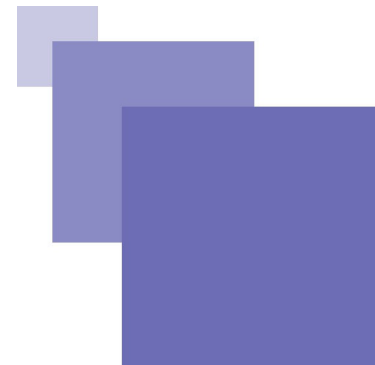


# **Documentation de référence du SLIS**

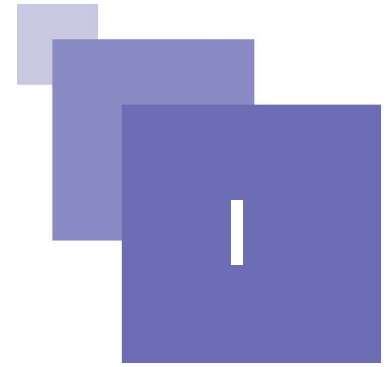
## **4.1**

# Table des matières



<b>I - Gestion des sous-réseaux</b>	<b>5</b>
<b>II - Redirection temporaire de ports (NAT)</b>	<b>11</b>
A. Interface de translation de port (NAT).....	11
B. Cas d'usage pour la redirection temporaire de ports.....	12
<b>III - Module de filtrage du SLIS</b>	<b>15</b>
A. Principe du filtrage sur un SLIS.....	15
B. Base de filtrage web.....	16
C. Règles de filtrage.....	18
D. Cas d'usage du filtrage de sites web.....	20
E. Bases prédéfinies dans le SLIS.....	21
<b>IV - Configuration de la redirection de services web</b>	<b>25</b>
<b>V - Délégation de droits simple</b>	<b>31</b>

# Gestion des sous-réseaux



## Introduction

Le module de gestion des sous-réseaux permet de structurer votre réseau local en le découpant en sous-réseaux. Vous pourrez ensuite définir une politique de gestion de l'accès internet pour chaque sous-réseau :

- Ouvrir ou fermer l'accès internet manuellement.
- Ouvrir ou fermer l'accès internet automatiquement selon une programmation horaire.
- Activer ou non l'authentification pour l'accès au web.

La gestion des accès internet se fait en collaboration avec le module de pare-feu.

La gestion des sous-réseaux peut être déléguée à une autre personne que l'administrateur local (droit d'administration partiel).

Si votre académie dispose d'un plan académique d'adressage, il est important de s'y référer. Par exemple, pour l'académie de Grenoble, vous trouverez sur le site "Assistance Technique aux AIPRT" les *préconisations académiques pour le plan d'adressage du réseau local*<sup>1</sup> des établissements secondaires de l'académie de Grenoble.



## Exemple

Dans un établissement, les machines du CDI auront une adresse IP attribuée dans la plage du sous-réseau 172.16.104.1 à 172.16.104.254. Les horaires d'accès à l'Internet des machines de cette salle pourront être gérés indépendamment de ceux des autres salles.

Il pourra être intéressant d'affecter à un même sous-réseau toutes les machines réservées aux professeurs, quelle que soit la salle d'appartenance. On pourra ainsi gérer le filtrage web et les horaires d'accès de ces machines indépendamment de celles réservées aux élèves.

## Présentation de l'interface

L'accès à la page d'administration des sous-réseaux se fait par le menu d'administration :

- Sécurité
  - Accès
    - Accès par sous-réseaux

On arrive alors sur la page suivante.

**Gestion des sous-réseaux**

### Configuration du réseau local

Le réseau local a la priorité sur tous les sous-réseaux. S'il est désactivé, aucun accès internet n'est possible..  
Les changements sont validés sur le système toutes les minutes  
L'authentification pour le LAN est l'authentification par défaut. Pour les sous réseaux, fixez là séparément.

**RÉSEAU :** 172.16.0.0      **MASQUE :** 255.255.0.0

Le réseau local a accès à internet.

Le réseau local est en mode manuel

**Passer en mode automatique**

**Par défaut, une authentification est exigée sur votre réseau local.**

---

### Configuration des sous réseaux.

Voici les sous-réseaux de votre réseau. L'accès internet et l'authentification peuvent être fixés pour chacun..

Action : Créer un nouveau sous-réseau Valider

[Tout sélectionner](#) | [Ne rien sélectionner](#) | [Inverser la sélection](#)

Status	Nom	Adresses des sous-réseaux	Horaire	Proxy authentifié
<input type="checkbox"/>	Serveurs	172.16.0.1 à 172.16.0.254		
<input type="checkbox"/>	Salle des professeurs	172.16.101.1 à 172.16.101.254		
<input type="checkbox"/>	Postes enseignants	172.16.102.1 à 172.16.102.254		
<input type="checkbox"/>	Portables	172.16.103.1 à 172.16.103.254		
<input type="checkbox"/>	CDI-D9	172.16.104.1 à 172.16.104.254		
<input type="checkbox"/>	CDI-GS	172.16.105.1 à 172.16.105.254		
<input type="checkbox"/>	CDI-annexe	172.16.106.1 à 172.16.106.254		
<input type="checkbox"/>	Salle 125	172.16.107.1 à 172.16.107.254		
<input type="checkbox"/>	exao-spc	172.16.109.1 à 172.16.109.254		
<input type="checkbox"/>	Salle 223	172.16.110.1 à 172.16.110.254		
<input type="checkbox"/>	CDI libre service	172.16.111.1 à 172.16.111.254		
<input type="checkbox"/>	Exao SVT	172.16.112.1 à 172.16.112.254		
<input type="checkbox"/>	S123 - TP SPC	172.16.116.1 à 172.16.116.254		
<input type="checkbox"/>	DHCP-libre	172.16.130.1 à 172.16.130.254		
<input type="checkbox"/>	DHCP-libre-2	172.16.131.1 à 172.16.131.254		
<input type="checkbox"/>	Serveurs tertiaire	172.16.200.1 à 172.16.200.254		
<input type="checkbox"/>	Salle 301	172.16.201.1 à 172.16.201.254		
<input type="checkbox"/>	salle 302	172.16.202.1 à 172.16.202.254		
<input type="checkbox"/>	salle 314	172.16.203.1 à 172.16.203.254		
<input type="checkbox"/>	salle 315	172.16.204.1 à 172.16.204.254		

*Page d'accueil des sous réseaux*

1. La première zone s'intéresse à la configuration du réseau local dans son ensemble. Elle indique
  - la définition du réseau local (LAN) en terme d'adresse IP
  - L'état du réseau (activé ou non). Si le réseau est activé, chaque sous réseau aura accès à internet en fonction de son état. Par contre, si le réseau local est désactivé, l'accès à internet est coupé pour l'ensemble de l'établissement. Si on est en mode manuel, cliquer sur la diode de statut fera basculer le statut entre ouvert et fermé.
  - Le mode du réseau : en mode manuel ou en programmation horaire. On peut modifier ce mode.
  - Enfin le mode d'authentification par défaut. Pour plus de détails voir ci

6

- après.
2. La seconde zone s'intéresse à la configuration des sous-réseaux de l'établissement. On y trouve :
    - Une zone d'action qui permet de :
      - supprimer les sous-réseaux sélectionnés.
      - passer les sous-réseaux sélectionnés en mode manuel
      - passer les sous-réseaux sélectionnés en mode programmation horaire
      - activer les sous-réseaux sélectionnés (s'ils sont en mode manuel)
      - désactiver les sous-réseaux sélectionnés (s'ils sont en mode manuel)
      - fixer le mode d'authentification sur chaque sous-réseau
    - Une zone de sélection qui vous permet de sélectionner en masse des sous-réseaux dans votre liste.
    - Un tableau contenant chacun des sous-réseaux de votre établissement.

### Authentification des accès au web par sous-réseau.

Il est possible d'exiger une authentification des utilisateurs lors de l'accès au web. L'authentification demandée utilise l'annuaire LDAP qui se trouve sur le LCS. Il est donc impératif que les comptes utilisateur du LCS soient créés. Référez vous à la documentation LCS si besoin est.

Le mode d'authentification pour le LAN est le mode d'authentification par défaut, qui sera utilisé pour les machines qui sont en dehors des plages des sous-réseaux programmés. Modifier cette authentification donnera accès à l'option "SQUID\_AUTH" du service de proxy. Elle peut prendre deux valeurs :

- 0 : pas d'authentification, les utilisateurs accèdent librement à internet.
- 1 : authentification exigée. Les utilisateurs doivent fournir au proxy leur identifiant pour accéder à internet.

La configuration conseillée est d'utiliser une authentification par défaut si votre LCS contient bien les comptes des utilisateurs. Vous pouvez la supprimer sur les réseaux correspondant à des machines bien identifiées.

L'authentification fixée pour chacun des sous-réseaux remplace l'authentification par défaut.



### Exemple

Dans un établissement, si le LCS est alimenté en compte utilisateur, on peut :

- par défaut, demander une authentification pour les machines en dehors des sous-réseaux connus
- pour les machines ayant une IP sur la plage d'IP dynamique, on exigera aussi une authentification
- pour les machines de salle de cours et de la salle des professeurs, où l'IP est connue et la connexion au domaine obligatoire, on peut se passer de l'authentification
- pour les machines dans des salles en libre service ou à fort passage (comme le CDI), l'authentification pourra être demandée.

### Sous-réseau

Pour chaque sous-réseau, vous avez une ligne dans le tableau comme la ligne suivante :



*Définition d'un sous-réseau*

Les items de la ligne sont :

- Une case à cocher pour appliquer l'une des actions définies précédemment.
- Une diode qui indique l'état du sous-réseau. Si le sous-réseau est en mode manuel, cliquer sur cette diode fera basculer l'état entre ouvert et fermé.









- Le nom du sous-réseau. L'icône avec le petit stylo permet de modifier ce nom.
- La page d'adresse IP concernée par le sous-réseau.
- Une icône qui indique le mode. Si l'icône est un carré gris, le sous-réseau est en mode manuel. S'il contient une petite horloge, il est en mode automatique. Cliquer dessus permettra d'accéder à la programmation horaire (voir ci dessous).
- Un cadenas. Si le cadenas est barré, le réseau n'exige pas d'authentification. S'il est décoché, le réseau nécessite une authentification lorsque l'utilisateur souhaite accéder au web.

### La programmation horaire

La programmation horaire permet de rendre accessible l'internet pour un sous-réseau suivant des horaires hebdomadaires pré-établis. C'est idéal pour paramétrer des salles de classe spécifiques de façon régulière. L'interface est sobre et se contente de proposer les fonctionnalités minimum. La page du planning horaire des sous-réseaux comprend une visualisation de chacun des jours de la semaine avec les horaires d'ouverture (symbolisés en vert) et de fermeture (en rouge).

#### Horaires pour le sous-réseau : CDI-D9

**Légende :** ● Activé ● Désactivé

Lundi :	
	<div style="display: flex; justify-content: space-between;"><span>0h -&gt; 6h</span><span>6h -&gt; 12h</span><span>12h -&gt; 18h</span><span>18h -&gt; 24h</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Activé de</span> <input type="text" value="0"/> : <input type="text" value="0"/> à <input type="text" value="0"/> : <input type="text" value="0"/> <span>ok</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Comme</span> <input type="text" value="lundi"/> <span>Copier</span></div>
Mardi :	
	<div style="display: flex; justify-content: space-between;"><span>0h -&gt; 6h</span><span>6h -&gt; 12h</span><span>12h -&gt; 18h</span><span>18h -&gt; 24h</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Activé de</span> <input type="text" value="0"/> : <input type="text" value="0"/> à <input type="text" value="0"/> : <input type="text" value="0"/> <span>ok</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Comme</span> <input type="text" value="lundi"/> <span>Copier</span></div>
Mercredi :	
	<div style="display: flex; justify-content: space-between;"><span>0h -&gt; 6h</span><span>6h -&gt; 12h</span><span>12h -&gt; 18h</span><span>18h -&gt; 24h</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Activé de</span> <input type="text" value="0"/> : <input type="text" value="0"/> à <input type="text" value="0"/> : <input type="text" value="0"/> <span>ok</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Comme</span> <input type="text" value="lundi"/> <span>Copier</span></div>
Jeudi :	
	<div style="display: flex; justify-content: space-between;"><span>0h -&gt; 6h</span><span>6h -&gt; 12h</span><span>12h -&gt; 18h</span><span>18h -&gt; 24h</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Activé de</span> <input type="text" value="0"/> : <input type="text" value="0"/> à <input type="text" value="0"/> : <input type="text" value="0"/> <span>ok</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Comme</span> <input type="text" value="lundi"/> <span>Copier</span></div>
Vendredi :	
	<div style="display: flex; justify-content: space-between;"><span>0h -&gt; 6h</span><span>6h -&gt; 12h</span><span>12h -&gt; 18h</span><span>18h -&gt; 24h</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Activé de</span> <input type="text" value="0"/> : <input type="text" value="0"/> à <input type="text" value="0"/> : <input type="text" value="0"/> <span>ok</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Comme</span> <input type="text" value="lundi"/> <span>Copier</span></div>
Samedi :	
	<div style="display: flex; justify-content: space-between;"><span>0h -&gt; 6h</span><span>6h -&gt; 12h</span><span>12h -&gt; 18h</span><span>18h -&gt; 24h</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Activé de</span> <input type="text" value="0"/> : <input type="text" value="0"/> à <input type="text" value="0"/> : <input type="text" value="0"/> <span>ok</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Comme</span> <input type="text" value="lundi"/> <span>Copier</span></div>
Dimanche :	
	<div style="display: flex; justify-content: space-between;"><span>0h -&gt; 6h</span><span>6h -&gt; 12h</span><span>12h -&gt; 18h</span><span>18h -&gt; 24h</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Activé de</span> <input type="text" value="0"/> : <input type="text" value="0"/> à <input type="text" value="0"/> : <input type="text" value="0"/> <span>ok</span></div> <div style="display: flex; justify-content: center; margin-top: 5px;"><span>Comme</span> <input type="text" value="lundi"/> <span>Copier</span></div> <div style="text-align: center; margin-top: 5px;"><a href="#">Continuer</a></div>

Planning horaire des sous réseaux



# Redirection temporaire de ports (NAT)

Interface de translation de port (NAT)

11

Cas d'usage pour la redirection temporaire de ports

12

## A. Interface de translation de port (NAT)

### Introduction

Il est parfois nécessaire, pour administrer des machines ou faire du support, d'accéder à certains services des machines du réseau pédagogique à partir de l'extérieur de l'établissement. Le mécanisme permettant ces accès s'appelle la translation de ports. Imaginons par exemple que l'on ait une machine qui fournisse un serveur VNC sur le port 5900. Au sein de l'établissement, nul problème pour y accéder. Par contre, de l'extérieur de l'établissement, cette machine n'est pas visible. Elle n'existe pas pour les utilisateur d'internet car elle fait partie d'un réseau privé.

Pour pouvoir y accéder, il va falloir faire appel à un mécanisme particulier. Le SLIS, en tant que routeur est visible sur internet. On va lui donner pour mission de relayer certaines requêtes qui arrivent vers la machine du réseau interne, de façon transparente. Ainsi, la machine deviendra accessible à partir d'internet. On va demander au SLIS par exemple : " tu vas écouter sur le port 8000. Toutes les requêtes qui arrivent sur ce port, tu les redirigeras vers la machine du réseau interne sur le port 5900". On peut maintenant prendre en main la machine de l'extérieur.

Pour des raisons évidentes de sécurité, afin de ne pas laisser de façon permanente des machines accessibles depuis l'internet, cette redirection ne peut être que temporaire.

### Présentation de l'interface

On accède à l'interface par le menu d'administration, en choisissant "sécurité" puis "Accès" puis enfin "Translation de port (NAT)". On aboutit sur la page suivante.

**Accès distant vers le réseau local ou la dmz (redirection temporaire de port)**

Adresse IP locale de l'ordinateur distant :

Port TCP distant :

Combien de temps voulez-vous accepter les nouvelles connections ?

*Avec ce module, vous pouvez prendre le control à distance d'un ordinateur situé sur votre réseau local (LAN) ou sur votre dmz depuis Internet à travers le SLIS.*

*Pour cela, vous pouvez utiliser n'importe quelle logiciel d'accès distant comme Utlr@VNC qui est un logiciel libre.*

Page de redirection temporaire de ports

En premier lieu, l'adresse IP de la machine qui fournit le service. La machine doit être sur le LAN ou la DMZ.

Ensuite, on doit renseigner le port du service que l'on cherche à atteindre. Parmi les ports classiques à connaître, il y a le 80 pour le http, le 443 pour le https, le 22 pour ssh, le 5900 pour VNC ou le 3389 pour le protocole RDP (MS terminal Server)

En dernier, on a la durée de la translation d'adresse pour les nouvelles connexions. Vous avez le choix de 30 minutes à 2 heures. Une ouverture de 30 minutes ne signifie pas nécessairement que la connexion durera au maximum 30 minutes. Une fois la connexion établie, elle peut perdurer même si la translation de port est coupée. On peut donc en général laisser 30 minutes, cela est suffisant.

Il n'y a plus qu'à valider et on a alors l'indication du port à utiliser sur la page suivante.

**Accès distant vers le réseau local (redirection temporaire de port)**

**lec.ac-grenoble.fr:8001** est maintenant redirigé vers **172.16.200.11:3389**

Avec Utl@VNC, vous avez au moins deux manières :

- En Utilisant l'applet Java d'Ultr@VNC intégré dans le SLIS en cliquant sur [ici](#)
- En utilisant le client Ultr@VNC configuré pour se connecter à :  
**Serveur : lec.ac-grenoble.fr**  
**Port : 8001**
- Vous pouvez aussi rajouter dans vos favoris [ce lien](#) pour réouvrir cette session plus tard.

*Vous venez d'ouvrir une nouvelle session sur ce SLIS pour accéder à une station de votre réseau local. Cette session va accepter les nouvelles connexions pendant 30 minutes. Toutes les connexions établies seront actives jusqu'à ce qu'elles soient désactivées. Cela signifie que vous ne serez pas déconnecté dans 30 minutes, mais que si vous voulez établir une nouvelle connexion après ce délai, il faudra ouvrir à nouveau un accès distant. Le port externe 8001 est maintenant redirigé vers l'ordination 172.16.200.11 de votre réseau local sur le port 3389.*

Translation de port : port utilisé

Comme on le voit sur cette image, on a une redirection vers le serveur interne sur le port 3389 qui est accessible par le port 8001

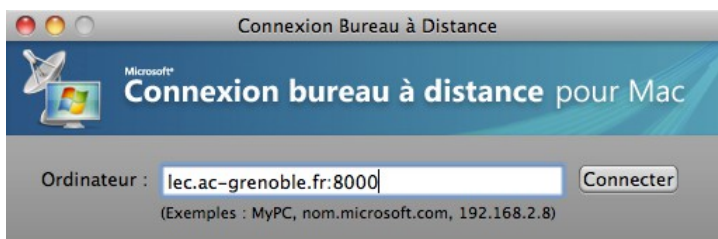
## B. Cas d'usage pour la redirection temporaire de ports



### Exemple : Prise en main d'un serveur windows

On peut souhaiter prendre en main le contrôleur principal de domaine. Si celui est configuré pour accepter les connexions terminal server, on effectuera une redirection temporaire avec comme IP celle du PDC, et comme port le port 3389. Il suffit alors d'utiliser le client Terminal Server pour accéder au PDC en donnant comme adresse l'adresse du SLIS, et comme port le port indiqué par le SLIS (8000 par défaut pour la première redirection).

On peut utiliser le client Terminal Server sur toute station XP correctement configurée.



Utilisation du client MSTSC pour accéder au PDC



### Exemple : prise en main à distance d'une station windows par VNC

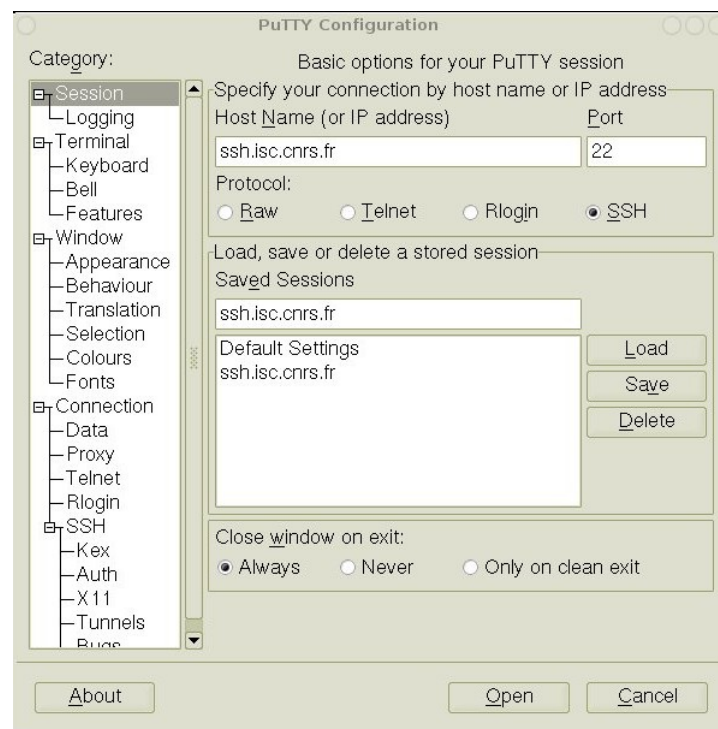
Pour l'utilisation de VNC, on procède de façon similaire. On donne au SLIS dans l'interface de redirection l'adresse IP de la machine dont on veut prendre le contrôle. Le port par défaut de VNC est le port 5900, et c'est celui qu'il faudra utiliser sauf configuration particulière.

Il ne reste plus qu'à ouvrir le client VNC et à lui donner l'adresse du SLIS et le port indiqué par le SLIS.



### Exemple : Prise en main d'un serveur unix/linux par ssh

Pour prendre en main un serveur unix/linux, on peut utiliser le "secure shell". Pour cela, il faut ouvrir le port 22, et utiliser soit ssh en ligne de commande à partir d'une machine linux ou d'un macintosh, soit utiliser le client putty sous windows. Dans la fenêtre de connexion putty, on indiquera le nom de l'établissement et le port que le SLIS indique ( toujours 8000 pour la première redirection par défaut )



*Connexion avec putty*



### Exemple : Prise en main d'un serveur web en https

Sur le réseau local, on peut trouver des serveurs qui ont des interfaces pour être administrés par un serveur web, comme les serveurs ORPEO de l'académie de Grenoble.

Pour prendre en main à distance un serveur ORPEO, on va indiquer dans l'interface de NAT du SLIS l'adresse d'ORPEO (par défaut 172.16.200.11), le port du serveur https (443).

On utilisera ensuite le navigateur en lui indiquant l'adresse du SLIS et le port indiqué par le SLIS, par exemple `https://lec.ac-grenoble.fr :8000/`

Il y aura sans doute un avertissement sur le certificat SSL qui ne correspond pas au serveur, et il faudra accepter de contourner cet avertissement de sécurité.

# Module de filtrage du SLIS



Principe du filtrage sur un SLIS	15
Base de filtrage web	16
Règles de filtrage	18
Cas d'usage du filtrage de sites web	20
Bases prédéfinies dans le SLIS	21

La législation a rendu obligatoire pour les établissements le filtrage des sites internet afin d'éviter le plus possible que les élèves aient accès à des contenus de type pornographique ou de grande violence. Le module de filtrage du SLIS est conçu pour répondre à cette obligation légale. Mais il va beaucoup plus loin en permettant à chaque établissement de paramétrer son accès internet pour utiliser cette ressource de façon optimum tant d'un point de vue pédagogique que d'un point de vue technique.

## A. Principe du filtrage sur un SLIS

### SquidGuard

Le filtrage de contenu sur le SLIS se base sur le logiciel SquidGuard. Ce dernier a largement fait ses preuves et présente l'énorme avantage de très bien tenir la montée en charge, contrairement à bon nombre de ses concurrents. L'interface du SLIS a été conçue pour être utilisable par un administrateur local afin qu'il puisse adapter SquidGuard à ses besoins sans avoir toute la complexité du logiciel à gérer lui-même.

### Principe du filtrage

Le filtrage repose sur une notion de règles de filtrage et de bases de filtrage.



#### Définition : Base de filtrage

Une base de filtrage est un constitué d'une liste de domaines internet ( lemonde.fr , youtube.com , etc...) ou de pages internet ( [http://www.lemonde.fr/politique/article/2010/09/21/seuls-54-des-francais-veulent-la-fin-du-bouclier-fiscal\\_1413808\\_823448.html#ens\\_id=1412212](http://www.lemonde.fr/politique/article/2010/09/21/seuls-54-des-francais-veulent-la-fin-du-bouclier-fiscal_1413808_823448.html#ens_id=1412212) , [http://www.slis.fr/static/html/doc/doc\\_install/html/co/Publications\\_web.html](http://www.slis.fr/static/html/doc/doc_install/html/co/Publications_web.html) , etc ... ) et éventuellement d'expressions régulières (c'est à dire des motifs complexes qui recherchent certains éléments dans l'adresse internet ).

Une base de filtrage est référencée dans le SLIS par un nom. Certaines bases sont maintenues au niveau national. D'autres bases peuvent être créées localement par l'administrateur du SLIS.



### Définition : Règle de filtrage

Une règle de filtrage est une liste de bases de filtrage, avec pour chacune l'accès ou l'interdiction d'accès. Dans une règle de filtrage, l'ordre a son importance. Les règles sont parcourues de haut en bas. Un exemple de règle de filtrage, en français, serait :

- Interdire les sites pornographiques
- Interdire les sites racistes et xénophobes
- interdire les sites d'anonymisation
- autoriser les sites prévus par l'académie
- interdire les sites donnés par adresse IP
- Autoriser tout internet

Ce qu'il faut bien comprendre, c'est que dans une règle de filtrage, la règle est parcourue jusqu'à ce que l'on trouve une ligne qui convienne.

Par exemple, une requête pour playboy.com sera interdite par la première ligne et les lignes suivantes ne seront pas parcourues.

Autre exemple, une requête pour l'adresse IP 193.54.149.75 qui est spécifiquement autorisée par l'académie va parcourir la règle. Les trois premières lignes ne sont pas prises en compte. La ligne 4 autorise la demande, car c'est un site autorisé par l'académie. Et la ligne 5 n'est donc pas évaluée. C'est une adresse IP mais elle est autorisée.

### Filtrage sur le SLIS

Le filtrage sur le SLIS se fait en associant à un sous-réseau de l'établissement une règle de filtrage. On peut ainsi différencier le filtrage suivant la salle : salle des professeurs, salle libre service, CDI, salle de sciences, etc ...

Le filtrage peut se faire en mode "liste noire", c'est à dire on autorise tout internet sauf les sites spécifiés, ou au contraire en mode "liste blanche", c'est à dire en interdisant tout internet sauf les sites spécifiés. Vous verrez plus loin comment faire concrètement.

## B. Base de filtrage web



### Définition : Bases de filtrage

Une base de filtrage est un ensemble de domaines internet, de pages web et d'expressions régulières. Une base de filtrage peut servir pour autoriser ou interdire l'accès à ces éléments à travers l'interface d'administration du SLIS



### Méthode : Accéder aux bases de filtrage

L'accès aux bases de filtrage web se fait via le menu par "sécurité", "filtrage web", "édition des bases de filtrage web". On peut aussi y accéder grâce au lien "Bases" qui figure en bas des pages du module de filtrage web.

On a alors accès à la liste des bases.

Bases d'URLs	
all	all internet
adult	porn site
academie	academic data base
agressif	agressif site
audio-video	audio-video site
dangerous_material	dangerous_material
drogue	drogue site
forums	forums
gambling	gambling site
hacking	hacker site
mobile-phone	mobile-phone site
phishing	phishing site
publicite	publicity site
radio	webradio site
redirector	anonimizer site
strict_redirector	strict anonimizer site
strong_redirector	strong anonimizer site
tricheur	cheating site
warez	warez site
webmail	webmail site
in-addr	ip address
img-search-rew	Filtrage adulte des moteurs de rech. img
 <a href="#">Facebook etc</a>	Interdiction de facebook etc
 <a href="#">custom24</a>	Custom base No 24
<a href="#">Ajouter une base personnalisée</a>	
<a href="#">&lt;&lt;Règles</a> <a href="#">&lt;&lt;Bases</a>	

#### Bases de filtrage Web

Les bases qui figurent en noir sont des bases prédéfinies, qui sont mises à jour chaque nuit sur le SLIS. Elles sont issues des bases nationales de Toulouse et ne peuvent pas être modifiées.

En dessous, on trouve éventuellement des bases qui sont des bases personnalisées. Elles se présentent sous la forme d'hyperliens cliquables. Suivre le lien permet d'aller modifier la base.

Enfin, on trouve un bouton qui permet d'ajouter de nouvelles bases.

Tout en bas, deux liens directs permettent en permanence de rejoindre la liste des bases ou la liste des règles de filtrage.



#### Méthode : Ajouter ou modifier une nouvelle base

En cliquant sur le bouton d'ajout d'une nouvelle base ou sur une base personnalisée, on est envoyé vers la page de création/modification d'une base.

<b>Nom:</b>	<input type="text" value="custom25"/>	<a href="#">Modifier</a>
<b>Commentaire:</b>	<input type="text" value="Custom base No 25"/>	<a href="#">Modifier</a>
<b>Liste des URLt</b> (ex: www.skyrock.com/skynautes/chat/home.phtm):		
Liste vide		
		<a href="#">Ajouter</a>
<i>Vous pouvez ajouter plusieurs items en une seule fois en les séparant par des " ; "</i>		
<b>Liste des DOMAINES</b> (ex: tchatce.com):		
Liste vide		
		<a href="#">Ajouter</a>
<i>Vous pouvez ajouter plusieurs items en une seule fois en les séparant par des " ; "</i>		
<b>Liste des EXPRESSIONS RATIONELLES</b> (ex: \.mp3\$):		
Liste vide		
		<a href="#">Ajouter</a>
<a href="#">&lt;&lt;Règles</a> <a href="#">&lt;&lt;Bases</a>		

#### Création ou modification d'une base de filtrage

Les champs de cette page sont les suivants :

- Le nom de la base de donnée. Il faut le choisir aussi explicite que possible, c'est celui qui apparaîtra dans l'interface. Au départ, l'interface propose un nom de type "customxx" ou xx est un numéro. Cela risque de n'être guère parlant dans le cadre d'une création de règle par la suite.
- Le commentaire, un peu plus détaillé, qui permettra de comprendre mieux ce que fait la base.
- La liste des URLs filtrés (cela représente des pages web proprement dit).
- La liste des domaines filtrés (cela représente des sites entiers).
- La liste des expressions régulières filtrées.

Après la modification d'un quelconque des champs, il faut appliquer immédiatement la modification en cliquant sur le bouton approprié.



### Attention : Expressions régulières

Attention à l'utilisation des expressions régulières. Mal rédigées, elles peuvent bloquer complètement l'utilisation de l'internet dans l'établissement. Il ne faut pas les utiliser si l'on ne sait pas précisément ce que l'on fait. La documentation est disponible sur le site de SquidGuard : <http://www.squidguard.org/Doc/expressionlist.html>

## C. Règles de filtrage



### Définition : Règle de filtrages

Une règle de filtrage est caractérisée par l'utilisation d'un ensemble de bases de filtrages qui permettent d'autoriser ou d'interdire une requête vers internet.



### Méthode : Accès aux règles de filtrage

Pour accéder aux règles de filtrage, on peut passer par le menu "sécurité", "filtrage web", "éditer les règles de filtrage web", ou utiliser les hyperliens "Règles" qui se trouvent en bas des pages du module de filtrage web. On aboutit alors à une page qui liste l'ensemble des règles de filtrage.

**Filtrage de sites Web**

\* [Règle par défaut.](#)

\* Règles personnalisées :

Nom	Réseau	Groupe
<a href="#">salle des profs</a>	172.16.101.0/255.255.255.0 (Salle des professeurs)	**DEFAULT** ▲▼ 🗑️
<a href="#">Salle 315</a>	172.16.204.0/255.255.255.0 (salle 315)	**DEFAULT** ▲▼ 🗑️
<a href="#">DHCP</a>	172.16.130.0/255.255.255.0 (DHCP-libre)	**DEFAULT** ▲▼ 🗑️
<a href="#">Serveurs</a>	172.16.0.0/255.255.255.0 (Serveurs)	**DEFAULT** ▲▼ 🗑️

*Cette règle est utilisé si aucune autre règle personnalisée n'existe ou ne correspond à la situation de l'utilisateur qui fait la requête.*

[<<Règles](#)   [<<Bases](#)

Liste des règles de filtrage

On trouve toujours en haut la règle par défaut, qui est appliquée quand aucune autre règle ne convient.

Ensuite, on trouve les règles créées spécifiques à l'établissement.

Toutes ces règles sont modifiables en cliquant sur l'hyperlien.



## Méthode : Modification des règles de filtrage web

En cliquant sur une règle de filtrage web, on a accès à la page de modification

Nom

**Définition de la source :**

Réseau

Groupe

*L'authentification des utilisateurs n'est pas active.  
Si vous souhaitez créer des filtres en fonction du groupe  
d'appartenance des utilisateurs, il vous faut alors activer  
l'option [Authentification des accès au Web](#).*

**Liste des bases :**

	<input type="button" value="▲"/> <input type="button" value="▼"/>	Bloquer	<b>phishing</b>	(phishing site)
	<input type="button" value="▲"/> <input type="button" value="▼"/>	Bloquer	<b>strict_redirector</b>	(strict anonymizer site)
	<input type="button" value="▲"/> <input type="button" value="▼"/>	Bloquer	<b>strong_redirector</b>	(strong anonymizer site)
	<input type="button" value="▲"/> <input type="button" value="▼"/>	Bloquer	<b>warez</b>	(warez site)
	<input type="button" value="▲"/> <input type="button" value="▼"/>	Bloquer	<b>in-addr</b>	(ip address)
	<input type="button" value="▲"/> <input type="button" value="▼"/>	Laisser_passer	<b>all</b>	(all internet)

*La dernière base est "Tout Internet".  
Si vous souhaitez ajouter d'autres bases de filtrage, il faut d'abord enlever  
cette dernière règle.*

[<<Règles](#)   [<<Bases](#)

### Édition des règles de filtrage web

on peut d'abord modifier le nom de la règle. Ensuite, chaque règle dans le SLIS est associé à un sous-réseau que l'on a la possibilité de choisir ici.

Comme pour la page d'édition des bases de filtrage, il faut bien cliquer sur le bouton modifier après chaque modification.

En dessous apparait la liste des bases. L'ordre ayant son importance dans l'établissement d'une règle (voir le principe de fonctionnement) , on a la possibilité de changer l'ordre des bases grâce aux petites flèches bleues ascendantes et descendantes.

Les petites poubelles permettent de supprimer une base de la règle que l'on est en train d'éditer.

À première vue, il n'est pas possible d'ajouter une base dans la règle. Pour ajouter des bases contenues dans la règle, il faut commencer par supprimer la règle correspondant à tout internet. On voit alors apparaître un ensemble de listes déroulantes pour ajouter une règle.

Bloquer **in-addr**

*Pensez à terminer votre liste de bases par **Laisser\_passer - all**  
(pour un fonctionnement en liste noire) ou par **Bloquer - all**  
(pour un fonctionnement en liste blanche)*

[<<Règles](#)   [<<Bases](#)

### Ajout d'une base dans la règle de filtrage

La première liste déroulante propose le mode d'utilisation de la base : doit on laisser passer ou au contraire bloquer les URLs qui correspondent à cette base.

La seconde colonne propose les bases de filtrage. Il suffit ensuite de cliquer sur le bouton ajouter pour que la base soit ajoutée dans la règle de filtrage.



### Attention : Finir les règles de filtrage

---

Pour que le filtrage soit achevé, il faut absolument terminer la règle de filtrage en disant ce qu'il convient de faire pour "tout internet". On peut laisser passer ou bloquer tout internet.



### Fondamental : Mode listes noires et listes blanches

---

Une règle de filtrage pourra fonctionner sur un modèle de listes blanches ou un modèle de listes noires suivant la terminaison de la règle.

Si la règle s'achève par "Laisser passer tout internet", tout ce qui n'a pas été spécifiquement interdit sera autorisé. On parle alors d'un mode en liste noire : on a une liste "noire" des éléments exclus, les autres sont autorisés.

Si la règle s'achève par "bloquer tout internet", seuls les sites explicitement autorisés pourront être atteints. On parle alors de fonctionnement en liste blanche. C'est un mode de navigation très restrictif.



### Méthode : Valider les modifications

---

Une fois les modifications terminées, elles seront enregistrées en cliquant sur le bouton "valider les modifications".

## D. Cas d'usage du filtrage de sites web

### Quelques cas d'usage du filtrage de sites web

---

On va imaginer un établissement de grande taille et considérer quelques fonctionnements :

- En salle des professeurs, l'accès à internet est assez largement ouvert. En particulier, les enseignants ont accès aux différentes ressources des sites de vidéos (youtube, google vidéo, dailymotion ) dont certaines ont un intérêt pédagogique.
- Au CDI, les machines sont réservées à un usage de recherche. Le filtrage est un peu plus strict : les sites de webmail, les forums, les réseaux sociaux sont interdits. La musique en ligne est bloquée aussi, pour éviter une trop grande consommation de bande passante.
- Il y a pour les internes de l'établissement une salle libre service. Dans cette salle, le filtrage est fait pour préserver la bande passante. Les sites de vidéo et de musique en ligne sont bloqués, mais on laisse l'accès aux webmails et aux réseaux sociaux.
- En salle d'EXAO de physique, le professeur ne veut pas utiliser l'accès internet sauf pour quelques sites bien spécifiques. Cette salle est gérée par une liste blanche, seuls les sites, voire les pages spécifiées par l'enseignant sont accessibles.

Dans tous les cas, les bases de filtrage sont utilisées pour bloquer les sites pornographiques, les sites donnés par adresse IP, les sites xénophobes et violents. Cela permet de se conformer aux obligations légales, et d'empêcher le contournement du filtrage.

On peut encore imaginer d'autres règles de filtrage. Par exemple, les adresses réseaux correspondant à des machines non enregistrées dans le DHCP pourraient être extrêmement filtrées.



## E. Bases prédéfinies dans le SLIS

### Liste des bases prédéfinies dans le SLIS

---

Un certain nombre de bases sont prédéfinies dans le SLIS et correspondent à des bases maintenues au niveau national, par l'université de Toulouse, à la demande du ministère de l'éducation nationale.

Base	Usage
in-addr	Cette base sert à filtrer les sites donnés par adresse IP. Si cette base n'est pas mise, le filtrage est aisément contourné, puisqu'il suffit de remplacer le nom d'un site interdit par son adresse IP !
adult	Les sites à caractère pornographique. Il est indispensable de positionner cette règle dès lors que l'on a des mineurs dans l'établissement.
agressif	Des sites racistes, antisémites et incitant à la haine. Là aussi, il est indispensable de positionner les sites dès lors que l'on a des mineurs dans l'établissement
audio-video	Des sites orientés vers l'audio et la video, surtout le partage de mp3.
dangerous_material	Sites avec des informations sur les explosifs.
drogue	Sites faisant l'apologie et décrivant les méthodes des produits stupéfiants.
forums	Des sites de discussions en ligne.
gambling	Des sites de jeux en ligne.
hacking	Des sites sur le piratage informatique.
mobile-phone	Sites pour les téléphones mobiles (sonneries, etc...).
phishing	Site de hameçonnage. Ces sites cherchent à imiter de vrais sites pour récupérer des identifiants et des mots de passe. Il est fortement recommandé d'interdire cette base.
publicite	Les différents sites connus de publicité. Il est très intéressant d'utiliser cette base pour bloquer les publicités. Cela permet de gagner énormément de bande passante à l'échelle d'un établissement (sur certains sites, les 4/5 du contenus sont des publicités en Flash !).
radio	Les sites de radios sur internet. Ce sont des gros consommateurs de bande passante.
redirector	Les sites qui permettent de contourner le filtrage (proxy public par exemple).
strict_redirector	Comme le filtre redirector, incluant en plus les moteurs de recherche.
strong_redirector	Comme strict_redirector, mais pour les moteurs de recherche, seuls certains

	termes sont bloqués.
tricheur	Sites qui permettent de tricher aux examens.
warez	Sites de logiciels piratés.
webmail	Sites de webmail sur internet. A ne surtout pas bloquer en salle des professeurs !

Ces listes sont maintenues à Toulouse. Si une URL manque dans la liste, ou si une URL est bloquée indument, vous pouvez utiliser l'interface en ligne pour demander une modification des listes :

[http://cri.univ-tlse1.fr/cgi-bin/squidguard\\_modify.cgi](http://cri.univ-tlse1.fr/cgi-bin/squidguard_modify.cgi)

# Configuration de la redirection de services web

## IV

### Introduction

Le SLIS offre via le serveur Apache une possibilité de rediriger les services web. Il fonctionne ainsi en serveur mandataire inverse (reverse proxy en anglais). Cela permet d'héberger au sein de l'établissement des services web qui seront accessibles de l'internet. Les services seront hébergés dans la zone démilitarisée et seront accessibles de façon transparente depuis l'internet.

En outre, la configuration du serveur Apache permet de sécuriser la transmission entre le client de l'internaute et le SLIS en utilisant une transmission cryptée par https, voire en l'imposant.

En conclusion, ce module permet :

- D'héberger des services web dans l'établissement
- De les rendre accessible de façon transparente et aisée
- De sécuriser les connexions en dehors de l'établissement pour des services qui ne le proposeraient pas.

### Présentation de l'interface

L'interface est accessible via le menu du SLIS, dans la partie réseau, en choisissant proxy inverse. Un tableau présente l'ensemble des règles de redirections avec les champs suivants :

- La description de la redirection (optionnelle). A côté de cette description, un cadenas éventuel indique la politique vis à vis de la sécurisation SSL de la connexion.
- L'URL de redirection. C'est vers cette cible que les requêtes seront redirigées.
- La partie hôte virtuel. Elle indique le nom du service qui sera utilisé pour construire l'URL qui sera redirigé. La redirection par hôte virtuel peut être désactivée, auquel cas cette zone est grisée.
- On trouve ensuite la redirection par sous répertoire qu'utilisait les anciennes versions de SLIS. Plus malaisée à utiliser, et source d'erreurs dans certaines applications, cette possibilité est surtout offerte à des fins de compatibilité avec le SLIS 3.2.
- La colonne suivante indique les sources qui sont concernées par la redirection. La redirection peut être activée sur le réseau interne, sur la zone démilitarisée et sur les requêtes venant d'internet.
- Les redirections peuvent être ou non activées, ce qu'indique la colonne d'état.
- Enfin, la dernière colonne contient les boutons qui permettent de modifier la redirection ou de la supprimer.

**Proxy inverse**


### Redirection web

Le trafic http et http sécurisé qui arrive sur le SLIS peut être redirigé vers des serveurs de la zone démilitarisée (DMZ). Ce mécanisme repose sur des noms d'hôtes virtuels ou des noms de sous-répertoires.

[Plus d'information.](#)

**+ Ajouter une redirection**

#### Liste des redirections web

Description	URL proxifiée	Hôte virtuel	Répertoire	Autoriser depuis	État	Modifier / Supprimer
 LCS Web Server	http://192.168.234.6/	 lcs	/	all		 

Interface du serveur mandataire inverse

## Ajout ou modification d'une redirection

**Proxy Inverse**

**Créer une redirection**

**description**  
Description de la redirection

**Source des requêtes**  
Sources permises pour la redirection Réseau pédagogique local (LAN) ⓘ

**Requêtes entrantes**

**Redirection par hôte virtuel**  
Utiliser la redirection par hôte virtuel   
Nom de l'hôte virtuel  ⓘ

Une redirection par hôte virtuel permet aux requêtes demandant un hôte virtuel du slis d'être redirigées, c'est à dire pour un hôte **exemple**, des requêtes demandant `http(s)://exemple.swirly-slis.ac-grenoble.fr/` sont redirigées vers la cible.



**Redirection par sous-répertoire**  
Utiliser la redirection par sous-répertoire   
Sous-répertoire à rediriger  ⓘ

La redirection par sous-répertoire permet à des requêtes pour des sous répertoires d'être redirigées. Si le répertoire est **exemple**, les requêtes demandant des adresses du type `http(s)://swirly-slis.ac-grenoble.fr/exemple/` seront redirigées vers la cible de redirection.

**Cible de la redirection**  
URL distante

**Options SSL**  
Comportement SSL Utiliser les protocoles http et http sécurisé ⓘ

Vous pouvez utiliser le protocole http ou le protocole http sécurisé. Il est possible de forcer l'utilisation du protocole http sécurisé en redirigeant les requêtes arrivant en http vers le https. L'utilisation du https est recommandée. Le forcer sans certificat valide n'est pas recommandé.

 Annuler  Valider

*Ajout ou modification d'une redirection*

On voit dans cette page d'ajout ou de modification d'une redirection l'ensemble des éléments.

En premier lieu, la description de la redirection, qui permettra de l'identifier clairement la redirection dans la page d'accueil.

Ensuite, une liste déroulante propose trois choix pour la source de la redirection :

- Le réseau interne : seules les requêtes du réseau interne seront redirigées vers la cible. Cela permet d'isoler un serveur dans la DMZ tout en le rendant accessible pour le réseau pédagogique.
- Le réseau interne et la zone démilitarisée : même fonctionnement mais valable aussi pour les machines de la DMZ.
- De partout : les requêtes venant d'internet seront aussi redirigées vers la cible.

Viennent ensuite les paramètres de la redirection. On peut utiliser une redirection

par hôte virtuel ou par sous répertoire. Pour chacune, une case à cocher indique l'activation, et un champ permet de saisir le nom de l'hôte virtuel ou du sous répertoire. Par exemple, si le nom de domaine du SLIS est monslis.net, cocher la case "redirection par hôte virtuel" et indiquer machine dans le champ "nom de l'hôte virtuel" permettra de rediriger les requêtes qui demandent `http://machine.monslis.net/` vers la cible.

De la même façon, si on utilise la redirection par sous-répertoire, en cochant la case "utiliser la redirection par sous-répertoire" et en indiquant dans le champs "sous répertoire à rediriger" monrep, les requêtes vers `http://monslis.net/monrep/` seront redirigées vers la cible.

La zone suivante définit la cible, c'est à dire l'adresse vers laquelle seront redirigées les requêtes.

Enfin, la dernière zone propose la politique de gestion de la sécurité du protocole. Trois possibilités sont offertes :

- Ne pas utiliser le protocole http sécurisé. Dans ce cas, seul l'adresse en `http://machine.monslis.net/` sera disponible.
- Utiliser les deux protocoles. Dans ce cas, aussi bien `http://machine.monslis.net/` que `https://machine.monslis.net/` seront disponible. Le protocole https vous garantit un chiffrement des données entre le client et le SLIS. Votre navigateur se plaindra sans doute qu'il n'a pas à disposition un certificat convenable. Cela signifie qu'il ne peut pas certifier que la machine est une machine de confiance validée par une autorité reconnue, mais cela ne diminue en rien le chiffrement du flux de données.
- Enfin, troisième et dernière possibilité, forcer le protocole http sécurisé. Dans ce cas de figure, les requêtes qui utilisent le protocole http seront redirigées vers le protocole sécurisé. Vous êtes ainsi assuré que les flux seront chiffrés. La contrepartie est le risque de voir les personnes ne pas accéder au site du fait des mises en garde au sujet des certificats par le navigateur.



#### Attention : Nom de domaine des hôtes virtuels.

Attention, pour le bon fonctionnement de la redirection par hôte virtuel, il est nécessaire que l'adresse DNS du service corresponde au SLIS. En effet, les requêtes doivent arriver au SLIS. Aussi, il faut que le DNS interne à l'établissement pointe `machine.monslis.net` sur l'IP du SLIS. De même pour le DNS externe. Un avertissement est émis si l'adresse n'est pas celle du SLIS ou si le nom ne correspond à aucune adresse IP.



#### Exemple : Cas d'un serveur de note

Voici donc la procédure à suivre pour rendre accessible depuis l'extérieur un serveur de relais de notes. On prend le cas d'une architecture où le serveur est sur le réseau pédagogique, et on a placé dans la DMZ un relais web.

Tout d'abord, on place le serveur dans la DMZ. Il va falloir ouvrir le pare-feu du SLIS pour le configurer proprement :

- Un accès à internet pour les mises à jours de ce serveur. Cet accès peut se faire via le proxy du SLIS.
- Autoriser l'accès au serveur de note sur le réseau pédagogique.

On ne définit aucun droit entrant vers ce serveur. C'est le SLIS qui sera utilisé comme serveur mandataire inverse (reverse proxy) pour accéder au serveur

Seconde étape, on définit une redirection dans l'interface de serveur mandataire inverse (revers proxy). Les champs pourront être les suivants :

- Description : serveur de notes
- Sources : toutes les sources
- Hôte virtuel activé.

- Nom d'hôte virtuel : note
- Pas d'activation du répertoire
- Cible de redirection : http://IP-dans-la-DMZ/
- Comportement SSL : autoriser le http et le http sécurisé

Dernière étape, vérifier qu'en terme de DNS externe, note.monslis.net corresponde bien au SLIS, ainsi qu'en DNS interne. On pourra en particulier renseigner le nom DNS note dans l'interface DNS du SLIS comme pointant sur le SLIS.

# Délégation de droits simple

V

## Droits spécifiques au SLIS

Il est possible sur le SLIS de déléguer la gestion de certaines parties de l'interface à un utilisateur qui n'est pas administrateur du SLIS. Il existe quatre droits qui permettent un accès à l'interface du SLIS :

- `slis_is_admin` : c'est un droit qui permet à l'utilisateur d'effectuer toutes les tâches d'administration sur le SLIS. Il a le contrôle total du SLIS.
- `slis_nat_is_admin` : ce droit permet à l'utilisateur d'accéder à la redirection temporaire de ports (NAT)
- `slis_blacklists_is_admin` : ce droit permet de contrôler le filtrage web (squidguard) sur le SLIS.
- `slis_subnets_is_admin` : ce droit permet de gérer la programmation horaire par sous-réseaux.



## Méthode : Attribution du droit

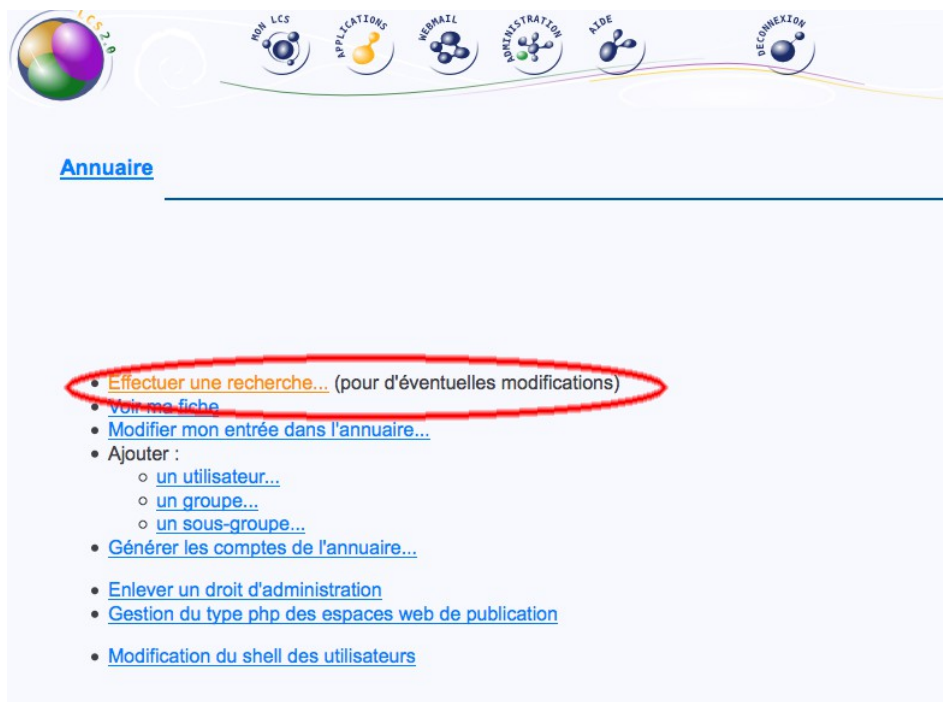
Pour attribuer le droit, il va falloir se connecter au LCS.

En tant qu'administrateur (ou personne avec le droit `lcs_is_admin`) du LCS, il faut se connecter à l'annuaire (application, annuaire des utilisateurs)



*Accès à l'annuaire LCS*

Dans l'annuaire, on va effectuer une recherche pour trouver l'utilisateur auquel on souhaite ajouter les droits.



Effectuer une recherche

On ouvre alors l'interface de recherche, dans laquelle on va pouvoir chercher la personne par son nom, son nom complet (avec le prénom), ou sa classe (pour les élèves)



Interface de recherche de l'annuaire du LCS

Une fois la recherche effectuée et l'utilisateur sélectionné, on a plus qu'à choisir les droits que l'on veut affecter à la personne et à cliquer sur le bouton "ajouter ces droits".

[Annuaire](#) -> [Recherche](#)Délégation de droits à Test Prof (**proft**)

Sélectionnez les droits à supprimer (liste de gauche) ou à

Droits actuels	Droits disponibles
proft n'a aucun droit	se3_js_admin Annu_js_admin sovaJon_js_admin system_js_admin computers_js_admin lcs_js_admin slis_js_admin stats_can_read lcs_js_superuseradmin slis_subnets_js_admin slis_blacklists_js_admin slis_nat_js_admin
	<input type="button" value="Ajouter ces droits"/>

*Ajout d'un droit dans LCS*