Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1245

(12/2010)

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

Sécurité du cyberespace – Lutte contre le pollupostage

Cadre de lutte contre le spam dans les applications multimédias IP

Recommandation UIT-T X.1245

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
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

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

Recommandation UIT-T X.1245

Cadre de lutte contre le spam dans les applications multimédias IP

Résumé

La Recommandation UIT-T X.1245 décrit le cadre général de lutte contre le spam dans les applications multimédias IP comme la téléphonie IP, la messagerie instantanée, les conférences multimédias, etc. Le cadre comporte quatre groupes de fonctions antispam, à savoir les fonctions antispam centrales (CASF), les fonctions antispam côté destinataire (RASF), les fonctions antispam côté expéditeur (SASF) et les fonctions du destinataire de spams (SRF). Cette Recommandation décrit les fonctionnalités et les interfaces de chaque fonction pour la lutte contre le spam multimédia IP.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1245	2010-12-17	17

Mots clés

Fonctions antispam, spam multimédia IP, 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/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1245

Cadre de lutte contre le spam dans les applications multimédias IP

1 Domaine d'application

La présente Recommandation décrit le cadre général de lutte contre le spam multimédia IP. Ce cadre s'applique aux applications multimédias IP comme la téléphonie IP, la messagerie instantanée, les conférences multimédias, etc. Il comporte quatre groupes de fonctions antispam, à savoir les fonctions antispam centrales (CASF), les fonctions antispam côté destinataire (RASF), les fonctions antispam côté expéditeur (SASF) et les fonctions du destinataire de spams (SRF). La présente Recommandation décrit les fonctionnalités et les interfaces de chaque fonction pour la lutte contre le spam multimédia IP. Les moyens techniques à utiliser pour mettre en œuvre le cadre ne font pas partie du domaine d'application de la présente Recommandation.

Il convient d'examiner la compatibilité des méthodes antispam décrites dans la présente Recommandation avec toutes les lois et règlements applicables avant de les adopter.

2 Références

Néant.

3 Définitions

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1 Termes définis ailleurs

3.1.1 spam [b-UIT-T X.1240]: le sens du mot "spam" dépend de la perception du respect de la vie privée et de ce que constitue le spam au niveau de chaque pays, du point de vue technologique, économique, social et pratique. En particulier, ce sens évolue et se diversifie au fur et à mesure du développement des technologies, donnant lieu à de nouvelles possibilités d'utilisation abusive des communications électroniques. Bien qu'aucune définition du spam n'ait été adoptée à l'échelle mondiale, ce terme est couramment employé pour décrire des communications électroniques de masse non sollicitées transmises par courrier électronique (courriel) ou par messagerie mobile pour promouvoir des produits ou services commerciaux.

3.1.2 spammeur [b-UIT-T X.1240]: entité ou personne qui crée et envoie des spams.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 fonction antispam (ASF) (*anti-spam function*): fonction logique de lutte contre le spam dans les applications multimédias IP. La fonction ASF peut être située dans des éléments de réseau comme un serveur proxy, un serveur d'application, etc.

3.2.2 liste noire: liste de personnes ou de sources utilisant des services de communication auxquelles l'accès à certaines ressources de communication est refusé.

3.2.3 fonction ASF centrale (CASF) (*core ASF*): instance d'une fonction ASF qui identifie et bloque le spam multimédia IP. La fonction CASF dispose de capacités permettant de gérer les politiques antispam et de commander les fonctions RASF et SASF.

3.2.4 spam multimédia IP: message ou appel non sollicité dans une application multimédia IP qui présente généralement les caractéristiques particulières d'un spam comme la diffusion en masse. Distinct du spam traditionnel par courrier électronique, le spam multimédia IP désigne le spam

transmis par des méthodes de communication sur IP, comme les services de messagerie instantanée et de téléphonie IP.

3.2.5 fonction ASF côté destinataire (RASF) (*recipient-side ASF*): instance d'une fonction ASF qui identifie et bloque le spam multimédia IP distribué aux destinataires de spams via la frontière du réseau interne. La fonction RASF peut être située dans les éléments de réseau dans lesquels les demandes de communication entrantes destinées aux destinataires de spams sont envoyées (dernier bond).

3.2.6 fonction ASF côté expéditeur (SASF) (*sender-side ASF*): instance d'une fonction ASF qui identifie et bloque le spam multimédia IP distribué par les spammeurs à la frontière du réseau externe. La fonction SASF peut être située dans les éléments de réseau dans lesquels les demandes de communication sortantes provenant des spammeurs sont envoyées (premier bond).

3.2.7 destinataire de spams: entité ou personne qui reçoit des spams.

3.2.8 fonction du destinataire de spams (SRF) (*spam recipient function*): fonction ASF dont le rôle est d'identifier et de bloquer le spam multimédia IP arrivé aux destinataires de spams. La fonction SRF peut être située dans le réseau domestique ou dans les terminaux des destinataires de spams.

3.2.9 liste blanche: liste de personnes ou de sources utilisant des services de communication qui sont connues, fiables ou bénéficient d'une autorisation explicite.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ARS système de réponse automatique (*automated response system*)

ASF fonctions antispam (*anti-spam functions*)

CA autorité de certification (*certification authority*)

CAS antispam central (*core anti-spam*)

CASF fonctions antispam centrales (*core anti-spam functions*)

CRL liste de révocation de certificats (*certificate revocation list*)

DAC contrôle d'accès discrétionnaire (*discretionary access control*)

HBAC contrôle d'accès basé sur l'historique (*history-based access control*)

IM messagerie instantanée (*instant messaging*)

IP protocole Internet (*internet protocol*)

IPSec sécurité du protocole Internet (*internet protocol security*)

L2TP protocole de tunnellisation de couche 2 (*layer 2 tunneling protocol*)

MAC contrôle d'accès obligatoire (*mandatory access control*)

MTA agent de transfert de courrier (*mail transfer agent*)

NDAC contrôle d'accès non discrétionnaire (*non-discretionary access control*)

OTP mot de passe à usage unique (*one time password*)

PBAC contrôle d'accès basé sur l'objet (*purpose-based access control*)

PKI infrastructure de clé publique (*public key infrastructure*)

RAS antispam côté destinataire (*recipient-side anti-spam*)

RASF fonctions antispam côté destinataire (*recipient-side anti-spam functions*)

RBAC contrôle d'accès basé sur le rôle (*role-based access control*)

RuBAC contrôle d'accès basé sur une règle (*rule-based access control*)

SAS antispam côté expéditeur (*sender-side anti-spam*)

SASF fonctions antispam côté expéditeur (*sender-side anti-spam functions*)

SPF cadre des politiques de l'expéditeur (*sender policy framework*)

SR destinataire de spams (*spam recipient*)

SRF fonctions du destinataire de spams (*spam recipient functions*)

SSL couche de connecteurs sécurisés (*secure socket layer*)

TCAC contrôle d'accès basé sur des contraintes temporelles (*temporal constraints access control*)

TTP tierce partie de confiance, tiers de confiance (*trusted third party*)

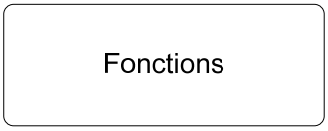
TTS texte vers parole (*text to speech*)

VoIP téléphonie utilisant le protocole Internet, téléphonie IP (*voice over internet protocol*)

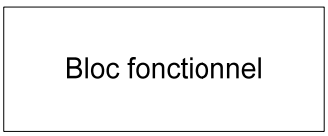
VPN réseau privé virtuel (*virtual private network*)

5 Conventions

Fonctions: dans le contexte du cadre de lutte contre le spam multimédia IP, des "fonctions" sont définies comme étant un ensemble de fonctionnalités. Elles sont représentées par le symbole suivant:



Bloc fonctionnel: dans le contexte du cadre de lutte contre le spam multimédia IP, un "bloc fonctionnel" est défini comme étant un groupe de fonctionnalités considéré comme un tout dans la présente Recommandation. Il est représenté par le symbole suivant:



6 Méthodes techniques de lutte contre le spam multimédia IP

Le spam multimédia IP peut être défini comme un message ou un appel non sollicité dans une application multimédia IP. Distinct du spam traditionnel par courrier électronique, le spam multimédia IP est le spam transmis par des méthodes de communication sur IP, comme la téléphonie IP, la messagerie instantanée, etc. Le spam multimédia IP présente généralement des caractéristiques particulières qui permettent de le distinguer des applications multimédias IP normales. Ces caractéristiques peuvent être utilisées dans des fonctions antispam mises en œuvre dans des éléments de réseau IP appropriés afin d'identifier et de filtrer le spam. Les méthodes techniques de lutte contre le spam multimédia IP peuvent être classées dans les trois catégories suivantes:

– Analyse de la source des applications multimédias IP.

– Analyse des caractéristiques des applications multimédias IP.

– Analyse du contenu des applications multimédias IP.

La Figure 1 présente les trois méthodes techniques de lutte contre le spam multimédia IP et des exemples de techniques antispam.

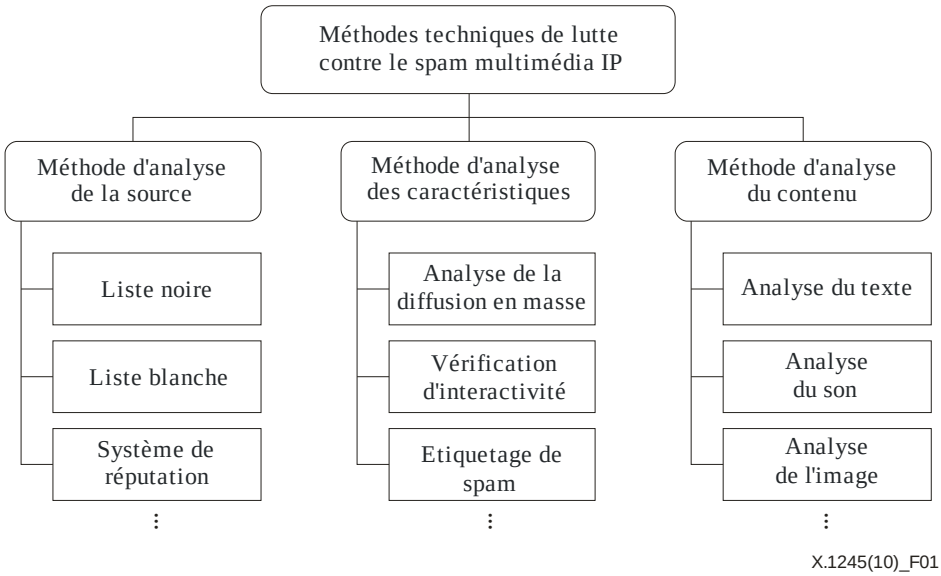


Figure 1 – Méthodes techniques de lutte contre le spam multimédia IP

De nombreuses techniques antispam indiquées sur la Figure 1 ont été appliquées pour la lutte contre le spam de courrier électronique et sont également applicables pour la lutte contre le spam multimédia IP. Les techniques de lutte contre le spam multimédia IP ne se limitent pas à ces exemples.

Concernant l'utilisation de ces techniques antispam, une interaction est nécessaire entre les fonctions antispam sur le réseau IP. Les fonctions et les interfaces des entités antispam nécessaires à la mise en œuvre des méthodes antispam sont décrites dans les paragraphes qui suivent. Pour lutter contre le spam multimédia IP, l'utilisation d'une seule technique antispam ne sera peut-être pas suffisamment efficace, auquel cas il pourra être nécessaire de mettre en œuvre simultanément plusieurs techniques antispam sur le réseau IP afin de filtrer le spam plus efficacement.

6.1 Méthode d'analyse de la source

On peut déterminer si une application multimédia IP provenant d'une certaine source est un spam ou non en analysant les informations relatives à la source de cette application comme les informations de réputation ou l'historique d'envoi de spams depuis cette source. L'adresse IP, le nom de domaine, le numéro de téléphone et l'identificateur de l'utilisateur peuvent être utilisés comme identificateurs de la source.

Parmi les exemples de techniques antispam basées sur la source, on peut citer la liste blanche, la liste noire, le système de réputation, etc. Ces techniques sont largement utilisées pour la lutte contre le spam de courrier électronique et peuvent aussi être appliquées pour la lutte contre le spam multimédia IP. L'applicabilité de ces techniques au spam multimédia IP est décrite dans [b-UIT-T X.1244]. Toutefois, les méthodes d'analyse de la source peuvent présenter certains points faibles qui diminuent l'efficacité des techniques antispam, par exemple les spammeurs peuvent essayer d'usurper l'identité de l'expéditeur ou peuvent créer de nombreux comptes de service. Par

conséquent, les mesures suivantes devraient contribuer à accroître l'efficacité des techniques antispam basées sur la source face au spam multimédia IP:

– Authentification forte des sources d'applications multimédias IP.

– Gestion efficace de la politique d'identification du spam et des informations connexes.

Tout d'abord, pour filtrer le spam efficacement, une grande fiabilité des informations relatives à la source des applications multimédias IP est nécessaire, car les spammeurs peuvent essayer de contourner ces techniques antispam en créant un grand nombre de comptes de service ou en tentant d'usurper l'identité de l'expéditeur pour masquer le fait que l'expéditeur est un spammeur. Par conséquent, une authentification forte des sources d'applications multimédias IP peut être utile pour garantir une grande fiabilité des informations relatives aux sources.

Comme décrit ci-dessus, on utilise des informations de filtrage du spam (par exemple liste blanche, liste noire, etc.) et les sources d'applications multimédias IP pour identifier le spam. Il faut donc gérer efficacement les informations de filtrage du spam et les critères d'identification du spam.

Cette technique a cet avantage que le spam peut être bloqué avant qu'il ne soit distribué au destinataire. De plus, dans l'hypothèse où les considérations ci-dessus sont satisfaites, cette technique nécessite relativement peu d'efforts pour lutter efficacement contre le spam par rapport aux autres techniques antispam comme l'analyse du contenu, l'analyse des caractéristiques, etc.

6.2 Méthode d'analyse des caractéristiques

6.2.1 Méthodes antispam basées sur une analyse des caractéristiques

Le spam multimédia IP présente de nombreuses caractéristiques particulières qui permettent de le distinguer des applications multimédias IP normales. Par exemple, le spam multimédia IP est parfois diffusé en masse et son interactivité est limitée par rapport aux applications multimédias IP normales. Une application multimédia IP peut être considérée comme étant un spam et éliminée par filtrage lorsqu'elle présente une ou plusieurs des caractéristiques suivantes (la liste n'est toutefois pas exhaustive):

– Diffusion en masse

Le spam multimédia IP est parfois diffusé en masse car les spammeurs essayent généralement d'envoyer des spams à un grand nombre de destinataires à la fois pour réduire leurs coûts au minimum. Lorsque de nombreuses applications multimédias IP sont distribuées depuis une source vers de nombreuses destinations en peu de temps, elles peuvent être considérées comme des spams potentiels.

– Interactivité limitée

Souvent, le spam multimédia IP n'offre qu'une interactivité limitée car les spammeurs ont tendance à envoyer des spams en utilisant des machines plutôt que des personnes afin de réduire leurs coûts. Par exemple, l'expéditeur d'un spam de messagerie instantanée ou d'un spam de bavardage en ligne ne répondra peut-être pas si le spam est envoyé par une machine. Le spam de téléphonie IP, une forme de télémarketing, peut aussi offrir une interactivité limitée lorsqu'il est envoyé au moyen d'un système ARS. Il est possible par conséquent d'identifier le spam en vérifiant si l'expéditeur de l'application multimédia IP offre ou non une certaine interactivité. Les techniques antispam basées sur cette méthode les plus courantes dans les systèmes de courrier électronique sont le test de Turing et la liste grise, qui permettent respectivement de vérifier l'interactivité de l'expéditeur et de l'agent MTA.

6.2.2 Utilisation d'informations de protocole pour la lutte contre le spam

Il est plus efficace d'utiliser les informations de protocole que d'utiliser les informations de contenu pour identifier le spam lorsqu'on utilise la méthode d'analyse des caractéristiques. La partie protocole d'une application multimédia IP peut être utilisée pour identifier le spam via une analyse

de la source de cette application. L'identification du spam grâce aux informations de protocole avant que le contenu des applications multimédias IP soit distribué au destinataire demande moins d'efforts et est plus efficace que d'autres techniques antispam qui utilisent les informations de contenu. Les considérations suivantes corroborent cette conclusion:

– Informations relatives à la fourniture des applications

La partie protocole des applications multimédias IP achemine des informations relatives à la fourniture de ces applications, par exemple la source, la destination, l'heure de distribution, le protocole de distribution utilisé, etc. Certaines de ces parties protocole peuvent être utilisées pour identifier le spam.

– Moment d'analyse

Les informations de protocole pour le lancement d'un service sont distribuées avant le contenu des applications multimédias IP. Par exemple, dans le service de téléphonie IP, le processus de signalisation pendant lequel les informations de protocole sont utilisées est exécuté avant que la session d'appel soit lancée. Il peut donc être possible d'identifier un spam avant qu'il ne soit distribué au destinataire via une analyse des informations de protocole.

– Chiffrement

Les messages de protocole sont généralement distribués sans chiffrement, alors que le contenu des applications multimédias IP peut être distribué avec chiffrement. Le chiffrement de paquets IP rend leur analyse très difficile voire impossible à décrypter. Par conséquent, il peut être plus facile d'analyser la partie protocole plutôt que la partie contenu des applications multimédias IP.

– Type de média

La partie protocole des applications multimédias IP n'utilise qu'un seul type de média alors que la partie contenu achemine parfois des informations multimédias qui sont difficiles à analyser.

– Trajet de distribution

Les messages de protocole pour le lancement d'une session ou d'un service transitent par des équipements de réseau, par exemple un serveur d'application pour la messagerie instantanée et des serveurs proxy pour les communications de téléphonie IP, qui peuvent obtenir des informations relatives à la fourniture des applications multimédias IP à partir de ces messages. Quant aux messages de contenu, ils peuvent être distribués directement de l'expéditeur au destinataire sans transiter par ces équipements de réseau. Dans ce cas, le contenu des applications multimédias IP peut être difficile à analyser.

6.3 Méthode d'analyse du contenu

Dans la méthode d'analyse du contenu, on utilise le résultat de l'analyse du contenu des applications multimédias IP pour identifier le spam. Cette méthode est largement utilisée pour la lutte contre le spam de courrier électronique. L'analyse de contenu peut être beaucoup plus difficile dans le cas des applications multimédias IP que dans le cas des courriers électroniques car les applications multimédias IP peuvent être en temps réel et/ou utiliser des informations multimédias tandis que les courriers électroniques sont généralement des messages de texte et ne sont pas en temps réel. Les considérations suivantes sont destinées à permettre de lutter efficacement contre le spam multimédia IP dans la méthode d'analyse du contenu:

– Durée de l'analyse du contenu

Le contenu doit être analysé dans un délai acceptable pour permettre aux utilisateurs d'une application multimédia IP de déterminer s'il s'agit d'un spam. Dans le cas des applications multimédias IP en temps réel, il se peut que l'analyse de contenu ne puisse pas être réalisée avant le lancement de l'application.

– Précision de l'analyse du contenu

L'analyse du contenu des applications multimédias IP doit être suffisamment précise pour pouvoir identifier le spam efficacement. Des technologies très évoluées de reconnaissance vocale et de l'image seront utiles car l'analyse de contenu multimédia est très difficile comparée à l'analyse de contenu textuel.

– Chiffrement du contenu

L'analyse de contenu des applications multimédias IP peut être très difficile voire impossible à décrypter lorsque les paquets IP sont chiffrés.

– Trajet de distribution du contenu

Le contenu d'une application multimédia IP est analysé lorsqu'il transite par certains équipements de réseau, par exemple un serveur d'application ou un serveur de média, qui ont une fonction d'analyse du contenu.

Dans de nombreux cas, les applications multimédias IP ne pourront pas satisfaire aux critères requis. Dans le cas des applications multimédias IP en temps réel comme la téléphonie IP, il semble impossible de détecter et de filtrer le spam via une analyse de contenu dans un délai acceptable pour les utilisateurs du service, car cette analyse n'est possible qu'une fois la session de communication établie entre l'appelant et l'appelé. En revanche, dans le cas des applications multimédias IP qui ne sont pas en temps réel comme les messages vocaux enregistrés, on pourrait avoir le temps de procéder à l'analyse du contenu. Néanmoins, il pourra être difficile, dans le cadre de l'analyse du contenu, d'obtenir suffisamment d'informations pour identifier le spam, faute de technologies de reconnaissance vocale et de l'image suffisamment développées ou d'un volume de contenu suffisant. Lors de l'analyse du contenu d'applications multimédias IP basées sur du texte comme les services de messagerie instantanée et les services de messages textuels, il peut également être difficile d'identifier le spam lorsque le contenu est chiffré ou distribué directement entre les utilisateurs de service sans transiter par un équipement de réseau adapté pour l'analyse de contenu.

7 Cadre de lutte contre le spam multimédia IP

Les entités de réseau IP ayant des fonctions antispam doivent interagir entre elles pour lutter contre le spam multimédia IP. Le présent paragraphe décrit les fonctions et interactions des entités antispam nécessaires pour la mise en œuvre des méthodes antispam. Pour lutter contre le spam multimédia IP, l'utilisation d'une seule technique antispam ne sera peut-être pas suffisamment efficace. Il pourra donc être nécessaire de mettre en œuvre simultanément plusieurs techniques antispam sur le réseau IP afin de filtrer le spam plus efficacement.

Le présent paragraphe décrit le cadre de lutte contre le spam multimédia IP. Ce cadre est conçu de manière à pouvoir être facilement étendu à divers moyens techniques de lutte contre le spam dans diverses applications et divers réseaux. Il est conçu pour assurer la protection des utilisateurs et des réseaux vis-à-vis du spam multimédia IP. Etant donné que le spam peut apparaître n'importe où, des mécanismes de détection et de filtrage du spam doivent être prévus dans l'ensemble du réseau.

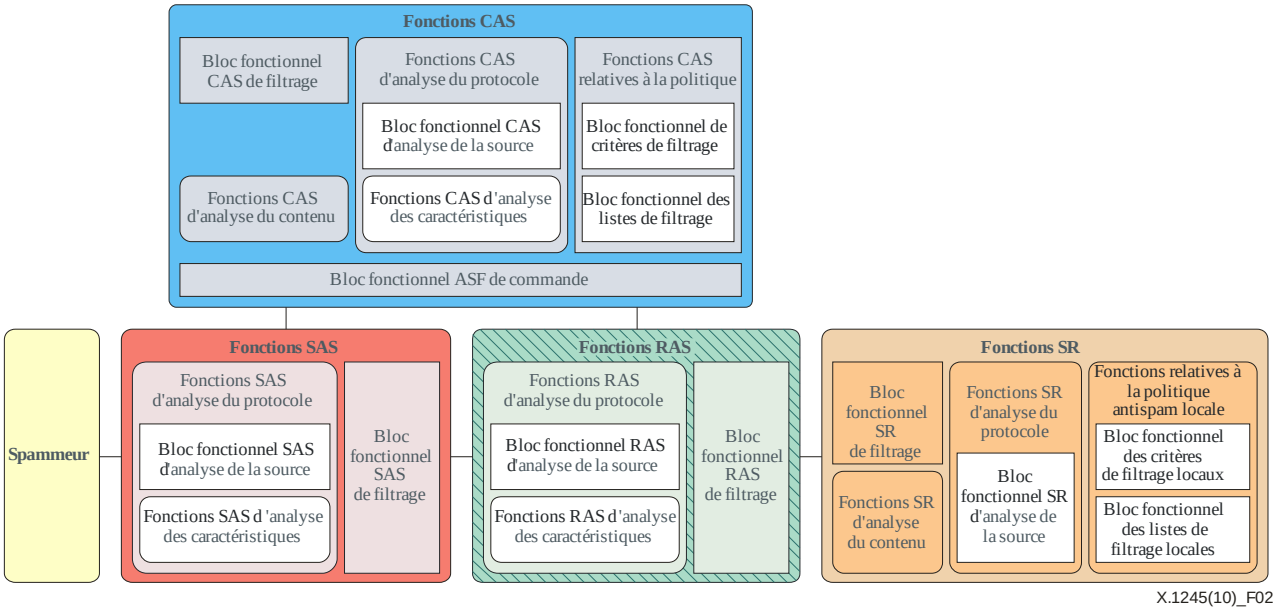


Figure 2 – Cadre de lutte contre le spam multimédia IP

Le cadre de lutte contre le spam multimédia IP est constitué des cinq éléments indiqués sur la Figure 2. Les paragraphes qui suivent décrivent les fonctions et interfaces de chaque élément.

7.1 Spammeur

Le spammeur crée un spam et le répand à travers le réseau. C'est l'expéditeur du spam. Aucune fonction antispam n'est mise en œuvre au niveau du spammeur.

7.2 Fonctions SAS

Les fonctions SASF (*sender-side anti-spam functions*) constituent un groupe de fonctions antispam dont le rôle est d'identifier et de bloquer le spam multimédia IP qui est lancé par les spammeurs. Elles peuvent être mises en œuvre dans des éléments de réseau (serveur proxy par exemple) dans lesquels les demandes de communication sortantes provenant des spammeurs sont envoyées (premier bond). Les fonctions SASF interagissent avec les fonctions CASF (*core anti-spam functions*) pour l'exécution des fonctions antispam dans les fonctions SASF. Il est plus efficace de bloquer un spam côté source avant qu'il ne se répande à travers le réseau, même si les fonctions SASF jouent peut-être un rôle moins actif que d'autres composants dans l'environnement de communication réel.

Les fonctions SASF sont constituées des fonctions SAS d'analyse du protocole et du bloc fonctionnel SAS de filtrage pour la commande du filtrage du spam. Les paragraphes qui suivent décrivent diverses techniques que les fonctions SASF peuvent adopter pour lutter contre le spam multimédia IP.

7.2.1 Bloc fonctionnel SAS de filtrage

Le bloc fonctionnel SAS de filtrage détermine si l'application multimédia IP analysée est un spam ou non, compte tenu du résultat de l'analyse par les fonctions SAS d'analyse du protocole et de la politique antispam. Il interagit donc avec les fonctions CASF et les autres fonctions ou blocs fonctionnels antispam des fonctions SASF.

7.2.2 Fonctions SAS d'analyse du protocole

Les fonctions SAS d'analyse du protocole analysent les informations de protocole relatives aux applications multimédias IP reçues. Elles sont constituées du bloc fonctionnel SAS d'analyse de la

source et des fonctions SAS d'analyse des caractéristiques qui analysent respectivement les informations de source et les caractéristiques relatives aux applications multimédias IP reçues.

i) Bloc fonctionnel SAS d'analyse de la source

Les fonctions SASF peuvent distinguer le spam multimédia IP des applications multimédias IP qui ne sont pas du spam sur la base des informations relatives à la source des applications multimédias IP. Deux opérations des fonctions SASF se rapportent à la source des applications multimédias IP: le filtrage de la source compte tenu de la politique antispam fournie par les fonctions CASF, d'une part, et l'authentification de l'expéditeur, d'autre part.

– Politique antispam

Les fonctions SASF peuvent identifier et filtrer le spam en utilisant l'adresse de source du paquet de données multimédias IP. Le filtrage n'est pas effectué uniquement sur la base de l'adresse de source mais aussi sur la base d'autres informations de protocole qui sont disponibles dans les fonctions SASF. La Figure 3 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP via l'analyse de la source dans les fonctions SASF.

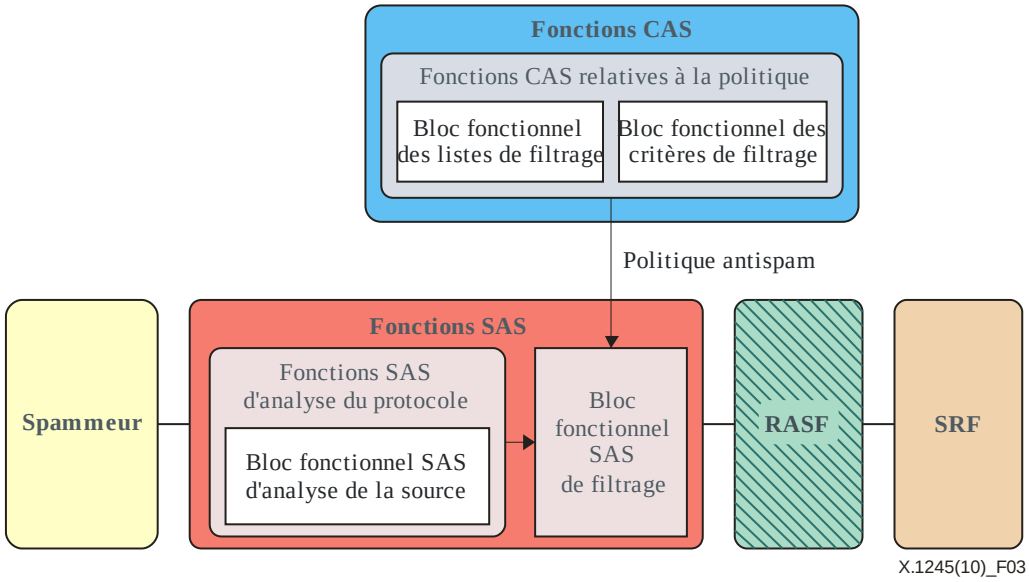


Figure 3 – Lutte contre le spam multimédia IP via l'analyse de la source dans les fonctions SASF

Le bloc fonctionnel SAS de filtrage peut obtenir la politique antispam auprès des fonctions CAS relatives à la politique. Il filtre les paquets IP envoyés par le spammeur qui sont identifiés comme étant du spam compte tenu du résultat de l'analyse.

– Authentification de l'expéditeur

Les fonctions SASF disposent des informations d'authentification de l'expéditeur et peuvent procéder à l'authentification de l'utilisateur à l'origine du trafic. Elles peuvent empêcher les entités non autorisées d'utiliser les applications multimédias IP lorsque c'est nécessaire.

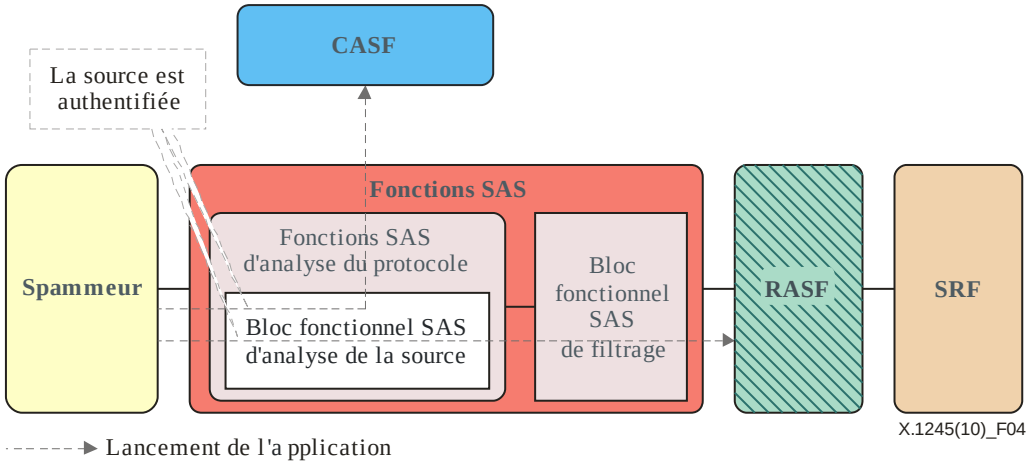


Figure 4 – Authentification de la source par les fonctions SASF

La Figure 4 illustre l'authentification de la source par les fonctions SASF. La capacité d'analyse de la source des fonctions SASF comporte une fonctionnalité d'authentification du trafic de spammeur avant que celui-ci ne soit envoyé aux fonctions CASF ou RASF (*recipient-side anti-spam functions*). Les fonctions SASF peuvent éliminer le trafic pour lequel l'authentification a échoué, si c'est nécessaire, et il est possible d'envoyer uniquement le trafic authentifié aux autres fonctions ASF. Le rejet du trafic non autorisé peut être utile pour éviter que des spammeurs tentent d'effectuer une usurpation d'identité.

– Procédure de filtrage

La procédure selon laquelle les fonctions SASF filtrent le spam multimédia IP via l'analyse de la source est la suivante:

1) Distribution de la politique antispam: les fonctions SASF reçoivent la politique antispam des fonctions CASF. La politique antispam peut être distribuée aux fonctions SASF dans le cadre d'une notification ou d'une procédure de demande/réponse.

2) Réception d'une application multimédia IP: les fonctions SASF reçoivent une application multimédia IP.

3) Authentification de la source: les fonctions SASF authentifient la source de l'application. Si le processus d'authentification échoue, les fonctions SASF refusent la demande du spammeur.

4) Identification et filtrage du spam: les fonctions SASF prennent une décision concernant l'application multimédia IP reçue compte tenu de la politique antispam reçue des fonctions CASF et de la source de la demande. Les fonctions SASF peuvent refuser ou ignorer le trafic qui est déterminé comme étant du spam multimédia IP.

ii) Fonctions SAS d'analyse des caractéristiques

Les fonctions SASF peuvent identifier le spam en utilisant les caractéristiques des applications telles que la diffusion en masse. Elles peuvent utiliser un seuil pour déterminer les cas de diffusion en masse. Les fonctions SAS d'analyse des caractéristiques peuvent comporter plusieurs blocs fonctionnels spécifiques d'analyse des caractéristiques. La fonctionnalité et l'interface de chaque bloc fonctionnel, qui correspond à un moyen technique particulier de lutte contre le spam multimédia IP, n'entrent pas dans le domaine d'application de la présente Recommandation. On trouvera ci-après quelques exemples de caractéristiques qui peuvent être identifiées par les fonctions SASF dans le cadre de la méthode antispam.

– Diffusion en masse

Les fonctions SAS d'analyse des caractéristiques peuvent être en mesure d'analyser la quantité de demandes de service provenant d'une même source et d'analyser la fréquence de ces demandes. Le bloc fonctionnel SAS de filtrage identifie le spam multimédia IP, compte tenu du résultat de l'analyse réalisée par les fonctions SAS d'analyse des caractéristiques et de la politique antispam reçue du bloc fonctionnel CAS des critères de filtrage.

– Interactivité limitée

Les fonctions SASF peuvent être en mesure de vérifier l'interactivité du service avec le spammeur, même si la vérification d'interactivité avec la source des applications multimédias IP peut généralement être effectuée par les fonctions CASF. Les spammeurs ont tendance à utiliser des machines plutôt que des personnes pour lancer des applications multimédias IP et ce, pour des raisons de coût. Par conséquent, la vérification d'interactivité est une des méthodes qui permettent d'identifier le spam multimédia IP.

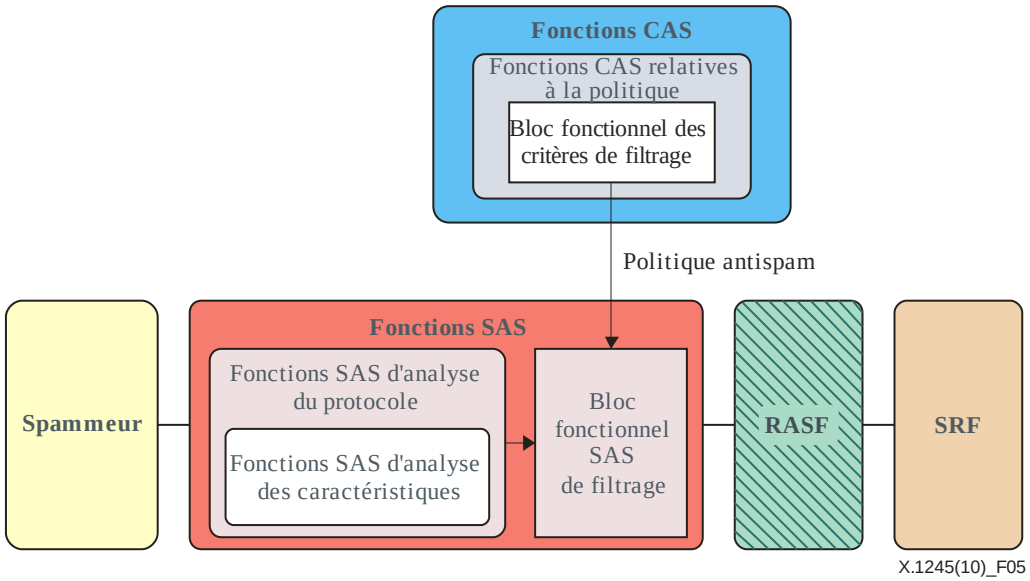


Figure 5 – Lutte contre le spam multimédia IP via l'analyse des caractéristiques dans les fonctions SASF

La procédure selon laquelle les fonctions SASF filtrent le spam multimédia IP sur la base de l'analyse des caractéristiques est la suivante:

1) Distribution de la politique antispam: le bloc fonctionnel SAS de filtrage reçoit des fonctions CASF la politique de lutte contre le spam basée sur une analyse des caractéristiques. La politique antispam peut être distribuée aux fonctions SASF dans le cadre d'une notification ou d'une procédure de demande/réponse.

2) Réception d'une application multimédia IP: les fonctions SASF reçoivent une application multimédia IP.

3) Analyse des caractéristiques: les fonctions SAS d'analyse des caractéristiques extraient les caractéristiques relatives au spam dans l'application multimédia IP reçue.

4) Traitement des résultats: les résultats de l'analyse des caractéristiques sont envoyés par les fonctions SAS d'analyse des caractéristiques au bloc fonctionnel SAS de filtrage.

5) Filtrage du spam: le bloc fonctionnel SAS de filtrage traite le spam conformément à la politique antispam. S'il ressort de l'analyse qu'il s'agit de spam, les fonctions SASF peuvent refuser ou ignorer le trafic qui est déterminé comme étant du spam multimédia IP.

La politique de gestion du spam multimédia IP dépend des fournisseurs de service, des utilisateurs de service, des applications multimédias IP, de la réglementation nationale, etc. C'est la raison pour laquelle les fonctions SASF et RASF doivent interagir avec les fonctions CASF pour obtenir des informations au sujet de la politique de lutte contre le spam basée sur les caractéristiques des applications multimédias IP.

7.3 Fonctions RAS

Les fonctions RASF constituent un groupe de fonctions dont le rôle est d'identifier et de bloquer le spam multimédia IP distribué à un destinataire de spams. Elles peuvent être mises en œuvre dans des éléments de réseau (serveur proxy par exemple) dans lesquels les demandes de communication entrantes destinées aux destinataires de spams sont envoyées (dernier bond). Les fonctions RASF interagissent avec les fonctions CASF pour l'exécution des fonctions antispam dans les fonctions RASF.

Les fonctions SASF et RASF peuvent être mises en œuvre dans le même équipement de réseau couvrant à la fois les spammeurs et les destinataires de spams. Toutefois, les fonctions antispam exécutées dans l'équipement sont différentes suivant le flux de trafic. En d'autres termes, ce sont les fonctions SASF qui sont appliquées lorsque le trafic provient d'utilisateurs d'applications multimédias IP couverts par l'équipement et ce sont les fonctions RASF qui sont appliquées lorsque le trafic est transmis à des utilisateurs d'applications multimédias IP couverts par l'équipement.

Les fonctions RASF sont constituées des fonctions RAS d'analyse du protocole et du bloc fonctionnel RAS de filtrage pour la commande du filtrage du spam.

Bien qu'il soit techniquement possible pour les fonctions SASF ou RASF d'analyser le contenu du trafic distribué en vue de la lutte contre le spam, ces fonctions ne comportent pas de fonctions d'analyse du contenu dans la présente Recommandation afin de ne pas leur imposer de contraintes supplémentaires en termes de traitement. Lorsqu'une application multimédia IP ne passe pas par les fonctions CASF par défaut, les fonctions RASF peuvent la distribuer aux fonctions CASF et leur demander d'en analyser le contenu en vue de déterminer s'il s'agit d'un spam.

Les paragraphes qui suivent décrivent diverses techniques que les fonctions RASF peuvent adopter pour lutter contre le spam multimédia IP.

7.3.1 Bloc fonctionnel RAS de filtrage

Le bloc fonctionnel RAS de filtrage détermine si l'application multimédia IP analysée est un spam ou non compte tenu du résultat de l'analyse et de la politique antispam. Il interagit donc avec les fonctions CASF et les autres fonctions ou blocs fonctionnels antispam des fonctions RASF.

7.3.2 Fonctions RAS d'analyse du protocole

Les fonctions RAS d'analyse du protocole analysent les informations de protocole relatives aux applications multimédias IP reçues. Elles sont constituées du bloc fonctionnel RAS d'analyse de la source et des fonctions RAS d'analyse des caractéristiques qui analysent respectivement les informations de source et les caractéristiques relatives aux applications multimédias IP reçues.

i) Bloc fonctionnel RAS d'analyse de la source

Les fonctions SASF peuvent distinguer le spam multimédia IP des applications multimédias IP qui ne sont pas des spams sur la base des informations relatives à la source des applications multimédias IP. Pour l'identification du spam, les fonctions RASF font appel à la politique de lutte contre le spam basée sur la source fournie par les fonctions CASF (liste noire, liste blanche, note de réputation, etc.). La Figure 6 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP via l'analyse de la source.

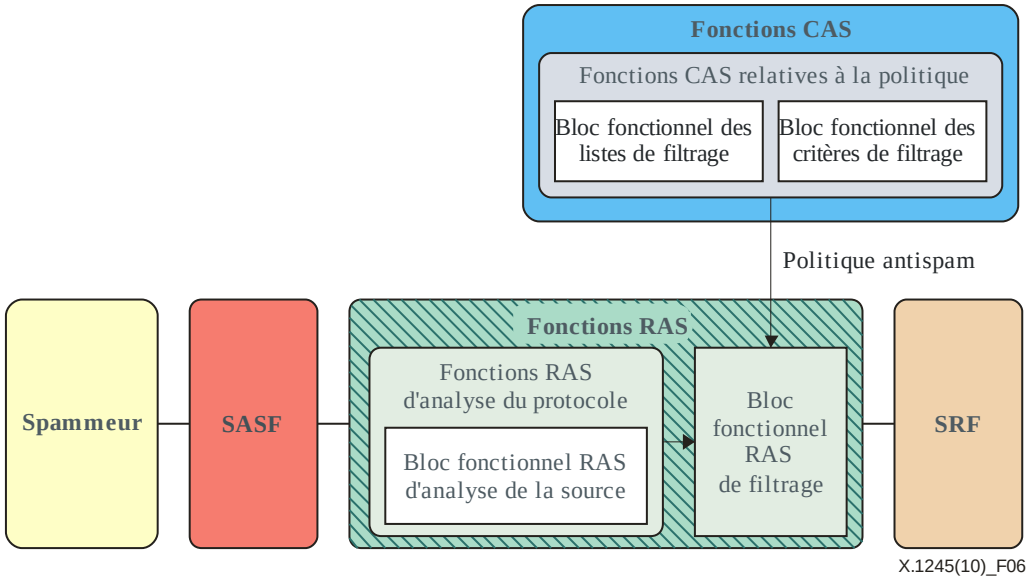


Figure 6 – Lutte contre le spam multimédia IP basée sur l'analyse de la source

Les fonctions RASF déterminent si une application multimédia IP est un spam ou non, compte tenu des informations relatives à la source de l'application multimédia IP, et la traitent en conséquence. Etant donné qu'une grande fiabilité des informations de source est nécessaire pour que la technique antispam basée sur la source soit efficace, on suppose que l'application multimédia IP que les fonctions RASF reçoivent des fonctions SASF est fiable, autrement dit qu'elle a été authentifiée. Pour identifier le spam multimédia IP, les fonctions RASF utilisent les critères de filtrage du spam ou les listes de filtrage du spam fournis par les fonctions CASF. Les fonctions CASF gèrent les listes de filtrage et les critères de filtrage destinés à faciliter l'identification du spam par elles-mêmes ou par les fonctions RASF ou SASF. La procédure selon laquelle les fonctions RASF identifient et filtrent le spam en utilisant la méthode d'analyse de la source est la suivante:

1) Distribution de la politique antispam par les fonctions CASF: les fonctions RASF reçoivent la politique antispam des fonctions CASF. La politique antispam peut être distribuée aux fonctions RASF dans le cadre d'une notification ou d'une procédure de demande/réponse.

2) Réception d'une application multimédia IP: les fonctions RASF reçoivent une application multimédia IP et vérifient sa source.

3) Identification et filtrage du spam: les fonctions RASF prennent une décision concernant l'application multimédia IP reçue compte tenu des informations relatives à la source et de la politique de gestion antispam reçue précédemment. Elles peuvent refuser ou ignorer le trafic qui est déterminé comme étant du spam multimédia IP conformément à la politique antispam du fournisseur de service ou à celle des utilisateurs du service.

Lorsque les fonctions RASF se basent sur une liste noire ou sur une liste blanche pour identifier le spam, elles peuvent utiliser la liste de filtrage provenant des fonctions CASF. Lorsque les fonctions RASF se basent sur une note de réputation pour identifier le spam, elles peuvent utiliser des critères de filtrage tels que la note de réputation seuil à partir de laquelle une application multimédia IP est déterminée comme étant d'un spam.

ii) Fonctions RAS d'analyse des caractéristiques

Les fonctions RASF peuvent identifier le spam en vérifiant si une application multimédia IP présente ou non les caractéristiques d'un spam multimédia IP. Les fonctions RAS d'analyse des caractéristiques peuvent comporter plusieurs blocs fonctionnels spécifiques d'analyse des caractéristiques. Les moyens techniques de lutte contre le spam multimédia IP n'entrent pas dans le domaine d'application de la présente Recommandation.

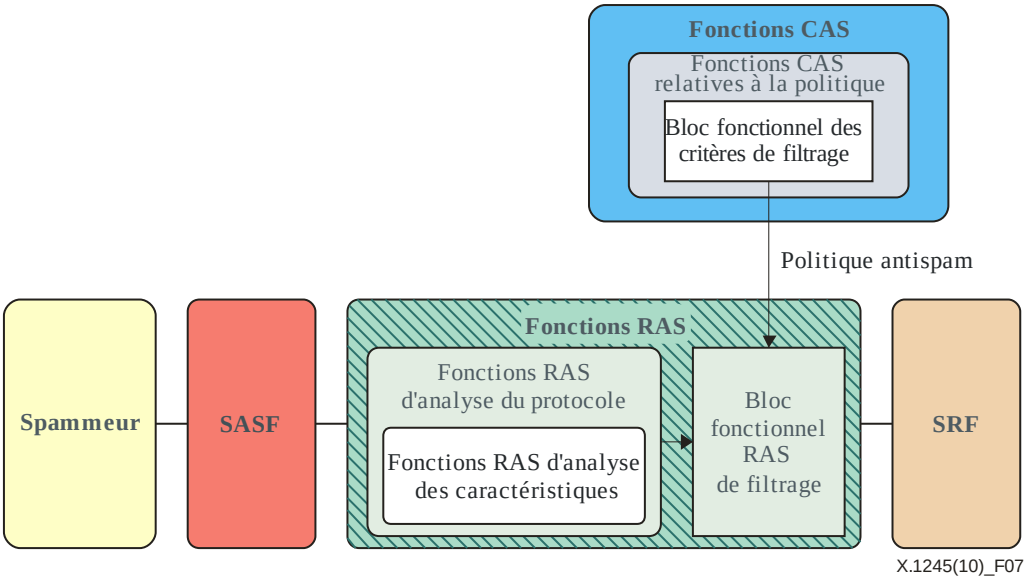


Figure 7 – Lutte contre le spam multimédia IP basée sur l'analyse des caractéristiques

La Figure 7 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP via une analyse des caractéristiques dans les fonctions RASF. La procédure selon laquelle les fonctions RASF identifient le spam multimédia IP sur la base de l'analyse des caractéristiques est la suivante:

1) Distribution de la politique antispam: le bloc fonctionnel RAS de filtrage reçoit des fonctions CASF la politique de lutte contre le spam basée sur l'analyse des caractéristiques. La politique antispam peut être distribuée aux fonctions RASF dans le cadre d'une notification ou d'une procédure de demande/réponse.

2) Réception d'une application multimédia IP: les fonctions RASF reçoivent une application multimédia IP.

3) Analyse des caractéristiques: les fonctions RAS d'analyse des caractéristiques extraient les caractéristiques relatives au spam de l'application multimédia IP reçue.

4) Traitement du résultat: les fonctions RAS d'analyse des caractéristiques fournissent le résultat de l'analyse au bloc fonctionnel RAS de filtrage.

5) Filtrage du spam: le bloc fonctionnel RAS de filtrage traite le spam conformément à la politique antispam. S'il ressort de l'analyse qu'il s'agit de spam, les fonctions RASF peuvent refuser ou ignorer le trafic qui est déterminé comme étant du spam multimédia IP.

7.4 Fonctions CAS

Les fonctions CASF sont en mesure de gérer les politiques antispam et de commander les fonctions RASF et SASF. Elles sont aussi en mesure d'analyser la source ou les caractéristiques des applications multimédias IP afin d'identifier et de filtrer le spam lorsqu'elles se trouvent sur le trajet de paquets IP entre les spammeurs et les destinataires de spams pour la fourniture des applications multimédias IP, en fonction du type d'application. Les fonctions CASF comportent les fonctions CAS d'analyse du protocole, les fonctions CAS d'analyse du contenu, le bloc fonctionnel CAS de filtrage, les fonctions CAS relatives à la politique antispam et le bloc fonctionnel ASF de commande. Le présent paragraphe décrit les fonctionnalités et les interactions de chaque entité des fonctions CASF pour la lutte contre le spam multimédia IP.

7.4.1 Bloc fonctionnel CAS de filtrage

Le bloc fonctionnel CAS de filtrage détermine si l'application multimédia IP analysée est un spam ou non compte tenu du résultat de l'analyse et de la politique antispam. Il interagit donc avec les autres fonctions ou blocs fonctionnels antispam des fonctions CASF.

7.4.2 Fonctions CAS d'analyse du protocole

Les fonctions CAS d'analyse du protocole analysent les informations de protocole relatives aux applications multimédias IP reçues. Elles sont constituées du bloc fonctionnel CAS d'analyse de la source et des fonctions CAS d'analyse des caractéristiques qui analysent respectivement les informations de source et les caractéristiques relatives aux applications multimédias IP reçues.

i) Bloc fonctionnel CAS d'analyse de la source

Lorsqu'une application multimédia IP est fournie sous le contrôle d'un composant de réseau comportant des fonctions CASF (par exemple lorsqu'un utilisateur se connecte à un service de messagerie instantanée ou à un service de téléphonie IP sous le contrôle de serveurs d'application), l'analyse de la source en vue de l'identification de spam peut se faire dans les fonctions CASF. La Figure 8 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP basée sur l'analyse de la source dans les fonctions CASF.

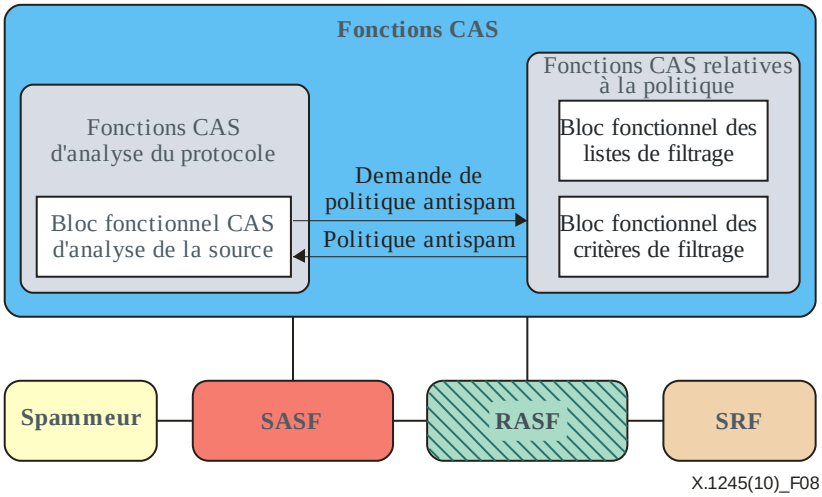


Figure 8 – Lutte contre le spam multimédia IP basée sur l'analyse de la source

Une procédure possible de lutte contre le spam multimédia IP basée sur les informations de source d'une application multimédia IP au niveau des fonctions CASF est la suivante:

1) Authentification: un utilisateur qui souhaite utiliser une application multimédia IP (par exemple un service de messagerie instantanée) est authentifié par un composant de réseau (par exemple un serveur d'application) disposant des fonctions CASF.
2) Réception d'une application multimédia IP: l'utilisateur envoie une demande de distribution de message IP aux fonctions CASF et le bloc fonctionnel CAS d'analyse de la source vérifie la source de l'utilisateur.
3) Obtention de la politique antispam: le bloc fonctionnel CAS d'analyse de la source demande la politique antispam et la reçoit des fonctions CAS relatives à la politique.
4) Identification et filtrage du spam: les fonctions CASF prennent une décision concernant l'application multimédia IP reçue compte tenu des informations de source et de la politique antispam reçue précédemment. Les fonctions CASF peuvent refuser ou ignorer le trafic déterminé comme étant du spam multimédia IP, qui est alors traité conformément à la politique antispam du fournisseur de services ou de l'utilisateur de service.

ii) Fonctions CAS d'analyse des caractéristiques

Lorsqu'une application multimédia IP est fournie sous le contrôle d'une entité de réseau comportant des fonctions CASF, l'analyse des caractéristiques pour la lutte contre le spam peut se faire dans les fonctions CASF. Les fonctions CASF analysent une application multimédia IP pour déterminer si elle présente les caractéristiques du spam et utilisent les critères de filtrage de la politique antispam pour déterminer s'il s'agit ou non d'un spam. La Figure 9 représente l'architecture globale et les interfaces pour la lutte contre le spam multimédia IP via l'analyse des caractéristiques dans les fonctions CASF.

Les fonctions CASF relatives à la politique comportent un bloc fonctionnel des critères de filtrage qui contient les critères de filtrage du spam nécessaires pour identifier le spam multimédia IP et qui fournit les critères aux fonctions SASF ou RASF pour les aider à identifier le spam. Par exemple, lorsque les fonctions CAS d'analyse des caractéristiques essaient de déterminer si une application multimédia IP diffusée en masse est un spam, le bloc fonctionnel CASF des critères de filtrage peut fournir les critères de quantité permettant de déterminer s'il s'agit d'un spam multimédia IP.

La Figure 9 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP via l'analyse des caractéristiques dans les fonctions CASF.

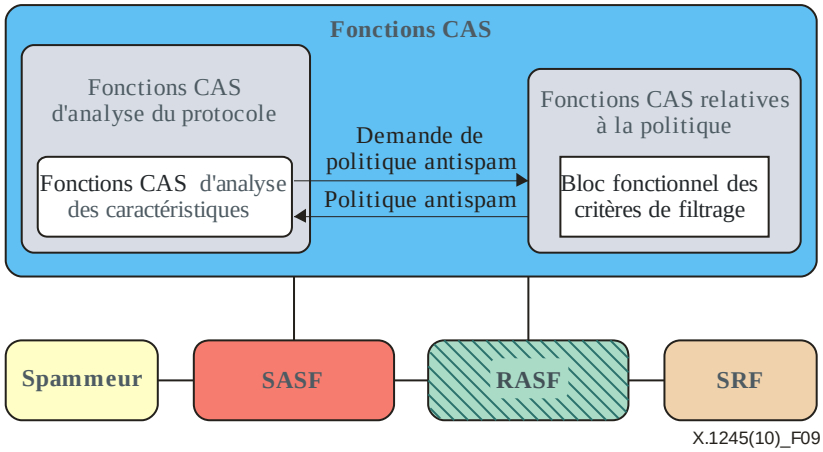


Figure 9 – Lutte contre le spam multimédia IP basée sur l'analyse des caractéristiques

La procédure de lutte contre le spam multimédia IP basée sur l'analyse des caractéristiques au niveau des fonctions CASF est la suivante:

1) Analyse des caractéristiques: en cas de tentative de connexion à une application multimédia IP sous le contrôle d'une entité de réseau comportant des fonctions CASF, ces fonctions procèdent à une analyse pour déterminer si l'application présente les caractéristiques du spam (par exemple diffusion en masse, interactivité limitée, etc.).
2) Obtention de la politique antispam: les fonctions d'analyse des caractéristiques demandent aux fonctions CAS relatives à la politique de leur fournir la politique de lutte contre le spam basée sur une analyse des caractéristiques pour le filtrage du spam. Le bloc relatif à la politique antispam envoie les informations demandées aux fonctions CAS d'analyse des caractéristiques.
3) Identification et filtrage du spam: les fonctions CAS d'analyse des caractéristiques déterminent si l'application multimédia IP est un spam ou non, compte tenu du résultat de l'analyse et de la politique antispam reçue.

7.4.3 Fonctions CAS d'analyse du contenu

Les fonctions CASF comportent les fonctions CAS d'analyse du contenu. Ces fonctions analysent le contenu d'une application multimédia IP afin de déterminer s'il s'agit d'un spam lorsque cette

application est distribuée au destinataire via un équipement de réseau comportant des fonctions CASF (par exemple serveur d'application ou serveur de média).

En ce qui concerne l'identification de spam basée sur les informations de protocole des applications multimédias IP (par exemple les informations de source ou les caractéristiques du spam), l'analyse peut se faire aussi bien dans les fonctions CASF que dans les fonctions SASF ou dans les fonctions RASF. Par contre, en ce qui concerne l'identification de spam basée sur l'analyse du contenu, il est logique que l'analyse du contenu se fasse dans les fonctions CASF, par lesquelles le contenu des applications multimédias IP transite lorsqu'on utilise des techniques antispam basées sur le contenu pour la lutte contre le spam multimédia IP.

La Figure 10 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP basée sur l'analyse du contenu dans les fonctions CASF.

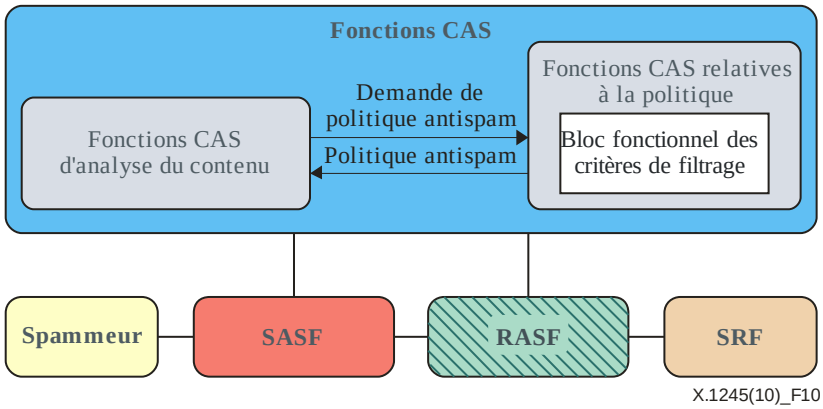


Figure 10 – Lutte contre le spam multimédia IP basée sur l'analyse du contenu

La procédure de lutte contre le spam multimédia IP basée sur l'analyse du contenu dans les fonctions CASF est la suivante:

1) Réception d'une application multimédia IP: le contenu d'une application multimédia IP arrive au niveau des fonctions CASF.

2) Analyse du contenu: les fonctions CAS d'analyse du contenu analysent le contenu de l'application multimédia IP.

3) Obtention de la politique antispam: les fonctions CASF demandent aux fonctions CAS relatives à la politique de leur fournir la politique antispam et reçoivent cette politique du bloc fonctionnel des critères de filtrage.

4) Identification et filtrage du spam: les fonctions CASF déterminent si l'application multimédia IP est un spam ou non, compte tenu du résultat de l'analyse et de la politique antispam.

Comme décrit au paragraphe 6, l'applicabilité de la méthode d'analyse du contenu peut être limitée en fonction des caractéristiques de l'application multimédia IP, par exemple si l'application est en temps réel ou non, si elle est multimédia ou non, ou si son contenu est chiffré ou non.

7.4.4 Fonctions CAS relatives à la politique

Les fonctions CAS relatives à la politique gèrent les politiques de lutte contre le spam multimédia IP et sont constituées du bloc fonctionnel des critères de filtrage et du bloc fonctionnel des listes de filtrage.

i) Bloc fonctionnel des critères de filtrage

Le bloc fonctionnel des critères de filtrage gère les critères de filtrage pour l'identification du spam multimédia IP. Divers types de critères de filtrage sont possibles en fonction des techniques antispam mises en œuvre. Par exemple, dans l'analyse de la diffusion en masse, un critère de filtrage peut être la quantité seuil d'applications multimédias IP qui sont envoyées simultanément depuis une même source. Les mécanismes de création et de gestion des critères de filtrage n'entrent pas dans le domaine d'application de la présente Recommandation.

ii) Bloc fonctionnel des listes de filtrage

Le bloc fonctionnel des listes de filtrage gère les listes de filtrage pour l'identification du spam multimédia IP basée sur l'analyse de la source. Divers types de listes de filtrage sont possibles, en fonction des techniques antispam mises en œuvre. Par exemple, on peut utiliser comme liste de filtrage une liste noire, une liste blanche ou une note de réputation. La liste de filtrage peut être une liste publique pour de nombreux utilisateurs d'un même service, une liste personnelle qui est gérée personnellement ou une combinaison des deux. Les mécanismes de création et de gestion des listes de filtrage n'entrent pas dans le domaine d'application de la présente Recommandation.

7.4.5 Bloc fonctionnel ASF de commande

Le bloc fonctionnel ASF de commande interagit avec les fonctions SASF et RASF pour les aider à identifier et filtrer le spam. Il distribue aux fonctions RASF et SASF les politiques antispam provenant des fonctions CAS relatives à la politique.

7.5 Fonctions SR

Le destinataire de spams est la cible de spams multimédias IP. En l'absence de mécanisme de lutte contre le spam, le spam multimédia IP peut affecter les utilisateurs et leur causer des préjudices.

Le destinataire de spams dispose de fonctions SR (*spam recipient*) destinées à le protéger du spam multimédia IP. Les utilisateurs peuvent établir la politique antispam ou la recevoir des fournisseurs de services pour filtrer le spam multimédia IP. Les fonctions SR sont constituées des fonctions SR d'analyse du protocole, des fonctions SR d'analyse du contenu, du bloc fonctionnel SR de filtrage et des fonctions relatives à la politique antispam locale. Le présent paragraphe décrit les fonctionnalités et interactions de chaque fonction antispam que le destinataire de spams peut adopter pour la lutte contre le spam.

7.5.1 Fonctions SR d'analyse du protocole

Les fonctions SR d'analyse du protocole comportent un bloc fonctionnel SR d'analyse de la source qui permet d'identifier le spam compte tenu des informations relatives à l'expéditeur. Même s'il est possible de filtrer le spam au niveau des fonctions CASF, SASF et RASF, dans le cas d'applications multimédias IP connectées directement, on peut utiliser les fonctions antispam et la politique antispam des fonctions SRF pour la lutte contre le spam multimédia IP.

Le destinataire de spams peut définir une liste de filtrage locale et des critères de filtrage locaux ou il peut recevoir la liste d'autres fonctions antispam comme les fonctions CASF. Les mécanismes spécifiques à utiliser pour définir la politique antispam n'entrent pas dans le domaine d'application de la présente Recommandation. La Figure 11 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP basée sur l'analyse de la source dans les fonctions SRF.

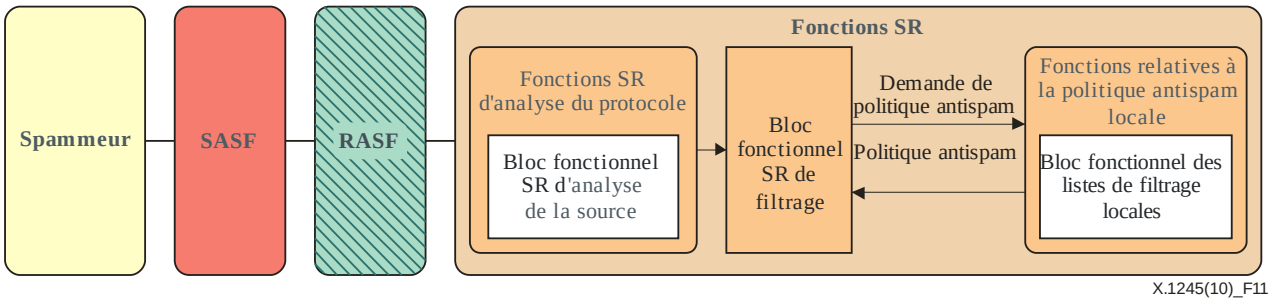


Figure 11 – Lutte contre le spam multimédia IP via l'analyse de la source au niveau du destinataire de spams

Une procédure possible de lutte contre le spam multimédia IP basée sur les informations de source d'une application multimédia IP au niveau du destinataire de spams est la suivante:

1) Réception d'une application multimédia IP: les fonctions SRF reçoivent une application multimédia IP et en vérifient la source.

2) Obtention de la politique antispam: les fonctions SR d'analyse du protocole demandent la politique antispam et la reçoivent des fonctions relatives à la politique antispam locale.

3) Identification et filtrage du spam: le bloc fonctionnel SR de filtrage prend une décision concernant l'application multimédia IP reçue compte tenu de la politique antispam et du résultat de l'analyse de la source. Le destinataire de spams peut refuser ou ignorer le trafic qui est déterminé comme étant du spam multimédia IP.

Les fonctions SR pourraient techniquement identifier le spam via l'analyse des caractéristiques. Toutefois, les fonctions SR d'analyse du protocole ne comportent pas de bloc fonctionnel d'analyse des caractéristiques. En effet, il est risqué de charger le destinataire de spams d'exécuter des fonctions sophistiquées de lutte contre le spam, comme c'est le cas avec la méthode d'analyse des caractéristiques, car les fonctions SR d'analyse du protocole sont sous le contrôle d'un groupe d'utilisateurs très variable.

7.5.2 Fonctions SR d'analyse du contenu

Le destinataire de spams peut lutter contre le spam via l'analyse du contenu. Il peut gérer un mécanisme d'analyse du contenu propre à l'utilisateur ou recevoir le mécanisme des fournisseurs de services. La politique de lutte contre le spam basée sur l'analyse du contenu est placée dans les fonctions relatives à la politique antispam locale et plus précisément dans le bloc fonctionnel des critères de filtrage locaux. La Figure 12 représente les fonctions antispam et les interactions entre les fonctions pour la lutte contre le spam multimédia IP basée sur l'analyse du contenu dans les fonctions SRF.

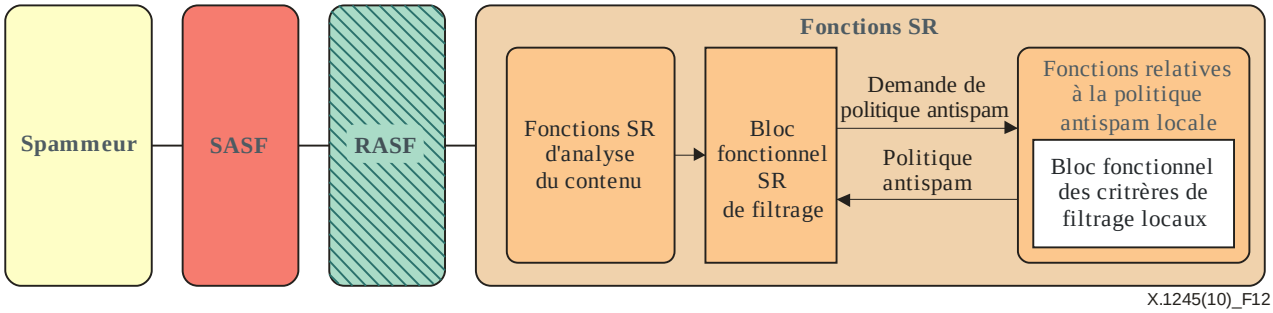


Figure 12 – Lutte contre le spam multimédia IP via l'analyse du contenu au niveau du destinataire de spams

La procédure selon laquelle le destinataire de spams filtre le spam multimédia IP via l'analyse du contenu est la suivante:

1) Réception d'une application multimédia IP: les fonctions SRF reçoivent une application multimédia IP. Les fonctions SR d'analyse du contenu analysent son contenu pour déterminer s'il s'agit d'un spam.

2) Obtention de la politique antispam: le résultat de l'analyse du contenu est envoyé au bloc fonctionnel SR de filtrage, qui demande et reçoit la politique antispam des fonctions relatives à la politique antispam locale.

3) Identification et filtrage du spam: le bloc fonctionnel SR de filtrage prend une décision concernant l'application IP reçue, compte tenu de la politique antispam et du résultat de l'analyse du contenu. Le destinataire de spams peut refuser ou ignorer le trafic qui est déterminé comme étant du spam multimédia IP.

7.5.3 Bloc fonctionnel SR de filtrage

Le bloc fonctionnel SR de filtrage détermine si l'application multimédia IP analysée est du spam ou non compte tenu du résultat de l'analyse et de la politique antispam. Il interagit donc avec d'autres fonctions ou blocs fonctionnels antispam des fonctions SRF.

7.5.4 Fonctions relatives à la politique antispam locale

Les fonctions relatives à la politique antispam locale gèrent des politiques de lutte contre le spam multimédia IP propres à l'utilisateur. Elles sont constituées du bloc fonctionnel des critères de filtrage locaux et du bloc fonctionnel des listes de filtrage locales.

i) Bloc fonctionnel des critères de filtrage locaux

Le bloc fonctionnel des critères de filtrage locaux gère les critères de filtrage propres à l'utilisateur pour l'identification du spam multimédia IP. Les types de critères de filtrage dépendent des fonctions antispam prises en charge par les fonctions SRF.

ii) Bloc fonctionnel des listes de filtrage locales

Le bloc fonctionnel des listes de filtrage locales gère la liste de filtrage propre à l'utilisateur pour l'identification du spam multimédia IP basée sur l'analyse de la source. Les types de listes dépendent des fonctionnalités d'analyse de la source prises en charge par les fonctions SRF.

7.6 Points de référence du cadre

Le présent paragraphe définit les points de référence entre les divers éléments du cadre. Ces points sont indiqués sur la Figure 13.

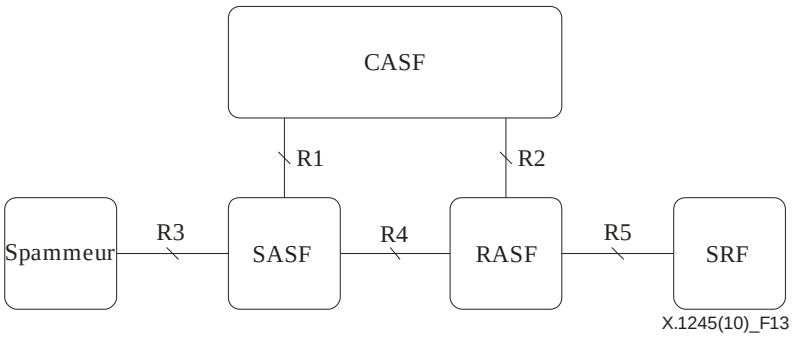


Figure 13 – Points de référence du cadre de lutte contre le spam

7.6.1 Point de référence R1

R1 est situé entre les fonctions CASF et SASF. C'est par ce point que les fonctions SASF obtiennent la politique de filtrage auprès des fonctions CASF et que les fonctions CASF commandent les fonctions SASF.

7.6.2 Point de référence R2

R2 est situé entre les fonctions CASF et RASF. C'est par ce point que les fonctions RASF obtiennent la politique de filtrage auprès des fonctions CASF et que les fonctions CASF commandent les fonctions RASF.

7.6.3 Point de référence R3

R3 est situé entre les spammeurs et les fonctions SASF. Il est utilisé dans le cadre du protocole des applications multimédias IP et/ou pour la transmission du trafic de données.

7.6.4 Point de référence R4

R4 est situé entre les fonctions SASF et RASF. Il est utilisé dans le cadre du protocole des applications multimédias IP et/ou pour la transmission du trafic de données.

7.6.5 Point de référence R5

R5 est situé entre les fonctions RASF et les destinataires de spams. Il est utilisé dans le cadre du protocole des applications multimédias IP et/ou pour la transmission du trafic de données.

Appendice I

Lutte contre le spam par l'imposition de contraintes aux spammeurs

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

L'imposition de contraintes aux spammeurs peut constituer l'une des méthodes techniques de lutte contre le spam multimédia IP. Cependant, cette méthode diffère quelque peu des autres qui identifient et filtrent directement le spam. Elle aide indirectement à réduire la quantité de spams, mais elle demande de l'énergie et du temps et s'avère coûteuse. L'une des manières de diminuer la quantité de spams multimédias IP consisterait à imposer davantage de contraintes aux spammeurs en augmentant les coûts et les efforts nécessaires pour créer et distribuer des spams. Ces coûts comprennent une redevance, qui inclut une provision pour amende en cas de spam illégal, les coûts d'utilisation d'applications multimédias IP payés au fournisseur de services ou au fournisseur de réseau, les frais de distribution des spams (vérification d'interactivité par exemple), etc. On peut utiliser les méthodes suivantes pour augmenter les contraintes pour les spammeurs:

– Entraver l'accès aux adresses IP: compliquer la collecte des informations au sujet des cibles des spams multimédias IP (par exemple adresses IP et comptes de service d'application multimédia IP) et rendre plus difficile l'envoi de ces spams par les spammeurs.
– Système de paiement: la taxation des spams multimédias IP peut être utile pour réduire la quantité de spams. L'adoption d'un système de paiement pour les spams potentiels (par exemple messages IP en masse) n'est toutefois pas une question technique.
– Prévention de la diffusion en masse: étant donné que les spams sont souvent envoyés en masse, la prévention de la diffusion en masse peut contribuer à diminuer la quantité de spams.
– Vérification d'interactivité: la vérification d'interactivité avec les spammeurs peut permettre d'augmenter le coût d'envoi des spams. Cependant, elle peut avoir comme effet secondaire de créer aussi des contraintes pour les utilisateurs normaux des applications multimédias IP.

Les méthodes de lutte contre le spam par l'imposition de contraintes aux spammeurs ne sont pas limitées aux exemples ci-dessus.

Concernant la vérification d'interactivité, les fonctions CASF peuvent jouer le rôle du vérificateur. Dans la méthode de prévention de la diffusion en masse, les fonctions CASF, SASF ou RASF peuvent déterminer une certaine quantité associée à la diffusion en masse et bloquer les applications multimédias IP diffusées en masse. La taxation des communications ou messages diffusés en masse sous le contrôle des fonctions CASF est également une méthode possible pour augmenter les contraintes pour les spammeurs.

Les fonctions SASF ou RASF peuvent parfois analyser les informations de protocole, mais elles ne prennent généralement pas de mesures supplémentaires pour accroître les contraintes pour les spammeurs (prévention de la diffusion en masse, paiement, vérification d'interactivité, etc.). Pour résumer, les fonctions SASF ou RASF devraient prendre certaines mesures pour aider les fonctions CASF à traiter le spam et ce sont essentiellement les fonctions CASF qui devraient imposer davantage de contraintes aux spammeurs.

Appendice II

Considérations liées à la sécurité et considérations pratiques concernant l'utilisation du cadre

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

II.1 Considérations liées à la sécurité

Quelques considérations relatives à la sécurité pour la lutte contre le spam multimédia IP sont énoncées ci-après.

– Authentification

L'authentification est un processus dans lequel une entité, soit le destinataire de spams, soit les fonctions CASF, confirme son identité en présentant des justificatifs qui sont difficiles à produire pour quiconque n'est pas le véritable utilisateur.

Il est nécessaire de procéder à une authentification d'utilisateur pour identifier l'expéditeur de messages d'applications multimédias IP afin de faciliter le blocage de nombreux spams dus à des attaques par usurpation d'identité. Si l'authentification de l'utilisateur n'est pas réalisée correctement, il sera impossible de pister les spammeurs car ils pourront falsifier leur adresse IP avec une attaque par usurpation d'identité.

Il existe de nombreuses méthodes d'authentification. Certaines, comme l'authentification par mot de passe en clair, sont faciles à mettre en œuvre mais donnent généralement lieu à une authentification faible et peu fiable. D'autres, comme les méthodes reposant sur les protocoles Secure Socket Layer (SSL), IPSec, secure shell ou Kerberos, qui peuvent être plus complexes à mettre en œuvre et à gérer, donnent lieu à une authentification forte et fiable.

D'autres technologies émergentes, comme les méthodes de signature cryptographique, peuvent constituer des solutions encore meilleures. Cependant, la méthode d'authentification de l'expéditeur la plus largement adoptée parmi les méthodes actuellement disponibles continue à être la méthode classique Sender Policy Framework (SPF) et DomainKeys.

– Contrôle d'accès

Le contrôle d'accès est un moyen de mettre en œuvre et d'appliquer des politiques d'autorisation. Il permet ou interdit à l'utilisateur de réaliser une action au niveau du destinataire de spams et des fonctions ASF, conformément à une politique de sécurité.

Les contrôles d'accès sont généralement appliqués après l'authentification. On distingue généralement le contrôle d'accès discrétionnaire (DAC) et le contrôle d'accès non discrétionnaire (NDAC). Pour le contrôle d'accès DAC, le propriétaire de l'objet spécifie qui a accès à l'objet ou spécifie des politiques. Toutes les politiques de contrôle d'accès ne relevant pas de la catégorie DAC sont classées dans la catégorie NDAC. Pour le contrôle d'accès NDAC, les politiques sont des règles qui ne sont pas spécifiées à la discrétion de l'utilisateur (par exemple contrôle d'accès obligatoire (MAC), contrôle d'accès basé sur le rôle (RBAC), contrôle d'accès basé sur l'objet (PBAC), contrôle d'accès basé sur l'historique (HBAC), contrôle d'accès basé sur des contraintes temporelles (TCAC) et contrôle d'accès basé sur une règle (RuBAC)).

– Confidentialité

Assurer la confidentialité consiste à faire en sorte que seuls les utilisateurs autorisés puissent accéder aux communications sécurisées. Il existe deux mécanismes principaux permettant d'assurer la confidentialité d'informations transmises par voie électronique: le chiffrement et la transmission sur une infrastructure sécurisée – par exemple via un réseau privé virtuel (VPN) ou une autre liaison chiffrée.

Le protocole IPSec est le protocole utilisé dans la plupart des VPN pour établir une connexion sécurisée sur l'Internet. IPSec est une norme largement acceptée de transmission sécurisée et constitue une solution souple et moins onéreuse que d'autres méthodes de chiffrement. IPSec permet d'assurer un chiffrement, une intégrité et une authentification excellents et est particulièrement utile pour les organisations qui ont besoin de transférer des données en toute sécurité sur l'Internet.

Le protocole de tunnellisation de couche 2 (L2TP) est un protocole de tunnellisation utilisé pour prendre en charge les VPN. Il encapsule un protocole de couche réseau donné à l'intérieur du protocole point à point (PPP) pour protéger cryptographiquement les trames PPP et pour encapsuler les données à l'intérieur d'un protocole de tunnellisation.

– Intégrité des données

L'intégrité signifie que les informations ne changent pas au cours de leur transmission entre l'expéditeur et le destinataire. Sans une protection correcte, des spammeurs pourraient altérer ou embrouiller le contenu de messages multimédias IP.

En utilisant les condensés de message produits par une fonction de hachage cryptographique, un administrateur de système peut détecter les modifications non autorisées des messages. Les fonctions de hachage peuvent aussi être combinées avec d'autres méthodes cryptographiques normalisées pour vérifier la source des données. La combinaison d'algorithmes de hachage avec le chiffrement permet de produire des condensés de message spéciaux grâce auxquels il est possible d'identifier la source des données.

Lorsque des signatures numériques sont utilisées pour assurer l'intégrité des données, une infrastructure de clé publique (PKI) peut être nécessaire pour gérer les clés de chiffrement. L'architecture PKI mémorise l'attribution et la révocation de clés de chiffrement publiques pour les utilisateurs et les organisations.

Au lieu d'utiliser des signatures numériques et une architecture PKI, on peut utiliser la cryptographie secrète pour assurer l'intégrité des données. L'application d'une clé secrète est plus simple en ce sens qu'on n'utilise qu'une seule clé, qui doit être en possession à la fois de l'expéditeur et du destinataire pour pouvoir procéder au chiffrement et au déchiffrement. Les systèmes à clé secrète sont largement utilisés mais il existe des difficultés liées à la distribution sécurisée des clés secrètes.

– Non-répudiation

La non-répudiation est le fait de garantir que l'expéditeur d'un message ou la personne à l'origine d'une transaction ne pourra nier ultérieurement que la transaction a eu lieu.

La non-répudiation est obtenue grâce à des documents juridiques et aux mécanismes de sécurité et processus de confiance suivants pour la gestion de serveur: SSL, jeton OTP défi-réponse, hachage sécurisé et journaux d'audit.

Une pratique courante pour la mise en œuvre de la non-répudiation consiste à tirer parti des signatures numériques, qui peuvent être considérées comme l'une des meilleures solutions pour remplacer les signatures traditionnelles dans le traitement des données électroniques. Pour activer les signatures numériques, un tiers de confiance (TTP) ou une infrastructure PKI doit être disponible, avec au moins une autorité de certification (CA) pour pouvoir délivrer les certificats numériques et des listes de révocation de certificats (CRL) pour pouvoir vérifier si un certificat fait partie des certificats révoqués.

II.2 Considérations pratiques

L'un des principaux objectifs du cadre est de faire en sorte que les conséquences négatives pour les entreprises soient réduites au minimum. Il faut bien avoir à l'esprit que le respect des mesures antispam donne des résultats positifs pour les particuliers et pour les entreprises.

Les considérations pratiques qui suivent sont basées sur les opérations de traitement. Elles sont destinées à servir de guide pour la mise en œuvre d'un système antispam et à donner des informations de haut niveau aux fournisseurs potentiels.

– Assurer une grande précision et une bonne qualité de fonctionnement.
– Faire en sorte que le système puisse être déployé au niveau du périmètre d'Internet.
– Intégrer le système avec les systèmes courants d'application multimédia IP.
– Permettre une exécution sur diverses plates-formes de serveur du client: UNIX, Windows, etc.
– Filtrer à la fois le spam multimédia IP entrant et le spam multimédia IP sortant.
– Assurer une souplesse permettant de s'adapter aux politiques et préférences des organisations.
– Permettre à l'utilisateur d'établir des filtres individuels ou spécifiques.
– Permettre aux utilisateurs finals de gérer leurs propres dossiers de spam d'application multimédia IP et de définir des préférences simples.
– Permettre la gestion de listes blanches et de listes noires.
– Permettre de filtrer le contenu et permettre d'ajouter un filtrage du contenu côté serveur, avec des niveaux d'administration jusqu'à l'utilisateur.

Bibliographie

[b-UIT-T X.1240] Recommandation UIT-T X.1240 (2008), *Technologies intervenant dans la lutte contre le spam par courrier électronique*.

[b-UIT-T X.1244] Recommandation UIT-T X.1244 (2008), *Aspects généraux de la lutte contre le spam dans les applications multimédias IP*.

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

Imprimé en Suisse
Genève, 2011