J-EOLE

Dijon

18 et 19 octobre 2012

Nouveautés Amon 2.3

Plan

- LightSquid
- Observatoire des navigations
- WPAD
- Double authentification
- Agrégation de liens ADSL

LightSquid

LightSquid

Qu'est-ce que LightSquid ?

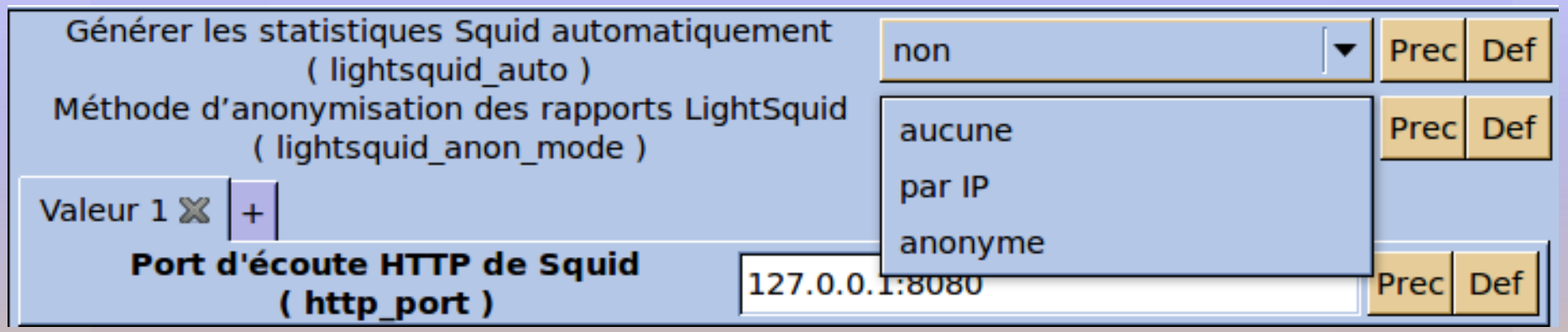
LightSquid est un analyseur de logs
pour le proxy/cache Squid.

Site de référence : *http://lightsquid.sourceforge.net/*

LightSquid

Configuration EOLE

Onglet Squid en mode *expert* :



LightSquid

Consultation EAD

- action proposée pour le rôle « admin »
- accès à un cgi local sur le port : 8062

=> limitations

- réauthentification nécessaire en mode "pam"
- accès impossible *via* un frontend EAD distant

LightSquid

pf-amon | Scribe

VOUS ÊTES CONNECTÉ(E) EN TANT QUE ADMIN Déconnexion

Consultation EAD

STATISTIQUES SQUID

Squid rapport d'accès utilisateur

Periode de travail: Oct 2012

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

Top Sites	Total	Groupe
ANNEE	ANNEE	ANNEE
MOIS	MOIS	MOIS

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

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

LightSquid

Consultation EAD

STATISTIQUES SQUID

Squid rapport d'accès utilisateur

Top Sites

Periode de travail: **Tout MOIS - 2012 Oct**

		Site(s) Accédé(s)	Connexion(s)	Octets	%
1	qui	www.google.fr	16 908	146.5 M	0.8%
2	qui	safebrowsing-cache.google.com	10 501	521.4 M	2.9%
3	qui	sweb.in.ac-dijon.fr	9 473	174.9 M	0.9%
4	qui	www.quizz.biz	9 042	63.1 M	0.3%
5	qui	bp-eole.ac-dijon.fr	7 178	3.2 M	0.0%
6	qui	www.lesite.tv	6 998	58.7 M	0.3%
7	qui	leparc.ac-dijon.fr:443	6 719	203.7 M	1.1%
8	qui	www.google-analytics.com	6 501	6.7 M	0.0%
9	qui	housefb.sng.ubi.com:443	6 484	4.6 M	0.0%
10	qui	upload.wikimedia.org	6 208	63.1 M	0.3%
11	qui	sketchup.google.com	4 949	151.6 M	0.8%
12	qui	profile.ak.fbcdn.net	4 706	11.8 M	0.0%
13	qui	googleads.g.doubleclick.net	4 129	20.8 M	0.1%
14	qui	www.facebook.com	4 118	23.4 M	0.1%
15	qui	www.google.com	4 012	199.5 M	1.1%
16	qui	www.bienpublic.com	3 898	14.2 M	0.0%
17	qui	clients1.google.com	3 673	2.0 M	0.0%
18	qui	kh.google.com	3 091	31.2 M	0.1%
19	qui	front-aggregator.lpn.fr	2 877	9.4 M	0.0%
20	qui	pagead2.googlesyndication.com	2 839	47.1 M	0.2%
21	qui	cbk0.google.com	2 647	54.6 M	0.3%
22	qui	bits.wikimedia.org	2 575	14.9 M	0.0%
23	qui	static.ak.fbcdn.net	2 491	38.9 M	0.2%
24	qui	10.121.58.5	2 326	4.5 M	0.0%
25	qui	i.ytimg.com	2 220	26.6 M	0.1%

LightSquid

Consultation EAD

Squid rapport d'accès utilisateur

Rapport des Gros Fichiers Downloadés

Date: 05 Oct 2012

Utilisateur: 172.16.0.105

#	Temps	Utilisateur	Taille	URL
1	09:53:56	172.16.0.105	35.5 M	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.0/fr_FR/AdbeRdr950_fr_FR.exe
2	09:54:00	172.16.0.105	4.7 M	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
3	09:54:05	172.16.0.105	4.8 M	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.2/misc/AdbeRdrUpd952_all_incr.msp
4	09:57:07	172.16.0.105	3.9 M	http://definitionupdates.microsoft.com/download/DefinitionUpdates/VersionedSignatures/AM/1.137.1152.0/amd64/mpas-fe_bd.exe
5	10:00:27	172.16.0.105	47.9 M	http://ardownload.adobe.com/pub/adobe/reader/win/10.x/10.1.4/fr_FR/AdbeRdr1014_fr_FR.exe
6	11:36:05	172.16.0.105	8.5 M	http://studentsdownload.autodesk.com/SWDLDDLM/2013/INVNTOR/ESD/Autodesk_Inventor_2013_French_Win_64bit.exe?__gda__=1349861725_afab38f409c5d1f584969a61dde8065a&ext=.exe
7	11:36:46	172.16.0.105	19.5 M	http://studentsdownload.autodesk.com/SWDLDDLM/2013/INVNTOR/WI/Autodesk_Inventor_2013_French_Win_64bit_wi_fr-FR_Setup1.exe
8	12:36:58	172.16.0.105	9.2 M	emsfs.autodesk.com:443
9	12:39:51	172.16.0.105	10.4 M	a248.e.akamai.net:443
10	13:28:54	172.16.0.105	3.4 G	http://studentsdownload.autodesk.com/SWDLDDLM/2013/INVNTOR/DLM/Autodesk_Inventor_2013_French_Win_64bit_dlm.tar.lzma2?%B8tH%02%C4
		TOTAL	3.5 G	

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

LightSquid

Évolutions prévues

- Traitement de plusieurs fichiers et/ou
  choix des fichiers de logs à analyser (#3913)
(actuellement : /var/log/rsyslog/local/squid/squid1.info.log)

- Ajout dans les documentations officielles 2.3 (#3411)

Observatoire des navigations

Observatoire des navigations

De quoi s'agit-il ?

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

Il existe depuis très longtemps.

Observatoire des navigations

Nouveauté

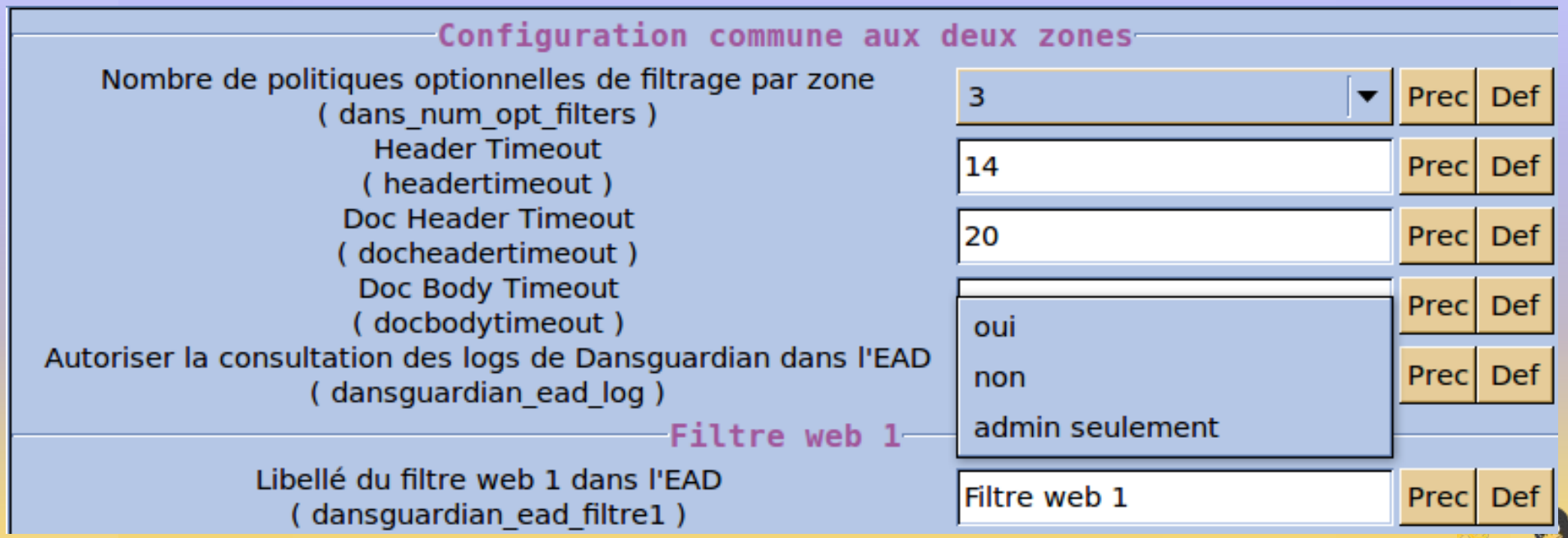
La nouveauté concerne la mise en place de restrictions quant à son utilisation !

- vieux débat sur la légalité de la consultation des logs
- politiques de responsabilisation académiques

Observatoire des navigations

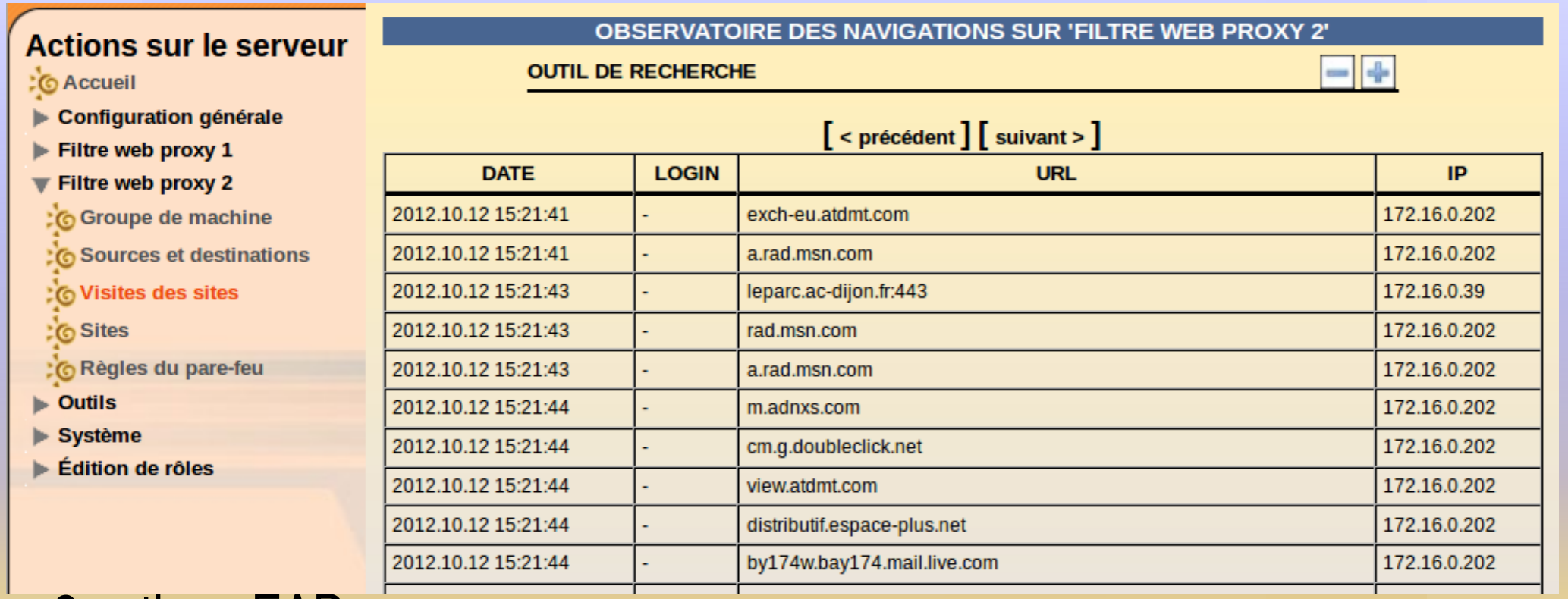
Configuration EOLE

Onglet Dansguardian en mode *expert* :



Observatoire des navigations

Rappel EAD



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

2 actions EAD :

- navigation_visit_admin
- navigation_visit_pedago

WPAD

WPAD

Qu'est-ce que WPAD ?

WPAD : Web Proxy Autodiscovery Protocol

Principe :
- téléchargement du fichier : wpad.<domaine>/wpad.dat
- Nginx distribue le fichier associé au sous-réseau

Exceptions :
- 127.0.0.1
- réseau local

WPAD

Configuration EOLE

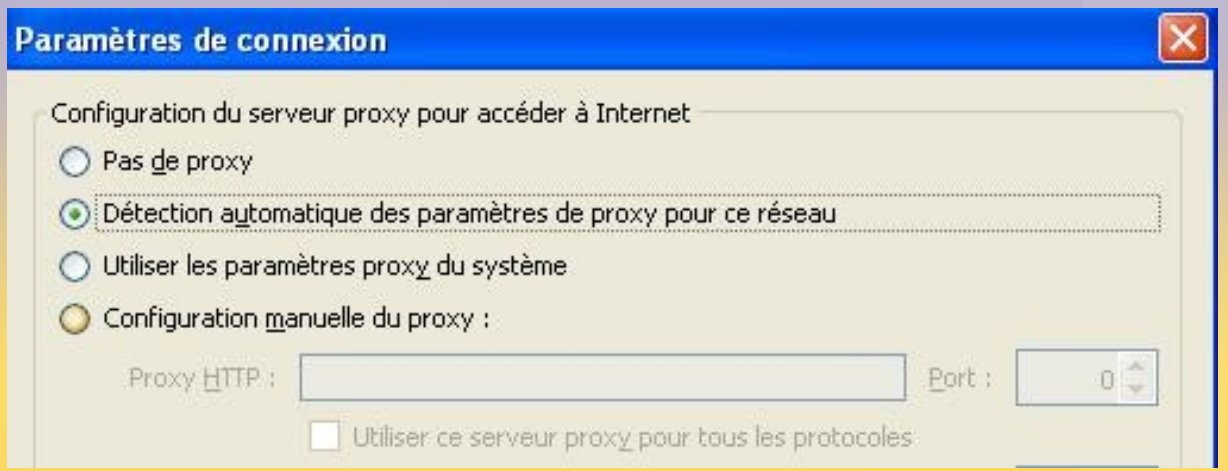
La configuration est automatique !

WPAD

Cas pratique

Avant...

Puis...



WPAD

Cas pratique

=> Après !

WPAD

Configuration des navigateurs

La détection automatique du proxy peut être imposée par :

- Esu/client Scribe
- Gaspacho

Double authentification

Double authentification

Problématique

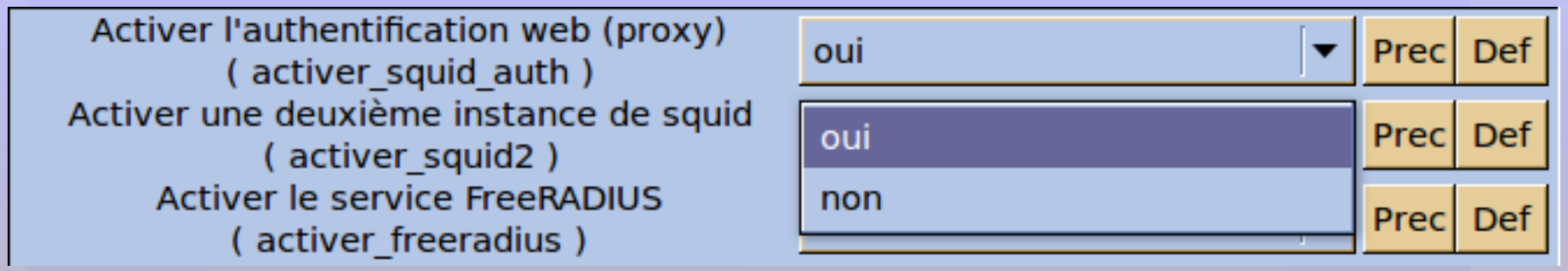
Pouvoir configurer 2 types distincts d'authentification proxy
Par exemple : SMB et LDAP

Dysfonctionnements constatés avec la configuration de base
=> utilisation de 2 instances de squid

Double authentification

Configuration EOLE 1/4

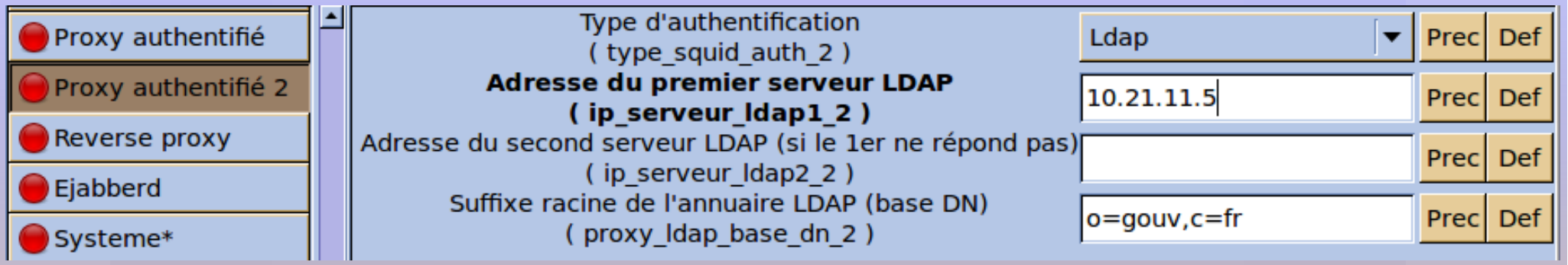
1. Onglet Authentification



Double authentification

Configuration EOLE 2/4

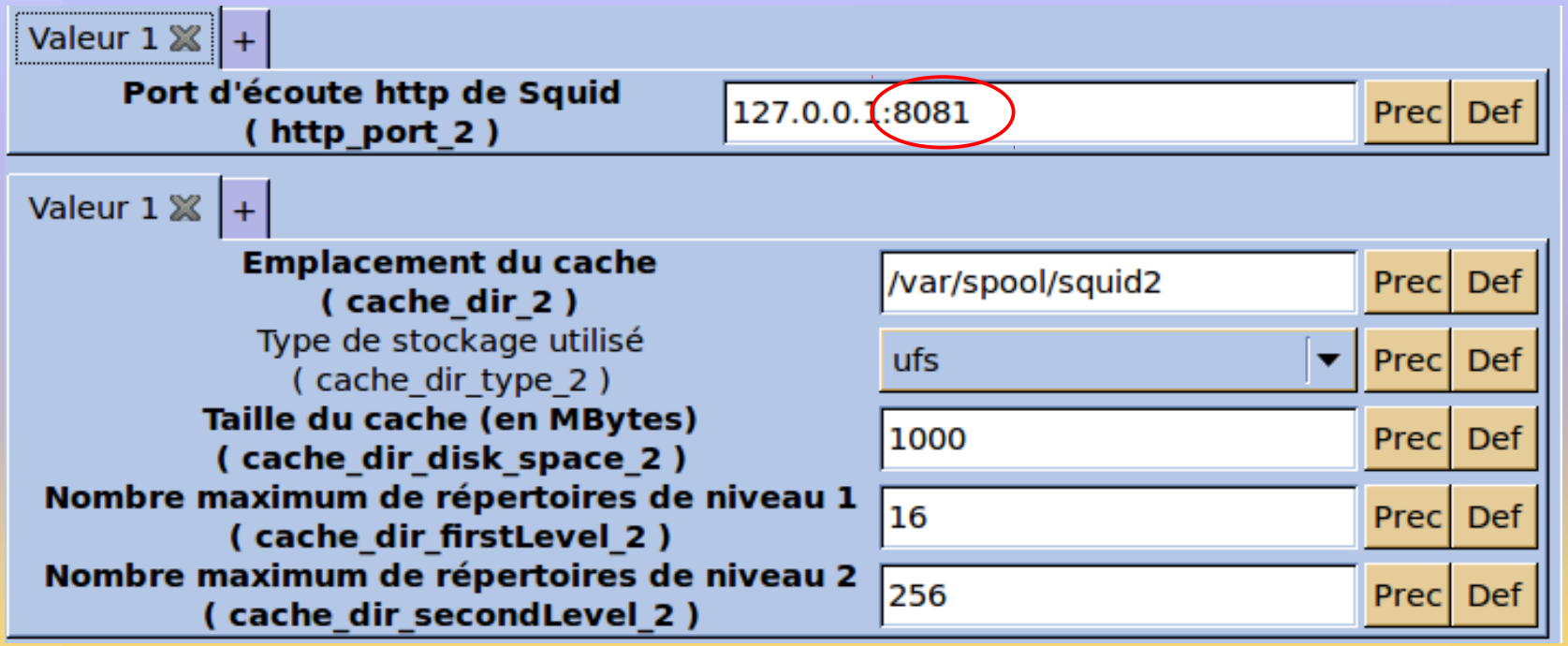
2. Onglet Proxy authentifié 2



Double authentification

Configuration EOLE 3/4

3. Onglet Squid2 en mode *expert* :

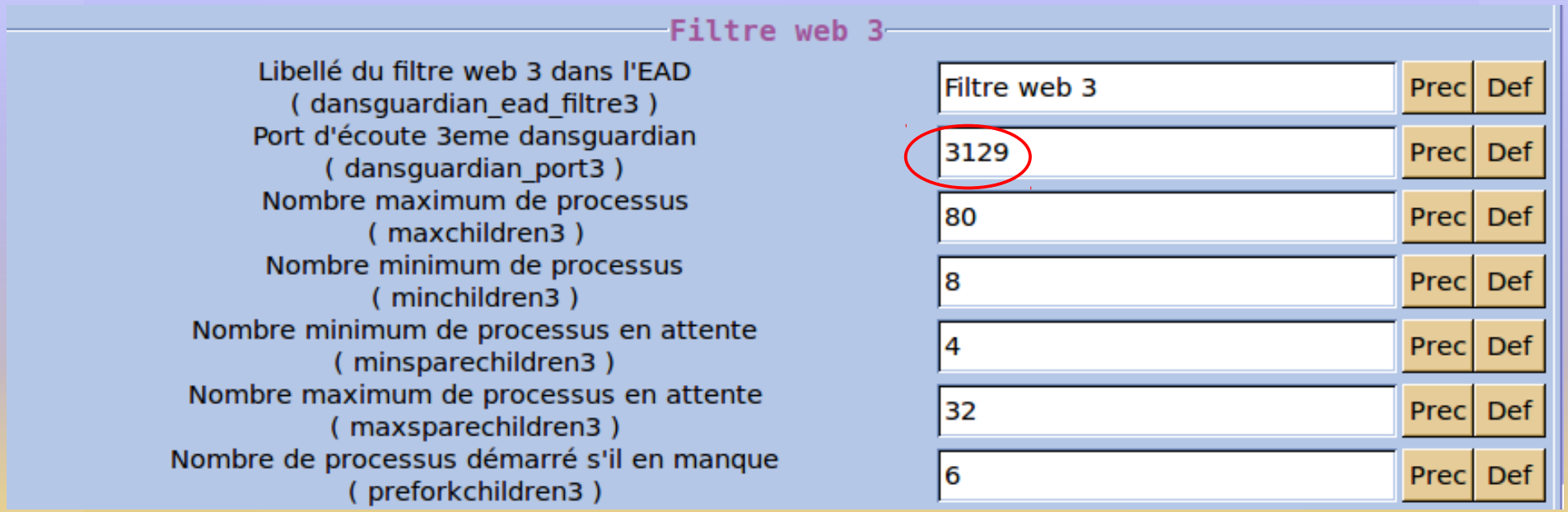


Port spécifique : 8081 (contre 8080)

Double authentification

Configuration EOLE 4/4

4. Onglet Dansguardian en mode *expert* :



Port spécifique : 3129 (contre 3128)

Double authentification

Autres modifications

Fichiers de logs spécifiques à la 2de instance :

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

Double authentification

Autres modifications

Découpage des fichiers de configuration (parties communes et spécifiques) :

- squid.conf *(01squid.conf)* ou squid2.conf *(02squid.conf)*
- common-squid1.conf
- 01inc-squid.conf ou 02inc-squid.conf
- common-squid2.conf

Double authentification

Limitations actuelles

- pas de WPAD pour le second proxy
- logs non consultables *via* l'EAD

Agrégation de liens ADSL

Agrégation de liens ADSL

De quoi s'agit-il ?

L'agrégation de liens permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

Contribution de plusieurs collègues en académie : Versailles, Nantes, Lyon, …

Agrégation de liens ADSL

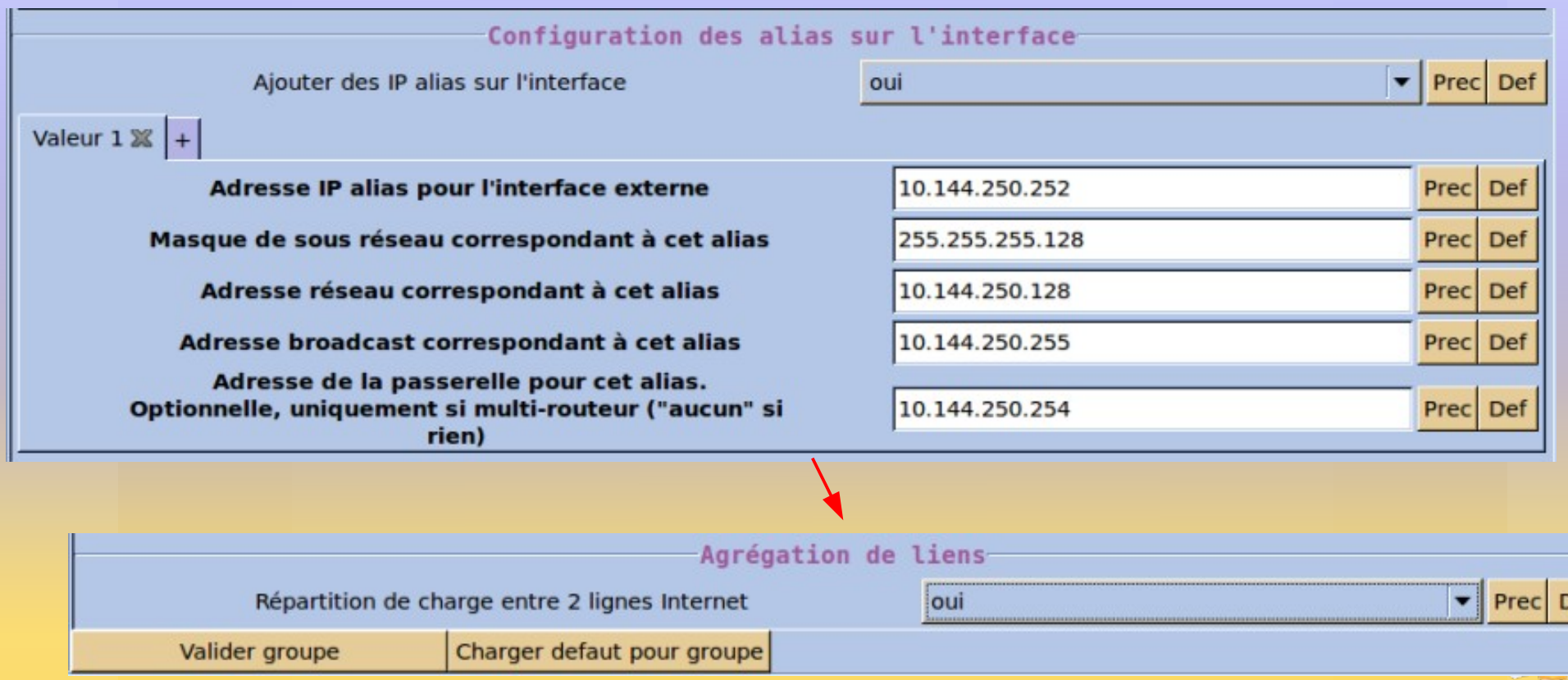
Nouveautés

- choix du mode : load balancing ou fail-over
- envoi de mail sur l'état des liens
- configuration des destinations réseaux forcées
- ajout des routes locales dans les tables T1 et T2

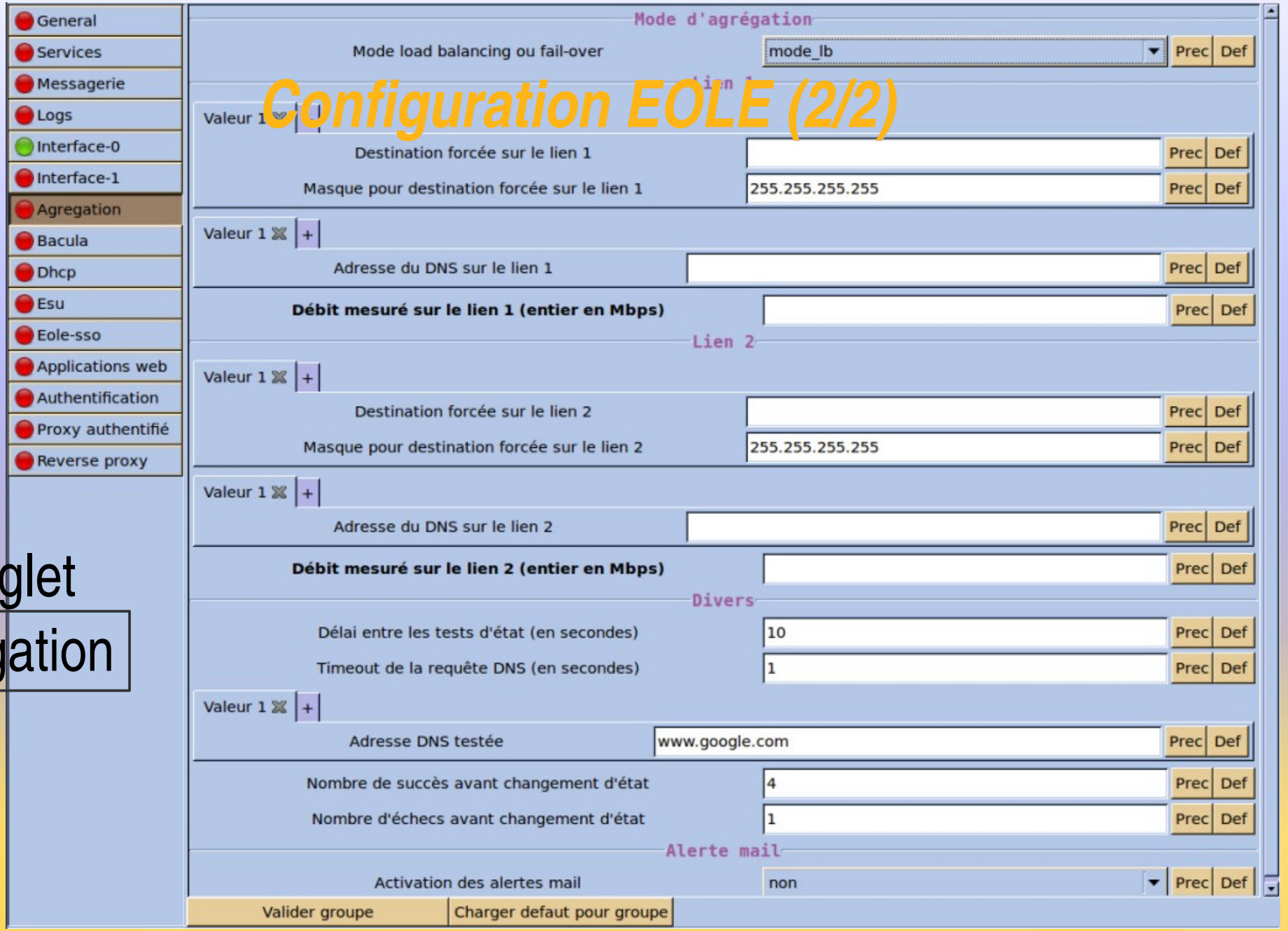
Agrégation de liens ADSL

Configuration EOLE (1/2)

1. Onglet Interface-0



Agrégation de liens ADSL



2. Onglet Agregation

Agrégation de liens ADSL

Documentation

La documentation 2.3 a été mise à jour :
http://eoleng.ac-dijon.fr/pub/Documentations/manuels/2.3/partielles/HTML/Agregation/co/Agregation.htm

Merci de votre attention