L’impact de la lutte contre le spam et les virus sur les architectures de messagerie

Claude Gross UREC

&

Serge Aumont CRU

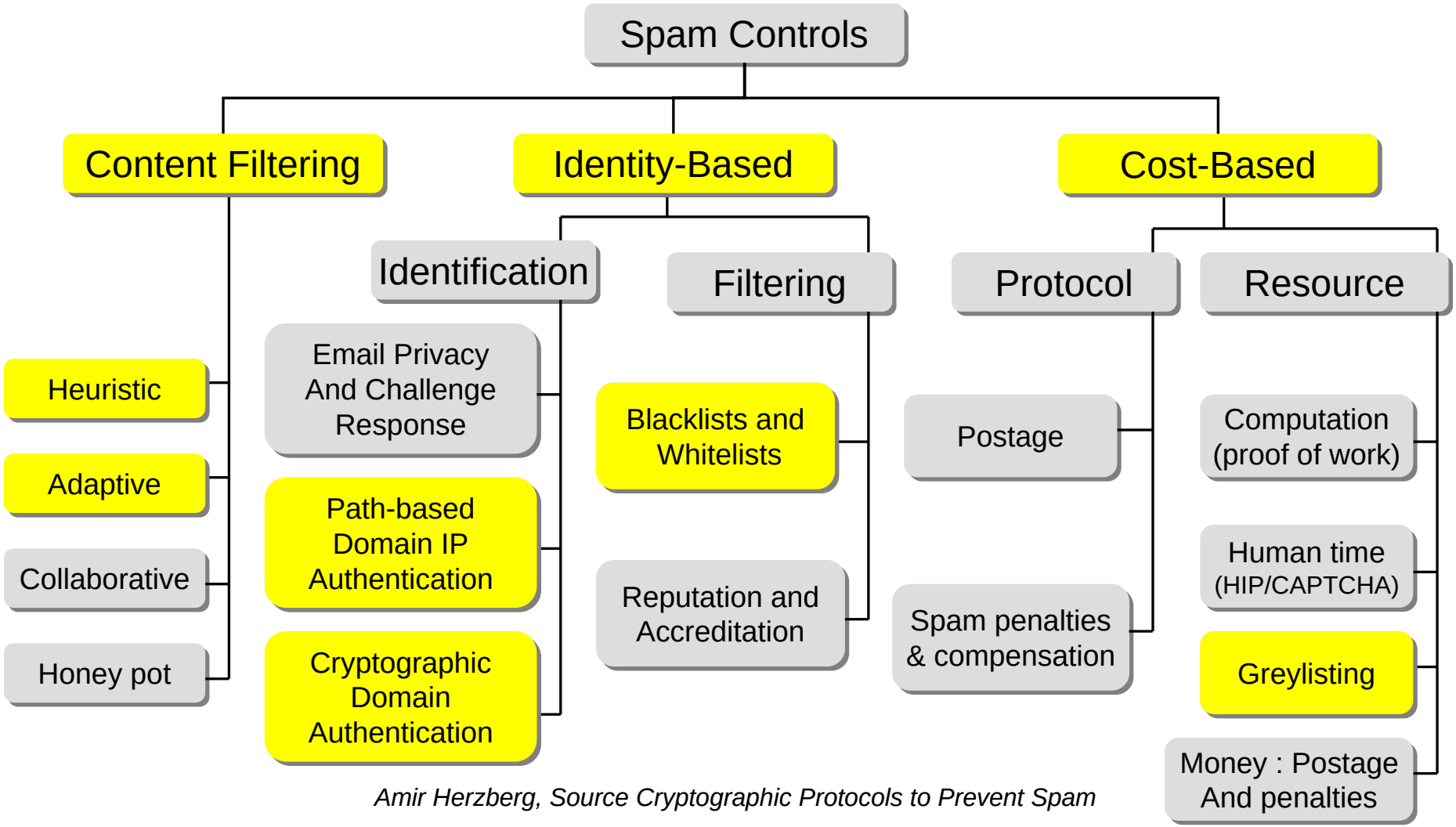
Sommaire

- Un constat déplorable
- Les buts
- Quelles méthodes?
- Impacts sur l’architecture de messagerie

Contraintes

- Messagerie
  - Disponibilité
  - Fiabilité
  - Délais d’acheminement
  - Accessibilité
- Respect de la législation

Complexité technique



Amir Herzberg, Source Cryptographic Protocols to Prevent Spam

Sender Policy Framework

- SPF vise à authentifier la provenance des messages. Les MTA autorisés à émettre des messages pour un domaine donné sont déclarés dans le DNS.
- On précise aussi dans le DNS comment interpréter un résultat négatif du test SPF (est-ce grave ?)

SPF

- Le « forwarding » n’est pas compatible avec SPF (faire suivre un courrier sans en réécrire l’enveloppe) .
- 2 solutions :
  - Sender Rewriting Scheme
    srs0+yf09=Cw=orig.org=ann@forwarder.org
  - Responsible Submitter.
    MAIL FROM:ann@orig.org size 1000 submitter=<bog@forwarder.org>
- Est-ce déployable ?

Mettre en place SPF

- Suppose de maîtriser la liste des MTA qui émettent des messages pour le compte de votre domaine.
- Dans le contexte greylist, SPF peut être utilisé comme une whitelist : « pass » pour un mail venant d'un réseau IP de Renater

Domain Key Internet Message

- DKIM vise à signer les messages (corps plus une partie des entêtes).
- Utilise de la crypto asymétrique
- Publication des clés par le DNS : pas de PKI, pas de tiers de confiance
- Dans la majorité des cas la signature est apposée par le MTA : pas de distribution de clés privées aux utilisateurs
- Les signatures sont vérifiées par le MX (pas de modification des UAs)

DKIM

- DKIM n’est pas une solution intrinsèque au spam, il règle le PB des messages forgés avec une fausse adresse
- L’authentification des messages doit limiter les pratiques illégales qui sont légion dans le SPAM

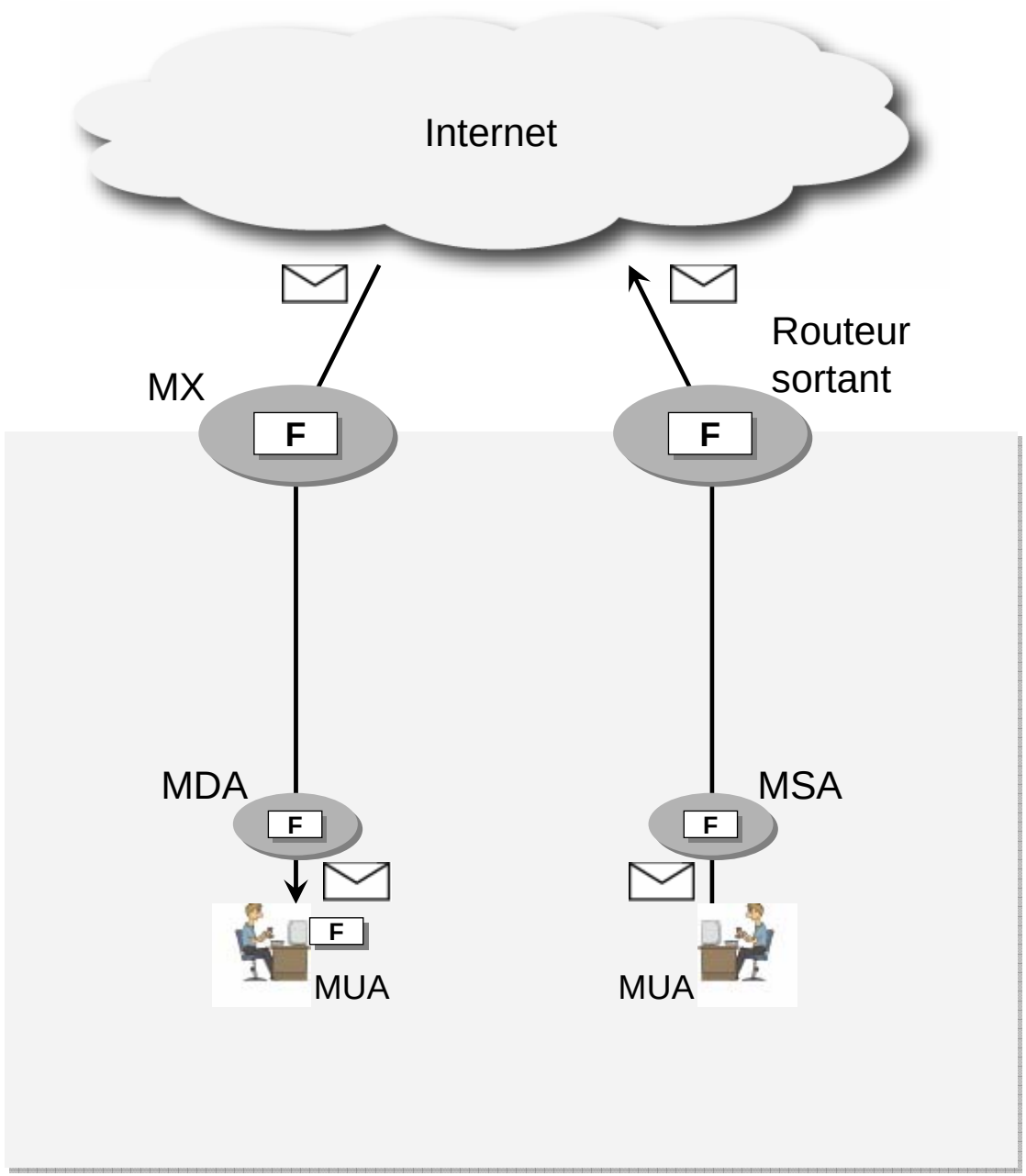
Stratégie

- Utilisation de nombreux outils
- Les outils intègrent souvent différentes méthodes

- Quelles méthodes?
- Quels outils?
- Où les utiliser ?

Les composants de l’architecture

- MX = *Mail eXchanger*
- MDA *Message Delivery Agent*
- MUA *Message User Agent*
- MSA = *Message Soumission Agent*
- Le routage sortant


Internet
Routeur
sortant
MX
F
F
MDA
MSA
F
F
F
MUA
MUA

MX

- Il est usuel de forcer le passage des messages via des MX. Cette architecture reflète l'organisation informatique des établissements (CRI), elle permet entre autre la traçabilité des échanges.
- Logiquement, beaucoup de fonctions anti-spam sont concentrées sur les MX
- Certains tests comportementaux sont obligatoirement sur ces serveurs : ex : greylist

MX

- Filtrage anti-virus sur le MX important car
  - Assure un service minimum pour tous avec une bonne administration de l'anti-virus
  - Localement ou via un serveur de filtrage (API milter de sendmail)

MX

- Un rejet dès le MX évite de consommer des ressources ailleurs dans le domaine
- Un rejet en session évite de décider si l'on génère un bounce ou pas.
- Induit une sensibilité d'un service essentiel face à des crises de trafic (mail bombing, attaque de type dictionnaire, …)

Le MDA

- Le service de dépôt des messages en boite aux lettres (souvent procmail)
- Le bon endroit pour filtrer les messages avec les marqueurs appliqués en amont car le filtrage (rejet et classement dans des dossiers) est appliqué quelque soit l'interface de consultation
- Suppose de mettre en place des outils à disposition des utilisateurs.

Le MUA

- Thunderbird et Outlook intègrent du filtrage Bayésien
- Efficace car bonne interface pour alimenter la base de connaissance en SPAM et en HAM.
- Mais base de connaissance trop limitée, en particulier en cas d'utilisation de plusieurs postes de travail par une personne.

Le MSA

- Souvent un seul serveur assure le MSA et le trafic sortant.
- Penser que les virus peuvent se propager en interne du domaine
- Généraliser l'authentification SMTP même sur les MSA interne au domaine :
  - Augmente la valeur de la signature DKIM par le serveur
  - Logs plus fiables
  - Mesure « *anti-botnet* »
  - Impose de configurer tous les clients et toutes les applications

Routeurs sortants

- Ne pas négliger le contrôle des flux sortants
- Une session SMTP peut être «retournée». Une machine ayant le droit SMTP sortant peut accepter des messages entrants non contrôlés.
- Centraliser les flux sortants pour l'*accounting*
- SPF plus utile avec une politique de routage centralisée
- Antivirus et anti-spam sur les flux sortant pour détecter les machines compromises.

Routeurs sortants

- Plus difficile à mettre en œuvre que le contrôle du trafic entrant : pas de DNS donc configuration de toutes les machines émettant des messages.
- Éviter le re-routage transparent du port 25
  - Dans ce cas les logs ne permettent plus de détecter les machines infectées
  - Risque juridique accru en cas de blocage de message ou d'atteinte à la confidentialité

Place des utilisateurs nomades

2 grands cas à distinguer :

1. Solution occasionnelle de type *cyber-café*. Seul le webmail est adapté à coup sur, mais beaucoup de limitations.
2. PC portable ou PC familial, pas d'hypothèse sur la qualité de la connectivité : consultation/émission

a1

Diapositive 21

a1 par exemple il n'est passible de travailler "offline" comme on peut le faire avec des clients dédiés tel que Thunderbird.
aumont; 15/11/2005

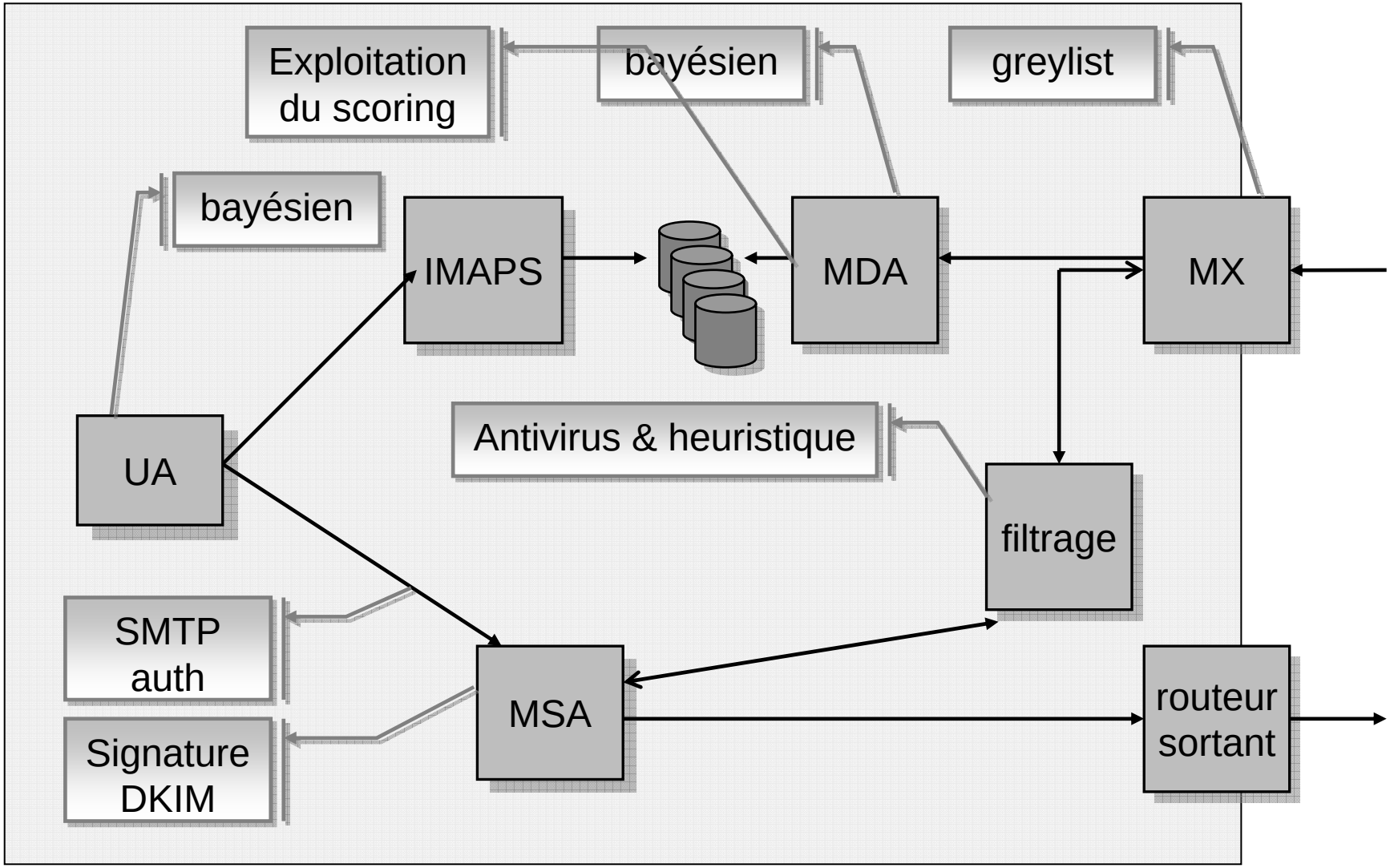
Place des utilisateurs nomades

- Utiliser le MSA du réseau d'accueil : c'est mauvais :
  - Oblige à configurer le mailhost pour chaque nouveau réseau
  - Contournement de la politique de messagerie du domaine d'origine (filtrage anti-virus, authentification systématique, accounting...)
  - Risque quant à la confidentialité
  - Affaibli SPF : on oblige l'utilisation du statut neutre
  - DKIM : oblige à implémenter DKIM sur le poste client ou dégrader la politique déclarée dans DKIM)

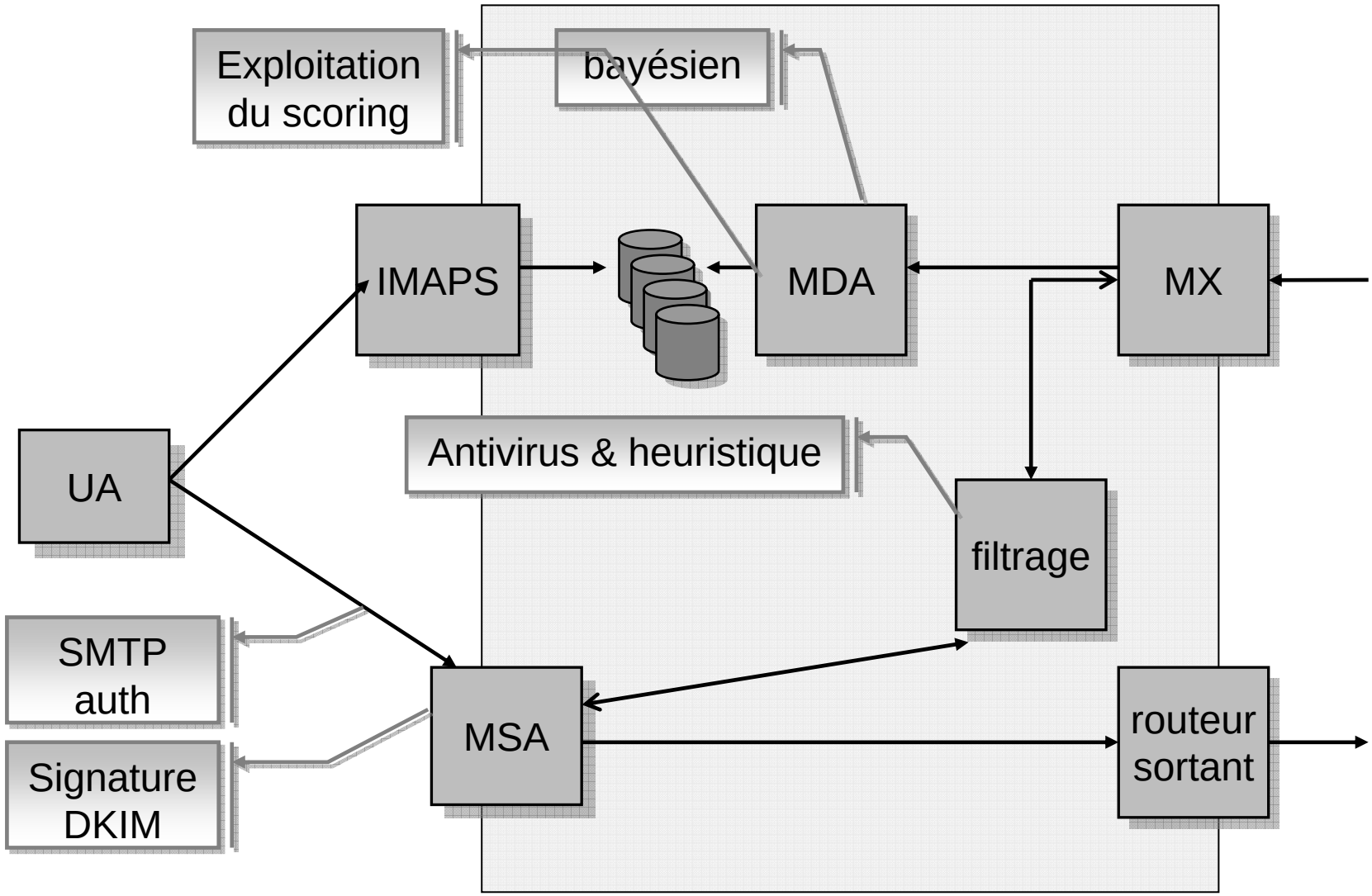
Place des utilisateurs nomades

- Utiliser le MSA de son domaine d'origine, si le réseau invité le permet :
  - **Sur les réseaux "invités",** ne pas filtrer les ports 25 et **587** !
  - ne jamais faire du re-routage transparent du protocole SMTP
  - au besoin, utiliser un classe C spécifique pour ne pas subir de "black listage"
  - n'empêche pas de faire de la métrologie pour détecter les PC « invités » compromis
- Utiliser un VPN

Un exemple d'architecture



Cas du service nomade



Conclusions

- La lutte anti-spam n’est plus une option, c’est un élément de la politique de sécurité
- Elle doit être intégrée dans l’architecture de messagerie
- Elle nécessite une (in)formation des utilisateurs

Conclusions

- la lutte anti-spam concerne le trafic entrant et sortant
- Vers la généralisation de l'authentification sur le MSA, même en interne
- Espoir de voir émerger DKIM ?