMOD)

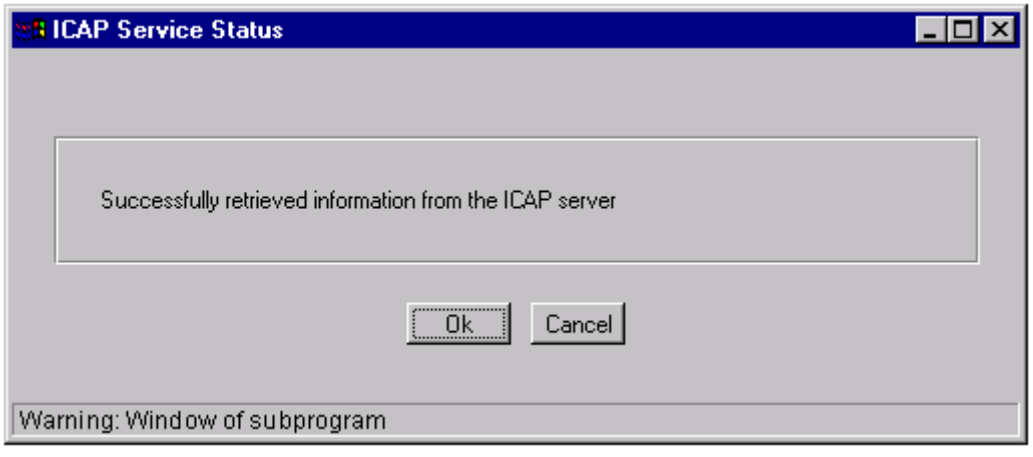
Connectez-vous à l'administration de votre BlueCoat puis allez à l'option ICAP. Sur le volet ICAP Services, pressez le bouton "New" et créez-en un selon la figure:



Dans la case "ICAP version", il faut assigner la version 1.0. d'ICAP. Dans le paragraphe Service URL, il faut indiquer l'URL à laquelle seront envoyées les demandes ICAP par exemple:

icap://192.168.0.111/reqmod bluecoat

Notez que l'IP correspond à l'IP de la machine où a été installé OPTENET et qu´on utilise comme route /reqmod_bluecoat. Il est important de maintenir cette nomenclature pour que le Server ICAP d'OPTENET s´intègre correctement avec votre BlueCoat. Maintenant, il faut marquer comme méthode "request modification" et utiliser la touche "Sense settings" pour forcer BlueCoat à se connecter avec OPTENET et obtenir ainsi automatiquement les autres paramètres de configuration du Server ICAP.
Notification d'obtention de paramètres automatique réussie.



Si pour une raison quelconque, la communication avec le Server ICAP ne fonctionne pas, vous pouvez configurer manuellement les autres champs. Il faudra sélectionner également la case “Client address” (disponible à partir de la version SG 2.1.07) pour activer l'envoi dans le message ICAP de l'adresse IP du client qui a réalisé la demande.

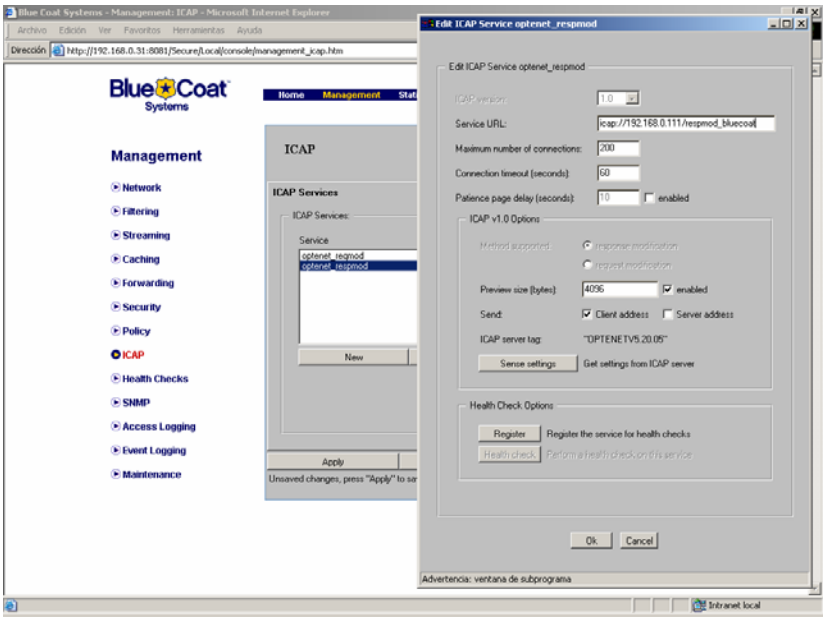
3.5.2. Créer un service de modification de réponse (RESPMOD)

Connectez-vous à l'administration de votre BlueCoat puis allez à l'option ICAP. Sur le volet ICAP Services, pressez le bouton “New” et créez-en un selon la figure:

Dans la case “ICAP version”, il faut assigner la version 1.0 d'ICAP. Dans le paragraphe “Service URL”, il faut indiquer l'URL à laquelle seront envoyées les demandes ICAP par exemple:

icap://192.168.0.111/respmod bluecoat

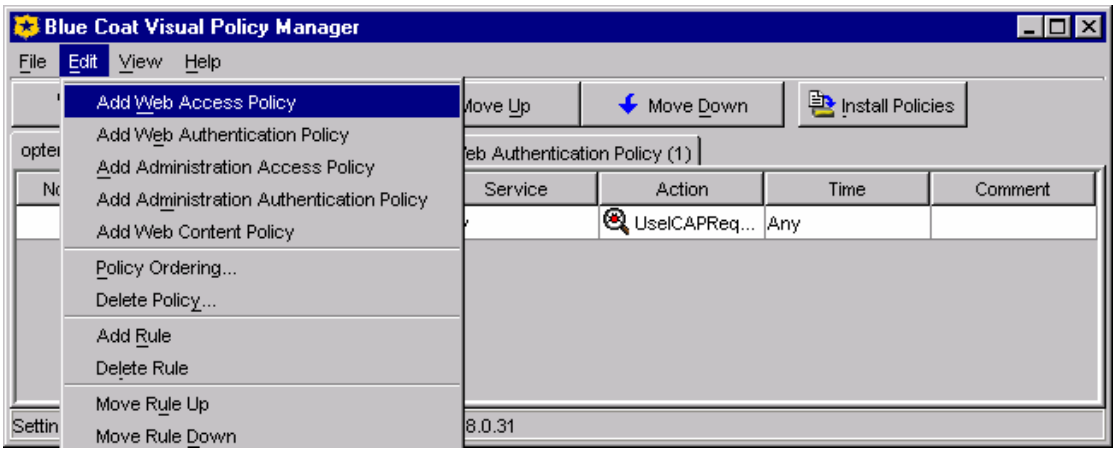
Notez que l'IP correspond à l'IP de la machine où a été installé OPTENET et qu´on utilise comme route /respmod_bluecoat. Il est important de maintenir cette nomenclature pour que le Server ICAP d’OPTENET s´intègre correctement avec votre BlueCoat. Maintenant, il faut marquer comme méthode "response modification" et utiliser la touche "Sense settings" pour forcer BlueCoat à se connecter avec OPTENET et obtenir ainsi automatiquement les autres paramètres de configuration du Server ICAP. Il faudra sélectionner la case "Client address" (disponible à partir de la version SG 2.1.07) pour activer l'envoi dans le message ICAP de l'adresse IP du client qui a réalisé la demande.



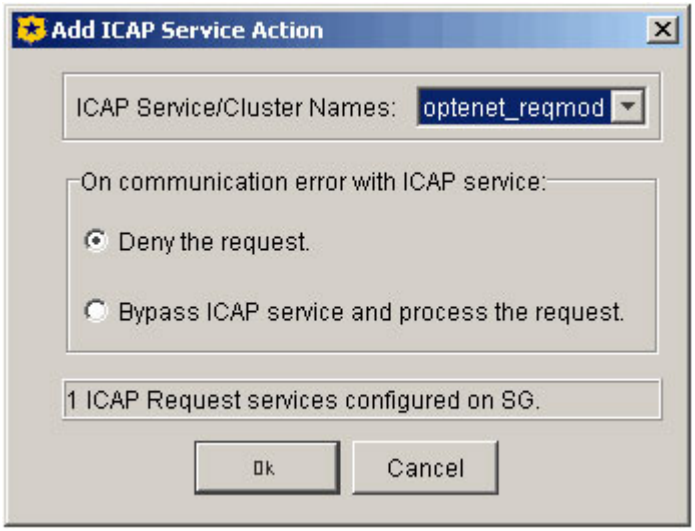
3.5.3. Établir une politique d'accès web

Une fois les services ICAP configurés, il faut indiquer si toutes les demandes sont reconduites par OPTENET. Pour cela, il faut aller à l'option Policy, onglet Visual Policy Manager et appuyer sur le bouton Start pour lancer le Visual Policy Manager.

Une fois lancé, sélectionnez le menu Edit -> Add Web Access Policy comme il est indiqué sur la figure:



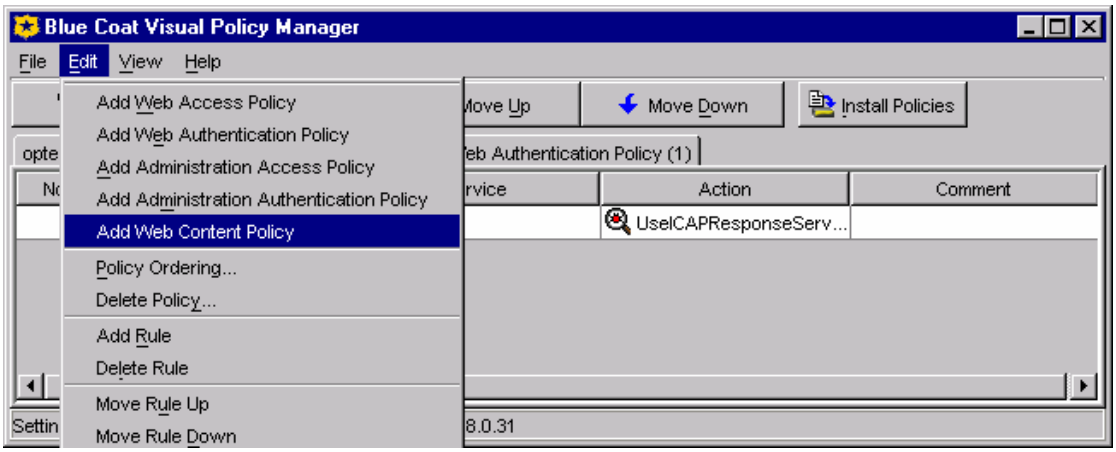
Il faut configurer l'action de cette nouvelle politique pour qu'à toutes les demandes de tous les clients, le service ICAP que nous avons appelé optenetreqmod soit utilisé. De cette manière, il est indiqué à BlueCoat qu´il envoie à OPTENET Server tous les accès web qui sont réalisés à travers ce dernier pour qu'ils puissent être analysées puis autorisées ou refusées.



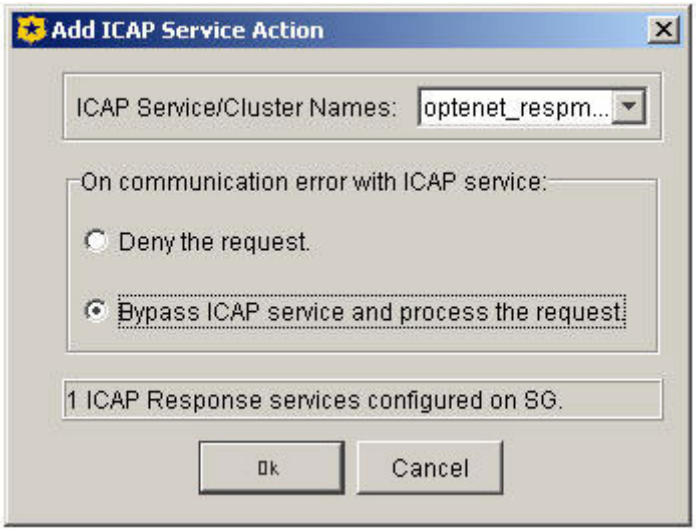
Pour sauvegarder les changements dans l'Appliance, il faudra presser la touche “Install Policies” avant de fermer le Visual Policy Manager.

3.5.4. Établir une politique de contenus web

OPTENET à la différence de la plupart des systèmes de filtrage analyse le contenu téléchargé d'Internet permettant de classer des sites selon leur contenu ou détecter le type réel de fichiers rebaptisés. Pour cela, il faut que BlueCoat passe à OPTENET le contenu déchargé avant d'être retourné au client qui l'a demandé.
Ceci est possible en définissant une politique de contenu web. Pour cela, il faut aller à l'option Policy, onglet Visual Policy Manager et boutton Start pour lancer le Visual Policy Manager.Une fois lancé, sélectionnez le menu Ediit -> Add Web Content Policy comme il est indiqué sur la figure:



Il faut configurer l'action de cette nouvelle politique pour que le contenu de toutes les demandes de tous les clients utilise le service ICAP que nous avons appelé optenetrespmod. De cette manière, il est indiqué au BlueCoat que tous les contenus web qui sont téléchargés à travers ce dernier avant d'être retournés aux clients soient envoyés à OPTENET pour qu'ils puissent être analysés puis autorisés ou refusés.



Pour garder les changements dans l'Appliance, il faudra appuyer sur le boutton “Install Policies” avant de fermer le Visual Policy Manager.

Pour activer l'authentification des utilisateurs, il faut lancer le Visual Policy Manager et créer une politique d'authentification Web. Pour plus d'informations, consultez la documentation deBlueCoat.

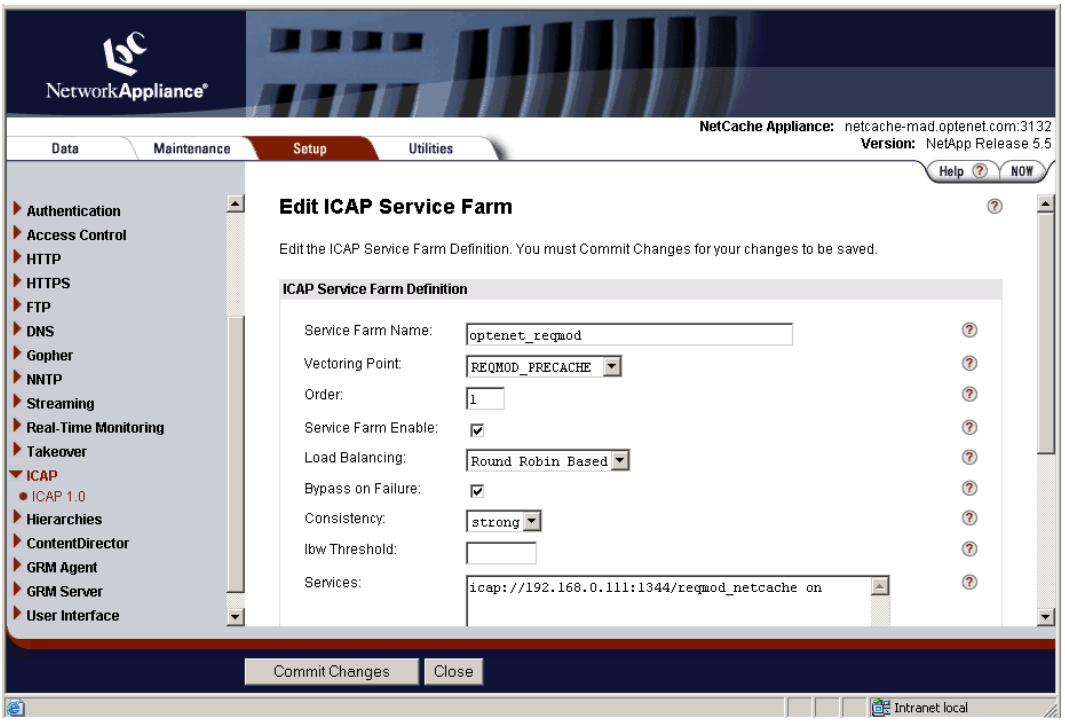
Après avoir réalisé ce dernier point, BlueCoat sera configuré pour qu'il utilise OPTENET comme système de filtrage.

3.6. Configuration d'un NetCache pour qu'il utilise OPTENET comme système de filtrage

La manière de configurer NetCache pour qu'il utilise OPTENET comme système de filtrage est décrite ci-après. Pour cela, il faut suivre les étapes suivantes:

3.6.1. Créer un service de modification de demande (REQMOD)

Connectez-vous à l'administration NetCache et allez à l'option Setup→ ICAP → ICAP1.0
Sur l'onglet ServiceFarm, pressez la touche "New Service Farm" et créez-en un selon la figure:



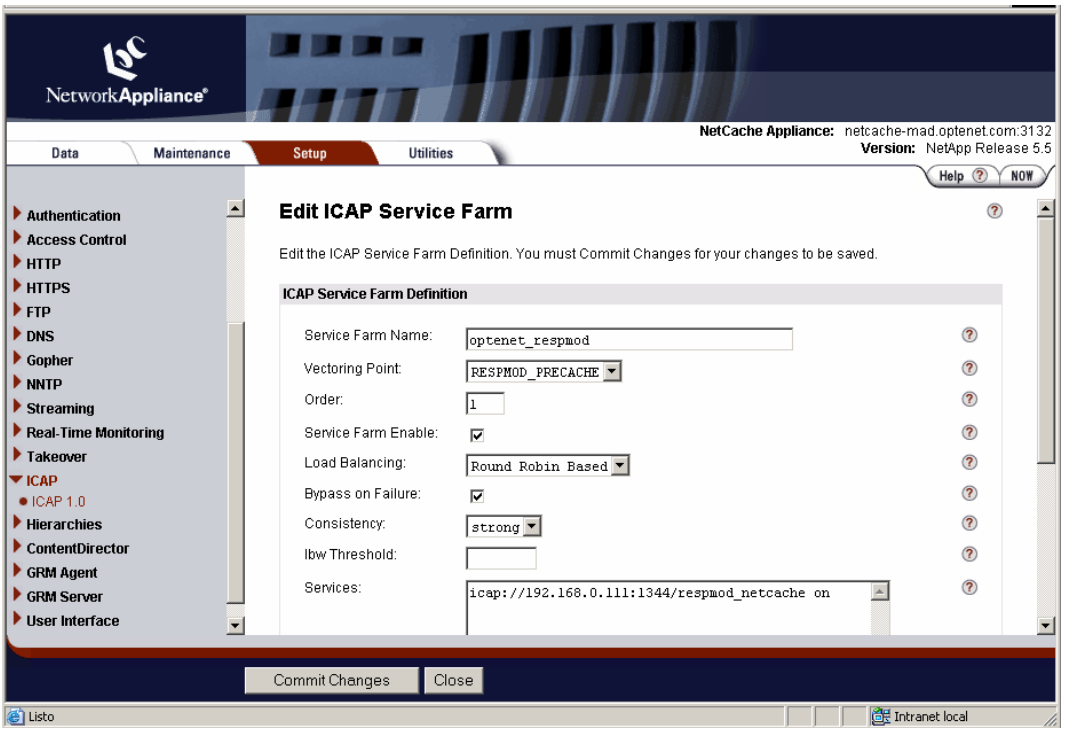
Dans la case "services", il faut indiquer l´URL où les demandes de ICAP vont être envoyées, par exemple:

icap://192.168.0.111:1344/reqmod_netcache on

Remarquer que l´IP correspond avec l´IP de la machine où est installé OPTENET et qu´on utilise comme route /reqmod_netcache. Il est important de maintenir cette nomenclature pour que le Server ICAP d'OPTENET s´intègre correctement avec votre NetCache.
Appuyer sur ¨Commit Changes¨ pour sauvegarder les changements.

3.6.2. Créer un service de modification de réponse (RESPMOD)

Recréez un nouveau Service Farm selon la figure suivante:



Dans la case “Service URL”, il faut indiquer l'URL à laquelle seront envoyées les demandes ICAP par exemple:

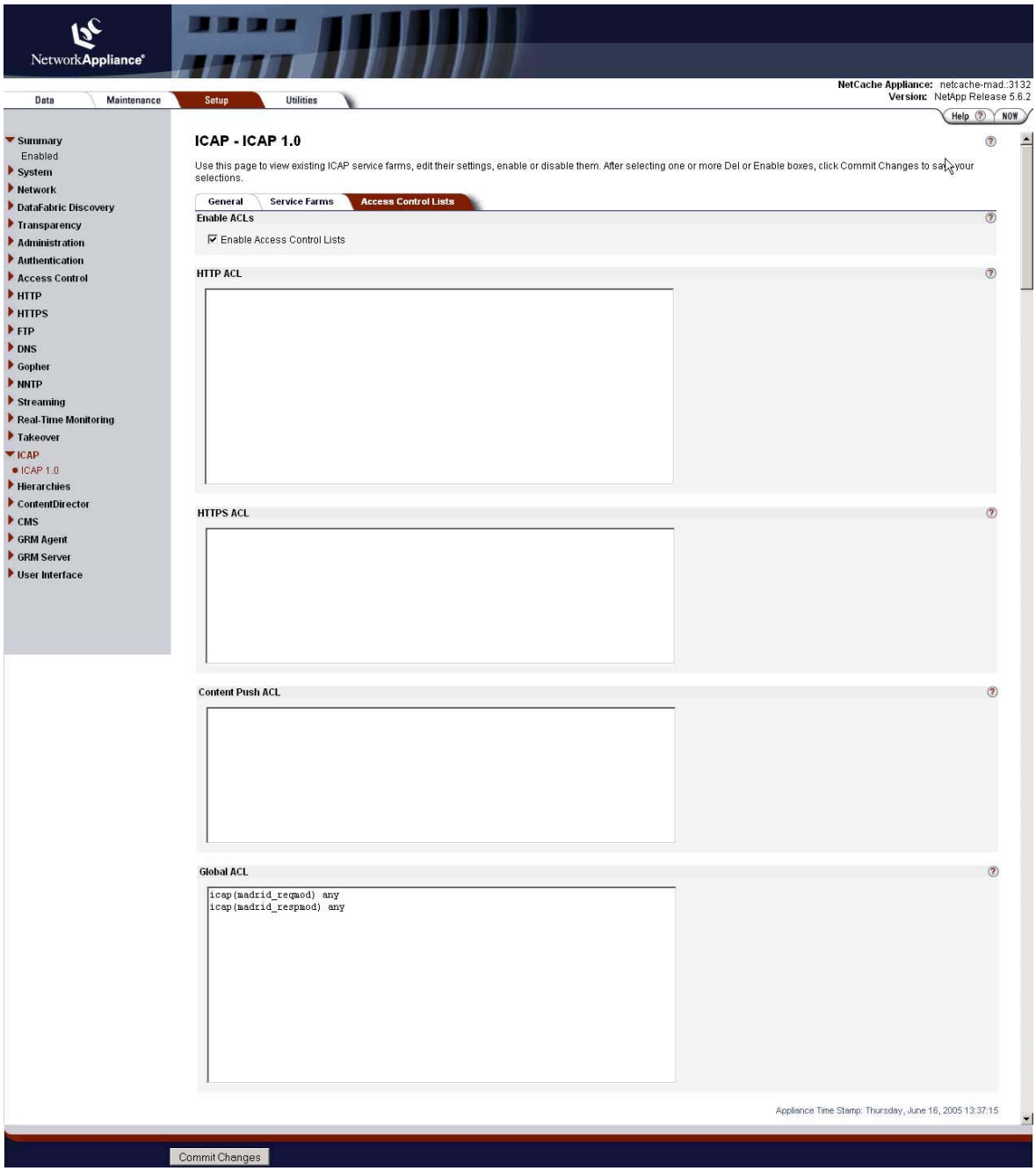
icap://192.168.0.111:1344/respmod_netcache on

Notez que l'IP correspond à l'IP de la machine où a été installé OPTENET et qu´on utilise comme route /respmod_netcache. Il est important de maintenir cette nomenclature pour que le Server ICAP d’OPTENET s´intègre correctement avec votre NetCache.

La raison de la création de deux Service Farms est qu'OPTENET, à la différence de la plupart des autres systèmes de filtrage, analyse le contenu téléchargé d'Internet, permettant de catégoriser les pages en fonction de leurs contenus ou détecter le véritable type de fichier qui ont été renommé. Le premier Service Farm permettra que, lorsque NetCache reçoit une demande, avant de s'en occuper, il passera l'URL demandée à OPTENET pour qu'il puisse décider si l'accès est autorisé. Cette décision est prise en vérifiant cette URL dans la base de données d'OPTENET et en analysant l’ URL.

Le deuxième Service Farm permet que, lorsque NetCache apporte un contenu d'Internet, avant de le stocker dans son cache, il passe à OPTENET ce contenu. OPTENET l'analysera et décidera s'il est autorisé ou s'il doit être bloqué.

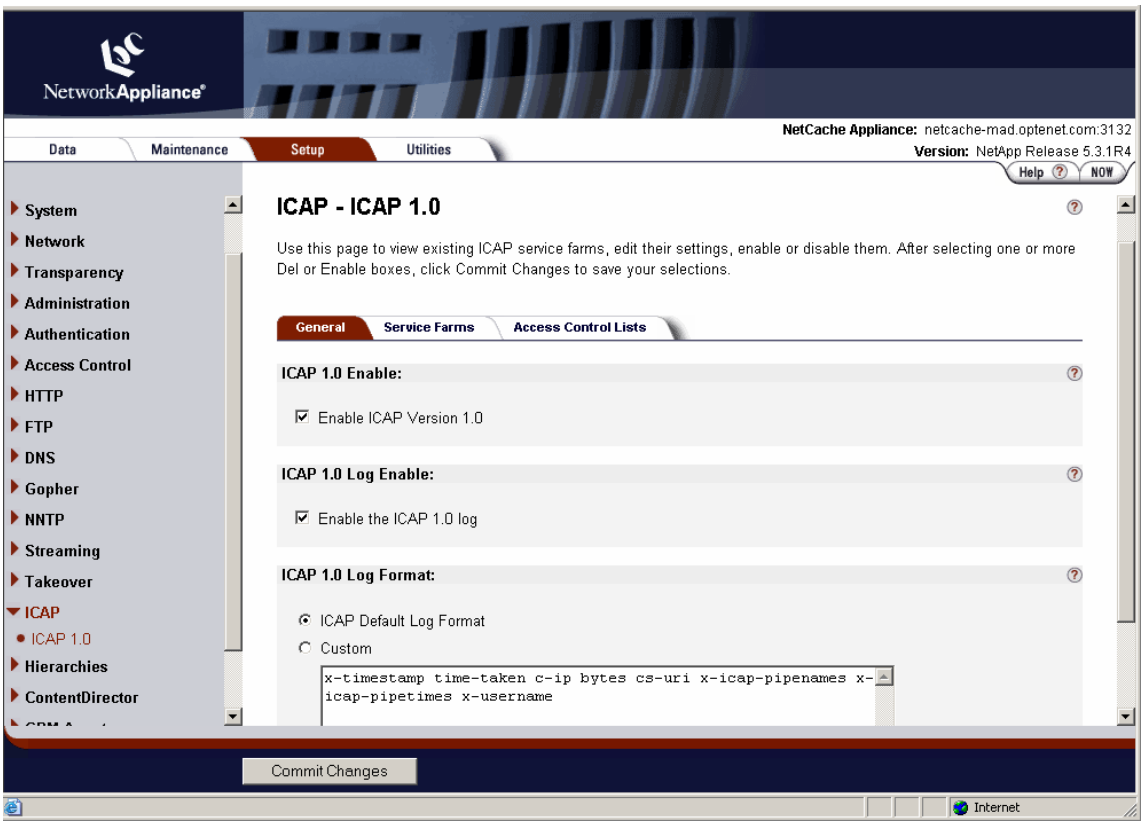
Une fois les Service Farm définis, il faut indiquer à quelles demandes il faut appliquer le filtre. Pour cela, il faut aller à l'option Access Control List et la configurer selon la figure.



C'est à dire en appliquant le filtre à toutes les demandes aussi bien http, https que ftp.

Enfin, il reste à activer le service ICAP de l'onglet General selon la figure.

Si vous souhaitez activer l'authentification d'utilisateurs, vous pouvez consulter la documentation de NetCache.


NetworkAppliance
NetCache Appliance: netcache-mad.optenet.com:3132
Version: NetApp Release 5.3.1R4
Data
Maintenance
Setup
Utilities
Help
NOW
System
Network
Transparency
Administration
Authentication
Access Control
HTTP
FTP
DNS
Gopher
NNTP
Streaming
Takeover
ICAP
ICAP 1.0
Hierarchies
ContentDirector
ICAP - ICAP 1.0
Use this page to view existing ICAP service farms, edit their settings, enable or disable them. After selecting one or more Del or Enable boxes, click Commit Changes to save your selections.
General
Service Farms
Access Control Lists
ICAP 1.0 Enable:
Enable ICAP Version 1.0
ICAP 1.0 Log Enable:
Enable the ICAP 1.0 log
ICAP 1.0 Log Format:
ICAP Default Log Format
Custom
x-timestamp time-taken c-ip bytes cs-uri x-icap-pipenames x-icap-pipetimes x-username
Commit Changes
Internet

4. CONCEPTS DE BASE

Nous allons maintenant vous expliquer quelques concepts de base nécessaires à l' administration d'OPTENET. Ces concepts apparaissent dans la partie Administration.

4.1. Utilisateur

Comme OPTENET communique avec un proxy (comme SQUID, ISA ou proxy OPTENET) ou avec un appliance ou cache qui font les fonctions de proxy comme BlueCoat ou NetCache), le concept d'utilisateur est similaire au concept d'utilisateur pour ces proxys. En d'autres termes, OPTENET reconnaît les utilisateurs identifiés par ces proxys. **Attention :** Ces utilisateurs peuvent être indépendants des utilisateurs des systèmes d'exploitation de tous les postes qui accèdent à Internet via le proxy. Cependant, OPTENET permet d'authentifier également les utilisateurs des domaines NT ou Servers LDAP.

4.2. Groupe

Normalement, les utilisateurs peuvent faire partie d'un ou plusieurs groupes. Ni ISA, ni SQUID, ni même des versions de BlueCoat antérieures à la version 3 ne transmettent d'informations à OPTENET en révélant les groupes auxquels appartient l'utilisateur en train d'effectuer une demande. Seuls NetCache et BlueCoat, à partir de la version 3 comprise, sont en mesure de fournir ces informations. Il en résulte que, pour qu'OPTENET puisse obtenir ces informations, la communication devra être établie en utilisant un certain nom de domaine NT ou Server LDAP. Pour configurer ce service, veuillez vous référer à la section 5.4 de ce manuel.

4.3. Adresse IP

TCP/IP est le sigle de Transmission Control Protocol/Internet Protocol, le langage qui régit toutes les communications entre les ordinateurs sur Internet. Tous les ordinateurs connectés à Internet disposent d'une adresse unique au format suivant:

aaa.bbb.ccc.ddd

Les adresses IP des ordinateurs clients qui vont accéder à Internet vont donc pouvoir faire partie des règles d'OPTENET.

Cependant, il faut tenir compte du fait que parfois, un proxy enchaîné est installé avant le filtre, toutes les demandes étant alors identifiées avec l'IP de ce proxy. Consultez la configuration de votre proxy dans ce cas.

4.4. URL

Sigle d'Uniform Resource Locator. Il s'agit de l'adresse d'un site ou d'une source, généralement un répertoire ou un fichier, se trouvant sur le World Wide Web, ainsi que de la convention utilisée par les navigateurs pour trouver des fichiers et d'autres ressources distantes. Une URL peut identifier un fichier, par exemple:

http://www.optenet.com/fra/index.htm

ou un site:

http://www.optenet.com

Grâce à OPTENET, vous pouvez autoriser ou bloquer l'accès à des pages concrètes en indiquant l'URL ou à des sites entiers ou à des parties de sites en indiquant l'URL suivie d'un astérisque. Par exemple:

http://www.siteentier.com/*

OPTENET fonctionne en interne avec des URL sans protocole (http, https, …). Si l'on saisit une url dans une catégorie déterminée, tous les protocoles relatifs à cette url appartiendront automatiquement à cette catégorie.
Par exemple, en saisissant http://www.siteentier.com en pornographie, les url suivantes vont être réparties en différentes catégories de pornographie:
http://www.siteentier.com
https://www.siteentier.com
ftp://www.siteentier.com

4.5. Catégorie

Une catégorie est un ensemble regroupant les fichiers du réseau World Wibe Web. Ces ensemblespeuvent être créés par le biais de listes d'URL et d'analyseurs de contenus et d'URL.

Cinq types de catégories sont établis:
- Catégories de contenus: elles répertorient le World Wide Web en contenus (par exemple : pornographie, sports, presse, etc.) qui sont soit admis ou rejetés selon les options établies dans les règles de filtrage.
- Catégorie blanche : si un fichier appartient à une catégorie blanche, ses catégories de contenus ne seront pas prises en compte; ce sera comme s'il n'appartenait à aucune catégorie de contenus.
- Catégorie noire : si un fichier est répertorié dans cette catégorie, ce sera comme s'il appartenait à l'ensemble et à chacune des catégories de contenus.
- Catégories moteurs de recherche : les fichiers appartenant à une catégorie de moteurs de recherche ne tiendront pas compte de l'option d'analyse de contenus multilingue pour établir ses catégories de contenus.
- Catégories de redirection : il s'agit de fichiers qui redirigent ou transforment d'autres fichiers. Si un fichier appartient à une catégorie de redirection, il sera travaillé directement avec l'autre fichier qu'il redirige ou transforme.

Une catégorie pourra posséder plus d'un type. A son tour, un fichier pourra appartenir à plus d'une catégorie.

Chaque catégorie utilise deux listes d'URL pour être définie : Oui et Non. La liste Oui contient toutes les adresses que nous considérons appartenir à une catégorie déterminée et la liste Non répertorie toutes les adresses que nous considérons NE PAS appartenir à cette catégorie.

A la fin de ce manuel, une annexe décrit les catégories fournies par OPTENET.

4.6. Règle

Il s'agit du concept fondamental sur lequel se base le fonctionnement d'OPTENET. Les règles définissent le niveau de filtrage que vont avoir tous les accès à Internet.
Une règle permet de définir:

- Les catégories auxquelles s'applique cette règle.
- Les utilisateurs affectés par cette règle.
- Les groupes d'utilisateurs affectés par cette règle.
- Les adresse IP des postes affectés par cette règle.
- Les types de fichiers pouvant être affectés par cette règle.
- Les horaires d'application de cette règle.
- Pour les URL auxquelles doit s'appliquer la règle, indépendamment de leur catégorie et du type de fichier, du moment où les autres caractéristiques sont remplies (jour et heure, utilisateur, groupe ou adresse IP), la règle jouera son rôle.
- Les URL qui ne respecteront jamais cette règle. Nous pouvons, sous cette forme, définir des exceptions au fonctionnement de chaque règle.

5. ADMINISTRATION

Après l'installation d'OPTENET Server, il est nécessaire d'effectuer une configuration minimum. OPTENET Server intègre un Server web pour sa configuration et son administration. Installé sur le port TCP 10237, ce Server web permet d'administrer et de configurer OPTENET Server au moyen d'un navigateur web.

Si OPTENET a été installé dans Windows, vous pouvez aller à l'élément WWW Administration du Groupe de programmes d'OPTENET Server (Voir paragraphe 3.2.1) pour ouvrir l'administration WWW dans le navigateur configuré par défaut dans votre système. Vous pouvez y accéder également de manière distante à partir d'un ordinateur branché au réseau en accédant à http://server:10237, où le « server » sera le Server avec OPTENET Server.

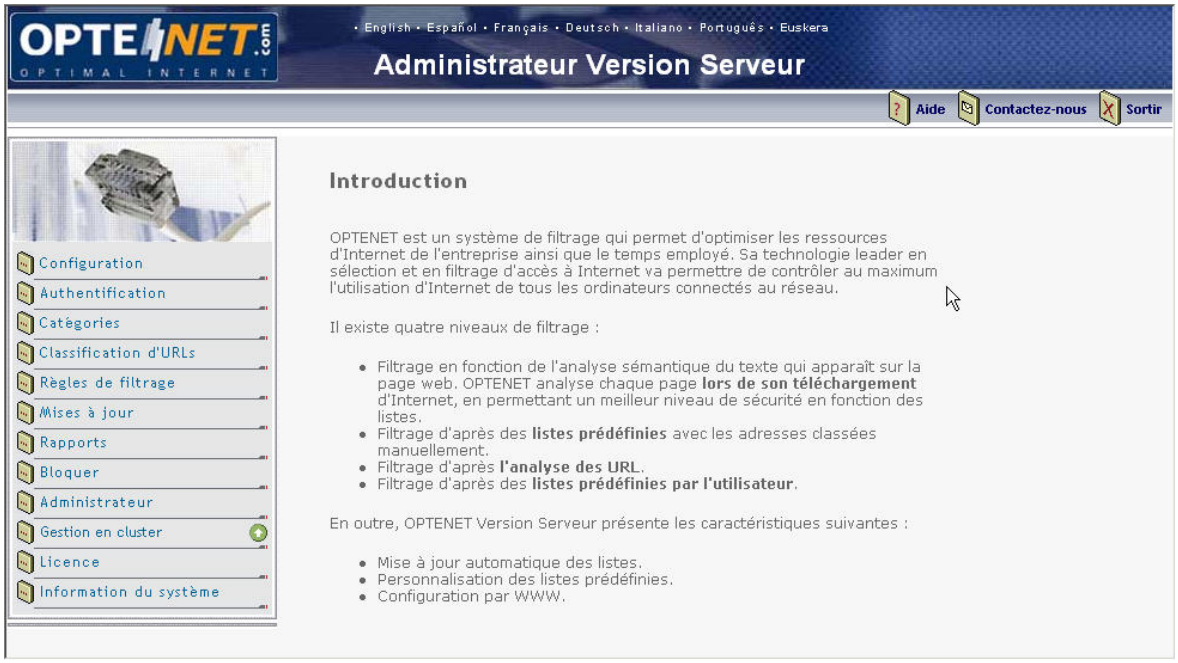
Si le système où est installé OPTENET Server est host.domain, il est possible d'accéder au Server web à l'URL suivante: http://host.domain:10237**.** Le démarrage d'OPTENET est nécessaire avant tout accès au Server web.

Pour garantir la confidentialité de la configuration et de l'administration, le Server web requiert une authentification de l'utilisateur qui devra introduire un nom d'utilisateur et un mot de passe dans la fenêtre comme l'indique la figure. Par défaut, le nom d'utilisateur est **optenet** et le mot de passe est **12345678**. Ces valeurs peuvent être modifiées à partir de ce même Server WWW d'administration. Il est conseillé de les modifier juste après l'installation d'OPTENET Server.

Il se peut qu'en saisissant le nom d'utilisateur et la clé, votre navigateur affiche une page en blanc. Pour pouvoir accéder correctement à l'administration, vous devrez ajouter à la liste de sites sécurisés de votre navigateur l'URL où sera installé OPTENET. Par exemple, si OPTENET est installé à l'adresse : http://192.168.0.240 et utilise Internet Explorer 6.0, vous devrez accéder au menu Outils -> Options d'Internet ->Sécurité -> Sites de confiance et y ajouter l'URL http://192.168.0.240.

5.1. Introduction

La fenêtre d'administration est celle qui s'affiche par défaut lorsque vous entrez dans l'administration après une authentification de l'utilisateur.
Elle propose une brève description du système de filtrage OPTENET. Si vous souhaitez obtenir l'administration web dans une autre langue, cliquez sur le drapeau de votre choix (sous le logotype d'OPTENET). L'administration s'affichera automatiquement dans la langue souhaitée. La figure 5.3. présente une fenêtre d'introduction en français.



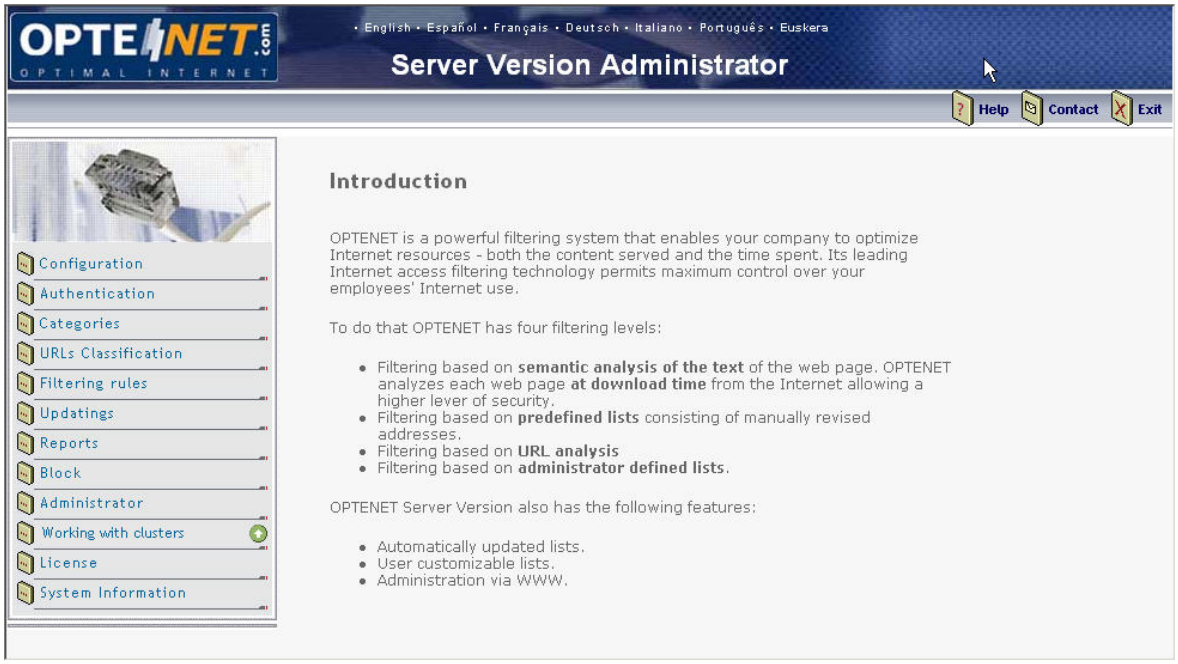
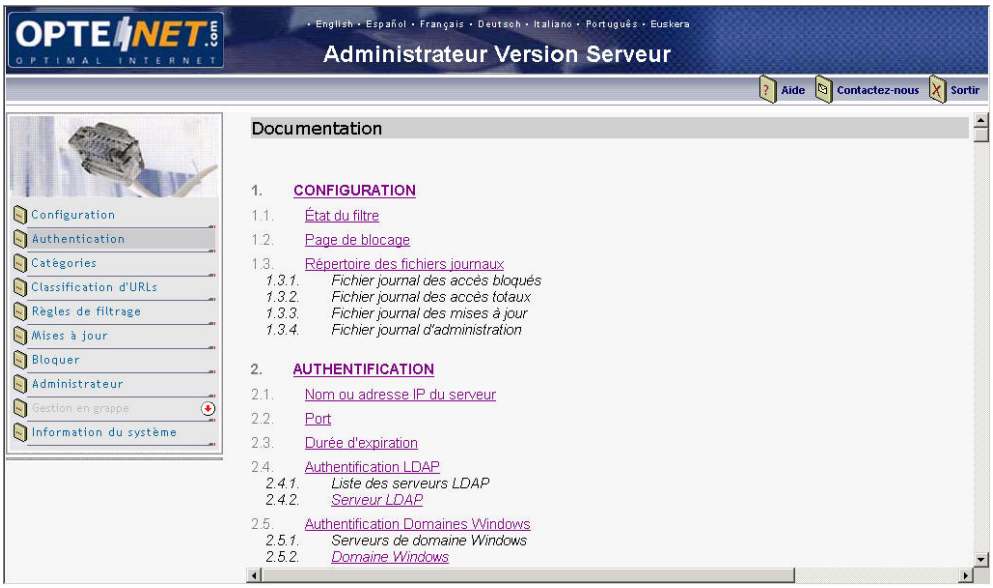


Figure 5.3 : Fenêtre d'introduction de l'administration WWW. en anglais.

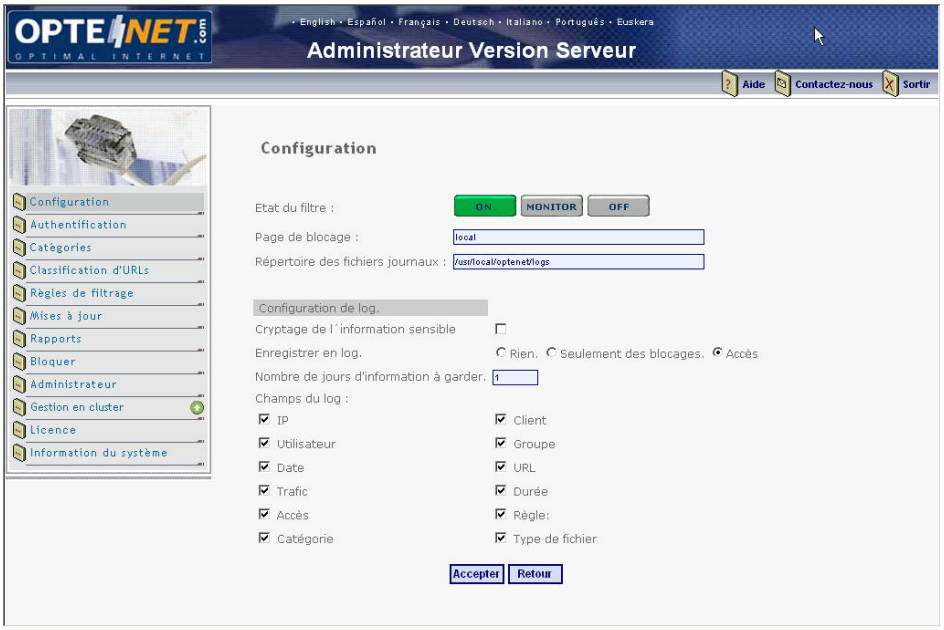
5.2. Documentation

L'icône située en haut à droite de la fenêtre d'administration affiche la documentation au format HTML.



5.3. Configuration

Cette option permet de configurer de nombreux aspects comme l'état du filtre, la page de blocage ou le répertoire de stockage des fichiers journaux. Voyons chacune de ces options.



5.3.1. État du filtre

Le filtre permet actuellement trois états:

- ON: état actif, le filtre traite toutes les demandes en appliquant les options des règles de filtrage. C'est l'état configuré par défaut qui permet au filtre de bloquer les accès.
- MONITOR: état au cours duquel sont traitées toutes les demandes en simulant l'application des règles de filtrage et en permettant l'écriture dans les logs mais **sans filtrage**. Il est utile pour les installations souhaitant procéder à une phase d'analyse de son navigateur avant d'appliquer le filtrage.
- OFF : état inactif, le filtre répond immédiatement à toutes les demandes reçues en les laissant passer, sans bloquer aucun accès.

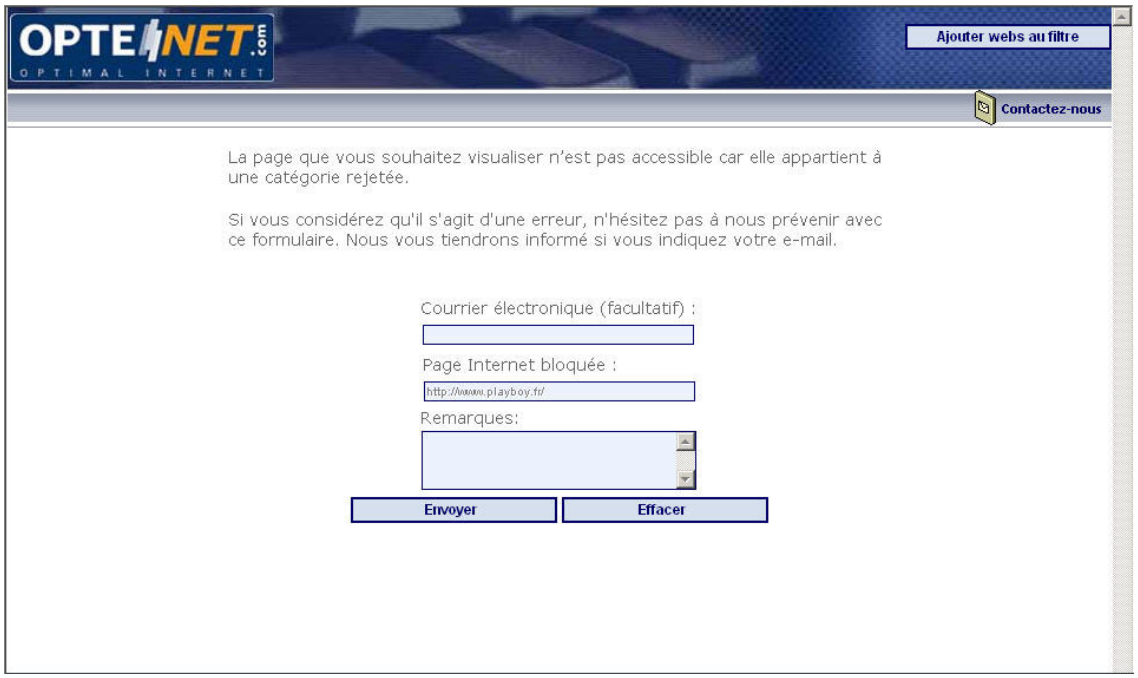
Faites bien la distinction entre l'arrêt du filtre et son état OFF. Lorsque l'état OFF est sélectionné, OPTENET Server est toujours en exécution mais ne surveille plus les accès à Internet. Si vous souhaitez arrêter le filtre, connectez-vous comme utilisateur optenet en ouvrant une session telnet auprès du Server Linux, Solaris ou AIX, puis tapez ./filterinit stop ou bien en arrêtant le service ou procédure dans le système Windows.

5.3.2. Page de blocage

OPTENET Server permet de personnaliser les messages affichés aux utilisateurs quand une page à laquelle ils ont essayé d'accéder est bloquée. Par défaut, le mot clef "local" apparaît dans le champ "Page de blocage". Ainsi, la page de blocage local située dans le répertoire d'installation (voir paragraphe 3.2.3. Système de fichiers installés par OPTENET) s'affiche. Pour que la page de blocage locale s'affiche correctement, il est nécessaire que le filtre soit capable d'obtenir l'IP locale du Server où il est exécuté. Assurez-vous qu'il existe une entrée du type « IP nom du Server » dans le fichier de configuration. Il est également nécessaire que l'ensemble des équipements à partir desquels sera effectuée la navigation disposent d'un accès à cette page de blocage. Au cas où vous ne verriez pas la page de blocage pendant une configuration « locale », essayez de mettre comme page de blocage : http://ip_del_servidor_optenet:10237/cgi-bin/stop. En supposant qu'OPTENET s'exécute sur le Server 192.168.0.235, la page de blocage serait :

http://192.168.0.235:10237/cgi-bin/stop

La figure montre la page de blocage par défaut d'OPTENET. Il faut créer un site propre et personnalisé, la placer sur l'Intranet de votre organisation et l'établir comme la page de blocage d'OPTENET Server.



Cette page Web de réponse peut aussi être générée dynamiquement à l'aide d'un script CGI ou d'un ASP ou PHP. Vous trouverez deux pages de blocage d'exemple ans le répertoire Tools (stop.asp et stop.php) que vous pourrez personnaliser à votre gré et placer ensuite sur l'Intranet comme pages de blocage.

Si les pages de réponse sont générées dynamiquement, vous pouvez recueillir les informations envoyées par OPTENET Server à la page de blocage. Le CGI/ASP reçoit dans la chaîne de requête (méthode GET) les variables suivantes:

- **URL** → indique l'URL qui a été bloquée.
- **DATETIME** → date et heure de la demande.
- **RULE** → règle qui a bloqué cette URL.
- **CAT** → catégorie à laquelle appartient l'URL bloquée.
- **FILE** → type de fichier de l'URL bloquée.

Ces informations peuvent s'avérer très utiles pour envoyer un message électronique à l'administrateur ou pour établir des statistiques.

Si l'option d'envoi du nom d'utilisateur et de l'IP est activée, il reçoit deux paramètres en plus :

- **USER** → indique l'utilisateur qui a réalisé la demande.
- **IP** → IP de l'ordinateur sur lequel est fait la demande.

Pour des raisons de sécurité, l'envoi de ces paramètres est désactivé par défaut.Si vous souhaitez l'activer, vous devez établir comme valeur **TRUE** sur la touche du registre de windows:
HKEY LOCAL MACHINE\SOFTWARE\OPTENET\OPTENET Server\SendIpUser
Si OPTENET Server est installé sous Linux, Solaris ou Aix, vous devez modifier le script **/usr/local/optenet/RunOPTENET** et ajouter comme paramètre d'OPTENET_server **-send_ip_user TRUE**. Ensuite, le filtre doit être redémarré sur les deux plateformes pour que le changement prenne effet.

Ces informations peuvent être très utiles, nous pouvons les utiliser pour envoyer un e-mail à l'administrateur ou pour regrouper des statistiques.

5.3.3. Répertoire des fichiers journaux

Cette option vous permet de spécifier le répertoire dans lequel OPTENET Server va stocker les fichiers journaux, dont il existe trois types.

5.3.4. Configuration de log

5.3.4.1. Filtrage de l'information sensible

Activer cette option forcera Optenet à crypter dans les logs, l'IP, le nom d'utilisateur, et le groupe de l'utilisateur. Cette option est désactivée par défaut.

5.3.4.2. Ecriture des fichiers de log.

Dans cette section, vous pouvez choisir l'information qui sera écrite dans les logs (requestsYYYYMMDD.log). Les valeurs que vous pouvez sélectionner sont:

- **Rien** → indique que vous n'enregistrez aucune demande ou blocage, vous n'enregistrez donc rien.
- **Seulement des blocages** → Indique que vous enregistrez uniquement les sites qui ont été bloqués.
- **Accès** → Indique que vous enregistrez tout, les accès comme les blocages.

5.3.4.3. Nombre de jours d'information à garder

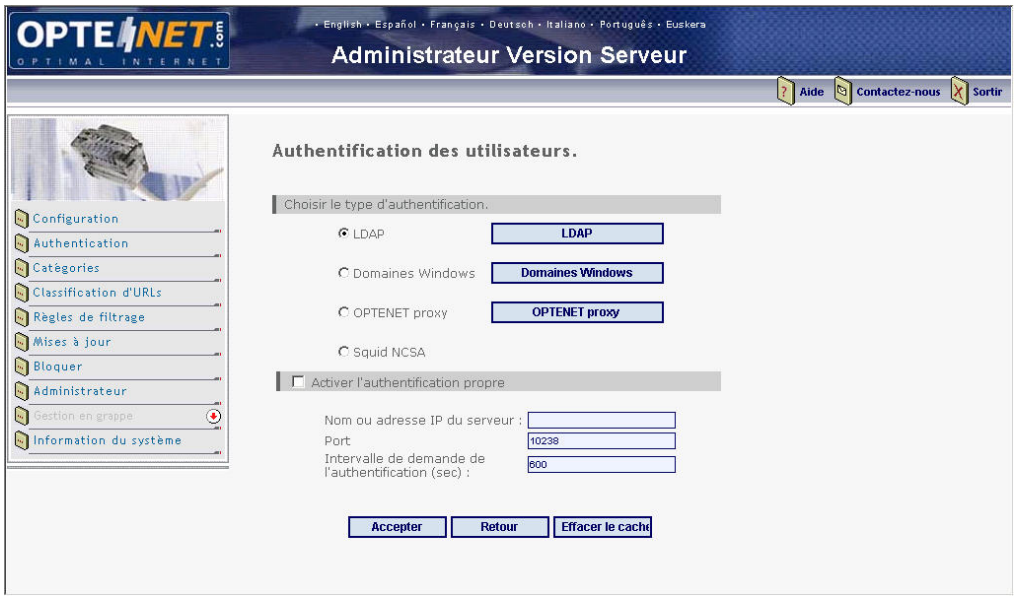
Ici, vous pouvez enregistrer le nombre de jours complets d'information que vous voulez que le filtre garde. Par défaut, la valeur est 1, ce qui veut dire que le filtre garde les logs complets, de la veille et du jour en cours. Au moment ou l'on change de jour, les log antérieurs à la période indiquée sont effacés.
A la différence des versions antérieures d'OPTENET, où le module de rapport était intégré à OPTENET, les logs ne s'accumulent pas dans le répertoire de logs d'OPTENET. C'est OPTENET Reporter, qui, une fois configuré, va appeler les filtres configurés et ainsi réaliser l'accumulation des logs dans son répertoire, en prenant compte les différents filtres. Le fait qu'OPTENET Reporter s'arrête de fonctionner temporairement ne signifie pas que des informations vont être perdues. Au moment où le reporter redémarre, il peut se synchroniser avec OPTENET et ainsi récupérer les derniers logs. Une journée d'information sauvegardée est suffisant pour que OPTENET Repoter et OPTENET synchronisent leurs logs, en cas d'arrêt d'OPTENET Reporter.

5.3.4.4. Champs des fichiers de logs

Dans cette partie, vous pouvez sélectionner les champs que vous voulez voir apparaître dans les fichiers de logs. Il faut prendre en compte le fait que lorsque l'on décide de supprimer un champ, on ne pourra plus récupérer les informations qui s'en réfèrent. Par exemple, si l'on désactive le champ utilisateur, on ne pourra plus obtenir d'information quant à l'utilisateur, ni à son groupe.

5.4. Authentification

Si vous souhaitez établir des règles de filtrage par utilisateurs ou par groupes d'utilisateurs, il est nécessaire que votre proxy ou votre appliance soit configuré pour réaliser l'authentification des utilisateurs ou bien que cette authentification soit directement réalisée par OPTENET. Inversement, vous ne pourrez établir des règles de filtrage que par IP des machines qui accèdent à Internet.



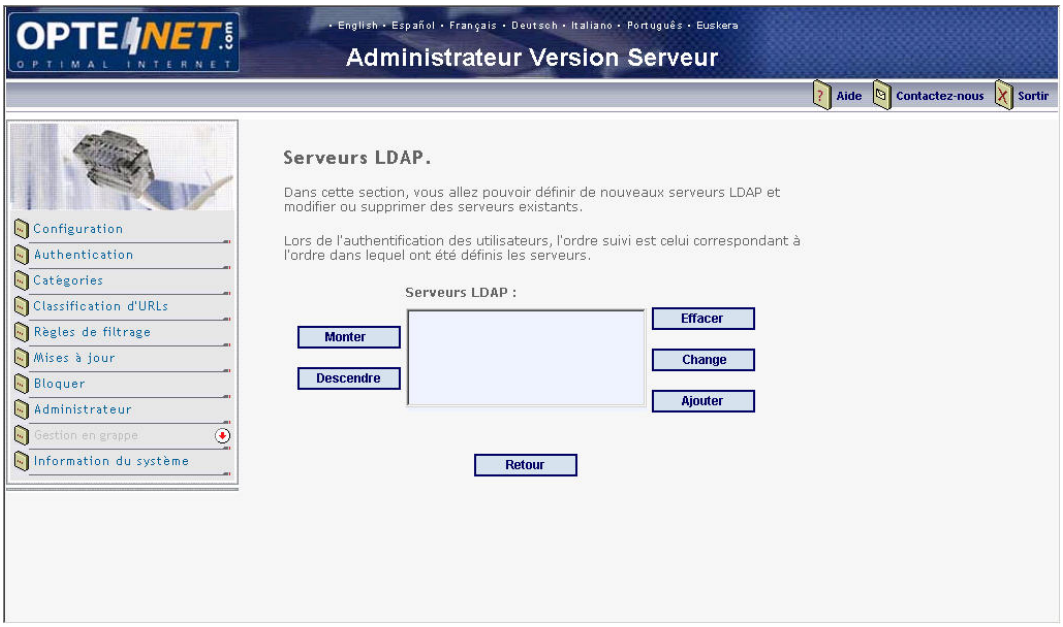
5.4.1. Origine des données (utilisateurs et/ou groupes)

Si vous souhaitez établir des règles de filtrage par utilisateurs et/ou groupes, OPTENET peut vous fournir la liste des utilisateurs et des groupes depuis les paragraphes utilisateurs/groupes dans chaque règle de filtrage. Pour qu'OPTENET puisse vous montrer ces informations, le paragraphe « Authentification » -> "origine des données" doit sélectionner la source des données qu'utilisera OPTENET pour reconnaître les utilisateurs et les groupes. De plus, comme cela est indiqué dans la section 4.2, la majorité des proxys ou caches (en réalité, l'intégralité de ceux-ci, à l'exception de NetCache et BlueCoat à partir de la version 3 incluse) n'envoie pas au filtre les groupes auxquels appartient l'utilisateur qui effectue la demande car OPTENET doit vérifier ces informations. En sélectionnant le type de source de données et en configurant chaque source possible de manière adéquate, OPTENET pourra répertorier les utilisateurs, les groupes et demander les groupes de chaque utilisateur.

Vous trouverez ci-dessous la description des origines des données avec lesquelles OPTENET peut travailler.

5.4.1.1. LDAP

Sélectionnez l'option LDAP si votre organisation gère des comptes utilisateurs et groupes avec des Servers LDAP. Parmi les exemples de ces Servers figurent Active Directory de Windows, Lotus Domino, iPlanet. Après avoir sélectionné l'option LDAP et appuyé sur le bouton Accepter dans la fenêtre "Authentification des utilisateurs", appuyez sur le bouton LDAP pour définir combien de Servers LDAP sont nécessaires.
En appuyant sur le bouton LDAP, vous accéderez à la fenêtre de configuration des Servers LDAP.



5.4.1.1.1. Liste des Servers LDAP

Dans cette section sont configurés les Servers LDAP avec lesquels OPTENET Server communiquera pour obtenir la liste des utilisateurs, des groupes et consulter les groupes d'un utilisateur. OPTENET permet de définir plus d'un Server LDAP.
Au moment de consulter les groupes d'un utilisateur, OPTENET consultera toujours le premier Server défini dans la liste, et consultera le suivant si le premier ne répond pas ou si cet utilisateur n'est pas défini dans le premier. Pour cette raison, l'ordre dans lequel sont établis ces Servers est fondamental. Au moment de répertorier tous les utilisateurs ou groupes, OPTENET consultera tous les Servers et montrera la totalité des utilisateurs et des groupes obtenus.
A partir de cette option, vous pourrez ajouter un nouveau Server LDAP, modifier ou supprimer un Server existant et également établir l'ordre de ces derniers.

5.4.1.1.2. Server LDAP

Dans cette section est configuré le Server LDAP sélectionné. En ajoutant un nouveau Server, une nouvelle entrée est créée dont le nom est aléatoire et qui dispose du port LDAP standard 389. Pour chaque Server LDAP, vous devrez configurer les données suivantes :

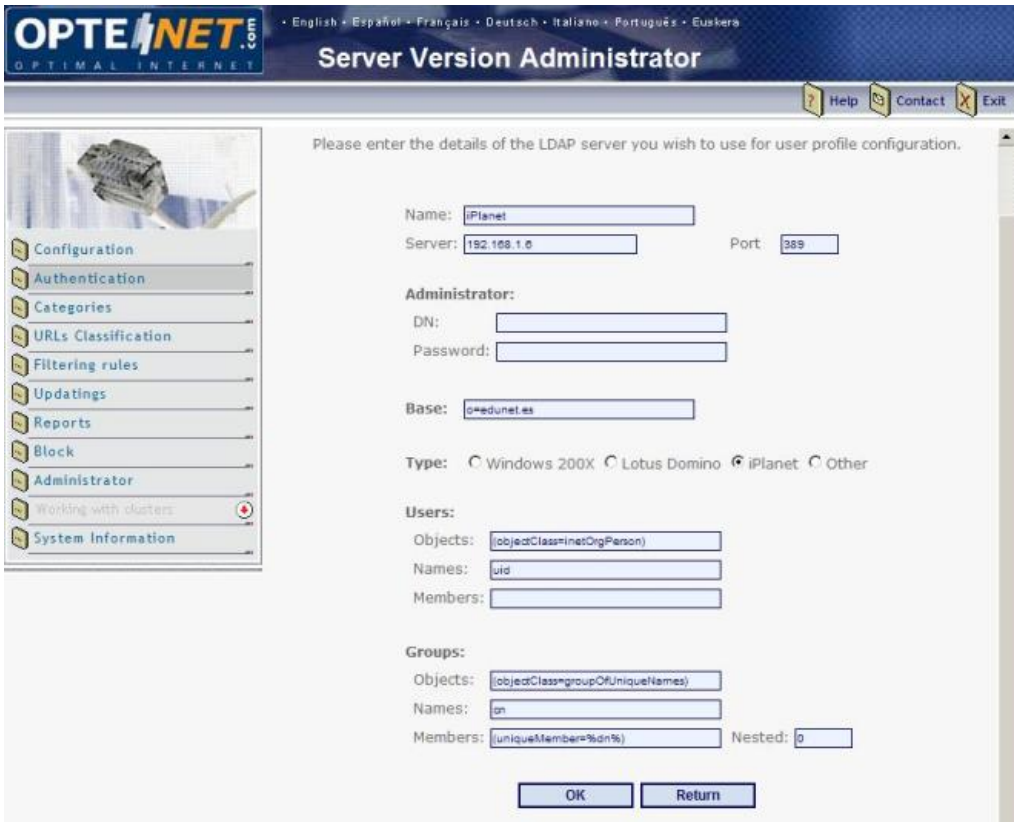
- Nom : nom grâce auquel vous identifierez ce Server LDAP dans la liste, ce nom est simplement symbolique mais il doit être unique dans la liste des Servers LDAP qu'il définit.
- Server : nom ou adresse IP du Server LDAP. Nous recommandons de toujours insérer l'adresse IP dans la mesure du possible pour que les consultations LDAP soient plus rapides et qu'il ne soit pas nécessaire de résoudre le nom de chacune d'entre elles.
- Port : port d'où le Server LDAP écoute.
- Administrateur : DN et mot de passe d'accès au Server LDAP. Si le Server LDAP permet des lectures anonymes, ce champ peut être laissé vide.
- Base : base pour les recherches d'utilisateurs ou de groupes.
- Type : type de Server LDAP.

Le type de Server LDAP sert à indiquer au filtre la manière selon laquelle il doit obtenir les utilisateurs, les groupes et les relations entre eux. Pour obtenir ces informations, le filtre requière les données suivantes:

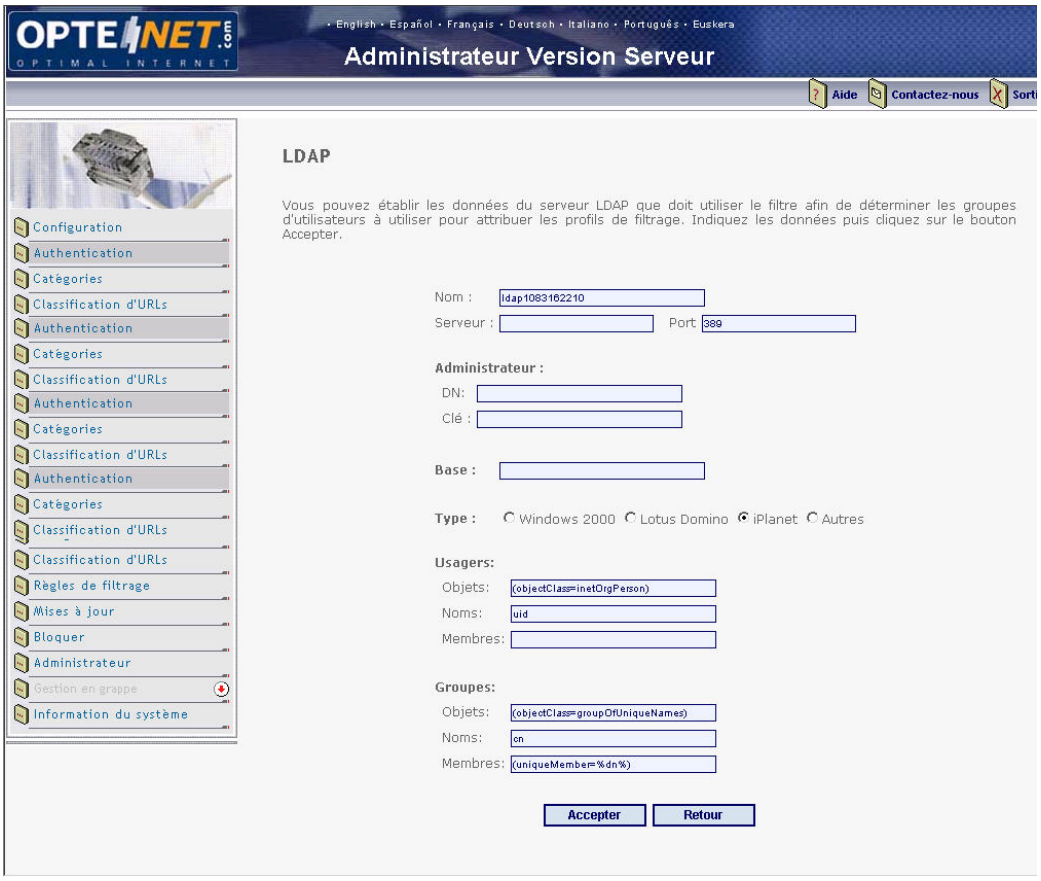
- Objets d'utilisateur : filtre LDAP pour rechercher les objets comportant les renseignements des utilisateurs. Par exemple : (objectClass=inetOrgPerson), (objectClass=rvUser), etc.

Noms d'utilisateur : attribut LDAP qui sera utilisé comme nom des utilisateurs. Par exemple : uid, shortname, etc.

- Critère de filtrage: Lorsque l'on fonctionne avec ICAP et qu'un nom d'utilisateur autre que "**Distinguished name**" a été configuré sur LDAP, l'option "consultez les alias d'utilisateur (LDAP)" doit être activée et un délai maximal doit être fixé au Server cache, tel qu'il est décrit ultérieurement dans ce manuel. Dans ce cas, OPTENET procèdera à une consultation afin d'obtenir les identifiants de l'utilisateur à partir de "**Distinguished name**". Afin de permettre à OPTENET de savoir quel identifiant utiliser, parmi tous ceux dévoilés lors de la consultation, il disposera de cette case où il pourra spécifier un patron de recherche (par exemple "U*"). Ainsi, OPTENET tiendra compte exclusivement des champs commençant par U. Enfin, pour résoudre d'éventuels cas où se présenteraient plus d'une concordance, il disposera du menu déroulant qui permettra de choisir entre "première valeur" ou "dernière valeur".
- Membres d'utilisateur : condition qui s'applique aux objets d'utilisateur pour obtenir les groupes auxquels ils appartiennent. Par exemple : (memberOf=cn=%cn%), (ou=%ou%), etc. Notez qu'il peut être indiqué entre % l'attribut des objets du groupe qui doivent respecter les conditions pour que l'utilisateur soit considéré comme membre de ce groupe.
- Objets de groupe : filtre LDAP pour obtenir les objets avec les renseignements du groupe. Par exemple : (objectClass=groupOfUniqueNames), (objectClass=rvGroup), etc.
- Noms de groupe : attribut LDAP qui sera utilisé comme nom des groupes. Par exemple : cn, ou, etc.
- Membres de groupe : condition qui s'applique aux objets de groupe pour obtenir les utilisateurs qui en font partie. Par exemple : (uniqueMember=%dn%), (memberUid=%uid%), etc. Notez qu'il peut être indiqué entre % l'attribut des objets d'utilisateur qui doit respecter les conditions pour que le groupe compte cet utilisateur parmi ses membres.
- Groupes imbriqués : niveau maximum d'imbrication des groupes. La valeur -1 sert à rechercher tous les groupes d'un utilisateur jusqu'à finir toutes les imbrications. Avec la valeur 0, aucune recherche des groupes imbriqués n'a lieu. Les utiliser avec précaution puisque le nombre de consultations LDAP augmente pour chaque niveau et peut affecter le rendement.



Vous trouverez ci-dessous un exemple de configuration d'un Server LDAP. Dans cet exemple, les utilisateurs consistent en des objets de type inetOrgPerson et leur nom est extrait de l'attribut uid. Les groupes consistent en des objets de type groupOfUniqueNames et leur nom est extrait de l'attribut cn. Pour connaître les groupes auxquels appartiennent les utilisateurs, seuls les objets de groupes sont consultés (la section Membres d'utilisateurs est vide) et comme condition, il est établit que l'attribut uniqueMember inclut l'uid de l'utilisateur dans le format donné. Pas de recherche des groupes imbriqués.



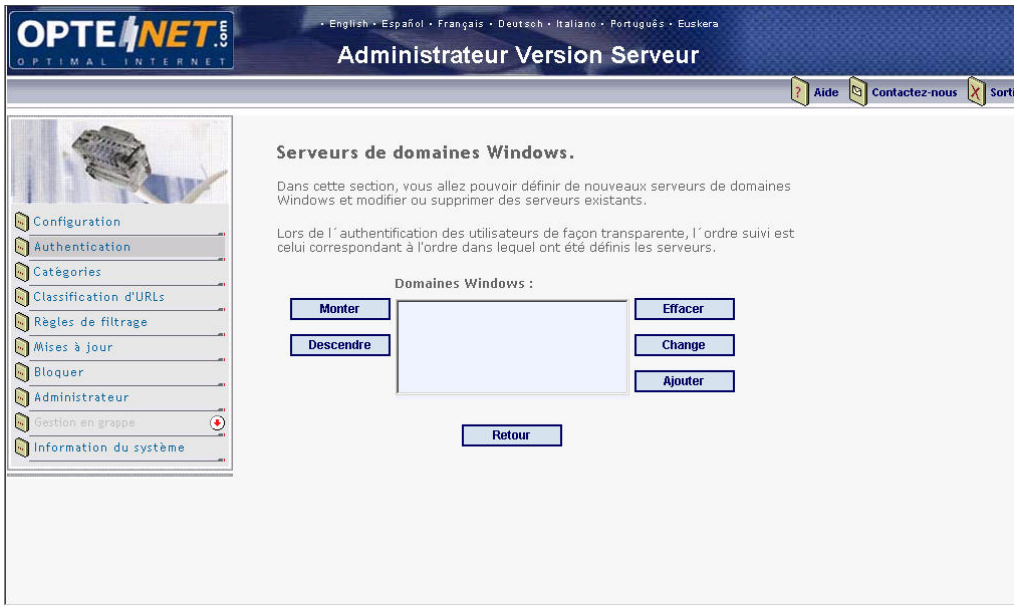
5.4.1.2. Domaine Windows

Sélectionnez l'option Domaines Windows si votre organisation gère les comptes utilisateurs et groupes avec des Domaines Windows, aussi bien NT que Windows 2000 ou 2003 installés en mode mixte. Il faudra disposer d'OPTENET DCAgent 2.xx. dans un Server Windows de son réseau qui aura accès aux contrôleurs de domaine que vous souhaitez consulter. Ce logiciel se charge de consulter les contrôleurs de domaines pour extraire les utilisateurs, groupes et les groupes de chaque utilisateur. A son tour, OPTENET server communique avec OPTENET DCAgent pour obtenir ces informations.

* Vous pouvez télécharger ce logiciel sur le site Web d'OPTENET. Nous vous conseillons également de consulter le manuel d'instructions avant de procéder à l'installation.

5.4.1.2.1. Servers de Domaines Windows

Dans cette section sont configurés les machines Windows où a été installé OPTENET DCAgent 2.xx avec lesquelles OPTENET Server communiquera pour obtenir la liste des utilisateurs, groupes et consulter les groupes d'un utilisateur. OPTENET permet de définir plus d'un DCAgent.
Au moment de consulter les groupes d'un utilisateur, OPTENET consultera toujours le premier Server défini dans la liste, et consultera ensuite le suivant si le premier ne répond pas ou si cet utilisateur n'est pas défini dans le premier. Pour cette raison, l'ordre dans lequel sont établis ces Servers est fondamental. Au moment de répertorier tous les utilisateurs ou groupes, OPTENET consultera tous les Servers et montrera la totalité des utilisateurs et des groupes obtenus.

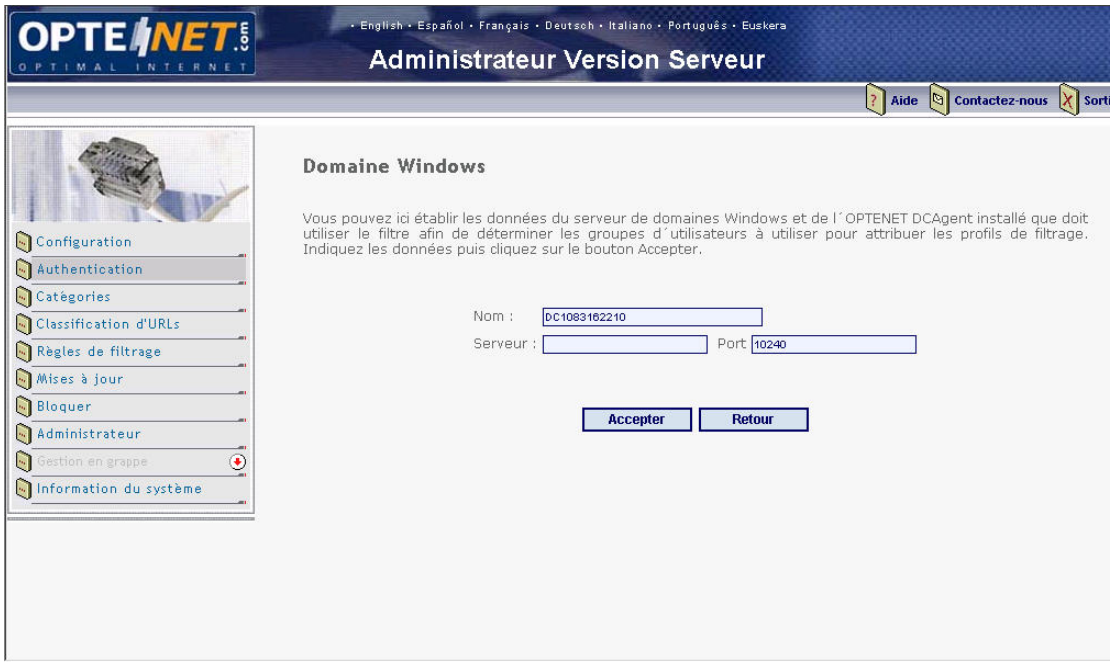


A partir de cette option, vous pourrez ajouter un nouveau OPTENET DCAgent, modifier ou supprimer un existant, et également établir l'ordre de ces derniers.

5.4.1.2.2. Domaine Windows

Dans cette section sont configurées les données de l'OPTENET DCAgent sélectionné. En ajoutant un nouveau Server, une nouvelle entrée est créée dont le nom est aléatoire et qui dispose du port d'écoute du DCAgent standard 10240. Pour chaque Server DCAgent, vous devrez configurer les données suivantes:

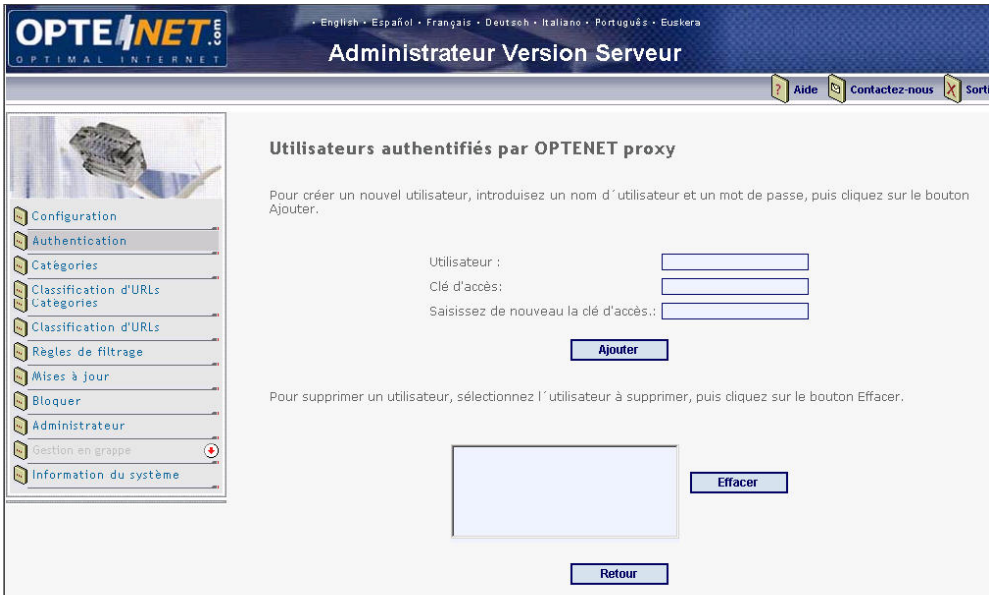
- Nom : nom grâce auquel vous identifierez ce Server dans la liste, ce nom est simplement symbolique mais il doit être unique dans la liste des Servers qu'il définit.
- Server : nom ou adresse IP où est installé et exécuté le DCAgent. Nous recommandons de toujours insérer l'adresse IP dans la mesure du possible pour que les consultations soient plus rapides et qu'il ne soit pas nécessaire de résoudre le nom de chacune d'entre elles.
- Port : porte d'où le DCAgent écoute.



5.4.1.3. OPTENET Proxy

Sélectionnez l'option OPTENET proxy si vous avez installé OPTENET Server dans un système Windows et que vous avez choisi le proxy OPTENET lors de l'installation. Ainsi, OPTENET affichera dans la section "Règles de filtrage" -> "utilisateurs" les utilisateurs que OPTENET proxy est capable d'authentifier. OPTENET Proxy ne travaille pas avec des groupes d'utilisateurs; par conséquent, il ne sera pas possible d'établir des règles par groupes d'utilisateur si votre organisation navigue par le biais d'OPTENET proxy.

En appuyant sur le bouton OPTENET Proxy, vous accèderez à l'écran qui s'affiche sur la Figure à partir duquel sont ajoutés ou supprimés les utilisateurs avec leurs mots de passe qu'OPTENET Proxy est capable de reconnaître. Au moment de l'intégration d'un premier utilisateur avec son mot de passe, OPTENET proxy commencera à demander une authentification à tous ceux qui naviguent par son biais, lorsque ce dernier utilisateur OPTENET Proxy est éliminé, il cessera de demander l'authentification des utilisateurs.



5.4.1.4. Squid NCSA

Sélectionnez l'option Squid NCSA si vous avez installé OPTENET Server dans des environnements UNIX (Solaris, Aix, FreeBSD ou Linux), que vous avez choisi l'option RPC qui installe Squid avec OPTENET et que vous avez configuré Squid pour qu'il demande une authentification élémentaire NCSA. Ainsi, OPTENET affichera dans la section "Règles de filtrage" -> "utilisateurs" la liste des utilisateurs de Squid qu'il est capable d'afficher. En réalité, OPTENET effectue une recherche du tag "auth_param basic program" du fichier de configuration de Squid (squid.conf) pour obtenir le fichier des utilisateurs, le parcourir et l'extraire de la liste des utilisateurs. L'authentification NCSA de Squid ne travaille pas avec les groupes d'utilisateurs ; par conséquent, il ne sera pas possible d'établir des règles par groupes d'utilisateur si votre organisation navigue par le biais de Squid dans lequel l'authentification NCSA est configurée.

5.4.2. Activer l'authentification propre

Si votre proxy ou votre appliance n'est pas configurée pour réaliser une authentification des utilisateurs, tous les utilisateurs pourront accéder à Internet sans avoir à s'identifier (en insérant un nom d'utilisateur et un mot de passe). Cela implique qu'OPTENET ne reçoit pas d'informations quant à savoir quel utilisateur effectue chaque demande et ne peut appliquer de règles de filtrage basées sur les utilisateurs ou les groupes; il ne peut établir différentes politiques que par les IP des machines qui accèdent à Internet.

Pour pouvoir établir des politiques de filtrages par utilisateurs ou groupes d'utilisateurs, deux options sont disponibles:

- A) Configurer votre proxy ou appliance pour authentifier les utilisateurs (option recommandée)
- B) Configurer OPTENET pour qu'il authentifie lui-même les utilisateurs qui naviguent.

Dans le cas de l'option A) où c'est le proxy ou cache qui authentifie les utilisateurs, ce proxy envoie à OPTENET avec chaque demande WEB l'utilisateur qui effectue la demande. Dans ce cas, OPTENET devra obtenir les groupes de cet utilisateur pour qu'il utilise l'origine des données qui a été configurée (LDAP ou domaine Windows, nous vous rappelons qu'avec le proxy OPTENET ou Squid NCSA, il est impossible d'établir des règles de filtrage par groupes).

Dans le cas de l'option B), c'est OPTENET qui identifie les utilisateurs qui naviguent. Pour l'activer, il faut cocher la case "Activer authentification propre" dans la fenêtre d'authentification des utilisateurs. Cette option peut être utile pour les organisations où le proxy/cache ne réalise pas d'authentification d'utilisateurs ou lorsque ce cache n'envoie pas les informations quant à l'utilisateur qui effectue chaque demande au filtre. Dans ce mode de fonctionnement, OPTENET effectue une association entre les IP qu'il reçoit à chaque demande et les utilisateurs qui naviguent depuis ces IP; par conséquent, il est strictement nécessaire que le proxy/cache, et OPTENET, effectuent les demandes par leur IP d'origine et non pas par l'IP d'un router ou gateway intermédiaire. Vous trouverez ci-dessous la description du processus d'identification que réalise OPTENET:

1. Un utilisateur commence à naviguer sur Internet, effectue les demandes web au proxy et celui-ci les transmet à OPTENET pour qu'il décide si elles doivent passer ou être bloquées.
2. OPTENET extrait l'adresse IP de la demande et la vérifie par rapport à son tableau interne qui contient les paires IP et utilisateurs.

3. Comme cette IP est nouvelle, OPTENET ne sait pas encore quel utilisateur se cache derrière cette demande. Pour le vérifier, il dispose de deux méthodes :

    3.1 Si "**LDAP**" est sélectionné comme origine des données, OPTENET redirige cette demande vers son Server d'authentification en exigeant que l'utilisateur qui navigue insère un utilisateur et un mot de passe qu'il comparera avec les données des Servers LDAP définis. Pour le comparer, le filtre peut réaliser une demande sur le champ "nom d'utilisateur" défini dans le Server LDAP, ou bien accéder directement au répertoire LDAP avec les accréditations fournies. De plus, et ce seulement en cas de sélection de "LDAP" comme origine des données, il est possible d'authentifier l'utilisateur par le biais des donnés contenues dans un certificat de client, via une communication sécurisée SSL. Pour cela, il convient d'indiquer le champ de la base de données LDAP sur lequel le contenu du certificat est demandé. Si cette dernière option est habilitée et que la vérification des données du certificat est erronée, un nom d'utilisateur et un mot de passe seront demandés. Une fois cela vérifié, la relation entre cette IP et cet utilisateur est réalisée de manière à ce que toutes les demandes provenant de cette même IP soient considérées comme provenant de cet utilisateur pendant l'intervalle de demande de l'authentification" qui peut être défini dans la même fenêtre.

    3.2 Si "**Domaines Windows**" est sélectionné comme origine des données, OPTENET effectue une demande aux DCAgents configurés en leur demandant quel utilisateur est entré dans la session des domaines Windows d'où provient cette IP. Ainsi, OPTENET peut identifier l'utilisateur sans que ce dernier ait besoin d'insérer un nom et un mot de passe. Cette modalité s'appelle **authentification transparente** et comme la reconnaissance intuitive est possible, il est nécessaire que cet utilisateur se soit préalablement connecté à une session dans un Domaine Windows. Une fois les informations du DCAgent reçues, OPTENET conserve cette relation entre cette IP et cet utilisateur de manière à ce que toutes les demandes provenant de cette même IP soient considérées comme provenant de cet utilisateur pendant l'intervalle de demande de l'authentification" qui peut être défini dans la même fenêtre.

    3.3 Si elle est sélectionnée comme origine des données "**OPTENET Proxy**" l'option "activer authentification propre" n'a pas effet et est désactivée. OPTENET extrait de la demande qui lui parvient du proxy l'utilisateur qu'il lui transmet et il n'est pas possible d'obtenir des groupes puisque le proxy ne les envoie pas. Pour que OPTENET Proxy demande une authentification d'utilisateurs, un ou plusieurs utilisateurs doivent être créés dans la section "OPTENET Proxy".

    3.4 Si elle est sélectionnée comme origine des données "**Squid NCSA**" l'option "activer authentification propre" n'a pas effet et est désactivée. OPTENET extrait de la demande qui lui parvient de Squid l'utilisateur qu'il lui transmet et il n'est pas possible d'obtenir des groupes puisque le proxy ne les envoie pas. Pour que Squid demande une authentification d'utilisateurs, il doit avoir été configuré de manière adéquate. Consultez par exemple l'exemple qui figure dans la section "Installation d'OPTENET avec SQUID" de ce manuel.

4. Une fois l'intervalle de "demande d'authentification" écoulé, l'étape 3 est réitérée pour vérifier que c'est le même utilisateur qui continue de naviguer ou au contraire, un autre.

En résumé, OPTENET peut réaliser l'authentification d'un utilisateur à chaque fois qu'il reçoit l'IP qui effectue la demande et lorsque les utilisateurs entrent dans une session

dans un domaine Windows ou que nous disposons d'un Server LDAP qui peut valider les utilisateurs à l'aide de leur mot de passe.

Il n'est cependant pas conseillé que le proxy/cache ou OPTENET réalisent tous deux l'authentification car dans ce cas, OPTENET rejète l'information de l'utilisateur que lui envoi le proxy/cache et tente d'établir sa propre authentification.

5.4.3. Nom ou adresse IP du Server

Dans cette case, il convient d'insérer l'adresse IP ou le nom du Server où est installé OPTENET. Si ce Server possède plus d'une interface réseau, insérez l'interface réseau qui est accessible depuis l'ensemble de l'Internet. Dans le cas où ces cases ne seraient pas cochées, OPTENET obtient l'adresse IP en consultant directement le Server. Dans le cas de plusieurs interfaces réseau, OPTENET reste avec le premier configuré qui coïncide avec le premier indiqué par les commandes (ifconfig ou ipconfig).
Cette case n'est valide que si vous avez activé l'authentification des utilisateurs. Pour qu'OPTENET puisse réaliser l'authentification des utilisateurs LDAP, le Server où est exécuté OPTENET doit être accessible à partir de tous les points de l'Intranet (directement ou bien par le biais du proxy); concrètement, le port vers lequel sont dirigées les demandes d'authentification. Dans cette option, vous pouvez écrire l'adresse IP "visible" de tout l'Intranet de cette machine, ou le nom "visible" de cette machine à partir de tout l'Intranet. Souvenez-vous que, dans la mesure du possible, vous devez ajouter ce nom de machine à votre Server DNS pour que les demandes d'authentification soient résolues.

5.4.4. Port

Ce port permet d'écouter le Server d'authentification d'OPTENET. Une fois la valeur de ce port modifiée, redémarrez OPTENET pour que la modification soit prise en compte. Sa valeur par défaut est 10238. Cette case est valide uniquement si vous avez activé l'authentification des utilisateurs.

5.4.5. Intervalle de demande de l'authentification

Il s'agit de la durée indiquée en secondes pendant laquelle OPTENET considère les associations qu'il établit entre les adresses IP et les utilisateurs comme valides. Une fois ce délai en secondes écoulé, OPTENET obligera tous les utilisateurs connectés à Internet de manière active à s'identifier de nouveau.

Cette durée indique les secondes pendant lesquelles OPTENET considère comme valide l'association d'un utilisateur avec ses groupes. Une fois ce délai écoulé, dès réception de la demande de navigation suivante de cet utilisateur, OPTENET consultera les groupes de cet utilisateur.

5.4.6. Effectuer une recherche du DN associé au nom d'utilisateur

Pour s'authentifier, l'utilisateur doit indiquer un nom d'utilisateur et un mot de passe pour comparer son identité à la base de données d'utilisateurs LDAP. Cette option permet de définir le mode de vérification qu'utilisera OPTENET avec ce nom d'utilisateur et ce mot de passe.

Si l'option est activée, OPTENET effectue une recherche dans la base de données LDAP pour récupérer le DN du registre qui est associé au nom d'utilisateur saisi par ce dernier.

Une fois le DN récupéré, OPTENET tente de valider ledit DN avec le mot de passe demandé par l'utilisateur.

Si l'option est désactivée, OPTENET ne recherche pas dans la base de données pour trouver le DN mais il construit le DN directement à partir du nom d'utilisateur saisi par le client. Pour cela, il enchaîne le champ "nom d'utilisateur" configuré dans le Server LDAP avec la valeur saisie par l'utilisateur et avec la base du Server LDAP. Ensuite, il tentera la validation avec le DN construit et le mot de passe fourni par l'utilisateur, comme dans le cas antérieur.

La grande différence est que le premier cas nous garantit que le DN que nous utiliserons est le bon, ce qui rend la configuration plus flexible pour n'importe quelle base de données LDAP. En revanche, cette option consomme un temps de résolution plus élevé puisqu'une demande préalable sur la base de données est nécessaire. Le deuxième cas ne nous garantit pas que les recherches sont réalisées correctement et n'est valide que pour les structures LDAP rigides, dans lesquelles tous les DN de ce dernier se composent du champ nom d'utilisateur et la base LDAP.

C'st pourquoi cette option est activée par défaut.

5.4.7. Utiliser des certificats de client

Comme nous l'avons vu dans la section précédente, il est possible que OPTENET obtienne les accréditations d'authentification à partir des données d'un certificat de client. Pour cela, nous devons activer cette option.

Pour cela, le Server d'authentification propre d'OPTENET devient un Server sécurisé auquel il faudra accéder par le biais du protocole https plutôt que le protocole http. À partir de là, la transmission de données entre OPTENET et l'utilisateur sera effectuée de façon sécurisée par le biais du protocole SSL.

En profitant de la possibilité que proposent les communications SSL d'envoyer des certificats de client, OPTENET demande aux utilisateurs un certificat numérique qui contienne ses accréditations. Une fois reçus, OPTENET peut valider l'identité dudit utilisateur en utilisant les informations contenues dans le certificat, sans que l'utilisateur n'ait besoin de saisir son nom d'accès et son mot de passe.

5.4.8. Champ LDAP pour vérifier le certificat de client

Pour vérifier qu'un certificat numérique fourni par un utilisateur correspond à l'un des contenus de la base de données LDAP que nous avons définis comme origine de données OPTENET doit le comparer à la base de données LDAP.

Pour cela, OPTENET obtient l'emprunte numérique du certificat du client et il la compare aux valeurs du champ LDAP que nous définissons dans cette section. Si la demande donne un résultat négatif, soit parce que le champ configuré n'existe pas, soit parce qu'aucun utilisateur n'est associé aux informations contenues dans le certificat numérique, OPTENET offre à l'utilisateur la possibilité de s'authentifier grâce à un nom d'utilisateur et un mot de passe.

5.4.9. Activer consultation des alias d'utilisateur (LDAP)

Lorsque l'on fonctionne avec ICAP ou ISA Server, en activant cette option, OPTENET peut travailler avec un nom d'utilisateur LDAP autre que "**Distinguished name**".
Quel que soit le nom d'utilisateur qu'il ait configuré sur LDAP, OPTENET reçoit de l'application ou de l'ISA le nom d'utilisateur "**Distinguished name**" dans la demande, au

titre de nom d'utilisateur. Pour le résoudre, OPTENET doit effectuer une consultation pour obtenir l'identifiant de l'utilisateur configuré sur LDAP et correspondant au nom "**Distinguished name**" reçu.
Par défaut, cette option sera désactivée. Une fois activée, il faudra configurer le Server cache utilisateur-alias (rubrique suivante du présent manuel) et le champ critère de filtrage devra être créé pour chaque Server LDAP ayant été défini dans l'administration d'OPTENET.

5.4.10. Durée de vie de la combinaison utilisateur-alias

Pour éviter de saturer les Servers LDAP en lançant une consultation pour chaque demande ICAP, OPTENET gère un cache interne associant "**Distinguished name**" avec l'identifiant de l'utilisateur configuré sur LDAP. Ainsi, la consultation LDAP est réalisée uniquement la première fois et, ensuite, c'est la valeur stockée dans le Server cache qui est utilisée. Ce cache est conservé pendant un délai maximal, les entrées arrivant à expiration à l'issue de celui-ci , ce qui nécessite de procéder à une nouvelle consultation LDAP.
Dans cette case, ce délai maximal de conservation, exprimé en secondes, devra être saisi.

5.5. Catégories

OPTENET Server vous permet de créer et de gérer vos propres catégories. Il vous suffit pour cela d'indiquer le nom et les types de la catégorie que vous souhaitez créer ou effacer et peu après, la catégorie sera disponible sur l'ensemble du filtre.

Les types possibles sont les suivants:

- content :catégorie de contenus.
  Ce type de catégories sera traité comme celles incluant le filtre par défaut, à savoir les catégories créées par OPTENET. Une fois créée, la catégorie pourra ajouter des URL à celle-ci dans la rubrique "Classification des URL" et, ultérieurement, elle pourra utiliser cette catégorie à partir de la rubrique de règles de filtrage.

- white : catégorie blanche.
  Dans les catégories de type "blanches", des URL jamais filtrées pourront être intégrées du fait qu'elles appartiennent à une certaine catégorie. Il peut exister des cas dans lesquels une URL appartient à plus d'une catégorie, à l'instar d'une page de presse économique qui appartient à la fois à la catégorie "presse" et "économie" et pourra, de ce fait, être bloquée dans différentes configurations de filtrage. Si l'on inclut l'URL dans le type de catégorie "blanche", elle ne sera en aucun cas filtrée.Les catégories blanches sont utiles pour nous assurer que les url que nous insèrerons ne seront classifiées par aucune autre catégorie. Une fois la catégorie créée, elle pourra ajouter des URL à celle-ci dans la rubrique "Classification des URL".

- black : catégorie noire.
  Les catégories de type "noires" servent à insérer des URL que nous souhaitons voir classées comme appartenant à toutes les catégories de contenus existants. Une fois la catégorie créée, vous pourrez y ajouter des URL dans la rubrique "Classification des URL".

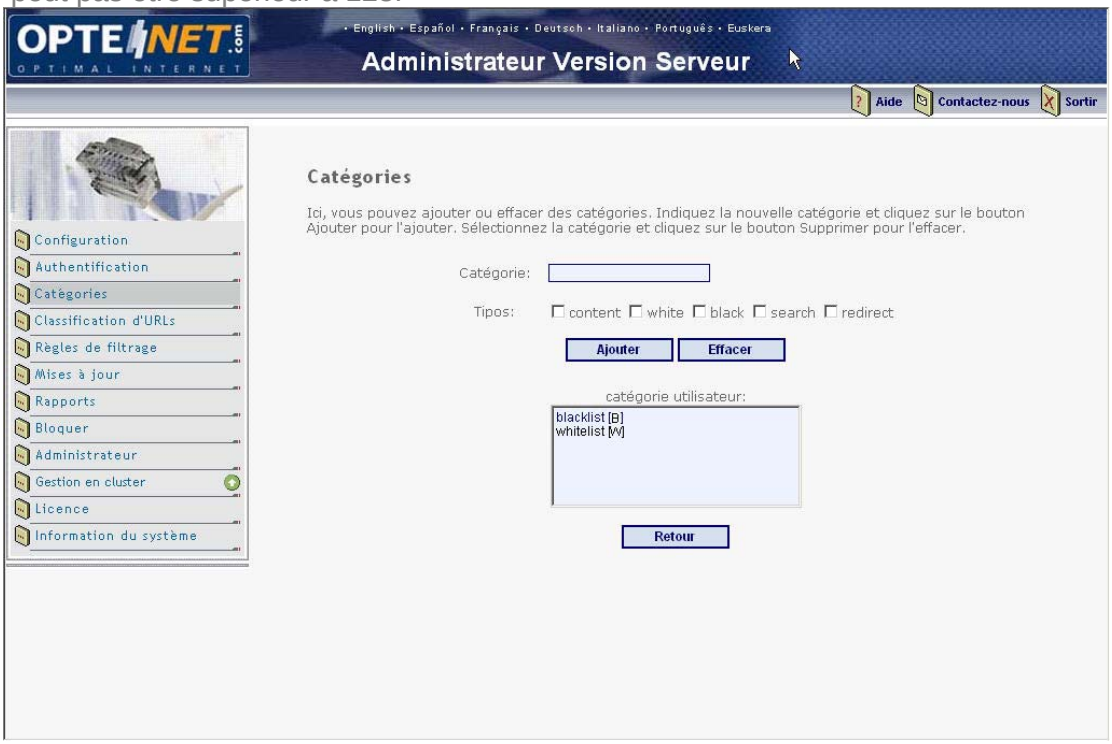
- search: catégorie de moteurs de recherches.

OPTENET fournit cette catégorie avec la liste de moteurs de recherche. On pourra, en outre, y inclure des URL qui seront traitées comme des moteurs de recherche. La différence pour les URL inclues dans ce type de catégories résidera dans le fait que, quand OPTENET Server les analyse, ce n'est pas l'analyse sémantique qui sera utilisée mais bel et bien l'analyse d'URL. Ceci permet d'améliorer l'efficacité quand il s'agit d'accepter ou de rejeter des contenus recherchés par l'utilisateur. Une fois la catégorie créée, vous pourrez y ajouter des URL dans la section "Classification des URL".

- redirect: catégorie de moteurs destinés à rediriger.

  OPTENET fournit cette catégorie avec la liste de moteurs destinés à rediriger, à rester anonymes, etc. En outre, on pourra y intégrer des URL pour lesquelles l'on accordera une attention toute particulière à des fonctions typiques destinées à rediriger. La caractéristique spéciale de ces types de catégories réside dans le fait que, lorsqu'OPTENET Server analyse les URL ayant été inclues, on procède en outre à une recherche spécifique dans l'url en essayant d'extraire des URL contenues dans celle-ci, pour ensuite chercher les catégories de ces URL intégrées. Une fois la catégorie créée, vous pourrez y ajouter des URL dans la rubrique "Classification des URL".

Sachez qu'il n'est pas possible d'ajouter une catégorie dont le nom existe déjà, ni d'effacer une catégorie qui n'ait pas été ajoutée au préalable. D'autre part, le nombre total réunissant les catégories de filtre préétablies ainsi que celles ajoutées par l'administrateur ne peut pas être supérieur à 128.



L'effacement d'une catégorie est un processus long et coûteux en ressources, sur le Server où est installé OPTENET, cela peut prendre quelques secondes.

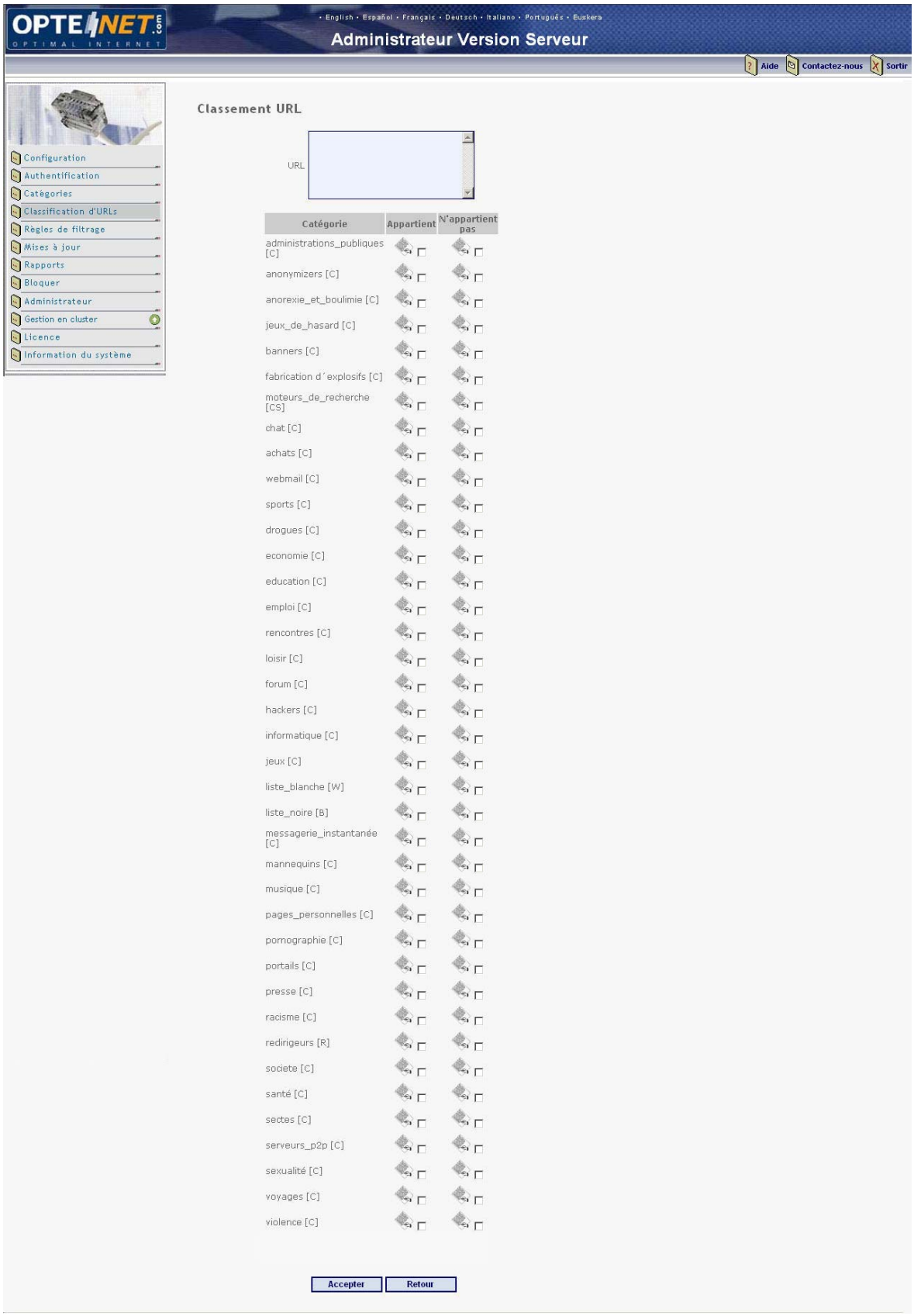
5.6. Classement des URL

Cette option vous permet d'ajouter des URL aux différentes catégories en indiquant si cette URL appartient ou non à une catégorie.

Esta opción es muy útil a la hora de desbloquear URLs que OPTENET asocia a una determinada categoría pero que el administrador no considera que deban pertenecer a dicha categoría.

Avec le nom de chaque catégorie, s'affiche le type de celle-ci :

- C : catégorie de contenus.
- W : catégorie blanche.
- B : catégorie noire.
- S : catégorie de moteurs de recherche.
- R : catégorie de moteurs destinés à rediriger.



Elle est très utile pour débloquer une URL associée par OPTENET à une catégorie donnée, mais qui selon l'administrateur ne devrait pas appartenir à cette catégorie.

Comme les catégories ne sont pas des ensembles exclusifs, cette fenêtre permet d'insérer une URL dans plusieurs catégories à la fois. Par exemple, la presse sportive est catégorisée à la fois comme de la presse et du sport. Ces listes d'utilisateurs sont prioritaires vis-à-vis des listes prédéfinies par OPTENET, ce qui permet de débloquer des URL filtrées par OPTENET ou de bloquer des URL non filtrées par OPTENET. Il est possible de spécifier qu'une page unique appartient ou n'appartient pas à une catégorie en introduisant son URL complète, par exemple:

http://www.dangerousplace.com/index.htm

ou, au contraire, de spécifier qu'un site web complet appartient ou non à une catégorie en le faisant suivre d'un *, par exemple:

http://www.dangerousplace.com/*

Il est également possible d'utiliser l'astérisque comme indicateur au début et au milieu de l'URL. Ainsi, nous pouvons indiquer que tous les host appartenant à une organisation appartiennent à une catégorie déterminée. Par exemple:

http://*.dangerousplace.com*

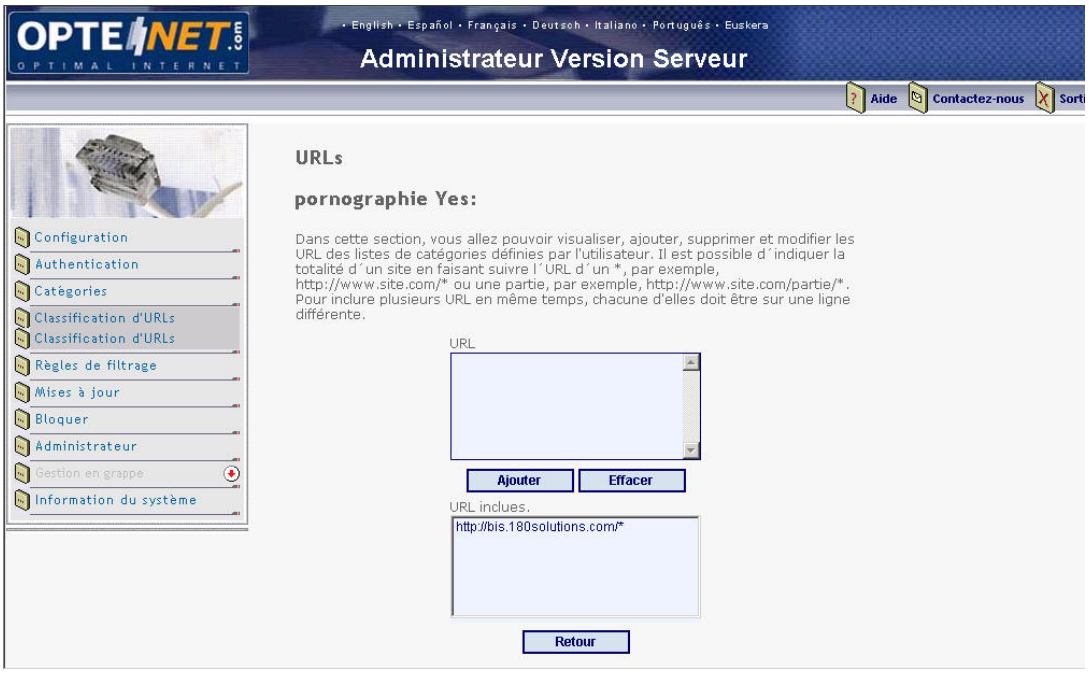
En cliquant sur l'icône à droite de chaque catégorie, vous pouvez éditer la liste des URL ajoutées au fur et à mesure dans cette catégorie. Afin de faciliter la localisation d'éléments concrets, cette liste est classée par ordre alphabétique.
Dans le cas de catégories de type redirectionnel, l'on peut également ajouter des modèles d'extraction d'URL, tels que:

http://www.google.com/search?q=cache:*:#+

où le signe '#' indique l'endroit où apparaîtra l'URL vers lequel il est redirigé. Vous pouvez également utiliser l'astérique très pratique dans des URL appartenant à des catégories comme des moteurs destinés à rediriger.

Il est important de vous rappeler qu'OPTENET fonctionne en interne avec des URL sans protocole (http, https, …).
C'est pourquoi, en saisissant http://www.siteentier.com en pornographie, les url suivantes vont être réparties en différentes catégories de pornographie:
http://www.siteentier.com
https://www.siteentier.com
ftp://www.siteentier.com

L'écran suivant vous permet d'ajouter de nouvelles URL à la liste de celles qui appartiennent à une catégorie ou d'en supprimer quelques-unes en cas d'introduction par erreur, voire d'éliminer toutes les URL saisies dans cette catégorie.. Il est enfin possible d'éditer les listes des URL qui n'appartiennent pas à une catégorie.



Par ailleurs, cet écran oofre la possibilité de consulter à quelles catégories appartient une URL déterminée. Cette fonctionnalité est très utile pour éviter des insertions d'adresses URL dans une certaine catégorie si elles lui appartiennent déjà.

À cette fin, l'utilisateur doit introduire l'URL dans le cadre du teste et presser la touche "Consulter". Le cadre du texte affichera alors la liste des catégories auxquelles appartient ladite URL. Si cette dernière n'appartient à aucune catégorie, le message "N'appartient à aucune catégorie" apapraîtra

5.7. Règles de filtrage

Grâce aux règles de filtrage, vous pouvez facilement personnaliser OPTENET Server pour l'adapter aux besoins de votre réseau.
Cette option vous permet ainsi de définir ces règles et l'ensemble de leurs critères : Groupes d'adresses IP, Utilisateurs, Groupes d'utilisateurs, Catégories, URL, Fichiers et Horaires.
En cas de conflit entre plusieurs règles, n'oubliez pas qu'il est tenu compte de leur priorité pour déterminer laquelle s'applique. En d'autres termes, s'il est possible d'appliquer plusieurs règles à une demande (parce que cet utilisateur est inclus dans plusieurs règles) lors d'une analyse destinée à déterminer si cette demande doit être bloquée ou non, la règle qui s'applique est la première qui apparaît dans l'ordre de priorité.

Après avoir sélectionné l'option «Règles de filtrage», apparaît la fenêtre suivante où figurent toutes les règles que vous avez définies dans le système, ainsi que leur ordre de priorité.
Cet écran permet de créer une nouvelle règle, de modifier ou de supprimer une règle existante, de modifier son ordre de priorité et voir un résumé de ce que contient cette règle. Il suffit de sélectionner la règle que vous souhaitez modifier et de cliquer sur le bouton correspondant. Une nouvelle fenêtre s'affiche où apparaissent le nom de la règle sélectionnée et les opérations disponibles.

5.7.1. Renommer

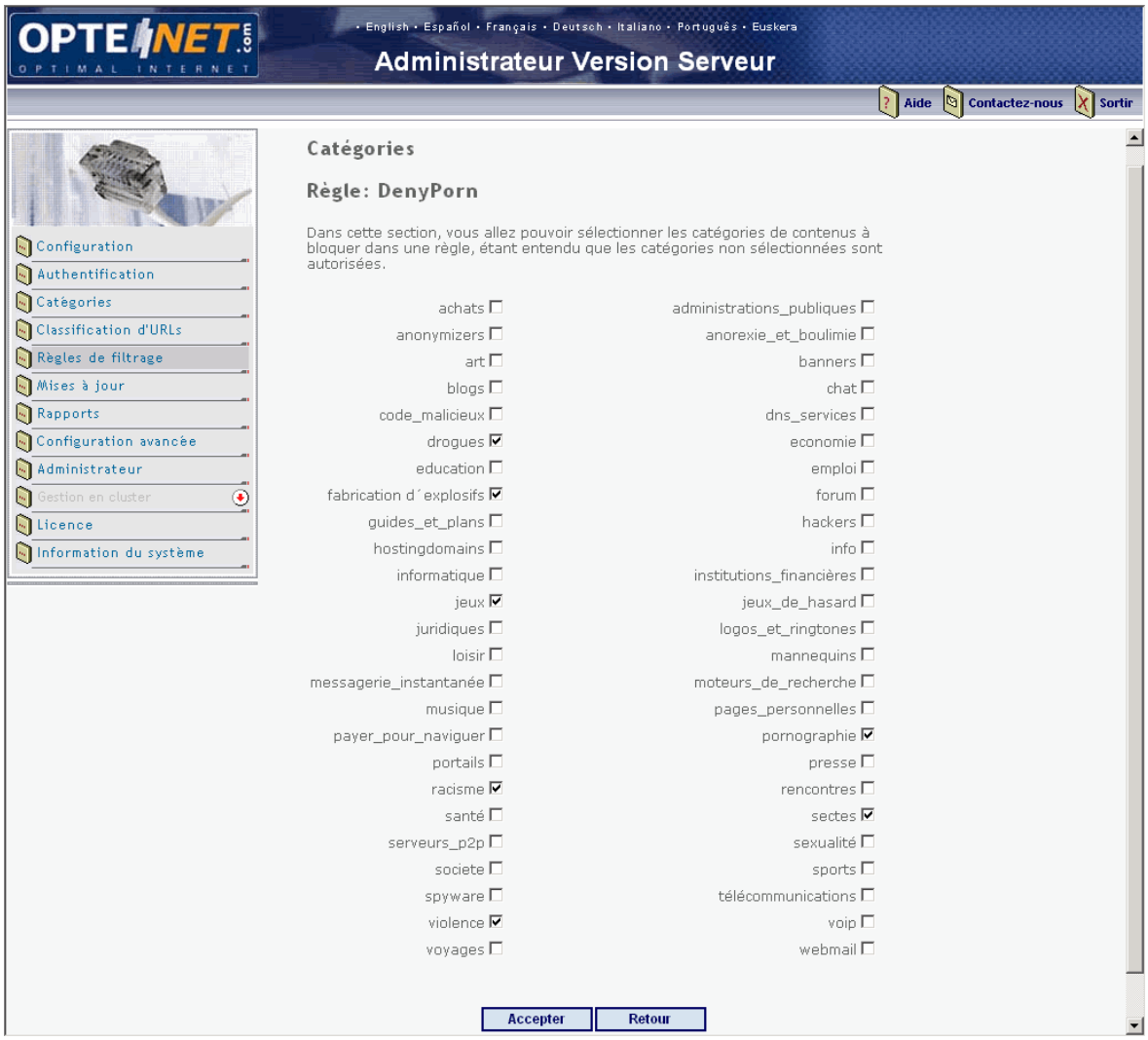
Cette option permet de renommer une règle. En effet, lorsqu'une nouvelle règle est créée, son nom par défaut est R1.Vous avez donc la possibilité de nommer cette règle de manière plus significative.

5.7.2. Action

L'action indique si cette règle va servir à autoriser ou au contraire à refuser les accès aux catégories sélectionnées dans cette règle. Cette option est sélectionnée dans la fenêtre principale de modification d'une règle de filtrage.

5.7.3. Catégories

Cette option vous permet de sélectionner les Catégories de contenus auxquelles s'applique cette règle. Seront uniquement affichées ces catégories dont le type inclut la catégorie de contenus.

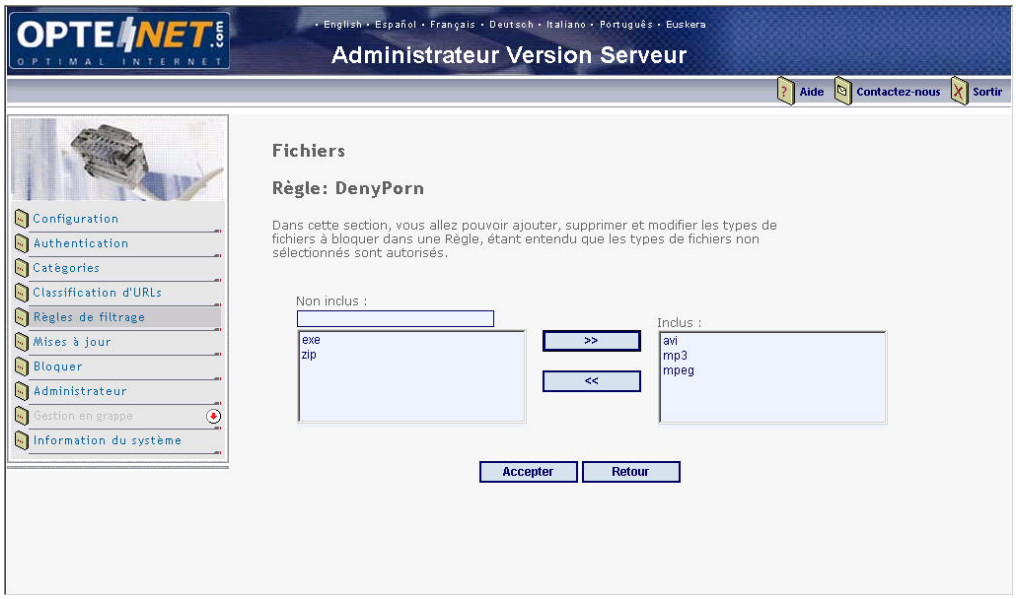


Es posible también crear reglas que se aplican sobre todas aquellas peticiones que el sistema de filtrado no es capaz de categorizar, ya que la URL solicitada no pertenece a ninguna de las categorías soportadas por la herramienta. Para ello, el usuario solo debe marcar la opción “Aplicar sobre peticiones no categorizadas (resto)”. Esta opción puede marcar simultáneamente junto con otras categorías. Así por ejemplo, si se marca esta opción y la categoría pornografía, la regla se aplicará sobre todas las peticiones pertenecientes a la categoría pornografía y además sobre todas las que no tengan ninguna categoría asociada.

5.7.4. Fichiers

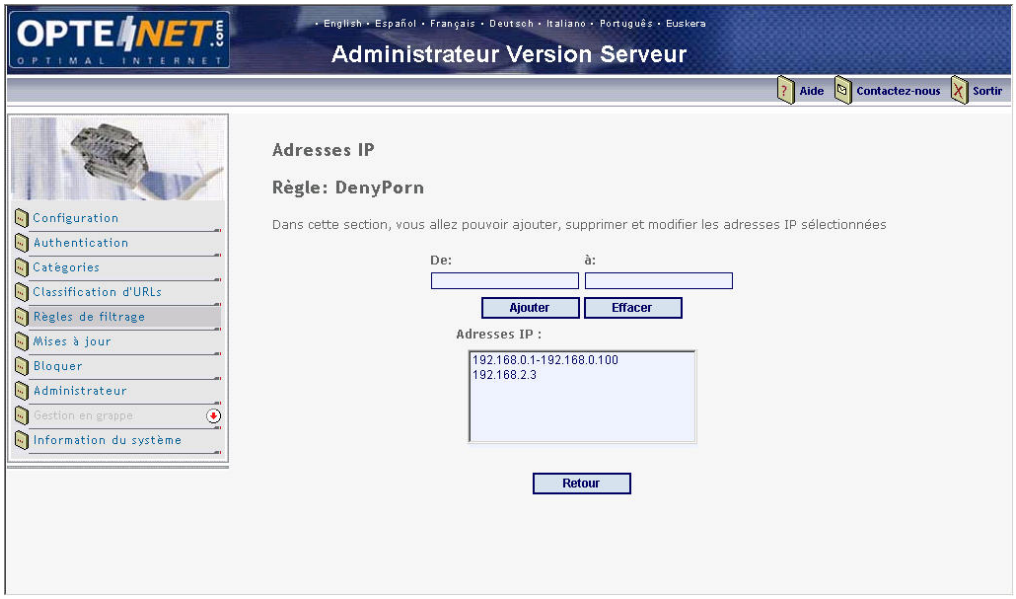
Cette option vous permet de sélectionner les types de fichiers auxquels s’applique la règle, étant entendu que celle-ci ne prend pas en compte les types de fichiers non sélectionnés. OPTENET identifie les types de fichiers affichés dans la colonne de gauche (avi, exe, mp3, mpeg, zip) en analysant leur contenu, tout en étant capable de détecter la multitude de fichiers renommés sur Internet afin d’éviter les filtrages par extension. Cette caractéristique, qui le différencie des autres systèmes de filtrage, peut être mise en œuvre car OPTENET analyse le contenu du fichier téléchargé du réseau.
Outre ce type de fichiers, il est également d’inclure d’autres fichiers différents en décrivant leur extension dans le cadre de texte "non inclus" et en appuyant sur le bouton ">>". Ces

types de fichiers seront filtrés uniquement en extrayant l'extension du fichier en cours de téléchargement.



5.7.5. Adresses IP

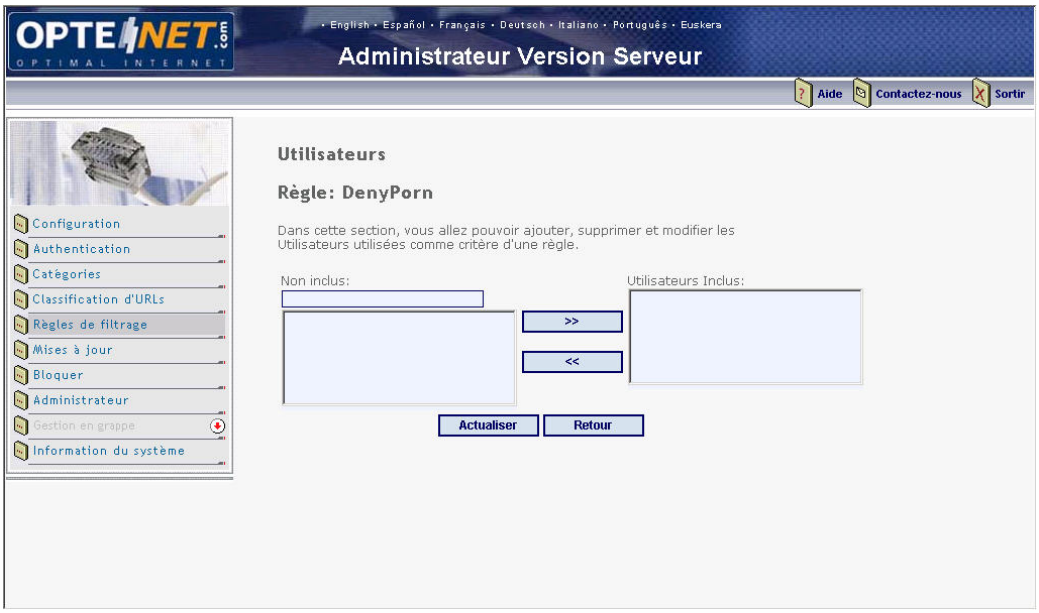
Grâce à cette option, vous allez pouvoir définir des groupes d'adresses IP clientes sur lesquels va agir la règle sélectionnée.



Pour cela, tenez compte des points suivants : Si vous n'indiquez aucune adresse IP, cette règle va s'appliquer à toutes les demandes, quelle que soit l'adresse IP. Au contraire, si vous indiquez une adresse IP, la règle ne va s'appliquer qu'aux demandes en provenance de cette adresse IP cliente. Pour le reste des demandes, il est donc considéré que cette règle n'est pas applicable.
Il est possible d'indiquer des IP isolées, en introduisant uniquement l'IP dans le champ **De :** ou bien d'indiquer des rangs d'IP, en introduisant l'IP initiale dans le champ **De :** et l'IP finale dans le champ **À :**

5.7.6. Utilisateurs

Cette option vous permet d'ajouter, de supprimer ou de modifier des utilisateurs auxquels va s'appliquer cette règle.

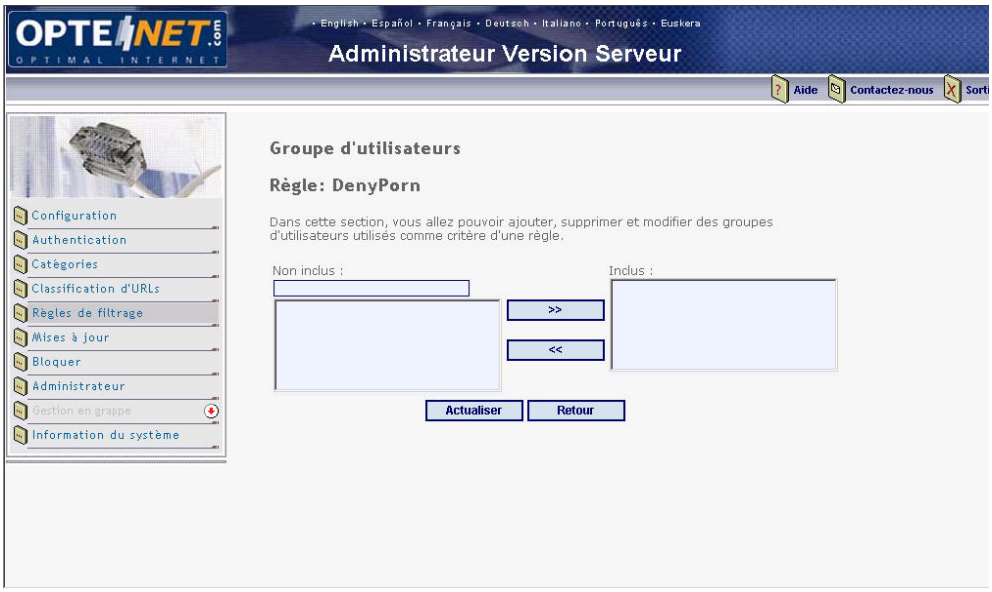


Pour pouvoir établir des règles par utilisateurs, vous devez configurer votre proxy ou appliance pour qu'il réalise l'authentification des utilisateurs ou bien forcer OPTENET à effectuer cette authentification en activant dans la section de configuration l'option « Activer authentification ».
Pour que les utilisateurs de votre Server LDAP ou de votre domaine Windows NT apparaissent dans la liste Non inclus, vous devez préalablement configurer ce Server à partir de l'option « Authentification ». Tous les utilisateurs apparaissent quand vous cliquez sur le bouton « Actualiser ». Si aucun utilisateur n'apparaît dans le syslog du système Linux (fichier /var/log/messages sous Linux ou /var/adm/messages sous Solaris ou AIX) ou bien dans l'observateur d´évènements de Windows, la cause pour laquelle les utilisateurs de ce Server n'ont pas pu être obtenus s'affiche.

Comme pour les IP, cette règle s'applique à tous les utilisateurs si aucun n'est indiqué ou aux utilisateurs sélectionnés dans le cas contraire.

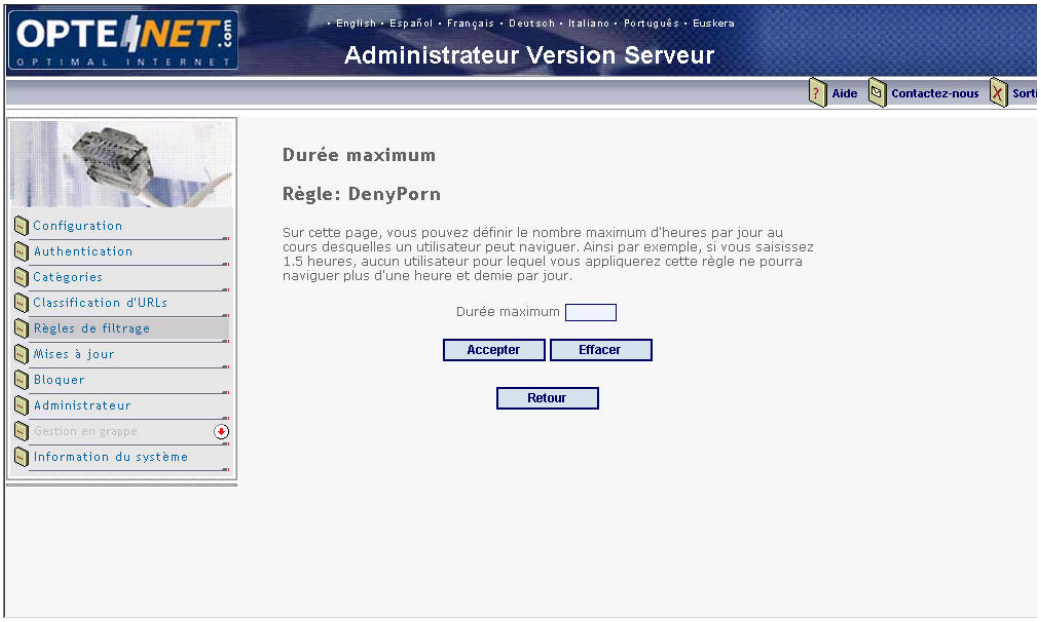
5.7.7. Groupes d'utilisateurs

Cette option permet d'ajouter et de supprimer des groupes d'utilisateurs auxquels va s'appliquer cette règle. Pour qu'ils apparaissent dans la liste Non inclus d'un Server LDAP donné ou d'un Domaine Windows, vous devez préalablement configurer ce Server à partir de l'option « Authentification », puis cliquer sur Actualiser. Si pour une même règle vous spécifiez des utilisateurs individuels et des groupes d'utilisateurs, cette règle s'applique à un utilisateur à condition qu'il se trouve dans la liste des utilisateurs introduits dans la règle ou que l'un des groupes auquel il appartienne se trouve dans la liste des groupes auxquels va s'appliquer cette règle. Veuillez prendre en compte les explications du chapitre 5.4 « Authentification des utilisateurs » si vous souhaitez associer des groupes d'utilisateurs aux règles de filtrage.



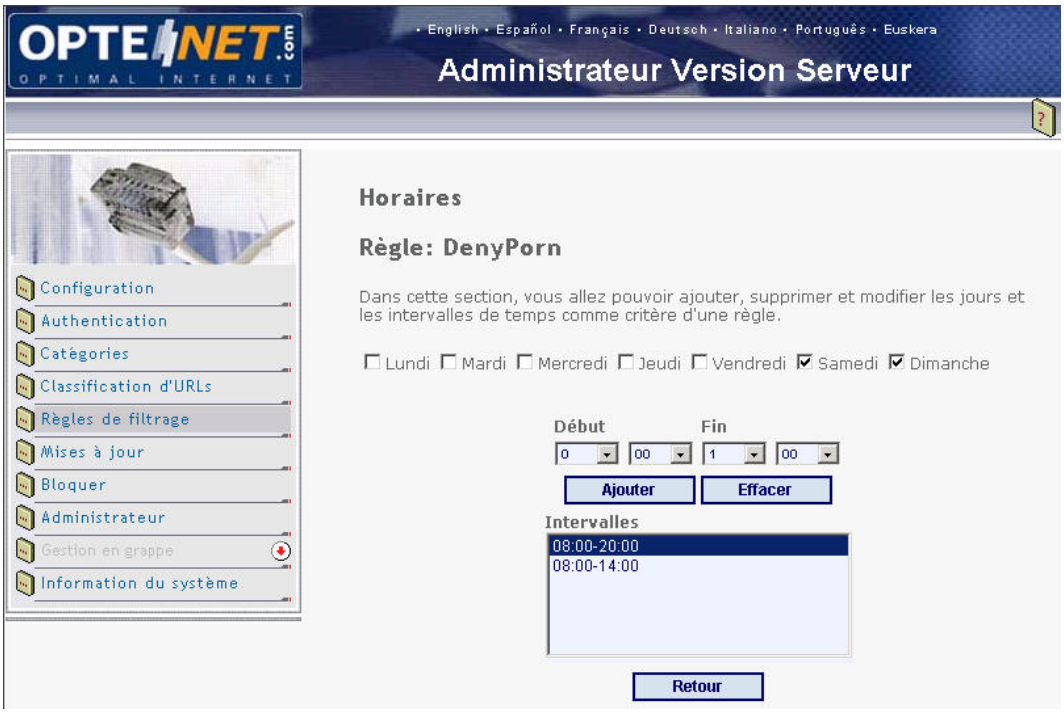
5.7.8. Durée maximum de navigation

Cette option vous permet d'inclure dans la règle sélectionnée la durée maximum en heure pendant laquelle les utilisateurs, les adresses IP ou les groupes d'utilisateurs définis dans cette règle ont le droit de naviguer sur Internet par jour. De même, vous avez la possibilité d'annuler cette option en cliquant sur le bouton « Effacer ».



5.7.9. Horaires

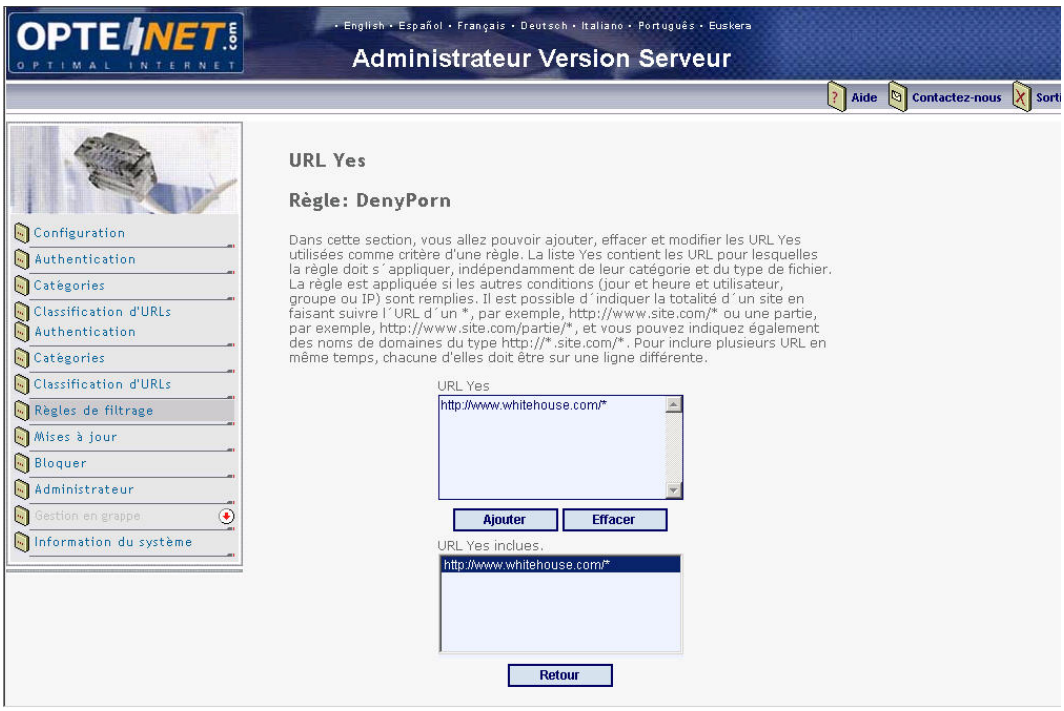
Vous avez ici la possibilité d'ajouter, de supprimer ou de modifier les jours de la semaine et les franges horaires d'application d'une règle. En dehors des franges horaires indiquées, la règle concernée n'aura aucun effet. Si aucune frange n'était indiquée, la règle serait valable 24 heures sur 24, 7 jours sur 7.



5.7.10. URL Yes

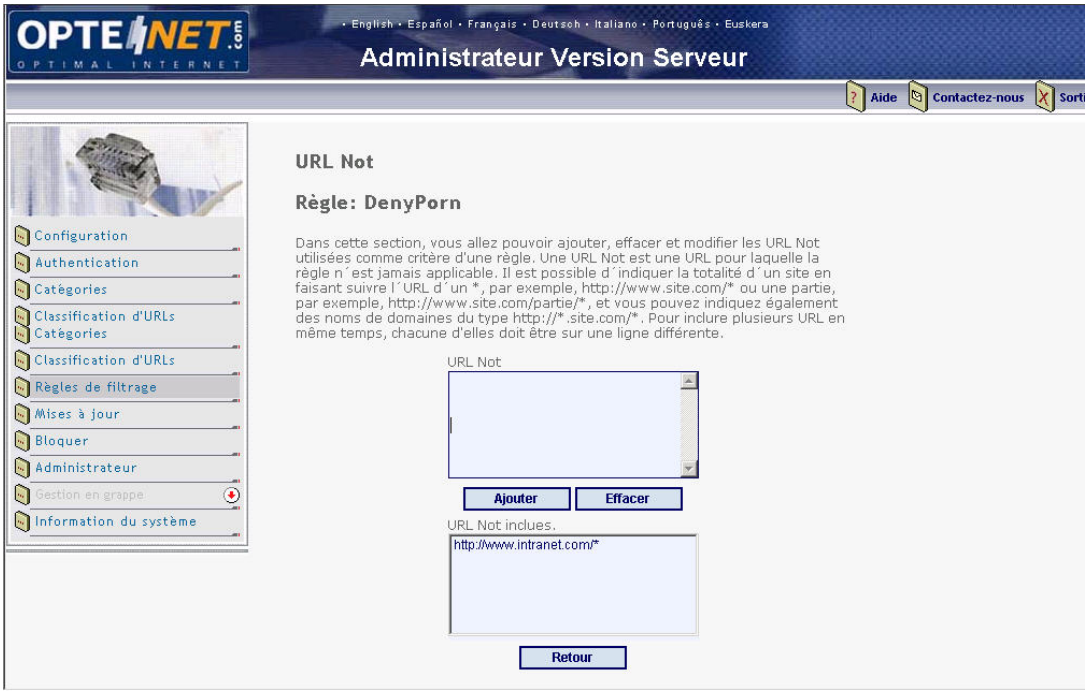
Cette option vous permet d'ajouter, de supprimer ou de modifier des URL Yes utilisées comme critère d'une règle. La liste Yes contient les URL pour lesquelles la règle doit s'appliquer, indépendamment de leur catégorie et du type de fichier. La règle est appliquée si les autres conditions (jour et heure et utilisateur, groupe ou IP) sont remplies. Si l'action de la règle est d'autoriser, les URL concernées sont alors explicitement autorisées. Au contraire, si l'action de la règle est de refuser, ces URL sont bloquées.

Il est possible d'indiquer la totalité d'un site en faisant suivre l'URL d'un *. Il est également possible d'utiliser l'astérisque comme indicateur au début et au milieu de l'URL.



5.7.11. URL Not

Cette option vous permet d'ajouter, de supprimer ou de modifier des URL Not utilisées comme critère d'une règle.



La liste Not contient les URL pour lesquelles la règle n'est jamais applicable, c'est-à-dire qu'il s'agit des exceptions à la règle. Il est possible d'indiquer la totalité d'un site en faisant suivre l'URL d'un *. Il est également possible d'utiliser l'astérisque comme indicateur au début et au milieu de l'URL.

5.7.12. Exemple d'utilisation des règles

Voyons comment les règles fonctionnent à l'aide de quelques exemples simples.

Par défaut, il n'existe à l'installation d'OPTENET qu'une règle unique, DenyPorn, qui bloque les accès à tous les sites à contenu pornographique. Voyons comment cette règle est configurée. Dans l'option « Catégories », cette règle ne spécifie que les catégories de base de filtrage : pornographie, racisme, violence, drogues et fabrication d'explosifs, c'est-à-dire qu'elle interdit ces cinq catégories. A qui ces contenus sont-ils interdits ? En regardant les utilisateurs, vous allez vous apercevoir qu'il n'y en a aucun défini. La règle s'applique donc à tous les utilisateurs. Il en va de même en ce qui concerne les groupes d'utilisateurs. A quels ordinateurs ? De même, aucune adresse IP n'est définie. Cette règle s'applique donc à toutes les adresses IP. Quels sont les horaires ? Cette règle s'applique toute la journée car aucun horaire n'a été spécifié. Existe-t-il des exceptions à cette règle ? Aucune URL n'apparaît ni dans la liste URL Yes (URL qui satisfont directement cette règle) ni dans la liste URL Not (URL qui ne satisfont jamais cette règle). Il n'y a donc aucune exception à cette règle.

Pour résumer, à l'installation du filtre, l'accès à ces contenus est bloqué par défaut à tous les utilisateurs et postes qui naviguent sur Internet par l'intermédiaire du proxy.

5.7.12.1. Règle pour le directeur

Imaginons maintenant que le directeur vous exige un accès sans filtre. Cela signifie que le directeur ne doit être affecté par aucune règle de filtrage. La solution est simple : il suffit de créer une règle pour le directeur dans laquelle vous allez inclure le nom d'utilisateur utilisé par le directeur pour s'identifier ou son adresse IP s'il n'y a aucune identification par nom d'utilisateur. Spécifier ensuite l'action de cette règle en indiquant « Autoriser » et ne sélectionnez aucune catégorie. Vous venez de créer une règle qui ne s'applique qu'au directeur. Mais qu'autorise-t-elle ? Comme vous n'avez spécifié aucune catégorie ni aucun type de fichier, tous les contenus seront autorisés. Quand ? Aucun horaire ni aucun jour n'ayant été sélectionné, cette règle autorise tout et tout le temps.

Un dernier détail. Vous devez maintenant placer cette règle comme étant la plus prioritaire. Ainsi, pendant que le directeur navigue sur Internet, OPTENET va analyser ses demandes en commençant par la règle la plus prioritaire, puis va voir que les demandes satisfont cette règle et ainsi autoriser l'accès à tous les contenus.

5.7.12.2. Règle de blocage de la presse et du sport pendant les horaires de travail

Autre exemple : Supposons que vous souhaitez maintenant bloquer les accès aux contenus liés aux sports et à la presse pendant les horaires de travail (9h-14h et 16h-19h) du lundi au vendredi. Rien de plus simple. Créez une nouvelle règle appelée PresseAuTravail et spécifiez l'horaire suivant : de 9h à 14h et de 16h à 19h du lundi au vendredi. Les catégories filtrées par cette règle sont Presse et Sports.

Quelle doit être sa position ? Parmi les trois règles existantes pour le moment, vous devez déterminer quelle est la règle la plus générale et la placer en fin de liste, et remonter dans la hiérarchie jusqu'à la plus spécifique. Ainsi, la catégorie la plus générale serait DenyPorn, interdisant la pornographie, puis viendrait PresseAuTravail et finalement celle du directeur.

Pouvons-nous inclure les catégories Presse et Sports dans la règle DenyPorn et spécifier comme horaire les horaires de travail ? La réponse est non. Il est nécessaire de créer une nouvelle règle, car si DenyPorn était modifiée par l'ajout de catégories supplémentaires et d'un changement d'horaire, il serait possible d'accéder à des contenus pornographiques en dehors de cet horaire (à partir de 19h).

5.8. Mises à jour

OPTENET Server se connecte de manière continue aux différents Servers d´actualisation pour compléter sa base de données d´URL de manière incrémentale et ainsi pouvoir filtrer les nouvelles adresses catégorisées d'Internet qui apparaissent jour après jour. Toutes ces nouvelles URL sont emmagasinées en mémoire pour un fonctionnement efficace et devront être sauvegardées sur disque au bout d´une certaine période. Cette option permet de définir la fréquence de mise à jour (Quotidienne, Hebdomadaire ou Mensuelle) de sauvegarde sur disque de ces nouvelles adresses reçues. A partir de cette option, nous pouvons configurer les paramètres suivants:

5.8.1. Par le biais d'un proxy

Sélectionnez cette option si le Server où est installé OPTENET ne peut accéder directement à Internet et a besoin de sortir par le biais d'un proxy. Indiquez l'adresse IP du proxy (ou son nom) et le port. Veillez à ce que ce proxy ne demande pas d'authentification pour les demandes d'OPTENET.

5.8.2. Fréquence des mises à jour

OPTENET demande les nouvelles URL qui vont être classées par ordre croissant et fractions de plusieurs Kbytes pour ne pas saturer le trafic du réseau. Le délai entre les mises à jour indique les secondes pendant lesquelles OPTENET patiente entre deux mises à jour consécutives, en supposant que de nouvelles URL doivent être mises à jour. Le délai entre les vérifications indique les secondes pendant lesquelles OPTENET patiente lorsque la mise à jour est totalement achevée et avant de réaliser une nouvelle vérification.
Les valeurs par défaut (30 et 300 secondes) sont conçues pour que les déblocages pouvant être demandés depuis la page de blocage parviennent au filtre en peu de temps.

5.8.3. Consolidation sur le disque

Les nouvelles adresses que reçoit le filtre sont stockées dans la mémoire pour des raisons d'efficacité et sont conservées sur le disque pendant le processus de consolidation. Ce processus peut être programmé à raison d'une fréquence quotidienne, hebdomadaire ou mensuelle, en indiquant l'intervalle d'heure de démarrage. OPTENET recommande une mise à jour quotidienne sur le disque, coïncidant avec les périodes d'activité les plus faibles sur le réseau, qui ont généralement lieu la nuit.

5.8.4. Chargement complet des listes

Actuellement, il est possible d'effectuer un chargement complet des listes en appuyant simplement sur le bouton "Charger maintenant" situé en bas de la fenêtre. Une fois le processus de chargement lancé, vous pourrez suivre l'évolution du chargement à partir de la section "Informations système", où seront indiqués les bytes chargés ainsi que la taille totale et le résultat du chargement.

5.9. Rapports

En appuyant sur cette option, une autre fenêtre de navigation s'ouvre et se connecte avec OPTENET Reporter. OPTENET Reporter est l'outil qui vous permet d'élaborer des rapports sur l'utilisation d'Internet. Par défaut, il peut être installé avec OPTENET Server car il est distribué conjointement.
Si, lorsque vous appuyez sur cette option, OPTENET Reporter ne s'exécute pas, un message indiquant qu'il est impossible d'établir le contact avec l'outil d'élaboration de rapports s'affiche. Veuillez vous assurer qu'OPTENET Reporter est en cours d'exécution et qu'il est installé sur l'IP de l'ordinateur en écoutant le port indiqué. Par défaut, OPTENET Server tente d'établir le contact avec un OPTENET Reporter installé sur le même Server.

Une fois que OPTENET Reporter a démarré et que vous êtes certain d'avoir correctement configuré votre IP et port d'administration dans cette section d'OPTENET Server, appuyez sur l'option "Rapports" et une nouvelle fenêtre de navigation s'ouvrira pour l'administration d'OPTENET Reporter. Nous recommandons de lire le manuel de l'utilisateur d'OPTENET Reporter pour plus de renseignements.

5.10. Identification Administrateur

OPTENET Server établit plusieurs niveaux d'administration selon le tableau ci-dessous:

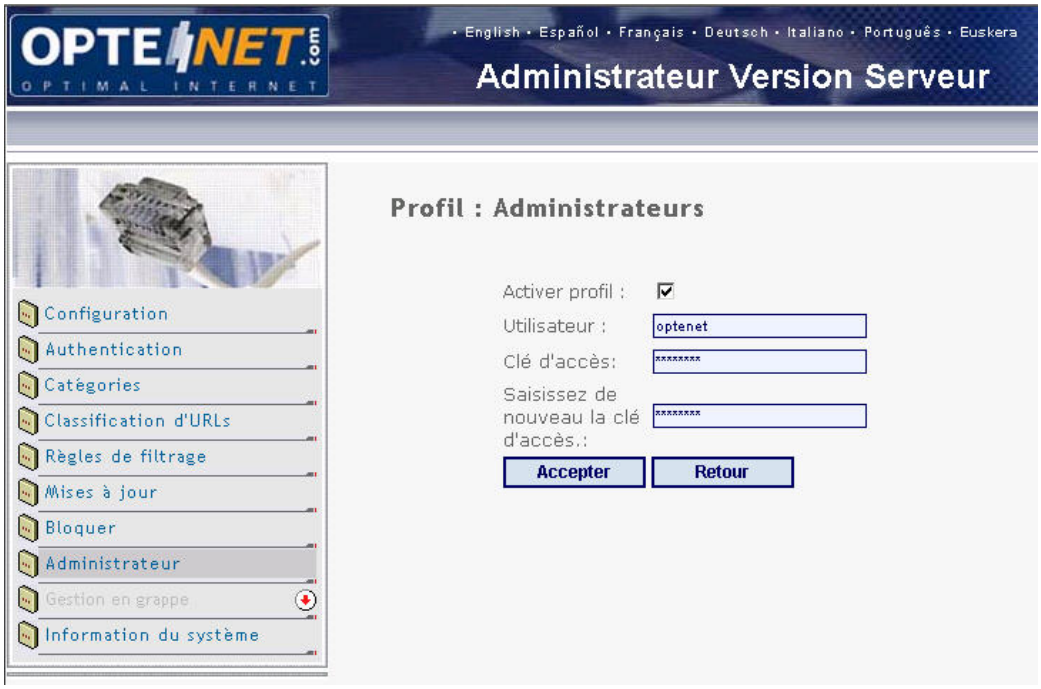
	Administrateur	Administrateur local	**Catégories et Administrateur URL**	**Rapports Opérateur**
Introduction	X	X	X	X
Documentation	X	X	X	X
Configuration	X			
Authentification	X			
Activer authentification	X			
Type d'authentification	X			
Catégories	X	X	X	
Classement des URL	X	X	X	
Voir	X	X	X	
Ajouter	X	X	X	
Supprimer	X	X	X	
Règles de filtrage	X			
Supprimer	X			
Ajouter	X			
Modifier	X			
Modifier les URLs et catégories associées à une règle	X		X	
Mises à jour	X			
Rapports	X	X		X
Blocage	X	X		
Administrateur	X	X		X
Administrateurs	X			
Administrateurs locaux	X	X		
Administrateur Catégories et Urls	X	X		
Opérateurs rapports	X	X		
Gestion en cluster	X			
Licence	X			
Information du système	X	X		X
Obtention des logs pour le reporter	X			X

Par défaut, il existe dans l'installation un utilisateur pour chaque profil et seuls les niveaux « Administrateur » et « Opérateur des informations » sont actifs. Le premier bénéficie d'un contrôle total sur le filtre et peut effectuer toutes les opérations d'administration, sauf celles de création et de suppression des utilisateurs appartenant au profil « Opérateur des informations » ni, par conséquent, celle de gestion de la clé de visualisation des informations sensibles. Par défaut, le nom d'utilisateur est **OPTENET** et le mot de passe est **12345678**. Ces valeurs peuvent être modifiées à partir de l'administration web par

l'intermédiaire de l'option «Administrateur du menu». Il est conseillé de les modifier juste après l'installation d'OPTENET Server.

Pour chaque profil, il est possible de modifier les données des utilisateurs existants par défaut dans l'installation et d'ajouter de nouveaux utilisateurs ou de supprimer ceux que vous souhaitez. Pour cela, en appuyant sur ¨Administrateur¨ on vous indique la liste de tous les utilisateurs regroupés par profil, sélectionnez l'utilisateur à supprimer ou à modifier et cliquez sur le bouton correspondant ou cliquez simplement sur le bouton « Nouveau » si vous souhaitez créer un nouvel utilisateur.

Pour activer les autres niveaux de mise à jour, cliquez sur le bouton associé au niveau souhaité sur l'écran suivant, cochez la case « Activer profil », introduisez le nom d'utilisateur, le mot de passe, puis cliquez sur le bouton « Accepter » comme indiqué sur la figure ci-après:



Il convient de prêter une attention particulière à l'opérateur des informations sensibles. OPTENET Server conserve dans les fichiers journaux toutes les demandes et tous les blocages qu'il a réalisés. Si vous voulez utiliser les informations des logs, vous devez installer OPTENET Reporter sur le même Server, ou sur un autre Server. Par la suite vous devez configurer OPTENET Reporter afin qu'il sache où est le Server OPTENET, et qu'il puisse ainsi récupérer les informations de logs et créer des rapports. Afin qu'OPTENET Reporter puisse demander les logs à OPTENET, il doit s'identifier via un utilisateur et un mot de passe valide. Cet utilisateur doit être un opérateur de rapports, qui doit être actif.

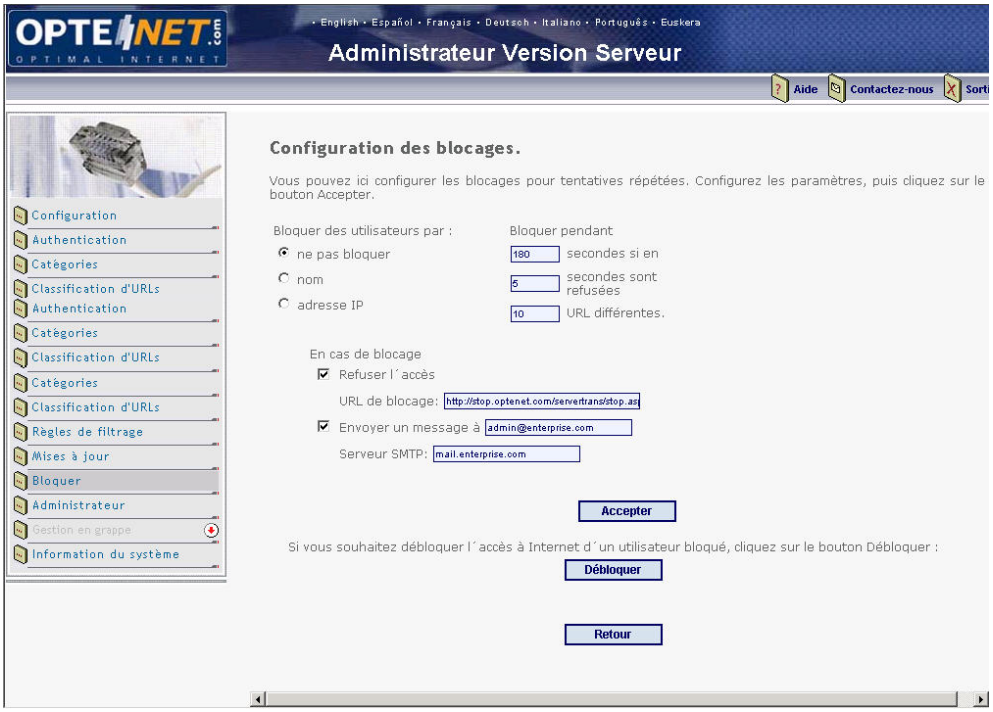
5.11. Configuration avancée

Cet écran permet à l'administrateur de réaliser une série d'actions à caractère avancé pour personnaliser de façon plus spécifique ses caractéristiques de filtrage. Parmi ces options, il peut:

- Configurer les blocages pour tentatives répétées.
- Configurer le filtrage de services de messagerie instantanée Skype.
- Vider les logs de navigation générés par OPTENET.

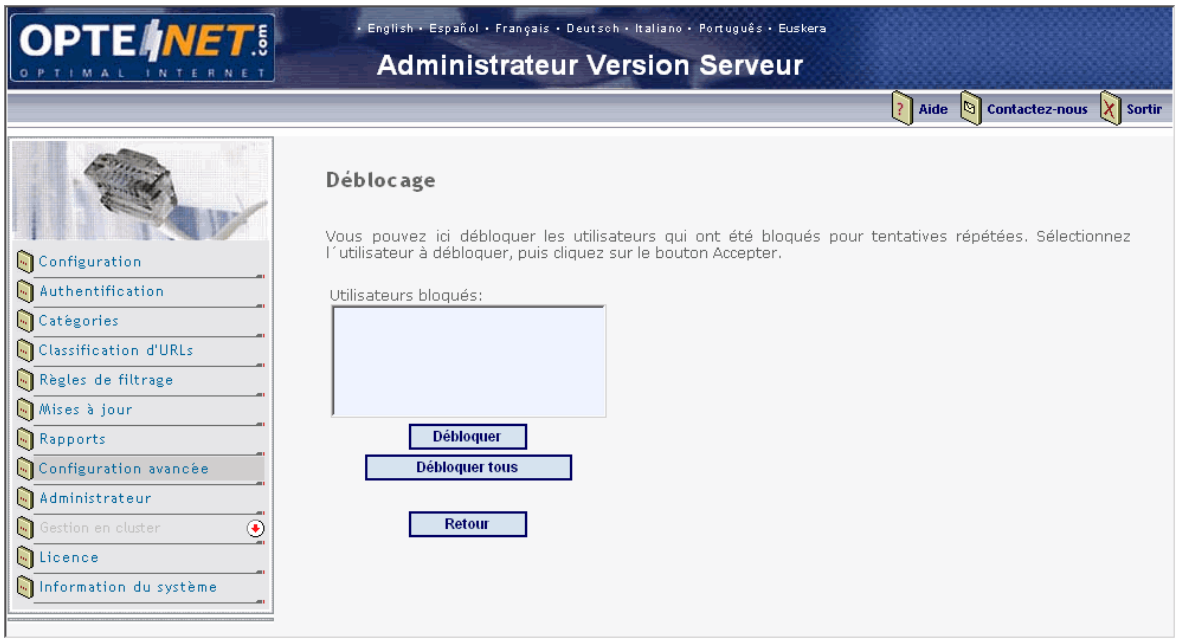
5.11.1. Configuration de blocages pour tentatives répétées

Cette nouvelle caractéristique permet de bloquer totalement l'accès d'un utilisateur à Internet qui, pendant une période donnée, a essayé d'accéder à plusieurs sites non autorisés. L'objectif de cette fonctionnalité est de pénaliser les utilisateurs qui essaient de passer outre le filtre.



Par défaut, cette option est désactivée. Pour l'activer, il suffit de spécifier si les utilisateurs vont s'identifier par nom (utilisateur en s'authentifiant) ou par adresse IP, la durée de blocage pour pénalisation et le nombre de blocages autorisés pendant une période donnée.
En outre, dans le cas du blocage, il est possible de spécifier la page de blocage à afficher à l'utilisateur et la possibilité d'envoyer un message électronique à l'administrateur du système pour l'avertir de la situation.

Si vous souhaitez débloquer une personne qui a été bloquée pour cette raison, il est possible de le faire depuis l'écran suivant, qui apparaît après avoir cliqué sur Débloquer.



Sur cet écran, apparaît une liste incluant tous les utilisateurs actuellement bloqués. Vous pouvez concrètement débloquer un utilisateur en le sélectionnant et en poussant la touche ‘Débloquer’. Vous pouvez également débloquer tous les utilisateurs en cliquant seulement sur le bouton ‘Débloquer tous’.

5.11.2. Détection de Skype

Skype est une célèbre application de messagerie instantanée qui permet à ses utilisateurs d'émettre des appels téléphoniques via Internet, d'établir des communications via Chat, d'envoyer des fichiers, etc.

La particularité de cette application est qu'elle n'utilise pas une série de ports prédéfinis pour établir les communications entre les différents utilisateurs. En effet, lorsque les ports par défaut ne sont pas disponibles, les communications sont réalisées par le biais des ports destinés aux communications HTTP (80) et HTTPS (443).

Ceci permet aux utilisateurs de Skype d'éviter les possibles limitations intégrées dans les pares feu puisque ceux-ci fonctionnent en coupant les communications sortantes ou entrantes à des ports déterminés. Par conséquent, la coupure de l'accès auxdits ports ne suffit pas à empêcher le fait que les utilisateurs de notre organisation ne puissent pas utiliser le service Skype.

En outre, Skype chiffre avec un algorithme propriétaire absolument tout ce qu'il transmet avant de le lancer sur Internet, ce qui rend encore plus difficile l'identification des paquets de données provenant des clients Skype.

Pour la détection des possibles communications Skype, Optenet utilise une analyse de la communication de façon à ce que tous les paquets suspectés de contenir des messages Skype soient analysés, en déterminant si un nœud précis utilise les ports HTTP ou HTTPS pour des communications de ce type.

Lorsque vous accédez à la configuration de détection Skype, l'écran suivant apparaît :

Celui-ci affiche toutes les options disponibles.

5.11.2.1. Activer détection Skype

Par défaut, l'option de détection de Skype est activée. Pour l'activer, il suffit de cocher l'option correspondante. Le reste des paramètres de configuration ne prendront effet que si cette option est activée. De plus, l'option de détection Skype n'est actuellement disponible que pour les intégrations avec des systèmes ICAP.

5.11.2.2. Nombre maximal de connexions simultanées

Pour réaliser la détection de trafic Skype, OPTENET analyse les messages suspectés d'appartenir à des communications Skype.

Pendant l'analyse, le fil ICAP qui gère la demande est occupé. Avec la définition de ce paramètre, nous pouvons limiter le nombre de fils ICAP simultanés que nous allons utiliser pour la détection Skype, de façon à pouvoir toujours libérer certains fils réservés à la navigation traditionnelle.

La bonne définition de ce paramètre est très importante puisque les clients Skype traditionnels, en se connectant, effectuent plusieurs demandes en parallèle avec plusieurs autres Servers Skype. Si nous laissons les détections Skype consommer toutes les connexions ICAP disponibles, nous resterons sans service WWW le temps de l'analyse Skype. Par conséquent, il est recommandé de ne pas attribuer de valeur supérieure ou égale à 50% du nombre total de fils ICAP habilités.

5.11.2.3. Durée de vie des nœuds détectés comme Skype

Lorsqu'un nœud est détecté comme Skype par OPTENET, ce nœud est conservé dans un cache interne pour éviter que les futures demandes à ce nœud ne soient pas à nouveau analysées. Les entrées dudit cache ont une durée de vie déterminée qui est

définie dans cette section. La durée de vie minimale d'une entrée dans ce cache est de 3600 secondes.

Il est possible que nous souhaitions que les entrées du cache n'expirent jamais. Pour cela, nous devons saisir la valeur zéro dans la case correspondante. Ainsi, les entrées resteront dans le cache et seront appliquées en permanence.

5.11.2.4. Timeout des connexions de détection Skype

Pour réaliser la détection Skype, une série de connexions sont activées contre les nœuds Skype potentiels. Il est possible que lesdites connexions soient refusées, comme toute autre connexion. Le temps qu'OPTENET attend pour recevoir une réponse du Server à tester est défini dans cette section. Par défaut, sa valeur est 10 secondes.

5.11.2.5. Activer détection aux ports

OPTENET permet de déterminer les ports sur lesquels le test de patrons Skype doit être effectué. Il est possible d'activer la détection sur les ports 80 et 443 de façon indépendante. Ainsi, un utilisateur peut décider de tester les communications qui se dirigent vers le port 80 uniquement, vers le port 443 ou vers les deux.

Si la détection de Skype est activée, il est obligatoire qu'au moins un port soit activé. De la même manière, il est recommandé que la détection soit faite pour les deux ports puisque les clients Skype utilisent indifféremment l'un ou l'autre pour encapsuler leurs communications.

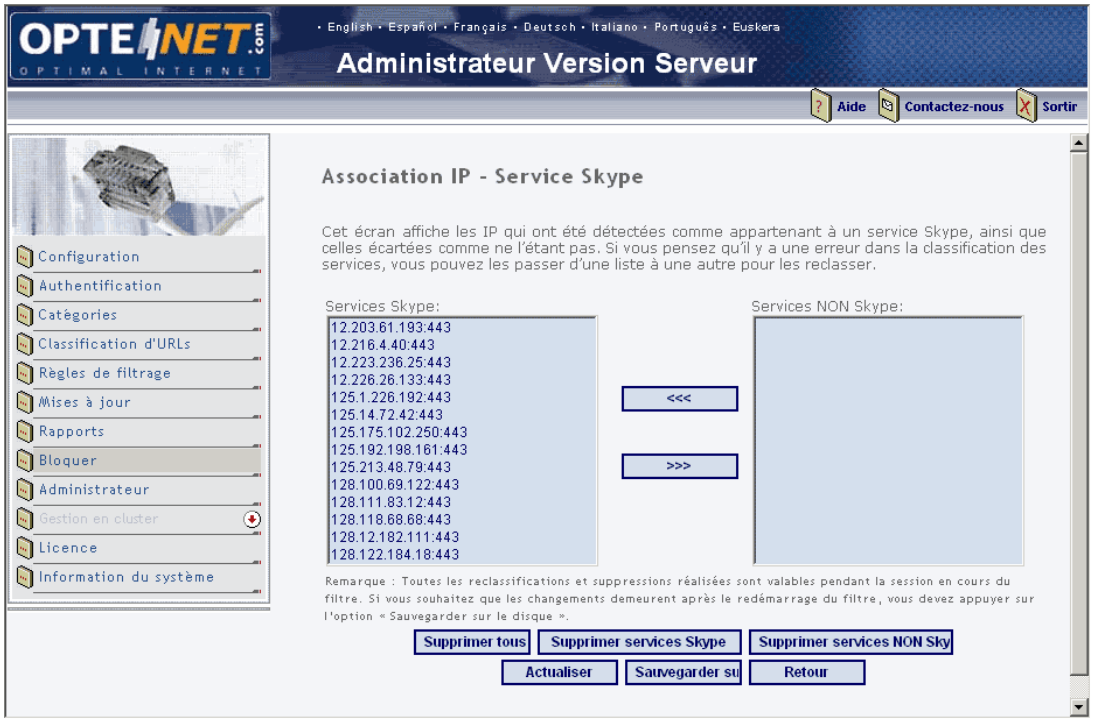
5.11.2.6. Politiques de fonctionnement

OPTNET permet à l'administrateur de définir les différentes politiques de fonctionnement en lui laissant le choix d'agir dans certains cas pouvant se présenter pendant la détection Skype. Les politiques pouvant être définies par l'administrateur sont :

- Bloquer les demandes ne pouvant pas être analysées pour avoir dépassé le nombre maximum de connexions simultanées : Lorsqu'une demande qui est susceptible de contenir du trafic Skype, elle ne peut être analysée puisque tous les fils destinés à la détection sont occupés. L'administrateur peut choisir de bloquer la demande ou de la laisser passer. Dans ce cas, quel que soit son choix, elle ne sera jamais incluse dans le cache interne, donc si une demande identique arrive et que des fils sont disponibles, elle sera analysée. Par défaut, elle est activée.
- Bloquer les nouvelles demandes destinées aux sites en cours d'analyse. Lorsqu'une demande arrive à un nœud qui est déjà en cours d'analyse, cette nouvelle demande peut être à nouveau analysée ou bloquée momentanément. Par défaut, ces demandes sont bloquées de façon à ne pas saturer les fils de détection rapidement.
- Bloquer les demandes ne pouvant être vérifiées de par l'écoulement du timeout de la connexion : Lorsqu'une demande à un nœud suspect d'être Skype est analysée, il est possible que ce nœud ne réponde pas dans les délais impartis par l'administrateur. Si ce temps de connexion s'écoule, l'administrateur peut décider de bloquer ou d'autoriser la demande. Par défaut, l'option de blocage est activée.
- Inclure dans le cache de Skype les entrées ayant été écartées comme trafic Skype : Lorsqu'une détection Skype a été menée, l'analyse peut avoir détecté que ledit nœud ne contient pas de trafic Skype. L'administrateur peut décider si ces entrées sont incluses ou non dans le cache interne de noeuds Skype, de façon à ce que, s'ils ne sont pas inclus, lorsque une nouvelle demande arrive, elle soit à nouveau analysée. Par défaut, cette option est activée.

5.11.2.7. Gestion du cache de détections Skype

De plus, l'administrateur peut gérer le cache de détections Skype. Pour cela, il doit appuyer sur le bouton "Voir caché". Un écran comme le suivant apparaît :



Cet écran affiche deux listes. La liste de droite contient une relation de tous les noeuds qui ont été détectés comme appartenant à des communications Skype et dont la durée de vie n'a pas encore expiré. La liste de gauche indique les noeuds qui ont été écartés comme appartenant à des communications Skype.

L'administrateur peut passer des noeuds d'une liste à l'autre en sélectionner une entrée d'une des listes et en appuyant sur le bouton correspondant. De la même manière, il peut supprimer les éléments de la liste de nœuds Skype, ceux de la liste de nœuds Non Skype, ainsi que toutes les entrées du cache.

Toutes ces opérations sont réalisées dans la session en cours d'OPTENET, de façon à ce que si vous souhaitez que les changements réalisés soient maintenus entre les sessions (si nous redémarrons le filtre par exemple), l'administrateur devra appuyer sur le bouton "Sauvegarder sur le disque". De plus, l'administrateur pourra actualiser la liste à tout moment puisque celle-ci peut être changée dynamiquement si la détection est activée.

5.11.3. Vidage de logs

OPTENET n'écrit pas les entrées des logs de navigation qui sont générés directement sur le disque. Il stocke ces entrées en interne pour les écrire en une seule action. Ceci permet au processus d'écriture de logs d'être plus efficace. Lorsque la taille maximale de l'espace de stockage temporaire est atteinte ou au-delà d'un intervalle de temps sans écriture sur le disque, OPTENET vide les données stockées automatiquement.

Grâce à cette option, l'administrateur peut provoquer un vidage immédiat des entrées en cours d'écriture.

5.12. Gestion en cluster

Cette version d'OPTENET Server permet de manipuler plusieurs instances* d'OPTENET Server à partir d'un seul Server web. Ce mode de travail s'appelle «Gestion en cluster».

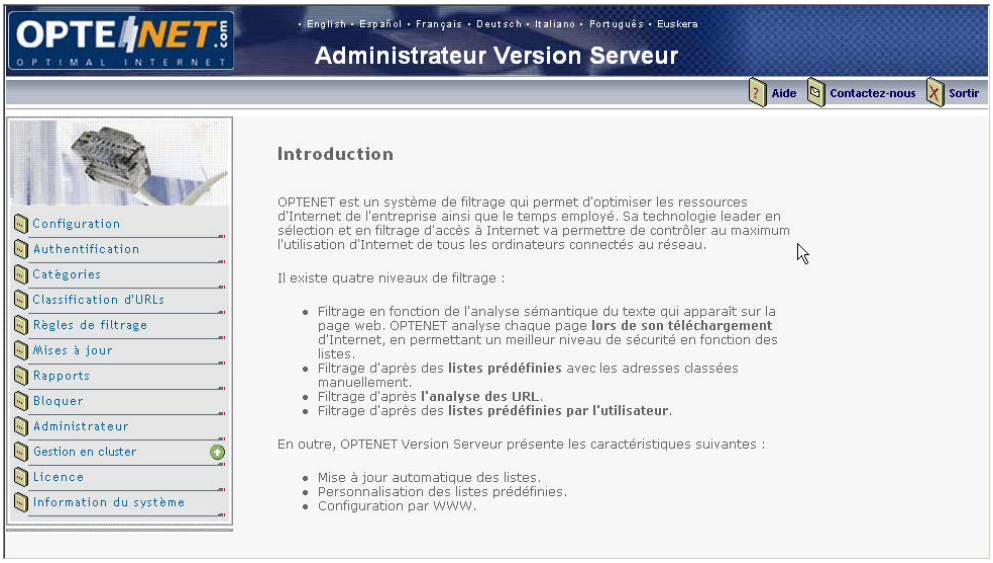
Une fois qu'ont été définies les instances d'OPTENET Server selon les conditions requises dans les paragraphes suivants, chaque changement appliqué à OPTENET Server sera reproduit automatiquement sur toutes les instances.

Si OPTENET Server ne peut se connecter avec une ou plusieurs instances, alors apparaîtra le message d'alerte suivant, avec la liste des instances pour lesquelles le changement n'a pu être appliqué.

*Instance indique une installation d'OPTENET Server en cours d'exécution sur une machine.

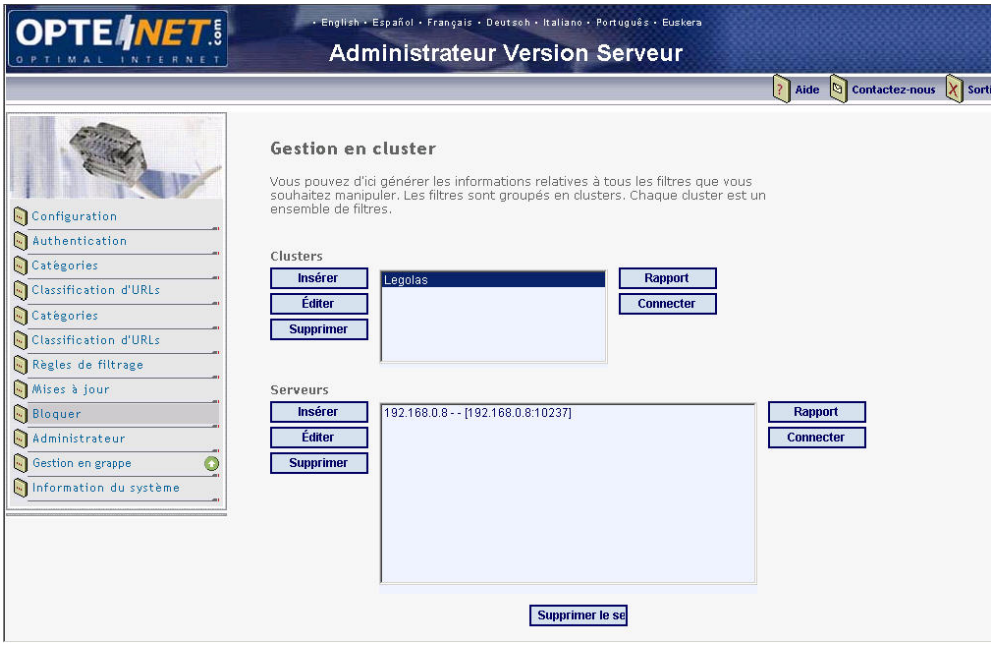
5.12.1. Activer / désactiver la gestion en cluster

L'élément le plus important du travail en cluster est l'icône située en bas à gauche de l'écran et qui sert à activer ou à désactiver la gestion en cluster.

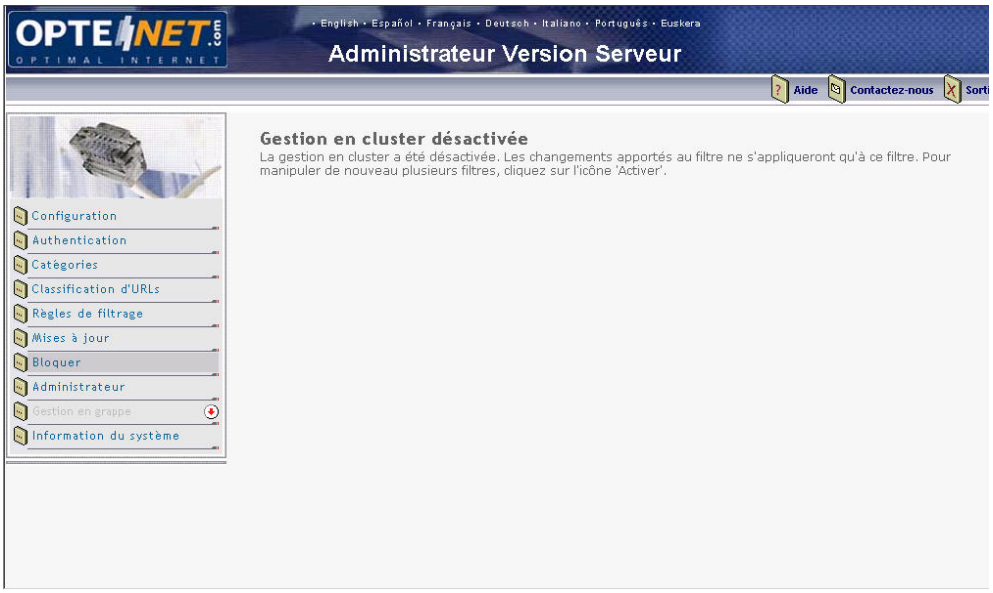


Lorsque cette option est désactivée, le mode de travail est conventionnel, c'est-à-dire qu'une seule instance d'OPTENET Server peut-être utilisée et les changements s'appliquent uniquement à l'installation en cours d'administration. Une fois activée, toutes les modifications apportées à la configuration du filtre sont répercutées à l'ensemble des installations d'OPTENET Server configurées au sein de la gestion en cluster.

Les validations des écrans de paramétrage « Configuration » et « Mises à jours » envoient une alerte pour prévenir que les nouvelles valeurs s'appliqueront à toutes installations OPTENET. (Pour garder des paramétrages différents, vous devrez désactiver provisoirement l'option Cluster).



Lors de l'activation de la gestion en cluster, l'écran permettant d'éditer les installations d'OPTENET Server apparaît. Le bouton « Gestion en cluster » est activé et l'icône qui montre le mode de travail (activé, désactivé) est actualisée.
L'écran suivant s'affiche à la désactivation de la gestion en cluster. Il indique que le mode de travail est traditionnel et que les changements effectués ne s'appliquent qu'à une seule instance d'OPTENET Server. Le bouton « Gestion en cluster » est désactivé et l'icône est de nouveau actualisé.



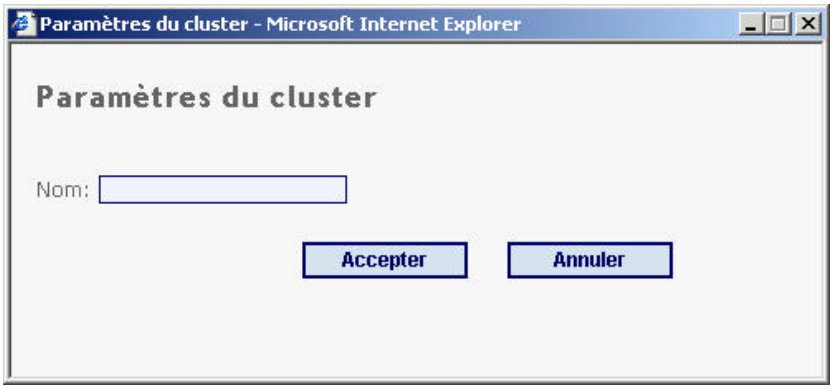
5.12.2. Clusters

Sous cette étiquette se trouvent les boutons permettant de modifier les clusters et une liste actualisée des clusters créés est affiché à tout moment.

Sauf pour « Ajouter », toutes les opérations requièrent la sélection préalable du cluster.

5.12.2.1. Ajouter

Pour ajouter un nouveau cluster, l'écran suivant s'affiche.



Il suffit d'introduire le nom du cluster pour que celui-ci apparaisse dans la liste.

5.12.2.2. Éditer

Permet de modifier le nom d'un cluster. La fenêtre qui s'affiche est identique à la précédente mais le nom du cluster apparaît dans le champ texte.

5.12.2.3. Supprimer

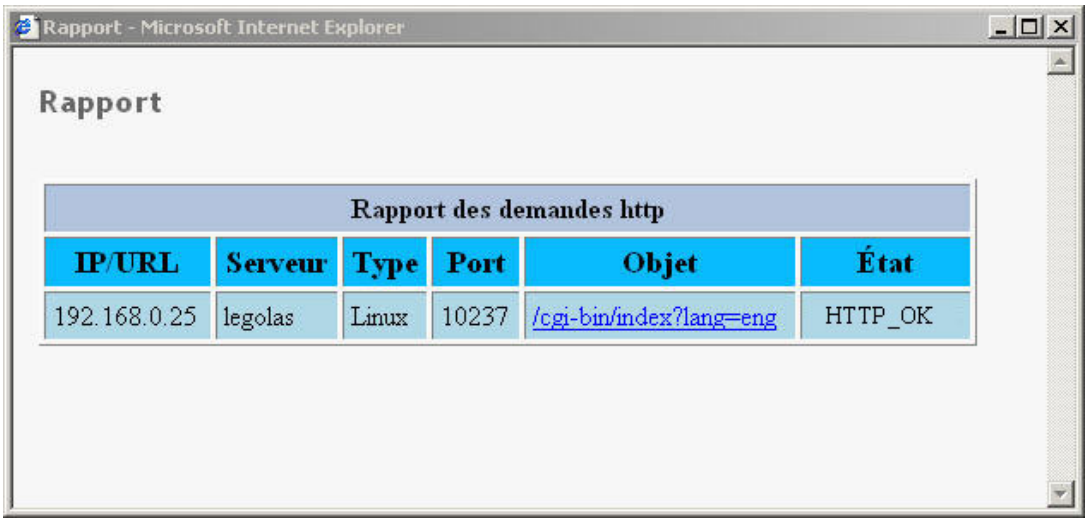
Supprime définitivement le cluster sélectionné de la liste des clusters.

5.12.2.4. Connecter

Établit les connexions avec tous les Servers du cluster sélectionné et affiche la fenêtre de rapport de la section suivante.

5.12.2.5. Rapport

Affiche le résultat des connexions réalisées avec les Servers (voir écran ci-après).



Les champs du tableau sont les suivants :
IP/URL: IP de l'instance d'OPTENET Server.
Server: Nom du Server.
Type: Type d'OPTENET Server.
Port: Port d'écoute de l'instance d'OPTENET Server.
Objet: Demande envoyée à l'instance d'OPTENET Server.
État: « HTTP_OK » (OPTENET Server est en cours d'exécution).
« HTTP_ERROR » (OPTENET Server n'est pas en cours d'exécution ou les paramètres introduits ne sont pas valides).

5.12.3. Servers

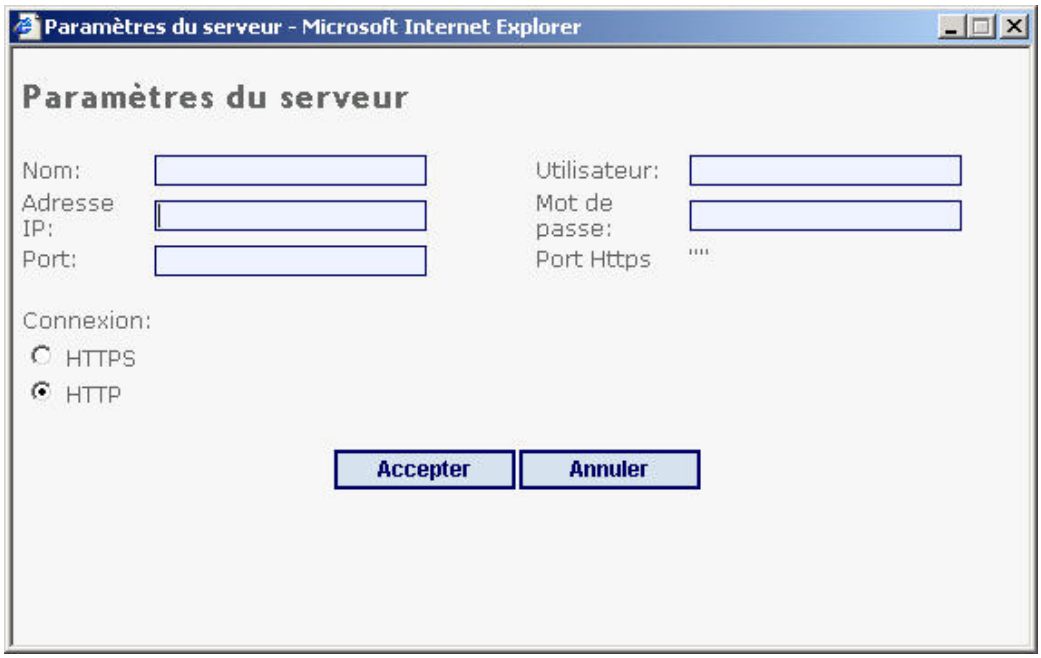
Sous cette étiquette se trouvent les boutons d'édition des Servers.

Une liste actualisée des Servers introduits pour un cluster sélectionné s'affiche en permanence.

Il est important de signaler qu'il n'est pas nécessaire d'ajouter à la liste des Servers l'installation d'OPTENET Server dont l'administration web est celle à laquelle vous êtes connecté. En effet, les modifications qui y sont apportées sont toujours appliquées, quel que soit le mode de travail.

Toutes les opérations requièrent la sélection préalable du cluster. En effet, le Server à modifier appartient à ce cluster et en le sélectionnant, vous pouvez visualiser tous les Servers qui lui sont rattachés.

Pour chaque Server, la zone de texte indiquera les informations suivantes :
IP – Nom – IP:Port – Type



5.12.3.1. Ajouter

Pour ajouter un nouveau Server, la fenêtre ci-après s'affiche.

Les paramètres pour créer une nouvelle entrée d'installation d'OPTENET Server que vous souhaitez contrôler sont les suivants:
Adr IP : Adresse IP.
Nom : Nom de l'instance.
Port : Port d'écoute.
Utilisateur : Nom d'utilisateur pour l'identification.
Mot de passe : Mot de passe de l'utilisateur.
Connexion : Type de connexion pour l'utilisation des autres installations : « http » (par défaut) ou « https » (connexion sécurisée).

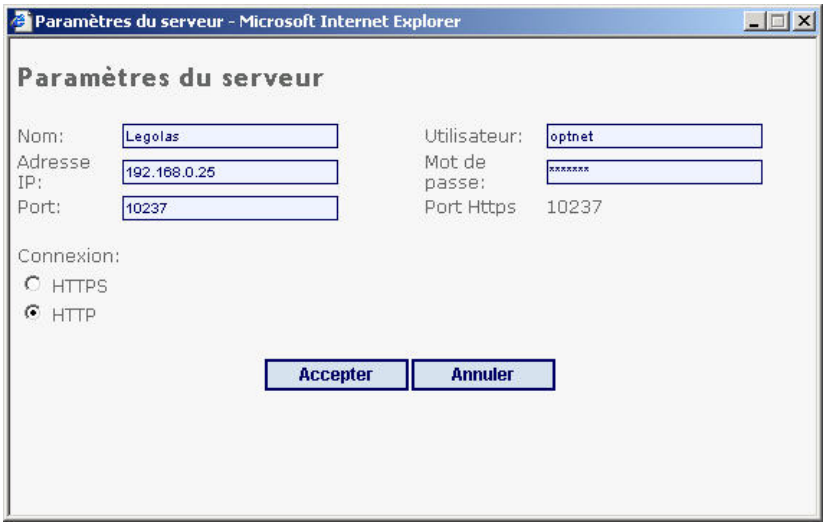
Pour travailler avec des connexions sécurisées https, veuillez consulter l'annexe 1 « Administration d'OPTENET Server via une connexion sécurisée », car dans ce cas le port qu´il faut introduire n´est pas celui où OPTENET Server écoute la machine à distance, mais le port d'écoute de Stunnel associé à OPTENET Server que vous devez introduire.
Ne confondez pas ce Stunnel avec celui associé au filtre local, car ils sont différents. Finalement, dans « Connexion », sélectionnez « https » au lieu de « http ».

Dans la fenêtre figure également une étiquette indiquant « Port http ». Lorsque vous ajoutez un Server, cette étiquette est vide. Nous verrons par la suite quelles valeurs lui attribuer.

Le nom et le mot de passe de l'utilisateur sont identiques à ceux requis pour l'accès à l'administration web d'OPTENET Server.

Il est important de noter que si l´on travaille en cluster, lorsque nous éditons le nom et le mot de passe de l´administrateur introduit lors de la définition du Server, celui se réplique dans les autres installations.

De plus il faut signaler que si nous éliminons le nom et le mot de passe de l´administrateur introduit lors de la définition des Servers, ceux ci cesseront de fonctionner en cluster. Ceci est du au fait que le nom et le mot de passe utilisés pour la gestion en cluster pour répliquer un changement dans une installation concrète n´existe plus dans celle ci. Dans ce cas pour que la gestion en cluster fonctionne de nouveau il faut introduire les paramètres du Server et introduire le nouveau nom et mot de passe.
Une autre manière de procéder consiste à introduire l´utilisateur au lieu de l´effacer et de le créer à nouveau.



5.12.3.2. Modifier

Affiche une fenêtre identique à celle de l'opération précédente, mais les champs sont ici remplis avec les paramètres du Server.

Si vous travaillez en http, notez que la valeur de l'étiquette « Port https » est identique à celle introduite dans le champ « Port », car il n'y a pas de port associé aux connexions https.

Toutefois, si vous travaillez avec des connexions sécurisées, vous verrez qu'un port a été attribué. OPTENET Server a cherché un port libre dans le système et a lancé une instance de Stunnel sur la machine locale afin d'obtenir une communication sécurisée.

Pour chaque nouveau Server créé, OPTENET Server lancera une instance de Stunnel sur votre machine locale.

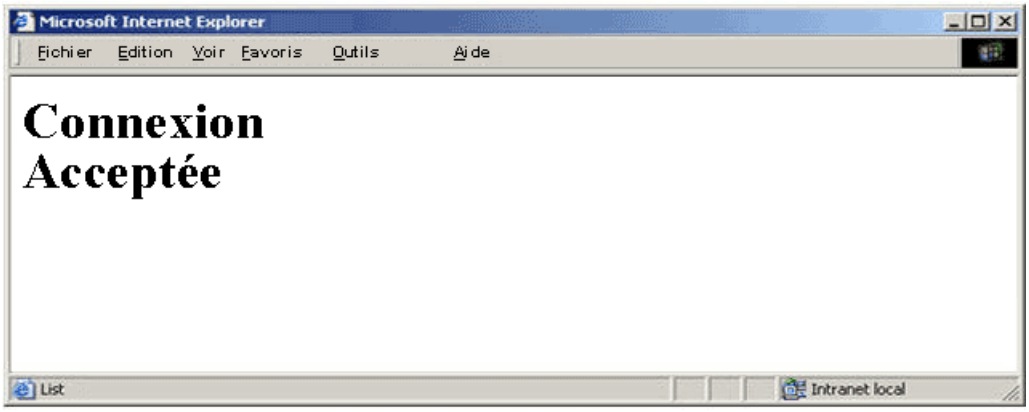
5.12.3.3. Effacer

Supprime définitivement le Server sélectionné de la liste des Servers.

Si vous travaillez avec des connexions sécurisées, la suppression d'un Server entraîne la suppression de l'instance de Stunnel associée au Server en question et située sur la machine locale.

5.12.3.4. Connecter

Établit une connexion avec le Server sélectionné et affiche la fenêtre suivante:



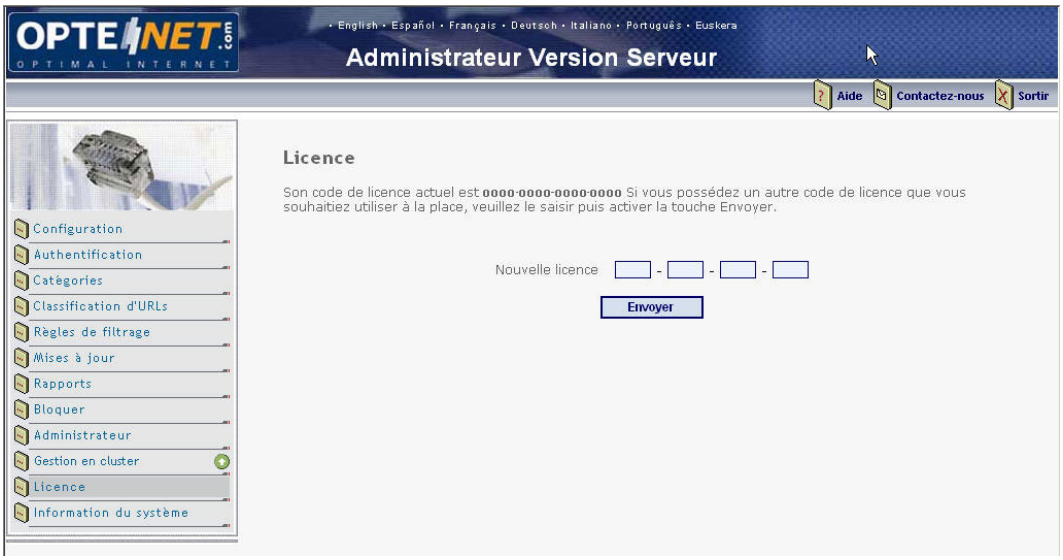
Le résultat de la connexion peut être :
« Connexion acceptée » : OPTENET Server est en cours d'exécution.
« Erreur : Impossible d'effectuer la connexion » : OPTENET Server n'est pas en cours d'exécution ou les paramètres introduits (utilisateur, mot de passe, adresse IP) ne sont pas valides.

5.12.3.5. Rapport

Affiche la fenêtre suivante avec le résultat de la connexion réalisée au Server.
Les champs du tableau sont identiques à ceux du tableau du rapport de la gestion en cluster.

5.13. Licence

Si vous possédez un code de licence qui n'a pu être enregistré au cours de l'installation, vous pouvez l'enregistrer à tout moment à partir de l'administration Web (option Licence).



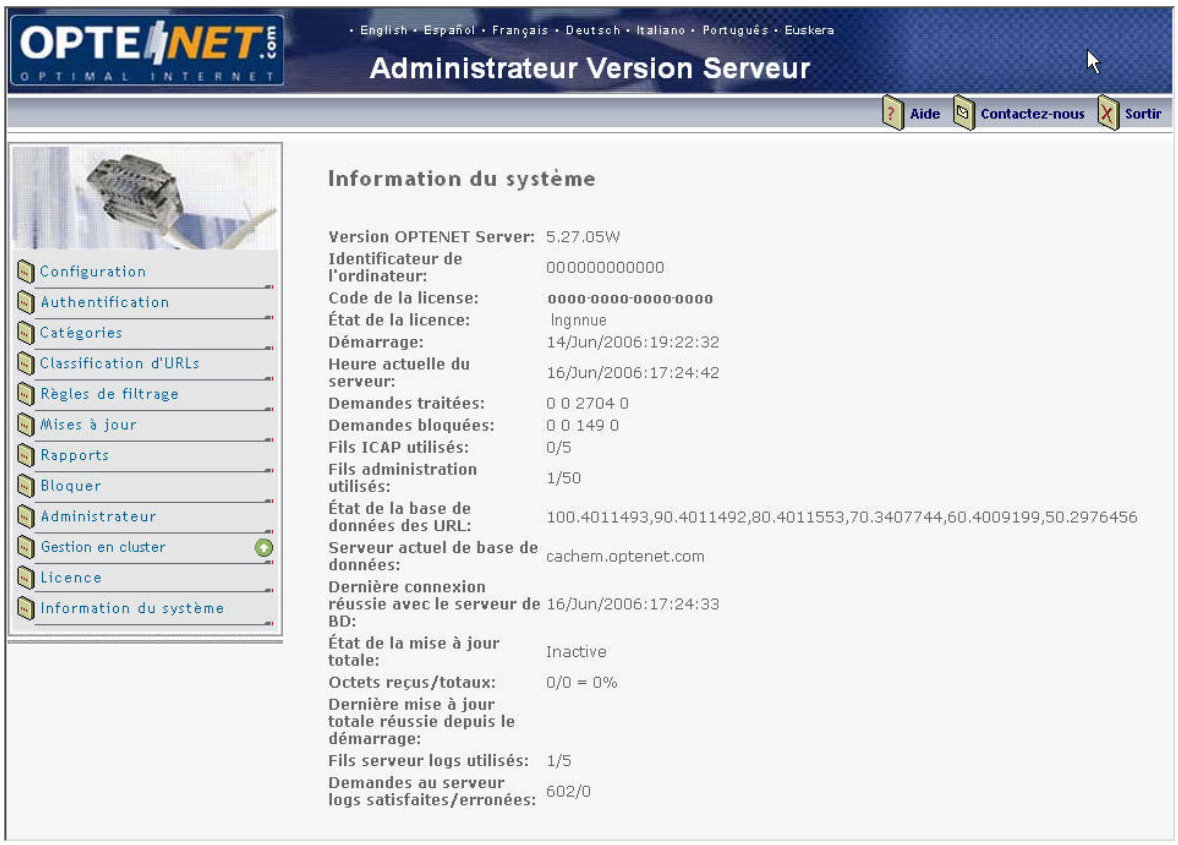
Si la licence actuellement utilisée est arrivée à expiration, vous devrez, en plus d'enregistrer une licence valide, relancer le filtre afin que le programme puisse fonctionner correctement. Si vous utilisez une licence valide et souhaitez simplement en changer, il vous suffira alors de saisir la nouvelle licence sans être obligé de relancer le filtre.

5.14. Informations système

Dans cette option, l'état présent du filtre s'affiche. Vous trouverez ci-dessous des explications relatives aux différentes sections affichant des informations:

- **Version :** Indique la version installée d'OPTENET Server.
- **Identificateur d'ordinateur :** c'est le code identifié par l'ordinateur par rapport aux programmes OPTENET.
- **Code de licence :**c'est le code de licence utilisé par le programme.
- **Etat de la licence :**indique l'état de la licence. Dans le cas où la licence . aurait expiré, veuillez contacter support@optenet.com pour la mettre à jour.
- **Démarrage :** Indique la date et l'heure du dernier démarrage du filtre.
- **Heure actuelle du Server :** indique la date et l'heure locale du Server où est exécuté le filtre.
- **Demandes traitées :** indique le nombre total de demandes analysées par OPTENET depuis son dernier démarrage. 4 nombres apparaissent, le premier indique les demandes ICAP REQMOD reçues pour chaque vérification dans les listes, le second indique les demandes ICAP RESPMOD reçues pour l'analyse de contenu, le troisième indique les demandes reçues via RPC (SQUID, ISA Server, OPTENET Proxy,…) et le quatrième indique les demandes ICAP REQMOD CATEGORY reçues.
- **Demandes bloquées :** indique le nombre total de demandes bloquées par OPTENET depuis son dernier démarrage.
- **Fils ICAP utilisés :** Le premier nombre indique le nombre de threads du Server ICAP exécuté et le deuxième nombre indique le nombre total de threads. Ceci comprend tout les services ICAP (reqmod, respmod et reqmod.
- **Fils administration utilisés** : le premier nombre indique le nombre de threads du Server web utilisé et le deuxième nombre, le nombre total de threads disponibles.
- **Etat de la base de données des URL :** affiche des compteurs internes de l'état de la Base de données du filtre. Utiles si vous avez besoin de recevoir une assistance technique de la part d'OPTENET.

- **Server actuel de base de données :** indique le Server d'OPTENET à partir duquel la base de données des URL est mise à jour.
- **Dernière connexion correcte au Server de BD :** Indique la date et l'heure de la dernière fois où la mise en contact avec le Server de mises à jour de la Base de données des URL a réussi.
- **Etat de la mise à jour totale :** indique l'état actuel du dernier chargement total de la Base de données des URL réalisé lors du dernier démarrage du filtre. Suivant la connexion Internet, cela peut prendre quelques secondes à quelques minutes.
- **Bytes reçus/totaux :** Indique les bytes reçus lors du dernier chargement total par rapport au nombre total de bytes à recevoir. Indique également le pourcentage chargé jusqu'à présent.
- **Dernière mise à jour totale correcte depuis le démarrage :** Indique la date et l'heure du dernier chargement total réussi de la Base de données des URL.
- **Fils Server logs utilisés:** Le premier nombre indique le nombre de threads utilisés par un OPTENET Reporter, et le deuxième, le nombre total disponible.
- **Demandes au Server logs satisfaites/erronées:** Le premier numéro indique le nombre total de demandes au Server de logs réalisées avec succès, et le deuxième le nombre total de demandes échouées.



6. PROBLÈMES COURANTS

Ce paragraphe décrit les problèmes les plus courants et propose des solutions de dépannage.

6.1. Le message OPTENET server error… apparaît lorsque j'essaie de naviguer

Lorsque l'écran ci-dessus s'affiche quand vous essayez de naviguer en utilisant le filtre, le problème provient de l'expiration de votre licence OPTENET Server. Contactez-nous par courrier électronique ou par téléphone:

support@optenet.com
+34 902 154 604 (Espagne)
+34 913579150
+33 (0) 1 73 03 90 60 (France)
+44 (0) 870 099 0322 (Royaume-Uni)
+1 305 249 7505 (Etats-Unis)

pour renouveler ou obtenir votre licence.

6.2. Impossible de démarrer le filtre

Si au démarrage du filtre celui-ci ne parvient à se mettre en fonctionnement, vous pouvez en trouver la raison dans le syslog du système. Connectez-vous comme utilisateur racine et consultez les dernières lignes du fichier /var/log/messages en Linux, /var/adm/messages en Solaris ou AIX, ou dans la fenêtre des évènements d´application en système Windows.
OPTENET Server enregistre un événement d'information à chaque démarrage du filtre ou indique le problème détecté lorsqu'il est impossible de démarrer le filtre.

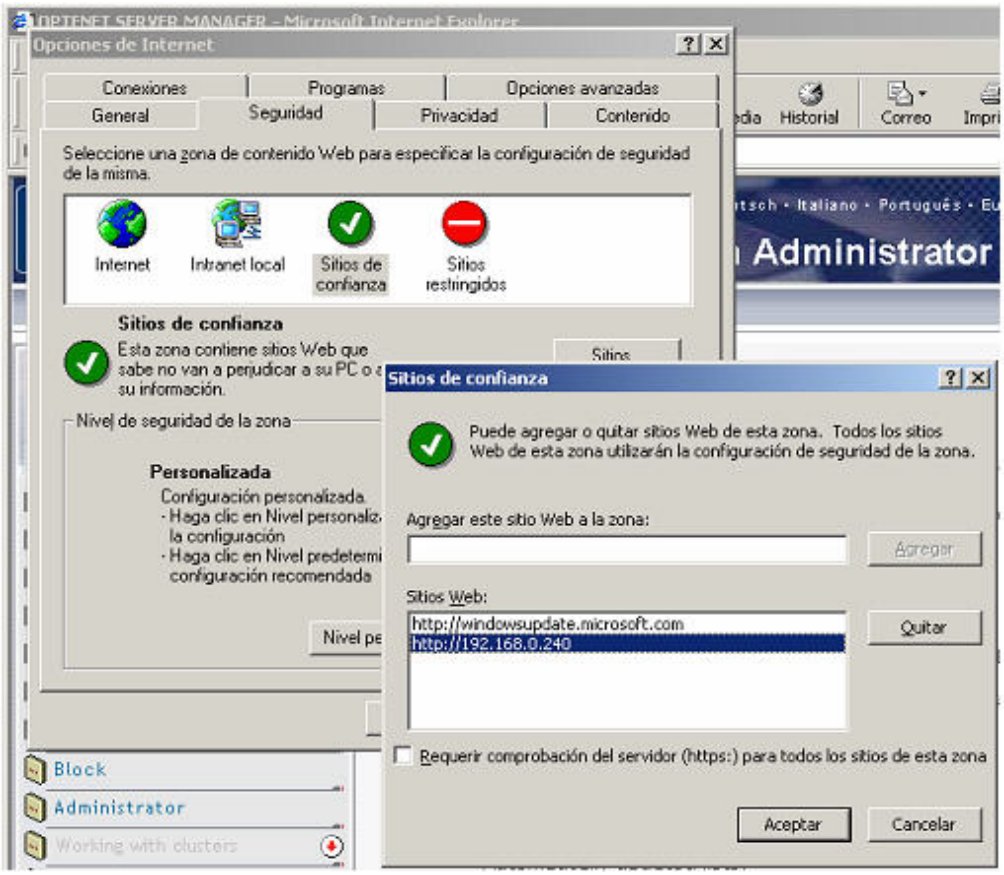
6.3. Les utilisateurs n'apparaissent pas en cliquant sur le bouton « Actualiser »

Pour que les utilisateurs apparaissent en cliquant sur le bouton « Actualiser », vous devez préalablement définir les Servers LDAP ou les domaines Windows d'où vont être extraits les utilisateurs en question. Assurez-vous d'avoir bien défini ces Servers et qu'ils sont bien accessibles depuis la machine sur laquelle est installé OPTENET Server. Consultez le syslog du système (fichier /var/log/messages pour Linux ou /var/log/messages pour

Solaris ou AIX, ou dans la fenêtre des évènements d´application en système Windows.) pour savoir pourquoi OPTENET n'a pas pu lister ces utilisateurs.

6.4. Je ne peux pas entrer dans le système d'administration du filtre

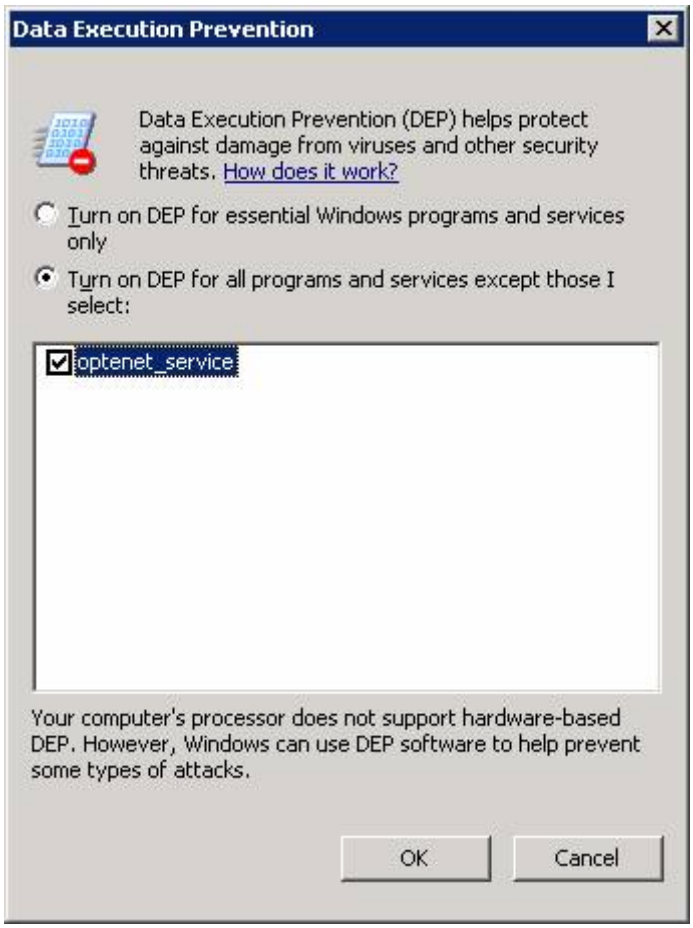
Il a été établi que lorsque Internet Explorer 6.0 est paramétré pour atteindre un niveau de sécurité élevé, il est possible qu'en saisissant l'utilisateur et la clé, votre navigateur affiche une page blanche. Pour pouvoir accéder correctement à l'administration, vous devrez ajouter à la liste des sites de confiance de votre ordinateur l'URL où est installé OPTENET.Par exemple, si OPTENET est installé sur http://192.168.0.240 et utilise Internet Explorer 6.0, vous devrez accéder au menu Outils -> Options Internet -> Sécurité -> Sites de confiance et ajouter l'URL http://192.168.0.240



6.5. DEP ferme OPTENET Server dans W2003 SP1

Windows2003 SP1 distribue l'outil DEP. Il est possible dans parfois, le DEP arrête OPTENET Server en affichant le message suivant.

Pour résoudre ce problème, cliquez sur « Poste de travail » avec le bouton droit et sélectionnez « Propriétés ». Ensuite, cliquez sur « Avancé » et dans le groupe « Performances », cliquez sur le bouton « Paramètres ». Enfin, sélectionnez l'onglet « Prévention de l'exécution des données » et l'écran suivant s'affichera :



Cliquez sur deuxième option « Activer lza prévention d’exécution des données pour tous programmes et les services, sauf ceux que je sélectionne : ». Enfin, sélectionnez OPTENET_service dans la liste des services et des programmes puis cliquez sur « Appliquer ».

ANNEXES

1. ADMINISTRATION D'OPTENET SERVER VIA UNE CONNEXION SÉCURISÉE (SEULEMENT PLATEFORME LINUX).

Il est possible d'administrer le filtre OPTENET via une connexion sécurisée au moyen du protocole HTTPS en accédant à l'URL suivante : https://host.domain à partir de tout navigateur. Pour cela, il est nécessaire que le programme Stunnel soit exécuté sur la machine où est installé le filtre. Si vous souhaitez accéder de manière sécurisée à la configuration web à partir du navigateur Internet Explorer, vous devez disposer de la version 3.22-1 ou ultérieure de Stunnel. Si Stunnel n'est pas installé ou si vous disposez d'une version antérieure, les étapes pour son installation sont les suivantes:

- Télécharger le progiciel stunnel-3.22-1.i386.rpm via FTP à l'adresse updates.redhat.com:/ 7.2/en/os/i386 en vous connectant, par exemple, comme utilisateur anonyme depuis la machine sur laquelle vous souhaitez installer Stunnel.

- Installez le progiciel. Dans le répertoire d'installation du fichier stunnel-3.22-1.i386.rpm, exécutez les commandes suivantes:

  rpm -i stunnel-3.22-1.i386.rpm (Stunnel non installé)
  rpm -U stunnel-3.22-1.i386.rpm (Version de Stunnel antérieure à la version 3.22-1)

- Vérifiez que l'installation s'est déroulée correctement:

  rpm -qa | grep stunnel
  Vous devez voir:
  stunnel-3.22-1

- Générez le fichier des certificats. Dans le répertoire /usr/share/ssl/certs, exécutez en tant qu'utilisateur racine:

  make stunnel.pem

  en introduisant les données demandées.

- Éditez le script stunnelinit situé dans le répertoire d'installation du filtre. Assurez-vous que le chemin d'accès des fichiers est correct en tenant compte du répertoire d'installation du filtre, et que le paramètre –r de Stunnel a pour valeur le port d'écoute du filtre (10237). Ce script établit aussi le port de connexion avec d'autres machines (par défaut, le port 443). Vous pourrez ainsi accéder à l'administration web du filtre en tapant dans votre navigateur l'adresse « https://host_ip ». Si vous décidez de choisir un port autre que le port 443, accédez à l'administration web du filtre à partir de votre navigateur en tapant « https://host_ip:Port ». Il est également important de signaler qu'en cas d'utilisation d'un port inférieur au port 1024, vous devrez exécuter Stunnel en tant qu'utilisateur racine.

- Pour démarrer Stunnel, exécutez le script stunnelinit dans le répertoire d'installation en tant qu'utilisateur racine:

  ./stunnelinit start

- Pour arrêter son exécution, exécutez le script stunnelinit dans le répertoire d’installation en tant qu’utilisateur racine:

```
./stunnelinit stop
```

À la réinitialisation du filtre, redémarrez Stunnel. Toutefois, veillez à le redémarrer après le démarrage du filtre, sinon ce dernier supprimerait toutes les instances de Stunnel en cours d’exécution sur la machine locale.

Si vous travailler en cluster utilisant plusieurs OPTENET Servers à la fois, il ne faut pas s´inquiéter de quoi que ce soit, car OPTENET Server se charge de que toutes les connexions soient sécurisées.

2. ADMINISTRATION D'OPTENET SERVER VIA LA LIGNE DE COMMANDES (OPTENET CLI V1.0)

2.1 Introduction

OPTENET CLI est une application qui permet d'administrer OPTENET Server par l'intermédiaire d'une ligne de commandes. OPTENET CLI est une alternative à l'administration web et présente l'avantage de pouvoir traiter des fichiers de script contenant plusieurs demandes. Cette application est aussi caractérisée par le fait qu'elle permet d'administrer n'importe quel filtre, en éditant simplement son fichier de configuration.

OPTENET CLI contrôle exhaustivement tout ce que vous saisissez dans la ligne de commande afin de minimiser le risque d'erreurs. L'interface des commandes d'OPTENET CLI est en anglais, mais le manuel de l'utilisateur est disponible en plusieurs langues.

OPTENET CLI peut être exécutée sur la machine sur laquelle est installé OPTENET Server ou sur tout autre. Notez que si OPTENET CLI administre un filtre à distance, son fonctionnement peut être perturbé s'il faut passer par un proxy.

Si vous gérer avec OPTENET CLI un OPTENET Server qui est maître dans la gestion en cluster, vous devez tenir compte du fait que les changements appliqués par CLI dans l´OPTENET Server maître vont influencer tous les OPTENET Server esclaves.

Les fichiers qui vont être utilisés par OPTENET CLI (fichier de configuration et fichiers de script) doivent se trouver dans le répertoire d'exécution d'OPTENET CLI. Il est donc nécessaire de copier ces deux types de fichiers dans son répertoire d'exécution si OPTENET CLI est exécutée à distance.

OPTENET CLI s´installe à côté d'OPTENET Server dans le sous répertoire outils avec son fichier de configuration cli.conf et le fichier de scripts par défaut script.txt où vous pouvez ajouter de multiples demandes. Ce fichier de script est vide.

2.2 Utilisation

Le présent chapitre explique comment utiliser OPTENET CLI et profiter au mieux des caractéristiques offertes.

2.2.1 Execution

Pour exécuter OPTENET CLI, allez à son répertoire d'installation et tapez:

```
optenetcli
```

Le message de bienvenue d'OPTENET CLI s'affiche.

À ce stade, vous vous trouvez dans la ligne de commandes d'OPTENET CLI et les commandes tapées seront interprétées et exécutées.

2.2.2 Aide

OPTENET CLI dispose d'un système d'aide complet en mode texte. Pour l'afficher, tapez:

?

Ce système d'aide affiche les noms de toutes les commandes d'OPTENET CLI. Notez qu'il ne s'agit que des noms des commandes. La plupart d'entre elles sont paramétrables et vous devrez en spécifier les paramètres par la suite.

2.2.3 Commandes

Pour connaître les paramètres d'une commande, il suffit de taper le nom de la commande suivie de « ? ».

Exemple :

saveconfig ?

Toutes les commandes d'OPTENET CLI suivent l'un des formats suivants:

- addxxxxxx
- savexxxxxx
- delxxxxxx
- sortxxxxxx

Où xxxxxx représente une chaîne de caractères.
Exemple : saveconfig, delurlyes, sortrule, etc.

Prenez garde aux caractères en majuscules et en minuscules, car OPTENET CLI est sensible à la casse. En d'autres termes, « saveconfig » est différent de « SaveConfig ».

Pour faciliter l'utilisation d'OPTENET CLI, toutes les commandes sont en minuscules. Toutefois, comme vous pourrez le constater par la suite, certains paramètres ont des caractères en majuscules.

La liste des commandes disponibles s'affiche en tapant l'une des commandes suivantes:

- ?
- Une commande non interprétée par OPTENET CLI.
- Une commande valide, mais avec un numéro de paramètre non valide.

Lorsque vous tapez une commande avec des numéros de paramètres valides, mais que certains d'entre eux sont néanmoins incorrects, OPTENET CLI vous indique comment utiliser ladite commande.
Un processus logique pour l'exécution d'une commande pourrait ainsi être le suivant :

- Tapez « ? » pour voir les commandes disponibles.
- Tapez le nom de la commande choisie dans la liste, suivi du point d'interrogation.
- Tapez le nom de la commande suivi de ses paramètres tel qu'indiqué par OPTENET CLI.

Quand la commande tapée est valide et qu'elle a été exécutée avec succès, OPTENET CLI affiche le message suivant :

Configuration added successfully

Quand la commande tapée est valide mais qu'elle n'a pas pu être exécutée, OPTENET CLI affiche le message suivant :

Error: Configuration couldn´t be added

Quand la commande saisie n'existe pas, la liste des commandes disponibles s'affiche. Au contraire, quand la commande existe mais que les numéros de paramètres ne sont pas valides, OPTENET CLI vous indique comment utiliser la commande en question.

Quand la commande et les numéros des paramètres sont valides, mais que l'un des paramètres ne l'est pas, OPTENET CLI vous indique comment utiliser la commande et affiche aussi le message suivant :

Error: Parameter XX is not correct

Où XX désigne le numéro du paramètre.

Pour certains paramètres précis, un message différent du précédent s'affiche. Par exemple, quand l'un des paramètres est un jour de la semaine et que vous tapez « quatorze », OPTENET CLI affiche le message suivant:

Error: quatorze is not a week day

Une liste de toutes les commandes valides figure au chapitre 4 du présent document. Vous pouvez utiliser ce chapitre comme un guide de consultation rapide.

2.2.4 Fichier de script

Pour qu'OPTENET CLI exécute toutes les commandes d'un fichier de script, tapez simplement le nom du fichier de script avec l'extension txt.

Exemple : script.txt

OPTENET CLI vous indique le résultat de l'exécution des demandes de la manière suivante. Si la demande a été exécutée avec succès:

Line XXX added successfully.

Où XXX fait référence au numéro de ligne du fichier.

Au contraire, si une demande n'est pas valide, l'application vous indique comment la construire de façon appropriée.

Exemple :

USAGE: savekey PASSWORD
PASSWORD: Password for protecting sensitive information

Notez bien que le format des demandes d'un fichier de script est exactement le même à celui que vous auriez tapé.

Le format d'un fichier de script consiste à avoir une seule demande par ligne. Ainsi, il est possible d'obtenir un fichier de script clair et facilement éditable. Pour cette raison, quand vous saisissez deux demandes sur une même ligne, OPTENET CLI indique que celle-ci est erronée et aucune des demandes ne peut être traitée.

2.2.5 Quitter

Pour quitter OPTENET CLI, tapez la commande suivant:

exit

Cette dernière met fin à l'exécution d'OPTENET CLI.

2.2.6 Fichier de configuration

Le fichier de configuration d'OPTENET CLI est « cli.conf » et doit se situer dans le même répertoire que celui de l'exécutable. Vous pouvez modifier ce fichier avec n'importe quel éditeur. Son format est le suivant:

UserName
Password
Server IP
Server Port

Comme vous pouvez le voir, le fichier ne comporte que 4 lignes, qui vous permettent de sélectionner n'importe quel OPTENET Server en cours d'exécution pour pouvoir l'administrer.

Les deux premières lignes se réfèrent au nom de l'utilisateur et à son mot de passe, nécessaire à l'administration d'OPTENET Server. Ce mot de passe est aussi celui qui vous permet de l'administrer, par exemple, via Internet. Les valeurs par défaut pour le nom d´utilisateur et le mot de passe sont respectivement ¨optenet¨ et ¨12345678¨.

Les deux lignes suivantes contiennent les informations nécessaires à OPTENET CLI pour savoir où se connecter : l'adresse IP de la machine où OPTENET Server est en cours d'exécution et son port d'écoute. Les valeurs par défaut pour la machine locale (¨127.0.0.1¨) et le port par défaut de l´administration web est (¨10237¨).

Il convient de signaler que ce fichier doit toujours contenir 4 lignes et qu'il doit s'agir de celles mentionnées ci-dessus. S'il manque des lignes, qu'il y en a de trop ou que vous essayez d'introduire plusieurs champs dans une même ligne, OPTENET CLI retourne un message d'erreur au chargement du fichier de configuration.

2.3 Référence des commandes

Dans ce chapitre figure une liste complète des commandes et de leurs paramètres respectifs, que l'utilisateur peut utiliser comme un guide rapide de consultation. Les commandes sont réparties en différentes sections, tout comme les boutons dans l'administration web.

2.3.1 Configuration

Cette option permet de configurer l'état du filtre, de spécifier la page de blocage ou de spécifier le répertoire de création des fichiers journaux.

2.3.1.1 Saveconfig

Toutes les caractéristiques mentionnées ci-dessus sont configurées à l'aide d'une seule commande.

saveconfig FILTER_STATE URL_BLOCK LOGS_DIR FLAG1 BLOCKING_LOGS FLAG2 QUERY_LOGS CRYPT STATUS
FILTER_STATE: "Active", "Inactive"
URL_BLOCK: Url indicating the blocking page
LOGS_DIR: Directory for logs output (local path)
FLAG1: "0", "1" (Disable/Enable Blocking_Logs)
BLOCKING_LOGS: IP USER DAY RULE CATEGORY FILETYPE URL
Each Value is:"0","1" Example: 0100110
FLAG2: "0", "1" (Disable/Enable Query_Logs)
QUERY_LOGS: IP CLIENT USER GROUP DAY URL TRAFFIC TIME ACCESSES RULE CATEGORY FILETYPE
Each Value is:"0","1" Example: 010011010011
CRYPT STATUS.¨0¨.¨1¨ (isable/Enable encryption of personal information in log files)

Voici le format qu'OPTENET CLI utilise pour vous montrer comment utiliser une commande. « saveconfig » est le nom de la commande et « FILTER_STATE », « URL_BLOCK » et « LOGS_DIR » quelques-uns des paramètres de cette commande.

Si un paramètre ne peut prendre que certaines valeurs concrètes, ces valeurs sont affichées entre guillemets après le nom du paramètre. Par exemple, dans le cas de « saveconfig », FILTER_STATE peut prendre uniquement les valeurs « Active » ou « Inactive ».

Remarquez que « Active » et « Inactive » commencent par une majuscule, mais que les autres caractères sont en minuscules.

2.3.2 Authentification

Vous pouvez ici configurer OPTENET afin qu'il procède à l'authentification des utilisateurs.

2.3.2.1 Saveauthen

saveauthen AUTENTICATION SERVER TIME PORT
AUTENTICATION: "1" (Active), "0" (Inactive)
SERVER: Server Ip or name
TIME: Expiration time
PORT: Server port

2.3.3 Authentification LDAP

Dans cette section, vous allez pouvoir définir de nouveaux Servers LDAP et modifier ou supprimer les Servers existants.

Lors de l'authentification des utilisateurs, l'ordre suivi est celui dans lequel ont été définis les Servers.

2.3.3.1 Delauthencach

delauthencache

Cette commande n'est pas paramétrable.

2.3.3.2 Sortldap

sortldap SORT LDAP_SERVER
SORT: "Up", "Down"
LDAP_SERVER: LDAP Server name

2.3.3.3 Delldap

delldap LDAP_SERVER
LDAP_SERVER: LDAP Server name

2.3.3.4 Saveldap

saveldap SERVER PORT BASE TYPE ADMIN PASSWORD LDAP_SERVER (OLD_LDAP_SERVER)
SERVER: Server Ip or name
PORT: Server port
BASE_TYPE: Base to search for users and groups
TYPE: "0"(Windows 2000) "1" (Lotus Domino) "2"(iPlanet)
ADMIN: Username to log on to server
Type if not administrator
PASSWORD: Password for username
Type if not administrator
LDAP_SERVER: Server name
OLD_LDAP_SERVER: Old server name or ip
Use OLD_LDAP_SERVER when modifying server, not when creating

Le dernier paramètre est entre parenthèses car il s'agit d'un paramètre facultatif. En d'autres termes, cette commande peut être utilisée pour réaliser deux demandes distinctes. Quand le dernier paramètre n'est pas spécifié, vous créez un nouveau Server LDAP ; mais quand il l'est, vous modifiez un Server LDAP existant et le nommez à l'aide de ce dernier paramètre.

2.3.4 Classement des URL

Cette option vous permet d'ajouter des URL aux différentes catégories en indiquant si cette URL appartient ou non à une catégorie.

2.3.4.1 Saveurlclas

saveurlclas URL CATEGORIES
URL: Url to be categorized
CATEGORY: An Optenet Server category
YES_NOT: "Yes" "Not"

2.3.4.2 Adduserurl

adduserurl CATEGORY LIST URL
CATEGORY: One of OPTENET Server categories
LIST: "Yes", "Not"
URL: The Url

2.3.4.3 Deluserurl

deluserurl CATEGORY LIST URL
CATEGORY: One of OPTENET Server categories
LIST: "Yes", "Not"
URL: The Url

2.3.5 Règles de filtrage

Les règles de filtrage vous permettent de personnaliser facilement OPTENET Server pour l'adapter aux besoins de votre réseau.
Cette option vous permet de définir ces règles et l'ensemble de leurs critères : Groupes d'adresses IP, Utilisateurs, Groupes d'utilisateurs, Catégories, URL, Fichiers et Horaires.

2.3.5.1 Addrule

addrule

2.3.5.2 Sortrules

sortrules SORT RULE_NAME
SORT: "Up", "Down"
RULE_NAME: Name of the rule to be sorted

2.3.5.3 Delrule

delrule RULE_NAME
RULE_NAME: Name of the rule to be deleted

2.3.5.4 Renrule

renrule OLD_RULE_NAME NEW_RULE_NAME
OLD_RULE_NAME: Old name of the rule
NEW_RULE_NAME: New name of the rule

2.3.5.5 Addips

addips RULE_NAME FROM_IP TO_IP
RULE_NAME: Name of the rule
FROM_IP: First ip of ip range
TO_IP: Last ip of ip range

2.3.5.6 Delips

delips RULE_NAME FROM_IP TO_IP
RULE_NAME: Name of the rule
FROM_IP: First ip of ip range
TO_IP: Last ip of ip range

2.3.5.7 Savecat

savecat RULE_NAME CAT1 CAT2 ... CATN
RULE_NAME: Name of the rule
CAT1,...CATN: An Optenet Server category
Categories not typed will be disabled

Cette commande n'a pas un nombre fixe de paramètres, car il est possible d'ajouter autant de catégories que vous le souhaitez. Les catégories dont le nom n'est pas indiqué

comme paramètres sont désactivées, tandis que celles qui sont indiquées comme paramètres sont activées.

2.3.5.8 Addurlyes

addurlyes RULE_NAME URL_YES
RULE_NAME: Name of the rule
URL_YES: The url to be added

2.3.5.9 Delurlyes

delurlyes RULE_NAME URL_YES
RULE_NAME: Name of the rule
URL_YES: The url to be deleted

2.3.5.10 Adduser

adduser RULE_NAME USER
RULE_NAME: Name of the rule
USER: User affected by the rule

2.3.5.11 Deluser

del user RULE_NAME USER
RULE_NAME: Name of the rule
USER: User affected by the rule

2.3.5.12 Addhours

addhours RULE_NAME FIRST_HOUR LAST_HOUR FIRST_MINUTE LAST_MINUTE
RULE_NAME: Name of the rule
HOUR_INTERVAL: Hour range. Type XX:XX-XX:XX. Example: 08:30-19:37
Hours should be in range 0-59
Minutes should be in range 0-23

Tous les paramètres de cette commande (sauf le premier) sont des entiers compris dans un intervalle. Si vous tapez des caractères ou un entier non compris dans l'intervalle, OPTENET CLI retourne une erreur.

2.3.5.13 Delhours

delhours RULE_NAME HOUR_INTERVAL
RULE_NAME: Name of the rule
HOUR_INTERVAL: Hour range (8:30-19:37)

Le deuxième paramètre est un intervalle horaire et il est très important de respecter le format spécifié, c'est-à-dire XX:XX-XX:XX.
Si vous saisissez l'intervalle horaire dans un autre format, OPTENET CLI retourne une erreur.

2.3.5.14 Saveday

saveday RULE_NAME DAY1 DAY2 ... DAY7
RULE_NAME: Name of the rule
DAY: A valid week day*
"Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday"

2.3.5.15 Addurlnot

addurlnot RULE_NAME URL_NOT
RULE_NAME: Name of the rule
URL_NOT: Url affected by the rule

2.3.5.16 Delurlnot

delurlnot RULE_NAME URL_NOT
RULE_NAME: Name of the rule
URL_NOT: Url affected by the rule

2.3.5.17 Savefile

savefile RULE_NAME FILE_TYPE1 FILE_TYPE2 ... FILE_TYPE7
RULE_NAME: Name of the rule
FILE_TYPE: A valid file type (mp3, avi,...)*

2.3.6 Mises à jour

OPTENET Server se connecte périodiquement au site web d'OPTENET pour mettre à jour ses listes et pouvoir filtrer les nouvelles adresses catégorisées d'Internet qui apparaissent chaque jour. Cette option permet de définir la fréquence de mise à jour des listes.

2.3.6.1 Saveact

saveact FRECUENCY DAY_OF_WEEK DAY_OF_MONTH START_HOUR
END_HOUR TRY_INTERVAL PROXY_ADDR PORT PROXY
FRECUENCY: "Daily", "Weekly", "Monthly"
DAY_OF_WEEK:"Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday"
DAY_OF_MONTH: "1", "2", "...", "28"
START_HOUR: "0", "1", "...", "23"
END_HOUR: "1", "2", "...", "24"
TIME_INTERVAL: Time between tries
PROXY_ADDR: Proxy address
PORT: Proxy port
PROXY: "0", "1"

Faites attention aux caractères en majuscules et en minuscules.

2.3.7 Identification Administrateur

Pour garantir la confidentialité de la configuration et de l'administration, le Server web requiert l'authentification de l'utilisateur et, pour cela, lui demande un nom d'utilisateur et un mot de passe. Par défaut, le nom d'utilisateur est **OPTENET** et le mot de passe **12345678**. Ces valeurs peuvent être modifiées à partir de l'administration web au moyen de l'option « Identification Administrateur ».

Vous devez tenir compte du fait que la création / édition d´utilisateurs dépend de certaines conditions. Par défaut les conditions pour réaliser ces opérations sont ceux du profil Administrateur (¨optenet¨ et ¨12345678¨). Pour changer ces conditions il faut éditer les deux premières lignes du fichier cli.conf.

2.3.7.1 Addadmin

addadmin NEW_USER_NAME NEW_PASSWORD ENABLED PROFILE
NEW_USER_NAME: New user name
NEW_PASSWORD: New password for new user name
ENABLED: Profile enabled ("1") or disabled ("0")
PROFILE: "1" (Ordinary administrator)
"2" (Local administrator)
"3" (Urls administrator)
"4" (Reports administrator)
"5" (Sensitive information administrator)

2.3.7.2 Saveadmin

saveadmin OLD_USER_NAME NEW_USER_NAME NEW_PASSWORD ENABLED PROFILE
OLD_USER_NAME: Old user name
NEW_USER_NAME: New user name
NEW_PASSWORD: New password for new user name
ENABLED: Profile enabled ("1") or disabled ("0")
PROFILE: "1" (Ordinary administrator)
"2" (Local administrator)
"3" (Urls administrator)
"4" (Reports administrator)
"5" (Sensitive information administrator)

2.3.7.3 Deladmin

deladmin USER_NAME PROFILE
USER_NAME: Administrator user name
PROFILE: "1" (Ordinary administrator)
"2" (Local administrator)
"3" (Urls administrator)
"4" (Reports administrator)
"5" (Sensitive information administrator)

2.3.8 Gestion en cluster

OPTENET Server permet d'utiliser de multiples instances d'OPTENET Server en cours d'exécution sur plusieurs machines. Vous pouvez créer, éditer, supprimer et vous connecter à autant d'instances d'OPTENET Server que vous le souhaitez.

2.3.8.1 Cluster

cluster FLAG
FLAG: "1" (Enable 'Working with Clusters')
"0" (Disable 'Working with Clusters')

2.3.8.2 Addcluster

addcluster CLUSTER_NAME
CLUSTER_NAME: Name of new cluster

2.3.8.3 Savecluster

savecluster CLUSTER_NAME NEW_NAME
CLUSTER_NAME: Name of cluster
NEW_NAME: New Name for cluster

2.3.8.4 Delcluster

delcluster CLUSTER_NAME
CLUSTER_NAME: Name of cluster

2.3.8.5 Addserver

addserver SERVER_NAME SERVER_IP SERVER_PORT HTTP_FLAG USERNAME PASSWORD CLUSTER_NAME
SERVER_NAME: Name of new server
SERVER_IP: Ip address of new server
SERVER_PORT: Port where server listens
HTTP_FLAG: "1" (Http), "0" (Https)
USERNAME: Username to log on to the server
PASSWORD: Password to log on to the server
CLUSTER_NAME: Server's cluster name

2.3.8.6 Saveserver

saveserver SERVER_NAME SERVER_OLD_NAME SERVER_IP SERVER_PORT HTTP_FLAG USERNAME PASSWORD CLUSTER_NAME
SERVER_NAME: New name for server
SERVER_OLD_NAME: Server old name
SERVER_IP: Ip address of server
SERVER_PORT: Port where the server listens
HTTP_FLAG: "1" (Http), "0" (Https)
USERNAME: Username to log on to the server
PASSWORD: Password to log on to the server
CLUSTER_NAME: Server's cluster name

2.3.8.7 Delserver

delserver SERVER_NAME CLUSTER_NAME
SERVER_NAME: Name of server
CLUSTER_NAME: Server's cluster name

2.3.9 Rapports

OPTENET Server permet de configurer un outil d'élaboration de rapports (OPTENET Reporter) qui recevra les logs.

2.3.9.1 StoreReporter

storereporter REPORTER_IP REPORTER_PORT
REPORTER_IP: Adresse IP où OPTENET Reporter est installé
REPORTER_PORT: Numéro de port où OPTENET Reporter écoute

2.4 PROBLÈMES COURANTS

Ce paragraphe décrit les problèmes les plus courants et propose des solutions de dépannage.

2.4.1 OPTENET CLI n’arrive pas à démarrer

Vérifiez que l’exécutable d’OPTENET CLI (optenetcli) se trouve dans le répertoire actuel. Assurez-vous que le fichier de configuration (cli.conf) s’y trouve également.

2.4.2 Un message d'erreur s'affiche à l'exécution d'une commande

Si vous recevez un message d'erreur pour l'un ou l'autre des paramètres, vérifiez-les un par un. Vérifiez aussi les caractères en majuscules et en minuscules de la commande et des paramètres.

Si l'erreur indique que la configuration n'a pas pu être ajoutée, vérifiez d'abord qu'OPTENET Server est en cours d'exécution. Vérifiez ensuite que les données du fichier de configuration (utilisateur, mot de passe, IP, port) sont correctes.
Finalement, vérifiez que vous ne passez par aucun proxy intermédiaire pour atteindre OPTENET Server.

2.4.3 Vous exécutez une commande mais n'en voyez pas le résultat sur OPTENET Server

À l'exécution d'une commande d'OPTENET CLI, vous ne recevez aucun message d'erreur, mais un message indique que la configuration a été ajoutée. Toutefois, vous vous apercevez que les modifications attendues suite à l'exécution de cette commande ne se sont pas produites. Dans ce cas, le problème est dû au fait qu'un des paramètres fait référence à un élément inexistant.

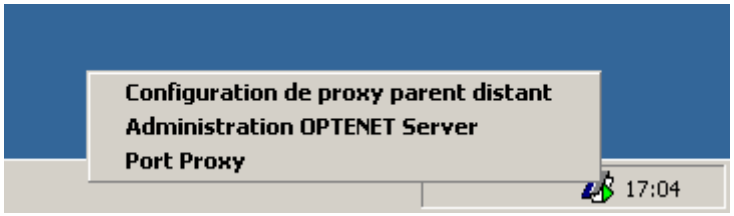
Il peut s'agir d'une règle, d'une catégorie, d'un type de fichier, d'un nom, de l'adresse IP d'un Server, etc.

3. CONFIGURATION DU PROXY OPTENET

Le proxy OPTENET possède certains paramètres configurables comme par exemple le port d´écoute (et dans le cas où il y a un autre proxy) la possibilité d´introduire les données de ce proxy en chaîne.

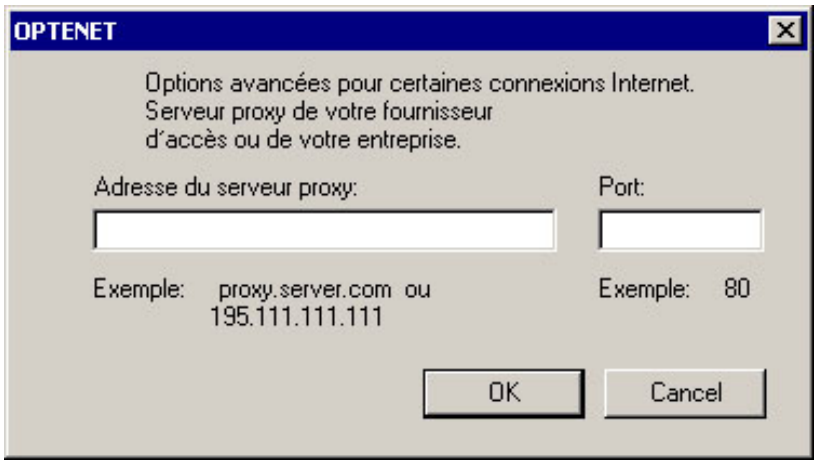
Ces options sont accessibles au travers de l´icône situé sur la barre des actions.

Lorsque vous sélectionner l´icône avec le bouton de droite ou de gauche de la souris apparaîtra le menu suivant où l´on pourra sélectionner l´option désirée.



3.1 Configuration du proxy en chaîne (Configuration proxy)

Si vous désirez configurer un proxy en chaîne au travers de la fenêtre ci dessous il faudra indiquer l IP du proxy et le port d´écoute.

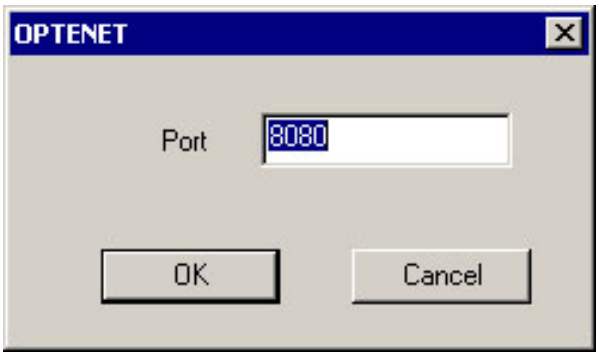


3.2 Administration d'OPTENET Server (Administration Optenet Server)

En sélectionnant cette option une page web s´ouvrira montrant la page d´administration du filtre OPTENET.

3.3 Configuration du port (Port Proxy)

Pour modifier le port que le proxy utilise par défaut il est possible de sélectionner cette option et de le changer facilement.



4. DEFINITION DES CATEGORIES FILTRÉES PAR OPTENET

1. **Administrations Publiques :** Gouvernements, administration locale, administration publique...

2. **Anonymat :** Ce sont les pages Web à travers lesquelles on évite de connaître les adresses Web auxquelles accèdent des tiers.

3. **Anorexie et Boulimie :** Sites qui encouragent l'anorexie et la boulimie.

4. **Arts :** Sites web donnant des renseignements sur les Arts: musées, sculptures, photographie, littérature, etc.

5. **Hasard :** Sites web à partir desquels il est possible d'accéder à des casinos et bingos on-line; sont également compris les sites où toutes sortes de paris, par exemple le loto sportif sont possibles.

6. **Banques et Institutions financières :**

7. **Banners :** Annonces publicitaires insérées dans les pages Web ainsi que les URL des entreprises qui se consacrent à l'élaboration de ce type d'annonces sur le Web.

8. **Blogs :** Pages gratuites où des particuliers publient sur Internet journaux, expériences, commentaires, idées... qu'ils souhaitent partager.

9. **Moteurs de recherche :** Pages Web qui sont utilisées pour effectuer des recherches d'autres adresses Web sur Internet, tels que Google, Yahoo, Altavista, Alltheweb, etc.

10. **Chat :** Sites Web qui fournissent des services pour communiquer (chat) avec d'autres utilisateurs en temps réel.

11. **Code malicieux :** Hardware, software ou firmware qui est introduit intentionnellement dans un système à des fins malicieuses ou de façon non autorisée. Un cheval de Troie est un exemple de code malicieux.

12. **Construction d'explosifs :** Sites web où il est expliqué comment fabriquer des explosifs.

13. **Achats :** Sites web où acheter des produits et utiliser des services variés.

14. **Web mail :** Sites Web qui fournissent des services permettant d'envoyer des messages par courrier électronique.

15. **Sports :** Sites web offrant des contenus relatifs aux équipes et à l'information sportive.

16. **DNS Services :** Catégorie qui regroupe les connexions d'ordinateurs à partir du réseau interne de l'entreprise à des ordinateurs d'utilisateurs sur Internet via http à un port de destination configurable et variable, à condition que le poste Internet de l'entreprise dispose d'outils de type Remotely Anywhere, permettant le contrôle total du poste Internet par l'utilisateur du réseau interne et fournissant par conséquent une issue de secours, via l'exécution de http, ftp, etc.

17. **Drogues :** Tous les sites web qui offrent ouvertement des contenus sur les stupéfiants, incitant à leur consommation ou fournissant des contacts et des lieux où les acheter. Les adresses d'Internet informant des dangers des drogues ne sont pas incluses.

18. **Économie :** Sites web dont les contenus sont consacrés à la bourse, à la banque, aux placements financiers, aux assurances, etc.

19. **Éducation :** Sites web dont les contenus sont consacrés aux écoles, aux universités, aux académies et aux cours en général.

20. **Emploi :** Sites web dont les contenus se rapportent aux offres et demandes d'emploi; les sites "head-hunters" en général sont également inclus.

21. **Rencontres :** Pages Web par le biais desquelles on peut faire la connaissance d'autres personnes : liens amicaux, recherche de l'âme soeur, etc….

22. **Loisirs :** Sites web d'information concernant les films, les pièces de théâtre, les livres, les restaurants, les hobbies, etc.; contenus, en général, consacrés aux loisirs, comment utiliser son temps libre, excepté les contenus appartenant aux jeux de hasard, sport, jeux et voyages.

23. **Forum :** Forum.

24. **Guides :** Sites web qui incluent des plans de ville, donnent des renseignements sur les adresses, les numéros de téléphone, etc.

25. **Hackers :** Sites web où trouver du software illégal. Des pages offrant des explications et des outils pour "pirater" des programmes et en général briser la sécurité des systèmes informatiques.

26. **Domaines hébergements :** Sites web des enterprises qui hébergent des sites web et où les domaines Internet peuvent être obtenus.

27. **Information :** Sites web qui donnent des informations générales et utiles, telles que l'état des routes, les prévisions météorologiques, etc.

28. **Informatique :** Sites web contenant de l'information concernant le hardware, sofware, Internet, etc.

29. **Jeux :** Sites où jouer "on-line" ou télécharger des jeux d'ordinateur.

30. **Juridiques :** Sites Web proposant des informations sur des questions légales.

31. **Logos/Ringtones :** Images ou chansons (mélodies monophoniques ou polyphoniques) qui sont téléchargées par les utilisateurs de téléphones mobiles.

32. **Liste blanche :** Pages Web qui n'appartiennent à aucun type de contenus. Les règles de filtrage restreignant le contenu ne leur sont pas applicables.

33. **Liste noire :** Pages Web qui sont considérées appartenir à tous les types de contenus. Les règles de filtrage restreignant le contenu leur sont applicables.

34. **Mannequins :** Sites où trouver des photographies de mannequins des deux sexes; les sites web où ce type de photos présentent les mannequins totalement ou partiellement nus sont compris dans la catégorie pornographie.

35. **Musique :** Sites web où acquérir ou télécharger de la musique ou encore trouver l'information concernant les chanteurs et groupes musicaux en général.

36. **Payer pour naviguer :** Pages Web qui permettent de gagner de l'argent sur le réseau en recevant des messages, en naviguant sur certaines pages, en souscrivant à des offres gratuites, etc.

37. **Pages personnelles :** Pages créées en hébergement spécialement prévu à cet effet et qui ne sont pas inclues dans d'autres catégories**.**

38. **Pornographie :** Sites web à contenus pornographiques ou érotiques. L'accès aux chats où l'on peut trouver ce type de matériel est inclus.

39. **Portails :** Pages Web où l'on peut trouver une large gamme de contenus : nouvelles, loisirs, sports, jeux, musique, etc.

40. **Presse :** Sites web qui sont des journaux ou des magazines virtuels.

41. **Racisme :** Sites web qui comprennent des contenus à caractère ouvertement xénophobe ou incitent à des comportements racistes en raison de la race, culture, religion, idéologie, etc.

42. **Redirecteurs :** Pages Web qui redirigent ou transforment d'autres pages Web.

43. **Société :** Sites web à contenus relatifs aux "célébrités". Comprend également d'autres types de contenus tels que mode, parfums, décoration, etc.

44. **Santé :** Pages Web dans lesquelles on peut trouver des informations à caractère informatif (non scientifique) sur les maladies et leurs remèdes.

45. **Sectes :** Sites web à contenus relatifs aux sectes très dangereuses, telles que celles dénommées de culte au diable, universellement acceptées comme sectes, mais pas celles qui en raison de législation différente dans les différents pays sont considérées comme des sectes dans certains pays et comme des associations religieuses de plein droit d'en autres.

46. **Sexualité :** Articles sur le sexe, le sexe destiné aux adolescents, l'éducation sexuelle etc. sans contenu à caractère pornographique**.**

47. **Servers de Messagerie Instantanée :** Sites où sont enregistrés ces programmes pour fournir le service et les pages qui y sont associées**.**

48. **Servers P2P :** Sites où sont enregistrés ces programmes pour fournir le service et les pages qui y sont associées**.**

49. **Spyware :** Pages susceptibles de contenir Spyware. On entend par Spyware le logiciel recompilant les informations d'un ordinateur pour ensuite les transmettre à une entité externe, à l'insu ou sans le consentement du propriétaire de l'ordinateur.

50. **Télécommunications :** Sites Web fournissant des informations sur la téléphonie fixe, la téléphonie mobile, les connexions à Internet, etc.

51. **Voyages :** Sites web d'agences de voyages et ceux d'information touristique des villes, places hôtelières et moyens de transport.

52. **Violence :** Sites web à caractère ouvertement violent, incitant à la violence ou qui en font l'apologie.

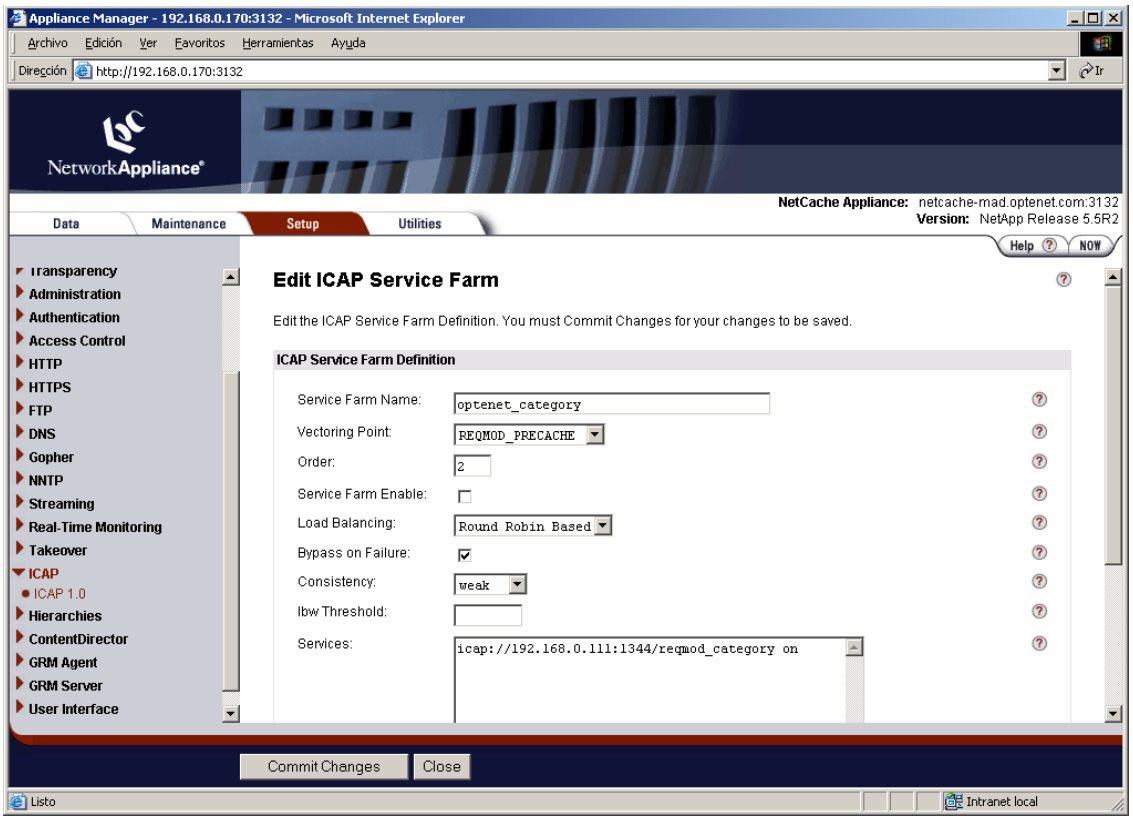
* Les sites peuvent appartenir en nombre d'occasions à deux catégories, voire davantage, en même temps.

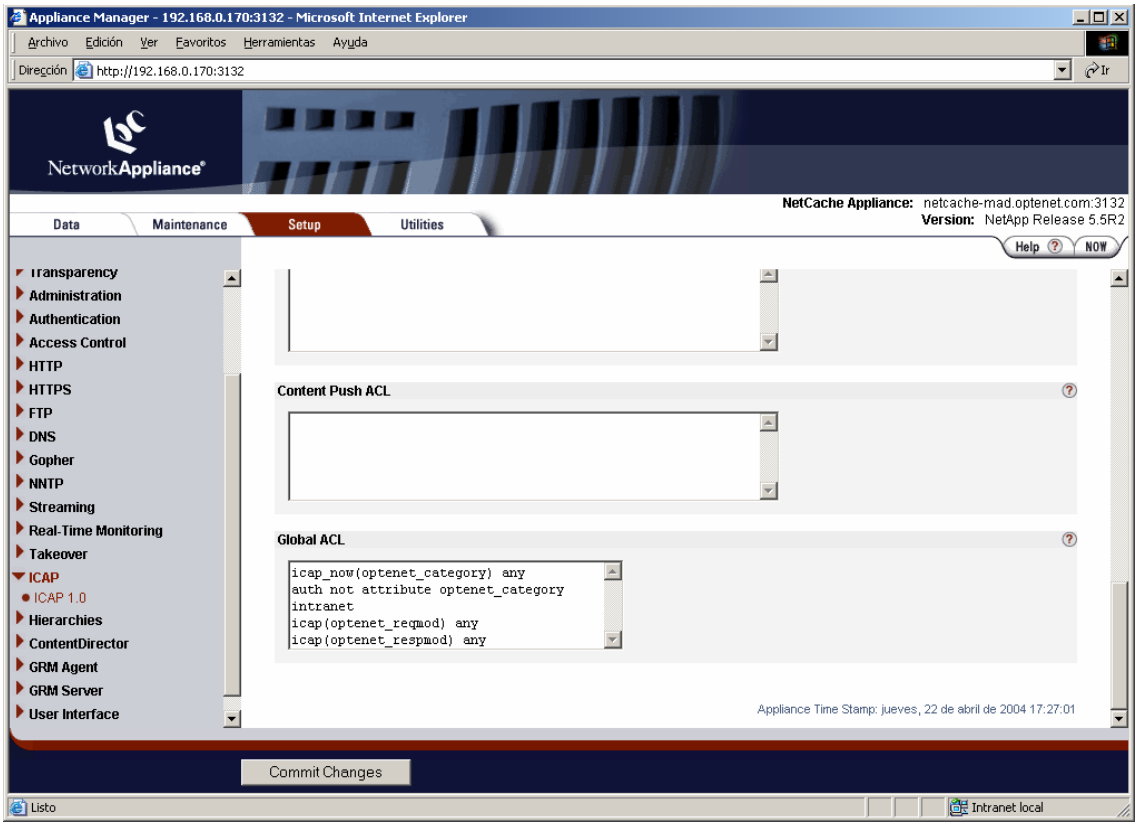
5. ICAP NOW

NetCache implante une méthode ICAP différente nommée icap now. La différence avec les méthodes icap habituelles est que la demande ICAP est transmise au Server ICAP, dans le cas présent OPTENET Server, avant même de procéder à l'authentification de l'utilisateur. Cela peut s'avérer utile dans les cas où vous souhaitez réaliser des opérations différentes en fonction du résultat que renvoie le Server ICAP en décidant, par exemple, de demander uniquement l'authentification aux utilisateurs qui vont accéder à des catégories précises.

OPTENET Server dispose d'un service ICAP appelé reqmod_category dont la seule mission est de catégoriser les accès qui lui parviennent depuis ce service. A la différence des deux autres services (reqmod_netcache et respmod_netcache) OPTENET Server ne bloque aucun accès, il les classe en retournant la catégorie à NetCache. Pour éviter qu'un accès ne soit catalogué dans plus d'une catégorie, OPTENET Server utilise le fichier de configuration etc/catpriority.txt qui se situe dans votre répertoire d'installation pour que, en cas de conflit entre catégories, lui soit assigné celle qui apparaît en premier dans ledit fichier. Les catégories qui n'apparaissent pas sont considérées comme les moins prioritaires, si aucune des catégories n'est écrite (les deux catégories ayant été créées par l'administrateur), la première du fichier créé dans le système est sélectionnée. Il est possible d'éditer catpriority.txt et de classer les catégories à votre goût. Une fois conservé, vous devrez redémarrer le filtre pour votre classement prenne effet. De plus, vous pouvez ajouter de nouvelles catégories au fichier en modifiant également le premier numéro qui apparaît dans le fichier, celui-ci indiquant le nombre de catégories comprises dans celui-ci.

Ci-dessous, vous trouverez un exemple de configuration dans un NetCache dans lequel le service reqmod_category a été défini pour demander l'authentification à tous les accès n'appartenant pas à la catégorie Intranet:





Pour pouvoir utiliser correctement ce nouveau service, nous devons demander à OPTENET Server qu'il lance plus de threads afin de répondre aux requêtes de ce nouveau service. Cela est indiqué dans les versions Windows en modifiant la clé du répertoire :

HKEY LOCAL MACHINE\SOFTWARE\OPTENET\OPTENET Server\IcapServices

En écrivant la valeur.
Pour les versions Unix, vous devrez modifier le script /usr/local/optenet/RunOPTENET en ajoutant le paramètre -**icap_services 3**
Dans les deux cas, vous devrez redémarrer le filtre pour que la configuration prenne effet.

6. SURVEILLANCE SNMP (SEULEMENT PLATE-FORME LINUX)

Le filtre a la possibilité d'être surveillé via le protocole SNMP, ce qui le rend facilement intégrable aux systèmes de surveillance du marché.

Pour cela, la distribution du filtre inclut un Agent SNMP, qui fonctionne comme un service totalement autonome et maintient en temps réel les valeurs des paramètres sur l'état du filtre à jour.

Par défaut, l'agent utilise le port d'écoute 161 (conFigureble) pour pouvoir disposer de plusieurs agents sur la même machine.

Les paramètres susceptibles d'être surveillés sont les suivants:

- État du filtre : ACTIF / INACTIF / ÉTEINT
  (ID : .1.3.6.1.4.1.2021.254.1.0)
  - ACTIF : Le filtre est actuellement actif (valeur 1).
  - INACTIF : Le filtre est allumé mais actuellement inactif (valeur 0).
  - ÉTEINT : Le filtre n'est pas en cours d'exécution (valeur -1).

- Nombre de demandes par seconde : X.
  (ID : .1.3.6.1.4.1.2021.254.2.0.0)

- Nombre de blocages par seconde : X.
  (ID : .1.3.6.1.4.1.2021.254.3.0.1849.0)

Des informations complètes sur le système sont également fournies, comme :

- L'heure ou la date du système.
  (ID : .1.3.6.1.4.1.2021.4.0)

- La durée d'exécution de l'agent.
  (ID : .1.3.6.1.2.1.1.3)

- Le nom du Server.
  (ID : .1.3.6.1.2.1.1.5)

6.1 Exécution de l'agent SNMP

Pour activer l'agent SNMP d'OPTENET, exécutez la commande suivante:

OptenetSnmp [–h] [–v] [–f] [–p PORT] [–l LOG_FILE]

- h : Indique l'aide en ligne sur les commandes,
- v : Indique la version du produit,
- f : Indique qu'il n'y a aucune exécution sur un thread enfant,
- p : Spécifie un port d'écoute des demandes différent du port 161,

l : Modifie le fichier journal par défaut (/usr/local/optenet/logs/optenet_snmp.log).

6.2 Démarrage automatique

Si vous souhaitez que l'agent SNMP démarre automatiquement avec le filtre, il est nécessaire de modifier les fichiers « RunOPTENET » et « filterinit » et de supprimer les commentaires des lignes indiquées, où apparaissent les appels nécessaires au démarrage et à l'arrêt de l'agent OptenetSnmp.

Par défaut, dans le fichier de démarrage, le port d'écoute de l'agent Snmp est **10237.**

6.3 Configuration de l'agent

L'agent possède un fichier de configuration dénommé « snmp.conf » contenant les informations suivantes:

Stat-url= 192.168.0.240 // URL ou IP d'écoute du filtre
Stat-port= 10234 // Port d'écoute du Server web du filtre (CGI de statistiques)

7. CGIS DE CONFIGURATION AVANCEE

Dans ce paragraphe, sont décrites les CGI ayant mis en oeuvre le filtre de configuration avancée et qui sont uniquement accessibles en saisissant directement au clavier dans les barres d'adresses du navigateur.

7.1 Rechargement

KNKJ
Cette option indique au filtre de recharger l'ensemble de sa configuration, ainsi que la base de données des URLs. Cette option est utile si vous décidez de « cloner » la configuration
d'une instance d'OPTENET à un autre Server récemment incorporé dans la gestion en cluster du réseau, sans pour autant redémarrer le service OPTENET.
Mise en garde : n'utilisez cette option qu'en cas de nécessité, le rechargement de la base de données étant un processus coûteux en temps CPU.
Pour lancer le rechargement vous devez exécuter le script cgi suivant :

http://ip_du_filtre:10237/cgi-bin/ResetConf?

7.2 Effacement des fichiers journaux sur le disque (cgi-bin/FlushLogs)

Cette option fait en sorte que le filtre vide sur le disque les logs qu'il a actuellement en mémoire. Pour optimiser le rendement, le filtre, au lieu d'écrire directement sur ses logs sur le disque chaque fois qu'une demande est analysée, utilise un système de buffering en stockant ces logs en mémoire et en les vidant sur le disque lorsque les buffers se rechargent, toutes les 5 minutes. Cette option provoque le vidage des logs dont il dispose en ce moment dans ses buffers de mémoire. Pour lancer le vidage des logs sur le disque, le cgi suivant doit être exécuté:

http://ip du filtre:10237/cgi-bin/FlushLogs.LANG=fra

7.3 Information du système en mode texte (/cgi-bin/sysinfo txt)

Cette option fait en sorte que le filtre restitue des informations sur son état au format texte, au lieu d'être une page html valide. Elle est très utile dans des installations unix où elle est administrée à partir d'une ligne de commandes et où l'on peut voir l'état du filtre par le biais de l'outil wget comme dans l'exemple suivant:

wget http://optuser:optpw@ip_del_filtro:10237/cgi-bin/sysinfotxt?LANG=fra -O sysinfo.txt

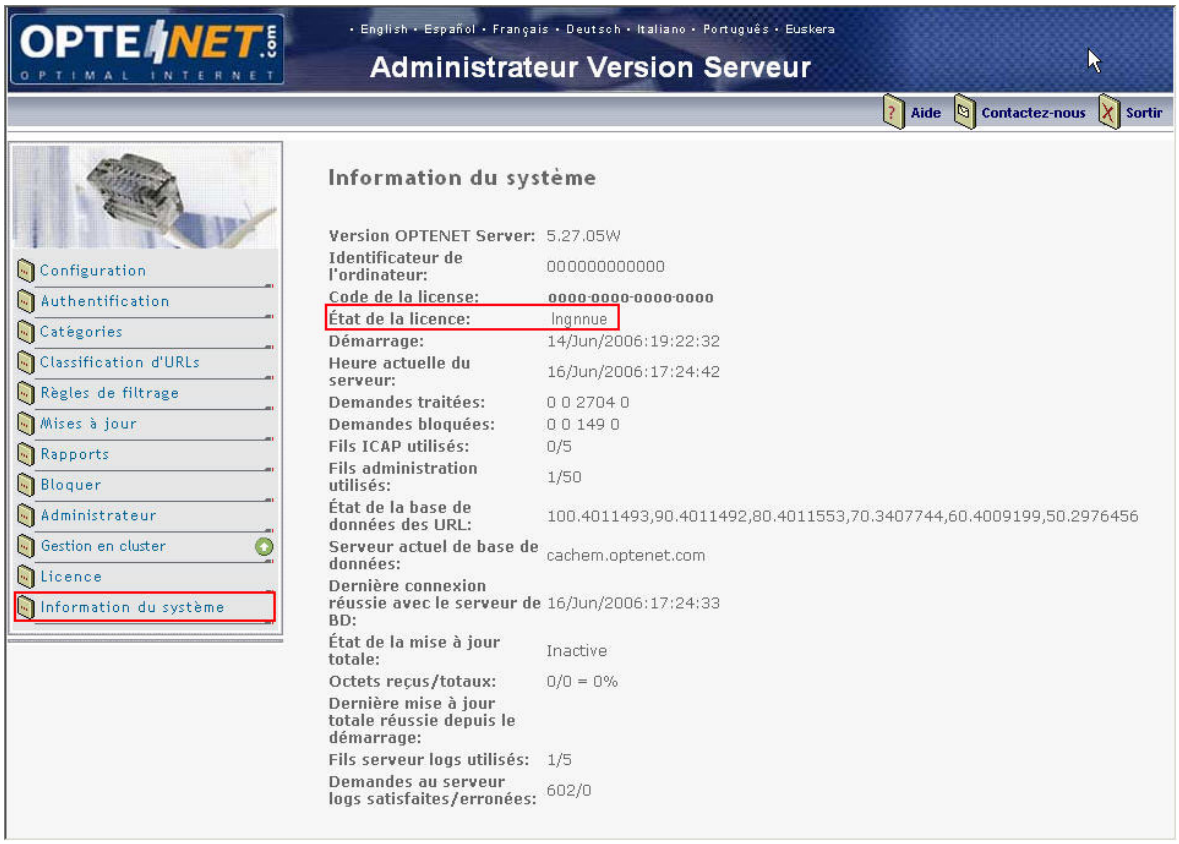
8. CONFIGURATION DE MICROSOFT ISA 2004

8.1 Introduction

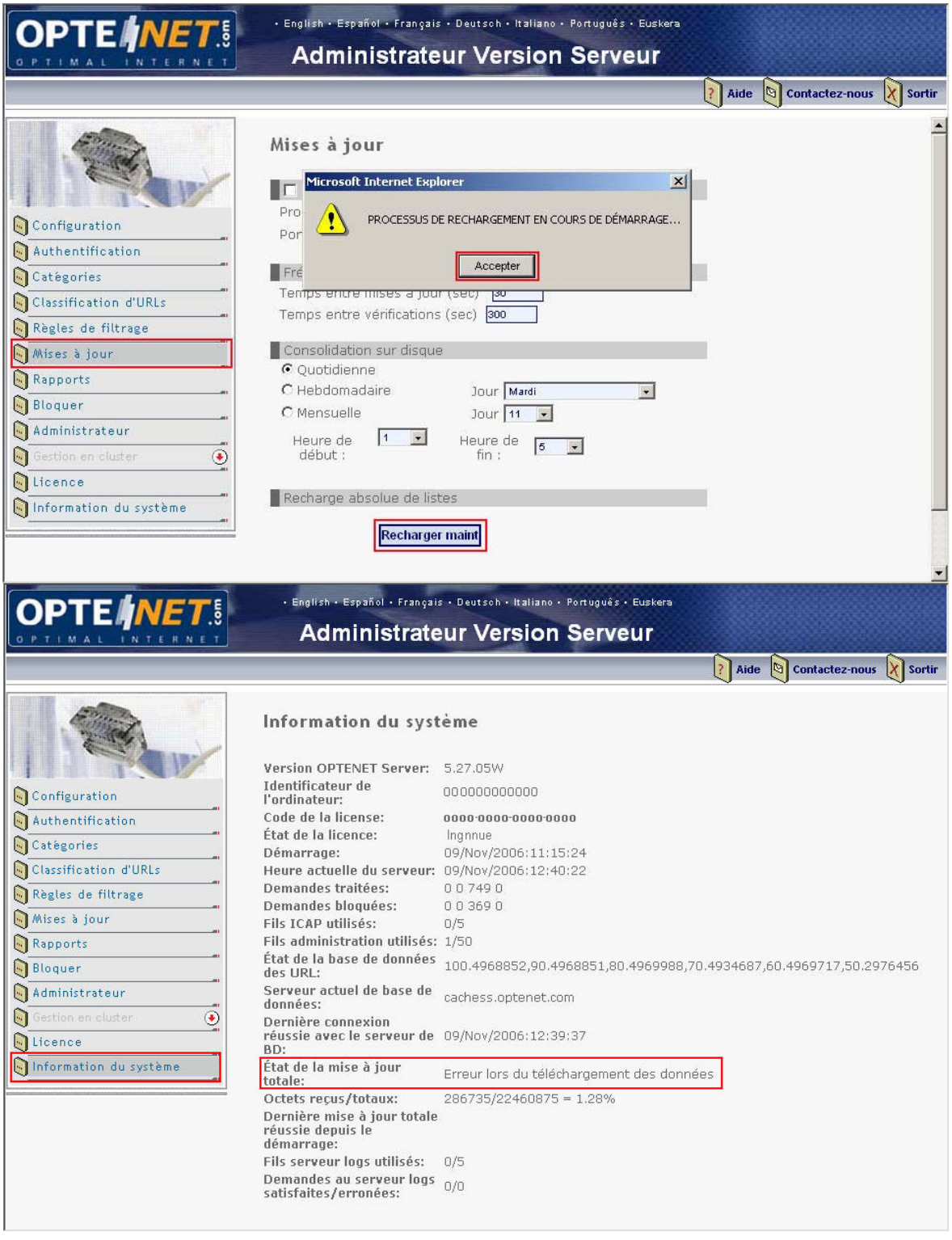
Une fois le produit installé sur **MICROSOFT ISA SERVER 2004** (compatible à partir de la version 5.21.03), une série de fonctionnaités ne fonctionnent pas par défaut de par le fait que MICROSOFT ISA SERVER 2004 n'est pas un simple PROXY mais un PARE-FEU avec des fonctions de PROXY. Pour que le produit fonctionne, nous devons établir diverses règles lors de la configuration de MICROSOFT ISA SERVER 2004.

8.2 Accès aux Servers de licences et mises à jour d'OPTENET

Par défaut, tous les accès du Server MICROSOFT ISA SERVER 2004 doivent être coupés, ainsi si OPTENET WEB FILTERING tente de se connecter à la centrale de licences d'OPTENET (http://www.edunet.es) pour connaître l'état de la licence, il nous indiquera que l'accès est impossible en affichant la valeur « *Inconnue* » dans « *État de la licence* ».



De la même manière, si nous tentons de mettre à jour la base de données du produit, que ce soit manuellement ou au moyen des tentatives automatiques réalisées par le produit, ce dernier nous indiquera que le l'accès aux bases de données est impossible en affichant la valeur « *Erreur d'extraction des données* » dans « *État de la mise à jour totale* ».



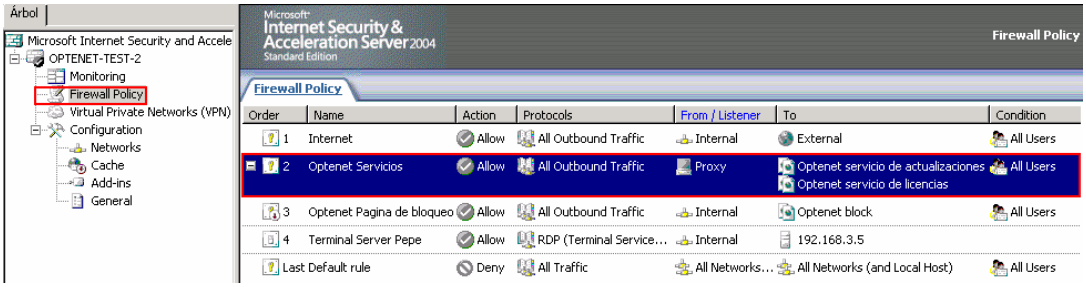
Pour que les accès à la centrale de licences soient effectués correctement, il convient d'autoriser le Server MICROSOFT ISA SERVER 2004 à cette adresse :

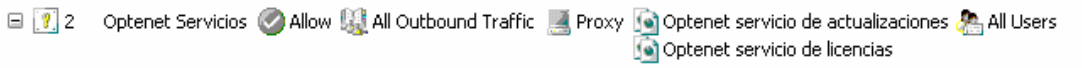
http://www.edunet.es/*

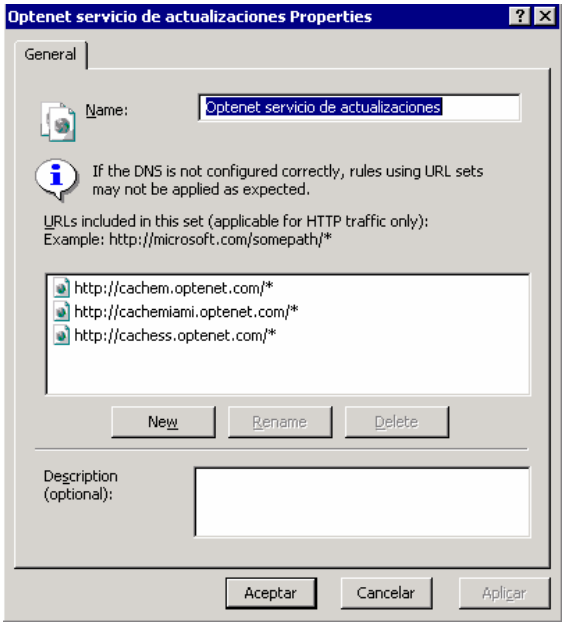
De la même manière, pour que les mises à jour puissent être réalisées correctement, il convient d'autoriser le Server MICROSOFT ISA SERVER 2004 aux adresses de bases de données d'OPTENET :

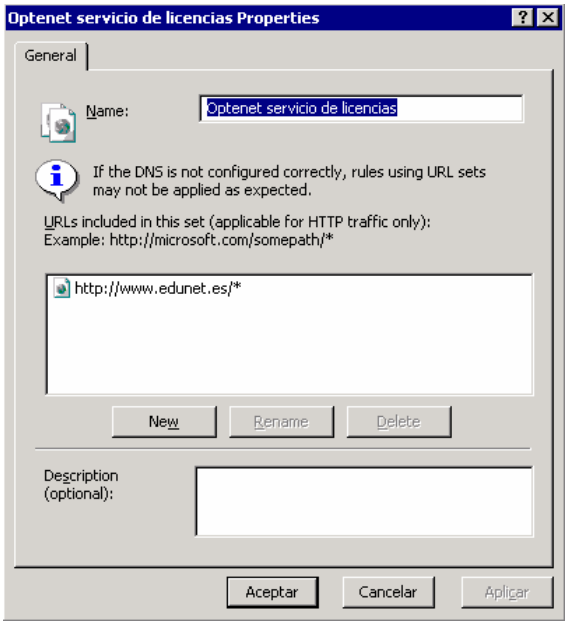
http://cachem.optenet.com/*
http://cachemiami.optenet.com/*
http://cachess.optenet.com/*

Pour cela, nous créons une règle qui autorise l'accès à tous ces services à patrir du Server MICROSOFT ISA SERVER 2004.



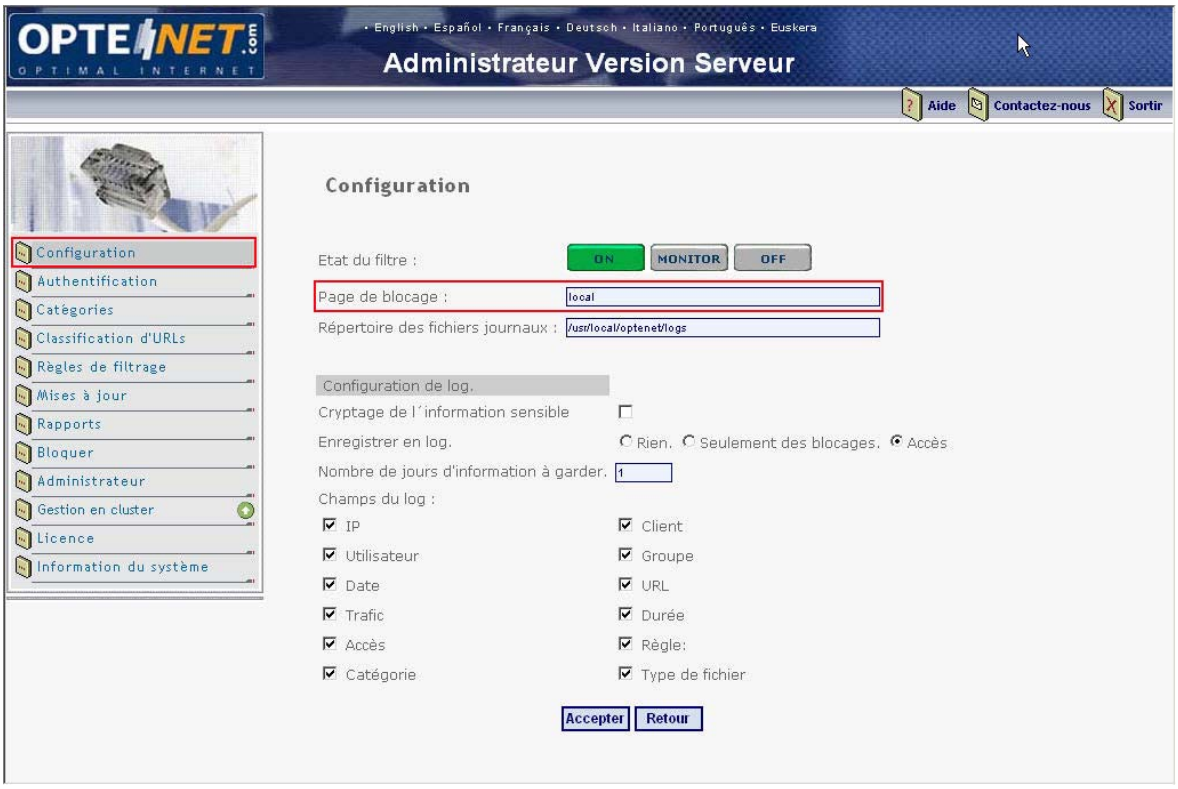






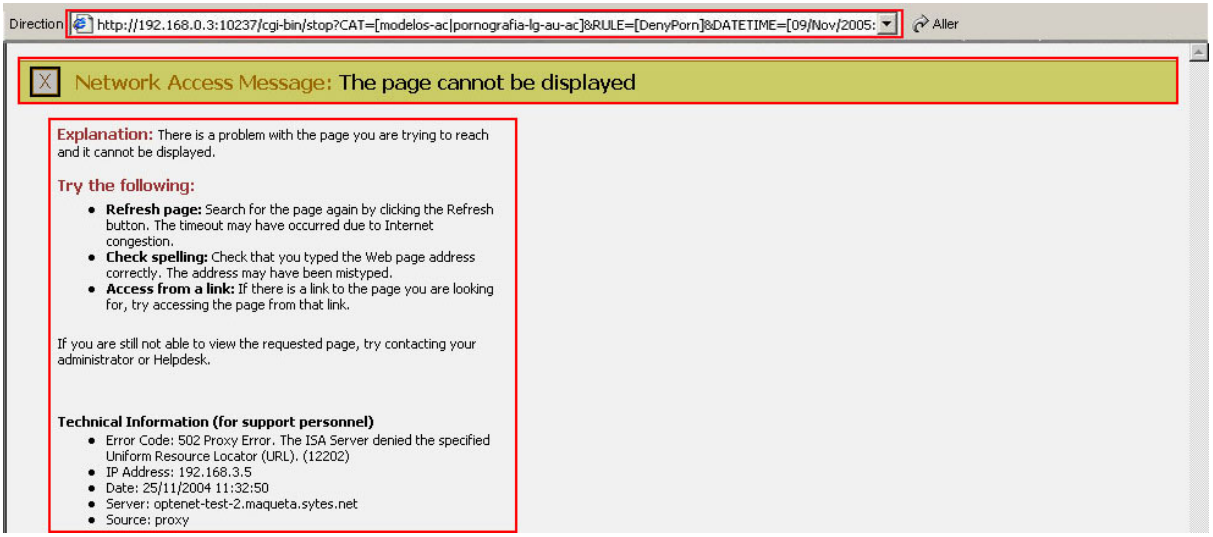
8.3 Accès à la page de blocage par défaut

Par défaut, tous les accès du Server MICROSOFT ISA SERVER 2004 sont coupés; ainsi, si un client qui a l'autorisation de naviguer à l'extérieur, une tentative d'accès à une page non autorisée est réalisée, et l'utilisateur est redirigé vers la page de blocage par défaut. Cette page se définit dans l'onglet « *Configuration* » dans la gestion Web du produit OPTENET WEB FILTERING. La valeur par défaut est « *locale* »

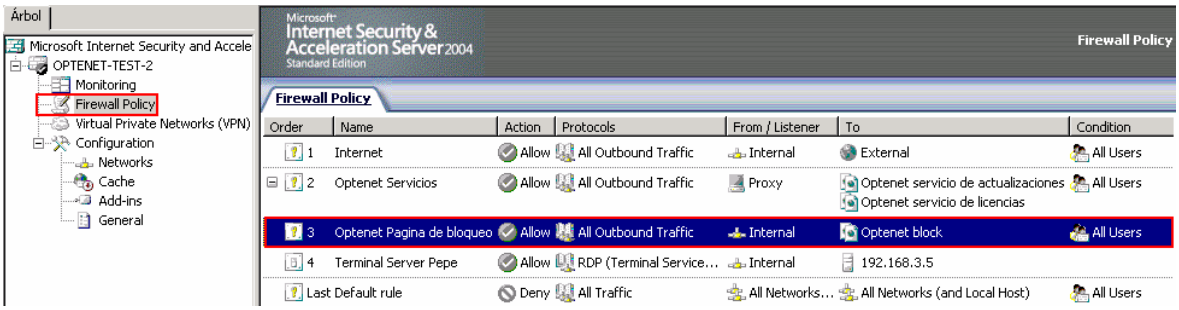


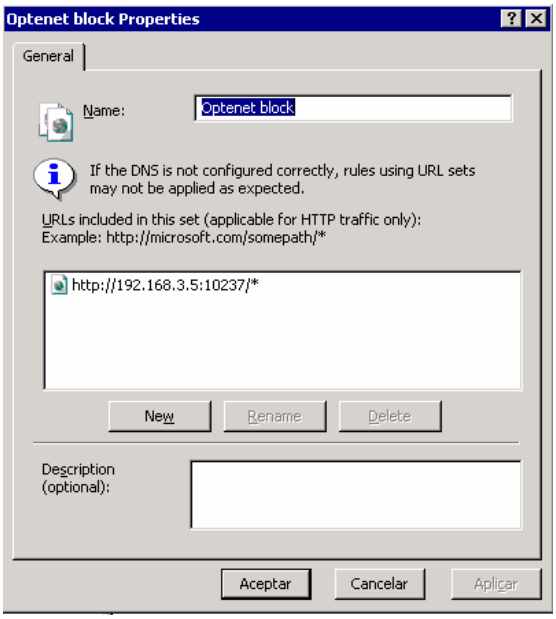
et celle-ci correspond au propre Server MICROSOFT ISA SERVER 2004 au port 10237 où le produit OPTENET WEB FILTERING a emplacé cette page.

Comme nous n'avons définie aucune règle permettant d'accéder à ce port, les demandes de blocage ne s'afficheront pas correctement et une page comme celle-ci s'affichera :



Pour que cela ne survienne pas, nous créons une règle qui permet l'accès à tous les utilisateurs avec droit de navigation vers le port 10237 de l'ordinateur où est installé le Server MICROSOFT ISA SERVER 2004.





Ainsi, nous pouvons être bloqués et parvenir à la page de blocage adéquate.