

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1241

(04/2008)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION
ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberspace – Lutte contre le pollupostage

**Cadre technique pour lutter contre les spams
par courrier électronique**

Recommandation UIT-T X.1241

RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1241

Cadre technique pour lutter contre les spams par courrier électronique

Résumé

La Recommandation UIT-T X.1241 fixe un cadre technique pour lutter contre les spams par courrier électronique. Ce cadre décrit une structure recommandée d'un domaine de traitement antispam, et définit la fonction de ses principaux modules. L'essentiel est qu'il établit un mécanisme de partage des informations sur les spams par courrier électronique entre les différents serveurs de messagerie électronique. Ce cadre devrait permettre d'améliorer l'efficacité des systèmes grâce à leur interconnexion.

Source

La Recommandation UIT-T X.1241 a été approuvée le 18 avril 2008 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Antispam, cadre technique, courrier électronique (e-mail), interconnexion, spam.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2009

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 1
3	Définitions 1
3.1	Termes définis ailleurs 1
3.2	Termes définis dans la présente Recommandation 1
4	Abréviations et acronymes 2
5	Conventions 2
6	Structure générale du domaine de traitement antispam..... 2
6.1	Structure générale..... 2
6.2	Modèle de référence 4
7	Fonctions du domaine de traitement antispam 5
7.1	Fonctions du client de messagerie électronique 5
7.2	Fonctions du serveur de messagerie électronique 5
7.3	Fonctions de l'entité de traitement antispam 6
7.4	Fonctions de la sous-entité de traitement antispam..... 6
8	Identification des spams par courrier électronique..... 7
8.1	Caractéristiques courantes des spams par courrier électronique 7
8.2	Règles communes pour combattre le spam par courrier électronique..... 8
9	Méthodes de lutte contre le spam par courrier électronique..... 9
9.1	Désactiver la fonction de relais ouvert 9
9.2	Maîtriser l'autorisation de délivrance des courriers électroniques 9
9.3	Technique de filtrage 9
9.4	Examen de la traçabilité 10
10	Interconnexion entre les domaines de traitement antispam..... 11
10.1	Interconnexion entre des entités de traitement de premier niveau 11
10.2	Interconnexion entre une entité et une sous-entité de traitement 12
10.3	Interconnexion entre une sous-entité de traitement et un serveur de messagerie électronique..... 12
	Bibliographie..... 14

Introduction

Avec le développement du réseau de télécommunication IP, les utilisateurs échangent un grand nombre de courriers électroniques, mais reçoivent de plus en plus de messages non sollicités, de spams, ce qui entraîne de graves problèmes.

Le spam par courrier électronique est devenu un vrai fléau qui nuit à l'utilisation du réseau de télécommunication IP. Les prestataires de services doivent dépenser des sommes considérables pour lutter contre les problèmes causés par le spam; quant aux utilisateurs, ils doivent passer beaucoup de temps à supprimer ces courriers non sollicités.

Des techniques ont été proposées pour détecter ces courriers et les supprimer, mais les spammeurs ne sont pas à court d'idée pour les contourner: par exemple, ils falsifient des courriers électroniques normaux et en randomisent le contenu pour éviter la détection des filtres à spam. Il est en conséquence urgent d'élaborer un cadre technique efficace pour faire face au problème mondial que pose le spam par courrier électronique.

Différentes solutions antispams peuvent recourir pour lutter contre le spam par courrier électronique à différentes techniques, qui évoluent sans cesse. Il est ainsi très difficile de proposer une description figée, qui puisse couvrir tous les détails des techniques antispams sur le long terme.

Il convient donc d'établir un cadre ouvert pouvant convenir à ces diverses solutions, cadre qui devrait être compatible avec toutes les techniques antispams et ne pas se limiter à un détail technique particulier. Ce cadre devrait répondre aux exigences suivantes:

- pouvoir systématiquement estimer si un courrier électronique est ou non un spam;
- permettre à divers systèmes de services de messagerie électronique de s'échanger des informations de lutte antispam;
- pouvoir améliorer la précision des outils antispams de ces systèmes;
- faire en sorte que des entités appartenant à différents domaines administratifs s'échangent des informations de lutte antispam.

Recommandation UIT-T X.1241

Cadre technique pour lutter contre les spams par courrier électronique

1 Domaine d'application

La présente Recommandation fixe un cadre technique pour lutter contre les spams par courrier électronique. Ce cadre décrit une structure recommandée d'un domaine de traitement antispam, et définit la fonction de ses principaux modules. L'essentiel est qu'il établit un mécanisme de partage des informations sur les spams par courrier électronique entre les différents serveurs de messagerie électronique. Ce cadre devrait permettre d'améliorer l'efficacité des systèmes grâce à leur interconnexion.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 champs d'en-tête [b-IETF RFC 2822]: les champs d'en-tête ont la même structure syntaxique générale: un nom de champ, deux points, et le corps du champ.

3.1.2 objets de courrier [b-IETF RFC 2821]: un objet de courrier est transporté par le protocole SMTP, et comporte une enveloppe et un contenu.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 domaine de traitement antispam: il s'agit d'un système indépendant, qui comprend une entité de traitement antispam, des sous-entités de traitement antispam, des serveurs de messagerie électronique et des clients de messagerie électronique.

3.2.2 entité de traitement antispam: l'entité de traitement antispam est le cœur du domaine de traitement antispam. Elle collecte des informations sur le spam par courrier électronique auprès d'entités situées à des niveaux inférieurs, et construit ensuite un système de règles uniforme et intégré. Finalement, le système de règles devrait être soumis à toutes les entités des niveaux inférieurs.

3.2.3 sous-entité de traitement antispam: une sous-entité de traitement antispam est connectée à un ou plusieurs fournisseurs de services de courrier électronique. Elle reçoit des serveurs de messagerie électronique ou des équipements antispams des informations sur le spam par courrier électronique, qu'elle fait suivre aux entités de haut niveau après les avoir analysées à intervalles réguliers. Elle reçoit également à intervalles réguliers des entités de haut niveau des règles d'actualisation qu'elle communique aux sous-entités.

3.2.4 règle composée: une règle composée comprend deux règles simples ou plus.

3.2.5 courrier électronique (e-mail): cette expression sert principalement à désigner le courrier électronique acheminé sur un réseau de télécommunication.

3.2.6 spam par courrier électronique: cette expression sert à décrire des communications électroniques non sollicitées par courrier électronique, habituellement envoyées à des fins particulières.

3.2.7 règle: une règle est un ensemble de conditions et d'actions de base. Les règles peuvent prendre de nombreuses formes, par exemple des comportements, des filtres, etc.

3.2.8 courrier électronique échantillon: cette expression sert à décrire un courrier électronique qui est reçu de serveurs de messagerie électronique selon certaines règles.

3.2.9 spammeur: ce terme sert à décrire l'entité ou la personne qui crée et envoie un spam par courrier électronique.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DNS	système de noms de domaine (<i>domain name system</i>)
e-mail	courrier électronique
ESMTP	protocole de transfert de messages en mode simple étendu (<i>extended simple mail transfer protocol</i>)
FTP	protocole de transfert de fichier (<i>file transfer protocol</i>)
HTTP	protocole de transfert hypertexte (<i>hypertext transfer protocol</i>)
IMAP4	protocole d'accès aux messages Internet version 4 (<i>Internet message access protocol version 4</i>)
IP	protocole Internet (<i>Internet protocol</i>)
POP3	protocole POP dans sa version 3 (<i>Post Office Protocol version 3</i>)
RBL	liste noire en temps réel (<i>real-time blacklist</i>)
SASL	couche simple d'authentification et de sécurité (<i>simple authentication and security layer</i>)
SMTP	protocole de transfert de messages en mode simple (<i>simple mail transfer protocol</i>)
URL	localisateur uniforme de ressource (<i>uniform resource locator</i>)

5 Conventions

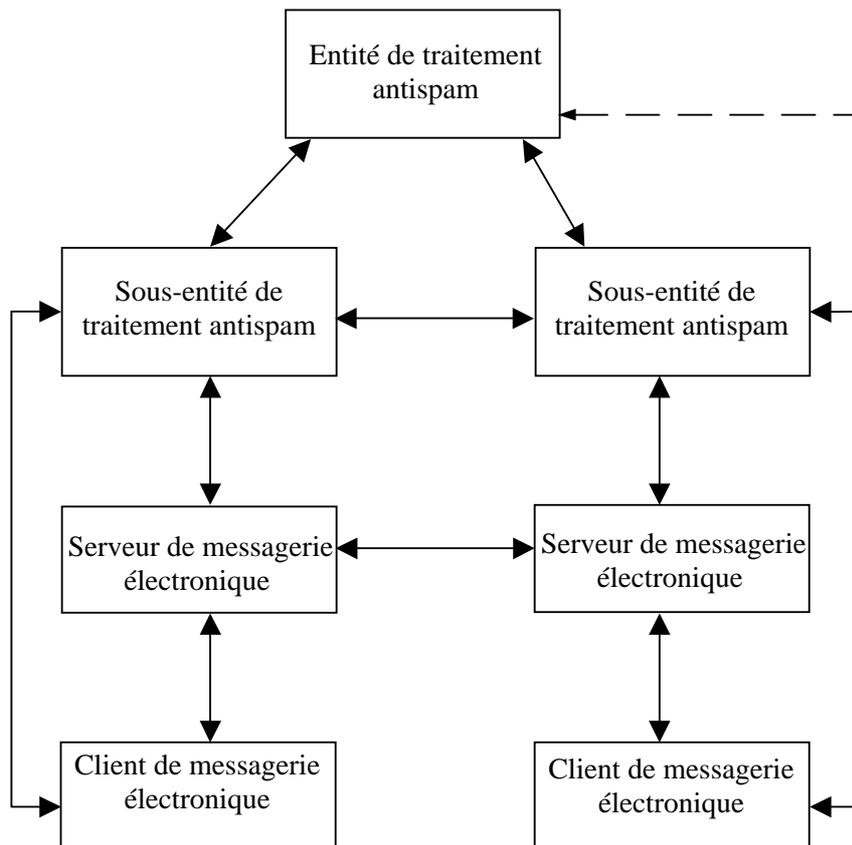
Aucune.

6 Structure générale du domaine de traitement antispam

6.1 Structure générale

La présente Recommandation décrit les composantes du cadre, à savoir l'entité de traitement antispam, les sous-entités de traitement antispam, les serveurs de messagerie électronique et les clients de messagerie électronique.

Ces composantes peuvent communiquer les unes avec les autres par des protocoles de messagerie courants. Leurs caractéristiques sont décrites dans le présent paragraphe.



NOTE – Les traits pleins représentent le trajet suivi par les informations échangées entre les composantes du domaine de traitement antispam.

Figure 1 – Structure générale

Dans la Figure 1, l'entité de traitement antispam reçoit des rapports des sous-entités de traitement antispam, auxquelles elle communique de nouvelles règles.

Les sous-entités doivent vérifier la validité de ces règles et les parfaire.

Le client de messagerie électronique est l'entité avec laquelle traitent directement les utilisateurs; le serveur de messagerie électronique assure la délivrance des courriers électroniques dans le réseau de télécommunication IP.

Le client de messagerie électronique transmet les réclamations à la sous-entité de traitement antispam, mais, dans des cas particuliers, il peut les communiquer directement à l'entité de niveau supérieur.

6.2 Modèle de référence

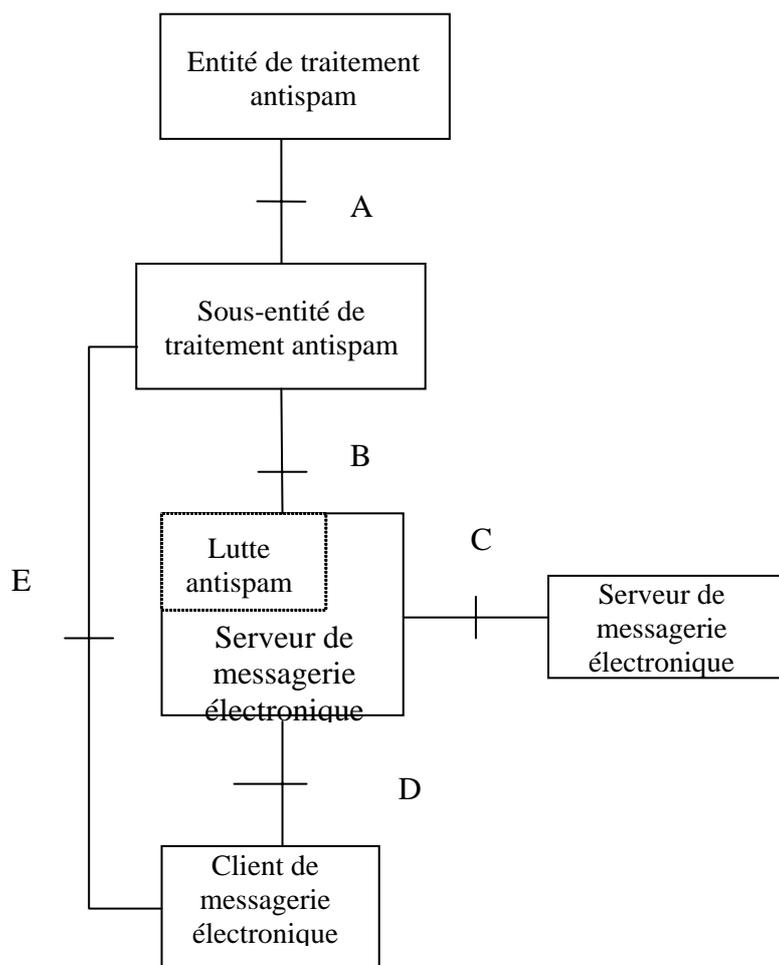


Figure 2 – Modèle de référence

L'interface A se situe entre l'entité et la sous-entité de traitement antispam. Les rapports de réclamation et les règles concernant la lutte antispam sont transmis par l'intermédiaire de cette interface A. Les règles peuvent être des règles composées, comme par exemple "source IP + URL". L'interface A devrait supporter les protocoles FTP et HTTP.

L'interface B se trouve quant à elle entre la sous-entité de traitement antispam et le serveur de messagerie électronique. Elle sert à transmettre les rapports de réclamation et les règles. Là aussi, les règles peuvent être des règles composées, comme par exemple "source IP + URL". L'interface B devrait supporter les protocoles FTP et HTTP. Dans des cas particuliers, le serveur de messagerie électronique peut communiquer directement avec l'entité de traitement antispam de niveau supérieur.

L'interface C se situe entre les serveurs de messagerie électronique, par lesquels les messages sont transmis au moyen du protocole SMTP.

L'interface D se trouve entre le serveur de messagerie électronique et le client de messagerie électronique. Divers protocoles peuvent servir à transmettre les courriers électroniques, par exemple POP3, IMAP4.

L'interface E se situe entre le client de messagerie électronique et la sous-entité de traitement antispam à laquelle le client peut envoyer des réclamations. Dans des cas particuliers, il peut les envoyer directement à l'entité de traitement antispam de niveau supérieur. Au niveau de cette

interface, on peut utiliser le web en ligne, le téléphone, le courrier électronique et les logiciels client.

7 Fonctions du domaine de traitement antispam

7.1 Fonctions du client de messagerie électronique

Le client de messagerie électronique a les fonctions suivantes:

- En plus d'exercer les fonctions générales de transmission des courriers électroniques, le client de messagerie électronique est un mécanisme qui aide les utilisateurs à transmettre leurs réclamations concernant le spam à l'entité de traitement antispam. Les destinataires de courriers électroniques doivent seulement juger si un courrier électronique est ou non un spam selon son contenu, titre ou adresse. Par exemple, si des destinataires ne veulent pas recevoir de publicités, de publications électroniques ou de contenus de propagande, ils peuvent dénoncer les courriers électroniques de ce type à l'entité de traitement antispam grâce au mécanisme du client de messagerie électronique.
- Le client de messagerie électronique peut télécharger automatiquement des règles de filtrage de spams depuis l'entité de traitement antispam. Les règles de filtrage sont établies selon les rapports de réclamation émanant des clients de messagerie électronique; elles indiquent la taille limite d'un courrier électronique unique, le nombre de courriers électroniques envoyés dans une période de temps donnée, des mots clés se trouvant dans le corps des courriers électroniques, etc. Les règles de filtrage sont périodiquement mises à jour selon les rapports de réclamation. Elles sont indexées par nom d'utilisateur de boîte aux lettres, adresse IP de sortie et nom de domaine.
- Le client de messagerie électronique peut transmettre des courriers non sollicités à l'entité de traitement antispam pour un nouveau traitement, ou supprimer certaines règles de filtrage qui sont à l'origine du mauvais tri. L'entité de traitement antispam peut mettre à jour les règles de filtrage immédiatement en fonction des besoins ou du rapport de réclamation émanant du client de messagerie électronique.
- Le client de messagerie électronique peut filtrer directement les courriers non sollicités. Normalement, les destinataires devraient connaître les résultats du filtrage afin d'éviter les erreurs de triage.

7.2 Fonctions du serveur de messagerie électronique

Le serveur de messagerie électronique a les fonctions suivantes:

- En plus d'exercer les fonctions générales de transmission des courriers électroniques, le serveur de messagerie électronique exécute ses opérations normales d'échange de courriers électroniques avec d'autres serveurs, ou d'envoi et de réception de courriers entre les clients de messagerie électronique; parallèlement, il devrait interdire la fonction de relais ouvert pour empêcher que les spammeurs lui imposent de transmettre des courriers non sollicités à d'autres serveurs.
- Tout abonné doit satisfaire à l'épreuve de vérification avant d'envoyer un courrier électronique par un serveur de messagerie électronique. Des systèmes de courrier électronique différents peuvent utiliser des mécanismes de vérification différents. L'opération de vérification intervient entre le serveur de messagerie électronique et le client de messagerie électronique.
- Tout fournisseur de services de messagerie électronique peut avoir une liste noire sur les spammeurs, liste dans laquelle sont répertoriés certains renseignements tels que le nom d'hôte, le nom de domaine ou encore l'adresse e-mail. Le serveur refuse de recevoir les courriers émanant de ces spammeurs.

- Le serveur peut renvoyer une demande de vérification à la source, qui est indiquée dans les renseignements (par exemple, DNS, nom d'hôte ou autres) sur l'expéditeur du courrier; si cette demande ne confirme pas l'authenticité de la source, le serveur rejettera le courrier électronique incriminé.
- Des spammeurs peuvent utiliser certaines commandes du protocole SMTP pour deviner le vrai compte du serveur de messagerie électronique, lequel interdit des commandes comme EXPN et VRFY.
- Des courriers publicitaires ou de propagande sont envoyés sans aucune information sur l'expéditeur. Le serveur devrait automatiquement ajouter un lien HTTP dans le corps du courrier électronique. Au besoin, les utilisateurs peuvent soumettre des rapports de réclamation.
- Les serveurs détectent les courriers électroniques non sollicités grâce à une technologie antispam et les signalent à la sous-entité de traitement antispam, à partir de laquelle ils téléchargent des règles de filtrage.
- Lorsqu'un spam est détecté, le serveur devrait le sauvegarder dans sa forme originelle qui comporte au moins l'en-tête du courrier source, et le soumettre à l'épreuve des filtres.
- Le serveur de messagerie électronique devrait fournir au système ses informations journalières et statistiques qui sont sauvegardées périodiquement et les soumettre à la sous-entité de traitement antispam.
- Le serveur de messagerie électronique renvoie un numéro d'état différent selon des règles différentes.
- Le serveur de messagerie électronique peut limiter le volume de trafic envoyé par un certain utilisateur du courrier électronique.

7.3 Fonctions de l'entité de traitement antispam

L'entité de traitement antispam a les fonctions suivantes:

- Echanger les règles de filtrage avec d'autres entités de traitement antispam; divers protocoles peuvent être utilisés pour la transmission des informations, tels que FTP et HTTP.
- Mémoriser les informations originelles des courriers non sollicités provenant des utilisateurs et des sous-entités de traitement antispam.
- Diffuser les règles de filtrage aux sous-entités de traitement antispam, et mettre en garde ces dernières contre les courriers électroniques dangereux.
- L'entité de traitement antispam devrait administrer et gérer les règles de filtrage, qui peuvent être obtenues via un site web pour:
 - recevoir les rapports des utilisateurs et des sous-entités de traitement antispam;
 - diffuser les renseignements faisant autorité, en particulier ceux concernant la supervision et la gestion.

7.4 Fonctions de la sous-entité de traitement antispam

La sous-entité de traitement antispam a les fonctions suivantes:

- Recevoir les rapports de réclamation des utilisateurs ainsi que les règles de filtrage émanant de l'entité de traitement antispam.
- Stocker les informations originelles sur les spams provenant des utilisateurs (au moins leur en-tête) et des autres entités.

- Diffuser les règles de filtrage aux serveurs de messagerie électronique ou aux clients de messagerie électronique, et mettre en garde les utilisateurs contre les courriers électroniques dangereux en tant que de besoin.
- Suivre la propagation des spams et collecter les renseignements y relatifs.
- Rendre compte de l'évolution de la propagation des spams et des informations y relatives aux entités situées à des niveaux supérieurs.
- Créer de nouvelles règles de filtrage à partir des courriers douteux sauvegardés, vérifier et modifier les règles de filtrage existantes. Ces règles pouvant être obtenues à partir d'un site web pour:
 - créer les rapports de spam en provenance d'utilisateurs et de serveurs de messagerie électronique;
 - créer de nouvelles règles de filtrage.

8 Identification des spams par courrier électronique

Le présent paragraphe décrit les caractéristiques courantes des spams par courrier électronique ainsi que les critères applicables.

8.1 Caractéristiques courantes des spams par courrier électronique

Les spams par courrier électronique présentent les caractéristiques courantes suivantes:

- L'adresse véritable de l'expéditeur est cachée ou falsifiée
Le contenu de "from" ou "sender" du champ Expéditeur est laissé en blanc ou n'est pas valable.
- La source véritable du courrier est cachée ou falsifiée.
Le "message-id" du champ Identification est laissé en blanc ou n'est pas valable.
- L'expéditeur est un spammeur connu
Une adresse de spammeur provenant d'une liste noire est incluse dans "from" ou "sender" du champ Expéditeur.
- Les informations concernant le destinataire sont fausses
Le contenu du champ Destinataire ("to") ou du champ Destinataire en copie ("cc") est faux ou concerne des spammeurs.
- Utilisation de termes propres aux spammeurs
Des termes propres aux spammeurs figurent dans le champ Sujet ("subject") ou dans le contenu du courrier électronique.
- Les informations de relais sont fausses
Le contenu de "resent-from" ou "resent-sender" du champ Nouvelle transmission est erroné.
- Les informations de trace sont fausses
Un contenu frauduleux figure dans le champ Trace.
- La taille est impropre
La taille de l'ensemble du courrier électronique, du champ d'en-tête ou du contenu du courrier est identique à la taille du champ d'en-tête et du contenu de courriers non sollicités.
- Un trop grand nombre de destinataires
Le nombre de destinataires dans certains champs est trop élevé.
- Le nombre de sauts de retransmission est trop élevé
Le nombre de traces dans le champ Trace est trop élevé.

- L'adresse IP de l'expéditeur figure dans certains champs
Des informations concernant des spammeurs figurent dans "from" ou "sender" du champ Expéditeur.
- L'adresse IP du serveur de messagerie électronique se trouve dans certains champs
Des informations concernant des spammeurs figurent dans "received" du champ Trace, ou dans "resent-from" ou "resent-sender" du champ Nouvelle transmission.
- Nouveau spam
L'entité de traitement antispam peut résumer des caractéristiques à partir du nouvel échantillon de spam, et créer les règles de filtrage correspondantes.

8.2 Règles communes pour combattre le spam par courrier électronique

Des règles individuelles peuvent être regroupées dans une règle composée avec des priorités différentes.

Le serveur de messagerie électronique peut appliquer une règle individuelle et/ou composée pour faire face à du spam.

8.2.1 Règles fondamentales communes

Le serveur de messagerie électronique peut fixer les critères selon les facteurs suivants:

- Le champ Expéditeur ("from" ou "sender") est laissé en blanc ou son contenu n'est pas valable.
- Le champ Identification ("message-id") est laissé en blanc ou son contenu n'est pas valable.
- Le champ Expéditeur ("from" ou "sender") comporte des mots clés qui figurent dans une liste noire.
- Des mots clés donnés par une liste noire figurent dans le champ Destinataire ("to") ou dans le champ Destinataire en copie ("cc").
- Le sujet ("subject") ou le contenu du courrier électronique comporte des mots clés donnés.
- La vraie source originelle ne peut pas être trouvée dans "resent-from" ni dans "resent-sender" du champ Nouvelle transmission, ou dans le contenu du champ Trace.
- La taille de tout le courrier électronique, du champ d'en-tête ou du contenu du courrier est (approximativement) égale à une valeur donnée.
- Le nombre total d'adresses définies dans "to", "cc" et "bcc" du champ Expéditeur excède la limite fixée par le serveur de messagerie électronique; ou le nombre de fois qu'un même courrier électronique doit être délivré excède la limite fixée par le serveur de messagerie électronique.
- Le nombre de traces dans le champ Trace excède la limite fixée par le fournisseur de services de courrier électronique ou l'administrateur de ce domaine.
- Le résultat de l'opération DNS inverse qui fait suite aux informations de "from" ou "sender" dans le champ Expéditeur figure dans la liste noire spécifique.
- Le résultat de l'opération DNS inverse qui devrait faire suite au "received" dans le champ Trace, au "resent-from" ou au "resent-sender" dans le champ Nouvelle transmission figure dans une liste noire spécifique.
- Si un spam par courrier électronique ne peut pas être identifié au moyen d'une règle simple, il est demandé d'utiliser une règle composée.

8.2.2 Ordre de priorité des critères

Confirmer l'ordre de priorité des critères. Si un courrier électronique relève de plusieurs règles (cas de conflit entre règles), il sera traité selon la règle pourvue de la priorité la plus haute. Dans le cas

d'une égalité de priorité entre deux règles, c'est la règle finale utilisée selon le principe de priorité en cas de conflit qui sera utilisée. Un conflit doit être évité dans toute la mesure du possible.

8.2.3 Détection de conflits entre critères

Une fonction sert à détecter les conflits entre différents critères attribués. Quelles sont les situations de conflit les plus courantes?

- Les deux "conditions de règle" comprennent le même type de "règles simples" (règles fondamentales) de la classe recherche de mots clés (par exemple "le sujet comporte XXX", "ce qui est décodé des 10 premières lignes comprend XXX", etc.), et les mots clés dans l'une et l'autre "règles simples" sont les mêmes et un mot clé en comporte un autre.
- Les deux "conditions de règle" comprennent le même type de "règles simples" de la classe IP restreint (par exemple "l'IP du client est XXX", etc.), et l'un et l'autre espaces IP indiqués dans les "règles simples" sont identiques ou sont pourvus d'un ensemble d'intersections.
- Les deux "conditions de règle" comprennent le même type de "règles simples" de la classe taille restreinte, et les conditions de taille restreinte sont du type "la taille de XXX est la valeur fixée" (elle ne peut pas être "plus que" ou "moins que"), et les valeurs sont identiques. Par exemple, les deux règles comprennent la même règle simple: "la taille du texte du courrier électronique est de 5 343 octets".

9 Méthodes de lutte contre le spam par courrier électronique

Les principales méthodes pour lutter contre le spam par courrier électronique consistent à désactiver la fonction de relais ouvert du serveur de messagerie électronique, à maîtriser l'autorisation de délivrance de courriers électroniques et à utiliser des techniques de filtrage. Le système de lutte contre le spam par courrier électronique devrait prendre en charge, ou prendre en charge facultativement, les méthodes suivantes.

9.1 Désactiver la fonction de relais ouvert

L'expression relais ouvert signifie que le serveur de messagerie électronique relaie tous les courriers électroniques entrants, que les expéditeurs ou destinataires soient ou non des abonnés légitimes. En général, si le serveur active la fonction de relais illimité, on considère qu'il s'agit d'un relais ouvert.

9.2 Maîtriser l'autorisation de délivrance des courriers électroniques

Pour empêcher des utilisateurs non autorisés d'utiliser le serveur de messagerie électronique,

- les expéditeurs doivent être des abonnés légitimes du serveur;
- le serveur devrait certifier les adresses IP des expéditeurs;
- le nombre de sauts de courrier électronique est limité pour éviter une propagation exponentielle du spam;
- le serveur de messagerie électronique peut vérifier la source du courrier électronique pour s'assurer de l'authenticité.

9.3 Technique de filtrage

La technologie de filtrage peut être divisée en deux classes: le filtrage par adresses IP et le filtrage par balayage des textes.

9.3.1 Filtrage par adresses IP

Le filtrage par adresses IP peut limiter la connexion au protocole SMTP du système de courrier électronique. Ses attributs essentiels sont l'intervalle IP et les modes de restriction.

L'intervalle IP comprend:

- l'intervalle IP en temps réel, émanant de l'entité de traitement antispam;
- l'intervalle IP en temps réel, émanant des règles de filtrage d'autres organisations;
- l'intervalle IP en temps réel, auto-ajouté.

Les modes de restriction sont:

- le refus de connexion;
- la permission de connexion sans condition;
- les connexions répétées depuis un même IP de client au serveur de messagerie électronique devraient être limitées à une certaine période de temps.

Si cet IP appartient à l'intervalle IP donné, les modes de restriction seront adoptés.

9.3.2 Filtrage par balayage du texte

Les règles de filtrage peuvent être fixées par le serveur de messagerie électronique et téléchargées depuis l'entité de traitement antispam. Elles peuvent être modifiées par les administrateurs sous certaines conditions.

Si un courrier électronique relève d'une certaine règle, il sera classé en fonction du comportement correspondant. Les comportements des règles de balayage du texte sont:

- Rejet: renvoyer le message de rejet à l'expéditeur après extraction des caractéristiques.
- Abandon: réponse normale pour chaque commande dépourvue de tout comportement.
- Délivrance: délivrance normale. L'abandon est ignoré après que la délivrance a été choisie.
- Etiquette: ajouter l'étiquette spécifique dans l'en-tête.
- Rapport: signaler au centre de rapports les caractéristiques extraites du courrier électronique.
- Tampon: garder le courrier électronique intact autant que possible, et en envoyer copie à l'entité de traitement antispam.

9.4 Examen de la traçabilité

Il est parfois difficile de détecter si l'expéditeur est un abonné valable. Comme il est impossible pour le serveur de réception des courriers électroniques d'obtenir toutes les informations sur le serveur d'expédition, le premier nommé ne peut pas certifier toutes les informations à l'intention des abonnés licites.

Les courriers électroniques peuvent être divisés en deux types: ceux dont on peut suivre la trace et les autres. Les courriers poubelles "traçables" seront soumis à des règles de filtrage si les avertissements sont inopérants. Il est difficile de se débarrasser des courriers poubelles non traçables car ils utilisent le plus souvent une fausse source de courrier électronique. La plupart des courriers qui ne sont pas traçables sont des courriers poubelles, de sorte que l'examen de la traçabilité est la base de la lutte contre le spam par courrier électronique. Il est recommandé de procéder selon les trois étapes suivantes:

Première étape: le besoin

- La plupart des serveurs de réception de courriers électroniques (le "MX" dans le nom de domaine) sont également des serveurs d'expédition de courriers électroniques.
- La plupart des serveurs de réception et des serveurs d'expédition qui ont une fonction unique ont des IP voisins les uns par rapport aux autres.
- D'autres ordinateurs susceptibles de délivrer des courriers électroniques peuvent avoir des IP voisins avec les serveurs de messagerie électronique "MX".

- Certains serveurs de messagerie électronique peuvent être consultés avec l'opération DNS inverse, et le résultat est le même que celui que prétend l'abonné.

Deuxième étape: mécanisme d'avis de traçabilité

Prise en charge de la certification sur le réseau de télécommunication:

- Confirmation que le champ Courrier électronique de l'expéditeur est autorisé.
- Confirmation que l'expéditeur est l'abonné licite du champ Courrier électronique.

Troisième étape: mécanisme de retour en arrière

- Le service de traçabilité et l'examen de traçabilité constituent une chaîne de retour en arrière.
- La chaîne de retour en arrière ne peut pas être falsifiée.
- Il est facile de distinguer une partie falsifiée d'une partie authentique.

Le système de trace peut procéder à des vérifications automatiques grâce à la chaîne de retour en arrière.

10 Interconnexion entre les domaines de traitement antispam

Lorsque des domaines de traitement antispam s'interconnectent, il est possible de choisir entre trois modes: l'interconnexion entre des entités de traitement de premier niveau, l'interconnexion entre entités de traitement et sous-entités de traitement et l'interconnexion entre sous-entités de traitement et serveurs de messagerie électronique. Chaque choix peut être dicté par certains scénarios ou besoins.

10.1 Interconnexion entre des entités de traitement de premier niveau

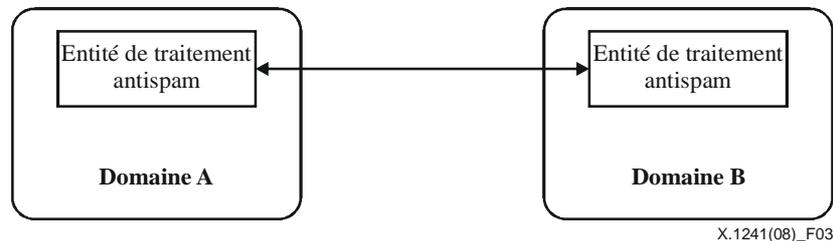


Figure 3 – Interconnexion entre entités de traitement de premier niveau

Le mode d'interconnexion est une connexion bidirectionnelle entre entités de traitement de premier niveau; seules des règles sont échangées entre les deux entités. Si une entité reçoit de l'autre des renseignements, elle appliquera certains mécanismes et procédures pour choisir les règles utiles à partir des informations de réception.

10.2 Interconnexion entre une entité et une sous-entité de traitement

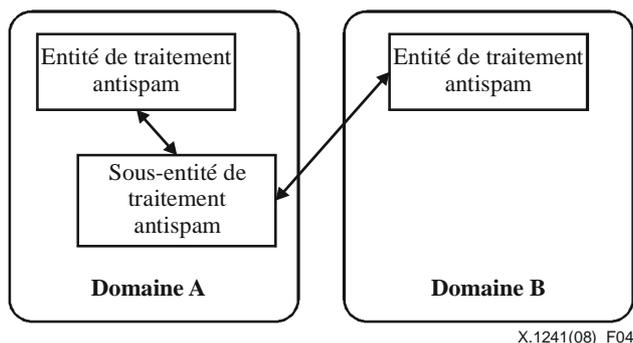


Figure 4 – Interconnexion entre une entité et une sous-entité de traitement

Le mode d'interconnexion est une connexion bidirectionnelle entre une entité et une sous-entité de traitement. La sous-entité devrait télécharger deux tableaux de règles de filtrage à partir des deux entités de traitement. Elle crée des règles selon les courriers douteux reçus des serveurs rattachés; elle devrait signaler les règles aux deux entités.

Ce mode est pourvu d'une certaine sécurité, mais il se fonde sur une relation administrative complexe entre la sous-entité et les deux entités. Ce mode peut présenter des problèmes en termes de modulabilité. Il ne s'agit pas d'une interconnexion totale entre des domaines.

10.3 Interconnexion entre une sous-entité de traitement et un serveur de messagerie électronique

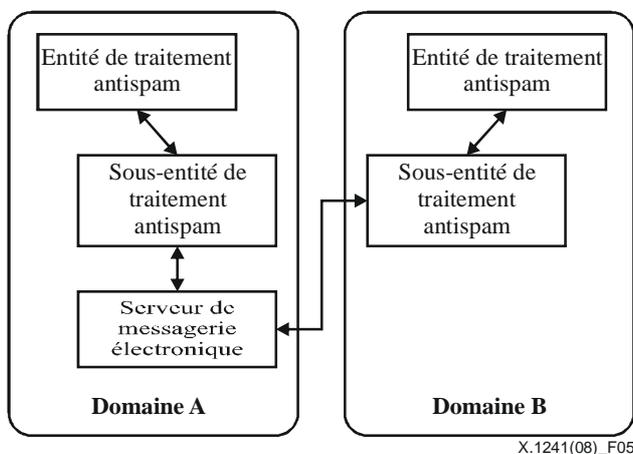


Figure 5 – Interconnexion entre une sous-entité de traitement et un serveur de messagerie électronique

Le mode d'interconnexion est une connexion bidirectionnelle entre une sous-entité de traitement et un serveur de messagerie électronique. Ce dernier téléchargera les règles de filtrage de spams depuis la sous-entité et signalera les courriers poubelles à la sous-entité de l'autre domaine. La sous-entité recevra des rapports concernant ces courriers poubelles du serveur de messagerie électronique et publiera ses propres règles à l'attention du serveur de l'autre domaine.

Ce mode est simple à réaliser entre domaines, mais les serveurs hors domaine peuvent attaquer le domaine de traitement antispam, de sorte que ce mode peut présenter des problèmes de sécurité. Il

présente par ailleurs des problèmes en termes de modulabilité. Il ne s'agit donc pas d'une interconnexion totale entre des domaines.

C'est le mode défini au § 10.1 qui est le plus sûr et qui est donc le mode d'interconnexion recommandé.

Bibliographie

- [b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*.
<<http://www.ietf.org/rfc/rfc1869.txt>>
- [b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3*.
<<http://www.ietf.org/rfc/rfc1939.txt>>
- [b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1*.
<<http://www.ietf.org/rfc/rfc2060.txt>>
- [b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL)*.
<<http://www.ietf.org/rfc/rfc2222.txt>>
- [b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.
<<http://www.ietf.org/rfc/rfc2505.txt>>
- [b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication*.
<<http://www.ietf.org/rfc/rfc2554.txt>>
- [b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.
<<http://www.ietf.org/rfc/rfc2821.txt>>
- [b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.
<<http://www.ietf.org/rfc/rfc2822.txt>>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication