Open-Source Web-SSO of the french administrations

OW2 Consortium

What is « Gendarmerie Nationale »

- 4300 agencies *(300 overseas)*
- 105000 users
- 1 private network connecting all agencies
- 2 datacenters

OW2 Consortium

What is Lemonldap::NG

- A powerful distributed Web-SSO system :
  - an assembly of well tested open-source libraries
  - based on ModPerl API to run inside Apache
- It centrally manages authentication, user's attributes propagation and access control
- It includes a sophisticated access rights management

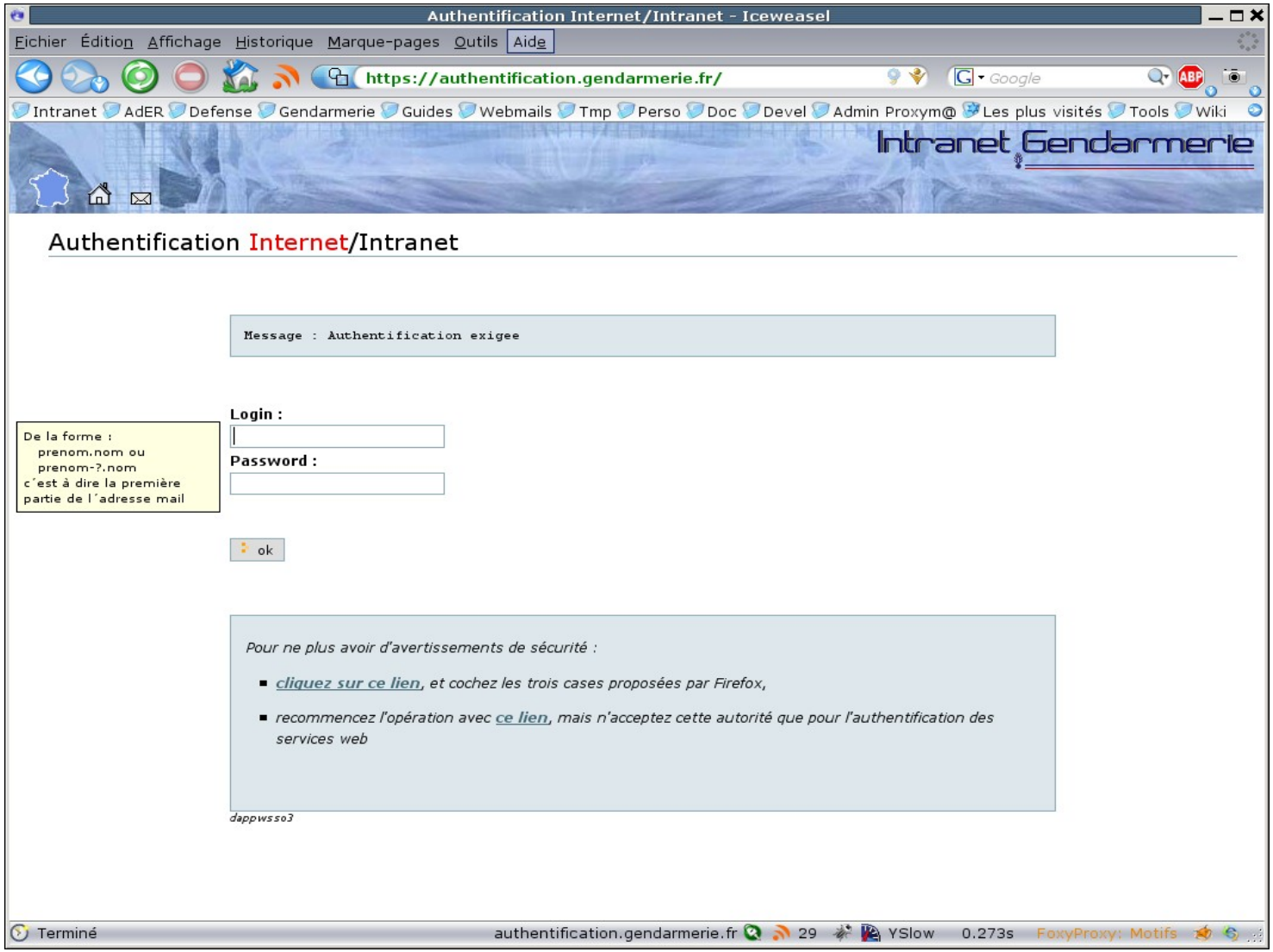
History of the project

- **2002 : First Web-SSO launched on the Gendarmerie's network**
- **2003 : Lemonldap developed by the Ministry of finance**
- **2004 : Studies to replace existing Gendarmerie's Web-SSO**
- **2005 : Lemonldap::NG developped and deployed by Gendarmerie**
- **2006 : Lemonldap::NG is chosen by Feder-Id project to become a Liberty-Alliance Service Provider**
- **2009 : Gendarmerie is funding the SAML-2 extension**

Lemonldap::NG on the Gendarmerie's network

- 105.000 users
- average of 40,000 sessions at the same time
- about 100 protected applications (98% of the whole) among which :
  - all specific applications (J2EE and PHP)
  - SAP
  - Fudforum
  - Mediawiki
  - Sympa management interface
  - Nagios *(all applications based on Apache htaccess)*
  - ...

Feedback and use cases



OW2 Consortium

Double cookie

- Separated protection for HTTP and HTTPS connections, so that less secured applications don't weaken the other ones

---

```
POST / HTTP/1.1
Host: authentification.gendarmerie.fr

HTTP/1.x 200 OK
Date: Tue, 24 Mar 2009 14:18:08 GMT
Server: Apache
Set-Proxy-Cookie: lmproxy=4c640e7ff9450bd3cc65c069f3fa920e; \
                  domain=gendarmerie.fr; path=/
Set-Cookie: lemonldap=d8a6a10a88bcfcdddd4906ad55119ad2; \
                  domain=gendarmerie.fr; path=/; secure
Set-Cookie: lemonldaphttp=ae92a75d4c15dd3d5eae40ce386594e7; \
                  domain=gendarmerie.fr; path=/
...
```

OW2 Consortium

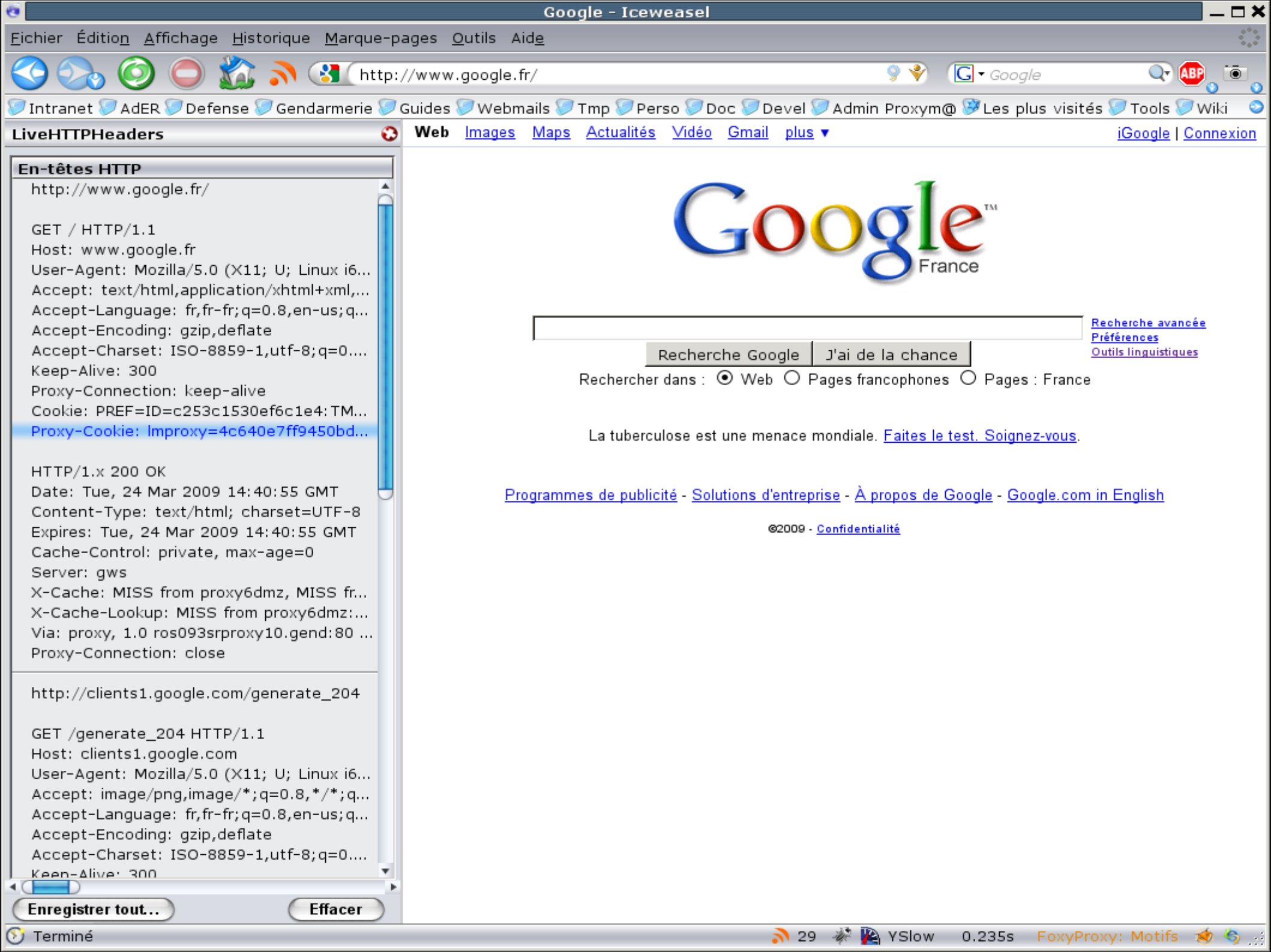
Internet authentication

- « Proxy-Cookie » enables the Single-Sign-On to control the access to Internet

---

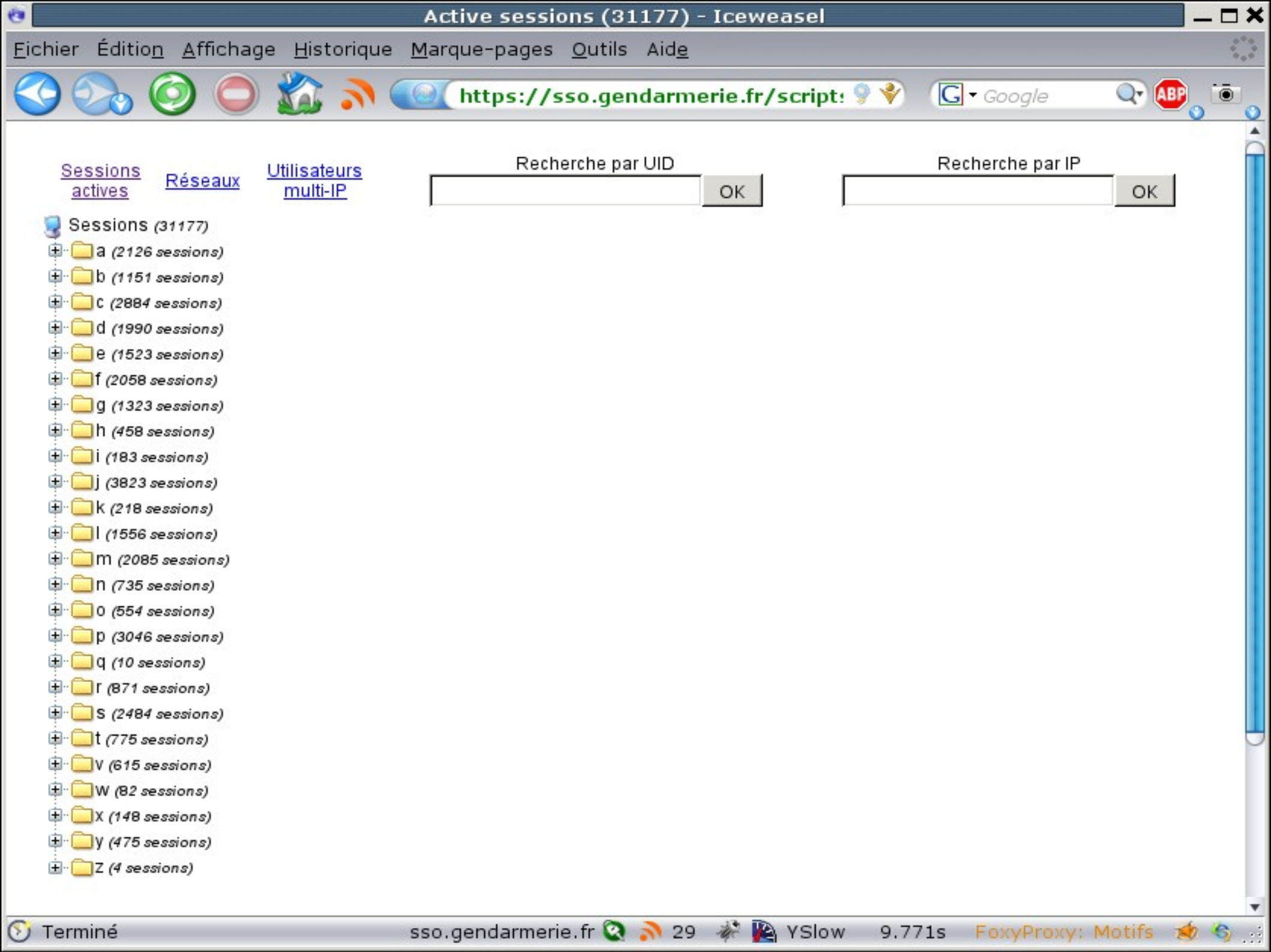
```
POST / HTTP/1.1
Host: authentification.gendarmerie.fr

HTTP/1.x 200 OK
Date: Tue, 24 Mar 2009 14:18:08 GMT
Server: Apache
Set-Proxy-Cookie: lmproxy=4c640e7ff9450bd3cc65c069f3fa920e; \
                  domain=gendarmerie.fr; path=/
Set-Cookie: lemonldap=d8a6a10a88bcfcdddd4906ad55119ad2; \
                  domain=gendarmerie.fr; path=/; secure
Set-Cookie: lemonldaphttp=ae92a75d4c15dd3d5eae40ce386594e7; \
                  domain=gendarmerie.fr; path=/
...
```

OW2 Consortium


Google - Iceweasel
Fichier Édition Affichage Historique Marque-pages Outils Aide
http://www.google.fr/
Google
Intranet AdER Defense Gendarmerie Guides Webmails Tmp Perso Doc Devel Admin Proxym@ Les plus visités Tools Wiki
LiveHTTPHeaders
En-têtes HTTP
http://www.google.fr/
GET / HTTP/1.1
Host: www.google.fr
User-Agent: Mozilla/5.0 (X11; U; Linux i6...
Accept: text/html,application/xhtml+xml,...
Accept-Language: fr,fr-fr;q=0.8,en-us;q...
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0....
Keep-Alive: 300
Proxy-Connection: keep-alive
Cookie: PREF=ID=c253c1530ef6c1e4:TM...
Proxy-Cookie: lmproxy=4c640e7ff9450bd...
HTTP/1.x 200 OK
Date: Tue, 24 Mar 2009 14:40:55 GMT
Content-Type: text/html; charset=UTF-8
Expires: Tue, 24 Mar 2009 14:40:55 GMT
Cache-Control: private, max-age=0
Server: gws
X-Cache: MISS from proxy6dmz, MISS fr...
X-Cache-Lookup: MISS from proxy6dmz:...
Via: proxy, 1.0 ros093srproxy10.gend:80 ...
Proxy-Connection: close
http://clients1.google.com/generate_204
GET /generate_204 HTTP/1.1
Host: clients1.google.com
User-Agent: Mozilla/5.0 (X11; U; Linux i6...
Accept: image/png,image/*;q=0.8,*/*;q...
Accept-Language: fr,fr-fr;q=0.8,en-us;q...
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0....
Keep-Alive: 300
Enregistrer tout...
Effacer
Web Images Maps Actualités Vidéo Gmail plus ▾
iGoogle | Connexion
Google France
Recherche avancée
Préférences
Outils linguistiques
Recherche Google
J'ai de la chance
Rechercher dans : Web Pages francophones Pages : France
La tuberculose est une menace mondiale. Faites le test. Soignez-vous.
Programmes de publicité - Solutions d'entreprise - À propos de Google - Google.com in English
©2009 - Confidentialité
Terminé
29
YSlow
0.235s
FoxyProxy: Motifs

Performances

- Overhead of 3ms per hit
- Average of 40.000 sessions at the same time
- servers can check more than 3000 queries by minutes without any slowdown


Active sessions (31177) - Iceweasel
Fichier Édition Affichage Historique Marque-pages Outils Aide
https://sso.gendarmerie.fr/script
Google
Sessions actives
Réseaux
Utilisateurs multi-IP
Recherche par UID
OK
Recherche par IP
OK
Sessions (31177)
a (2126 sessions)
b (1151 sessions)
c (2884 sessions)
d (1990 sessions)
e (1523 sessions)
f (2058 sessions)
g (1323 sessions)
h (458 sessions)
i (183 sessions)
j (3823 sessions)
k (218 sessions)
l (1556 sessions)
m (2085 sessions)
n (735 sessions)
o (554 sessions)
p (3046 sessions)
q (10 sessions)
r (871 sessions)
s (2484 sessions)
t (775 sessions)
v (615 sessions)
w (82 sessions)
x (148 sessions)
y (475 sessions)
z (4 sessions)
Terminé
sso.gendarmerie.fr
29
YSlow
9.771s
FoxyProxy: Motifs

Development environment

- Principles :
  - developers must have a valid account (the « real user's account »)
  - they can choose any other account (the « spoofed user's account ») to test access control
  - accounting and access rules involve both spoofed user's and real user's attributes

Portail d'authentification - Iceweasel

Fichier Édition Affichage Historique Marque-pages Outils Aide

https://authentification.ppgendarmerie.fr/

Intranet AdER Defense Gendarmerie Guides Webmails Tmp Perso Doc Devel Admin Proxym@ Les plus visités Tools

Authentification exigée

Authentification pré-production

Vous devez vous authentifier avec votre compte intranet. Le champ *"Identifiant souhaité"* peut être utilisé pour prendre les droits d'un autre utilisateur.

Identifiant

Mot de passe

Identifiant souhaité

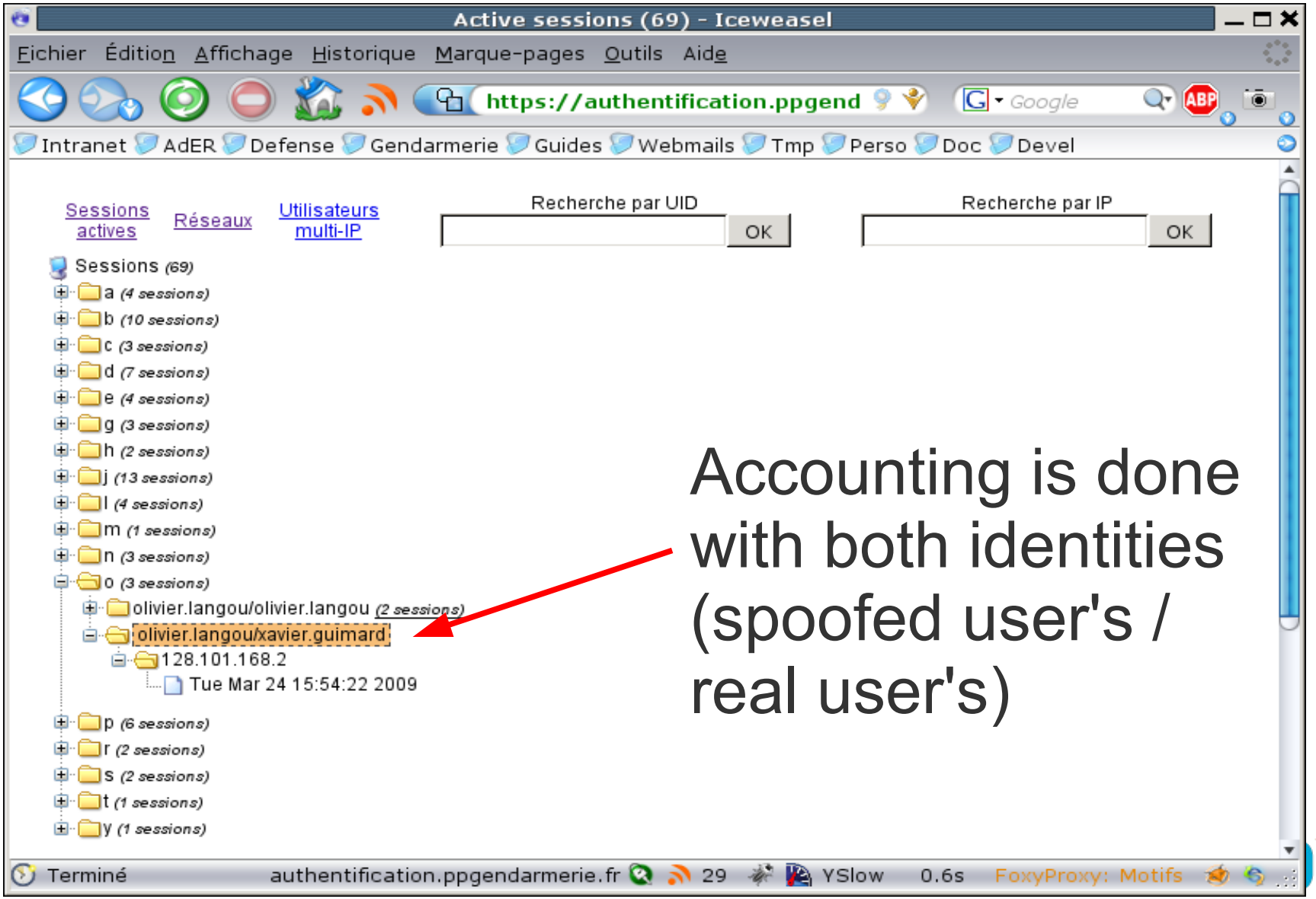
Se connecter Annuler

W3C XHTML 1.0 W3C CSS

Terminé authentification.ppgendarmerie.fr 29 YSlow 0.411s FoxyProxy: Motifs

OW2 Consortium

Session Explorer

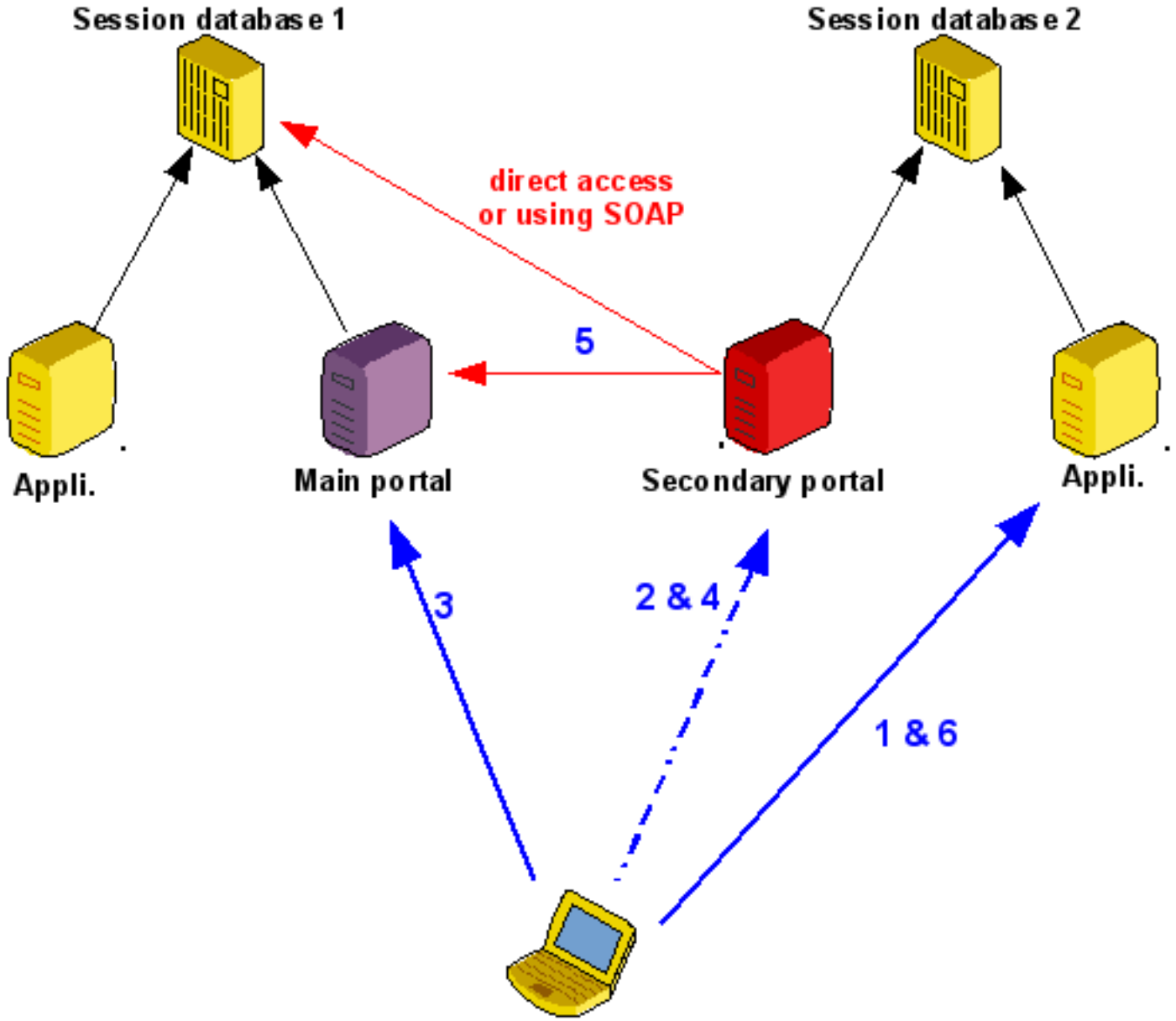


Accounting is done with both identities (spoofed user's / real user's)

Sharing authentication with remote applications

- Extending the core environment with additional features to enable sharing of authentication with remote applications :
  - only a short list of attributes is exported to remote applications

Principles


Session database 1
Session database 2
direct access
or using SOAP
5
Appli.
Main portal
Secondary portal
Appli.
3
2 & 4
1 & 6

Client-Server over HTTP

- LemonIdap::NG provides 2 ways to control access from non-browser clients :
  - SOAP authentication : the client gets a cookie with a SOAP request, then uses the cookie as a normal browser
  - HTTP Auth-Basic authentication : the application is protected by an agent *(handler)* which requests the portal by SOAP using user/password transmitted by the client (by Auth-Basic mechanism) :
    - authorization still uses LemonIdap::NG rules

Conclusion

- Cost of the project (for the Gendarmerie) :
  - 4 servers
  - 4 months of work for 1 developper
- Result :
  - a flexible and suitable solution

Any questions ?