



Le service antispam de RENATER

Laurent.Aublet-Cuvelier@renater.fr



Sommaire

- Contexte
- Architecture de la solution
- Caractéristiques du filtrage
- Procédure de raccordement et utilisation
- Evolutions du service
- Quelques indicateurs
- Conclusion





Contexte

- Enquête auprès des RSSI sur les solutions déployées à l'échelle des sites RENATER (2008)
- Création d'un groupe de travail antispam (sept. 2008)
 - Point sur l'état de l'art et identification des solutions techniques existantes
 - Lancement d'un service pilote (test plusieurs solutions)
 - Préparation du cahier des charges
- Lancement d'un appel d'offres
 - pour l'obtention d'un service national antispam
- Déploiement (sept. 2009)
- Ouverture du service (1^{er} octobre 2009)

Antispam : service RENATER



3



Sommaire

- Contexte
- Architecture de la solution
- Caractéristiques du filtrage
- Procédure de raccordement et utilisation
- Evolutions du service
- Quelques indicateurs
- Conclusion

Antispam : service RENATER



4



Architecture de la solution

- Equipement Cloudmark (IMP Bizanga) = MTA avec des briques logicielles :
 - Moteur antispam VadeRetro
 - Moteur antivirus VadeRetro (heuristique)
 - Moteur antivirus DrWeb (base de signatures)
- Haute disponibilité
 - 2 équipements IMP distribués sur 2 NR
 - 2 serveurs pour collecte/mise à disposition des logs
- Evolutif
 - Licences initiales jusqu'à 500 000 boîtes aux lettres
 - Possibilité d'évolution jusqu'à 2 000 000 sur la même infrastructure

Antispam : service RENATER

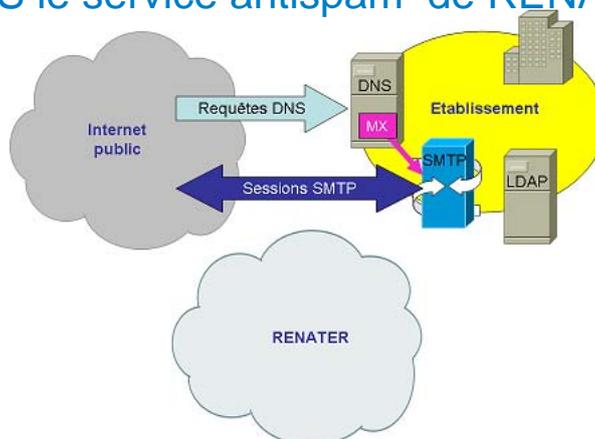


5



Architecture : flux de messagerie

- SANS le service antispam de RENATER :



Antispam : service RENATER

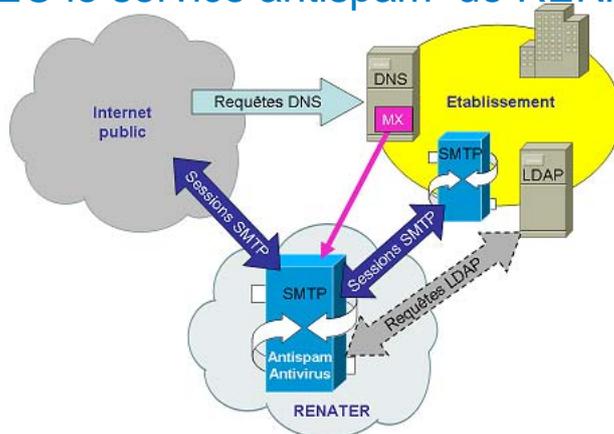


6



Architecture : flux de messagerie

- AVEC le service antispam de RENATER :



Antispam : service RENATER



7



Sommaire

- Contexte
- Architecture de la solution
- Caratéristiques du filtrage
- Procédure de raccordement et utilisation
- Evolutions du service
- Quelques indicateurs
- Conclusion

Antispam : service RENATER



8



Caractéristiques du filtrage

- Filtrage des flux entrants uniquement (pour l'instant)
 - Filtrage antispam
 - Protocolaire :
 - Filtrage sur la réputation (RBL SpamHaus)
 - Greylisting pour les domaines dynamiques et les IP non résolues
 - Rejet SPF Hard Fails
 - ...
 - Vérification via annuaires LDAP des @mail (prévention du backscattering)
 - Filtrage de contenus
 - Application de listes blanches/noires : globales + par domaine
 - Personnalisation de règles de filtrage par domaine
 - Traçabilité des décisions de filtrages (logs)
 - Pas de gestion de quarantaine => problématique des sites
 - Filtrage antivirus (optionnel)

Antispam : service RENATER



9



Sommaire

- Contexte
- Architecture de la solution
- Caractéristiques du filtrage
- Procédure de raccordement et utilisation
- Evolutions du service
- Quelques indicateurs
- Conclusion

Antispam : service RENATER



10



Procédure de raccordement au service (1/2)

- **Etape 1 : demande de souscription au service**
 - Communication
 - des domaines concernés
 - et des adresses IP des serveurs SMTP par domaine concerné
 - Validation de la demande pour chaque domaine
 - auprès du « postmaster » du domaine
- **Etape 2 : interconnexion au service**
 - Annuaire LDAP obligatoire
 - Définition des paramètres de filtrages :
 - pièces jointes à refuser (taille, extensions), seuils (marquage/rejet), marqueurs souhaités, etc.

Antispam : service RENATER



11



Procédure de raccordement au service (2/2)

- **Etape 3 : validation**
 - Validation de la chaîne de transmission
- **Etape 4 : mise en production**
 - De la responsabilité de l'administrateur du site
 - Bascule des MX de chaque domaine

Antispam : service RENATER



12



Raccordement : utilisation

- **Ajustements :**
 - Spécification de listes blanches/noires pour chaque domaine (si besoin)
 - Ajustements : des seuils de filtrage (éventuellement), des PJ filtrées, etc.
- **Boucle de feedback**
(signalement des faux positifs/négatifs)
 - 2 boîtes IMAP (Spam et NoSpam) à disposition des administrateurs de sites

Antispam : service RENATER



13



Raccordement : utilisation

- **Retour administrateurs :**
 - Mise à disposition des logs
 - Fichiers temps réel
 - Récupérables par mirroring FTP.
 - Génération de tableaux de bord quotidiens (+ mensuels) :
 - 1 global à un site + 1 pour chaque domaine

Antispam : service RENATER



14



Sommaire

- Contexte
- Architecture de la solution
- Caractéristiques du filtrage
- Procédure de raccordement et utilisation
- Evolutions du service
- Quelques indicateurs
- Conclusion



Evolutions

- **Recemment :**
 - Marquage des messages commerciaux (UCE)
- **En cours :**
 - Portail web pour l'administration
 - Phase 1 : gestion des listes blanches/noires de domaine
 - Actuellement en version alpha
 - en pré-prod cet été : importance de la recette !
 - Boucle feedback
 - Un plugin Thunderbird pour le signalement (beta test)
- **A l'avenir :**
 - Etude de la mutualisation de listes blanches et noires
 - IPv6, tests DKIM, etc...
 - Selon vos suggestions !
 - (=> support-antispam@renater.fr !)
- **Veille technologique pour évolution**





Sommaire

- Contexte
- Architecture de la solution
- Caractéristiques du filtrage
- Procédure de raccordement et utilisation
- Evolutions du service
- Quelques indicateurs
- Conclusion



Indicateurs

- Juin 2011
 - 42 sites, 240 domaines
 - 500 000 boîtes aux lettres
 - Statistiques : cf. retour d'expérience





Conclusion

- Support techniques et informations :
 - support-antispam@renater.fr
 - <http://www.renater.fr/antispam>
- Liste de diffusion :
 - antispam-forum@renater.fr
 - Utilisateurs et futurs utilisateurs du service
 - Avec wiki utilisateurs

