Journée RSSI/CSEC - 3 Décembre 2004

Expérience de filtrage des machines "à problèmes" sur le réseau REAUMUR Campus

Laurent FACQ
facq@u-bordeaux.fr
Directeur Technique & Responsable Sécurité

www.reaumur.net
REseau Aquitain des Utilisateurs des Milieux Universitaire et de Recherche
Version du 12/1/04 07:02:51 am

Plan

- Présentation du réseau REAUMUR
- Historique des problèmes de sécurité
- Stratégie mise en oeuvre
- Fonctionnement
- Pourquoi ça marche ?
- Conclusion

Le réseau REAUMUR

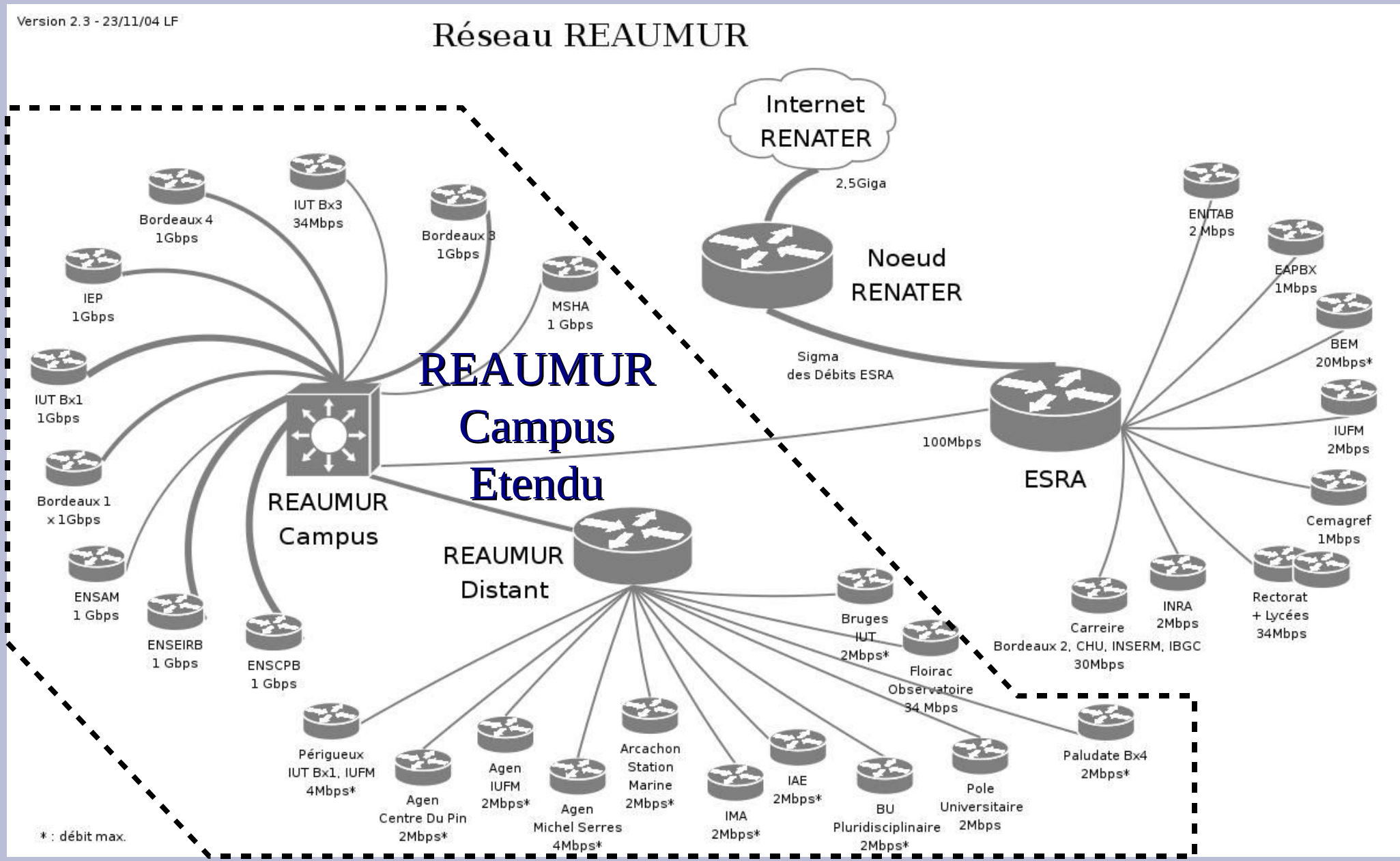
REseau Aquitain des Utilisateurs des Milieux Universitaires et de Recherche

- 3 Pôles : Réseau de Campus, Urbain & Régional
  - 7 personnes (1 Dir, 1 Sec, 2 Ing+1 Apprenti, 1 AI, 1 Tech)
  - + 2 Directeurs de Pôles (Urbain & Régional)

- REAUMUR Pôle “Campus étendu”
  - Réseau inter-universitaire Bordelais
  - 3 Universités, Ecoles, Labos CNRS, ...
  - ~ 200 correspondants de site
  - ~ 10.000 machines
  - ~ 50.000 utilisateurs potentiels
  - Agrément RENATER : 100Mbps
  - Une centaine de routeurs & commutateurs

Le réseau REAUMUR

REseau Aquitain des Utilisateurs des Milieux Universitaires et de Recherche



REAUMUR Campus Etendu Sécurité

- Organisation :
  - Chaque entité est responsable de sa sécurité
    - Un correspondant sécurité par entité
  - Service sécurité REAUMUR vient en plus

- Techniques utilisées depuis 1995
  - Préventive
    - analyse réseau active (satan puis nessus)
  - Réactive
    - analyse réseau passive (IDS maison puis snort)

Historique des problèmes de sécurité (1/2)

- 1995 : Quelques scans & piratages par an
  - Remontées manuelles au CERT Renater
  - Scans significatifs (trafic entant) => recherche d'intrusion
  - Machines Unix

- ???? : Dégradation progressive
  - Banalisation des scans & tentatives d'intrusions
  - Remontées automatiques au CERT Renater
  - Détection d'intrusion (trafic sortant)
  - Machines Windows

- 2001 : Début du P2P
  - abus très important de bande passante (>50% bande passante au début!)

Historique des problèmes de sécurité (2/2)

- 2002 : Explosion des problèmes de vers SMTP (Magister)
  - Déploiment d'anti-virus sur serveur messagerie
- 2003 : Explosion des problèmes de vers Réseau (Saphir, Blaster, Bagle, Agobot, Mydoom & Co).
  - Scans sur ports “Windows” (135 à 139, 445, ...)

Août 2003 - Mai 2004 : 900 machines Windows infectées

=> Trouver une solution pour ne pas faire que ça !

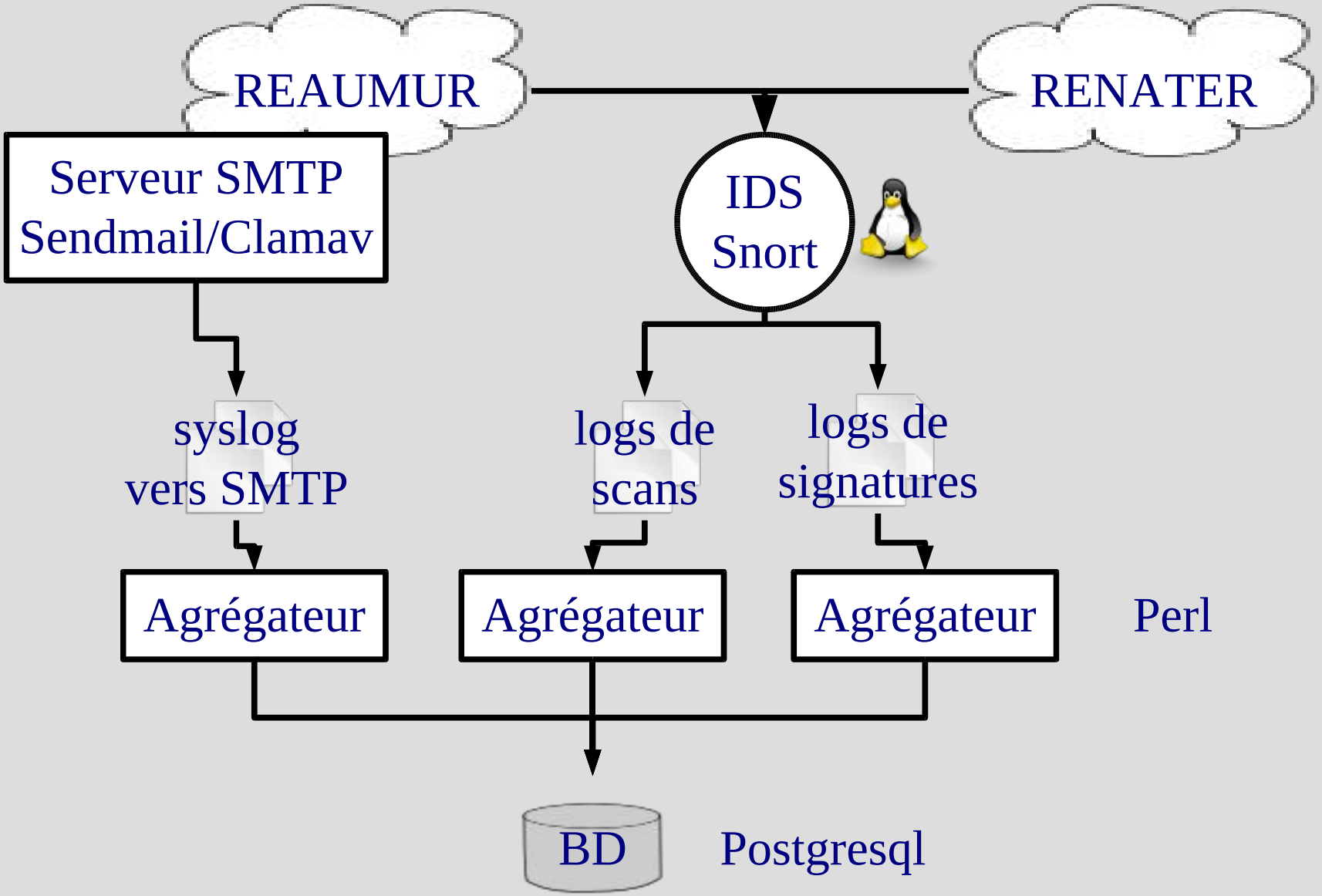
Stratégie

- Fermeté : Blocage de l'accès Internet des machines “à problèmes” (sans aucune distinction : avec ou sans fil, administration, recherche, pédagogie, ...)
  - compromise (vers, piratage, ...) => pb machine
  - violation charte (p2p, abus, ...) => pb utilisateur...
- Intranet et internet restent accessibles pour
  - les mises à jour (anti-virus/windows)
  - permetre de travailler un minimum
    - lire son mail en interne + acces proxy
    - nettoyer la machine dans le cas d'une compromission
- Le correspondant du site doit explicitement demander la réouverture après résolution du “problème”

Détection & Collecte Fonctionnement (1/2)

- Détection des “problèmes” par analyse passive :
  - IDS snort
    - signatures
    - scans (détection générique des vers & p2p)
      - ports, hosts, mixte (p2p)
  - analyse des logs (sendmail/clamav pour vers SMTP)
  - analyse métrologique (netflow/netmet) (en cours)
- Agrégation & stockage dans une base

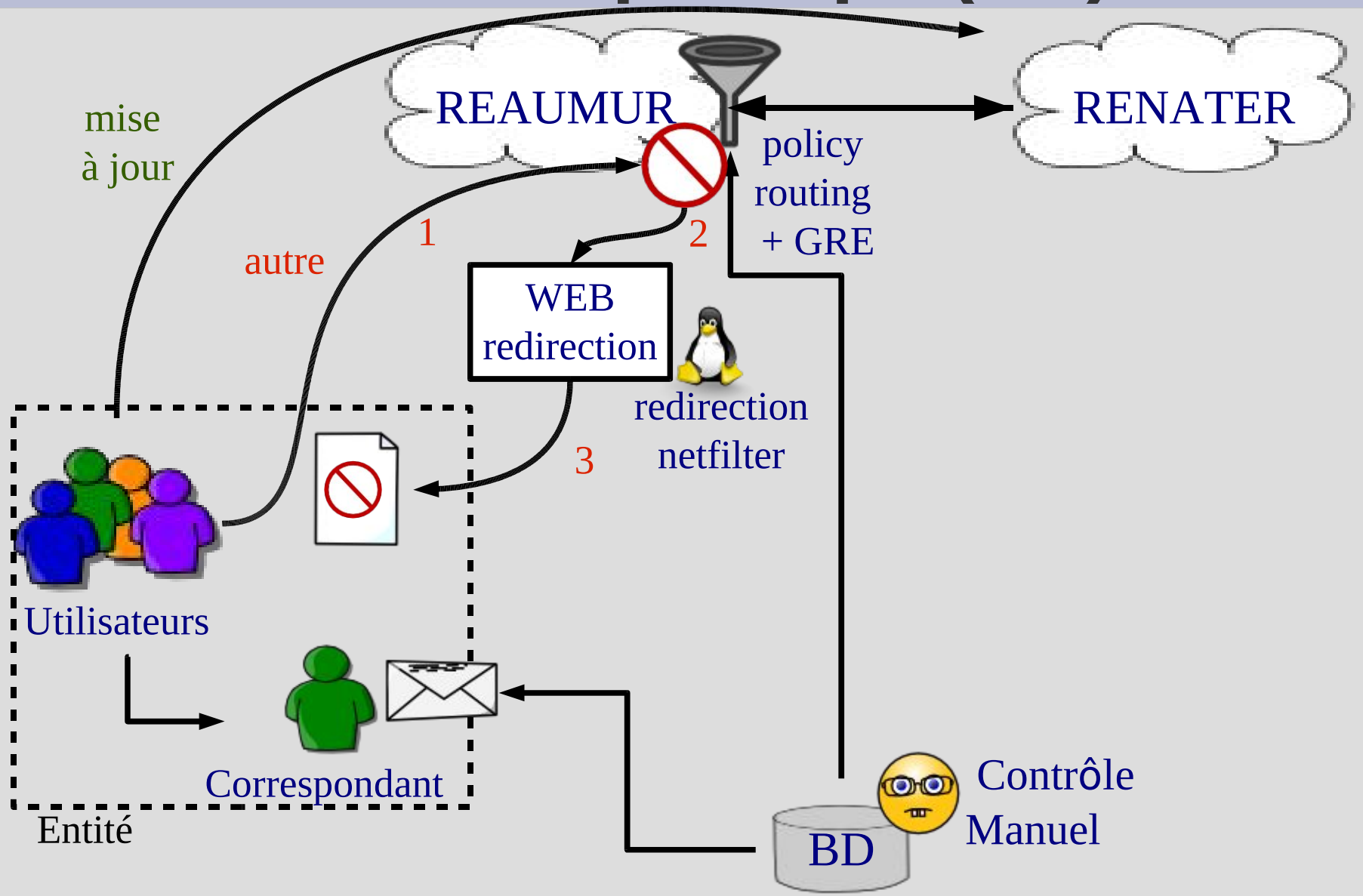
Détection & Collecte
Schéma de principe (1/2)



Réaction & Signalement Fonctionnement (2/2)

- Fonctionnement semi-automatique
  - synthèse par IP
  - faux positifs => *whiteliste* + Contrôle manuel systématique
- Blocage et signalement simultané
  - sur adresse IP
- Courrier aux correspondants
  - Adresse IP bloquée + Raison + Dates détection
- Redirection des machines sur une page web d'info (policy routing)
  - l'utilisateur sait tout de suite “pourquoi ça bloque”

Réaction & Signalement
Schéma de principe (2/2)



Statistiques depuis Janvier 2004

- environ 50 blocages par mois (2 à 3 par jour ouvré)
- 60% vers & virus
  - 50% via courrier électronique, 50% via réseau - scan
- 30% P2P
- 10% Autres
  - FTP Warez
  - Backdoor de redirection de spam
  - Piratages
  - ...

Audits Préventifs

- Analyse Active permanente du campus
  - nessus cyclique sur 20 jours ou ciblé en cas d'urgence
  - rapports envoyés aux correspondants pour info seulement
    - pas d'action obligatoire ou blocage sur cette base (pas assez fiable)
    - blocage ponctuel (vague de piratage)
  - quelques réaction négatives
    - sentiment d'être “évalué” ?
    - rapport très verbeux et pas 100% fiable
  - rapports appréciés dans la très grande majorité

Organisation
Pourquoi ça marche ? (1/2)

- Bloquer, c'est possible !

- Conseil d'Administration REAUMUR
  - Constitué des représentants des partenaires & utilisateurs
  - Soutient une politique sécurité ferme, réelle volonté d'avoir un réseau sécurisé
  - Effet de “pression de groupe” positif

- Service Réseau inter-universitaire bien perçu par les correspondants – climat de confiance
  - problèmes de compromission détectés en premier par REAUMUR dans la plupart des cas
  - Réactions négatives exceptionelles des utilisateurs (sur violation de charte) : 3 cas en 9 ans

Organisation
Pourquoi ça marche ? (2/2)

- Impact favorable de la chaîne

utilisateurs <-> correspondants <-> REAUMUR <-> RENATER

permettant une politique ferme

  - REAUMUR fait respecter les chartes (locale & RENATER)
  - Les correspondants locaux (admin. des sites) ne sont pas responsables des filtrages
  - Ils apprécient que ces filtrages soient mis en place au niveau inter-universitaire
  - Les utilisateurs peuvent difficilement faire pression sur REAUMUR

- Exceptions toujours possibles pour des besoins légitimes (ex: recherche sur P2P)

Conclusion (1/3)
Technique - Méthode

- Limites du fonctionnement par adresse ip
  - inadapté pour :
    - les adresses ip dynamiques
    - les proxy & machines multi-utilisateurs
    - la translation d'adresse, ...
  - Coopération avec les correspondants pour remonter à la source
  - Nécessité du filtrage au vol en complément

- MAIS le filtrage au vol (ex: NBAR cisco, module netfilter) n'est pas suffisant car :
  - ne contraint pas l'utilisateur à changer d'attitude ou à réparer/faire réparer sa machine
  - décision instantanée n'est pas toujours possible

Conclusion (2/3)
Technique - Futur

- Système actuel atteint ses limites
  - écrit dans l'urgence
  - semi-automatique
  - => contrôles manuels systématique
  - => lévée manuelle sur courrier

- Refonte en cours
  - par Grégoire MOREAU (apprenti ingénieur)
  - Automatique 24h/24h + Contrôles si nécessaire
  - Interface Web pour correspondants
    - levée des filtrages,
    - tableau de bord, journal

- Diffusion du logiciel (2005)

Conclusion (3/3)
Politique

- Le blocage est une des rares méthodes efficace pour contraindre réellement l'utilisateur à respecter les règles de sécurité
  (avoir à demander le déblocage de sa machine est dissuasif)

- Une fois de plus, la technique seule, comme la politique seule ne résoud rien : les deux sont nécessaires.