Architecture Messagerie au C.I.C.T

- Les contextes (CICT et technique)
- L'architecture du service de MESSAGERIE
- Les outils utilisés
- L'architecture interne des passerelles
- Le routage des messages
- Quelques outils d'exploitation

Le contexte

- **Centre Interuniversitaire:**
  - Multi organismes dans des domaines d'activités variés
  - Gestion de plusieurs domaines de messagerie
  - Hébergement de services et de serveurs
- **Structure informatique:**
  - Centralisée pour la gestion des passerelles
  - Décentralisée pour la gestion des serveurs

Quelques chiffres

- **Nombre de domaines de messagerie: 36**
- **Nombre de serveurs de messagerie: 29**
- **Nombre de boîtes aux lettres: 60 000**
  (30 000 étudiants UPS)
- **Nombre de messages reçus:**
  - sur les passerelles par jour: 800 000 (potentiel)
  - déposés dans les boîtes aux lettres: 90 000
- **Nombre de messages envoyés par jour: 50 000**

Le contexte technique

- Linux CentOS / sendmail /greylisting / IMSS / spamassassin
- Séparation des flux entrants et sortants
- Filtrage SMTP sur les routeurs du campus
- Tous les messages (en entrée et en sortie) passent par les passerelles antivirus
- Relayage autorisé que pour les domaines gérés
- Refus de machines (@ IP ou domaines) via le fichier /etc/mail/access

L'Architecture du service de MESSAGERIE

Internet

•Utilisateurs autorisés

gw1-mail.xxx.fr

gw2-mail.xxx.fr

gw3-mail.xxx.fr

smtp1.xxx.fr

smtp2.xxx.fr

smtp.xxx.fr

Serveurs mail

BAL

pop.xxx.fr

externe vers interne

interne vers interne

interne vers externe

Les outils choisis :
Configuration des serveurs gwx-mail

- Machine : quad-core Xeon 2.33 Ghz, 4Go RAM, 2x146Go disque
- MTA : sendmail
- greylisting : relaydelay
- Antivirus : IMSS
- Marquage des spams : spamassassin

Les outils choisis :

Sendmail (1/4)

- Refus de machines (@ IP ou domaines) via le fichier /etc/mail/access = liste noire manuelle
- Relayage pour les domaines que nous autorisons
- Routage des messages (Interrogation ou non de LDAP selon les domaines)

Les outils choisis:

Greylisting (2/4)

- Refuse systématiquement tout message venant d'une machine non inscrite dans la liste blanche avec une erreur temporaire, note la tentative dans la table mysql et accepte le message à la 2ième tentative (minimum 40 min)
- L'entrée est conservée 15 heures en attente de la 2ème tentative
- Si 2ème tentative, l'entrée sera conservée 15 jours
- Champ X-Delayed rajouté dans les entêtes pour indiquer la durée du retard.

Les outils choisis:

Antivirus (3/4)

- **IMSS – Interscan Messaging Security Suite :**
  - Produit Trendmicro
  - Version 7.0
  - Mise à jour des fichiers de signatures toutes les 15 minutes
  - Management via interface WEB = possibilité de filtrer un champ particulier, une extension de fichiers attachés (mise en quarantaine de tous les fichiers attachés en cas d'attaque virale en attendant la mise à jour des signatures)

Les outils choisis:

Marquage des spams (4/4)

- **Spamassassin :**
  - grand nombre de tests sur le contenu et les entêtes des messages pour les repérer. Sur chacun des tests, des points sont attribués et si le total
    - **Est > à 5 alors ajoute la chaîne de caractères [MESSAGE MARQUE SPAM] dans le champ sujet et ajoute un champ X-status à HIGH**
    - **Est entre 4 et 5 alors ajoute un champ X-status à MEDIUM**
    - **Est entre 3 et 4 alors ajoute un champ X-status à LOW**
  - Implémente le module bayesien – apprentissage des ham et des spam
  - Analyse image: plugin FuzzyOcr
- **Interface entre sendmail et spamassassin = miltrassassin**

Les outils choisis :

Configuration des serveurs de sortie smtpx

- **Machine : processeur pentium 2,4 Ghz, 2 Go RAM, 120 Go disque**
- **Logiciels :**
  - Antivirus : IMSS
  - Sendmail
    - **Connexions smtp que pour les domaines que nous autorisons**

Architecture interne des passerelles

Internet

Sendmail
port 25

greylisting

Antivirus
port 10025

antispam

Sendmail
port 10026

Routage des messages: « statique »

user@xxx.ups-tlse.fr
user@cict.fr
user@autres.fr

Passerelles

Serveur UPS

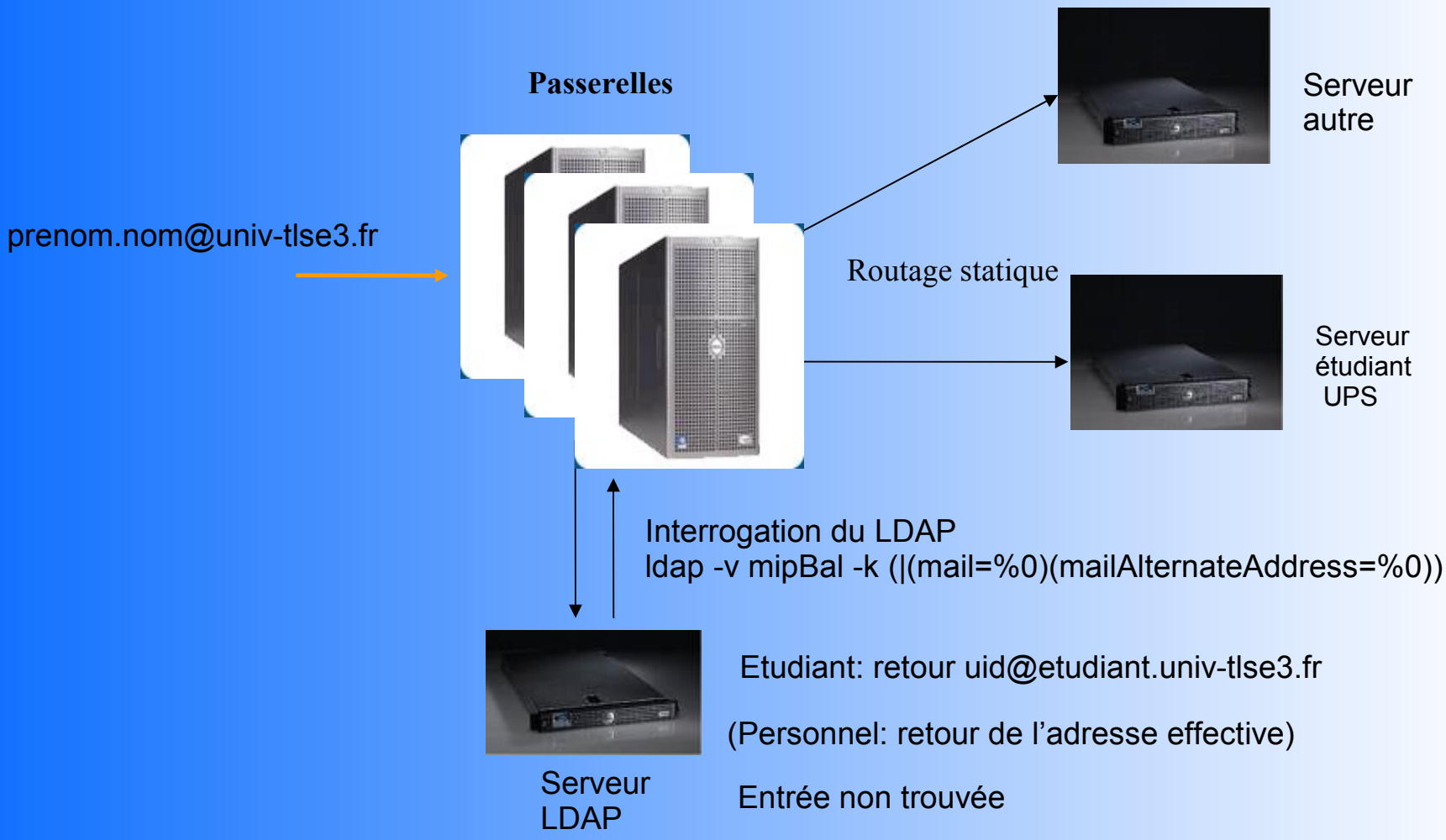
Serveur CICT

Serveur autres

Les passerelles transfèrent les messages en fonction du nom de domaine vers le serveur de messagerie correspondant (mailertable)

xxx.ups-tlse.fr esmtp:[serveur.xxx.ups-tlse.fr]
cict.fr esmtp:[mail.cict.fr]
autres.fr esmtp:[servmail.autres.fr]

Routage des messages: LDAP



Quelques outils d'exploitation

- **Les modifications « maison »:**
  - Insertion du délai dans en-tête des messages
  - Modifications de relaydelay.pl pour récupérer:
    - **Les machines en listes blanches**
    - **Les machines qui reviennent**
    - **La durée des retards**
- **Supervision**
  - Nagios: surveillance machine et queue
  - Scripts internes de surveillance des process

Quelques outils d'exploitation

- **Script de surveillance des connexions smtp:**
  - Toutes des heures, analyse du nombre de connexions sur l'heure écoulée:
    - **Alerte si nombre > 500**
    - **Blocage si nombre > 2500**
  - En entrée et en sortie