

# Configuration de la messagerie électronique

Elisabeth Piotelat

http://perso.limsi.fr/zabeth

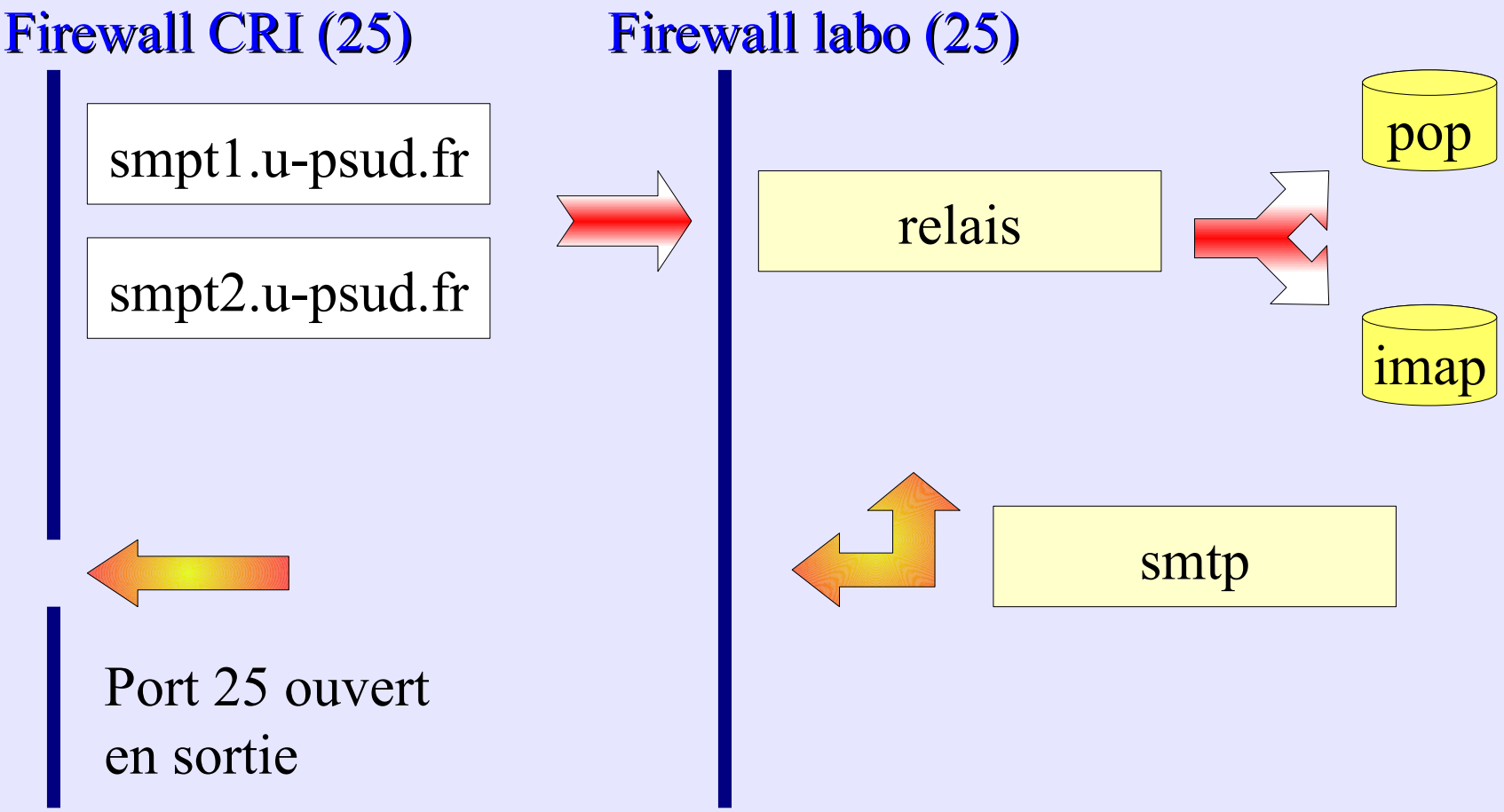
# Plan



- Configuration actuelle
- Mail interne
  - Exemple de configuration sendmail
  - Serveurs pop/imap
  - Filtrage (mailscanner, sendmail, spamassassin)
- Configuration / CRI
  - Solutions en cas de panne : sécurisée / tmp

# Configuration actuelle (schéma)

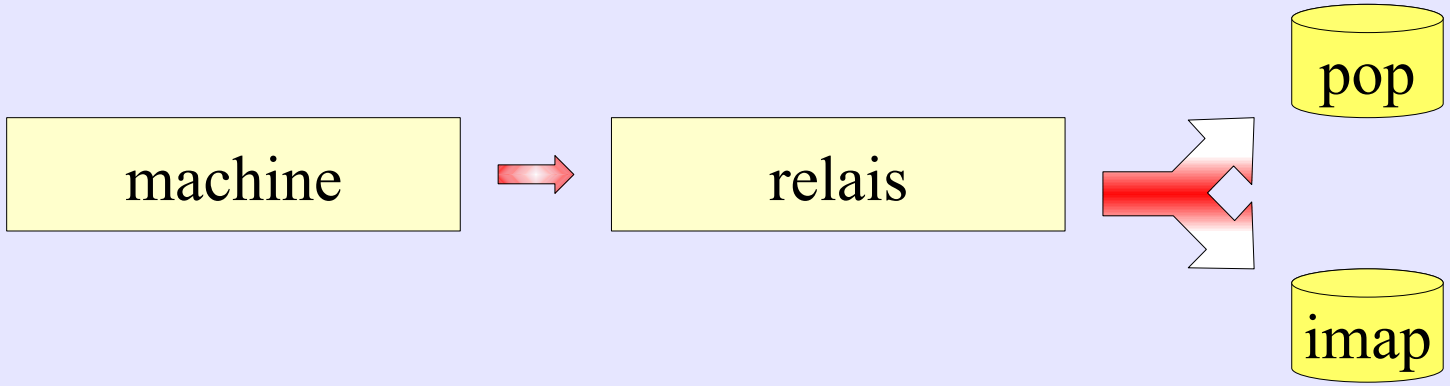




# Mail interne 1/2



- Pour la plupart des machines, c'est le relais qui gère le mail.
  - Host -t MX machine.limsi.fr
  - machine.limsi.fr mail is handled by 10 relais.limsi.fr



# Mail interne 2/2



- Configuration DNS
  - Machine IN MX 10 relais.labo.fr.
  - Serveur IN MX 10 serveur.labo.fr.
- Configuration sendmail/postfix/exim
  - Pas indispensable sur les machines
  - Sur les serveurs (web, dns, imprimante) :
    - Supprimer le nom du serveur
    - Sauf pour certains utilisateurs (root, www-data)
    - Renvoyer les messages vers le relais

# Exemple sendmail.mc



http://perso.limsi.fr/zabeth/sendmail/

```
dnl # Masquerading options
dnl #FEATURE(`always_add_domain')dnl
dnl #Pour que l'adresse email soit en @labo.fr et pas @machine.labo.fr
MASQUERADE_AS(`labo.fr')dnl
```

```
dnl #Le nom de la machine doit apparaître pour certains utilisateurs
EXPOSED_USER(`root,sympa,www-data')dnl
```

```
dnl #On renvoie vers relais.labo.fr
define(`SMART_HOST', `relais.labo.fr')dnl
Cwlists.labo.fr,www.labo.fr,machine.labo.fr
```

# Serveurs pop/imaps



- Pop
  - Pour les stagiaires (configuration rapide)
  - Pour les utilisateurs d'Eudora
- Imaps
  - 220 utilisateurs (permanents, doctorants)
  - Webmail

# MailScanner



- Uvscan : antivirus
- filename.rules
  - Récupération des fichiers bloqués par protocole http (TD en .exe, noms de fichiers à rallonge)
  - Eventuellement filtrage antispam (mp5.jpg)
- Whiteliste

# Sendmail : Liste noire



- /etc/mail/access
  - Recherche de suspects
    - Grep « is spam » /var/log/mail.log
    - Wc -l
  - Surveillance derniers domaines ajoutés
  - Utilisateurs peuvent réagir rapidement
  - En début de mois :
    - suppression des domaines gentils (<90 messages)
    - Passage REJECT > DISCARD

# Exemple : recherche de suspects



| Domaine | Total | Détail | | | | | | | MX |
|---|---|---|---|---|---|---|---|---|---|
| **listserv.linguistlist.org** | 217 | 29 | 31 | 15 | 16 | 31 | 58 | 37 | listserv.linguistlist.org. |
| **compuserve.com** | 48 | 7 | 5 | 7 | 8 | 9 | 8 | 4 | mail.mx4.compuserve.com. |
| **solid.phys.ethz.ch** | 37 | 4 | 14 | 2 | 12 | 0 | 2 | 3 | phys.ethz.ch. |
| **cavani.net** | 36 | 6 | 5 | 14 | 9 | 1 | 1 | 0 | mediaweb.msw.it. |
| **geocities.com** | 34 | 8 | 3 | 3 | 7 | 6 | 4 | 3 | d.mx.mail.yahoo.com. |
| **stinkkiller.com** | 34 | 9 | 4 | 9 | 6 | 3 | 3 | 0 | smtp.secureserver.net. |
| **usd235.org** | 34 | 8 | 6 | 6 | 9 | 4 | 1 | 0 | mail.usd235.org. |
| **intuition-eunetwork.net** | 33 | 4 | 8 | 4 | 5 | 5 | 4 | 3 | mail.ans.gr. |
| **juanrreyes.com** | 33 | 9 | 6 | 7 | 8 | 1 | 1 | 1 | mail-incoming.gate.com. |
| **n3rds.com** | 31 | 10 | 6 | 7 | 7 | 1 | 0 | 0 | mail.n3rds.com. |
| **ctnc.org** | 30 | 6 | 7 | 9 | 7 | 1 | 0 | 0 | mail.ctnc.org. |
| **ebay.fr** | 30 | 0 | 0 | 0 | 0 | 0 | 0 | 30 | gort.ebay.com. |
| **karlahouse.com** | 30 | 6 | 6 | 8 | 4 | 5 | 1 | 0 | inbound.karlahouse.com.n[illegible]solmail.net. |
| **wglz.com** | 29 | 8 | 2 | 7 | 6 | 2 | 2 | 2 | smtp.secureserver.net. |
| **cabaces.org** | 28 | 0 | 2 | 25 | 1 | 0 | 0 | 0 | |
| **btu.unesp.br** | 27 | 0 | 4 | 0 | 5 | 9 | 0 | 9 | servmail.btu.unesp.br. |

# Spamassassin



- Filtres baysiens
- Fichier local.cf mis à jour « de temps en temps »
- http://perso.limsi.fr/zabeth/spam/local.cf

# Intérêt de cette configuration



- Rapidité de l'échange de mails en interne
  - Pas de firewall à traverser
  - Contrôle des délais
- Développements possibles (appli web)
- Echanges internes indépendants du CRI
- Possibilité d'envoyer du mail à l'extérieur pour signaler un problème

# Coopération / CRI



- Pas d'attaque directe : (whois limsi.fr)

| | |
|---|---|
| **Serveurs DNS :** | dns1.dns.u-psud.fr<br>dns2.dns.u-psud.fr |
| **Serveur(s) mail :** | smtp2.u-psud.fr<br>smtp1.u-psud.fr |

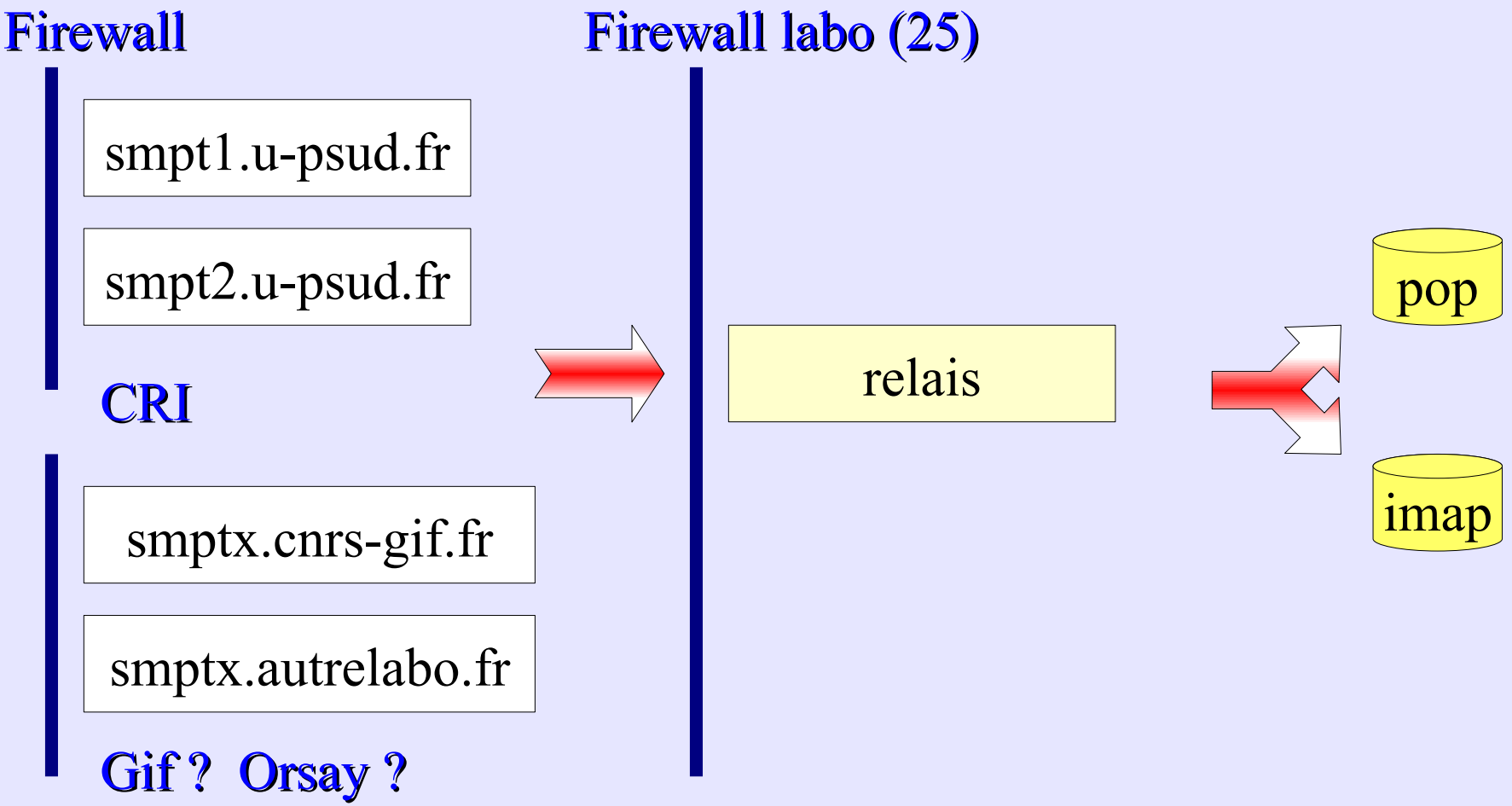
- Flux réduit (user unknown)

- Filtrage aléatoire (antivirus)

- Dépendance en cas de panne (onduleur)

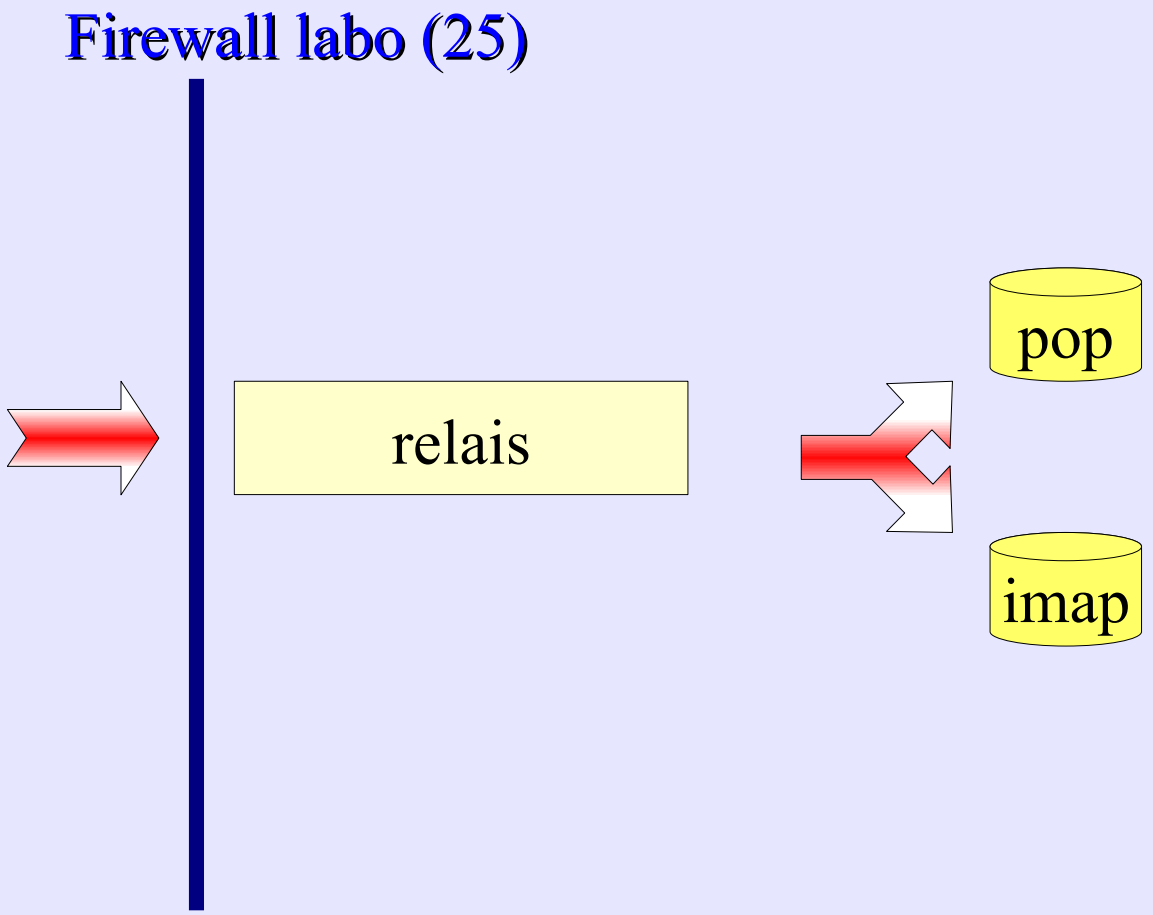
# Solution sécurisée





# Solution temporaire

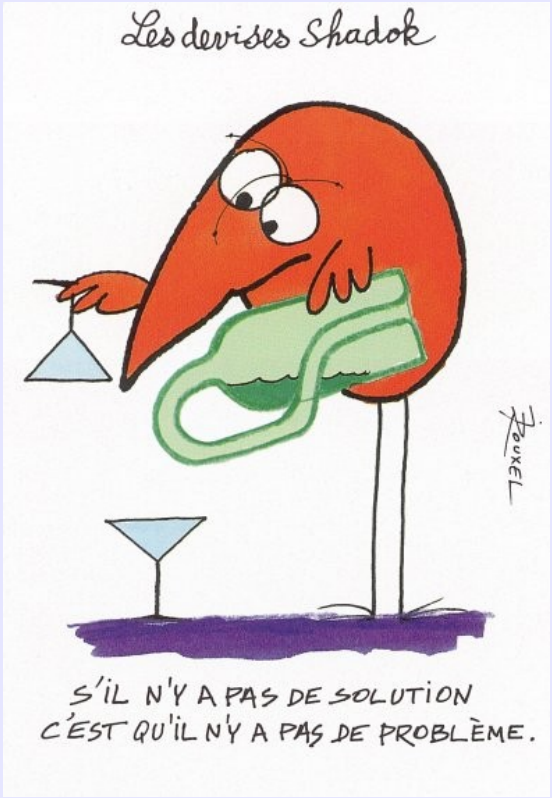




# Configuration du DNS



- Solution actuelle (vue externe)
  - limsi.fr in MX
    - 10 smtp1.u-psud.fr
    - 10 smtp2.u-psud.fr
- Solution sécurisée
    - 50 smtpx
- Solution temporaire :
    - 50 relais.limsi.fr



# Fin



- Des questions ?