Sécurisation des flux Internet et de messagerie au Centre Hospitalier de Montbert

Éric Boisdon

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL DES PAYS DE LOIRE DE NANTES

MEMOIRE

présenté en vue d'obtenir

le DIPLOME d'INGENIEUR CNAM en INFORMATIQUE

OPTION : SYSTEME D'INFORMATION

Par Eric BOISDON

Sécurisation des flux Internet et de messagerie au Centre Hospitalier de Montbert.

Soutenu le 16 décembre 2011

JURY

Présidente :	Mme METAIS, professeur CNAM Paris
Membres :	M. BRIAND, professeur émérite, Ecole Polytechnique de Nantes
	M. GERARDIN, tuteur CNAM
	M. PRAUD, tuteur entreprise, directeur du Centre Hospitalier de Montbert
	M. TESSON, Référent Sécurité Système d'Information à L'Agence Régionale de Santé des Pays de la Loire

Remerciements

Je tiens à remercier le Centre Hospitalier de Montbert et plus particulièrement son directeur, Monsieur Yves Praud, de m'avoir donné l'opportunité de réaliser mon mémoire au sein de l'établissement.

Je remercie Madame Françoise Mainguet pour ses conseils sur les aspects financiers de ce projet, appliqués à la fonction publique hospitalière.

Je remercie Monsieur Gerardin, mon tuteur CNAM, de m'avoir suivi tout au long de ce projet, pour ses conseils.

Je remercie Monsieur Tesson, d'avoir accepté de m'accompagner sur ce projet.

Je remercie les éditeurs des solutions évaluées Trend Micro, Websense, Olfeo, Vade Retro de m'avoir fourni des clés d'évaluation afin de réaliser ces comparatifs. Je remercie plus particulièrement M. Tetga (Trend Micro) M. Bonnet et M. Lermusiaux (Olfeo), M. Griffon et M. Gendre (Vade Retro)

Je remercie les intégrateurs : M. Condou-Labardisse de la société CAPACITI, M. Maurel de la société NOVALINK, pour leur travail sur les cotations financières des solutions évaluées.

Je remercie M. Carre, ingénieur en informatique au Conseil Général du Maine et Loire (49) pour son retour d'expérience sur la solution Websense, en appliance matérielle et la présentation de la console « Triton ».

Je remercie le Centre Hospitalier de Saint-Nazaire et particulièrement Mme Philipot pour m'avoir accueilli et présenté le résultat de l'intégration des produits Olfeo et Mail In Black.

Je remercie les professeurs du CNAM du centre régional de Nantes qui m'ont permis de suivre, de comprendre et de valider l'ensemble des unités d'enseignements pour atteindre cet objectif.

Enfin, je remercie ma famille pour leur soutien pendant toutes ces années.

Table des matières

1 Introduction

1.1 Présentation du mémoire

Ce mémoire a été réalisé au sein du Centre Hospitalier de Montbert, en Loire-Atlantique afin d'obtenir le diplôme d'ingénieur en ingénierie des systèmes d'information du CNAM. Le sujet porte sur l'étude des solutions de sécurisations des flux de navigation Internet et de messagerie électronique.

Ce mémoire a pour but de faire un état des lieux des solutions actuellement déployées sur le site, mais surtout d'apporter des propositions d'amélioration de la sécurité par la mise en œuvre de nouvelles solutions, plus performantes, prenant en compte les problématiques rencontrées au quotidien et la réglementation en vigueur. Dans cet objectif, plusieurs solutions du marché ont été évaluées. Ce mémoire doit également servir de base à la rédaction d'une future consultation pour l'acquisition d'une nouvelle solution de sécurisation des flux web et mails.

Le document se découpe en quatre parties :

- La législation en vigueur et les textes de références,
- L'état de l'art des techniques de filtrage des flux Internet et de messagerie,
- L'évaluation de solutions de filtrages Internet et de messagerie,
- Une analyse financière des solutions évaluées.

1.2 Problématique de la sécurisation des flux

L'accès aux réseaux de communication, surtout Internet, est indispensable aux pratiques développées par les unités de soins avec les patients.

Le CH de Montbert est confronté au quotidien à ces problématiques d'évolution des usages, de protection des données médicales, administratives et des besoins professionnels des agents à accéder à des informations très variées. Le déploiement de la solution de sécurisation des accès distants par une passerelle VPN/SSL a permis de sécuriser les connexions des prestataires de services, des éditeurs et des supports qui peuvent demander l'accès au réseau interne pour la maintenance ou la correction des applications. Dans la continuité de cette démarche, il est nécessaire pour l'établissement de pouvoir sécuriser ses flux Internet et de messagerie, par l'adoption de solutions matérielles ou logicielles en amont du réseau interne.

L'hôpital est un établissement public de santé mentale. Les équipes font évoluer leurs pratiques et travaillent avec les patients sur l'utilisation de ces nouvelles technologies pour les aider dans des recherches d'emplois, administratives … En effet, la multitude des services directement accessible depuis Internet facilite les démarches et l'accompagnement des patients dans leur quotidien. Mais l'outil Internet est aussi nécessaire pour la préparation des activités ou des séjours thérapeutiques. Il en est de même pour les temps de recherches documentaires dont bénéficient certaines professions. De plus, la forte mobilité des personnels, entre les sites distants et le site central impose de fournir les mêmes autorisations d'accès quelque soit leur lieu de connexion, sur le système d'information du CH de Montbert.

A travers ces besoins, le constat d'une solution de filtrage des flux Internet personnalisable s'impose. Parmi l'ensemble des besoins recensés, il apparait des spécificités pour certaines unités liées à leurs missions de soins, comme la consultation de sites Internet interdits par la loi : jeux d'argents, drogues et stupéfiants. La consultation des blogs est aussi prédominante dans les équipes. Or de nombreuses pages ou domaines de ce type sont bloqués par la solution actuelle, sans intervention préalable du service informatique. Les sites marchands sont aussi un problème, notamment pour les services économiques et techniques qui travaillent avec des enseignes. L'usage de la messagerie doit également être abordé, notamment pour la problématique du transfert d'informations confidentielles, en interne ou en externe, mais aussi sur les contenus des pièces jointes.

Les solutions de sécurisations à déployer pour la partie flux web doivent instaurer une transparence totale. D'un coté le service informatique ne doit pas être désigné comme juge du blocage de certains sites par les équipes. D'autre part, les utilisateurs doivent être responsabilisés face à l'usage de ces réseaux. La traçabilité des connexions, la charte informatique, l'évolution des usages sont des objectifs à atteindre. De la même façon, la sécurité des courriers électroniques doit être améliorée. Les critères de diffusion des pièces jointes, le contenu, la lutte contre le spam, les publicités et les virus sont des points critiques auxquels des réponses vont être apportés. Cette sécurisation sera complémentaire à la mise en œuvre de la messagerie sécurisée à destination des médecins pour les échanges d'informations entre hôpital et médecine de ville.

Afin de mieux comprendre les technologies aujourd'hui disponibles sur le marché et proposées par différents éditeurs, des connaissances sur les éléments des réseaux sont indispensables (Annexe A), mais aussi sur les textes réglementaires importants.

2 Le contexte

2.1 Présentation du Centre Hospitalier de Montbert

Etablissement Public de Santé Mentale, le Centre Hospitalier de Montbert offre des soins à la population du Sud du département de la Loire Atlantique.

La prise en charge des patients s'organise dans le cadre d'équipements diversifiés. Au-delà de l'accueil en hospitalisation temps plein sur le site de Montbert, l'établissement dispose des structures suivantes :

- Hôpitaux de Jour (HJ) : accueil à la journée ou en séquentiel pour des soins polyvalents individuels.
- Centres Médico Psychologiques (CMP) : organisent des actions de prévention et de diagnostic et de traitement ambulatoire.
- Centres Accueil Thérapeutique à Temps Partiel (CATTP) : visent à maintenir ou à favoriser une existence autonome par des actions de soutien et de thérapies de groupes.
- Visites à domicile (VAD) : suivis des patients au plus près de leur lieu de vie.

L'évolution des soins en psychiatrie a conduit à élargir le panel de services offerts à la population. Ainsi, s'est créé en complémentarité aux pôles d'activité clinique, un pôle intersectoriel composé de plusieurs unités d'accueil et de soins ambulatoires :

- Centre d'accueil psychologique pour adultes et enfants.
- Unité de prévention du suicide.
- Unité d'addictologie et de d'alcoologie.
- Unité de psychiatrie-précarité.
- Unité de psychogériatrie.

Parallèlement, se développe un important travail avec d'autres institutions sanitaires mais également des partenaires du secteur social, médico-social et associatif. La mise en réseau de tous ces acteurs participe à l'amélioration de la qualité de la prise en charge des quelques 6000 patients suivis annuellement par les équipes du Centre Hospitalier.

L'engagement « Qualité » de l'établissement constitue aujourd'hui le fil conducteur de l'action de chacun des professionnels de l'établissement. La certification attribuée par la Haute Autorité en Santé Publique en 2008 reconnaît cette qualité tant dans l'organisation de nos services que dans la dispensation des soins.

Installé actuellement sur la commune de Montbert, le Centre Hospitalier prépare une profonde mutation architecturale avec un positionnement à l'échéance de janvier 2012 sur la commune de Bouguenais, en périphérie de Nantes. L'ouverture de ce nouvel établissement constitue une opportunité pour améliorer les conditions d'accueil des patients, de travail des personnels mais aussi pour procéder à une refonte globale du système d'information informatique de l'établissement.

L'utilisation du réseau Internet est devenu indispensable pour communiquer, rechercher de l'information, pour le fonctionnement de nombreuses applications. L'intégration rapide de tous ces nouveaux services directement au sein des équipes soignantes, pour exercer leur activité professionnelle, dévoile des problématiques de sécurisation des échanges majeures.

2.2 Le système d'information du CH de Montbert

Le système d'information informatique du CH de Montbert a été créé au début des années 2000 et évolue chaque année, et plus fortement depuis 2007. Le service informatique est directement associé à la direction générale (Annexe S). Le responsable est le directeur de l'établissement, M. Praud. La perspective de la construction d'un nouveau site permet de repenser entièrement l'organisation existante dont la gestion des flux Internet et de messagerie.

L'ensemble des ressources informatiques sont supportées par une ferme de deux serveurs physiques qui assurent le fonctionnement d'une trentaine de serveurs virtuels. Une baie de stockage héberge les données de ces serveurs. Une seconde ferme de six serveurs accueille les bureaux virtuels des utilisateurs et les applications publiées.

L'architecture réseau WAN du CH de Montbert est centralisée sur le site principal du CH et les sites distants y sont raccordés par des connexions VPN (Annexe B). L'ensemble des flux (navigation Internet, impression, messagerie pour certains) transitent alors par la ligne SDSL principale de 4Mo. La bande passante utilisée est souvent très importante et parfois même saturée. Le futur établissement disposera d'un lien en fibre optique de 100 Mo qui devrait régler une partie des problèmes rencontrés à ce jour.

Dans le cadre du déménagement vers le nouveau site, de nombreuses consultations ont été lancées et certaines sont toujours en cours. L'ensemble du système est réactualisé avec des matériels neufs : matériels actifs du réseau, système de stockage, déploiement de la téléphonie sur IP. Le futur Centre Hospitalier disposera de deux salles serveurs qui auront la charge d'assurer la continuité de service. Des scénarios de basculement sont en cours d'étude pour

répondre aux situations imprévues les plus diverses, surtout lors de l'absence de l'équipe informatique les soirs et week-ends.

A l'image de la profonde mutation nécessaire de son système informatique, la continuité de service pour les accès Internet et de messagerie est également indispensable et impose la mise en œuvre d'outils dédiés.

2.3 Les enjeux de la sécurité et de l'accès aux données

L'utilisation de l'outil informatique au CH de Montbert est en forte progression ces dernières années. L'informatisation du recueil des données médicales des patients et du circuit du médicament a impulsé une dynamique forte. Les soignants sont contraints aujourd'hui à saisir sur informatique toutes les informations concernant le patient. Il en est de même pour les personnels administratifs avec l'accès à de nombreux services en ligne. De plus, les nouvelles générations, déjà aguerries à l'usage de l'outil informatique, mettent en évidence des risques de sécurité non rencontrés jusqu'à présent.

La sécurisation des flux entrants et sortants de l'établissement devient un problème majeur, de part la « culture informatique » de plus en plus développée, mais aussi par la multitude des possibilités d'accès à Internet. Dans son dernier rapport, l'institut Osterman Research se montre inquiet face à l'évolution des spams et malwares sur les réseaux. En effet, en 2010 près de 61% des attaques subies ont pénétré les réseaux d'entreprises par la navigation Internet et les échanges de courriers électroniques [WEBSENSE1]. En mars 2010, Microsoft a réussi à faire fermer l'un des plus gros réseaux informatiques utilisés depuis 2006 pour envoyer des spam à travers le monde : le réseau Rustock. Celui-ci comptait un million de machines. Infectées « *Malheureusement, le démantèlement de ce botnet ne règlera pas le problème car il existe aujourd'hui d'autres botnets comptant jusqu'à 10, 12 ou même 15 millions d'ordinateurs prêts à faire feu* » [COLOMBAIN]. Le périmètre d'accès aux données n'est plus limité à l'organisation seule, car le travail à la maison et la multiplication des accès distants, de tout type, rendent de plus en plus difficile la sécurisation des flux et par conséquent la perte ou le vol de données. Ce dernier point est très important et justifie les moyens affectés à la sécurisation. Ainsi, le ministère des finances français a été la victime d'une attaque en décembre 2010 [MANENTI]. Un pirate a exploité une faille de sécurité des fichiers pdf pour y introduire un cheval de Troie. Celui-ci s'est propagé sur le réseau interne après l'ouverture du fichier afin de dérober des informations confidentielles. En avril 2011, la société SONY a elle aussi subit une attaque de dénis de service très important au cours de laquelle les coordonnées bancaires, utilisées sur le réseau

« PlayStation Network », de 77 millions de clients au travers le monde ont été dérobées [NYTIMES]. Ces actualités récentes démontrent que le vol de données est devenu l'objectif principal des pirates informatiques. Dans le domaine médical, le secret de ces informations est d'autant plus capital.

Ces quelques évènements prouvent l'importance que l'établissement se doit d'accorder à la problématique de la sécurisation, tout en offrant aux usagers des outils performants et qui répondent à leurs attentes.

2.4 Les objectifs du mémoire

Pour répondre à la problématique de sécurisation des flux sur le CH de Montbert, j'ai défini les objectifs suivants :

- Je présente un état des lieux des méthodes actuelles de sécurisation des flux, en analysant les avantages et défauts de chacune.
- J'évalue trois solutions de filtrage des flux Internet et j'en déduis les fonctionnalités et service les plus appropriés pour un déploiement sur l'établissement.
- J'évalue également deux solutions de filtrage des flux de messagerie et j'en déduis les fonctionnalités importantes à embarquer dans la future solution.
- Je présente un comparatif financier des différentes solutions et l'impact sur le budget de l'établissement.
- Je propose un planning de déploiement prenant en compte les nombreuses contraintes liées au déménagement début janvier 2012.

L'étude de ces solutions de sécurisation des flux me permettra de rédiger par la suite les documents nécessaire à la publication d'un marché public à procédure adaptée. Celui-ci contiendra un Cahier des Clauses Techniques Particulières (CCTP), le Cahier des Clauses Administratives Générales (CCAG) et le Règlement de Consultation (RC). J'y ajouterai les tableaux de réponses contenant les fonctionnalités souhaitées par l'établissement et celles complémentaires de la solution proposée par le soumissionnaire.

Ces consultations devraient être réalisées avant la fin du contrat de maintenance de la solution actuelle. J'ai l'opportunité avec ce mémoire d'aborder dès aujourd'hui les souhaits et les problématiques à traiter.

3 Législation et cybersurveillance

Le développement du monde Internet n'était à l'origine pas encadré. Afin de résoudre nombres de problématiques sur ce sujet, la réglementation cherche à rattraper son retard pour définir des règles, aussi bien pour les particuliers que pour les entreprises.

3.1 La loi Hadopi

La loi Hadopi ou loi Création et Internet, (Loi n°2009-669 du 12 mai 2009) doit favoriser la diffusion et la protection de la création sur Internet. C'est une loi française qui vise à mettre un terme aux partages de fichiers lorsque ces partages se font en infraction avec les droits d'auteurs. Cette loi crée une « Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet » (Hadopi), organisme indépendant de régulation. Elle comporte deux volets : le volet de la « riposte graduée » et le volet d'amélioration de l'offre légale.

Le premier instaure le principe d'une « riposte graduée », en trois étapes, pour l'internaute qui sera soupçonné de téléchargement illégal : un email d'avertissement, puis une lettre recommandée et enfin la suspension ou résiliation de son abonnement Internet. Le titulaire de la ligne doit donc mettre en place des outils pour sécuriser son accès et éviter ainsi l'usurpation de leur adresse IP à des fins de piratages ou de téléchargements illégaux [QUADRATURE1]. Le second volet doit permettre le développement des offres de téléchargements légales, par l'intermédiaire de plateformes dédiées.

Les conséquences pour les entreprises de l'adoption de cette loi sont importantes, car il n'y a pas de distinction entre particuliers et entreprises. Des investissements importants doivent être réalisés dans le domaine de la sécurité informatique, notamment dans des solutions de filtrage de flux Internet. En effet, dans les grandes sociétés, plusieurs centaines de personnes peuvent utiliser Internet avec une seule adresse IP. L'identification des personnels effectuant des téléchargements illégaux est donc très difficile dans ce cas. L'installation de ces outils de filtrage au sein des systèmes d'information doit entraîner simultanément la mise à jour des chartes informatiques des établissements et leur diffusion auprès de tous les agents [LE POINT].

Cette loi fait suite à la directive européenne 2001/29/CE transposée en droit français par la loi DADVSI qui cherche spécifiquement à protéger les droits d'auteur sur Internet. Elle a été censurée en partie par le conseil constitutionnel sur certaines mesures clés, mais tout de même promulguée le 12 juin 2009. Un complément a été apporté par une nouvelle loi, dite « Hadopi

2 » adoptée par le Sénat le 21 septembre 2009. Le décret n°2009-1773 du 31 décembre 2009 institue la création de la Hadopi.

Le Centre Hospitalier de Montbert se doit de respecter les obligations légales et réglementaires et pour ce faire souhaite acquérir prochainement des solutions de filtrage appropriés afin de sécuriser sa connexion Internet.

3.2 La loi LOPPSI 2

La loi n° 2011-267, publiée au journal officiel le 15 mars 2011, loi d'orientation et de programmation pour la performance de la sécurité intérieure, appelée LOPPSI 2, est une loi qui concerne la gestion de la police et de la gendarmerie sur la période 2009-2013. Le texte traite de la criminalité en générale, de la récidive, de la délinquance routière, de la « cyber-pédopornographie ». Il donne également de nouveaux pouvoirs à la police et prévoit d'en déléguer aux polices municipales et aux entreprises de sécurité privée.

L'objectif de cette loi est d'engager une lutte contre la cybercriminalité sur Internet. Ainsi, l'usurpation d'identité est maintenant reconnue et sanctionnée par l'article 222-16-1 du code pénal. Les fournisseurs d'accès à Internet sont directement mis à contribution et doivent appliquer directement des demandes émanant des autorités sur le blocage de site pédopornographique, sans avoir à demander l'aval de l'autorité judiciaire. Ils doivent également mettre en œuvre les moyens techniques pour bloquer les accès à une liste noire de sites, non publique, ainsi que le filtrage des adresses IP, constituée par l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), organisme dépendant du ministère de l'Intérieur. La police, sur autorisation du juge des libertés, pourrait utiliser tout moyen (physiquement ou à distance) pour s'introduire dans des ordinateurs et en extraire des données dans diverses affaires. Le collectif La Quadrature du Net a lancé des démarches auprès du Parlement européen dans le but « *d'encadrer strictement les mesures de filtrage mises en œuvre au niveau national* » et ainsi protéger les utilisateurs d'actes malveillants.

3.3 Les entreprises peuvent-elles filtrer ?

Le droit de filtrer autorise les entreprises à intégrer dans leurs systèmes d'informations les moyens techniques nécessaires pour sécuriser les flux Internet afin de protéger juridiquement et pénalement les entrepreneurs et décisionnaires. Parallèlement à ce droit de filtrer, il faut y adjoindre un droit de loguer, qui consiste à conserver les traces des connexions des utilisateurs, en suivant des règles précises.

La notion de « filtrage » apparait déjà dans un arrêté du 27 juin 1989 et est définie comme « la mise en correspondance de formes selon un ensemble prédéfini de règles ou de critères ». La circulaire relative à l'usage d'Internet dans le cadre pédagogique et de protection des mineurs du 18 février 2004 a permis « la mise en œuvre d'outils de filtrage dans les établissements scolaires et les écoles ». Enfin, il existe un certain nombre de documents réalisés par la Commission Nationale Informatique et Libertés (CNIL), et en particulier : les Fiches de synthèse « Cybersurveillance sur les lieux de travail » du 11 février 2002, le rapport de la CNIL « La cybersurveillance sur les lieux de travail », édition mars 2004, ou plus récemment, en 2008, le Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2008 dont la Fiche n°6 porte sur le « Contrôle de l'utilisation d'Internet et de la messagerie ».

Au-delà des mots « filtre » et « filtrage », il existe d'autres textes qui visent à travers des terminologies différentes un même objet. Ainsi l'article 6 I.– 1° de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (« LCEN ») ne retient pas le terme de filtre mais, utilise celui de *« moyens techniques permettant de restreindre l'accès à certains services de communication au public en ligne ou d'opérer une sélection de ces services* ». De même que l'article L. 335-12 du Code de la propriété intellectuelle utilise les termes *« moyens de sécurisation* » et dernièrement, la « loi Hadopi ». Le droit communautaire reconnaît également le droit de filtrer, et ce depuis 1999 à travers : La décision 276/1999 CE du 25 janvier 1999 du Parlement et du Conseil Européen, qui adopte un plan d'action pluriannuel visant à promouvoir une utilisation plus sûre d'Internet, par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux.

3.4 Les entreprises peuvent-elles enregistrer et conserver les traces ?

Les logs ou les traces sont un corollaire technique des outils de filtrage. Ces outils permettent en effet non seulement de restreindre ou de contrôler des accès à des sites web sur Internet, mais ils permettent également de tracer de manière individuelle ou collective l'usage d'Internet.

Il apparaît que ce droit existe bien au travers des terminologies différentes du mot « log » ou « loguer ». De plus, il semblerait également que la jurisprudence reconnaisse le droit de loguer. Dans un arrêt du 9 juillet 2008, la Cour de Cassation a retenu que les connexions à Internet étaient présumées professionnelles. L'employeur peut donc rechercher ces données et ce, hors de la présence de l'employé.

L'OSSIR, au travers de son livre blanc sur les logs [OSSIR], recommande d'informer et de sensibiliser l'ensemble des personnels, en portant à leur connaissance les référentiels et en complétant cette information par des formations.

3.5 Les obligations et responsabilités en vigueur

3.5.1 Les catégories interdites

Il existe deux types de sites web illicites, de part leur contenu ou bien des produits et services qu'ils peuvent commercialiser. S'agissant de la première catégorie, il s'agit de sites dédiés à des contenus portant notamment atteinte aux mineurs, tels que les contenus pédopornographiques, ou encore les contenus incitant à l'anorexie et aux monopoles, comme par exemple en matière de jeux de hasard, ou à la protection des auteurs, s'agissant des sites contrefaisants.

Il s'agit également de sites dont les contenus dépassent la liberté d'expression, tels que les sites racistes ou révisionnistes.

Pour ce qui concerne la seconde catégorie de sites web, il s'agit de la mise à disposition, de la vente, de la location de produits tels que notamment et plus généralement, des produits interdits ou réglementés :

- Des organes et produits du corps humain ;
- Des drogues ;
- Des objets à caractère pédophile ;
- Des armes à feu et explosifs ;
- Des médicaments ;
- Du tabac ;
- De l'alcool ;
- Des logiciels permettant de porter atteinte à un système de traitement automatisé de données ;
- Des logiciels de contournement de mesures techniques de protection ou d'information.

Le service d'addictologie du CH de Montbert travaille notamment sur les thèmes de l'alcool, du tabac et des drogues et rencontre de nombreuses difficultés dans ses activités au quotidien, car toutes ces catégories sont bloquées par le système mis en place.

3.5.2 Les personnes tenues de filtrer

L'obligation légale la plus exemplaire dans ce domaine correspond à celle qui pèse sur les fournisseurs d'accès à Internet à travers l'article 6 I. – 1° de la LCEN**.** Cet article, s'il impose directement au fournisseur d'accès de proposer à ses abonnés un moyen technique permettant de restreindre l'accès à Internet, implique indirectement l'obligation pour ledit abonné de le mettre en œuvre, sous sa responsabilité.

Cependant, il existe des articles et cas de jurisprudence qui instaurent des doutes quant à l'unique responsabilité des opérateurs. En effet, l'article L. 34-1 du Code des Postes et Communications Electroniques impose le filtrage aux opérateurs déclarés auprès de l'ARCEP, mais également à toute personne qui permettrait au public de disposer d'une connexion à Internet. En effet, l'article L.6 I.- 1° de la LCEN énonce : « *Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.*» De plus, l'article L. 34-1 du même code précise également que : « *Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article »*. Enfin, l'arrêt de la Cour d'appel de Paris du 4 février 2005 aurait pour certains auteurs, assimilé l'employeur qui donne accès à ses employés à Internet, à un fournisseur d'accès. De fait, si cette interprétation devait s'imposer, tout employeur qui mettrait à disposition de ses employés, de ses agents ou de toute autre personne un accès à Internet, pourrait se voir opposer l'obligation légale de à l'article 6 de la loi pour la confiance dans l'économie numérique, qui est de mettre à disposition des outils de filtrage et d'informer les utilisateurs.

Il convient également de tenir compte de certains projets ou propositions de loi et autres lois complémentaires, comme les lois Hadopi et Lopsi, dans le but de protéger les auteurs contre le téléchargement illégal et par conséquent de mettre en place des outils de filtrage.

3.5.3 Les responsabilités engagées

3.5.3.1 Responsabilité civile et pénale

L'article 1384 alinéa 5 du Code civil, énonce : « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. (...) Les maîtres et les*

commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ». L'employeur est alors considéré comme responsable des agissements de ses employés. La jurisprudence relativise cependant cette responsabilité, mais incite fortement à mettre en œuvre tous les outils permettant de maîtriser et de contrôler l'utilisation d'Internet.

A côté de la responsabilité civile de l'employeur se pose naturellement la question de sa responsabilité pénale. Cette responsabilité peut elle-même être appréhendée sous deux angles. L'employeur est-il responsable des infractions pénales commises par ses employés qui utilisent les accès professionnels à Internet ? L'employeur est-il responsable s'il n'empêche pas ou permet même de manière fortuite à ses employés d'accéder à des contenus illicites ? L'article 121-1 du Code pénal stipule que par principe, l'employeur n'a pas à être responsable des fautes pénales commises par ses employés. Il s'agit ensuite de savoir lors d'une infraction si celle-ci est commise en lien avec l'entreprise ou non. Suivant le cas, la responsabilité pénale peut-être engagée.

En résumé, que l'employeur soit tenu par obligation ou qu'il y soit vivement invité, selon le célèbre principe de précaution, il est dans son intérêt aujourd'hui de mettre en œuvre et de déployer des mesures de contrôle d'accès à Internet.

3.5.3.2 Les responsabilités des administrateurs du système d'information

Comme le précise la CNIL dans son « *Guide pratique pour les employeurs et les salariés* », les administrateurs ont pour fonction d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Dans le cadre de leurs fonctions, ils peuvent être amenés à accéder à des informations personnelles concernant les utilisateurs (messagerie, historique des sites consultés, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…). D'après la CNIL, un tel accès n'est justifié que lorsque le bon fonctionnement des systèmes informatiques ne pourrait être assuré.

Les administrateurs sont en outre soumis à une obligation de confidentialité. Ils ne doivent donc pas communiquer les informations dont ils auraient eu connaissance dans le cadre de leurs fonctions. En particulier, ils ne peuvent révéler les informations entrant dans le champ du secret des correspondances et de la vie privée des utilisateurs, dès lors que de telles informations ne portent atteinte ni au bon fonctionnement technique des applications, ni à la sécurité, ni à l'intérêt de l'entreprise.

Enfin, les responsabilités des administrateurs pourront être recherchées dans le cas ou le Directeur des Systèmes d'Information (DSI) n'aurait pas informé ses dirigeants de l'existence de moyens de contrôles et de restrictions, mais aussi dans le cas de l'exécution de demandes formulées par l'employeur et qui s'avéreraient illicites.

3.6 Les chartes d'informations

Le déploiement de solutions de sécurisations des flux web et mails nécessite la création ou la révision d'une charte d'utilisation des nouvelles technologies de l'information et de la communication adaptée. En effet, ce document permet de préciser les responsabilités civiles et pénales de chacun, mais il est de plus admis et connu de tous.

Dans le cadre du plan hôpital 2012, le CH de Montbert est en cours de rédaction de sa politique de sécurité des systèmes d'informations, travail toujours difficile et long à finaliser. Une révision de la charte a été validée le 21 février 2011. Cependant, une charte informatique plus succincte pourrait être rédigée. La CNIL a émis de nombreuses recommandations à destination des entreprises et de leurs salariés [CNIL-EMPSAL] pour répondre à l'évolution des technologies. Pour être effective et opposable, la charte doit être diffusée nominativement, accessible par tous sur le lieu de travail, soumise au directoire et CHSCT, déposée au greffe du tribunal administratif et enfin transmise à l'inspection du travail en double exemplaire. A l'issue de toutes ces démarches, les responsabilités sont établies et la charte est un véritable outil en cas de litige.

La démarche de mise en œuvre de la charte NTIC s'inscrit dans une logique de cohérence entre contrainte technique et politique de ressources humaines. La charte doit fixer clairement les règles quant à l'utilisation des ressources informatiques et être approuvée par les utilisateurs.

4 Les techniques de filtrage de flux Internet

Au travers de son livre blanc « *Rapport sur les menaces 2010* » [WEBSENSE1], la société Websense dresse un constat surprenant de l'évolution des menaces sur Internet. En effet, le nombre de sites malveillants aurait augmenté de près de 112% par rapport à 2009 et 80% des sites Internet diffusant des codes malveillants étaient des sites légitimes victimes d'attaques de pirates informatique. Enfin, 52% des attaques informatiques auraient pour but le vol de données, afin d'accéder à des éléments financiers. D'après Websense, ce sont les recherches effectuées

dans un cadre extra-professionnel qui représentent le risque le plus important d'exposition aux logiciels espions.

Figure 1 : proportion de pages visitées contenant des liens malveillants dans un échantillon de trafic Web hébergé prélevé dans le courant de l'année 2010 (WEBSENSE1)

Ce graphique démontre qu'une solution antivirale, bien qu'indispensable, ne protège pas suffisamment les utilisateurs et les entreprises des nombreuses menaces d'Internet. Il convient alors de mettre en place les solutions techniques nécessaires pour protéger les réseaux internes de ces agressions extérieures. Pour atteindre ces objectifs de sécurité, il existe différentes méthodes d'analyse et de sécurisation des flux Internet.

4.1 Le filtrage par IP

Le blocage par adresse IP repose sur un principe simple qui consiste à comparer les adresses IP des paquets à acheminer avec une liste prédéfinie d'adresses IP. Si une adresse appartient à cette liste les paquets ne seront pas acheminés et la navigation vers cette adresse sera alors bloquée.

4.1.1 Principe de fonctionnement

Le blocage IP consiste précisément à analyser l'entête IP qui contient les adresses des machines émettrices et destinataires du paquet. Les filtres de niveau 3 permettent de définir des règles sur les adresses source et destination. Dans le cas de blocage d'accès à un site web hébergé sur une machine physique, tout le trafic entrant et sortant de l'adresse de cette machine se trouvera bloqué.

Lorsque le blocage IP est effectué de manière asymétrique dans le sens du trafic descendant du serveur vers l'utilisateur, ce dernier perçoit un allongement du temps de réponse suivi d'un message d'erreur de type « *connection timed out* ». Lorsque le blocage est effectué dans le sens

montant, c'est-à-dire de l'utilisateur vers le serveur, ce dernier n'a pas la possibilité de contrôler les tentatives de connexion, par conséquent l'utilisateur recevra sans délai un message d'erreur comme « *connection timed out* » ou « *couldn't connect* ».

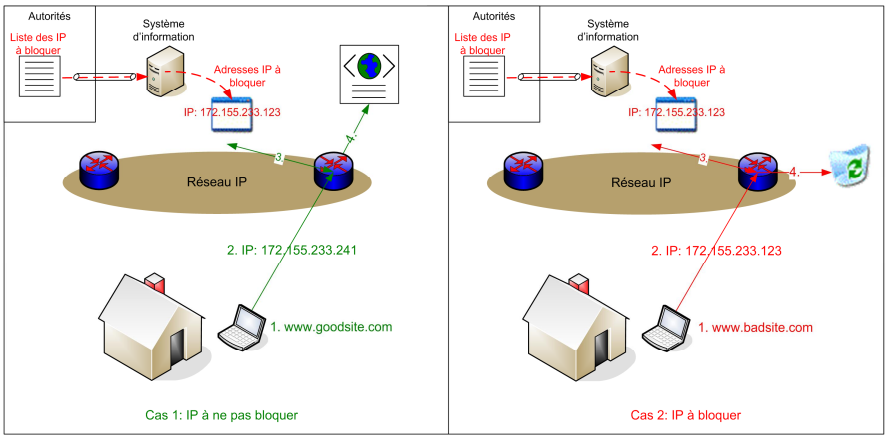


Figure 2 : principe de fonctionnement du blocage IP (Marpij)

Le blocage IP permet donc de rompre toutes les communications entre la machine bloquée et le réseau du FAI. Cela signifie que non seulement les accès web sont bloqués, mais aussi tous les autres services hébergés sur cette machine comme l'email, le chat … [DEIBERT-AD]. De même la machine bloquée ne pourra pas faire de requêtes web à partir du réseau du FAI ou initialiser toute forme de communication internet avec ce réseau.

Le blocage IP utilise relativement peu de ressources réseau, car les routeurs analysent de manière classique les adresses dans les entêtes IP et décident en fonction de router ces paquets. Mais en pratique, les routeurs ne peuvent appliquer qu'un nombre limité de règles. Le plus souvent ils sont déjà utilisés au maximum de leur capacité en raison de la forte croissance des trafics. Le traitement des règles supplémentaires est assuré sur une faible bande passante.

Il existe une autre variante du blocage IP de niveau 3 et qui permet d'apporter une meilleure granularité. Il s'agit du blocage de niveau 4 qui utilise toutes les informations disponibles au niveau 3 (IP) et qui les complète par une inspection des entêtes de données à l'intérieur des paquets IP dans le but de déterminer le numéro de port utilisé [DEIBERT-AD].

En basant les décisions de blocage sur une combinaison d'adresse IP et de numéro de port, il devient possible d'opérer un blocage par service. Cela permettrait de bloquer les accès http sur le port 80 et de laisser ouverts les autres services comme l'email ou le chat. Dans une procédure de routage classique, le routeur n'analyse pas les informations de la couche 4, ce qui signifie qu'il

faudrait accroître la charge de traitement au niveau des routeurs pour permettre un blocage de niveau 4.

Le blocage de niveau 4 apporte de nouvelles possibilité et une meilleure granularité de blocage par type de service. Le problème de différenciation des noms de domaines hébergés sur un même serveur, identifié par une seule adresse IP à bloquer n'est pas résolu. En effet, une machine peut héberger entre une dizaine et plusieurs milliers de sites web tout en utilisant un ou plusieurs noms de domaine. Les serveurs web des universités hébergent souvent plusieurs sites pour les différents départements et les pages personnelles des étudiants. Le site www.xs4all.nl a hébergé entre 3000 et 6000 sites web différents lorsqu'il a fait l'objet de blocages en 1996/1997 par les FAI allemands pour une douzaine de pages illégales [DORNSEIF].

Une telle concentration de sites sur un même serveur web a été rendue possible par l'adoption de la technique d'hébergement virtuel ou *« name based virtual hosting* » et qui est naturellement supportée en http/1.1 et par les logiciels compatibles http/1.0. Cette méthode est utilisée sur les serveurs web pour héberger plusieurs noms de domaines différents à la fois et parfois avec la même adresse IP. Grâce à cette technique il devient plus aisé pour un serveur d'héberger le contenu de différents sites web en utilisant des noms de domaines différents tout en partageant une même adresse IP. Cela signifie que bloquer une adresse IP entraine naturellement l'isolement de tous les noms de domaines hébergés sur ce serveur.

4.1.2 Impacts sur les architectures déployées

Ainsi, tout échange de données passant par un routeur appliquant ce blocage devient impossible. Cette technique reste très peu utilisée dans un contexte de blocage légal car elle ne permet pas d'effectuer un blocage fin et précis. En effet, elle bloque tout accès à un serveur ou un groupe de serveurs, et ne permet pas de traiter séparément des sites web différents localisés sur une même machine.

Cela est devenu particulièrement vrai avec l'adoption massive de techniques de partage d'adresses DHCP et de translation d'adresses NAT. Une étude universitaire menée à Harvard en 2003 souligne que plus de 87% des noms de domaines partagent leurs adresses IP avec un ou plusieurs autres domaines, et que plus des 2/3 des noms de domaines actifs partagent leurs adresses avec plus de 50 autres [EDELMAN1].

Le blocage IP a été une des premières techniques utilisées pour bloquer l'accès à certains sites web. Cette technique a été utilisée en Chine et au Vietnam et certaines études indiquent que le

blocage IP est utilisé par une large sélection de filtres encore disponibles sur le marché et installés dans les universités et bibliothèques publiques. En application d'une loi de 2002, le procureur général de l'état de Pennsylvanie a ordonné le blocage des sites pédopornographiques. Les FAI de cet état, notamment Worldcom, ont répondu rapidement en utilisant les techniques de blocage IP disponibles sur leurs routeurs pour empêcher l'accès à certaines adresses IP, bien que les serveurs en question contenaient une majorité de sites légaux. Une décision de justice rendue en septembre 2004 a jugé anticonstitutionnelle une telle loi et a mis fin au blocage des sites par cette technique. En France, certains opérateurs ont fait appel au blocage IP dans l'affaire Aaargh bloquant ainsi le site d'origine et son site miroir [EDELMAN1].

La technique de blocage IP ne fait intervenir que l'analyse des adresses IP et leur comparaison avec une liste d'adresses IP de sites à bloquer. Ce faisant, l'utilisateur final n'est pas informé du blocage effectué et perçoit simplement une absence de réponses à ses requêtes, ce qui le pousse le plus souvent à réessayer.

L'analyse de la technique de blocage IP et les expérimentations qui s'en sont suivi suggèrent que cette technique mène à des surblocages fréquents. Cela survient pour deux raisons au moins : la première, est que les responsables du blocage ne disposent pas de moyens permettant de savoir *ex-ante* quels autres sites partagent le même serveur web. La deuxième raison, à supposer que la première condition soit vérifiée, est que le principe même du blocage IP impose que tous les sites hébergés à la même adresse soient inaccessibles. A partir de ce constat, les opérateurs ont imaginé de nouvelles techniques de blocage.

4.2 Le filtrage par BGP

Le blocage BGP repose sur le principe de re-routage des adresses IP à bloquer vers un routeur spécifique chargé d'implémenter un traitement particulier à ce trafic. Elle fait appel au protocole BGP qui achemine les trafics à l'intérieur du réseau IP entre systèmes autonomes et utilise l'agrégation de routes afin de limiter la taille des tables de routage. Ce protocole n'était à l'origine supporté que par les routeurs de cœur de réseau ou de peering ayant des fonctionnalités d'apprentissage des routes à partir des routeurs auxquels ils sont interconnectés. Mais de plus en plus de routeurs disposent aujourd'hui de cette fonctionnalité. Par conséquent, ce blocage peut être mis en œuvre à n'importe quel niveau du réseau du FAI.

4.2.1 Principe de fonctionnement et mise en œuvre

Le blocage BGP, sous toutes ses formes, repose sur la mise en place d'un routeur BGP qui annonce des routes particulières à ses voisins. Dans un contexte de blocage, ce routeur va annoncer au reste du réseau qu'il détient les informations de routage pour la liste des adresses IP des sites à bloquer. De façon dynamique, chaque paquet ayant pour destination l'adresse IP d'un site à bloquer sera redirigé vers le routeur BGP spécifique [FERRARI]. Ce principe général reste valable quelles que soient les options d'implémentation. Trois d'entre elles paraissent les plus adaptées à une implémentation au niveau des réseaux des FAI français.

4.2.1.1 Option 1 : le routeur BGP d'annonces est hébergé par les autorités

Cette option consiste à falsifier les annonces de routes vers les IP à bloquer au niveau d'un routeur BGP qualifié d' « externalisé Etat » et qui sera mis à disposition des FAI par les autorités (ou par un sous-traitant des autorités). Il peut être situé au niveau d'un centre de co-localisation où tous les FAI sont déjà présents. Il devra alors s'interconnecter aux routeurs de peering de chacun des FAI à travers des liaisons locales (en pratique, quelques jarretières fibres à tirer entre les paires de routeurs). La liste des adresses IP des sites à bloquer sera mise à jour au niveau de ce routeur BGP d'annonces qui publiera vers les autres réseaux de façon dynamique les annonces de routes correspondantes. Au final, cela se déroule comme si deux FAI étaient interconnectés dans le cadre d'un accord de peering. Cette technique est communément appelée « puits de blocage » (Sink Hole).

Concrètement, le routeur BGP d'annonces se déclare autoritaire sur les adresses IP (/32) correspondant aux sites à bloquer, et annonce à ses voisins les routes vers ces adresses IP avec la plus forte préférence locale. Cela signifie que les routes annoncées seront systématiquement empruntées par les paquets, bien que différentes des routes réelles en situation de non blocage.

De son côté le réseau du FAI reçoit des annonces eBGP du routeur « externalisé Etat » lui indiquant que les adresses IP des sites à bloquer sont accessibles via ce routeur. Une première possibilité consisterait à router tout ce trafic vers le routeur BGP d'annonces qui se chargera ensuite de le détruire. Mais les FAI ne sont en général pas favorables à une telle solution car elle ne préserve pas la confidentialité des trafics de leurs abonnés. Ils préfèrent donc utiliser les annonces de routes eBGP qu'ils reçoivent du routeur BGP d'annonces pour labelliser le trafic et lui opérer un traitement adapté. Il est possible de configurer les routeurs du réseau du FAI de sorte que le trafic labellisé passe par une interface particulière, qu'il suffit de choisir judicieusement comme l'interface « poubelle » et tout le trafic sera alors détruit. Il est également

possible de rediriger le trafic vers un serveur qui publie une page web des autorités pour notifier le blocage à l'internaute.

La figure suivante illustre de manière schématique la mise en œuvre de cette option. Le serveur de blocage peut être hébergé dans le réseau « Etat» (variante 1),. Dans ce cas tout le trafic bloqué est renvoyé vers les équipements des autorités, ou dans le réseau du FAI (variante 2).

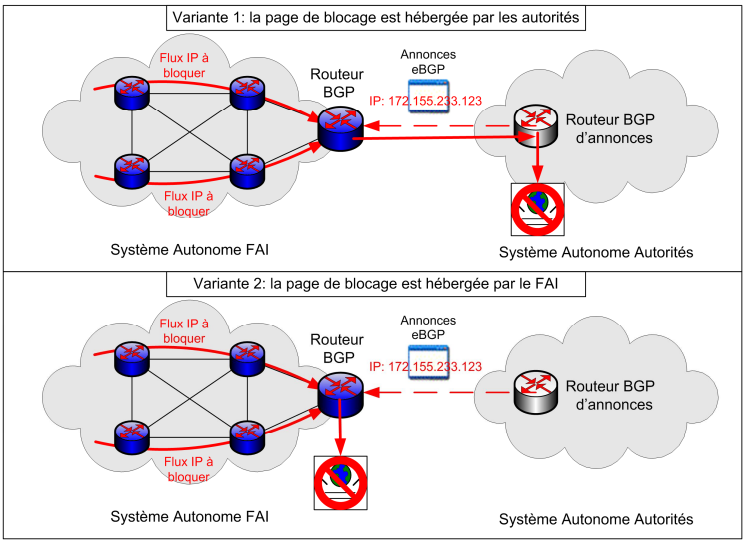


Figure 3 : mise en œuvre du blocage BGP – option 1 externalisé Etat (Marpij)

Cette option présente l'avantage d'être la même pour tous les FAI qui s'interconnectent au routeur BGP autoritaire. Ils n'ont donc pas à gérer de liste d'adresses IP ni à mettre à jour leurs configurations de routeurs. Ils se trouvent donc sur un même pied d'égalité et subissent de la même manière les surblocages éventuels engendrés par le blocage de certaines adresses IP.

4.2.1.2 Option 2 : le routeur BGP d'annonces est hébergé par les FAI

Dans le cas où les autorités ne souhaitent pas centraliser le routeur BGP d'annonces, chaque FAI devra mettre en place un tel routeur dans son réseau. Les listes des adresses IP à bloquer sont reçues régulièrement des autorités et injectées dans le routeur BGP d'annonces. Tout le reste fonctionne de manière identique, à la simple différence que les autorités n'hébergent plus aucun équipement. L'impact pour le FAI réside dans la mise en place dans son réseau d'un ou plusieurs routeurs BGP d'annonces et d'un système d'information spécifique. Par rapport à l'option 1, cela implique des coûts d'investissement et de fonctionnement supplémentaires. La figure suivante illustre de manière schématique la mise en œuvre de cette option.

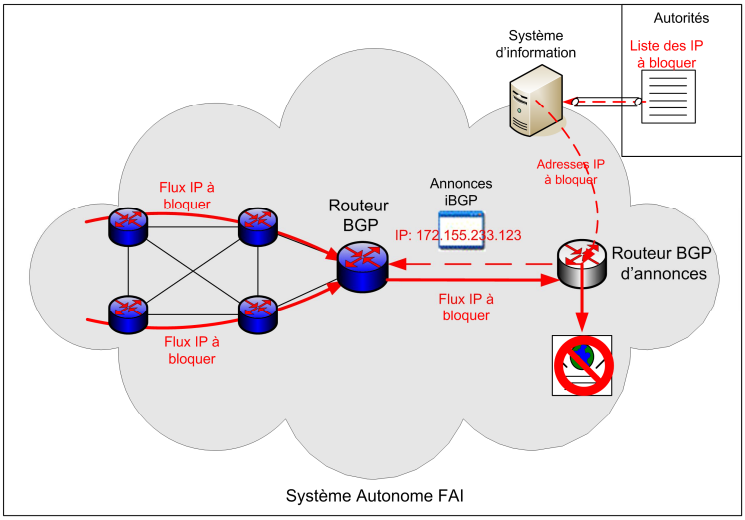


Figure 4 : mise en œuvre du blocage BGP – option 2 internalisé FAI (Marpij)

4.2.1.3 Option 3 : blocage BGP avec inspection d'URL

Il existe une troisième option d'implémentation du blocage BGP. Celle-ci est conditionnée à la fourniture par les autorités d'une liste d'URL des sites à bloquer, et non uniquement d'une liste d'adresses IP. En annonçant les routes pour ces adresses IP au reste du réseau, ce dernier attire et concentre tout le trafic IP qu'on peut qualifier de suspect.

Contrairement aux deux options précédentes, le traitement ne s'arrête pas au niveau du routeur BGP d'annonces. Ce dernier relaie le trafic vers un serveur DPI qui analyse les URL et les compare à celles de la liste noire. Lorsqu'il y a correspondance entre les URL, les paquets sont envoyés vers un serveur hébergeant une page spécifique, qui notifie les internautes du motif de blocage. Dans le cas où les URL ne correspondent pas, le trafic n'est pas à bloquer et il est routé à travers un lien dédié vers un opérateur de transit chargé de l'acheminer jusqu'à sa destination finale. Cette variante du blocage BGP est appelée hybride et sera définie ultérieurement.

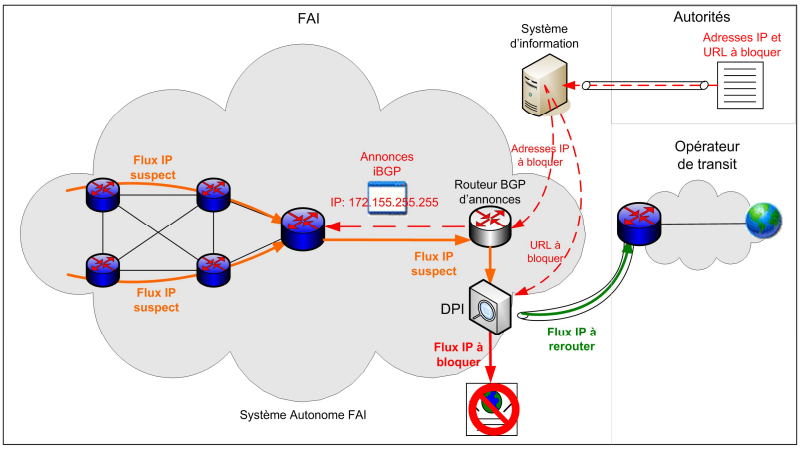


Figure 5 : blocage BGP avec inspection d'URL (Marpij)

Comparativement aux deux options de blocage BGP présentées plus haut, elle offre une granularité supérieure et ne bloque que les sites dont les URL figurent dans la liste. En revanche, elle présente des coûts d'investissement et de fonctionnement plus élevés en raison du serveur DPI, du lien de transit IP à mettre en place et des reconfigurations des routes BGP à chaque mise à jour de la liste d'URL. La figure ci-dessus illustre la mise en œuvre du blocage BGP avec inspection d'URL.

4.2.2 Impacts et effets de bord

Le surblocage induit par le blocage BGP est en tout point identique à celui du blocage IP. En effet, le blocage BGP se base sur les adresses IP pour bloquer les flux, ce qui entraîne un risque de surblocage. Cet effet de bord s'applique aux options 1 et 2 décrites précédemment, où les flux IP à bloquer sont concentrés sur un routeur unique du réseau du FAI et ne subissent aucune analyse ultérieure.

Dans l'option 3, le niveau de blocage supplémentaire que représente le DPI élimine le risque de surblocage lié aux adresses IP, puisque seules les URL de la liste (et non tous les domaines ayant la même adresse IP) sont bloquées. En contrepartie, le DPI peut constituer un goulot d'étranglement car sa capacité est limitée, et peut entraîner une congestion importante, si une adresse IP à fort trafic (ex. serveur Google, Youtube) a été insérée dans la liste d'adresses IP par erreur. De plus, il est difficile de dimensionner *ex-ante* le lien de transit IP à la sortie du DPI, en raison de la non prédictibilité du trafic bloqué, qui peut atteindre des niveaux élevés si tout le flux IP correspondant est redirigé vers le DPI pour inspection.

Par ailleurs, le BGP est un protocole complexe et son implémentation ne se prête pas à des mises à jour fréquentes des routes, car à l'origine il n'a pas été conçu pour le blocage, mais pour

router les paquets entre réseaux interconnectés. Il présente donc une certaine sensibilité aux erreurs pouvant survenir lors de mises à jour et reconfigurations fréquentes. Il convient de souligner qu'il s'agit d'un risque déjà assumé dans le cadre du peering.

Dans une note intitulée « *Principe, intérêts, limites et risques du blocage hybride à des fins de blocage de ressources pédopornographiques hébergés sur des serveurs étrangers*», l'auteur cite en illustration des risques que présente le blocage BGP, le cas de Youtube « *lorsque le Pakistan a ordonné le blocage de l'accès à des caricatures de Mahomet hébergées sur le service YouTube, un opérateur pakistanais a envoyé une commande BGP à des équipements mal paramétrés : ils ont propagé la demande aux réseaux d'opérateurs hors juridiction pakistanaise. L'accès à YouTube a alors été interdit pendant plusieurs heures dans plusieurs pays du monde. Cet événement a permis de mettre en évidence des risques pour la sécurité nationale, comme l'ont relevé des spécialistes réseaux».* [ESPERSN1]

En pratique, BGP est utilisé par tous les FAI au niveau des routeurs de peering, par lesquels transite tout le trafic internet.

4.3 Le filtrage par DNS

Le blocage par redirection DNS ou blocage DNS est une technique qui permet d'interdire l'accès à un nom de domaine hébergeant un contenu à bloquer. Cette technique repose sur le principe de falsification de la réponse à une requête DNS pour l'accès à un site interdit.

Aujourd'hui, toutes les communications internet faisant référence à un nom de domaine impliquent une résolution DNS préalable au routage. La redirection DNS n'agit pas en tant que telle au niveau du transport des données entre le site bloqué et l'utilisateur, mais permet de renvoyer une adresse IP différente selon que le site demandé est à bloquer ou pas. Cette technique est aujourd'hui déployée dans plusieurs pays européens comme la Norvège, le Danemark, l'Allemagne, l'Italie…

4.3.1 Principe de fonctionnement et mise en œuvre technique

Les données DNS sont distribuées sur une base de données mondiale gérée de manière partagée par les FAI, les hébergeurs et leurs partenaires. De ce fait chaque acteur gère ses domaines en zones et sous-zones sur lesquelles il détient tous les droits (il est dit alors autoritaire) et se réfère à ses partenaires pour les ressources situées en dehors de ses propres zones. Le système DNS définit plusieurs types d'enregistrements dont les principaux sont [TANENBAUM] :

- Les enregistrements d'Adresses – DNS A, Address record – qui donnent la correspondance entre un nom d'hôte et son adresse IP. Ce sont de loin les enregistrements les plus utilisés.
- Les enregistrements MX – DNS MX, Mail eXchange record – qui indiquent les serveurs mail SMTP à contacter pour envoyer des mails à un utilisateur de ce domaine.
- Les enregistrements NS – DNS NS, Name Server record – qui identifient les serveurs DNS de ce domaine.

Le protocole DNS prévoit un code de réponse « REFUSED » pour indiquer que le service de noms de domaine refuse de répondre à la demande pour des raisons de gestion. Ce code constitue donc un moyen simple d'interdire l'accès aux noms de domaine à bloquer. Cela se traduit pour l'utilisateur par un message d'erreur de type « Host not found ».

Pour opérer le blocage par DNS, une des méthodes dite par « détournement de nom (Name Hijacking) », consiste à créer une sous-zone spécifique pour les noms de domaine à bloquer à l'intérieur des zones de noms dont le FAI détient l'autorité. Il doit ensuite implémenter le type de réponse à donner en cas de requête portant sur cette sous-zone, par exemple l'adresse IP de la page de blocage des autorités à retourner [DEIBERT-AD].

Pour les noms de domaine qui ne sont pas à bloquer, le FAI doit mettre à jour sa base et la synchroniser avec les enregistrements des DNS autoritaires correspondants. Il peut également mettre en place un serveur DNS autoritaire (ou une paire de serveurs DNS pour assurer une haute disponibilité) dédié à répondre aux requêtes des noms de domaines figurant sur la liste noire. Il faut également créer au niveau de chaque serveur DNS récursif une sous-zone pour ces noms de domaine.

Lorsqu'une requête se présente au niveau d'un serveur récursif, il vérifie d'abord dans son cache si une requête similaire a été traitée récemment. Si aucune réponse n'y figure, il interroge le DNS autoritaire de blocage. Si le nom de domaine n'y figure toujours pas, la requête est relayée par le DNS récursif vers les autres DNS autoritaires et résolue normalement, comme l'illustre la figure suivante :

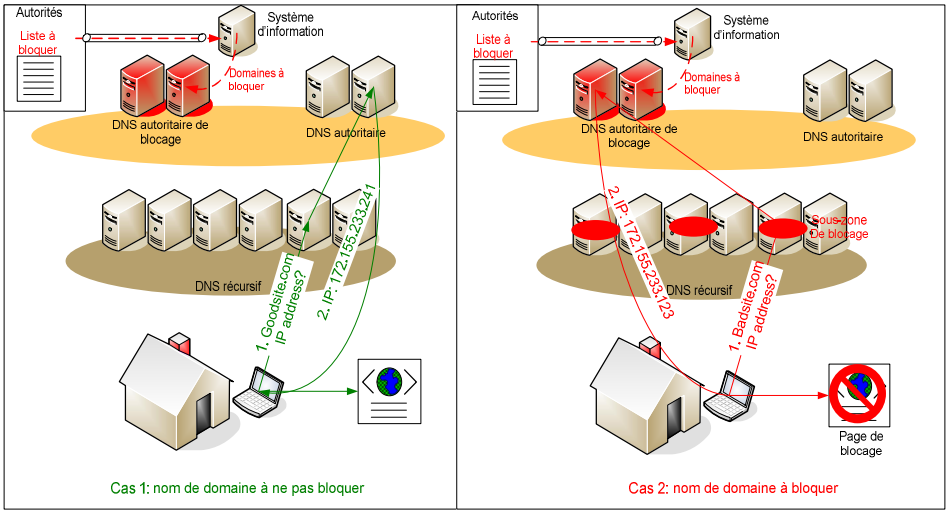


Figure 6 : principe de fonctionnement du blocage DNS (Marpij)

L'exemple suivant illustre quelques difficultés pouvant survenir dans la mise en œuvre du blocage DNS. Il s'agit par exemple d'interdire uniquement l'accès aux sites web du nom de domaine : bloquercesite.com. Le FAI crée alors dans sa base « DNS A » une zone pour ce domaine et y insère des données erronées visant à interdire l'accès (par exemple, l'adresse IP de la page de blocage des autorités). Il doit également récupérer les enregistrements MX et autres ressources DNS correspondantes, afin de ne pas bloquer les autres services comme l'email.

4.3.2 Impacts et effets de bord

A l'image du blocage IP, la redirection DNS ne permet pas de distinguer les pages à bloquer de celles qui ne le sont pas à l'intérieur d'un même nom de domaine. Elle peut entraîner le blocage de sous-domaines (ex : perso.bloquercesite.com à l'intérieur du nom de domaine bloquercesite.com) en fonction du type de redirection de la requête. Elle comporte donc un risque de surblocage, qui se limite cependant à des pages hébergées sur le même domaine.

Une étude universitaire de 2003, étudiant le blocage par DNS d'un site nazi en Allemagne, a montré que tous les FAI étudiés ont fait au moins une erreur de configuration lorsqu'ils ont configuré leurs filtres DNS. Sur 27 FAI, 45% étaient en situation de surblocage et de sous-blocage, 55% étaient "uniquement" en situation de surblocage, et 16 FAI sur 27 (59%) bloquaient les emails de plusieurs domaines non visés. Tous bloquaient l'adresse de l'administrateur du site ciblé qui ne pouvait donc plus communiquer avec cette adresse, y compris avec les services de police ou la justice. [DORNSEIF]

Les opérations nécessaires au blocage sont donc relativement simples dans leur principe, mais elles peuvent entrainer une complexité opérationnelle dans la maintenance et la mise à jour des

données, et donc avoir un coût de fonctionnement élevé. En effet, il faut rester vigilant aux services non visés par ce blocage, comme la messagerie électronique.

Par ailleurs, certaines entreprises disposent de leurs propres DNS. La mise en place de cette technique de blocage ne concernerait que les clients utilisant le DNS du FAI. Il ne faut pas globaliser à tous les clients grand public.

4.4 Le filtrage DPI

Les technologies de blocage de contenu par DPI consistent à analyser les contenus des paquets IP en forçant leur passage par un serveur DPI. En fonction des critères de blocage, le DPI autorise ou interdit le transit des paquets vers leur adresse destination.

4.4.1 Principe de fonctionnement et mise en œuvre technique

Le principe général repose sur le blocage des paquets IP selon une liste de critères définis par le FAI. Ces critères peuvent être de plusieurs natures : URL, numéro de port, signature de l'application… Les paquets qui répondent aux critères de blocage subissent un traitement particulier, par exemple un routage différent du reste du trafic ou un blocage pur et simple sans notification.

Les critères sont compilés et triés par catégorie avant d'être chargés dans un logiciel de blocage qui peut être configuré de façon à ne bloquer que certaines catégories. Quand les utilisateurs tentent d'accéder à une page Web, le logiciel vérifie sa liste de sites interdits et bloque l'accès à toute page qui s'y trouve. Adopté à l'origine dans des pays peu démocratiques pour contrôler les trafics internet sortants, le DPI peut être utilisé pour faire de l'inspection d'URL dans le contexte de blocage de sites.

Dans le contexte de blocage légal de contenus pédopornographiques, l'approche par inspection d'URL faisant appel à du DPI s'avère coûteuse et inappropriée.

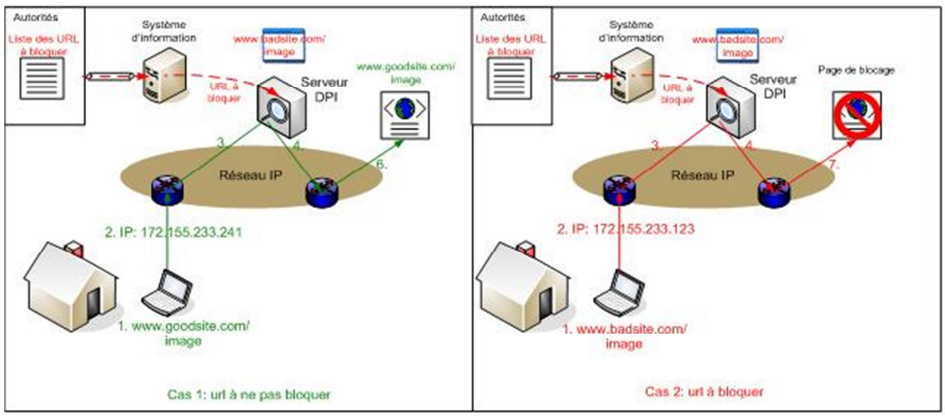


Figure 7 : principe de fonctionnement du blocage par inspection de contenu (Marpij)

Lors de son étude sur le filtrage mis en place en Chine [CLAYTON1], Richard Clayton a démontré que les pare-feux chinois injectent des paquets RST dans le but de clore les connexions interdites en cours et ce pendant un temps de 20 minutes à 1 heure, rendant toute nouvelle tentative de connexion infructueuse. Cependant, il a été possible de prouver que cette technique était contournable, suite à une modification du comportement des pare-feux de destination, à la réception de ces paquets. Malheureusement, les internautes chinois ne peuvent abuser de cette technique, tous leurs faits et gestes étant enregistrés puis analysés ultérieurement. Cette étude prouve tout de même que ce filtrage n'est pas infaillible !

Dans un document à l'attention des FAI, le cabinet Network Strategy Partners présente les pré-requis matériels et logiciels à la mise en place de la solution DPI au sein d'une infrastructure. Les switchs de niveaux 2 et 3 ne sont pas considérés comme performants pour répondre à des problématiques de filtrage poussées. Il est alors recommandé d'utiliser des switchs, avec une analyse de niveau 7, c'est-à-dire du 1er au dernier bit transmis. De plus, il est recommandé d'installer une solution de « DPI avancée » afin d'avoir un seul outil pour gérer les différents filtres à utiliser [NSP].

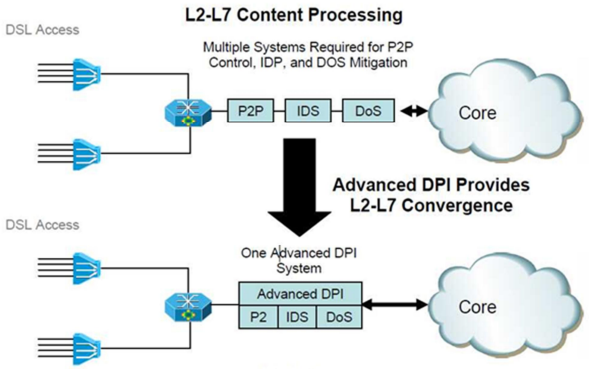


Figure 8 : Convergence using advanced DPI [NSP]

Cette solution technique présente néanmoins des impacts non négligeables, aussi bien pour les FAI que pour leurs clients.

4.4.2 Impacts et effets de bord

La technique de blocage par inspection d'URL agit au niveau d'un point unique du réseau qui concentre tout le trafic et qui refuse l'accès aux contenus interdits. Elle impose pour l'opérateur d'acheminer tout son trafic vers un point unique avant de le router vers sa destination. Cela crée un goulot d'étranglement et limite fortement la fluidité du trafic. Pour y remédier, un opérateur peut maintenir son architecture réseau inchangée mais devra disposer au niveau de chaque sortie de réseau un serveur DPI pour analyser tous les flux entrants et sortants.

Lors d'une interview télévisée, Benoit Bechetoille, PDG de la société Qosmos, évoque les problèmes liés à la diffusion de la technologie DPI dans le monde. Tout d'abord, il précise que la France est un des premiers exportateurs de DPI. Le marché est organisé autour d'intégrateurs plus ou moins scrupuleux ou regardant sur l'utilisation qui sera faite de leur solution. Il insiste particulièrement sur la vente d'outils de DPI faite à certains États, en échange d'accords de collaboration entre services de surveillance et de défense : « Quand la France vend ces outils, qu'elle sait être, dans les mains de certains, des armes, elle obtient régulièrement des accords en matière de renseignement. Les pays acheteurs surveillent donc leur population mais s'engagent à fournir à la France des informations en matière -par exemple- de lutte anti-terroriste. Tout n'est pas blanc, tout n'est pas noir ». Les outils de Deep Packet Inspection sont fort utiles pour de nombreuses autres applications que de la censure. Elles font aujourd'hui partie du paysage pour n'importe quel fournisseur d'accès à Internet ou opérateur mobile. Elles couvrent un champ d'une vingtaine d'utilisations possibles, dont beaucoup parfaitement utiles et éthiques. C'est aussi ce large éventail de possibilités qui d'après lui peut permettre de rapidement glisser vers des dérives : atteintes à la neutralité des réseaux, distorsion concurrentielle, surveillance et exploitation des données personnelles par des tiers non mandatés… [BECHETOILLE]

Les solutions de filtrage de ce type peuvent cependant être contournées facilement par l'utilisation de connexion sécurisée de type « https », de serveurs proxy anonymisants de type « TOR » [MISC-TOR]. L'adoption de la loi Hadopi en France a également relancé les « newsgroups », dont la structure distribuée rend impossible une surveillance efficace [MISC-HADOPI].

Bien qu'en apparence efficace, cette technique reste contournable et surtout nécessite des investissements disproportionnés par rapport au gain d'efficacité qu'elle peut apporter. Un seul

opérateur dans les sept pays de notre échantillon a mis en place un blocage par inspection d'URL, qu'il est en train de migrer vers une solution hybride.

4.5 Le filtrage hybride

Le blocage hybride combine plusieurs techniques pour répondre aux contraintes de sur-blocage que peuvent provoquer les techniques de blocage IP et DNS, et aux contraintes de coûts qu'engendrerait un blocage de type DPI. En effet, le blocage hybride est la combinaison du blocage BGP et du blocage par inspection d'URL. Le blocage hybride est mis en œuvre dans plusieurs réseaux européens, au Royaume Uni, en Suède et à Monaco.

4.5.1 Principe de fonctionnement et mise en œuvre technique

Cette technique repose sur le principe de communication par une autorité nationale d'une liste noire d'URL répertoriant les sites aux contenus illégaux. Une fois la liste chargée dans le système de blocage, ce dernier opère une résolution DNS permettant de retrouver les adresses IP des hôtes où sont hébergées les URL à bloquer. La liste d'adresses IP est ensuite injectée dans un routeur BGP, qui annonce les routes correspondantes et attire vers lui tous les flux vers ces adresses IP. Les flux IP sont ensuite routés vers un serveur DPI voisin qui opère une inspection d'URL pour vérifier la correspondance avec la liste noire. En cas de correspondance, les flux sont rejetés ou routés vers la page de blocage hébergée sur un autre serveur. Dans le cas contraire, ils sont routés vers leur destination finale à travers un lien de transit IP dédié, ce qui évite de remettre dans le réseau des paquets dont les adresses IP sont attirés par le routeur BGP, et ainsi créer des boucles à l'infini.

Il est également possible d'introduire dans le système une liste blanche, qui contient la liste d'URL à ne pas filtrer, quand bien même elles se trouveraient dans la liste noire. Ce mécanisme permet de préserver d'un blocage par erreur les URL hébergées sur les serveurs de l'opérateur. Il est également possible d'introduire en plus de la liste des autorités nationales celles d'autres pays, toujours dans un mode sécurisé et assurant la confidentialité nécessaire à un tel dispositif.

Ainsi, deux niveaux de blocage sont effectués, un premier blocage sur adresse IP permet de ne sélectionner que la partie suspecte du trafic. Un deuxième blocage plus approfondi au niveau des URL est opéré par un serveur DPI. Ce système en cascade, permet donc de réduire fortement le volume de données à traiter, réduisant ainsi la charge globale du système et donc son coût de mise en œuvre. La mise en place dans cette solution d'un serveur DPI (certes, bridé à l'inspection des URL) peut théoriquement étendre l'inspection à un niveau plus approfondi allant

même jusqu'à la reconnaissance d'images. Seulement, la charge de traitement serait telle que le coût de la solution deviendrait prohibitif.

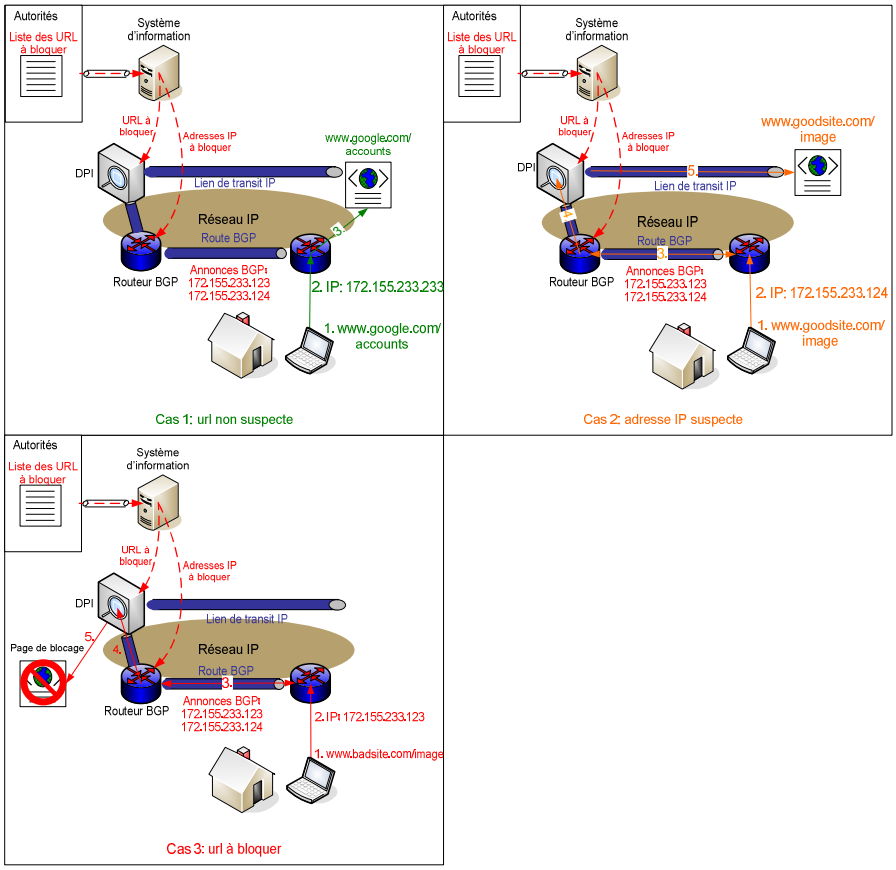


Figure 9 : principe de fonctionnement du blocage hybride (Marpij)

Au Royaume Uni, les données filtrées à ce jour n'excèdent pas le millier d'URL, [DEIBERT-AC] ce qui implique un volume comparable de routes à reconfigurer au niveau des routeurs BGP. Elle présente un coût plus élevé que les solutions IP, BGP et DNS, qui est fonction de la taille de la liste noire ; plus la liste s'allonge, et plus il faut accroître la capacité de traitement du DPI.

4.5.2 Impacts et effets de bord

Le blocage hybride subit le cumul des effets de bord du blocage DPI final.

Le trafic redirigé vers la plateforme de blocage et en particulier sur l'équipement DPI, doit pouvoir être absorbé à tout instant, ce qui pose un problème de dimensionnement. Il en est de même de la liaison de transit IP à la sortie du DPI pour évacuer le trafic qui après inspection d'URL s'avère normal. Dans le cas où des sites à fort trafic (Google, Youtube, Facebook,

Wikipedia, ...) se retrouvent dans la liste noire, le système peut se trouver très vite surchargé et induire une dégradation importante de service pour les utilisateurs.

Cela peut être acceptable dans un réseau FAI de petite taille comme c'est le cas au Royaume-Uni (100 FAI), en Australie (200 FAI). En revanche, cela s'avère impossible dans le cas des FAI français. En effet, leurs réseaux sont très éclatés géographiquement et hiérarchiquement, et reposent sur un grand nombre de routeurs qui se répartissent la charge. Concentrer le trafic de blocage au niveau d'un point unique du réseau serait donc incompatible avec l'architecture réseau des FAI français et ferait porter de gros risques en cas de congestion de la plateforme de blocage hybride [DEIBERT-AC].

Des précédents sont déjà arrivés, comme le blocage par erreur du site Wikipédia au Royaume-Uni. Le 5 décembre 2008, L'IWF inscrit par erreur la page de l'album « Virgin Killer » du groupe Scorpions dans sa liste noire, la considérant comme du contenu pédopornographique. Elle diffuse ensuite la liste noire aux FAI du Royaume-Uni et la page se retrouve bloquée. De plus, les FAI utilisant un blocage hybride n'ont bloqué que la page en question et laissé accessibles les autres, tout en les faisant transiter par leurs serveurs de blocage. Observant que les requêtes des internautes provenaient de la même adresse IP (celle des serveurs de blocage hybride), Wikipédia s'est cru attaqué et a répondu en filtrant ces adresses IP, rendant ainsi le site inaccessible au Royaume-Uni jusqu'au 8 décembre 2008.

On peut également imaginer la situation suivante dans le futur, en cas de généralisation du blocage hybride où plusieurs opérateurs utilisent ce mécanisme au niveau de leurs réseaux respectifs et s'échangent du trafic dans le cadre d'accords de peering. Les inspections successives introduiraient une latence et une probabilité importante de perte de paquets liée à la multiplication du risque d'erreurs dans les listes utilisées.

Un surdimensionnement important de la solution, une mise à jour fréquente des listes (au moins une fois par jour comme au Royaume Uni), des procédures de surveillance de trafic alertant les opérationnels en cas de surcharge de la plateforme, et des procédures de débrayage du système lorsque les limites statiques sont atteintes, sont quelques précautions minimales à prendre par les FAI qui souhaitent déployer ce type de blocage.

Enfin, une étude universitaire [CLAYTON2] a montré que les systèmes de filtrage hybride en production au Royaume-Uni (CleanFeed, WebMinder) appliquent un traitement particulier aux communications électroniques des utilisateurs. L'auteur a établi qu'il était possible pour un

abonné anglais d'obtenir anonymement en 24h00 la liste de tous les sites russes filtrés à la demande de la police anglaise. Cet évènement met en avant le fort risque de voir cette liste publiée au niveau mondiale dans le but de contourner ou de préparer une attaque informatique.

Les techniques de filtrage des flux Internet évoquées permettent donc d'assurer un contrôle relatif des flux afin de répondre à des exigences de sécurité réglementaires ou alors d'optimisation du trafic sur les réseaux des opérateurs. La problématique rencontrée sur ce sujet est assez similaire à celle de la gestion des flux de messagerie électronique et par conséquent de la gestion du spam, dans les réseaux opérateurs et au niveau des entreprises.

5 Les techniques de filtrage des flux de messagerie

La messagerie est un des services les plus utilisés sur Internet et sur les réseaux d'entreprise. Elle permet une communication à la fois rapide, asynchrone et bon marché, en complément du téléphone, du courrier postal et du fax. C'est également un moyen simple et universel d'échange de fichiers. Ce service, devenu incontournable, comporte cependant de nombreux risques en termes de sécurité informatique. L'ouverture de ce service vers Internet nécessite un filtrage efficace pour se prémunir des nombreux risques inhérents au protocole de messagerie SMTP/MIME : virus, vers, contenus actifs, vulnérabilités des clients de messagerie et des serveurs, chevaux de Troie, usurpation d'identité, relais, spam mais aussi les publicités.

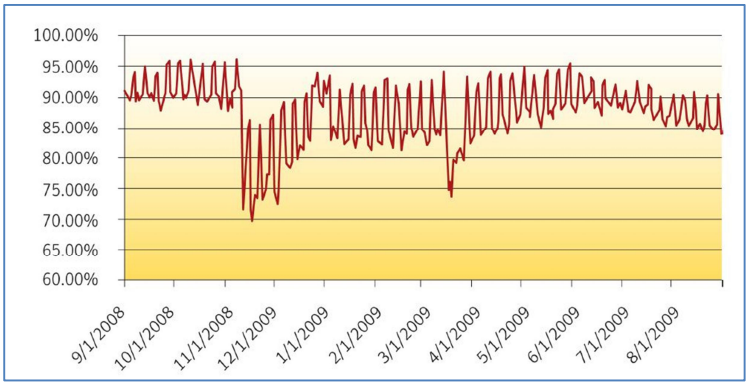


Figure 10 : Pourcentage de spam détectés de 2008 à 2009 (SYMANTEC)

Différentes méthodes ont été mises en place pour parvenir à filtrer les messages correctement et ainsi sécuriser les flux Internet de courriers électroniques.

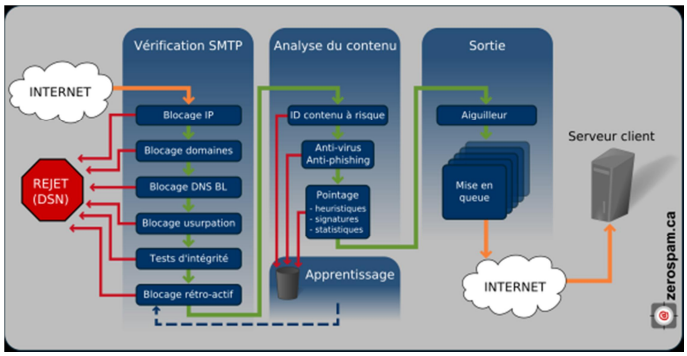


Figure 11 : Mode de filtrage mis en place chez Zerospam (ZEROSPAM)

5.1 Le filtrage d'enveloppe

Ce type de filtrage s'applique uniquement à l'en-tête du message, qui contient souvent assez d'informations pour pouvoir distinguer un pourriel. Il ne s'attache pas au contenu du courriel.

Cette technique présente l'avantage de pouvoir bloquer les courriels avant même que leur corps ne soit envoyé, ce qui diminue grandement le trafic sur la passerelle SMTP (puisque le corps du message est envoyé après que l'en-tête ait été reçue et acceptée). De plus, le taux de faux positifs dans ce type de filtrage est quasiment nul : lorsqu'un filtre d'enveloppe a identifié un courriel comme du pourriel, il se trompe rarement.

5.1.1 Filtrage par serveur expéditeur, listes et RBL

Ce type de filtrage permet de bannir des adresses courriel, des domaines, ou des serveurs. Ainsi, tout message provenant d'éléments de la liste noire sera bloqué par le système anti-pourriels. Ces éléments de liste sont très souvent définis par un administrateur système qui, par expérience, est en mesure de déterminer les sources les plus communes de pourriel. Il est également possible de s'appuyer sur des Realtime Blackhole Lists (RBL), qui sont des listes noires hébergées sur des serveurs et mises à jour en temps réel. Les solutions qui s'appuient sur ces listes les consultent régulièrement [GALLOT].

La mise en place d'un système de « liste blanche » permet à l'inverse d'autoriser automatiquement le délivrement des messages concernés, qui ne seront donc jamais considérés comme des pourriels. Il est possible de se construire une liste blanche rapidement, en considérant que tous les messages envoyés par les utilisateurs de votre organisation ont tous un destinataire réel. Cette technique peut facilement être ajoutée en complément d'autre type de filtrage [GRAHAM1].

Cependant, le risque de faux positifs est très élevé avec ce type de solutions, c'est pourquoi le temps de gestion à y consacrer est très important. Paul Graham conseille fortement d'utiliser des systèmes à base de filtre pour améliorer le filtrage et non des listes [GRAHAM2]

Cette technique a pour caractéristique d'être très souple, car elle permet de ne pas se limiter aux pourriels seulement : elle peut également bloquer des sources de courriel légitime, si l'administrateur système les considère comme nuisible. Évidemment, ce type de filtrage est hautement subjectif et dépend du bon vouloir et de l'assiduité de la personne créant la liste.

5.1.2 Le filtrage par passerelle SMTP

Les différents champs utilisés par les protocoles SMTP et MIME permettent un filtrage simple suivant divers critères. Un des filtrages les plus importants consiste à interdire tout message provenant de l'extérieur avec une adresse émetteur correspondant au domaine interne, afin d'éviter l'usurpation d'identité d'un utilisateur local. Ce filtrage est souvent dénommé « antispoofing ». De même, tout message entrant doit avoir une adresse destinataire correspondant au domaine interne, afin d'éviter les problèmes de relais. Pour les messages sortants, il est nécessaire de vérifier que l'émetteur appartient bien au domaine local, et que le destinataire n'en fait pas partie.

Enfin, il est très important de traiter avec attention le problème des bounces. Ce sont des messages automatisés envoyés aux expéditeurs pour leur notifier que la livraison n'a pu être effectuée. La RFC 821 qui définit le protocole SMTP décrit les différents cas dans lesquels sont générés des bounces [RFC821]. Or, en environnement d'entreprise, il est courant d'utiliser plusieurs serveurs de mails pour traiter le courrier. Dans ce cas, un serveur sert le plus souvent de passerelle : il accepte tous les mails en provenance d'Internet et les envoie ensuite soit vers un serveur interne, soit vers un antivirus ou un anti spam. Cette passerelle est rarement configurée pour vérifier l'existence des utilisateurs : elle est là pour accepter tous les mails à destination du domaine et les router. A charge pour les serveurs internes d'effectuer la vérification. Cette configuration amène deux problèmes. Il est possible d'usurper l'identité du destinataire du bounce avec un faux reply-to, ou même un faux émetteur. Le destinataire reçoit alors un Non Delivery Notification (NDN) pour un message qu'il n'a jamais reçu. Le NDN contenant une copie du mail original, l'attaquant peut y joindre aisément un virus, trojan. Enfin, si le serveur envoie un bounce individuellement à chaque destinataire invalide, on peut l'utiliser pour attaquer une adresse mail : si l'attaquant envoie un seul mail à 100 destinataires invalides avec un faux reply-to, le reply-to usurpé recevra en retour une centaine de bounces [ALTOSPAM].

La passerelle SMTP est donc un outil complémentaire de la solution antivirale de l'entreprise qui permet d'accroître la sécurité des échanges en analysant les messages entrant et sortant avant qu'ils ne soient transmis sur le réseau interne ou Internet. De plus, cette technique limite l'engorgement des réseaux par des messages non désirés.

5.2 Le filtrage de contenu

Les filtres de contenu analysent le contenu des messages et détectent les pourriels qui ont réussi à passer à travers le filtre d'enveloppe. Le filtrage de contenu peut se développer en plusieurs couches. Par exemple, le filtre peut faire appel à un logiciel antivirus, à un désarchiveur pour analyser les fichiers archivés s'il y a lieu, à un analyseur bayésien et ainsi de suite. SpamAssassin est une solution open source bien connue des administrateurs et déployée dans de nombreuses organisations afin de filtrer les courriels.

5.2.1 Le filtrage heuristique

Le filtrage heuristique regroupe toutes les techniques qui analysent différentes caractéristiques du message. Ainsi, avant qu'une décision ne soit rendue sur la nature d'un message, plusieurs caractéristiques seront examinées et participent à la classification du message.

Le contenu du message est testé à l'aide de différentes règles. La technique analyse et note la présence de forme comme par exemple l'objet du message tout en MAJUSCULE, la proportion de code html, d'images par rapport au reste du message, si l'objet est vide ou non, …. Des points sont affectés après l'exécution de chaque règle. La somme de tous les points est comparée à un seuil défini par l'administrateur du système. A la charge de celui-ci d'affiner ce seuil de façon à déterminer le meilleur équilibre entre le nombre de faux positifs et de faux négatifs [GALLOT].

L'utilisation d'un filtrage heuristique nécessite une maintenance assez importante, car en général les spammeurs s'adaptent aux règles et ajoutent de "nouvelles règles". Ainsi, la mise à jour de ces règles dans ce système de filtrage est permanente.

5.2.2 Le filtrage Baéysiens

Le filtrage bayésien du spam, du mathématicien Thomas Bayes, est un système basé sur l'analyse d'une grande quantité de pourriels et courriels pour déterminer si un courriel est légitime ou non. Afin de bien fonctionner, l'ensemble de *spam* et de *ham* (courriels légitimes) doit contenir idéalement plusieurs milliers de messages.

Le message à identifier est découpé en morceaux qui sont comparés à tout l'ensemble de courriels (pourriels ou non), pour déterminer la fréquence des différents morceaux dans les deux

catégories. Une formule statistique est utilisée afin de calculer la probabilité que le message soit un pourriel ou non. Lorsque la probabilité est suffisamment élevée, le système bayésien catégorise le message comme du pourriel. Sinon, il le laisse passer. Le seuil de probabilité est à définir par l'administrateur système et doit être ajusté au fur et à mesure de l'apprentissage du filtre.

Paul Graham présente cette technique comme la meilleure à mettre en place, car elle permet de « voir » ce qui est mesuré, contrairement aux filtres définissant des scores pour prendre la décision, car personne ne sait exactement ce que le score signifie. Il cite en exemple que le mot « sex » a 97% de chance d'être contenu dans un spam et le mot « sexy » a 99%. La combinaison de ces deux mots dans le même message permet de spécifier que celui-ci est un spam à 99.97%. Dans cette situation, il s'interroge sur la façon de donner une note à un message contenant ce même mot « sex ». Comme il l'annonce, personne ne sait que la note affectée est celle-ci parce que ce mot est contenu dans le corps du message. Le risque d'erreur est donc beaucoup plus grand d'après lui [GRAHAM1].

Cette méthode de filtrage fiabilise la détection de courriels indésirables car elle tient compte de l'ensemble du message, des probabilités jugées « bonnes » et « mauvaises » pour chaque élément. La langue du message a également peu d'impact à partir du moment où le filtre dispose d'une grande base statistique sur laquelle s'appuyée.

5.2.3 Filtrage par mots-clés

Le filtrage par mots est toujours très utilisé, même si cette technique a été une des premières solutions de détection.

Il s'agit d'un indicateur simple pour la détection des spams. Cette méthode est très limitée car elle se base sur le rejet ou le tri du courrier en fonction de règles de vocabulaire préalablement établies, comme une liste noire des mots interdits. Certains mots-clés revenant souvent dans les pourriels, tels que « sexe », « viagra » ou « money » pourront servir de base pour la constitution de ces règles. De même, on pourra décider de bloquer tous les messages en provenance d'un expéditeur précis, d'un domaine spécifique, voire d'un pays entier. Cette méthode est de moins en moins efficace car les spammers utilisent diverses méthodes de camouflage qui rendent la détection de mots-clés de plus en plus difficile. De plus, elle engendre de fortes probabilités d'erreur et s'avère peu efficace lorsque les polluposteurs maquillent les mots utilisés, comme par exemple « vi@gr@ ». [LAGADEC]

L'utilisation des expressions rationnelles doit permettre de limiter ces erreurs.

5.2.4 Filtrage par expression rationnelle

Une expression rationnelle régulière est un motif que l'on peut appliquer à une chaîne afin de voir si ladite chaîne correspond au motif prédéfini. En utilisant des expressions rationnelles afin de trouver des variations de mots « sensibles », on augmente les chances de découvrir des pourriels. Par exemple, si un polluposteur tente de déjouer un filtre de mots-clés en utilisant le mot « viiaaagraa », l'expression rationnelle /^vi+a+gra+$/i (un « v » suivi d'un ou plusieurs « i » suivi d'un ou plusieurs « a », suivi d'un « g », d'un « r », et de un ou plusieurs « a », sans se soucier de la casse) permet de retrouver le mot. Les expressions rationnelles complexes permettent de détecter des expressions et des déclinaisons beaucoup plus subtiles et sophistiquées.

Cependant, la mise en œuvre de ces expressions s'avère difficile, car il faut pouvoir définir toutes les expressions possibles et recenser tous les mots utilisés dans les courriers indésirables [HASSANE]. De plus, les règles définies peuvent produire des faux-positifs si elles sont mal construites. Ainsi, un habitant de la ville de Scunthorpe se voyait refuser son inscription à un FAI car « scunt » est extrêmement péjoratif en anglais [SET]. Le moteur de recherche Google par exemple filtrait automatiquement le site www. Part**sEx**press.com car il contenait le mot « sex ». Ces deux exemples illustres parfaitement la problématique de mise en œuvre de ces règles.

Les différentes techniques évoquées consistent à analyser les messages afin de déterminer si les courriels sont légitimes ou non. Une autre méthode consiste à utiliser une procédure d'authentification en amont de l'expéditeur, avec la mise en place d'un test de Turing.

5.3 Le filtrage « machine de Turing »

Cette technique, également nommée challenge/réponse, consiste à renvoyer un email de demande d'authentification à l'expéditeur du message afin de s'assurer de son existence physique réelle. Une fois l'authentification de l'expéditeur réussie, son adresse électronique est enregistrée dans une liste blanche et il ne lui sera plus demandé de prouver son identité.

Cette technique connait aujourd'hui un développement important, comme en témoigne le développement de la société « Mail In Black » qui base sa lutte contre le spam sur le test de Turing. La plupart des tests se base sur la recopie d'un code dont l'écriture est déformée, de

manière à empêcher l'utilisation de logiciels de reconnaissance de caractères. Il existe des challenges dits « classiques », « cognitifs » ou par communauté à handicap :

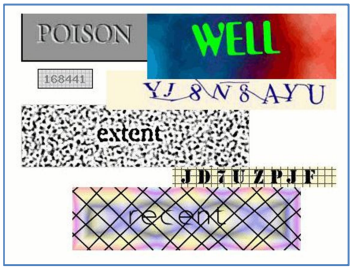


Figure 12 : Challenge classique (MAILINBLACK)

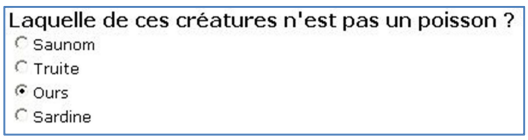


Figure 13 : Challenge cognitif (MAILINBLACK)

Figure 14 : Challenge pour les communautés à handicap (MAILINBLACK)

Cependant, utilisée seule cette technologie comporte de nombreux inconvénients. En effet, elle reporte le travail de filtrage sur l'expéditeur du message, augmente le nombre de messages non sollicités, mais surtout peut générer beaucoup de faux-positifs. De plus, elle doit impérativement prendre en compte certains cas spécifiques, comme les risques de bouclage entre deux solutions effectuant des tests de Turing pour valider les expéditeurs.

Cette solution, intégrée à d'autres technologies, peut être utilisée en fin d'une chaîne d'analyses et permet de libérer des faux-positifs non résolus par les solutions précédentes.

5.4 Les pièces jointes, une faille de sécurité

La messagerie électronique est aussi très utilisée pour échanger des documents entre utilisateurs. Or, ces pièces jointes peuvent contenir des programmes malveillants destinés à exploiter les failles de sécurité du système ou bien voler des informations confidentielles.

Le format « MIME » est un standard conçu pour support des textes en différents codage de caractères, autres que le traditionnel ASCII, des contenus non textuels ou multiples. Le format de base est défini dans la RFC2822 et 822. Celui-ci spécifie le format des en-têtes et du corps des courriels contenant du texte, ainsi que les règles d'en-têtes générales comme "To:", "Subject:",

"From:" ou "Date:". On y trouve également les champs utilisés pour spécifier les noms et type de fichiers transférés, comme présenté ci-dessous :

```
Content-Type: application/octet-stream; name="fichier.xyz"
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="fichier.xyz"
```

Le filtrage par extension peut permettre de reconnaitre certaines pièces jointes, jugées à risque, comme les exécutables et les scripts Windows comportant des extensions connues : EXE, COM, BAT, CMD, SCR, VBS, JS, VBE, JSE... Cependant, les informations contenues dans ces champs sont purement déclaratives et ne permettent pas de s'assurer que le fichier transmis est réellement celui nommé. Il est ainsi possible d'envoyer des fichiers en utilisant des extensions peu connues ou en modifiant celle d'origine par une autre. Les documents Microsoft Office sont particulièrement utilisés pour ce type d'attaque.

Enfin, il faut tenir compte des failles de sécurité non découvertes à ce jour dans des documents fréquemment utilisés, comme les fichiers pdf. C'est ainsi qu'en décembre 2010, 150 ordinateurs du ministère des finances en France a été piraté [MANENTI]. Un pirate a exploité une faille de sécurité des fichiers pdf pour y introduire un cheval de Troie. Celui-ci s'est propagé sur le réseau interne après l'ouverture du fichier afin de dérober des informations confidentielles.

La problématique des pièces jointes est importante car c'est un moyen d'échange d'information de plus en plus utilisé sur Internet. Les spammers ont bien compris cet enjeu et cherchent maintenant à déjouer les filtrages classiques en utilisant des images jointes à des messages électroniques conformes.

5.5 Le spam image

Afin de contourner au maximum les solutions antispams, les spammers essaient de diffuser leurs messages aux travers d'images, insérées en pièces jointes dans les messages. Le volume de ces pièces peut varier et augmenter de façon significative le délai de livraison des courriels légitimes. La société Symantec avait à ce sujet constaté ce phénomène dès 2009.

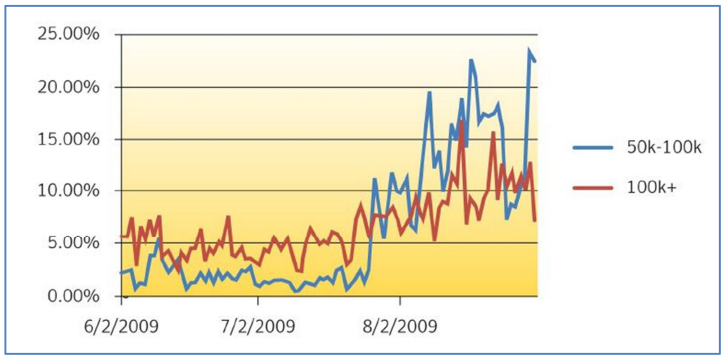


Figure 15 Volume des images jointes aux spams (SYMATENC)

La technique de la reconnaissance des caractères OCR est une solution pour essayer de reconnaître les spams dans les images. Cependant, cette solution ne parait pas complètement fiable dans des environnements de production.

Le plugin FuzzyOCR peut être intégré à la solution Spam Assassin pour traiter ce type de message. Une base de connaissance est établie à partir des spam-images connus et est utilisée pour déterminer si un message est « presque » équivalent ou non aux éléments de la base, mais le niveau de performance reste faible et le temps processeur requis pour le traitement de ces analyses est significatif.

Le spam image est donc particulièrement difficile à traiter car il faut analyser de nombreux éléments. L'algorithme « Spam Image Distance » répertorie les images en fonction de leurs nombres de points et leurs similitudes. La variation des couleurs dans un message peut alors être prise en compte dans l'analyse. Le résultat de l'algorithme est un score, c'est-à-dire la distance, qui est comparée à celle des spams-images déjà recensés dans la base de données. Cependant, les spammers ajoutent des altérations dans l'image de départ afin de fausser les analyses, en découpant l'image en sous-images. Celle-ci sera ensuite recomposée dans une page HTML classique. Cette technique peut être contournée en reliant les différents histogrammes obtenus à partir des sous images et en recréant celui de l'image originale afin de l'analyser avec l'algorithme SID.

5.6 Les limites du filtrage des flux de messagerie

Malgré toutes les techniques disponibles pour le filtrage de messagerie, il est toujours très difficile de se protéger de façon complète et sûre contre tous les risques. Chaque technique de filtrage possède des faiblesses qui peuvent être contournées en associant plusieurs techniques de filtrage différentes avant de délivrer les messages aux destinataires [LAGADEC].

Les flux de messagerie doivent être surveillés au quotidien afin de prévenir les attaques potentielles, mais aussi pour rechercher et déployer les nouveaux outils de filtrage mis sur le marché. Le système installé ne doit pas être figé et nécessite une maintenance et une évolutivité importante pour faire face aux évolutions des techniques de piratages. La sécurisation de ces flux peut alors se faire au détriment des utilisateurs auxquels il peut être nécessaire d'imposer des formats d'échanges de fichiers ou des quotas de pièces jointes. Philippe Lagadec démontre la grande difficulté à pouvoir différencier des fichiers HTML et XML en fonction des syntaxes utilisées. Il insiste également sur le problème de la détection des scripts dans les messages HTML et des macros dans les documents échangés. Enfin, il met en garde contre l'utilisation des webmails, car le trafic n'est pas filtré par les solutions de filtrage de messagerie. Il est alors possible d'enregistrer facilement des fichiers corrompus sur les réseaux internes des entreprises. Il est important de mettre en place des systèmes de filtrage des flux Internet sur les protocoles http, https et ftp afin de sécuriser les échanges de fichiers par ces webmails. Enfin, la mise en place de tous ces moyens de contrôles n'assure pas une détection infaillible des spams et autres programmes malveillants. Des courriers légitimes peuvent être placés en quarantaine sans raison. Les utilisateurs finaux doivent alors pouvoir assurer la gestion des faux-positifs au travers d'interfaces dédiées et faciles à utiliser.

La sécurisation des flux de messagerie au CH de Montbert est un aspect important de la mise en place de la politique de sécurité de l'établissement. En effet, de nombreux messages sont réceptionnés tous les jours, légitimes ou non, mais la solution en place est peu maintenue et nécessite donc une remise en cause globale.

6 Le filtrage des flux Internet au CH de Montbert

Le Centre Hospitalier de Montbert est équipé des applications de la société Trend Micro, chargés d'assurer la sécurisation des flux Internet. L'association entre l'antivirus et la passerelle Internet a permis jusqu'à présent de sécuriser un minimum les échanges et communications des utilisateurs. Cependant, l'évolution des usages et des technologies ne permet plus à l'établissement de garantir sa sécurité face à un environnement en mutation permanente.

6.1 Description de l'architecture existante

Les flux Internet de l'établissement transitent tous par un serveur dédié, dénommé « serveur proxy ». Celui-ci est placé dans une zone DMZ, accessible depuis des réseaux extérieurs à celui de l'hôpital. Ce serveur est chargé d'assurer le filtrage et la sécurisation des flux Internet, en

s'appuyant sur la solution de l'éditeur Trend Micro Interscan Web Security Server (IWSS) et les solutions libres Squid et Squidguard (Annexe C).

Le serveur « squid » est un serveur mandataire qui est chargé de transférer les requêtes entre les clients et les serveurs de destinations. Il apporte plusieurs services : la gestion d'une mémoire cache pour accélérer l'affichage sur les postes des utilisateurs quand une page web est souvent demandée, la journalisation des requêtes, la sécurité du réseau local et un début de filtrage des flux Internet. Le chargement des données est accéléré et la bande passante nécessaire est optimisée en utilisant le cache disponible. Les protocoles ftp, http et https peuvent être captés et cette analyse, associée à des règles d'utilisation, permet d'élaborer un filtrage de flux Internet. Ce type de serveur est très utilisé [SQUID].

Le serveur « Squidguard » est un applicatif complémentaire à « squid », qui assure le filtrage, la redirection et le contrôle d'accès. Il est utilisé pour la gestion d'un système de listes blanches et noires, mais aussi pour la classification des sites Internet en catégories. Il est alors possible de définir quelles sont les adresses autorisées à la consultation de celles à interdire, de façon automatique ou après une authentification de l'utilisateur [SQUIDGUARD].

Enfin, la solution IWSS, installée sur le même serveur assure la sécurisation des flux Internet de l'ensemble de l'établissement. Cette solution logicielle permet de lutter contre la combinaison de menaces et de bloquer l'accès aux sites web malveillants, d'intercepter les spywares et autres menaces de Internet et de faciliter la gestion au travers d'une console unique. Cette solution logicielle essaie de limiter les risques de téléchargements de virus ou de spywares lors de la navigation des utilisateurs.

L'architecture de sécurisation des flux Internet mise en place en 2004 ne permet pas de répondre aux nouvelles demandes des utilisateurs, ni aux demandes réglementaires, comme la problématique de la durée de conservation des traces. L'utilisation d'un serveur « proxy » a également limité les fonctionnalités natives de IWSS 3.1.

6.2 La méthodologie mise en œuvre

Le CH de Montbert est équipé d'une infrastructure virtuelle de type VMware. Cette plateforme est utilisée comme environnement de production avec un « cluster serveurs » et « cluster clients », mais aussi à des fins de qualifications d'applications. En effet, il est facile de mettre en place des machines virtuelles de tests qui hébergeront les différents produits. Ces machines sont regroupées dans un « pool de ressources » sur le « cluster serveur »ce qui facilite

la gestion des ressources mémoires et processeurs, afin de ne pas impacter l'environnement de production.

Du point de vue architecture réseau, la mise en place d'une nouvelle solution de ce type nécessite la configuration de nouvelles règles de transports au niveau du pare-feu de l'établissement, pour ne pas modifier la configuration de production. J'ai alors autorisé les transferts de flux entre quatre zones. Dans un premier temps, j'ai routé les flux du réseau interne vers la passerelle IWSVA et de la passerelle vers le réseau Internet afin d'autoriser la navigation vers Internet. Puis j'ai poursuivi pour les flux du réseau Internet vers la passerelle et de la passerelle vers le réseau interne afin d'autoriser le chargement des pages web consultées.

Un annuaire Active Directory est déployé, avec des comptes utilisateurs nominatifs et partagés, regroupés dans des groupes d'utilisateurs auxquels sont affectés des droits d'accès spécifiques. Des stratégies ordinateurs et utilisateurs sont déployées au travers de « Group Policy Object » (GPO), notamment pour configurer le script de connexion automatique de Internet explorer. Ce script, appelé « proxy.pac » permet de diriger les requêtes des utilisateurs en fonction de leurs destinations (sur le réseau internet ou bien vers Internet). Dans le cadre de la mise en œuvre des solutions tests, j'ai créé un autre script de connexion qui a été déployé par GPO, pour rediriger les flux Internet vers les nouvelles passerelles de sécurisation. Cette technique permet de cibler des groupes d'utilisateurs afin de ne pas basculer l'ensemble de l'établissement sur l'environnement de test.

Enfin, du point de vue fonctionnel, la démarche mise en œuvre est constituée de trois phases pour chacune des trois solutions testées. La première consiste à éprouver la solution sur un seul poste client, en l'occurrence mon poste du service informatique, pour procéder aux tests et à la vérification de bon fonctionnement de la solution. Cette première étape validée, la seconde consiste à rediriger les connexions de quelques utilisateurs vers cette nouvelle plateforme pour prendre en compte les éléments non encore intégrés. Le dimensionnement de la solution est vérifié ainsi que les phases de montée en charge. Enfin, la dernière étape consiste à rediriger l'intégralité des flux Internet vers cette nouvelle passerelle et ainsi constater l'efficacité de la nouvelle solution, des outils d'analyse, de la traçabilité et des performances.

La charte informatique de l'établissement ne spécifie pas l'existence de filtrage des flux Internet et de messagerie à ce jour, ni de l'enregistrement des traces et de leur conservation pendant un an. En conséquence et en accord avec la direction, les tests effectués seront d'abord fait avec un niveau d'analyse identique à celui existant à ce jour. Afin de pouvoir tester toutes les

fonctionnalités des solutions choisies, une analyse plus poussée pourra être effectuée sur certains groupes d'utilisateurs, après les avoir informés de l'existence de ces tests. Cet aspect institutionnel sera absolument à prendre en compte dans le cadre du déploiement de la solution finale. En effet, il sera peut-être nécessaire de procéder à la révision de la charte informatique actuellement en vigueur et de la communiquer à tous les personnels de l'établissement.

La validation des moyens techniques, fonctionnels et institutionnels permet de débuter les phases de tests. Afin de déterminer la solution la plus adaptée au CH de Montbert, j'ai sélectionné trois solutions majeures du marché, reconnues en France et également déployées par d'autres Centres Hospitaliers.

6.3 Comparatifs de solutions du marché

6.3.1 La solution Trend Micro

Trend Micro Incorporated est un leader mondial dans le domaine des logiciels et services de protection antivirus pour réseaux et de sécurité de contenu Internet. Fondée en 1988, Trend Micro est une société pionnière dans les domaines de gestion de contenu sécurisé et de gestion des menaces, des postes de travail au serveur réseau et à la passerelle Internet. La société poursuit aujourd'hui son développement en proposant de nouveaux services tout en consolidant les produits qui ont fait sa réputation.

J'ai évalué les deux produits Trend Micro : filtrage et rapports. Le produit « InterScan Web Security Virtual Appliance » (IWSVA) est une passerelle Internet chargée de filtrer les flux Internet entrants et sortants. Puis, le produit « Advanced Reporting Management » (ARM) est un outil d'aide à la génération de rapports complémentaires à l'utilisation de la passerelle.

6.3.1.1 Architecture cible et licences logicielles évaluées

Les clés de licences d'évaluation fournies par la société Trend Micro sont de plusieurs types et permettent d'évaluer l'intégralité des produits afin de mieux définir les besoins.

Trend Micro propose plusieurs mode d'installations possibles afin de s'adapter aux infrastructures de leurs clients.

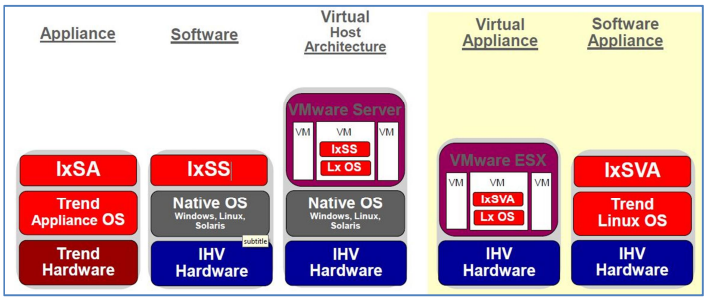


Figure 16 : Méthode d'installation des solutions Trend Micro (Trend Micro)

Une infrastructure virtuelle de type VMware étant en place sur le CH de Montbert, j'ai déployé la solution IWSVA en mode « Virtual Appliance », afin de disposer de toutes les ressources matérielles et logicielles disponibles (Annexe D).

La plateforme de filtrage des flux Internet nécessite l'activation de trois types de licences différents pour activer toutes les fonctionnalités du produit. La première licence concerne l'activation du produit IWSVA, qui est le produit principal sont ajoutés des modules. Ceux-ci sont chargés de bloquer les menaces venant du Web avant leur entrée sur le réseau interne de l'établissement. L'analyse des programmes malveillants, l'évaluation de la réputation des sites Web en temps réels et le filtrage d'URL doivent permettre d'assurer la sécurité des flux Internet. L'objectif est de renforcer la protection au niveau de la passerelle et ainsi de diminuer les risques et la gestion de la sécurité sur les terminaux des utilisateurs. Un antivirus et un antispyware analysent en temps réel le trafic Internet et le stoppe quand un danger est détecté. La seconde licence active le module « URL Filtering » de la passerelle. Celui-ci assure le filtrage des flux HTTP, HTTPS et FTP, entrants et sortants, en s'appuyant sur des stratégies personnalisables et prédéfinies par les administrateurs. Enfin, la troisième licence est utilisée pour renforcer la sécurisation des flux susceptibles de contenir des codes malveillants au travers d'applet Java ou de scripts ActiveX en bloquant les téléchargements de ces fichiers.

Les informations enregistrées par la passerelle Internet sont centralisées par la solution « Advanced Reporting and Management ». Cette architecture permet de disposer d'un aperçu instantané de l'activité Internet de l'établissement, tout en proposant des outils de restauration pour résoudre rapidement des problèmes d'interruptions de service sur un ou plusieurs serveurs IWSVA.

6.3.1.2 Installation des solutions « IWSVA » et « ARM »

L'installation des passerelles IWSVA et ARM ne nécessite pas des connaissances particulières et complexes des produits Trend Micro. En effet, des images systèmes sont

disponibles au téléchargement et préconfigurées par l'éditeur. Les documentations de dimensionnement, d'installation et d'administration sont disponibles et très complètes directement sur la plateforme de téléchargements de Trend Micro [TMIWSVA1].

Le système d'exploitation sur lequel s'appuient les deux solutions est un système linux sous licence GNU/Linux, CentOS. Cette version de linux est principalement destinée aux serveurs web. Elle est déployée à ce jour sur 30% de ce type de serveurs. Les paquets utilisés sont identiques à ceux déployés dans la distribution « Red Hat Enterprise Linux », pour laquelle il est obligatoire d'acquérir une licence d'utilisation.

Pour un fonctionnement optimal, les ressources affectées à la machine virtuelle sont conformes à celles conseillées dans les guides de dimensionnement édités par Trend Micro (4 CPU virtuels, 4 Go de mémoire vive et un disque de 20 Go). L'espace disque attribué est dans notre cas limité, mais doit être augmenté pour conserver les traces des connexions. Il est alors nécessaire d'estimer le volume des connexions des utilisateurs et de définir une durée de conservation de ces traces, de 6 mois minimum afin de respecter la réglementation. L'éditeur VMware recommande fortement l'installation des « vmware tools » pour optimiser les aspects graphiques et les mouvements de la souris et la gestion de la mémoire pour ces serveurs. Hors, l'installation de ces outils est bloquée par Trend Micro. Cela n'impacte pas le fonctionnement, car la gestion s'effectue principalement via une interface web.

Enfin, la plateforme IWSVA est déployée dans la zone « DMZ » déjà existante, en frontal du réseau interne de l'établissement pour sécuriser les flux entrants et sortants. La solution ARM est déployée dans le réseau interne, avec les autres serveurs. Les adresses IP, masques de sous réseau, serveurs DNS, NTP et pare-feu sont renseignés pendant la phase d'installation de la solution avec des adresses disponibles. Il convient de choisir lors du déploiement le type d'architecture à mettre en place :

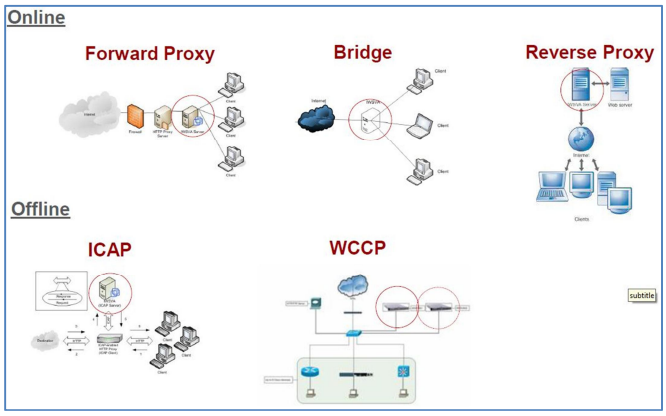


Figure 17 : Architecture de déploiement possible avec IWSVA (Trend Micro)

Chaque architecture répond à des besoins spécifiques. Le choix doit donc se faire en fonction des contraintes et objectifs à atteindre. Une solution IMSS étant déjà déployée en mode « Forward Proxy », les pares-feu et les navigateurs clients configurés. J'ai donc conservé la même architecture pour IWSVA.

La facilité d'installation de ces solutions se retrouve également dans leurs utilisations respectives au quotidien.

6.3.1.3 La configuration de la passerelle « IWSVA »

La passerelle concentre le trafic réseau de l'ensemble des connexions utilisateurs afin de procéder à différentes analyses sur les flux entrants et sortants. Trend Micro a choisi de se concentrer sur les principaux protocoles utilisés sur Internet (http, https et ftp) et propose des outils et compléments logiciels pour sécuriser les communications qui transitent sur ces canaux.

Le filtrage des flux http est le plus important car le plus utilisé par les utilisateurs, sur le port 80. L'analyse s'appuie sur des règles prédéfinies par les administrateurs de la solution. Il est possible de construire des règles avec des exceptions pour des utilisateurs ou groupes d'utilisateurs pour répondre à des contraintes spéciales. La solution s'appuie sur l'annuaire Active Directory de l'établissement pour faciliter la configuration. L'analyse du flux http est divisée en quatre phases. La première consiste à vérifier la réputation du site Internet consulté en s'appuyant sur les bases de données téléchargées depuis la plateforme de Trend Micro. La solution scrute les en-têtes des pages html et leur contenu à la recherche de codes malveillants, de domaine suspects. Si des éléments non conformes sont détectés, la note globale est dégradée et l'accès au site peut-être bloqué. Trend Micro recommande d'autoriser la diffusion de ces informations sur ces plateformes afin de prendre en compte rapidement ce nouveau danger. En complément, un module « anti-pharming » est chargé de vérifier que la page demandée ne sera

pas redirigée vers une destination non prévue initialement. Le module « anti-phishing » doit interdire l'accès aux sites qui tente de soutirer des informations personnelles et confidentielles, comme par exemple de faux sites bancaires.

La seconde phase est l'analyse antivirale des objets qui doivent être téléchargés sur le client pour afficher la page demandée. Ainsi, il est possible d'interdire le téléchargement de fichiers en fonction de leur extension (images, exécutables, vidéos, …). A l'image de la configuration actuelle, j'ai bloqué les fichiers exécutables. La mise en œuvre de cette stratégie a montré que de nombreux fichiers de ce type sont téléchargés quotidiennement sur les ordinateurs de l'établissement, parfois automatiquement ou volontairement. J'ai constaté que la stratégie actuelle ne fonctionne pas et représente une faille de sécurité importante. Du point de vue antivirus, il est possible de scanner tous les fichiers ou les fichiers reconnus potentiellement dangereux. Cette dernière option est activée via le module IntelliScan, car l'analyse de tous les fichiers nécessite des performances élevées de la passerelle. J'ai alors appliqué un traitement spécial aux fichiers volumineux. En effet, l'analyse des fichiers d'un volume trop important n'est pas effectuée car cela ralenti grandement le trafic global. Cette stratégie déporte alors l'analyse antivirale sur le poste client, sur lequel l'antivirus pourra analyser ces fichiers. Cette option est impérativement activée, car elle bloque l'affichage des fichiers pdf dans le navigateur si la taille de celui-ci est trop importante. La décision d'appliquer cette stratégie représente tout de même un risque, à l'image du piratage des ordinateurs du ministère des finances par un cheval de Troie introduit dans un fichier pdf en mars 2011 [LE MONDE 1].

La troisième phase vient en complément des analyses antivirales habituelles et vise à protéger les utilisateurs d'autres types de programmes, comme les malwares ou spywares. En effet, ceux-ci peuvent récupérer et transmettre des informations personnelles à l'insu des utilisateurs, mais aussi provoquer des changements dans les configurations des applications, comme modifier les pages de démarrages des navigateurs, afficher des fenêtres publicitaires non voulues. Trend Micro peut être configuré pour se protéger contre les « spywares, dialers, hacking tools, programmes pour casser les mots de passe, Adware, Joke programs, outils de prise de contrôle à distance ». J'ai mis en œuvre cette option complémentaire afin de visualiser si des programmes de ce type existent.

Enfin, la dernière phase vise à définir quelles sont les actions à réaliser en fonction des résultats des analyses précédentes et des exceptions configurées, pour les fichiers infectés mais « nettoyables », infectés mais « non nettoyables », contenant des macros ou bien des fichiers

protégés par des mots de passes. Les exceptions autorisées portent sur une liste d'URL considérées comme sûres mais aussi sur une liste de fichiers autorisés au téléchargement. Il est ainsi possible d'optimiser les communications vers des serveurs approuvés.

La navigation Internet « classique » est surveillée par la solution IWSVA. Le nombre de services en ligne accessibles aux utilisateurs est en augmentation constante. L'accès à ces services doit alors être sécurisé par un certificat associé au protocole http. On parle alors de connexion https. Jusqu'à présent ces flux sécurisés n'étaient pas soumis aux mêmes analyses que pour les flux non cryptés. Désormais, la nécessité d'augmenter la sécurité sur les réseaux impose de devoir analyser ces flux pour éviter l'intrusion de virus ou tout autre code malveillant. Pour établir une connexion https, il est impératif d'installer un certificat SSL, édité par une autorité de certification, qui assure l'intégrité et le cryptage des données transmises sur les réseaux entre le client et le serveur Web.

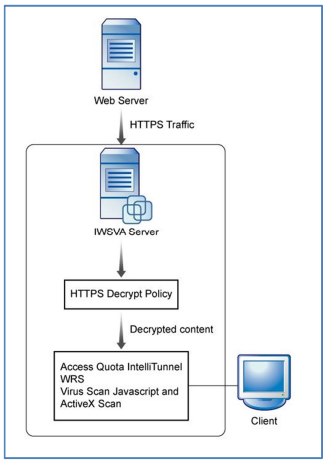


Figure 18 : Décryptage des flux https avec IWSVA (Trend Micro)

Avant de déployer cette stratégie, j'ai identifié les certificats utilisés au sein de l'entreprise, puis je les ai configurés dans la solution. Les connexions utilisant ces certificats seront alors considérées comme valides et ne seront pas soumises aux mêmes analyses que pour des flux non maitrisés. Pour tous les autres flux sécurisés, il faut déterminer ce que l'on souhaite analyser, en fonction de la nature des connexions. Ainsi, Trend Micro a réparti les sites Internet dans sept catégories et laisse la possibilité de créer des catégories personnalisées. Concrètement, l'utilisation de cette fonctionnalité est rendue complexe car les certificats utilisés ne sont pas tous émis par des autorités de confiance, mais sont parfois « auto-signés » par des solutions logicielles, comme l'accès au webmail sur les messageries Microsoft Exchange.

Enfin, la solution IWSVA permet de filtrer les flux sur le protocole « File Transfert Protocol » (FTP). La configuration s'effectue de la même manière que pour les flux http, avec les mêmes options à définir. Le filtrage de ce protocole est de plus en plus important, car de nombreux sites Internet proposent maintenant le téléchargement de fichiers directement depuis leurs plateformes via le protocole FTP. Des contrôles d'accès complémentaires aux analyses antivirales peuvent être mis en place. Par défaut, tous les clients sont autorisés à utiliser le protocole FTP. Or il est possible de restreindre ces accès par trois modes d'identification différents. Le premier consiste à définir des postes clients spécifiques et d'autoriser les connexions FTP uniquement depuis certaines adresses IP. Le second autorise les connexions seulement vers des adresses IP externes prédéfinies et considérées comme fiables, ce qui permet d'augmenter les performances, car les paquets transmis ne sont pas scannés par la solution. Enfin le troisième permet de définir les ports à utiliser obligatoirement pour se connecter aux sites FTP, car par défaut, tous les ports sont utilisables, entraînant des risques de sécurité.

J'ai démontré que l'analyse des flux http, https et ftp permet d'analyser les contenus de la plupart des flux Internet qui transitent sur le réseau de l'établissement. A aucun moment ces stratégies ne permettent d'interdire la consultation de sites considérés comme « valides » mais qui engagent tout de même la responsabilité de l'utilisateur et par conséquence celle du chef d'établissement. Le module « URL Filtering » de la solution Trend Micro met à disposition pour résoudre ce problème une liste de sept groupes représentants plusieurs catégories. En effet, l'éditeur procède au classement de chaque site Internet dans une catégorie, en s'appuyant sur les informations relayées par ses clients. Pour chaque catégorie, il est possible d'autoriser l'accès au site demandé, de l'interdire ou de surveiller l'accès. Dans le cas de l'interdiction, une page spéciale est renvoyée à l'utilisateur pour l'informer de la raison du blocage et l'évènement est enregistré dans les logs. Si le site appartient à une catégorie marquée comme « monitor », l'utilisateur peut consulter le site, mais cet accès est enregistré dans les logs pour une analyse ultérieure. Il est ainsi très facile de définir une politique d'accès aux sites Internet applicable à tous les utilisateurs. J'ai créé une catégorie personnalisée chargée de surveiller les flux à destination de sites de paris en lignes, comme l'illustre la figure ci-dessous. Les résultats ont montré que ces sites sont quotidiennement consultés directement depuis l'établissement.

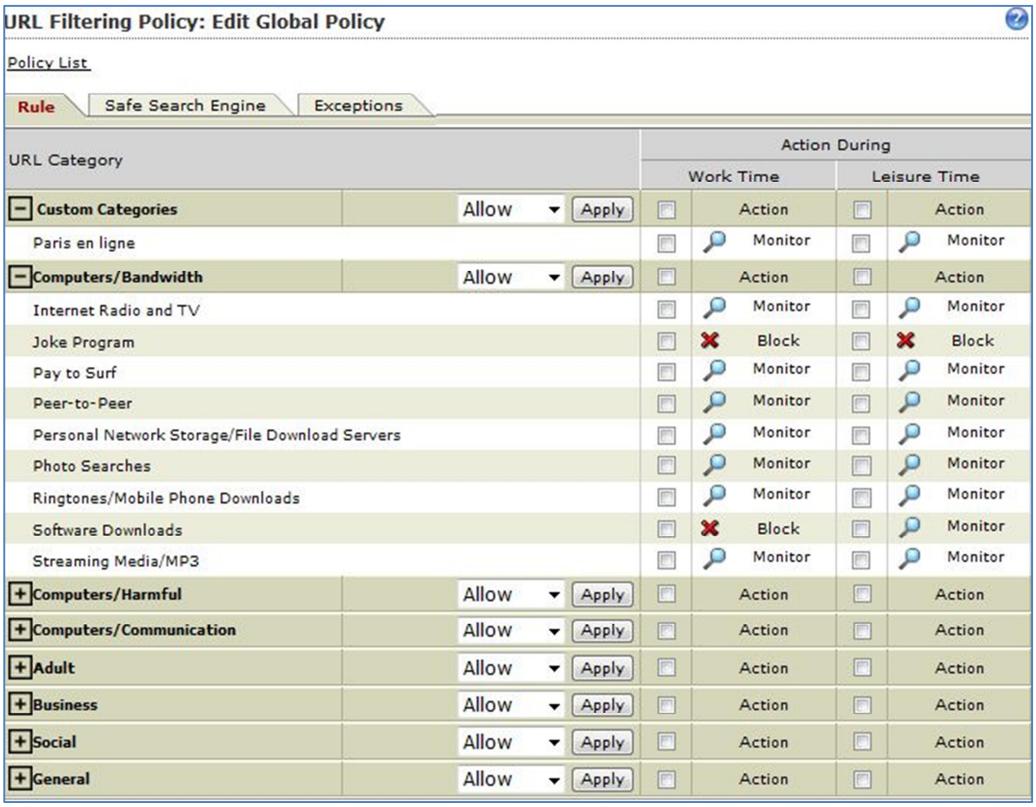


Figure 19 : Les catégories de filtrage selon Trend Micro (Trend Micro)

A titre d'exemple, la charte informatique de l'établissement interdit la consultation des messageries personnelles sur le lieu de travail. L'accès à tous les webmails est alors désactivé en marquant la catégorie « Email related » comme interdite. Cependant, devant le nombre important de nouveaux sites publiés quotidiennement, il est impossible pour la société Trend Micro et à ses concurrents, de classifier tous les sites en temps réels. La possibilité est alors offerte de pouvoir créer ses propres catégories de sites Internet et d'appliquer une gestion personnalisée des accès à ces sites. Sur le même principe, l'administrateur de la solution, peut constituer des listes blanches « Global Trusted URL », de sites Internet fréquemment consultés et considérés comme fiables, ainsi que des listes noires d'URL « Global URL Blocking » qui doivent être interdites à la consultation et ce quelque soit l'utilisateur. Ainsi, après avoir bloqué l'accès au site Facebook, j'ai constaté de nombreuses tentatives à toute heure de la journée. La mise en œuvre de ces listes peut améliorer les performances globales en limitant les analyses aux sites non répertoriés.

Pour sécuriser toujours plus l'infrastructure, Trend Micro encourage la création d'un cluster de serveurs pour répondre aux problématiques de continuité et de reprise d'activité, en cas d'incidents majeurs sur une plateforme. Le cluster fonctionne en mode actif/passif et des échanges permanents entre les deux serveurs sont effectués, sur un réseau dédié, afin de détecter

les problèmes système, réseau ou d'application et ainsi de basculer le trafic sur le serveur opérationnel. La gestion des nœuds peut-être assuré indépendamment, par un mécanisme de synchronisation. Le serveur ARM intègre aussi l'existence de ces deux nœuds et centralise les sauvegardes et restaurations des configurations. L'utilisation de cette option est fournie depuis peu dans la version 5.1 d'IWSVA et apporte une sécurisation du service de filtrage des flux Internet.

Le déploiement de la solution IWSVA apporte une sécurisation et une surveillance active des flux Internet sur l'établissement. La consultation régulière des journaux de la solution est indispensable pour optimiser le traitement des flux, informer et modifier les comportements des usagers, mais aussi pour détecter les failles de sécurité. La solution « ARM » de Trend Micro offre la possibilité d'atteindre ces objectifs.

6.3.1.4 L'analyse et les rapports via la solution « ARM »

La passerelle IWSVA intègre une base de données PostgreySQL dans laquelle est enregistrée la configuration et l'ensemble des journaux et des traces des connexions utilisateurs. Un module de rapport est fourni mais est peu convivial et ne permet pas de générer tous les rapports souhaités. J'ai souhaité évaluer également un produit complémentaire de Trend Micro. La solution ARM doit apporter une interface d'élaboration de statistiques et de rapports plus complète.

Le serveur virtuel ARM héberge la base de données de la passerelle IWSVA et centralise ainsi toutes les traces des connexions et des évènements liés à la navigation des utilisateurs. La configuration s'effectue directement dans ARM. J'ai créé un nouveau serveur à partir de l'interface et validé la connexion entre les deux modules. Les données sont alors téléchargées de la passerelle vers ARM et la configuration d'IWSVA est modifiée pour utiliser ARM comme base de données principale. Un message d'information est par la suite ajouté pour informer l'administrateur qu'ARM gère la passerelle.

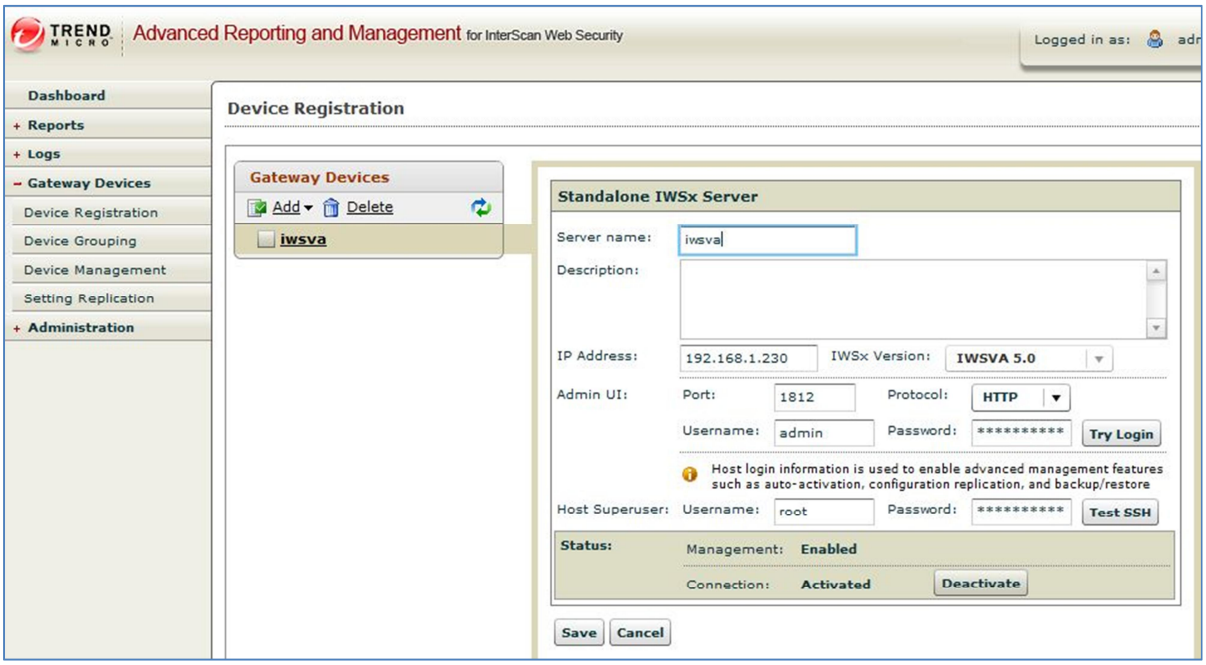


Figure 20 : Ajout d'un serveur IWSVA dans ARM

L'interconnexion entre la passerelle et le module de rapport est très forte, car il n'est plus possible d'arrêter ARM sans au préalable être intervenu sur la passerelle. Un des intérêts de ce module est de pouvoir centraliser la gestion et les journaux de plusieurs serveurs IWSVA, au travers de groupes.

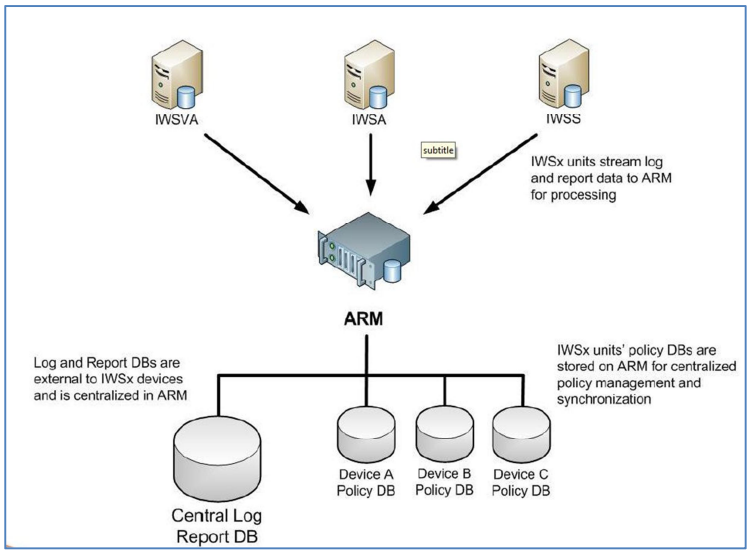


Figure 21 : Architecture ARM (TREND MICRO)

Trend Micro fournit avec ce produit une solution d'administration des clusters de serveurs IWSVA, en planifiant des réplications et pour limiter les temps de rétablissements de services en cas d'incidents majeurs sur un serveur, sans perdre d'informations.

Les évènements enregistrés dans la base de données sont de deux types : ceux du système et ceux liés à l'activité des utilisateurs. Les « system logs » contiennent des messages non structurés liés à des changements d'état ou des erreurs du système d'exploitation ou bien de l'application ARM. Par exemple, les informations relatives aux performances de la solution permettent de vérifier le dimensionnement de la machine, du point de vue ressources et volume de stockage. Les « reporting logs » sont les informations enregistrées suite à l'activité des utilisateurs en fonction des stratégies d'analyse mise en place. L'ensemble de ces données sont consultables et interrogeables via un module de rapports. La durée de rétention de ces informations est de 30 jours par défaut, dans la base de données. Il est possible d'exporter ces journaux sur un serveur de fichier ou bien sur un serveur FTP afin de les conserver pendant la durée recommandée de 1 an.

La force de la solution ARM est de pouvoir générer des rapports à partir des informations recueillies, pour que l'analyse et la lisibilité soit facilitée. Ces rapports peuvent être demandés « à la volée » ou bien faire l'objet d'une planification par jour, semaine ou mois. Ils sont consultables au format *.pdf ou *.csv et peuvent être également transmis par messagerie électronique aux gestionnaires.

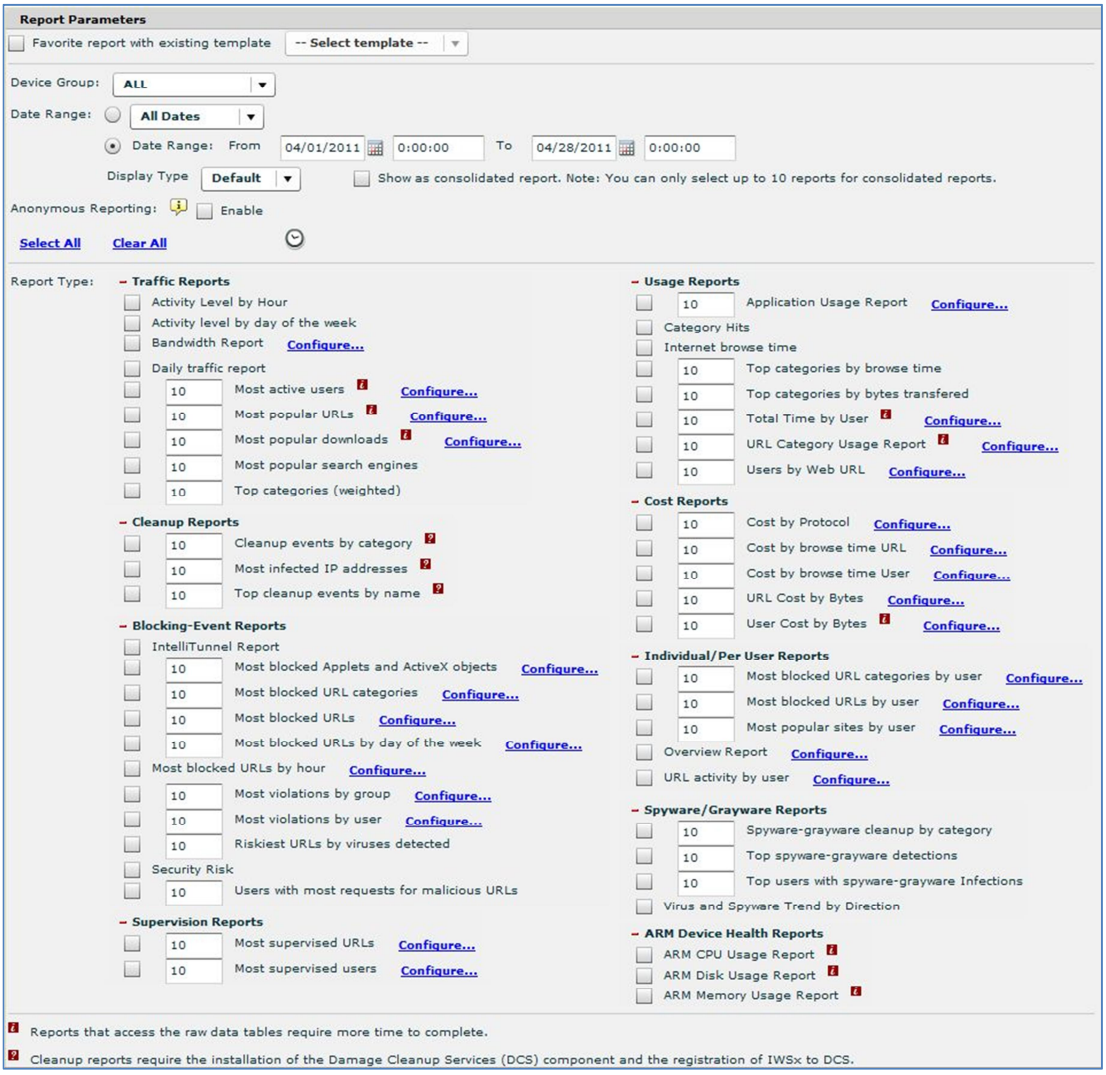


Figure 22 : Les options de rapports via ARM (TREND MICRO)

Les informations recueillies correspondent aux stratégies définies sur la passerelle IWSVA et sont affichées sous forme de tableau et de graphiques dans les rapports. L'interconnexion avec l'annuaire LDAP de l'établissement apporte la possibilité de générer des rapports précis, concernant un utilisateur seul ou bien un groupe d'utilisateurs. Il est alors facile de la liste des sites les plus consultés, les plus bloqués, le temps passé en navigation par utilisateur.

Enfin, Trend Micro propose l'utilisation de l'utilitaire de génération de rapport open source « iReport » pour compléter son offre. Cette application permet de sélectionner les champs à inclure dans les rapports, directement à partir de la base de données. Chaque client peut alors construire ses propres rapports totalement personnalisés et les intégrer ensuite dans ARM comme modèle. Après avoir évalué ce module, j'ai constaté que le temps d'administration à accorder à

ce module est non négligeable. La maintenance est aussi importante si l'on souhaite appliquer les mises à jour du module « iReport »

Le module ARM est donc un outil complémentaire à la plateforme IWSVA pour faciliter l'analyse de toutes les informations recueillies, mais surtout pour optimiser la configuration déployée. Cependant, le bilan de ces tests met en évidence des atouts et des inconvénients à l'acquisition de cette solution de filtrage des flux Internet.

6.3.1.5 Bilan des tests de maquettage

Les phases de tests de la solution de filtrage des flux Internet de la société Trend Micro effectués ont permis de mettre en avant les atouts et défauts de cette solution logicielle mais aussi certaines pratiques méconnues de l'utilisation d'Internet au CH de Montbert.

La passerelle IWSVA sécurise les flux Internet avec une surveillance active sur les protocoles les plus utilisés : http, https et ftp. Trend Micro s'appuie sur son expérience, avec la généralisation des outils comme : « Intelliscan », pour analyser uniquement les types de fichiers considérés à risque (le type est déterminé après vérification de l'en-tête du fichier), « Intellitrap » pour détecter les codes malicieux dans les pages Internet consultées et « Intellitunnel » pour interdire les flux de messagerie instantanée ou l'utilisation de tunnel sur le port 80. L'activation de ces options permet d'optimiser les performances des serveurs en sélectionnant ce qui doit être analysé ou non. Afin d'améliorer la navigation, Trend Micro propose différentes solutions pour intégrer un serveur de cache de type « Squid ». Cette solution accélère les téléchargements des pages Internet les plus souvent consultées, diminue les temps de réponses et optimise les ressources de la bande passante si celle-ci est faible. Sur le même principe de mise en cache des pages Internet, Trend Micro déploie un espace de stockage qui va contenir les informations relatives à des URL, extraites des bases de données de réputation, comme la catégorie, les alertes anti-phishing et anti-pharming, afin de limiter le trafic réseau et de traiter ces flux plus rapidement. Les problématiques de performances et de fiabilité de la solution sont alors fortement associées à la mise en place d'un cluster dédié.

En effet, la possibilité de créer un cluster de serveurs IWSVA renforce la sécurisation des accès Internet. Il est alors possible d'assurer le transit des flux Internet par un serveur opérationnel, dans l'attente du rétablissement de l'autre nœud. La maintenance du système et des applications de chaque passerelle est alors plus facile car aucune interruption de service n'est à prévoir. Cet aspect est très important, car devant la multiplicité des services et des applications hébergées sur Internet, une coupure de l'accès pendant plusieurs heures peut entraîner de

nombreux problèmes de fonctionnement et d'organisation. Le cluster sécurise la continuité de service, mais n'offre pas l'authentification de l'utilisateur à l'origine des connexions. Cette sécurité doit être couplée avec l'identification des utilisateurs.

L'interconnexion de la solution IWSVA avec l'annuaire Active Directory apporte des informations complémentaires sur la navigation Internet des utilisateurs. Ces informations d'identification peuvent ensuite être traitées et analysées au travers de rapports. Cette authentification à postériori m'a offert la possibilité d'améliorer la configuration de la politique de filtrage détaillée dans la charte informatique. J'ai également validé le service d'authentification de l'utilisateur, avant d'accéder à un portail Internet. En effet, je rencontre cette problématique quotidiennement avec les postes de travail partagés, et l'accès aux applications métiers. Ainsi, après l'installation du programme « ShellRunAs » sur le poste, lors de l'ouverture du navigateur par défaut Internet Explorer, l'utilisateur doit saisir ses identifiants pour accéder à Internet. Cette option apporte une sécurisation complémentaire à la navigation déjà effectuée par IWSVA et assure la traçabilité de tous les utilisateurs potentiels.

La sécurisation des flux Internet s'appuie également sur le filtrage d'URL mis à disposition dans la solution au travers du module « URL filtering ». Chaque jour Trend Micro recense et classe un grand nombre de sites dans l'un des sept thèmes, contenant chacun plusieurs catégories. Les stratégies que j'ai définies pour bloquer, surveiller ou toujours autoriser la consultation des sites classés dans une catégorie sont à réévaluer régulièrement. Les sites non répertoriés peuvent être répartis dans des catégories personnalisées et faire l'objet de traitements spécifiques. J'ai créé des politiques d'accès différentes pour quelques utilisateurs en fonction de l'appartenance ou non à un groupe. Cette option doit permettre de répondre aux problématiques du CH de Montbert rencontrées dans certains services de soins, tout en assurant la surveillance des flux au travers de l'utilisation des rapports.

Enfin, le serveur ARM assure la gestion de la supervision des flux Internet. En effet, l'émission de rapports automatiques ou manuels apporte aux administrateurs la possibilité de réévaluer les politiques mises en place, de les optimiser, mais aussi de prévenir de potentiels risques de sécurité. La possibilité de créer des rapports totalement personnalisables via le plugin « iReport » assure de disposer uniquement des informations utiles aux administrateurs. De plus, les rapports peuvent s'appuyer sur les groupes utilisateurs déjà utilisés dans l'Active Directory, ce qui permet de mieux cibler les besoins en fonction des professions et ainsi répondre aux attentes des utilisateurs qui doivent accéder à des informations jugées sensibles.

Cependant, la combinaison des produits IWSVA et ARM présente des aspects négatifs qu'il convient de prendre en compte.

Tout d'abord, la solution propose un filtrage des flux Internet sur les trois protocoles les plus utilisés, que sont http ; https et ftp. Les connexions sur des sites ftp sécurisés ne sont donc pas prises en compte malgré une utilisation de plus en plus fréquente. Les flux sécurisés par https peuvent être décryptés mais ces travaux nécessitent des traitements importants qui peuvent impacter les performances globales. La mise en œuvre de cette technologie doit par ailleurs respecter les conditions réglementaires d'informations des usagers avant le déploiement des modifications. De plus, la généralisation de l'usage des serveurs proxys anonymes, via le réseau THOR par exemple, peut être une source de problèmes pour la sécurisation des réseaux de l'établissement, ce qui confirme la nécessité de pouvoir filtrer sur plus d'un niveau de protocoles. La problématique du filtrage des flux https est aussi liée à celle de la gestion des certificats de sécurité SSL.

La gestion des certificats est un vrai problème dans la solution et présente un fonctionnement médiocre. En effet, l'utilisation de certificats de sécurité, émis par des autorités de certifications reconnues, fonctionne parfaitement. Or, ce n'est pas le cas pour tous les certificats auto-signés par des applications, ce qui représentent la majorité de ceux utilisés sur le CH de Montbert. J'ai observé de nombreux dysfonctionnements lors de cette phase de tests. La gestion est de plus complexifiée lorsqu'il s'agit de certificats nominatifs, pour l'accès à des sites Internet gouvernementaux ou bien institutionnels. J'ai également constaté des problèmes, aléatoires, dans la gestion de l'authentification interne à IWSVA, car une mire d'identification peut demander à tout moment de saisir ses identifiants, sans raison particulière. Ce problème peut à priori se résoudre en ajoutant l'adresse IP du serveur dans la liste des sites autorisés du navigateur, mais cela ne représente t-il pas une faille de sécurité potentielle ? Dans le cas du déploiement de cette solution, il faudrait étudier si l'activation de cette option est vraiment essentielle, car elle pourrait générer des problèmes de fonctionnement importants. Ces incidents ou défauts liés à l'authentification existent aussi pour la gestion des connexions utilisateurs.

Trend Micro propose une authentification nominative pour accéder au réseau Internet, à partir des identifiants de la session Active Directory. Ce choix nécessite le déploiement du plugin « ShellRunAs » sur tous les postes du parc, mais surtout il impose l'utilisation du navigateur Internet Explorer de Microsoft, comme navigateur par défaut. Or, le CH de Montbert utilise aussi Mozilla Firefox et ne souhaite pas contraindre les utilisateurs à changer de navigateur en

fonction de la nature de leur travail. Il est regrettable que cette option ne soit pas déployée pour les navigateurs, du moins les plus fréquents, afin de répondre aux besoins de nombreuses organisations qui auraient elles aussi fait le choix de logiciels libres. Ce problème d'ergonomie peut-être rapproché de l'architecture globale de la solution et donc des ressources à déployer pour assurer un fonctionnement optimal.

L'infrastructure de filtrage Trend Micro s'appuie sur la technologie de virtualisation de serveurs. Deux machines virtuelles sont alors nécessaires, au minimum. Ce nombre augmente si l'on souhaite utiliser un serveur proxy indépendant et ne pas impacter la production lors de la génération des rapports. La mémoire et les temps processeurs consommés sont importants et doivent impérativement être évalués. Trend Micro conscient de ce problème a publié un guide des bonnes pratiques dans un environnement virtuel de type VMware [KWAN]. La problématique du volume disque réservé de la machine virtuelle n'est pas pris en compte, ni celui de la conservation des traces, pendant la durée choisie. Le déploiement d'une solution de haute disponibilité avec la mise en place d'un cluster multiplie les coûts matériels et par conséquents financiers. La nécessité de mettre à disposition des ressources élevées se confirme avec l'utilisation du serveur ARM.

La passerelle IWSVA sécurise et analyse les flux sortants et entrants et collecte des informations enregistrées dans une base de données. Le rôle du serveur ARM est de fournir des outils afin d'exploiter ces traces au travers de rapports, standards ou personnalisés. Or, les tests ont mis en évidence des temps de latence élevés pour générer ces rapports, ralentissant pendant ce temps de traitement la collecte des informations issues de IWSVA. Il apparait important de prévoir la création de ces rapports dans des tranches horaires ou l'activité est moindre pour ne pas pénaliser la production. Ce problème peut néanmoins être résolu si l'on déporte ces traitements sur un autre serveur, dédié à cet usage. J'ai également observé une augmentation du trafic réseau entre ces deux serveurs, qui peut s'expliquer par l'externalisation de la base de données du serveur IWSVA. Ces échanges permanents peuvent également impacter les performances.

En conclusion, la solution de filtrage de flux web de la société Trend Micro est une bonne solution pour les petites ou moyennes entreprises car elle répond aux besoins les plus fréquents. Une maintenance et une vérification régulière des rapports doivent cependant être réalisées, car la configuration doit évoluer avec l'usage et les habitudes des utilisateurs.

6.3.2 La solution Websense

La société Websense est le leader mondial de la sécurité intégrée du Web, des données et de la messagerie. Elle assure la protection d'environ 40 millions d'employés et plus de 40000 organisations dans le monde. Distribuées à travers un réseau mondial de partenaires, les solutions de sécurité de Websense aident les entreprises à bloquer les codes malveillants, à prévenir la perte d'informations confidentielles et à appliquer des règles de sécurité et d'accès Internet. Websense s'appuie sur son réseau « ThreatSeeker » qui fournit l'intelligence nécessaire aux analyses en temps réel de la réputation Web, du comportement et des données, afin d'assurer la protection de l'information.

L'évaluation de la solution Websense me permet d'apporter de nouvelles solutions aux problématiques du CH de Montbert. Les services proposés permettront de mieux appréhender l'utilité ou non du déploiement de ces outils par la suite.

6.3.2.1 Architecture cible et licences logicielles évaluées

L'évaluation de la solution Websense nécessite de remplir un formulaire sur le site Internet et de choisir la solution à tester parmi les produits disponibles.

Parmi les nombreux produits disponibles à évaluation, j'ai choisi d'éprouver la solution « Hosted Web Security Gateway ». Ainsi, le filtrage est effectué dans le « cloud » au niveau des datacenters de Websense (Annexe E). L'utilisation en mode « SaaS » apporte une grande facilité de déploiement et permet de ne pas modifier la configuration des éléments actifs ou très peu. Cette architecture hébergée décharge les services informatiques de la maintenance et des évolutions de sécurité nécessaires. Dans ce cas, il n'y a donc pas de serveurs physiques ou virtuels à maintenir. La mise en place de la solution consiste uniquement à utiliser une nouvelle configuration de serveur proxy dans les navigateurs des utilisateurs afin de router les flux vers les serveurs Websense. Dans le but de tester cette solution, une licence pour 25 utilisateurs a été mise à disposition pendant 13 jours consécutifs.

La décision d'évaluer ce type d'infrastructure est importante car elle doit permettre de valider le fonctionnement d'une solution de filtrage en mode hébergée pour le CH de Montbert, mais aussi de prendre toute la mesure des avantages et contraintes de ce type d'architecture.

6.3.2.2 Configuration, exploitation et optimisation

L'évaluation de la solution Websense nécessite un enregistrement en ligne afin d'obtenir une licence d'accès. Les démarches administratives réalisées, j'ai réceptionné un lien de connexion joint à un message pour lancer la procédure de configuration de la solution.

Tout d'abord, pour utiliser cette nouvelle plateforme, il est nécessaire de configurer son navigateur Internet avec une nouvelle adresse de serveur proxy. Tous les flux seront alors redirigés vers les serveurs Websense afin de les sécuriser. Pendant cette période de test, les navigateurs sont configurés manuellement sur les postes du service informatique et quelques utilisateurs. Cependant, pour faciliter le déploiement, cette adresse peut-être déployée automatiquement par les stratégies de groupe (GPO) via les contrôleurs de domaine. Ainsi, chaque stratégie de filtrage nécessitera de créer une GPO spécifique pour pouvoir l'appliquer sur les groupes d'utilisateurs souhaités.

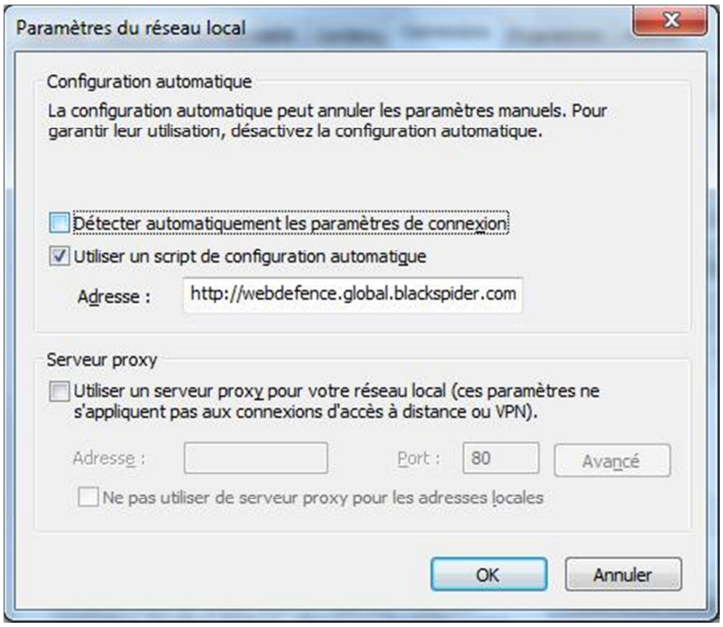


Figure 23 : Configuration d'un serveur proxy dans le navigateur

L'application de filtrage étant hébergée, la console d'administration et de supervision l'est également. Celle-ci permet de gérer l'ensemble des politiques de filtrages appliquées aux utilisateurs, les catégories, les exceptions. Au démarrage, une stratégie par défaut est proposée. Websense conseille de la personnaliser à l'établissement dans un premier temps pour faciliter l'apprentissage.

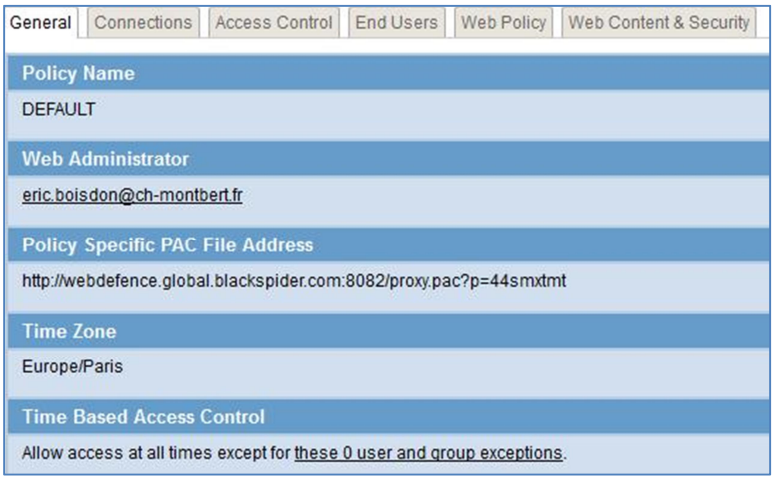


Figure 24 : Informations générales sur la stratégie par défaut

En premier lieu, les adresses IP de l'établissement doivent être renseignées de façon à pouvoir identifier les flux et appliquer les principes de sécurité qui seront définis par la suite.

Figure 25 : Configuration des sites dont les flux sont à sécuriser.

A l'aide de cette option, il est possible de configurer une stratégie pour chaque site distinct. Cette option est intéressante, car les sites distants pourraient accéder directement à Internet, sans avoir à faire transiter les flux par le site central. La bande passante serait donc optimiser pour les applications métiers et bureautiques.

Après avoir déterminé les flux à sécuriser, les modes d'authentification doivent être paramétrés. Chaque stratégie peut avoir une configuration différente et donc une authentification spécifique en fonction des besoins ou des utilisations. J'ai évalué la solution depuis le site de l'hôpital, mais également depuis mon domicile. J'ai alors constaté les différences qui peuvent s'appliquer en fonction du type et du lieu de l'authentification.

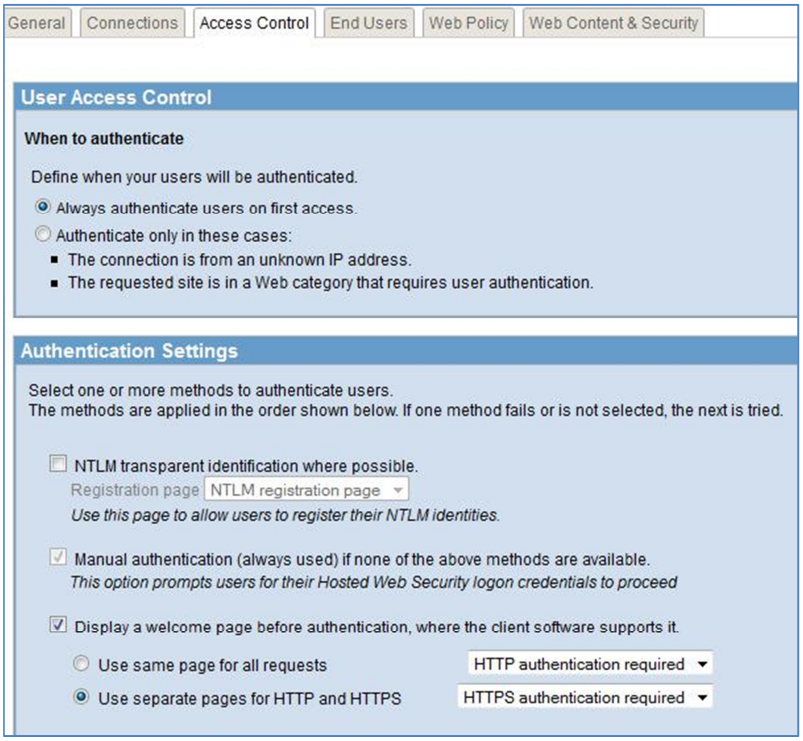


Figure 26 Contrôle des accès par stratégie.

L'authentification est déterminée lors de l'ouverture du navigateur. Soit l'utilisateur doit impérativement saisir ses identifiants pour accéder à Internet et ce à chaque connexion, soit il est automatiquement connecté. Une identification peut être demandée dans deux cas. Le premier correspond à un accès provenant d'une adresse IP non connue de la stratégie. Le second cas impose l'identification lorsque l'accès à certaines catégories le nécessite. L'authentification est facilitée lorsque la synchronisation avec un annuaire LDAP est mise en œuvre. Cependant, si aucun annuaire n'est disponible, il est possible d'utiliser le protocole NTLM pour identifier automatiquement l'utilisateur avec les identifiants de la session Windows, afin d'éviter à l'utilisateur de les saisir trop souvent, en s'appuyant sur les applications Squid, Samba et Kerberos. Au CH de Montbert, la majorité des comptes utilisateurs sont nominatifs, mais quelques comptes partagés subsistent. Je n'ai pas réalisé de tests à partir de comptes partagés pour ne pas impacter les habitudes des équipes soignantes. Il serait alors nécessaire de définir des stratégies spécifiques pour les utilisateurs nominatifs ou partagés. Cependant le déploiement des cartes de professionnels de santé (CPS) pourrait imposer la suppression prochaine de ce type de compte. Des accès transparents n'impliquent pas un libre accès à Internet, sans catégorie interdite.

Websense s'appuie sur d'immenses bases de réputation afin de catégoriser les sites Internet. A ce jour, plus de 90 catégories et 50 langues sont répertoriées. Ce travail permanent s'appuie sur les informations du réseau « ThreatSeeker », sur des chercheurs mais aussi sur les données des clients renvoyées dans le monde entier. Chaque client peut néanmoins construire ses propres catégories pour répondre au mieux à son activité professionnelle.

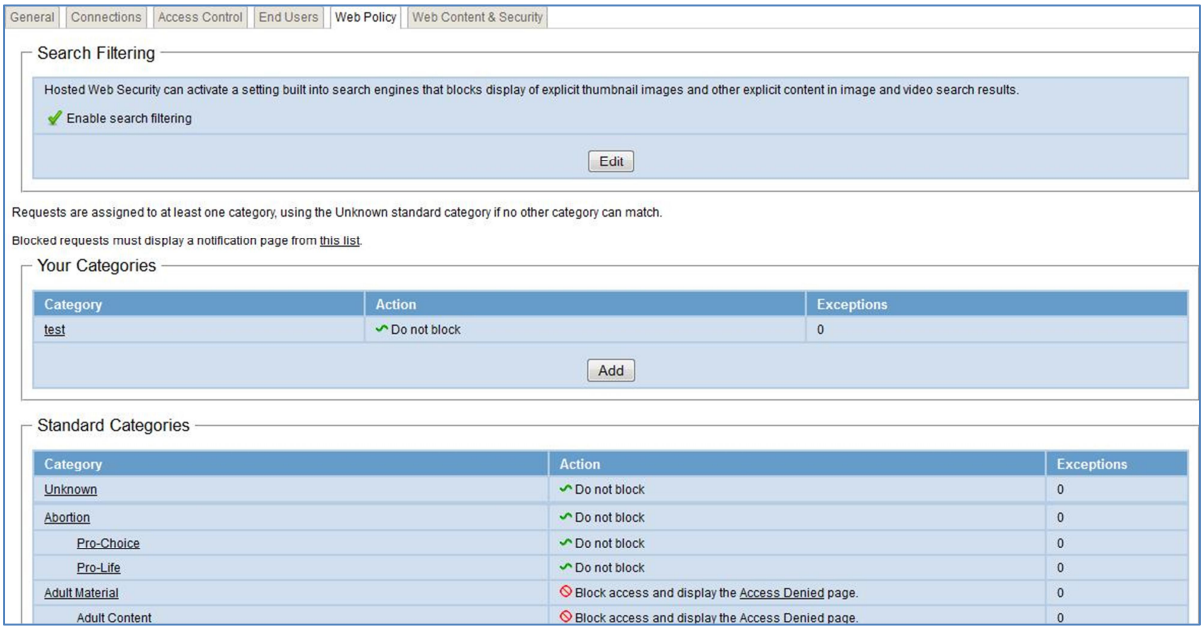


Figure 27 : Gestion des catégories avec Websense

Pour chaque catégorie, il existe 4 types d'actions : autoriser, requiert authentification, ne pas bloquer, bloquer. Le cas particulier de « ne pas bloquer » correspond à laisser un site accessible. Cependant s'il est répertorié dans une catégorie interdite, il sera interdit. Il existe également une priorité entre « autoriser » et « bloquer ». En effet, si un site appartient à une catégorie «autorisé », il le sera toujours même si il est ensuite référencé comme site à bloquer. La possibilité de créer des catégories personnalisées est importante afin de gérer la liste des sites souvent consultés dans l'organisation. J'ai initialement apprécié cette souplesse dans le choix des actions, mais j'ai ensuite rapidement constaté que celle-ci pouvait devenir difficile à gérer avec une multitude de sites configurés. Des exceptions peuvent néanmoins être configurées pour chaque catégorie et attribuées à des utilisateurs spécifiques, pour limiter à juste titre cette gestion. Enfin, dans le cas de sites bloqués, des pages d'informations sont affichées aux internautes. Celles-ci spécifient les raisons du blocage. Toutes ces notifications sont entièrement personnalisables, dans le texte, mais également à l'aide de balises utilisées décrites dans le

support Websense. Cependant, la définition de catégories et la gestion des accès ne sont pas des paramètres suffisants pour assurer la sécurité des flux d'informations.

L'onglet « Web Content & Security » de chaque stratégie apporte des outils complémentaires pour sécuriser les flux.

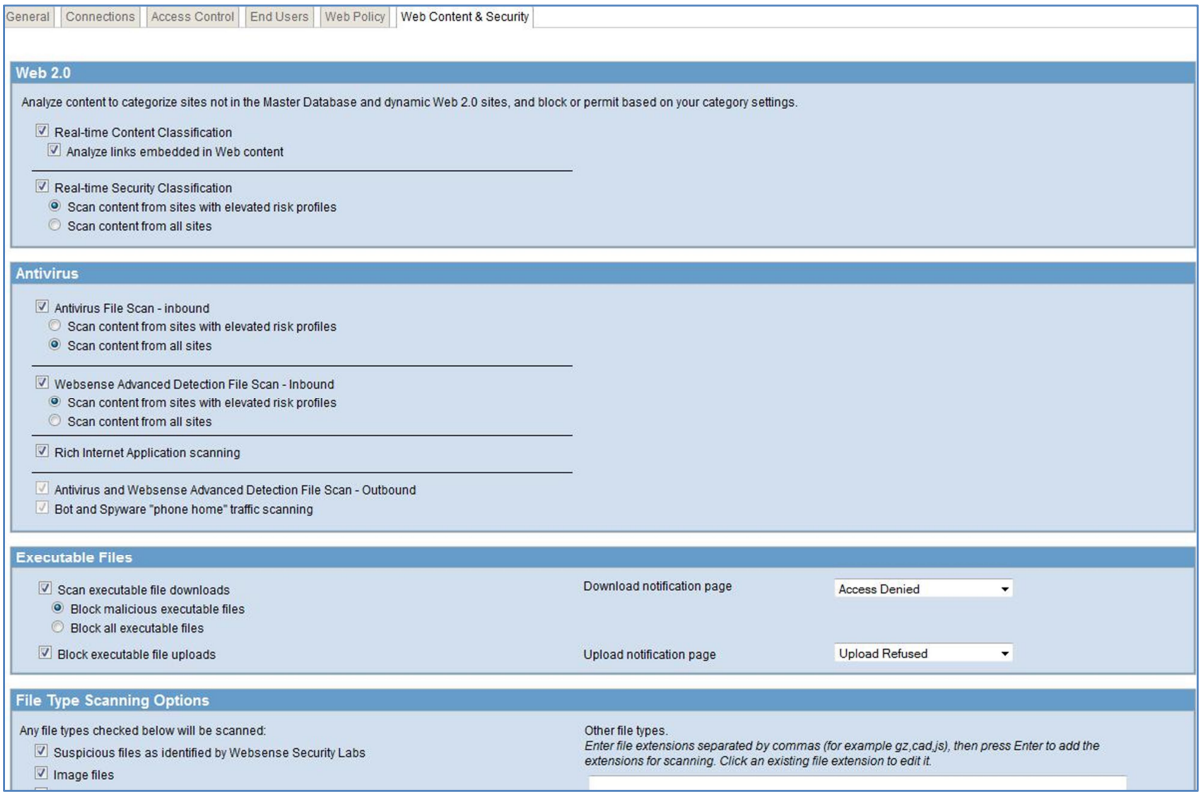


Figure 28 : Gestion des paramètres de sécurité avancés

La problématique du filtrage du « Web 2.0 » est traitée par Websense en temps réel, par l'analyse des contenus et des liens hypertextes présents sur les pages à afficher afin de mieux prévenir des dangers potentiels. Des analyses antivirus sont également effectuées sur les fichiers échangés afin de détecter les virus, malware et autres programmes malveillants. Les fichiers exécutables disposent d'une gestion particulière des autres types de fichiers (son, vidéo, image, document). J'ai rencontré des difficultés dans ces paramétrages, car les impacts sur les sites contenant du « Web 2.0 » sont parfois inattendus. Cela se traduit par l'affichage de pages incomplètes ou alors par le blocage d'éléments essentiels du site. Après avoir créé de nouvelles stratégies, j'ai réussi à corriger ces problèmes, mais cela peut entrainer une gestion lourde. Ces différents paramétrages terminés, il faut alors gérer la liste des utilisateurs qui devront utiliser cette stratégie.

Le dernier point de configuration est donc la gestion des utilisateurs et l'affectation des stratégies préalablement établies. Tout d'abord, un client de synchronisation doit être installé sur un poste de travail de l'hôpital. Celui-ci assure la liaison, sécurisée via https, entre l'annuaire LDAP et les serveurs chez Websense. Il permet de synchroniser les données des utilisateurs entre ces deux bases de données.

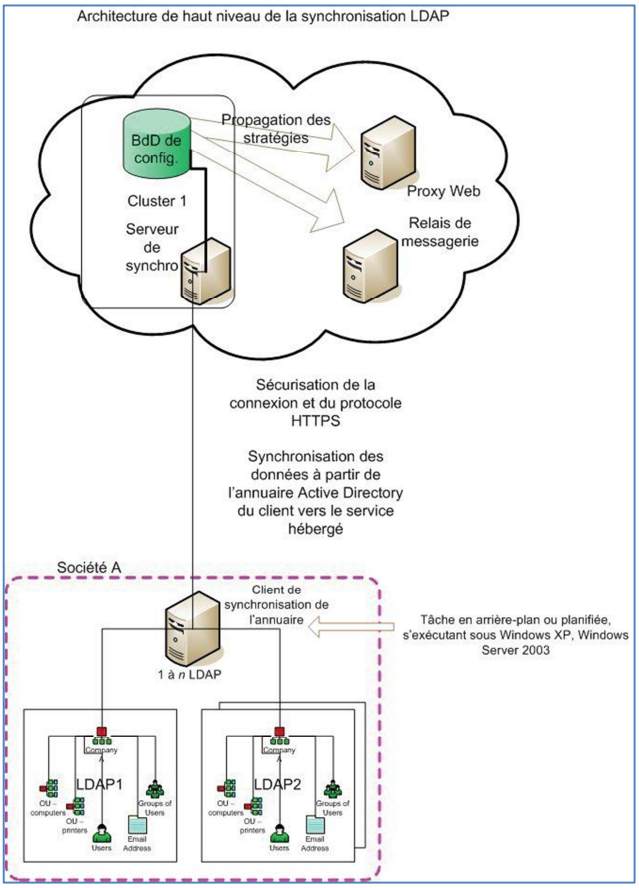


Figure 29 : Synchronisation entre l'annuaire LDAP et HWS (WEBSENSE)

Tous les utilisateurs n'ont pas nécessité à être importés. Dans ce cas il faut prévoir la création de groupes ou d'unité d'organisation pour pouvoir appliquer les stratégies propres à chacun. La sélection des groupes à synchroniser est effectuée à l'aide du client Websense. La synchronisation est planifiée à l'aide d'une tâche automatique. Cet outil facilite donc la gestion des utilisateurs au quotidien car il évite une double saisie des comptes utilisateurs dans le système d'information et les services HWS.

Enfin, la solution Websense affiche dès la connexion avec le compte administrateur une visualisation rapide de la bande passante utilisée, du nombre de requêtes, mais surtout des virus détectés sur Internet, pour la messagerie et la navigation. Ce résumé est complété par la mise à

disposition de rapports, qui peuvent être envoyés comme courrier électronique aux administrateurs. Ceux-ci sont de 4 catégories : par volumes, navigation, malware et services. Les rapports de services permettent de surveiller les processus de synchronisation. Les rapports par volume présente la quantité d'informations qui a circulé par utilisateurLes rapports de malware mettent en évidence les menaces interceptées dans les flux Internet, la volumétrie des sites consultés diffusant du Web 2.0. Les rapports disponibles dans la catégorie « navigation » proposent des résumés de l'activité.

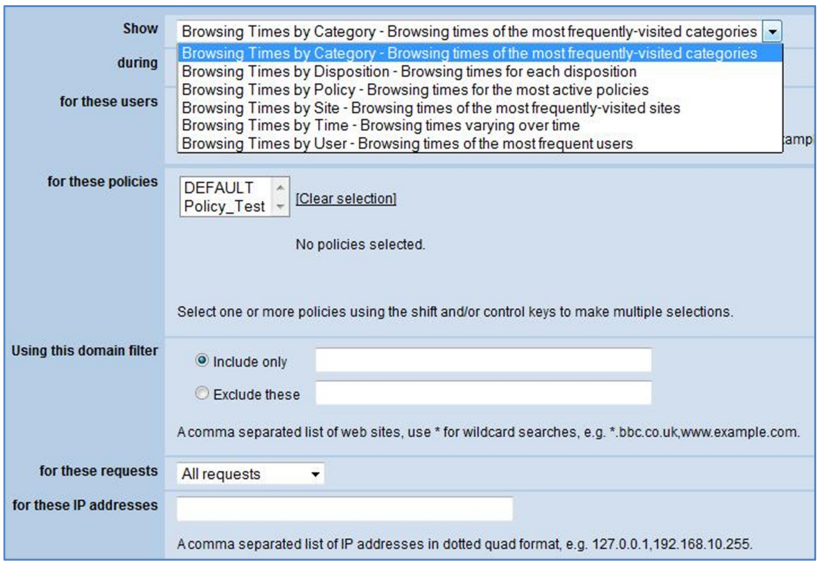


Figure 30 : Rapport d'activité avec HWS (WEBSENSE).

Des critères de requêtes sont à renseigner afin de rechercher des éléments précis dans l'ensemble des traces enregistrées. Les informations de navigation des utilisateurs sont enregistrées afin de déterminer par exemple la liste des sites consultés, les temps de navigation par utilisateur, les stratégies les plus utilisées. L'analyse régulière de ces données réduit les risques d'intrusion en essayant de les anticiper et offre une image complète des habitudes de navigation des utilisateurs qu'il sera nécessaire de corriger à l'aide de session d'informations ciblées.

Cette période d'évaluation de la solution Websense a mis en avant les qualités et défauts du produit et de ce mode de déploiement.

6.3.2.3 Bilan des tests de maquettage

La solution « Hosted Web Security » de la société Websense est une solution de filtrage Internet en mode hébergé. La mise en œuvre d'un produit de ce type a mis en évidence les avantages de cette solution.

Tout d'abord, l'hébergement de la solution sur les serveurs Websense permet de s'affranchir de la maintenance des logiciels et matériels nécessaire au bon fonctionnement de la solution. Les coûts d'investissement sont diminués et la solution n'affecte pas les performances des autres serveurs de l'établissement. Les maintenances des applications et le suivi du dimensionnement sont à la charge de Websense, qui assure également la continuité de service à 99.99% du temps grâce aux datacenters répartis dans le monde entier. La garantie de cette continuité est assurée uniquement si le client met en œuvre une architecture de « double lien » sur son ou ses sites principaux pour assurer ce service. Dans le cas de l'installation d'une « gateway » sur site, il est impératif de déployer non pas une mais deux passerelles, accompagnées d'un système d'équilibrage de charge afin d'optimiser la disponibilité et la fiabilité du service. En effet, Internet devient de plus en plus critique, même à l'hôpital, car de nombreux services et informations institutionnelles sont diffusés uniquement par ce réseau.

Puis, l'utilisation d'un mode hébergé apporte la possibilité de mise en place d'une nouvelle architecture réseau. En effet, les sites distants accéderaient directement à Internet sans avoir à faire transiter les flux par le site central, tout en profitant d'une gestion centralisée. Des rapports pour chaque site seraient disponibles. La mobilité des utilisateurs ne serait donc plus un problème. De plus, celle-ci pourrait même être étendue aux terminaux mobiles. Les protocoles utilisés et ceux encapsulés sont analysés sans provoquer de rupture de session. Les rapports apportent une visualisation sur les habitudes de navigation des utilisateurs.

Enfin, les administrateurs disposent d'outils performants et intuitifs pour gérer la solution au quotidien, notamment avec la console d'administration « Triton ». Je n'ai pu la déployer lors de cette évaluation, mais le Conseil Général du Maine et Loire (49) a accepté de me la présenter. Avec l'ensemble des outils Websense, il est envisageable de mettre en œuvre une architecture hybride, avec une passerelle sur le site principale et un mode hébergé sur les sites distants. Les logs et la gestion sont alors intégralement centralisés dans la console. Cette souplesse d'utilisation se retrouve également avec la synchronisation sécurisée des utilisateurs entre l'annuaire du CH de Montbert et celui utilisé pour Websense pour l'authentification. Les procédures d'identification sont par ailleurs performantes car la solution peut imposer de saisir

des identifiants avant d'autoriser l'accès au réseau Internet. Cette option assure à l'établissement de respecter le cadre législatif en conservant les traces des accès. Cependant, un tel système peut être perçu comme une contrainte pour les utilisateurs. Un système de « Single Sign On » pourrait résoudre ce problème en identifiant automatiquement l'internaute et ainsi améliorer la perception du système.

La solution Websense présente aussi des défauts dont il faut tenir compte. En effet, au niveau applicatif, il apparait que toutes les fonctionnalités ne sont pas disponibles en mode hébergé par rapport à la passerelle installée sur le site, notamment au niveau des rapports et de la gestion des stratégies à appliquer. L'uniformisation des produits entre passerelle et hébergé est une priorité de développement pour Websense en 2011, d'après le service commercial. En contrepartie, l'installation locale impose de maintenir du matériel supplémentaire, mais aussi de le dupliquer et d'investir si besoin dans une solution d'équilibrage de charge afin de prévenir les risques de dysfonctionnement et donc d'arrêt de service. De plus, le mode de déploiement des fichiers PAC dans les navigateurs est réalisé soit manuellement, soit par l'utilisation de GPO. Dans ce dernier cas, il convient de créer autant de GPO qu'il n'y a de stratégies web différentes. L'organisation du schéma de l'annuaire LDAP pourrait être modifiée, avec des conséquences non négligeables sur d'autres applications, tel que l'annuaire centralisé de l'établissement. Puis, le mode de synchronisation, asynchrone, avec les serveurs Websense est problématique, car il faut surveiller la fréquence, la réussite des opérations, mais aussi par l'obligation d'exporter des informations nominatives sur des plateformes non maîtrisées par l'établissement, avec des risques de vols des identifiants par exemple. Enfin, les rapports fournis ne font pas apparaître clairement les protocoles utilisés et la volumétrie de chacun d'eux. J'ai par conséquent rencontré des difficultés à évaluer le trafic https, http et ftp pour les protocoles les plus utilisés. Les outils de paramétrages à ce niveau sont inexistants en mode hébergé. Pour conclure, Wenbsense étant une société internationale, le référencement et le support le sont également. Les caractéristiques du public français ne sont alors pas entièrement prises en compte comme cela peut l'être avec d'autres éditeurs. Une personnalisation poussée de la solution est donc impérative pour s'adapter au métier du client potentiel.

La solution Websense, en mode hébergé, est une solution efficace car elle intègre toutes les technologies actuelles, sans avoir à assurer les maintenances. Cet aspect est très confortable pour les petites équipes. Le produit est assez ergonomique et l'appropriation est rapide. J'ai néanmoins regretté le module de rapport, peu convivial et non personnalisable. Une réelle

réflexion doit aussi être menée afin de déterminer si un mode hébergé conviendra au CH de Montbert, en terme d'architecture réseau, mais aussi sur le plan financier.

6.3.3 La solution Olfeo

La société OLFEO est un éditeur français qui intervient dans le domaine de la sécurité des flux Internet, de l'analyse à l'optimisation. L'approche est basée sur une solution technique internationale, associée à la proximité culturelle et le respect du cadre légal applicable dans le pays concerné. Olfeo se distingue de ses concurrents par cette proximité et l'adaptation du produit. Grâce à cette vision exclusive, Olfeo est un des éditeurs ayant connu la plus grosse croissance ces dernières années en Europe. La solution Olfeo est composée d'une suite de 4 produits complémentaires : le proxy cache QoS, le filtrage d'url, le filtrage protocolaire et l'antivirus. La solution dispose d'une architecture technique exclusive lui assurant de très hautes performances et une grande richesse fonctionnelle.

J'ai souhaité évalué la solution Olfeo sur une période d'évaluation d'un mois, avec toutes les options actives afin de réaliser une mise en situation la plus fiable possible.

6.3.3.1 Les différents modes d'intégration et leurs spécificités

Suite à l'évaluation des produits Trend Micro en version logicielle, Websense en mode hébergé, j'ai souhaité évaluer la solution Olfeo en version « appliance matérielle », afin de prendre toute la mesure des différentes solutions d'architecture envisageable.

L'appliance se présente sous la forme d'un serveur matériel habituel « 1U », avec les connectiques suivantes : 4 ports ethernet, 1 port série et 2 ports USB.

Figure 31 : Appliance d'évaluation fournie par OLFEO.

J'ai initialement déployé ce serveur dans le réseau DMZ de l'établissement, connecté physiquement sur le pare-feu. La configuration du serveur s'effectue intégralement via un navigateur web. La prise en main est facile car l'interface est intuitive. La documentation de l'éditeur est également très complète et apporte les réponses aux questions les plus courantes. Cette intégration correspond au mode « Ecoute » qui peut être mis en place avec la solution. Cependant, je n'ai pu conserver cette architecture, car il était nécessaire de créer de nombreuses règles sur le pare-feu et des vlans. En effet, le pare-feu et les serveurs ne sont pas situés dans la

même salle, ni dans le même bâtiment. Afin de limiter les modifications des configurations matérielles existantes, j'ai affecté à ce serveur physique une adresse IP interne au réseau du CH de Montbert, hors DMZ, avec un miroring de ports sur les switchs du cœur de réseau (Annexe F).

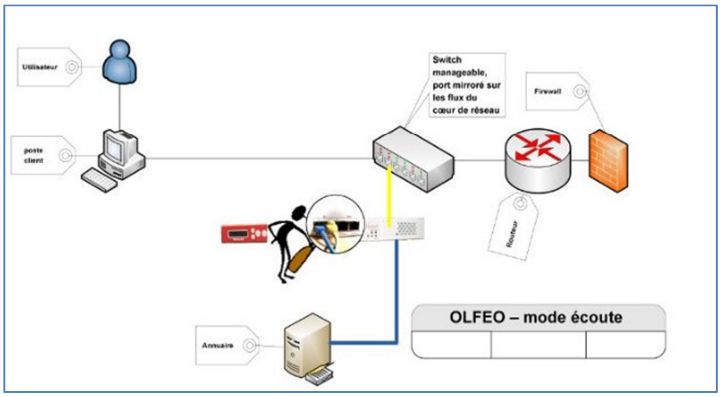


Figure 32 : Intégration en mode « Ecoute » (OLFEO)

En complément de ce mode d'intégration, il est nécessaire de définir un connecteur afin de personnaliser le mode d'intégration et les plages d'adresses à analyser.

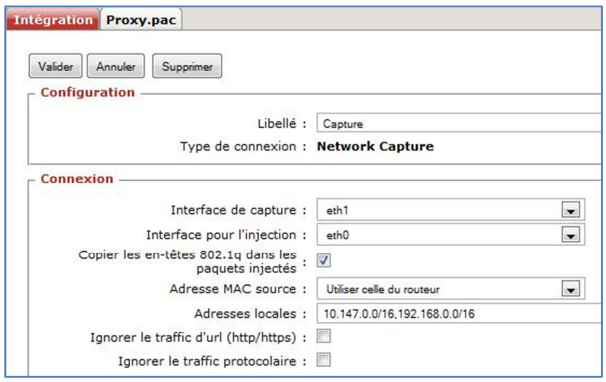


Figure 33 : Configuration du mode de capture.

L'administration de la solution s'effectue par l'interface « eth0 » alors que l'intégralité du trafic transite par l'interface « eth1 ». Avec ce mode de déploiement, les analyses sont effectuées sur une copie du trafic Internet. Le blocage des urls est réalisé simplement par l'envoi d'une requête « tcp reset » qui provoque l'abandon de la connexion en cours.

Il existe néanmoins d'autres modes d'intégration de la solution en fonction des besoins de chaque client, avec l'authentification incluse en standard pour tous ces modes. Le mode « Proxy » est le plus simple à mettre en place.

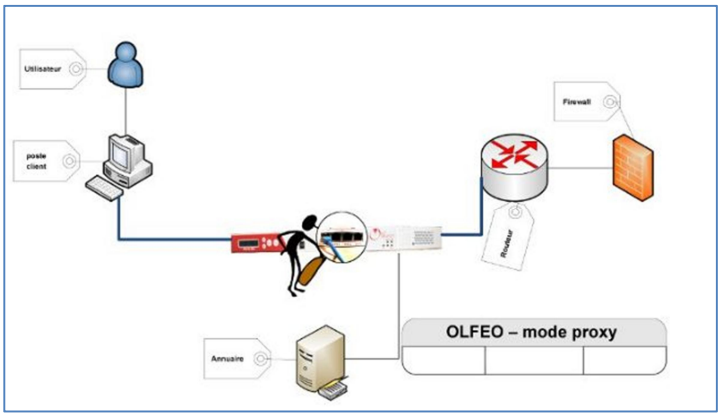


Figure 34 : Intégration en mode « Proxy » (OLFEO)

Le port ethernet « eth0 » est utilisé à la fois pour la connexion à la console et pour les flux Internet. La configuration du proxy peut-être transparente pour les utilisateurs, ou bien explicite, avec la diffusion des paramètres de connexion dans les sessions clientes via des gpo par exemple.

Le mode « Coupure » offre la possibilité de faire transiter tous les flux de tous les ports par Olfeo, via un pont noté « br0 » sur l'appliance. Un pont est établi entre les ports eth2 et eth3. On relie alors le réseau « lan » sur « eth2 » et le réseau « wan » sur « eth3 ». Si on attribue une adresse IP au pont, on peut diriger certains ports (80, 433...) vers le proxy Olfeo.

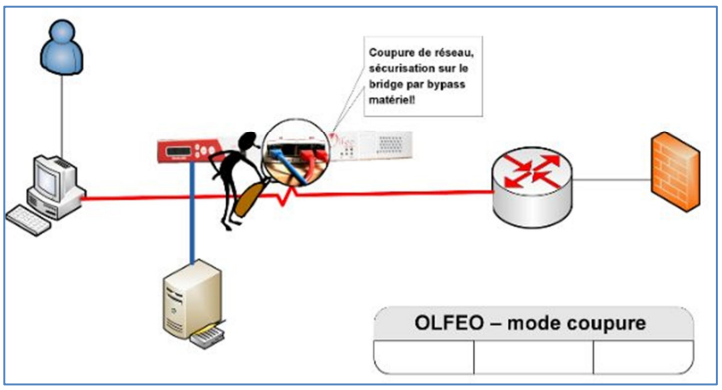


Figure 35 : Intégration en mode « Coupure » (OLFEO)

Le trafic réseau sortant transite sur le réseau interne jusqu'à l'interface « eth2 ». Après analyse par la solution, il est renvoyé via « eth3 » vers le pare-feu ou la connexion Internet. Afin de ne pas bloquer les flux lors de pannes sur l'appliance, une fonction de « bypass » est intégrée sur ce pont « br0 » ce qui assure un accès à Internet libre, sans sécurisation des flux. Cette situation doit être exceptionnelle et s'appliquer uniquement en mode dégradé.

Le mode « Connecteur/Protocole » utilise les spécificités de nombreux équipements comme les pare-feux ou routeurs qui permettent de déléguer des fonctions (antivirus, filtrage d'url...) à des équipements tierces. Ces équipements communiquent à l'aide de protocoles libres ou propriétaires. Ces interfaces sont capable d'envoyer à Olfeo au minimum l'url demandé et l'identifiant utilisateur. L'appliance recevant ses informations va jouer le rôle d'une base de données en analysant si l'url demandé est accessible à l'utilisateur à l'instant donné. Elle renvoie ensuite à l'équipement une réponse de type oui ou non. Dans le cas d'un non elle retourne, en plus, une page d'explication du refus destinée à l'utilisateur.

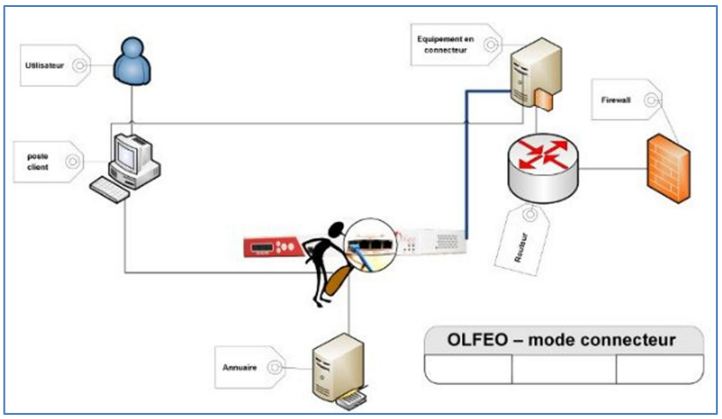


Figure 36 : Intégration en mode « Connecter » (OLFEO)

Ce mode d'intégration est particulièrement intéressant car il évite l'analyse du trafic jusqu'aux couches réseaux, ce qui se traduit par un gain de performance, de temps de réponse, mais aussi de bande passante. Cette solution est particulièrement adaptée au déploiement de la solution Olfeo avec des sites distants.

Enfin, Olfeo répond aussi aux problématiques de sécurisation des flux Internet sur les sites distants. L'appliance est installée sur le site central et communique avec des équipements distants spécifiques. L'administration est entièrement réalisée depuis le site principal, car Olfeo sait gérer distinctement les passerelles IP des utilisateurs et par conséquent des plans d'adressage différents.

Les modes d'intégration proposés par Olfeo sont variés et s'adaptent à toutes les architectures clientes. Il convient de choisir quels sont les produits à utiliser pour définir l'intégration cible.

Intégration / Solutions	Mode Proxy	Mode Connecteur	Mode Ecoute	Mode Capture
Filtrage URLs	✓	✓	✓	✓
Filtrage protocolaire	✗	✗	✓	✓
Antivirus	✓	✓ (avec icap)	✗	✓
Cache QoS	✓	✗	✗	✓
Nb de ports nécéssaires	1	1	2	3
Avantages / Limitations	Couvre les 3/4 de l'offre. Authentification tranparente forte	Nécesiite peu de ressources machine. Utilisable sur les sites distants	Peu intrusif. Authentification peu sécurisée	Universel Authentification peu sécurisée

Figure 37 : Avantages de chaque mode d'intégration (Olfeo)

Le CH de Montbert souhaite sécuriser ses flux de communication Internet. L'optimisation de ceux-ci pour les sites distants est un plus et pourrait apporter des gains sur l'occupation des bandes passantes concernées. Olfeo propose également d'associer sur un même serveur 2 modes d'intégration différents, afin de disposer des avantages de chacun. Ainsi le mode proxy associé au mode écoute sur le filtrage protocolaire pourrait constituer un compromis idéal.

6.3.3.2 La configuration logicielle de la solution Olfeo

J'ai choisi d'utiliser le mode d'intégration « Ecoute » pour évaluer les fonctionnalités de la solution. Le choix du type d'intégration effectué il reste à paramétrer la solution Olfeo.

Tout d'abord, les informations essentielles à la solution doivent être saisies. Il s'agit du nom du serveur qui apparaitra dans les DNS. Les serveurs DNS doivent aussi être renseignés, avec les adresses IP des DNS internes ou externes. J'ai choisi de renseigner des serveurs DNS externes, même s'ils ne sont pas utilisés quand la passerelle est intégrée au domaine. Ils peuvent néanmoins servir de secours en cas de dysfonctionnement des DNS du domaine. Sur le même principe, il est possible de forcer la synchronisation des dates et heures sur un serveur NTP externe, ou bien sur celui de l'Active Directory. Ce paramètre est important, car il impacte directement les stratégies déployées (analyse, plage horaire, …). La passerelle est obligatoirement synchronisée en UTC et l'horodatage dans les journaux de traces en temps réel est alors décalé de 1h ou 2h. Le serveur SMTP est aussi à configurer pour la diffusion de courriels aux administrateurs ou utilisateurs. Une configuration parallèle est nécessaire sur le serveur de messagerie Exchange à relayer ces messages en mode anonyme, dans le réseau interne. Dans le cas de l'utilisation d'un serveur proxy http autre que celui d'Olfeo, les informations de connexions doivent être saisies pour autoriser les flux, requêtes ou téléchargement des mises à jour. Dans un premier temps, j'ai configuré le serveur proxy existant pour valider le fonctionnement de la solution. Afin de vérifier l'exactitude de tous ces éléments, des tests internes à la solution sont exécutés pour valider la configuration. Olfeo propose

également d'intervenir sur la partition de démarrage à utiliser. En effet, la passerelle contient 3 partitions de 30 Go chacune avec le même système installé. Cette option permet de relancer un système vierge sur lequel il faudra réimporter la configuration, ou bien réinitialiser une partition existante. Enfin, il est nécessaire de savoir si l'on souhaite activer les statistiques et les options d'anonymisation avant la mise en service. Les éléments du système déterminé, le paramétrage de l'annuaire des utilisateurs doit être réalisé.

Afin d'authentifier les utilisateurs, une synchronisation avec l'annuaire Active Directory du CH de Montbert doit être mise en place, après intégration de la passerelle dans le domaine. Il est nécessaire d'identifier le type d'annuaire LDAP à utiliser pour établir la connexion (Active directory, active directory 2008, NTLM, …) et de disposer d'un compte utilisateur autorisé à parcourir l'ensemble de l'annuaire, en lecture.

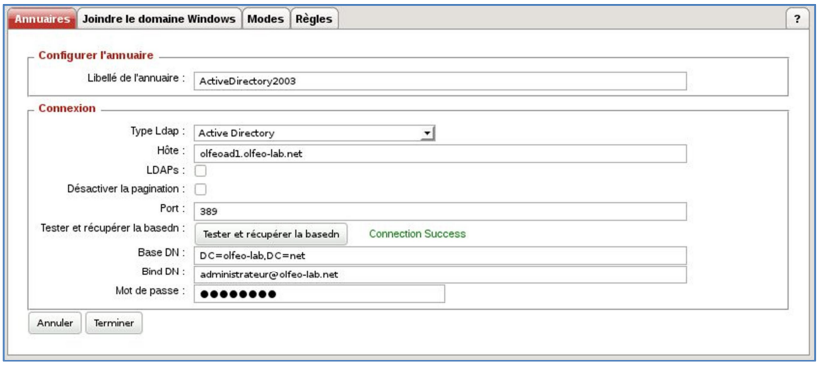


Figure 38 : Connexion à un annuaire ldap

Afin de ne pas synchroniser tous les comptes existants de l'active directory et donc d'importer des données inutiles, Olfeo propose de synchroniser les utilisateurs appartenant à des groupes déterminés. Si lors de la synchronisation, un utilisateur appartient à plusieurs groupes, le premier groupe d'appartenance détecté dans la liste des priorités sera sélectionné et synchronisé. Dans le cas du CH de Montbert, j'ai synchronisé initialement le groupe « utilisateur du domaine » de façon à inclure tous les utilisateurs potentiels. J'ai ensuite modifié cette configuration en sélectionnant uniquement quelques groupes d'utilisateurs représentatifs des problématiques à résoudre. Il serait préférable par la suite de créer des groupes d'utilisateurs spécifiques, auxquels il sera possible d'attribuer des droits de navigation différents. A partir de l'onglet « Mode », Olfeo permet de créer plusieurs annuaires ldap distincts, option utile dans le cas de société disposant de plusieurs organisations ou départements, chacun équipé d'un annuaire, mais disposant d'un seul point d'accès à Internet. Dans ce cas, l'authentification suit le processus suivant :

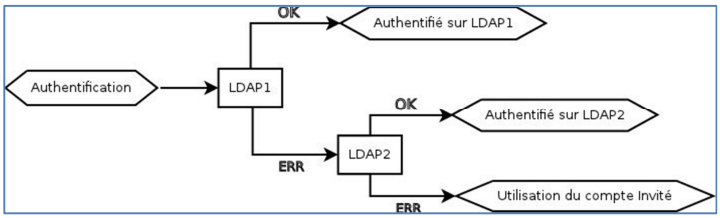


Figure 39 : Processus d'authentification ldap (Olfeo)

Après avoir configuré les annuaires d'authentification, l'onglet « règles » offre la possibilité de segmenter l'authentification des utilisateurs en fonction de la topologie réseau et/ou de plusieurs plages horaires. Olfeo assure non seulement l'authentification des connexions, mais aussi la sécurisation avec des analyses antivirus.

La solution Olfeo est chargée de sécuriser les flux de navigation des utilisateurs. La société s'était initialement rapprochée d'un spécialiste de l'antivirus, F-Secure, via un partenariat. Cependant, n'étant pas propriétaire du code de l'antivirus, Olfeo a choisi de mettre un terme à cette collaboration et a développé sa propre solution antivirale. Les bases de données utilisées sont maintenues par un autre éditeur, ClamAV, avec des mises à jour régulières et automatiques, sans configuration spécifique des administrateurs. L'utilisation de cet antivirus est soumise à licence, car c'est un module complémentaire à la solution de filtrage. L'activation est réalisée automatiquement lors de la création de règles anti-virus dans le moteur de règles, moteur présenté ultérieurement. Certains paramètres sont tout de même configurables et permettent ainsi de contrôler le comportement de la fonction antivirus :

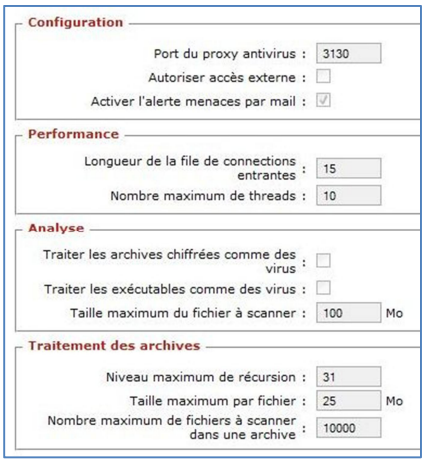


Figure 40 : Options de configuration de l'antivirus Olfeo (Olfeo)

La section « Performance » permet de fixer le nombre maximum de connexions simultanées et le nombre de processus à lancer. Les attaques de type DOS utilisent cette file de connexion

entrante afin de neutraliser l'antivirus. Une valeur trop élevée est donc une faille de sécurité. De même, un nombre de processus trop élevé entraîne une dégradation des performances. Lors de l'évaluation, j'ai laissé ces paramètres par défaut et aucun problème n'a été remonté. La section « Analyse » offre la possibilité de bloquer ou non les archives chiffrées, les exécutables et la taille maximale du fichier à scanner. J'ai également ici conservé les paramètres par défaut, à l'exception des exécutables qui ont été interdits. La dernière section, « Traitement des archives » apporte des outils de configuration pour la conservation et la rotation des fichiers de traces.

Le paramétrage de la passerelle nécessite de bien maîtriser les différents modes d'intégration disponibles en fonction des objectifs d'utilisation, mais aussi de disposer d'une visualisation complète de l'architecture, notamment de l'annuaire. Dans le cadre de cette évaluation au CH de Montbert, j'ai intégré la passerelle en mode « Ecoute » afin de ne pas impacter les flux Internet. Ce test a mis en évidence la nécessité de pouvoir associer les modes d'intégration de proxy et d'écoute afin de sécuriser l'ensemble des flux. Ces étapes de configuration système terminées, les politiques de filtrage et d'analyses doivent être élaborées.

6.3.3.3 Définition des politiques de navigation

La mise à disposition de politiques de navigation par défaut, avec une personnalisation possible, assure à Olfeo de répondre à toutes les demandes et spécificités de leurs clients. Plusieurs éléments sont à déterminer sur ces aspects, dont la charte informatique.

La problématique de la diffusion et de la prise de connaissance des chartes informatiques est un problème majeur. Olfeo apporte une solution concrète et propose d'imposer à l'utilisateur d'accepter la charte en vigueur, lors de sa première connexion et avant d'accéder à Internet. Plusieurs chartes peuvent être définies afin de répondre aux spécificités de chaque organisation ou services dans le cas du CH de Montbert.

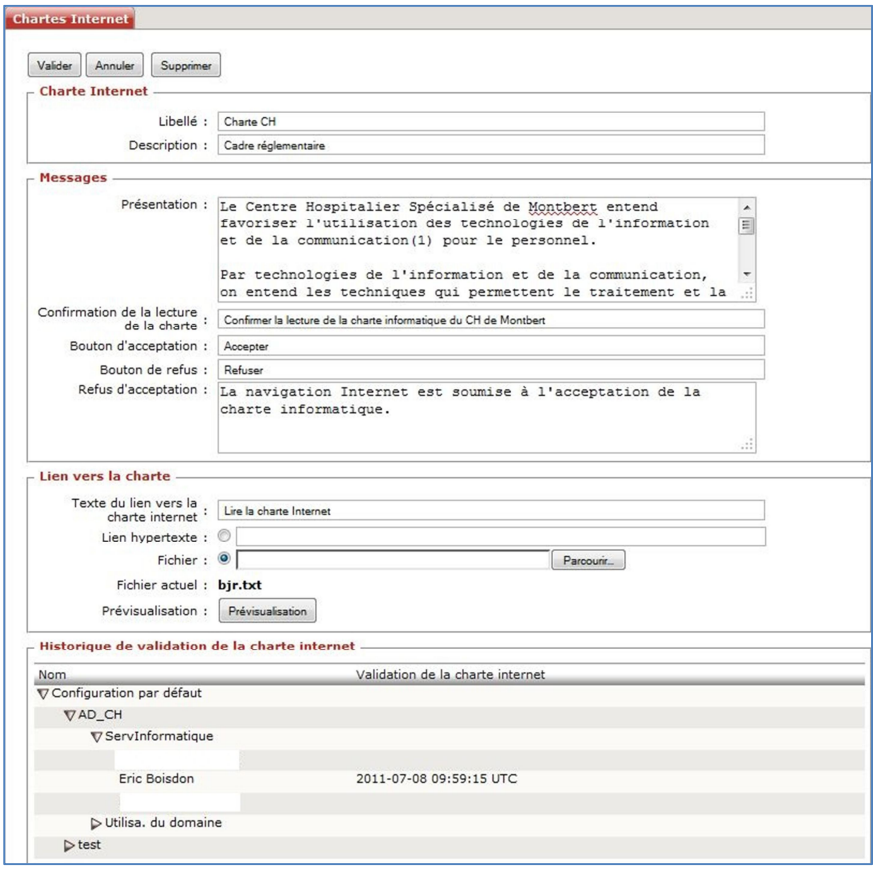


Figure 41 : Configuration de la charte Internet

Cette illustration met en avant les éléments qui seront visualisés par l'utilisateur avant validation. La charte complète peut être jointe pour faciliter la consultation de ce document très important. Pour garantir la validation des utilisateurs, Olfeo enregistre également les dates et heures de validation de la charte. Les utilisateurs sont à partir de ce moment pleinement responsables de leurs actes s'ils ne respectent pas les éléments énoncés dans ce document. L'activation de la charte est réalisée par la création d'une règle spéciale dans le moteur de règles d'Olfeo :

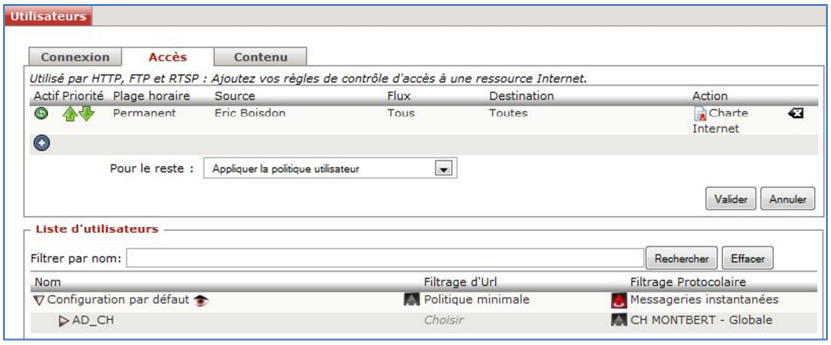


Figure 42 : Activation de la charte Internet au CH de Montbert

J'ai appliqué ce paramétrage sur mon compte et j'ai confirmé que les dates et heures de la validation sont enregistrées dans la solution. De plus, lors de la modification de cette charte, il est possible de diffuser rapidement la nouvelle version et de demander la validation de ce nouveau document. Il est alors obligatoire de créer une nouvelle règle car Olfeo ne permet pas la ré-acceptation d'une charte déjà validée. Cet outil de diffusion est plus performant et plus rapide que les procédures actuellement suivies sur le CH de Montbert et qui demandent beaucoup de temps de préparation. Au final, très peu d'utilisateurs prennent connaissance de ce document. Or celui-ci peut contenir les raisons du blocage de certaines pages et définir les politiques de filtrage mises en œuvre.

Les bases de réputation Olfeo sont alimentées quotidiennement, par des actions automatiques et manuelles. Les catégories proposées sont maintenues à jour et parfaitement adaptée au pays dans lequel la solution est déployée, afin de tenir compte des spécificités de chacun. Les sites Internet non recensés par l'éditeur sont transmis pour être classés à postériori, dans les catégories correspondantes. Ces transmissions de données sont entièrement automatisées. L'annexe G présente les catégories utilisées par Olfeo. La solution s'appuie sur ces classements pour créer des règles, dans le moteur de règles et décider des actions à réaliser. Malgré tous les efforts de l'éditeur, il est impossible de disposer d'un classement complet de tous les sites Internet existants. Pour résoudre cette problématique, une catégorie spéciale existe, dans laquelle les administrateurs peuvent créer des sous-catégories personnalisées.

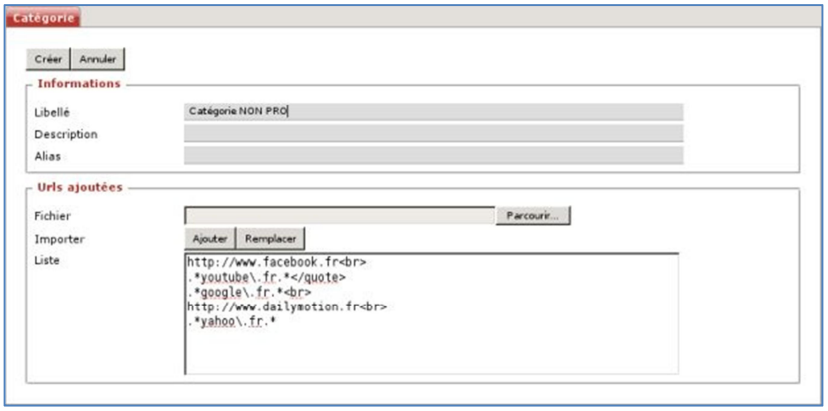


Figure 43 : Création de catégories personnalisées

Dans le but de prendre en compte toutes les urls associées à un nom de domaine, yahoo par exemple, l'utilisation des expressions régulières est indispensable, mais peut-être difficile à mettre en œuvre. J'ai rencontré ces difficultés lors de mes essais, notamment pour prendre en compte tous les liens existants en France, mais aussi à l'étranger. Le site de facebook par

exemple présente des urls spécifiques suivant les pays. Le classement des sites en catégorie permet de les regrouper par thématique et ainsi définir des listes de catégories et politiques d'accès.

Les listes de catégories sont indispensables dans Olfeo pour regrouper dans un même conteneur des sites appartenant à des catégories et des thématiques différentes. J'ai configuré une liste de sites considérés comme « non professionnels » car n'ayant pas de rapport avec l'activité des utilisateurs, pour essai.

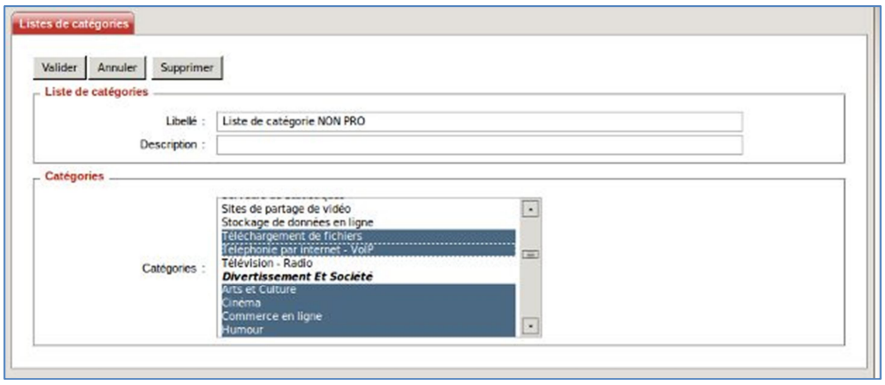


Figure 44 : Création d'une liste de catégories (Olfeo)

Ces listes sont ensuite intégrées dans des politiques de filtrage plus large. Olfeo s'appuie sur ces politiques pour allouer les accès aux sites internet à différents utilisateurs, groupes ou unités organisationnelles. Celles-ci sont constituées de plusieurs paramètres, obligatoires et optionnels. Tout d'abord, il faut décrire les conditions d'activation de la règle, c'est-à-dire les destinations. Celles-ci peuvent être des catégories, des listes de catégories ou des listes d'urls. Puis, il faut décider de l'action à réaliser : une autorisation, un blocage, ou une mise en place d'un quota. Enfin, la politique peut contenir des critères optionnels, comme la définition de plages horaires pendant lesquelles l'utilisateur peut accéder à des sites, le protocole utilisé pour la consultation (http, https, …), mais aussi la notion de quota d'outrepassement. Cette dernière est très importante, car elle permet d'autoriser un utilisateur à accéder à un site bloqué, avec un simple avertissement, par la saisie d'un mot de passe, ou alors par un quota de temps, qui est tracé au niveau de la solution. De cette façon, j'ai autorisé sur mon compte la consultation de sites bancaires pendant 10 minutes sur le créneau du repas. Cet intervalle de temps écoulé, je n'ai jamais pu me reconnecter à cette catégorie de sites le reste de la journée.

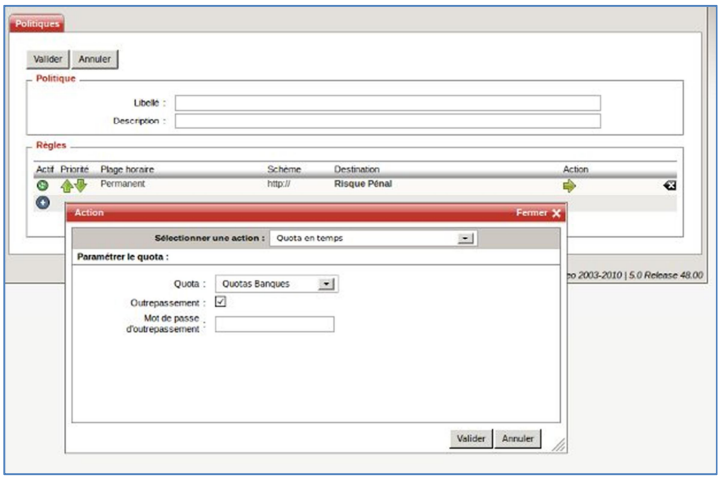


Figure 45 : Création d'une règle avec outrepassement (Olfeo)

Cette fonctionnalité est très intéressante, car elle autorise la création d'exception sans avoir à modifier son annuaire ou ses catégories. L'exploitation des listes et politiques de filtrage facilite la gestion des urls et la lisibilité dans le moteur de règles. Les principes ci-dessus le sont pour le filtrage protocolaire.

Le filtrage protocolaire est une des qualités de la solution Olfeo, complémentaire au filtrage d'urls. L'annexe H présente la liste des protocoles reconnus par la solution. Il est alors très intuitif de déployer des stratégies basées sur des politiques pour analyser les types de flux.

Libellé	Description
CH MONTBERT - Globale	
Messageries instantanées	Bloque les messageries instantanées (Msn, Psi, etc...) Politique à dépendance politique supérieure.
Politique Protocolaire DSI	Tout accès
Politique protocolaire Globale Société	Interdiction d'utilisation des outils de prise en main à distance, tunneling, et P2P

Figure 46 : Exemple de politique de filtrage protocolaire

En effet, l'évaluation a permis de mettre en évidence l'existence de flux de messagerie instantanée (MSN, MSN Web Messenger, Yahoo messaging), mais aussi des flux FTP ou de sessions sécurisées. Le pare-feu interdit à ce jour l'utilisation de protocoles autres que http depuis les postes clients, sauf pour ceux disposant d'autorisations spécifiques. Cependant, avec la généralisation de l'encapsulation des flux, la question du contenu des flux peut être posée. Il est possible de s'interroger sur l'existence de téléchargements de type « peer-to-peer » ou « bitorrent » sur l'établissement. Olfeo propose de gérer l'intégralité de ces flux depuis la passerelle au lieu de les administrer sur le pare-feu et donc de gérer de multiples spécificités. En complément de l'utilisation de ces politiques, Olfeo fournit d'autres produits comme le proxy, la qualité de service ou le cache.

J'ai mis en œuvre un proxy.pac déployé sur les navigateurs des utilisateurs via des stratégies de groupes pour rediriger les flux Internet vers notre serveur proxy. Un serveur http est donc installé pour cette seule utilisation. Olfeo propose d'utiliser la passerelle pour héberger ce fichier et s'affranchir de la maintenance d'un serveur complémentaire. Ce proxy propose une configuration en mode transparente, sans possibilité d'authentifier l'utilisateur, ou explicite, c'est-à-dire avec une authentification basée sur un annuaire. J'ai donc déployé une authentification explicite basée sur la session Windows pour ces essais. Dans le cadre d'un déploiement complet, il sera nécessaire d'étudier la mise en œuvre d'une mire d'authentification à l'ouverture du navigateur, afin d'identifier les utilisateurs des comptes Windows partagés, principalement les bureaux infirmiers.

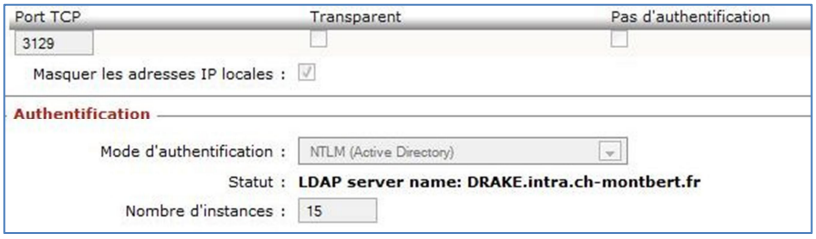


Figure 47 : Configuration du proxy http de Olfeo

D'autres types de proxy peuvent être configurés, afin de s'intégrer au mieux dans les architectures existantes : FTP, RTSP, SOCKS, TCP. Associés au proxy http, des caches mémoires et disques sont disponibles pour accélérer le trafic des pages web visitées.

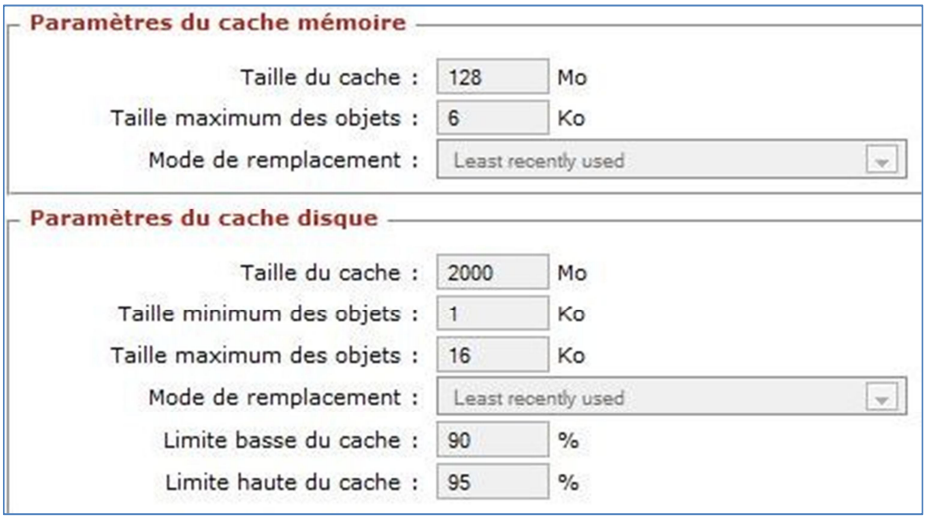


Figure 48 : Propriété du cache Olfeo

Le cache mémoire est plus rapide que le cache disque, mais ce dernier permet de stocker de plus gros volumes. Un compromis est donc à trouver par rapport aux habitudes de navigation des

utilisateurs. Des règles peuvent être créées pour accélérer le chargement de pages ou catégories spécifiques. De même, il est possible d'interdire de stocker dans le cache des fichiers en fonction de leur type MIME, ou alors de déterminer une durée maximale de stockage de ces fichiers. Des statistiques sont disponibles afin d'optimiser le paramétrage du cache et par conséquent les temps de réponses moyens. Enfin, Olfeo intègre un outil de qualité de services qui permet de définir des règles limitant l'utilisation de la bande passante en fonction : de plages horaires, d'utilisateurs et de la destination des navigations.

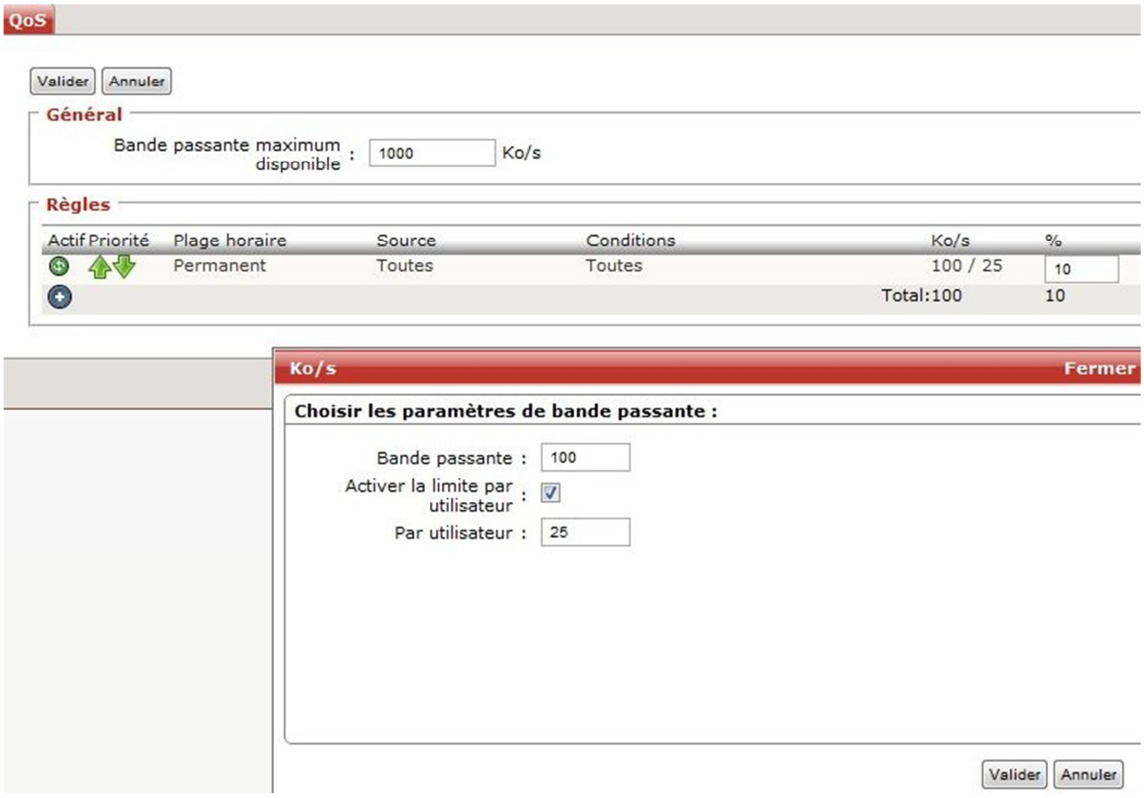


Figure 49 : Gestion de la QoS avec Olfeo (Olfeo)

A l'aide de cet outil, il serait possible pour le CH de Montbert de déterminer les flux qui seraient les plus prioritaires, comme l'accès au logiciel de gestion de planning, des flux vers des organismes ou institutions liées au pilotage économique de l'établissement, des autres flux Internet plus classiques.

La mise en œuvre de l'ensemble des politiques au niveau de la passerelle assure une gestion centralisée des flux Internet et l'optimisation des accès. L'évaluation sur le site de Montbert m'a également permis d'utiliser les fonctionnalités de rapports de la solution Olfeo.

6.3.3.4 Supervision, rapports et analyse des comportements

Olfeo assure la sécurisation des flux de navigation Internet et trace par conséquent l'intégralité des requêtes qui lui sont soumises. A partir de ces données, des outils sont mis à disposition pour avoir une visualisation rapide sur la nature des flux.

Tout d'abord, à l'ouverture de l'interface d'administration, un tableau de bord, personnalisable, est présenté pour prendre rapidement connaissance des flux du moment. Mais, Olfeo dispose surtout d'un module de rapports et d'analyses très performant. Les rapports sont des documents synthétiques de l'activité sur la passerelle, sur des thèmes fréquemment consultés.

Figure 50 : Liste de rapports disponibles à la consultation

Les analyses sont utilisées pour effectuer des recherches plus précises et de manière plus exceptionnelles.

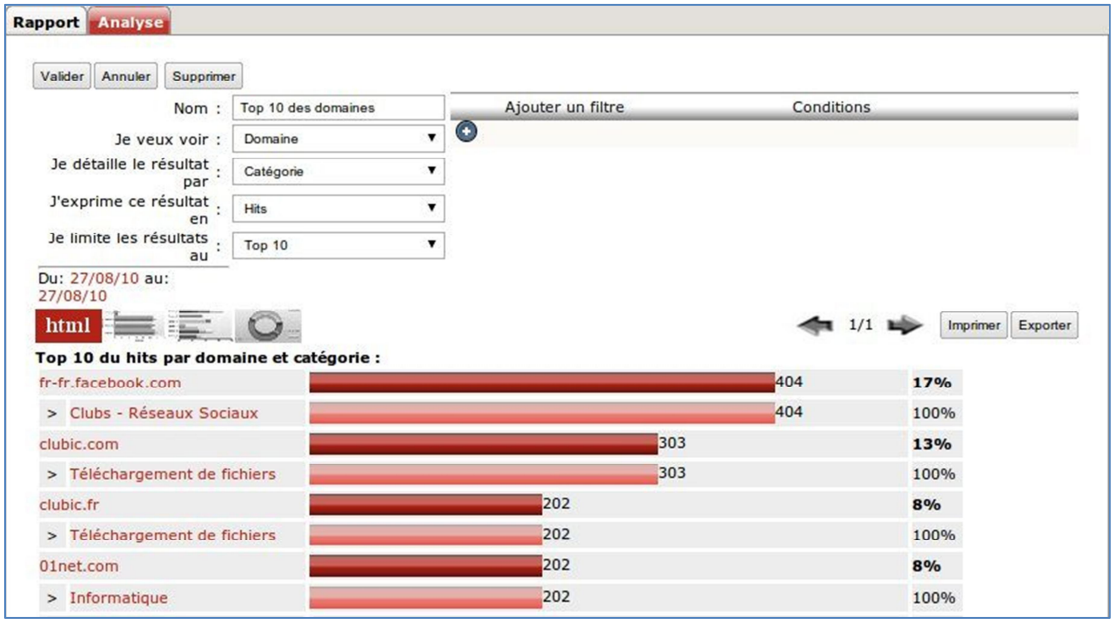


Figure 51 : Exemple d'analyse avec Olfeo

Les libellés des critères de sélection posent des questions précises sur le rapport à définir. Des filtres complémentaires peuvent être ajoutés pour afficher des statistiques sur des éléments recherchés très précisément. Il existe plusieurs types de rapports et d'analyses ; sur les urls, les protocoles, les menaces et le temps passé par utilisateur. Toutes ces informations sont enregistrées directement sur le disque dur de la passerelle, mais elles peuvent aussi être externalisées pour augmenter la durée de rétention.

Olfeo dispose d'un module de diffusion et de « coaching » qui est chargé d'émettre les rapports d'activités programmés aux administrateurs, gestionnaires ou utilisateurs, par messagerie électronique, à des fréquences prédéfinies. Le module de « coaching » est particulièrement intéressant car il permet de transmettre à un utilisateur les statistiques de ses navigations Internet.

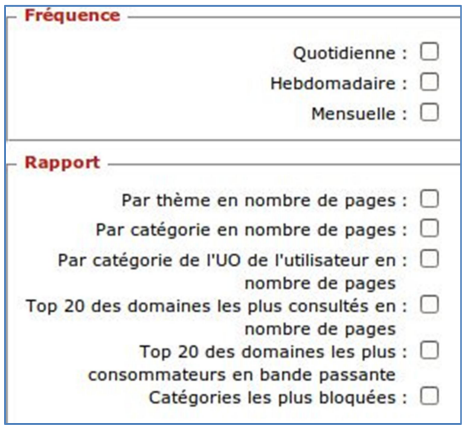


Figure 52 : Paramètres du « coaching » pour un utilisateur

L'objectif de cet outil est de responsabiliser les utilisateurs dans leurs navigations en les informant de leurs statistiques. L'utilisation de la connexion Internet sur leur lieu de travail à des fins non professionnels est autorisée, dans des limites qui doivent rester raisonnables et définies dans la charte informatique. L'activation de cette fonctionnalité au niveau utilisateur cherche à influencer celui-ci et lui demander intuitivement de restreindre les navigations non professionnelles.

Enfin, du point de vue administrateur, l'éditeur fournit les fichiers de description des alertes qui sont remontées vers des applications de supervision du type « nagios », dont le CH de Montbert est équipé. La consultation des flux en temps réel est aussi accessible, mais difficilement exploitable à cause de la vitesse importante de défilement.

L'évaluation de la solution Olfeo en version « appliance » a mis en évidence les caractéristiques du produit et des fonctionnalités utiles.

6.3.3.5 Bilan de l'évaluation

L'évaluation de la solution Olfeo sur une période d'un mois, intégrée dans l'environnement du CH de Montbert s'est révélée très instructive. Des remarques ou améliorations peuvent néanmoins être prises en considération. L'exploitation des données sur cette période a révélé des comportements et habitudes de navigation méconnus, problèmes déjà rencontrés au travers du retour sur expérience de deux Centres Hospitaliers avec cette solution.

Tout d'abord, l'utilisation d'Olfeo est intuitive et ergonomique. Cet aspect est important car dans le cas du CH de Montbert avec une petite équipe informatique, il est nécessaire de trouver rapidement les éléments recherchés, sans perte de temps à se réapproprier le produit à chaque connexion. La synchronisation périodique de groupes prédéfinis avec l'annuaire Active

Directory apporte la possibilité d'authentifier da manière transparente ou explicite les utilisateurs et ainsi répondre aux exigences réglementaires concernant la conservation des traces. Le moteur de règles, associé aux politiques d'accès, est puissant et offre des possibilités de personnalisation des accès afin de répondre aux spécificités des clients, à l'image de la problématique des services qui nécessitent des accès particuliers. Cependant, une attention particulière doit être portée sur l'ordonnancement des règles afin de ne pas créer de conflits ou effets de bords.

Le filtrage des urls est performant et adapté aux habitudes de navigation des utilisateurs français, via un référencement manuel des pages. Le filtrage protocolaire proposé par Olfeo est aussi très performant et couvre un très grand nombre de protocoles existants. Cet outil analyse jusqu'à 8 niveaux le contenu des trames à la recherche d'encapsulation ou de transfert d'information non autorisé. Il a permis de mettre en avant l'existence de flux de messagerie instantanée, théoriquement bloqués par la solution en place. L'antivirus, développé par Olfeo, assure la sécurisation des contenus transférés en s'appuyant sur les signatures de virus de l'éditeur ClamAV. Néanmoins, Olfeo n'est pas un éditeur spécialisé dans les antivirus. Des doutes quant aux performances de détection de ce module peuvent exister. La conservation de la solution Trend Micro IWSVA avec seulement le module antivirus est à étudier pour renforcer la sécurité.

Cependant, la mise en œuvre de la totalité de ces analyses peut entraîner des dégradations de performances de l'appliance et donc de disponibilité auprès des utilisateurs. Il est néanmoins envisageable de déployer une version logicielle d'Olfeo, sur une machine virtuelle par exemple et de dédier ce serveur à des tâches spécifiques pour soulager la passerelle principale. Les gestions de proxy (http, ftp, …), de cache et de qualité de services apportent des outils complémentaires indispensables pour disposer d'une solution complète de filtrage. En effet, la section QoS pourrait permettre au CH de Montbert de déployer une priorisation des flux en fonction de leur destination. Ainsi, les accès aux sites de gestion de planning, gestion financière ou de gestion stratégiques (ARS, gouvernement, …) pourraient être prioritaires sur les autres navigations. Du point de vue sécurisation physique, la mise en cluster de la solution avec l'utilisation de deux passerelles apporte la garantie de s'affranchir des pannes matérielles et augmente la disponibilité de la solution et par conséquent du service aux utilisateurs.

Cette simplicité est aussi présente au travers l'exploitation des rapports et analyses. En effet, il suffit de répondre aux questions posées pour obtenir les résultats. L'ajout de filtre est disponible pour affiner le niveau de recherche dans les données. Différentes mises en formes graphiques

sont proposées. Cette période d'évaluation a mis en évidence les habitudes de navigation des usagers au CH de Montbert. Ainsi, j'ai constaté (Annexe I) une fréquentation importante sur les sites de la catégorie « Bande passante », du type, Facebook, Youtube, Twitter, alors qu'ils devraient être bloqués par la solution en place. J'ai particulièrement apprécié la mise à disposition de la catégorie « Risque pénale », qui présente les statistiques entraînant la responsabilité des utilisateurs et par conséquent celle de l'établissement. Les analyses protocolaires montrent aussi l'existence de flux de messagerie instantanée (Messenger, Yahoo messaging, …), encapsulés dans les flux Internet (Annexe I). Les résultats démontrent l'inefficacité de la solution déployée. Les volumes de pages web transférés par jour (Annexe I) sont supérieurs à 2Go du lundi au vendredi et autour de 1 Go le week-end. Ces données résultent de l'analyse des flux au mois de juillet 2011, pendant la période des vacances scolaires. Il est à supposer que ces valeurs sont certainement supérieures hors vacances. Enfin, les statistiques de temps passé par utilisateur offrent une visualisation précise du temps consacré à la navigation par agent. La fonction de coaching disponible, une fois activée, diffuse périodiquement, les rapports de navigation à l'utilisateur sélectionné. Cette fonctionnalité est très utile et est complémentaire à celle qui consiste à diffuser les chartes d'information directement à partir de la solution. Chacun est alors responsabilisé dans ses usages et ne peut nier l'existence de ces documents.

Enfin, le produit Olfeo a été choisi et déployé, entre autres, sur les centres hospitaliers de Saint Nazaire et Le Mans avec une grande satisfaction. En effet, les problématiques étaient similaires à celles rencontrées au CH de Montbert. La mise en place s'est échelonnée sur plusieurs mois avec des analyses des flux et des reconfigurations successives pour optimiser la sécurité. Ce travail a été complété par une révision de la charte Internet pour l'adapter au nouvel outil, mais aussi par des campagnes d'informations fortes afin de rappeler aux utilisateurs leurs responsabilités sur le lieu de leur activité professionnelle. Depuis la mise en marche, des modifications des usages ont été constatées, même si avec le temps, des tendances à l'oubli apparaissent. Il convient alors de rappeler régulièrement les règles, de manière globale ou plus précise avec la fonction de coaching. Les chefs de projets ont insisté sur le fait que la mise en place de cette solution devait impérativement être appuyée par la direction pour aboutir. Cela ne doit pas être un projet interne au service informatique, car des difficultés sont toujours été rencontrées pour faire accepter ce filtrage et la traçabilité associée, malgré des obligations réglementaires. Ces deux établissements sont extrêmement satisfaits de la solution, qui leur a permis de prendre en compte toutes les spécificités de leurs activités.

En conclusion, la solution Olfeo est la solution qui serait la plus pertinente à installer au CH de Montbert pour répondre aux problématiques actuelles, réglementaires et fonctionnelles. De nombreuses fonctionnalités sont disponibles pour optimiser les usages. Cependant, la mise en place d'un tel produit doit s'accompagner de démarches administratives, notamment concernant la charte, mais aussi de communication afin d'obtenir l'approbation des usagers qui ne doivent pas considérer cet outil pour du « flicage » mais comme un véritable outil de sécurisation.

7 Le filtrage des flux de messagerie

La sécurisation des flux de messagerie est un travail quotidien, car les spammeurs s'adaptent très rapidement aux nouvelles technologies de lutte contre le spam. Sur l'année 2010, 84.3% des messages électroniques ayant transités sur les réseaux étaient du spam et 90% d'entre eux contenaient des liens vers des sites malveillant [CROTTY]. Les courriers illégitimes sont donc aujourd'hui encore un point d'entrée sur les ordinateurs, dans le but d'extraire le maximum de données possible. Les analyses à partir de base de réputation sont devenues inefficaces, car ces courriers sont devenus partie intégrante d'attaques de plus grande envergure, par l'association des spams à des composants Web et de données. Ainsi les spammers profitent de la nature dynamique d'Internet pour créer des attaques en temps réel.

Dans ce contexte, le CH de Montbert souhaite revoir les stratégies actuelles et rechercher une solution performante pour sécuriser son réseau contre ces attaques, au travers de tests. Dans cet objectif, j'ai procédé à l'évaluation de deux solutions.

7.1 Description de l'architecturé existante

A l'image de l'architecture décrite pour les flux Internet, les courriers électroniques transitent tous par le même serveur proxy. Celui-ci héberge donc les solutions de sécurisation des flux de l'ensemble de l'établissement. L'application logicielle déployée est celle de l'éditeur Trend Micro, dénommée Interscan Messaging Security Server (IMSS). Elle est associée à un service de filtrage de l'opérateur Gigalis, à un serveur de messagerie libre Postfix et à la solution libre SpamAssassin pour détecter les courriers indésirables (Annexe J).

L'établissement est client du fournisseur d'accès à Internet GIGALIS. Celui-ci est chargé d'acheminer les flux Internet et de messagerie, mais aussi d'interconnecter via le réseau Internet tous les sites distants. Le CH de Montbert a de plus souscrit aux services de relai SMTP et d'anti spam. Ce filtre anti spam effectue alors une sélection des messages à transmettre avant qu'ils ne

soient délivrés à l'établissement. Un email d'alerte est envoyé aux utilisateurs quotidiennement pour les prévenir que des messages considérés comme spams sont bloqués sur une plateforme dédiée. A charge de chaque agent de consulter cette zone de quarantaine et de débloquer les faux-positifs. Pour plus de sécurité, seuls les courriels provenant des serveurs de GIGALIS sont autorisés à être délivrer sur notre serveur proxy, pour y effectuer de nouvelles analyses.

Spam Assassin est une application libre très utilisée dans la lutte contre le spam. Elle est intégrée au serveur proxy afin de filtrer autant que possible les courriers légitimes des illégitimes avant la remise dans la boîte aux lettres de l'utilisateur. Chaque courrier entrant est soumis à différentes méthodes de détection de spams parmi celles étudiées précédemment (filtre bayésien, expressions rationnelles, RBL, …). Chaque filtre génère un score. La moyenne de tous les scores est comparée à la limite définie par les administrateurs afin de déterminer si le message est légitime ou non.

Le serveur de messagerie Postfix est utilisé au CH de Montbert comme un relai de messagerie. En effet, tous les messages en provenance des serveurs Gigalis sont routés par le pare-feu dans la zone DMZ. Une fois les traitements antispam réalisés, le serveur proxy renvoie les messages vers le serveur de messagerie si le courrier est légitime, ou en zone de quarantaine hébergée sur la plateforme IMSS dans le cas contraire.

Enfin, le CH de Montbert autorise la consultation des boîtes aux lettres des agents depuis l'extérieur de l'établissement, via un webmail. Un accès direct est configuré sur le pare-feu afin d'accéder au serveur de messagerie situé sur le réseau interne. Or, à ce jour, aucune solution de sécurisation n'est déployée pour analyser les flux de messagerie interne. Cette faille de sécurité est majeure, car la plupart des attaques ou des vols de données sont réalisés depuis des sources internes.

L'architecture de sécurisation des flux de messagerie aujourd'hui déployée se concentre principalement sur la détection des virus et peu sur la lutte contre le spam. Or, la solution doit-être améliorée notamment concernant la lutte contre le spam, les programmes malveillants et les échanges internes.

7.2 La méthodologie mise en œuvre

A l'image des tests de sécurisation des flux Internet j'ai souhaité pouvoir évaluer de nouveaux produits pour sécuriser les échanges de courriers électroniques, sur une période prédéfinie. L'infrastructure virtuelle existante sera mise à disposition pour créer de nouvelles machines

virtuelles. L'intégration d'un boitier complémentaire en lieu et place d'un serveur virtuel aurait pu être possible. Cependant, pour des contraintes de planning je n'ai pas évalué ce type d'architecture.

La mise en place de ces périodes de tests impose de modifier ou de compléter la configuration réseau existante. Tout d'abord, il s'agit de traiter les messages sortants de l'établissement. L'adresse IP du nouveau relai SMTP doit être renseignée directement sur le serveur Microsoft Exchange, afin que celui-ci transfert les messages vers la plateforme de sécurisation, située en zone DMZ. Il s'agit ensuite de gérer les messages entrants. Ceux-ci doivent être réorientés vers le serveur de tests pour être analysés. Lui-même les remettra au serveur de messagerie, si le message est considéré comme valide qui se chargera de la distribuer dans la boîte aux lettres de son destinataire. Pour réaliser ce changement, l'adresse IP du nouveau serveur est configurée directement sur le firewall pour recevoir tous les messages adressés au domaine « ch—montbert.fr ». Les modules de détection de spams des différents éditeurs seront mis en œuvre, en complément de filtrage déjà effectué par le service de notre fournisseur d'accès GIGALIS.

La modification des règles de transports des messages impacte l'ensemble de l'établissement, par la redirection de tous les courriers vers la plateforme de tests. Tout d'abord, le fonctionnement du relai SMTP devra être validé pour l'ensemble des messages sortants. Dans un second temps, les messages entrants seront redirigés vers le nouveau serveur. Enfin, les politiques de filtrage seront optimisées au fil des jours, notamment pour la lutte contre le spam.

7.3 Comparatifs de solutions du marché

7.3.1 La solution Trend Micro

La société Trend Micro développe des produits destinés à sécuriser les flux Internet, mais aussi les flux de messagerie électronique. La plateforme IMSVA est la solution qui doit répondre aux évolutions des attaques par courriels et lutter contre le spam.

7.3.1.1 Architecture cible et licences logicielles

Afin d'évaluer la plateforme Trend Micro IMSVA j'ai créé une nouvelle machine virtuelle sur l'infrastructure de l'établissement. Celle-ci est identique à celle réalisée pour les maquettes de sécurisation des flux Internet. En effet, Trend Micro fournit le même système d'exploitation, CentOS et les applications, disponibles en téléchargement sur le site Internet. La mise en place s'effectue en suivant les différentes étapes de l'assistant d'installation. Enfin, la machine virtuelle est placée dans la zone « DMZ » du réseau, afin de se trouver entre le réseau Internet et

le réseau interne de l'établissement (Annexe K). Tous les messages électroniques transitent alors par cette passerelle et font l'objet d'analyses multiples pour sécuriser les destinataires et expéditeurs.

La société Trend Micro a fourni des licences d'évaluation de 60 jours. Toutes les fonctionnalités embarquées dans la solution sont activées au travers de quatre types de licences : le « cloud pre-filter », l'antivirus et le filtre de contenu, une solution anti spam et enfin un module de filtrage des adresses IP. Tous ces éléments nécessitent une configuration spécifique pour optimiser la sécurisation des flux de courriers électroniques.

7.3.1.2 Configuration de la solution IMSVA

La configuration initiale de la passerelle est effectuée à l'aide d'un assistant, qui nous guide au travers des différentes étapes d'initialisation de la plateforme.

Tout d'abord il est nécessaire de configurer différents paramètres réseaux de la plateforme : adresse IP, masque, serveurs DNS externes, passerelle pour l'accès à Internet, serveur de temps. Par mesure de sécurité, j'ai créé de nouvelles règles de routage en parallèle de celles existantes sur le pare-feu, dédiées à la gestion de ces flux de qualifaication. Ensuite, j'ai configuré les paramètres de déploiement. IMSVA utilisée comme passerelle, propose un service de gestion des messages en quarantaine par les utilisateurs. L'activation de ces options est modifiable par la suite à partir de l'interface de management.

Puis, j'ai défini les paramètres de routage des messages au sein de l'application. Le paramètre « Relay Domain » spécifie que les messages à destination d'utilisateurs externes doivent obligatoirement être émis par un utilisateur du domaine « ch-montbert.fr ». Dans le cas contraire, les messages seront bloqués. Cette sécurité permet de ne pas utiliser la plateforme comme relai de messagerie anonyme et ainsi d'interdire aux spammers l'utilisation de ce serveur pour le transit de leurs spams. En complément, le paramètre « Domain Based Delivry » définit le serveur de messagerie vers lequel doivent être transmis tous les messages à destination du domaine cible, afin d'être livrés dans les boîtes aux lettres. Tous les messages n'étant pas émis à destination de ce domaine ne sont pas traités. La configuration peut-être poussée jusqu'à interdire à certains clients l'envoi de message par exemple, ou alors d'imposer une authentification via l'option « Transport Layer Security » (TLS), qui permet de sécuriser les communications entre deux serveurs à l'aide d'un cryptage connu et d'un certificat SSL :

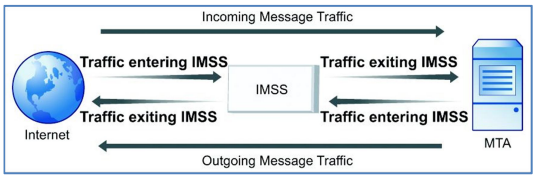


Figure 53 : Communication sécurisée TLS avec IMSVA (Trend Micro)

En complément du trafic SMTP, il faut aussi se préoccuper des flux potentiels s'appuyant sur d'autres protocoles, comme POP3. En effet, un utilisateur pourrait à partir d'un client messagerie de l'établissement se connecter à un serveur de ce type et télécharger ses messages sur le poste de l'établissement sans contrôles de sécurité.

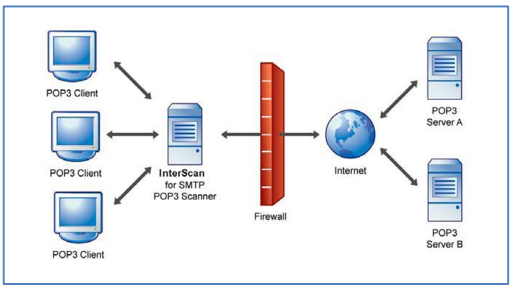


Figure 54 : Analyses des messages avec le protocole POP3 (TREND MICRO)

Toutes les connexions POP3 issues des clients vers l'extérieur sont bloquées au niveau du pare-feu. Seules les connexions des clients vers IMSVA sont autorisées. Avec cette architecture, il est alors possible de scanner tous les messages qui transitent sur ce protocole.

Enfin, l'assistant demande de renseigner différents champs pour finaliser l'installation. Ainsi, le serveur de messagerie utilisé pour l'envoi des notifications et des alertes est à renseigner. Les sources de mises à jour d'IMSVA doivent être téléchargées sur les serveurs de Trend Micro afin de disposer des dernières versions. J'ai également configuré l'interconnexion avec l'annuaire LDAP de l'établissement pour permettre l'authentification des destinataires et disposer de rapports précis.

Ces configurations effectuées ne sont cependant pas optimisées pour l'établissement. En effet, les règles de lutte contre le spam et les programmes malveillants ne sont pas mises en œuvre. De nouvelles règles doivent alors être définies afin d'appliquer les stratégies souhaitées au CH de Montbert.

7.3.1.3 Exploitation et optimisation

La solution IMSVA est livrée avec des stratégies de détection des programmes malveillants et du spam pré-configurées et générales. L'établissement doit alors impérativement personnaliser cette configuration afin de l'adapter aux caractéristiques de ces flux.

Le fonctionnement d'IMSVA s'appuie sur des règles, appliquées à tous les messages entrants et sortants de l'établissement. Celles-ci sont de deux types : la protection « antivirus globale » et « autres ».

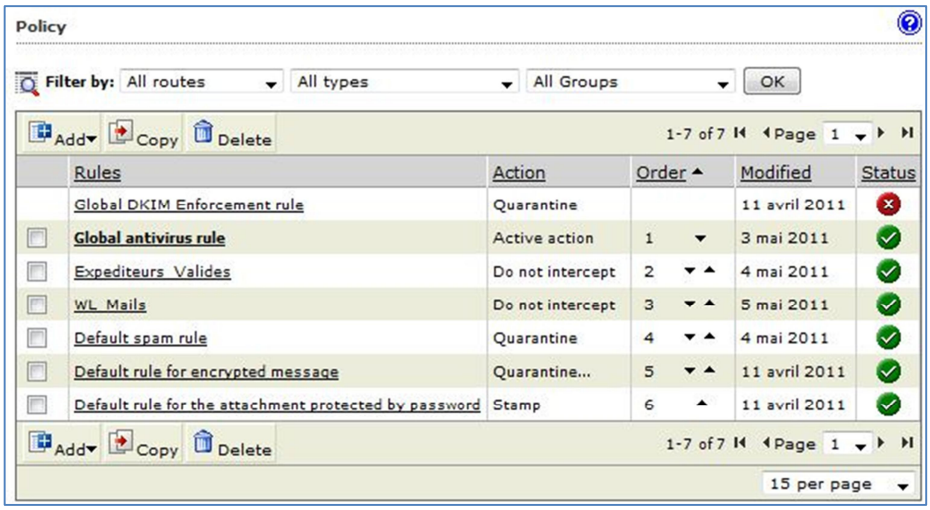


Figure 55 : Règles définies sur le CH de Montbert

Trend Micro conseille de placer la règle antivirus comme la première à exécuter pour détecter aussitôt les dangers potentiels et les traiter. Lorsqu'un message à délivrer arrive sur la plateforme, celle-ci vérifie les conditions spécifiées et applique si besoin les actions à mener, comme l'illustre la figure ci-dessous :

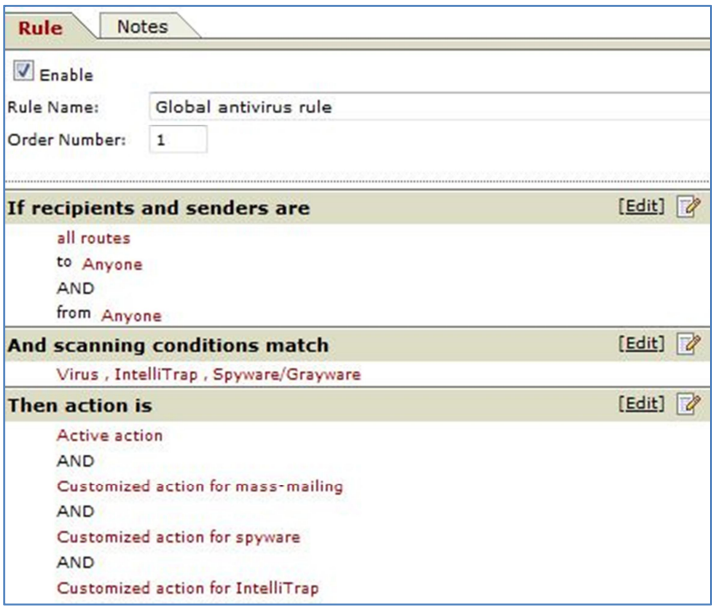


Figure 56 : Définition de la stratégie antivirus sur IMSVA

La section « And scanning conditions match » permet de déterminer les éléments à rechercher dans le message pour le considérer comme sûr.

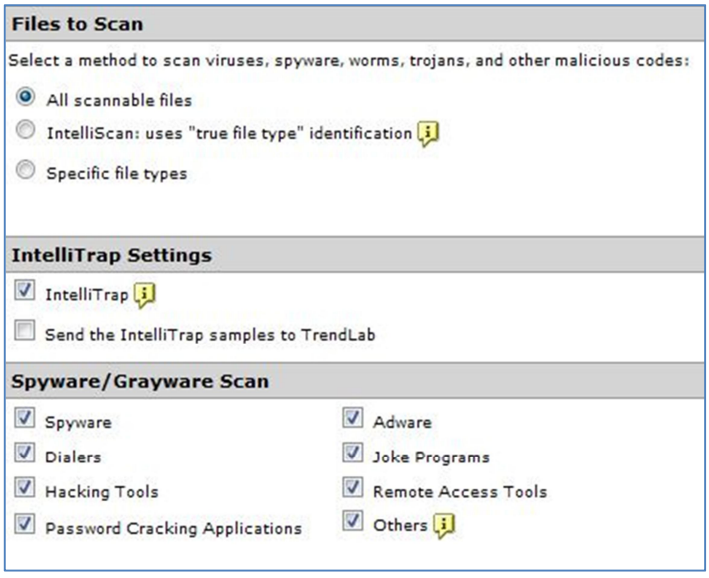


Figure 57 : Conditions d'analyse d'un message électronique

En fonction des résultats des conditions précédentes, il faut déterminer les actions à appliquer suivant les cas. Dans cette stratégie, j'ai demandé la mise en quarantaine du message, dans l'attente de décision de l'administrateur. L'objet est aussi modifié pour avertir du danger potentiel et une notification de violation de la sécurité est envoyée aux administrateurs et aux destinataires.

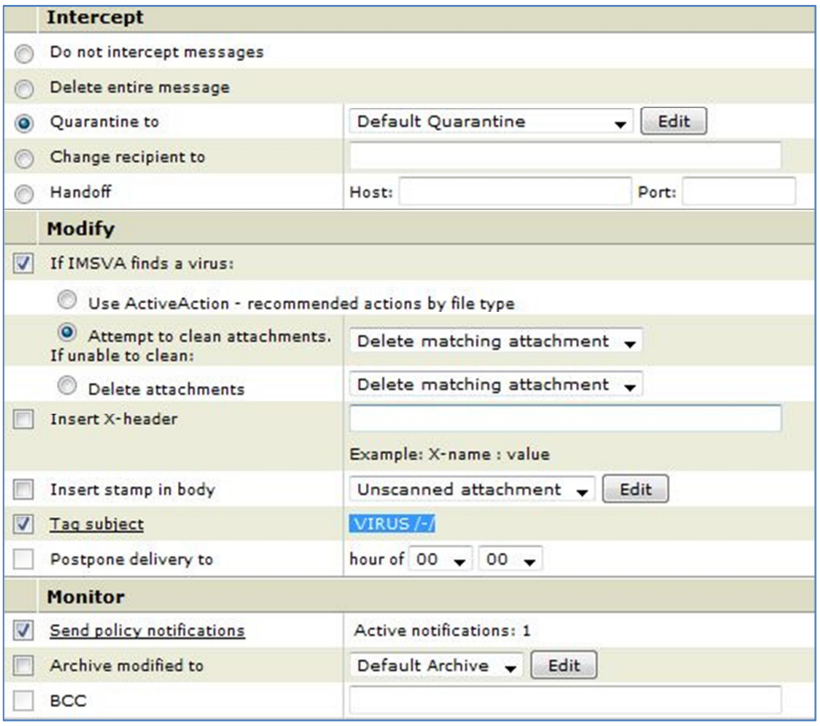


Figure 58 : Actions menées suite à une détection virale.

Cependant, la détection des virus ne permet pas de lutter contre le spam. Il convient alors de créer d'autres règles qui sont chargées de détecter les messages indésirables.

Trend Micro a mis en place une architecture de prévention contre les pourriels multi-couches et a intégré dans ses outils de détections différentes techniques de filtrage. Le but est d'identifier le plus tôt possible d'éventuels spams, en utilisant toutes les solutions connues à ce jour :

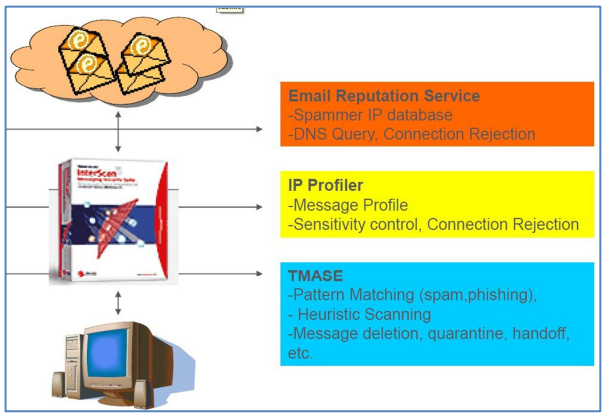


Figure 59 : Architecture de prévention contre les spams (TREND MICRO)

Le service de réputation des courriels bloque les spams avant leur arrivée sur la plateforme, grâce à l'utilisation de bases de données statiques et dynamiques RBL. Le module « Cloud Pre—Filter » doit être configuré et activé pour réaliser ce premier niveau de filtrage.

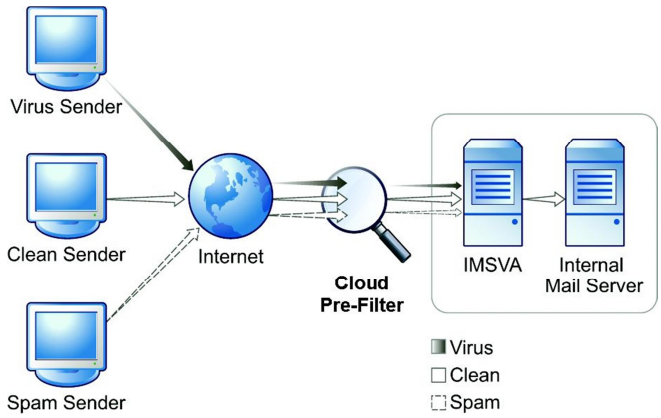


Figure 60 : Flux de messagerie avec Cloud Pre-Filter (TREND MICRO)

Le module de filtrage en ligne analyse donc les messages puis transmet vers IMSVA les messages validés, via SMTP. Les opérations de configuration et d'exploitation de ce module sont réalisées par https. Le principe consiste à définir des règles de filtrage directement dans ce filtre en ligne, comme cela a été fait pour l'antivirus précédemment et de les activer. Ce module fournit des outils de rapports et une quarantaine. Il enregistre les traces dans des journaux, comme le fait IMSVA. Il faut alors mettre en place des procédures d'exploitations et de maintenance complémentaires à IMSVA. Cependant, cette architecture fonctionne uniquement si tous les messages sont routés vers ce filtre. Il est alors impératif de créer un nouvel enregistrement MX pour mettre en œuvre cette redirection, avec un poids plus fort que l'enregistrement existant, ou alors de modifier celui utilisé. La mise en œuvre de ce module peut-être une contrainte dans le cas ou la bande passante est faible ou limitée. En effet, le trafic réseau est amplifié par les échanges entre le « cloud » et IMSVA. De plus, Trend Micro recommande, suite à l'activation de cette option, de désactiver le module « IP Filtering », soumis à licence, si cette stratégie est déployée. L'éditeur justifie cette action car ce service est redondant avec le module « IP filtering » et augmente les temps de latence dans la remise des messages.

Si l'on souhaite activer la licence « IP filtering », il est possible de définir des actions en fonction des serveurs qui émettent les courriels à analyser. Ce service s'appuie sur deux composants : un filtre de réputation des courriels qui bloque les serveurs expéditeurs à la source

et un profilage IP qui aide à protéger le serveur de messagerie des attaques extérieures en bloquant des adresses IP spécifiques si nécessaire.

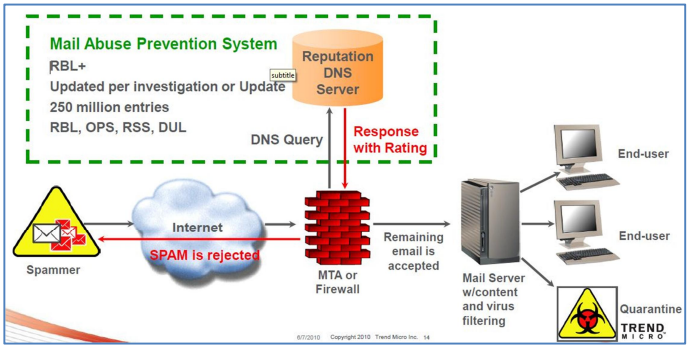


Figure 61 : La technologie IP Filtering (Trend Micro)

Cette licence active également le module « Spam Prevention Protection » qui apporte des outils complémentaires pour détecter les spams. L'opérateur Gigalis fournit au CH de Montbert un service anti spam qui effectue déjà une détection des spams avant leur arrivée sur IMSVA. Les messages reçus proviennent uniquement des serveurs Gigalis, dont les adresses IP sont connues. Il convient de les renseigner dans la liste « Approuved List » d'IMSVA pour autoriser tous les éléments provenant de ces adresses. A l'inverse, il est possible d'interdire des domaines ou des adresses IP de serveurs de délivrer leurs courriels sur IMSVA, si ceux-ci sont connus pour leur rôle dans la diffusion de spams. Pour nous aider à détecter ces serveurs, le service « Suspicious IP » permet de retrouver sur un intervalle de temps donné, tous les serveurs ayant émis des courriels vers notre plateforme. Selon leur activité, il est alors possible de les bloquer temporairement ou bien définitivement. La détection de ces serveurs est effectuée après configuration d'une règle comme celle-ci :

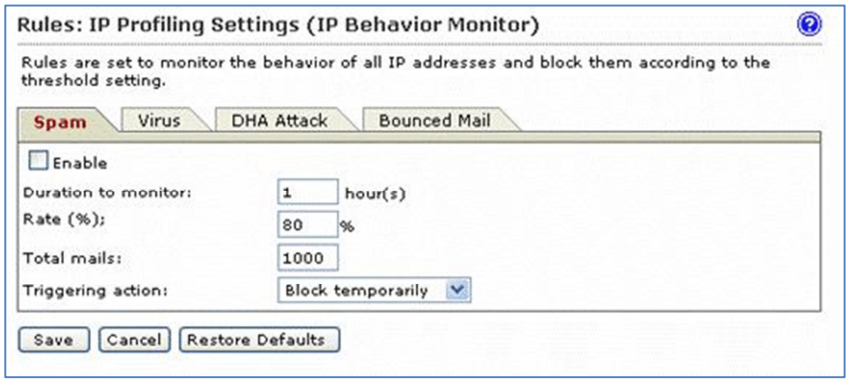


Figure 62 : Configuration de détection d'un serveur potentiel de spam

L'objectif est alors de surveiller pendant une heure le nombre de spams émis par ce serveur par rapport au nombre de courriels reçus de ce même serveur. Si le taux calculé est supérieur à 80%, on détermine l'action à exécuter, c'est-à-dire un blocage temporaire du serveur émetteur. Cette option est inutile dans notre cas, car seuls deux serveurs nous relaient des messages et doivent être toujours autorisés, sinon aucun message ne serait délivré. L'arrêt du service anti spam de Gigalis prochainement devrait redonner un but à cette fonctionnalité. Mais la lutte contre les pourriels est aussi réalisée au travers de règles propres à l'établissement.

Afin de détecter le plus fidèlement possible les spams, Trend Micro fonctionne à partir de règles basées sur le même principe que pour les analyses virales. Chaque règle exécute une procédure spécifique suivant des conditions d'entrée, les résultats et les actions à mener. Il est alors possible de personnaliser le filtrage. Les règles sont exécutées les unes à la suite des autres, comme ci-dessous.

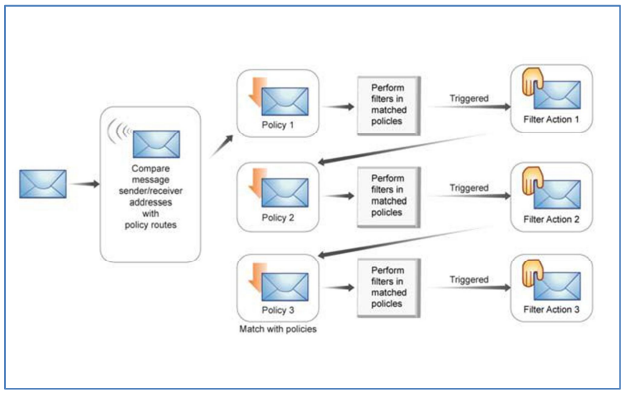


Figure 63 : Processus d'analyse des messages (Trend Micro)

La configuration d'une règle est relativement simple. Il s'agit d'analyser tous les messages à destination d'un utilisateur du domaine « ch-montbert.fr » et en provenance d'expéditeurs inconnus. Ainsi, seuls les messages à destination d'utilisateurs existants dans l'annuaire Active Directory sont traités et si ce n'est pas le cas, un message d'erreur est renvoyé à l'expéditeur.

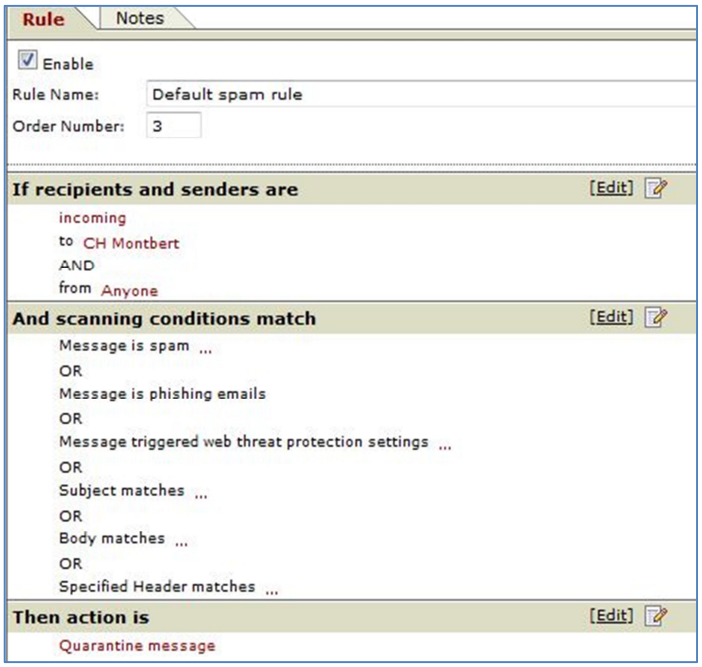


Figure 64 : Création d'une règle de détection des spams

Puis, il est nécessaire de définir les conditions ou les catégories sur lesquelles vont porter les traitements : spams, web réputation, contenu, pièce jointe, taille, autres. Dans chacune, des options sont à activer, afin de configurer des listes d'expéditeurs ou de domaines approuvés, bloqués, des exceptions ou bien encore des listes de mots-clés ou expressions rationnelles préalablement définis. Le moteur de détection des spams de Trend Micro s'appuie sur le filtrage bayésien et sur une analyse des contenus pour décider si un message est un spam. La liste des règles à définir est propre à chaque établissement Chacun doit personnaliser ses filtres afin d'obtenir un filtrage le plus performant possible.

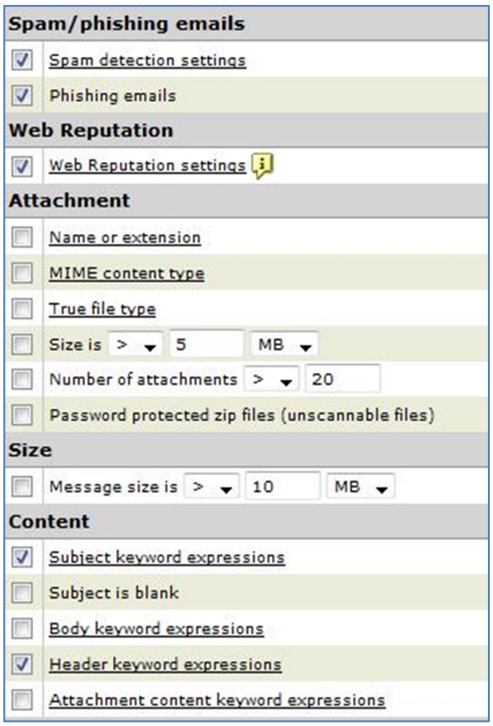


Figure 65 : Critères de détection des spams

Enfin, suite à ces différentes analyses, un score est déterminé par le moteur de scan. En fonction de la valeur de ce score, les actions choisies sont appliquées. Dans la plupart des cas, le message considéré comme spam est placé en zone de quarantaine. L'objet peut-être modifié pour y inclure un code en avertissement, comme « SPAM ? / ». Une notification peut également être transmise axu destinataires ou aux administrateurs.

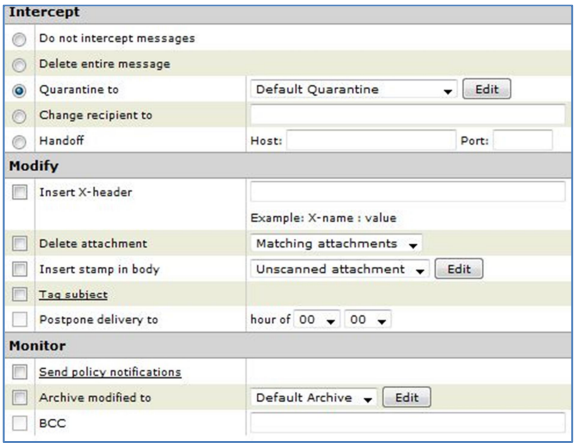


Figure 66 : Actions à appliquer si détection de spams

Pour être performant, le moteur de détection des spams doit passer par une phase d'apprentissage, pour s'adapter aux types de messages qui transitent sur la plateforme. Une

vérification régulière des stratégies déployées et leur efficacité est impérative, car les spammers s'adaptent aux différentes techniques de détection. La solution doit alors être réactive et être capable de s'adapter au fur et à mesure de l'évolution des messages.

Le déploiement de la solution IMSVA pendant plusieurs semaines a permis d'évaluer pleinement le produit et de constater ses qualités et défauts.

7.3.1.4 Bilan des tests de maquettage

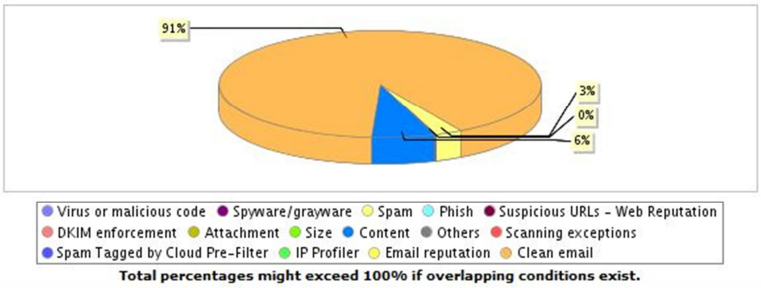
Le CH de Montbert utilise depuis plusieurs années une version antérieure, couplée à un autre système de détection des spams. La nouvelle plateforme testée ici se montre plus performante et intègre de nouvelles fonctionnalités, mais présente aussi des faiblesses.

L'architecture en trois niveaux proposée par Trend Micro permet d'analyser les flux de messages depuis le serveur expéditeur jusqu'au poste client. Le réseau SPS est largement mis à contribution et le module « Cloud Pre-Filter » utilise ces résultats disponibles en temps réel pour affiner ses traitements. La plateforme analyse alors les flux avec les dernières informations disponibles sur les sources de spams. La qualité du filtrage est donc optimale. Cependant, cette interactivité génère du trafic réseau et donc de la bande passante. Or, dans le cas du CH de Montbert, cette problématique est importante car la bande passante disponible est faible. Ce dialogue permanent avec des serveurs distants s'ajoute aux flux quotidiens des sites distants et peut alors impacter l'ensemble de l'établissement. Il est conseillé de déployer cette technologie lorsque les ressources réseaux disponibles sont conséquentes. De plus, il faut mettre en place une double gestion. En effet, la maintenance doit être assurée sur la plateforme IMSVA du site, mais aussi sur celle disponible sur le « cloud Pre-Filter ». Il y a par conséquent deux quarantaines distinctes à gérer, ce qui peut s'avérer long et difficile pour les utilisateurs, dont ce n'est pas le cœur de métier.

Le second niveau assure une détection des serveurs potentiellement dangereux et offre des outils afin de les limiter ou les bloquer, via le module « IP Filtering ». Cette technologie s'avère très utile pour détecter les attaques virales, de spams ou de type bounce et par conséquent les serveurs de messagerie. L'utilisation de liste blanche et noire propre à l'établissement permet de personnaliser la protection en fonction des flux émis ou réceptionnés. Les besoins doivent être parfaitement déterminés afin de ne pas acquérir une licence pour le module « IP filtering » qui ne serait pas utilisé ! De plus, si un traitement antispam est déjà effectué par le FAI, comme dans le cas du CH de Montbert, cette fonction est inutile car l'intégralité des messages qui arrivent sur la plateforme sont toujours émis par les serveurs du FAI.

Enfin, le dernier niveau de filtrage se situe directement sur la solution IMSVA, avec les traitements effectués par le moteur de scan. Différentes techniques de filtrage sont associées (filtre bayésien, mots-clés, expressions rationnelles, web réputation) afin de détecter au mieux les spams et de limiter les faux-positifs. L'évaluation a conduit à créer des groupes de mots ou d'expressions spécifiques aux flux du CH de Montbert qui ont ensuite été utilisés dans des règles de filtrage. Malgré ces tentatives de personnalisation, il s'avère que certains types de messages sont difficiles à traiter, comme les listes de diffusion ou bien les messages publicitaires, ne sachant si ces messages doivent être considérés comme spams ou non. J'ai aussi constaté que l'analyse du contenu génère beaucoup de faux-positifs. Une attention forte est alors à porter sur la zone de quarantaine, ce qui n'est pas la démarche première des utilisateurs de l'établissement.

Traffic Summary	Total		Incoming	Outgoing
Total # of messages	3435		3197	238
Total size of messages (MB)	443.165		343.764	99.402



Total percentages might exceed 100% if overlapping conditions exist.

Scanning Conditions	Total	Message %	Incoming	Outgoing
Total message count	3435	100.00	3197	238
Virus or malicious code	0	0.00	0	0
Spyware/grayware	0	0.00	0	0
Spam	93	2.71	93	0
Phish	0	0.00	0	0
Suspicious URLs - Web Reputation	4	0.12	4	0
DKIM enforcement	0	0.00	0	0
Attachment	0	0.00	0	0
Size	0	0.00	0	0
Content	219	6.38	219	0
Others	0	0.00	0	0
Scanning exceptions	0	0.00	0	0
Spam Tagged by Cloud Pre-Filter	0	0.00	0	0
IP Profiler	0	0.00	0	0
Email reputation	0	0.00	0	0
Clean email	3124	90.95	2886	238

Figure 67 : Bilan hebdomadaire des flux de messagerie sur le CH de Montbert

Après analyse de ce rapport, on constate que la messagerie du CH de Montbert est principalement utilisée pour recevoir, mais peu pour émettre. Sur la période d'évaluation, aucune attaque virale n'a été recensée. Seuls le spam et la publicité sont les principaux problèmes et touchent certains utilisateurs plus que d'autres. Les pièces jointes attachées aux messages sont

nombreuses et principalement du type « document » ou bien « image ». Aucun fichier exécutable et quelques fichiers cryptés ont été détectés pendant cette phase de tests. L'acheminement de message contenant des pièces jointes cryptées et à prendre en compte, car l'analyse du contenu n'est pas garanti dans ce cas. Enfin, du point de vue performance, la plateforme est peu consommatrice de temps processeur et de mémoire et présente un nombre d'accès disque raisonnable, du moins avec la configuration déployée. Elle nécessite cependant un volume minimum de 120 Go sur la baie de stockage pour le système et la gestion des journaux et traces. Cet espace peut paraître élevé mais permet la mise en place d'une politique d'archivage des traces généralisée à l'échelle de l'établissement.

La solution Trend Micro IMSVA s'avère être un produit fiable et efficace par rapport aux flux de messagerie du CH de Montbert. La période d'évaluation a permis de mettre en avant certaines spécificités liées à l'activité de l'établissement, mais aussi de prendre toute la mesure d'une solution logicielle installée en locale. Une supervision active et régulière pour disposer de règles d'une efficacité maximale est impérative. La solution n'est donc pas autonome, comme peuvent l'être d'autres solutions concurrentes.

7.3.2 La solution Vade-Retro

La société Vade Retro technology est la division sécurité de GOTO Software, éditeur français de solutions logicielles depuis 1982 et a été créée en 2001. Leurs solutions protègent plus de 100 millions de comptes de messagerie à travers l'Europe, à destination de fournisseurs d'accès Internet, mais aussi pour les entreprises et les postes clients. Vade Retro repose sur un moteur de filtrage propriétaire. Basé sur un système intelligent de règles de filtrage, le composant PHF (Predictive Heuristic Filter) est capable d'anticiper automatiquement les attaques massives de spams et de virus, et de protéger les utilisateurs, pendant le délai critique et incompressible d'intervention des éditeurs.

Le CH Le Mans a déployé cette solution en mode hébergé pour sécuriser ses flux de messagerie. Afin de prendre toute la mesure des capacités du produit, la solution MailCube2 je l'ai installé en machine virtuelle dans l'infrastructure du CH de Montbert.

7.3.2.1 Choix d'architecture et licences logicielles

Vade Retro propose plusieurs solutions d'intégrations et des modules spécifiques afin de sécuriser les flux de messagerie sur le CH de Montbert.

Le filtrage du flux de messagerie est un service. A ce titre, Vade Retro offre le choix de l'externaliser (Annexe L). Dans cette configuration, aucune installation matérielle ou logicielle n'est à réaliser sur le site. Il est alors nécessaire de modifier l'enregistrement MX déjà publié, pour renvoyer le flux vers les datacenters Vade Retro et non pas vers le CH de Montbert. Ceux-ci se chargeront du traitement et renverront ensuite les courriels légitimes vers le CH. Une quarantaine utilisateur seulement est accessible. Une configuration plus précise des filtres ou des règles est impossible. L'objectif de ce service est « de se faire oublier ».Cette architecture à l'avantage de proposer un délai de rétention des messages de 5 jours en cas de coupure du lien réseau, afin de ne pas perdre de courriels. Cependant, de nombreuses fonctionnalités ne sont pas disponibles en mode hébergé. L'appliance « MailCube2 » ou l'installation de la solution sur une machine virtuelle, assure de disposer de tous les outils de la solution. Pour cette évaluation, le déploiement de la solution logicielle était le plus rapide à mettre en œuvre.

La solution logicielle proposée est une machine virtuelle, préinstallée, à installer en zone DMZ. Les ressources requises sont très correctes, puisque seulement 2 Go de mémoire et 30 Go d'espace disque sur la baie de stockage SAN sont nécessaires. Le système, en 64 bits, doit aussi être supporté par l'infrastructure d'accueil. Du point de vue routage, des modifications ont été effectuées sur le pare-feu, mais surtout sur le serveur de messagerie lui-même, pour aboutir à l'architecture cible (Annexe M). J'ai donc créé sur le serveur de messagerie un nouveau connecteur, dédié à Vade Retro. En effet, la passerelle gère deux chemins distincts. Le flux entrant utilise le port 25 et est redirigé vers le port 25 du serveur de messagerie, configuration par défaut des solutions. Dans le cas de l'envoi, le serveur de messagerie doit acheminer le flux sortant vers le port 8025 de la passerelle et non le 25. De plus, la connexion avec le serveur de messagerie doit impérativement être non sécurisée et les authentifications TLS désactivées sur le connecteur de réception. Les pré-requis système et réseaux pris en compte, la configuration peut se poursuivre

La solution Vade Retro est de conception modulaire. Dans le cadre de cette évaluation, toutes les fonctionnalités disponibles sont évaluées. Tout d'abord, il existe deux types d'antivirus. Le premier est une protection antivirale classique qui s'appuie sur les compétences de l'éditeur DrWeb pour détecter les virus et malwares, y compris dans les archives compressées. Le second

est un antivirus heuristique qui est chargé de découvrir les signatures et codes malicieux qui sont contenus dans les messages. Le module anti spam quant à lui est chargé de nettoyer le flux des courriels illégitimes. A l'image des autres solutions, plusieurs techniques de filtrage sont combinées afin d'obtenir le meilleur résultat et surtout le moins de faux-positifs. Il est pour cela doté d'un auto-apprentissage qui lui permet de s'adapter aux évolutions des pourriels. Si le score affecté au courriel après analyses est compris entre 100 et 300, alors la qualification de « spam faible » est appliquée. Entre 300 et 500 il s'agit d'un « spam moyen ». Enfin, si le score est supérieur à 500, le courriel est considéré comme un « spam fort ». En fonction de ces éléments, des actions, à personnaliser, sont exécutées. Enfin, le filtre anti-publicités doit éliminer les courriels de type publicitaire et newsletters non désirés du flux. L'ensemble de ces outils doit assurer une protection optimale sur les flux entrants et sortants de messagerie.

L'installation et les licences disponibles, la solution reste à être configurée pour assurer sa mission de sécurisation du flux de messagerie.

7.3.2.2 Configuration de la solution

La configuration de la solution Vade Retro dans le cas du CH de Montbert est relativement simple et consiste à renseigner les paramètres réseaux, de sécurité et de domaine.

Avant d'accéder à l'interface de configuration, il est impératif de configurer les paramètres réseaux du serveur dans la DMZ. Ensuite, l'accès à l'interface est réalisé à partir d'un navigateur Internet en attaquant la passerelle sur le port 8080. Dans un premier temps, il faut établir le lien entre le domaine à filtrer et le serveur de messagerie. La procédure est simple puisque le CH de Montbert dispose d'un seul serveur de messagerie et d'un seul nom de domaine à filtrer. De plus, il n'existe aucun équipement entre la passerelle et le pare-feu. Il n'y a donc pas de routes spéciales à établir pour acheminer les messages. Des options de configuration pour le filtrage de domaines sont disponibles. Cependant, je ne les ai pas mises en œuvre pendant cette évaluation. En effet, il est préférable de gérer ces paramètres directement au niveau des analyses sur les courriels. Du point de vue sécurité, la solution dispose de fonctionnalités pour éviter la diffusion de pourriels depuis le CH de Montbert, ou les attaques du type DoS. En effet, le nombre de connexions simultanées sur le serveur SMTP est limité par défaut à 500 et à 10 par adresse émettrice. J'ai aussi personnalisé la réponse de la commande « HELO ». Cette commande est utilisée par des serveurs distants pour établir une correspondance entre le domaine de l'expéditeur et celui de la commande « HELO » afin de valider la prise en charge du message. Enfin, il est envisageable de renseigner les adresses IP des serveurs qui relaient les messages.

Pour le CH de Montbert, j'ai saisi les IP des serveurs de l'opérateur GIGALIS. Cette configuration est complémentaire au filtrage déjà actif au niveau du pare-feu. Après la réalisation de ces étapes, j'ai élaboré les politiques de filtrage pour le moteur anti spam de la solution Vade Retro.

En effet, les messages qui transitent sur la passerelle sont spécifiques à chaque client. Bien qu'une configuration par défaut soit proposée, il est impératif de personnaliser certains éléments à l'installation et régulièrement par la suite. Le premier niveau de filtrage est effectué sur les adresses IP des serveurs émetteurs. Vade Retro conseille de s'appuyer sur une liste RBL régulièrement mise à jour et gratuite. Dans cette section, les adresses IP reconnues à bloquer sont à renseigner. Une distinction est faite entre les adresses IP crédibles, pour lesquelles les connexions seront toujours acceptées et les messages soumis aux analyses des « relais serveurs sécurisés », qui seront directement transmis au serveur de messagerie sans appliquer de filtrage. Cette dernière option doit être utilisée uniquement lorsque l'on connait parfaitement les serveurs émetteurs. Dans le cas contraire cela serait une faille de sécurité potentielle. Le filtrage IP effectué, le courriel est transmis au filtre de domaine.

Le second niveau de filtrage consiste à évaluer les caractéristiques du courriel sur son domaine. Sur un principe identique au filtrage IP, Vade Retro s'appuie sur des listes à bloquer et à autoriser. Cependant, une distinction est faite sur la notion de domaine. En effet, Vade Retro soumet le message à un filtrage sur le « domaine protocolaire ». Ce filtrage permet d'accepter ou de refuser des courriels dont le serveur émetteur ne serait pas du même domaine que l'adresse de l'expéditeur. Le filtrage sur le « domaine expéditeur » compare le domaine de l'adresse de l'expéditeur, celle visible dans l'en-tête « From » du message avec des listes blanches ou noires. Lors de l'évaluation ce sont ces listes que j'ai renseignées progressivement afin d'améliorer le niveau de filtrage. Enfin, la solution dispose des options de vérifications DNS, Sender Policy Framework (SPF) et DKIM. La première s'assure que le nom de domaine de l'expéditeur existe réellement au niveau des entrées DNS. La seconde compare les adresses IP des serveurs légitimes du nom de domaine annoncé à celle du serveur qui relaie le message. Enfin l'option DKIM vérifie que le cryptage de l'en-tête du message correspond bien à celui du serveur qui relaie le message. Cette dernière fonctionnalité présuppose que les serveurs de mails utilisent en majorité ce système. Or ce fonctionnement n'est pas généralisé à ce jour. Je n'ai donc pas activé cette option. Une fois ce filtrage de domaine réalisé, le niveau suivant est d'analyser les adresses.

A l'image du filtrage de domaine, les processus d'analyses sur les adresses s'appuient sur des listes à autoriser ou à bloquer. Le même schéma est reproduit, avec des inspections au niveau protocolaire et adresse. Une adresse électronique ajoutée en liste crédible pour le filtrage protocolaire ne subira pas les analyses sur le domaine expéditeur (DNS, SPF, DKIM). De la même façon, une adresse crédible pour le filtrage par adresse d'expéditeur ne sera pas soumise aux analyses de contenu. Enfin, Vade Retro fournit en complément une option de vérification des adresses des destinataires, lors de la réception d'un message. L'objectif est de s'assurer de l'existence de l'utilisateur à qui est destiné le courriel. Cette authentification peut être réalisée par une interrogation LDAP sur un annuaire existant, ou alors directement sur le serveur de messagerie. Dans ce dernier cas, une requête « CHECK-SMTP » est adressée au serveur de messagerie qui répond si la boîte aux lettres de destination est réelle ou non. Pendant toute la durée de ces tests, les messages sont placés en zone de quarantaine administrative, puis délivrés si la requête est réussie. Cette option assure de transmettre au serveur de messagerie des courriels pour lesquels les adresses existent réellement. Celui-ci est alors déchargé du traitement des échecs. Après avoir activé cette fonctionnalité, j'ai constaté le blocage du routage de nombreux messages à destination d'utilisateur inexistants. Le gain de performance au niveau du serveur de messagerie est donc significatif. Les processus de filtrages sur les en-têtes terminés, le contenu doit aussi être traité.

Le filtrage de contenu est chargé de définir le niveau de sécurité du contenu du courriel. Pour cela, plusieurs filtres sont mis en œuvre. La recherche heuristique de virus consiste à découvrir des virus potentiels à partir de leurs comportements plutôt que par leurs signatures, en s'appuyant les observations enregistrées dans un arbre de décisions. Ainsi le filtre considère que c'est un virus seulement si un certains nombre de conditions sont remplies. Puis, une analyse antivirus classique est appliquée au contenu et aux pièces jointes, à la recherche de malwares, virus, vers, … Enfin, Vade Retro intègre un filtre « anti-publicités » pour détecter et bloquer les publicités indésirables. En effet, bien que le spam représente un volume important de message, pour le CH de Montbert le problème principal est celui des newsletters, listes de diffusions et publicités diverses qui sont délivrées chaque jour aux utilisateurs. Le dernier filtrage disponible s'applique aux options régionales, pour analyser les courriels contenant des caractères cyrilliques ou asiatiques. Le CH de Montbert exerçant son activité uniquement en France, je n'ai pas activé ces options. Le score de tous les filtrages réunis détermine l'action à réaliser.

Après l'exécution de tous les niveaux de filtrage, un score est affecté à chaque courriel afin d'appliquer la politique de traitement du message.

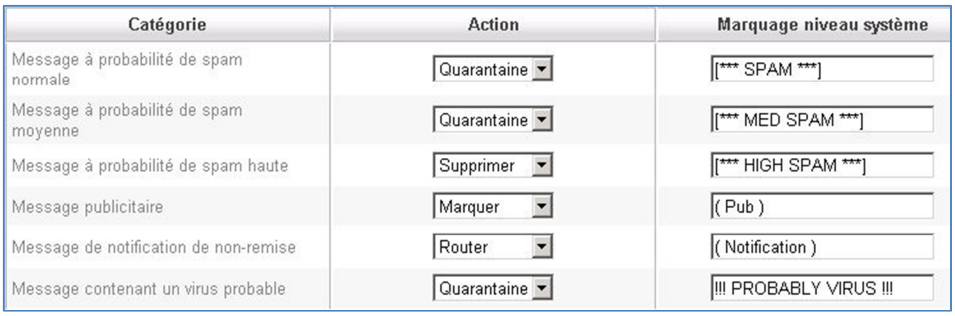


Figure 68 : Liste des actions disponible après analyses

Suivant les cas, le message peut être placé dans la quarantaine de l'utilisateur, supprimé, marqué ou simplement routé. Les objets des courriels sont modifiés afin de faire apparaître clairement le résultat des analyses et ainsi faciliter la lecture aux utilisateurs dans leurs clients de messagerie.

La configuration de ces paramètres ne peut être définitive et nécessite de vérifier régulièrement les caractéristiques des flux entrants et sortants de la passerelle. Cette surveillance est nécessaire pour améliorer la qualité du filtrage et par conséquent la satisfaction des utilisateurs quant au contenu des courriels délivrés dans leurs boîtes aux lettres. La supervision du produit et des flux est indispensable.

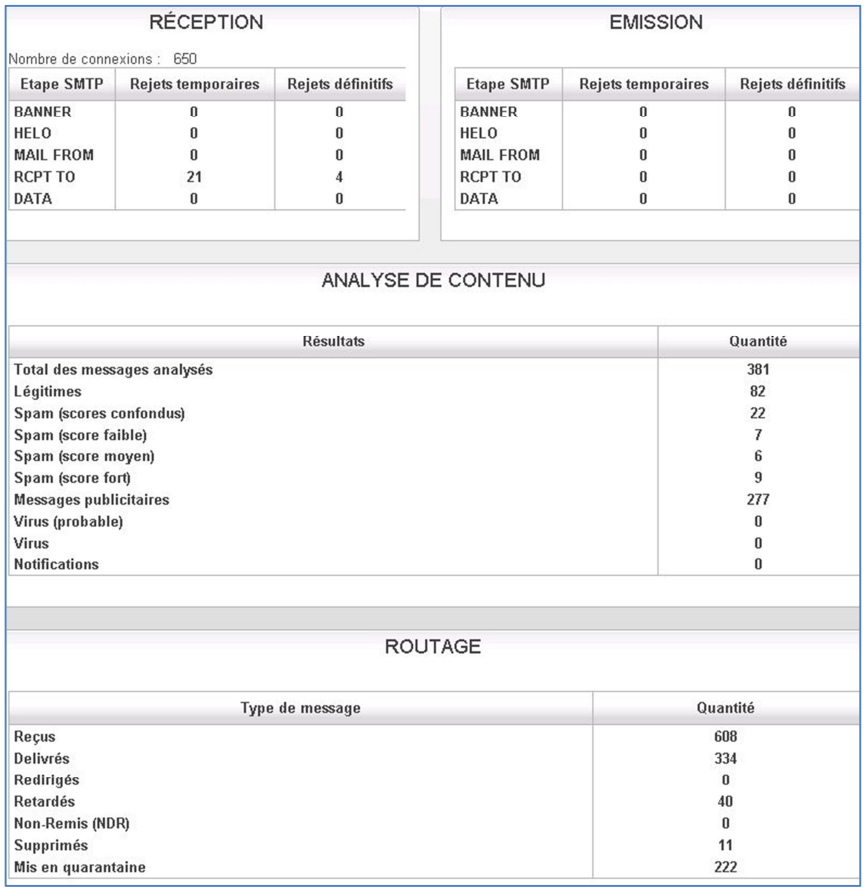
7.3.2.3 Statistiques, supervision et gestion des quarantaines

La solution Vade Retro fournit des outils de statistiques, rapports d'activité et tableaux de bords pour superviser les flux et le système, mais aussi une gestion individuelle de la quarantaine.

Dès la connexion sur l'interface d'administration, un résumé des statistiques de la journée est affiché afin de visualiser rapidement le volume des flux et les erreurs rencontrées :

Figure 69 : Tableau de bord du 11/08/2011 des flux de messagerie

Un tableau de bord plus précis pour chaque type de flux, entrant et sortant, est consultable en complément. Les éléments importants sont sur la ligne « RCPT-TO » sur laquelle les erreurs temporaires et définitives apparaissent. Ces valeurs indiquent le nombre de messages pour lesquels une ou plusieurs adresses de destination étaient erronées. Après quelques tentatives, le serveur ignore la réception des courriels vers des adresses inexistantes sur le serveur de messagerie du CH de Montbert.



RÉCEPTION

Nombre de connexions : 650

Etape SMTP	Rejets temporaires	Rejets définitifs
BANNER	0	0
HELO	0	0
MAIL FROM	0	0
RCPT TO	21	4
DATA	0	0

EMISSION

Etape SMTP	Rejets temporaires	Rejets définitifs
BANNER	0	0
HELO	0	0
MAIL FROM	0	0
RCPT TO	0	0
DATA	0	0

ANALYSE DE CONTENU

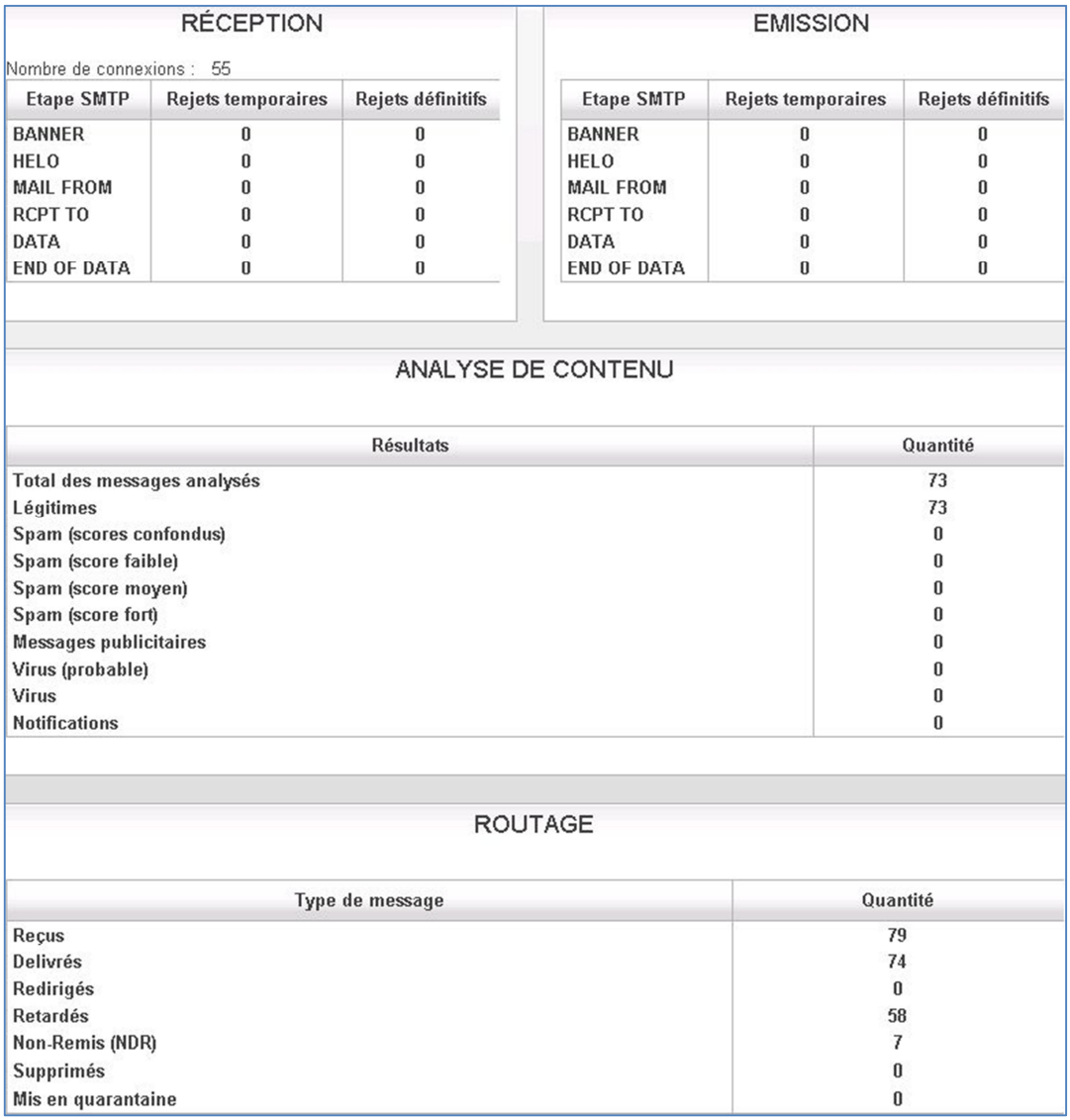
Résultats	Quantité
Total des messages analysés	381
Légitimes	82
Spam (scores confondus)	22
Spam (score faible)	7
Spam (score moyen)	6
Spam (score fort)	9
Messages publicitaires	277
Virus (probable)	0
Virus	0
Notifications	0

ROUTAGE

Type de message	Quantité
Reçus	608
Delivrés	334
Redirigés	0
Retardés	40
Non-Remis (NDR)	0
Supprimés	11
Mis en quarantaine	222

Figure 70 Tableau de bord du flux entrant du 11/08/2011

Ces informations offrent aux administrateurs une visualisation rapide du résultat des politiques de filtrage mise en œuvre, mais aussi sur les types de courriels qui transitent. En effet, pour le CH de Montbert, le constat est surprenant. Peu de spams sont réellement détectés, mais il existe une proportion importante de messages publicitaires stoppés par la solution, soit plus de 70% du flux en réception. Or, ces messages ne sont actuellement pas traités par la solution en place. Du temps est alors nécessaire à chaque utilisateur pour trier les messages, au détriment de son activité professionnelle. Ces données sont confirmées graphiquement lorsque l'on accède au module statistique de la solution. Celui-ci peut afficher un graphique sur la dernière heure, la journée, ou le dernier mois pour le volume du trafic, la répartition des actions réalisées ou le nombre d'erreurs SMTP rencontrées.



RÉCEPTION

Nombre de connexions : 55

Etape SMTP	Rejets temporaires	Rejets définitifs
BANNER	0	0
HELO	0	0
MAIL FROM	0	0
RCPT TO	0	0
DATA	0	0
END OF DATA	0	0

EMISSION

Etape SMTP	Rejets temporaires	Rejets définitifs
BANNER	0	0
HELO	0	0
MAIL FROM	0	0
RCPT TO	0	0
DATA	0	0
END OF DATA	0	0

ANALYSE DE CONTENU

Résultats	Quantité
Total des messages analysés	73
Légitimes	73
Spam (scores confondus)	0
Spam (score faible)	0
Spam (score moyen)	0
Spam (score fort)	0
Messages publicitaires	0
Virus (probable)	0
Virus	0
Notifications	0

ROUTAGE

Type de message	Quantité
Reçus	79
Delivrés	74
Redirigés	0
Retardés	58
Non-Remis (NDR)	7
Supprimés	0
Mis en quarantaine	0

Figure 71 : Tableau de bord du flux sortant du 11/08/2011

Néanmoins, il n'existe pas de module de statistiques personnalisable. Celui-ci serait utile pour explorer quels sont les courriels classés en « spam moyen » ou « spam fort », pour consulter rapidement les historiques des connexions des administrateurs, mais aussi pour connaître quels sont les utilisateurs avec le plus gros trafic ou les domaines les plus utilisés. En complément, la passerelle fournit d'autres fonctionnalités, plus orientées « système ».

Vade Retro intègre également des services de gestion de son produit, plus communs. Ainsi, un module « Journaux » offre la possibilité de rechercher dans les logs, avec un affichage formaté.

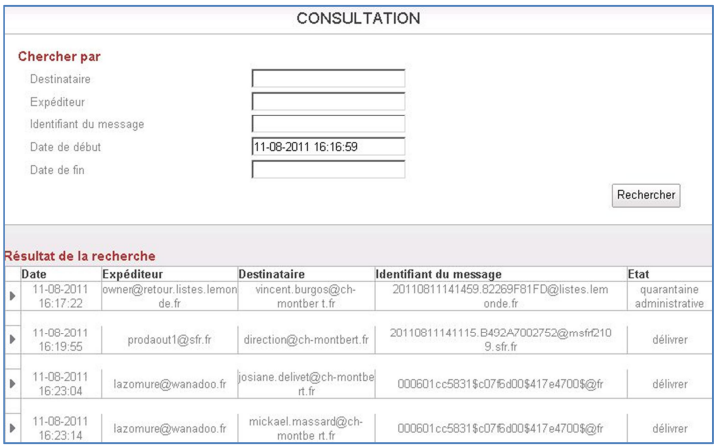


Figure 72 Affichage formaté des journaux du 11/08/2011

Il est aussi possible de consulter directement le contenu des fichiers de logs, qui pour ces derniers sont téléchargeables au format texte.

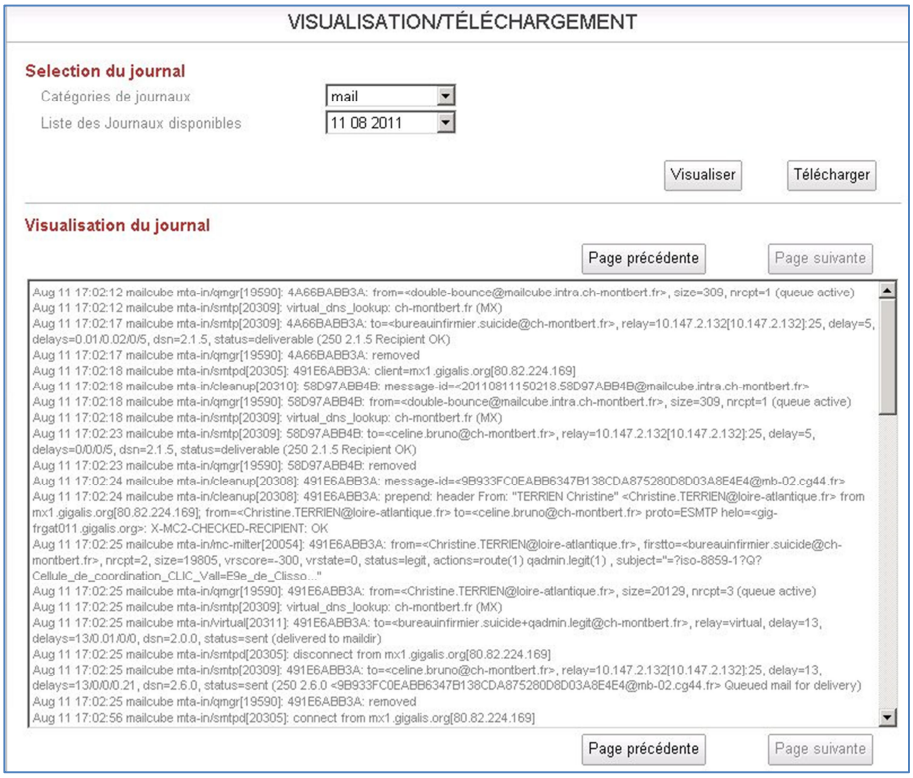


Figure 73 : Contenu des logs du 11/08/2011

Il est à noter que la durée de conservation des logs sur la passerelle est de 21 jours seulement. L'utilisation d'un serveur syslog est obligatoire si une durée de conservation supérieure est souhaitée. Un autre module « Maintenance » est aussi disponible. Celui-ci fournit les outils de sauvegarde ou de restauration de la configuration, des informations concernant les licences, d'un

onglet pour la mise à jour du firmware de la solution et d'un onglet d'import et d'export des sauvegardes. Cependant, il n'existe à ce jour pas d'outil de planification de la sauvegarde. Celle-ci doit être réalisée et exportée manuellement. Des fonctionnalités de planification et d'exports automatisés vers des dossiers partagés seraient un plus. Enfin, un module « Haute disponibilité » apporte les services nécessaires à la gestion d'un cluster Vade Retro Mailcube. Cet aspect est important car il offre la possibilité de déployer deux passerelles et ainsi maintenir la disponibilité du service de messagerie électronique en cas de défaillance matérielle ou logicielle d'un des éléments. La supervision de la passerelle coté administrateur est aussi couplée à une gestion des espaces de quarantaines.

Vade Retro propose deux quarantaines distinctes : une quarantaine administrative et des quarantaines utilisateurs. La quarantaine administrative est chargée de recevoir tous les courriels qui ne peuvent être redirigés vers une quarantaine utilisateur, suite à des erreurs ou bien à des configurations établies. Les listes de diffusion par exemple ne sont généralement pas administrées par les utilisateurs. Plusieurs intervenants auraient accès à la quarantaine et seraient susceptibles d'en assurer la maintenance. La situation contraire serait une « non gestion » de cette quarantaine. Ce travail supplémentaire est laissé aux administrateurs du système en tenant compte du fait que ce ne sont pas les listes de diffusion les plus polluées.

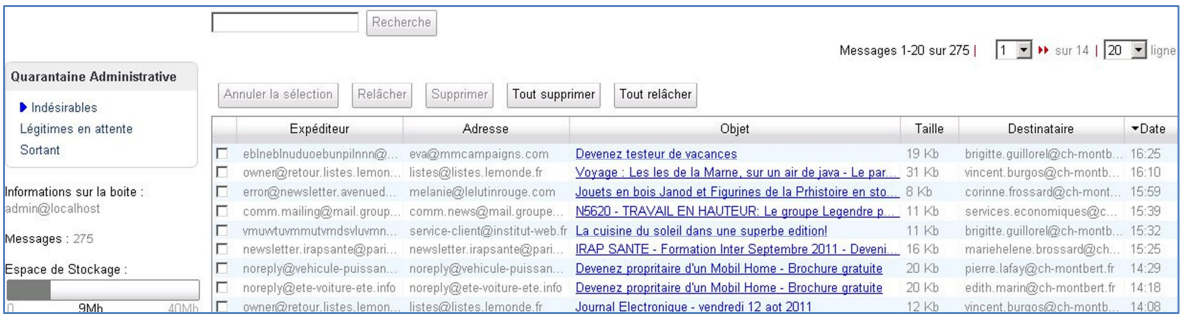


Figure 74 : La quarantaine administrative avec Vade Retro

Mais cet espace accueille aussi tous les messages en attente, dans un onglet « légitime en attente ». Ainsi, lors de la réception d'un courriel à destination d'un utilisateur non encore référencé par la solution, celui-ci est placé en quarantaine administrative en attente du retour de la commande CHECK-SMTP. Si l'utilisateur existe bien, alors le message lui sera remis. La quarantaine administrative contient également la liste des messages en attente d'émission. Les fonctionnalités de cet espace sont limitées, car l'objectif de la solution Vade Retro est de responsabiliser les utilisateurs et de les inciter à gérer leur propre quarantaine. Ainsi, lors de la mise en production, un espace est associé, automatiquement ou avec validation, à une adresse

électronique. L'utilisateur gère lui-même ses messages et maintient ses listes blanches et listes noires d'adresses ou de domaine.

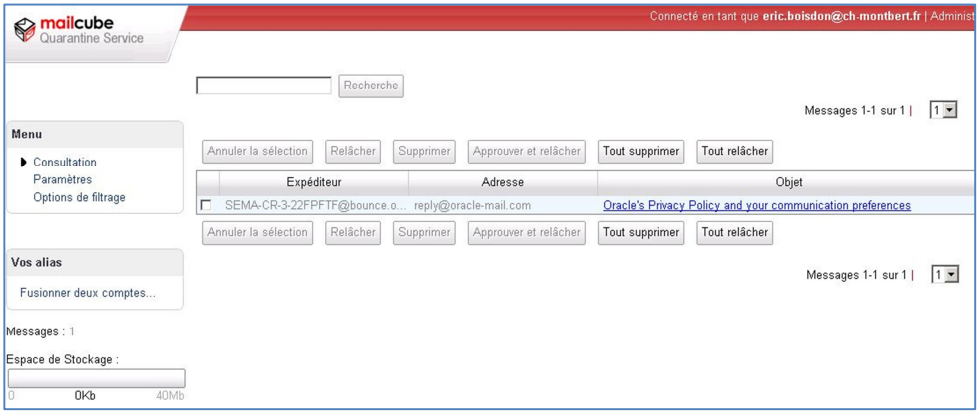


Figure 75 Gestion d'une quarantaine utilisateur

Trois autres fonctionnalités sont disponibles, indépendantes des configurations mises en place par l'administrateur. La première invite les utilisateurs à renseigner une période d'absence, pendant laquelle les éléments indésirables ne seront pas supprimés, même si le délai de rétention maximum est dépassé. La seconde consiste à paramétrer ses propres périodes d'envoi de rapports. Enfin, la dernière offre la possibilité de rattacher un nombre illimité d'alias à une adresse principale. Ainsi, les utilisateurs disposant de plusieurs adresses (pour des raisons de changement de nom par exemple) gèrent une seule quarantaine et non pas plusieurs. Cette option est très intéressante et à prendre en compte pour le CH de Montbert, pour lequel plusieurs cas de ce type existent.

L'intégration de la solution Vade Retro au sein de l'infrastructure du CH de Montbert m'a permis de dresser un bilan de cette évaluation.

7.3.2.4 Bilan de l'évaluation

La mise en œuvre de la solution Vade Retro pendant 15 jours sur le CH de Montbert s'est avérée très instructive.

Le déploiement de la solution et la prise en mains sont extrêmement rapide car la solution est très intuitive. Les ressources de fonctionnement nécessaires sont correctes et même faibles comparées à des produits concurrents. Cela peut s'expliquer par la faible durée de rétention des logs, sur 21 jours. Une augmentation serait souhaitable, même si un export vers un serveur syslog reste possible. Le moteur de règle est entièrement administré par Vade Retro. Il n'y a donc pas de paramétrage complexe à réaliser (création des règles), mais seulement à renseigner

des listes d'adresses IP, de domaines ou d'adresses crédibles ou polluantes. Il y a ici une limite à la simplicité de l'application. En effet, il serait souhaitable de pouvoir activer des règles destinées à des cas particuliers de filtrage, ce qui est ici impossible. Ce problème de simplicité se rencontre également dans l'exploitation des statistiques et des journaux. Il serait agréable de disposer d'un outil de recherche par critère, sur des périodes de temps personnalisables et ce afin de pouvoir améliorer la qualité du filtrage. L'objectif serait de déterminer par exemple le nombre de message avec pièces jointes, leurs types, les scores affectés aux courriels définis comme spams et la raison de ce classement, le classement des utilisateurs ou domaines les plus usités. L'export de ces informations, manuel ou automatique serait aussi recommandé. Du point de vue accessibilité, un lien avec un annuaire LDAP serait bienvenu de façon à utiliser les identifiants des administrateurs et assurer la traçabilité des connexions dans les logs, conformément aux politiques de sécurité. Malgré ces quelques défauts, le filtrage est très performant et a mis en avant certains constats et problèmes sur les caractéristiques du flux de messagerie au CH de Montbert.

En effet, il apparait que moins de 20% des messages réceptionnés sont légitimes. La part restante est répartie entre spams avérés et publicités non désirées. Or, j'ai constaté que le CH de Montbert reçoit peu de spam par rapport aux publicités. Le filtre anti-publicité de VadeRetro se montre très efficace dans la détection de ce type de message. L'implantation de ce filtrage pourrait également être étudiée au niveau des FAI, pour un premier tri, comme ce qui est actuellement fait pour le spam. Les statistiques alertent aussi sur le nombre d'erreurs smtp entrantes et sortantes. Dans le premier cas, il s'agit de courriels réceptionnés sur la passerelle mais dont la boîte aux lettres de destination n'existe pas ou plus, suite à un départ de l'agent par exemple, ou avec un utilisateur erroné mais le domaine correct. Le second cas peut être une erreur de saisie dans l'adresse du destinataire, ou alors une tentative d'envoi de spams depuis le CH de Montbert. L'erreur de saisie parait à ce jour la plus probable à la vue du peu d'alertes remontées. Enfin, une attention particulière doit être portée sur la gestion de la quarantaine pour la problématique du filtrage sur les listes de diffusion. Le CH de Montbert dispose de 136 listes pour 250 boîtes aux lettres. Bien que celles-ci ne soient pas les plus attaquées par la publicité ou le spam, ce travail de vérification est souvent laissé aux administrateurs. Enfin, l'accès à l'espace de quarantaine de l'utilisateur est possible non seulement depuis le site du CH, mais aussi depuis l'extérieur, pour les utilisateurs du webmail.

En conclusion, la solution proposée par Vade Retro pour la sécurisation des flux de messagerie est performante et assure de libérer les messageries des utilisateurs de la majorité des

spams mais surtout publicités non désirées. Le moteur de règles est entièrement administré par l'éditeur lui-même qui affine le filtrage sans interventions des administrateurs. La gestion des quarantaines est laissée à chaque utilisateur afin de le responsabiliser et de le laisser libre de ces choix. Cependant, la volonté évidente de proposer un produit simple dans son exploitation rend impossible une configuration plus personnalisée. Les statistiques et rapports sont aussi à améliorer afin de disposer d'une solution complète. La solution MailCube2 répond donc aux principaux besoins du CH de Montbert, tant pour les administrateurs par sa simplicité, que pour les utilisateurs pour la qualité du filtrage mis en œuvre.

8 Un choix de solution de sécurisation difficile

Le CH de Montbert souhaite améliorer la sécurisation de ses flux Internet et de messagerie électronique. Dans cet objectif, j'ai évalué plusieurs produits sur une période de plusieurs jours à deux mois. D'après les résultats de ces évaluations, des solutions se montrent plus efficaces que d'autres.

8.1 Le choix d'un mode d'intégration

La volonté de sécuriser les flux Internet et de messagerie est inspirée par des enjeux de sécurité, d'évolution des comportements des utilisateurs, mais aussi pour répondre à des exigences réglementaires, notamment de traçabilité des connexions et de conservation des traces. A ce titre, les solutions des éditeurs Trend Micro, Websense, Olfeo et Vade Retro ont été testées. Les évaluations de ces produits ont été réalisées avec un mode d'intégration différent. Ainsi, j'ai eu la possibilité de constater les avantages et inconvénients de chacun.

L'intégration dans un environnement virtuel offre tous les services de sauvegardes, de réplication et de disponibilité mis en œuvre pour les autres serveurs de l'organisation. Ceux-ci sont déjà connus des équipes informatiques et utilisés quotidiennement. Aucunes connaissances complémentaires sur ces aspects ne sont à acquérir. Il n'est pas nécessaire de disposer de l'encombrement physique dans les racks, ni de s'occuper des alimentations électriques et du secours associé. Cependant, les pré-requis de performances des serveurs physiques et des baies de stockage sont absolument à prendre en compte dans les procédures de fonctionnement et en mode dégradé. En effet, le nombre de serveurs virtuels est augmenté et les serveurs physiques les hébergeant supportent la charge complémentaire. De plus, il est impératif de déterminer leur criticité et d'organiser leur gestion. La mise en œuvre de cluster pour assurer la haute disponibilité augmente d'autant plus les besoins en ressources matérielles. Ces coûts annexes

doivent être intégrés dans les simulations financières. Enfin, la mise à disposition d'un serveur de statistiques complémentaire optimise les performances au niveau du filtrage et donc de la satisfaction des utilisateurs, mais nécessite plus de ressources mémoire et disques. Le déploiement d'une solution en mode hébergé astreint à des contraintes et avantages différents.

Le choix d'une architecture en mode hébergé apporte une facilité de gestion et d'administration. En effet, l'équipe informatique ne supporte plus les charges des évolutions techniques, de maintenance car l'éditeur prend le relais. Il fournit un service de filtrage par la mise en place d'une redirection des flux vers son infrastructure. Il s'engage alors sur la qualité de service et la disponibilité de ses installations et versions logicielles. Le déploiement est en apparence très simple et réalisé par la diffusion de fichiers proxy.pac directement dans les navigateurs, à l'aide des stratégies de groupes. La gestion des profils de connexion est assurée par l'attribution de droits spécifiques à chaque proxy.pac. Cette apparente simplicité impose de multiplier le nombre de stratégies de groupes, du moins pour le CH de Montbert, pour lequel de nombreux profils devraient être déterminés. Il existe alors un impact fort sur l'organisation de l'annuaire active directory, des utilisateurs et des groupes. L'avantage du mode hébergé réside dans la possibilité d'offrir un accès direct à Internet aux sites distants sans que leurs flux aient à revenir sur le site central avant leur acheminement. Les bandes passantes sont dans ce cas moins sollicitées et les temps de réponse pour les utilisateurs améliorés. Cependant, il est regrettable que les versions logicielles des modes hébergées soient généralement plus anciennes et les fonctionnalités réduites par rapports à celles disponibles en appliance. De plus, il est à prévoir un espace de récupération des traces sur le site à des fins de conservation. L'éditeur Websense pour remédier à ce problème, propose l'installation en interne d'un serveur spécial hébergeant une console chargée d'offrir plus de services, notamment pour les statistiques, rapports et logs. Même si ce serveur n'est pas critique, il doit être administré en complément du service hébergé. Enfin, cette console centralise les flux des sites distants et du site central dans le cas d'une architecture hybride. Cette architecture se montre intéressante pour le CH de Montbert pour la problématique de ses sites distants. L'intégration avec une appliance matérielle est un autre choix.

L'appliance matérielle est un serveur physique à intégrer dans un rack et qui occupe généralement une unité. L'alimentation électrique secourue est conseillée et à prévoir dans les calculs de dimensionnement des onduleurs et du groupe électrogène. Le système d'exploitation linux, le plus intégré pour ce type de mise en œuvre, héberge l'application. Une grande majorité d'éditeurs conseille de déployer un cluster, avec deux boitiers installés dans deux salles

informatique différentes afin d'assurer la haute disponibilité. Un surcoût pour l'acquisition mais aussi pour la maintenance des deux passerelles est à prendre en compte. Les performances du matériel sont à définir par l'éditeur en fonction du nombre d'utilisateurs et des délais de rétention. Ceci est une limite à ce type d'intégration. En effet, si le nombre d'utilisateurs est amené à augmenter brusquement, le serveur sera sous-dimensionné et devra être remplacé pour absorber les nouveaux flux, entraînant des dépenses non provisionnées. Cette contrainte ne s'applique pas au CH de Montbert, dont l'effectif en nombre d'utilisateurs, d'ordinateurs ou de boîtes aux lettres n'a pas de perspective d'évolution forte. Les limites sont déjà connues et peuvent être anticipées. La version logicielle déployée, comme dans le cas de serveurs virtuels, peut-être soumise à des mises à jour majeures imposant le remplacement du matériel à moyen terme. Les mises à jours sont généralement supportées par les appliances, Les administrateurs sont en charge de les appliquer. Une maintenance minimum est donc à assurer.

Pour conclure, l'architecture avec appliance est celle qui correspond le mieux au CH de Montbert. Cette architecture est celle qui apporte le plus de fonctionnalités et de possibilités de paramétrage pour s'adapter à l'établissement. Le choix de la solution logicielle pour les flux Internet reste à valider.

8.2 Choix d'une solution de sécurisation des flux Internet

Les produits Trend Micro IWSVA et ARM ont été déployés sous forme de machines virtuelles, en DMZ, la solution Websense en mode hébergé et la solution OLFEO en appliance matérielle. Une préférence entre ces produits pour une intégration au CH de Montbert se dessine.

Le produit de filtrage de Trend Micro est satisfaisant, si l'on souhaite sécuriser uniquement les principaux protocoles (http, https, ftp). Ceux encapsulés dans des flux http ne sont par conséquent pas détectés (messagerie instantanées, téléchargement, …). Or, le CH de Montbert souhaite pouvoir analyser avec précision les contenus des flux qui transitent sur le port http. Le point fort de cette offre est la performance de son antivirus, très complet et reconnu par de nombreuses sociétés et intégrateurs. Une certaine « philosophie » est aussi à acquérir, personnellement ou par une formation, pour l'utilisation courante lorsqu'il n'existe pas de connaissances Trend Micro au sein des équipes. Cette solution ne répond pas réellement aux objectifs de sécurisation souhaités. Du point de vue financier, une licence par poste est requise.

La solution « Hosted Web Security » de Websense, en mode hébergé se montre très rapide au niveau des temps de réponses. Elle offre aussi la possibilité d'une gestion multi-sites à partir de

l'identification d'adresses IP et libère de la bande passante, paramètre très important pour le site actuel, mais beaucoup moins pour le nouvel établissement, relié en fibre optique. Des fonctionnalités de priorisation des flux sont aussi disponibles. Une synchronisation des comptes utilisateurs entre le service hébergé et l'annuaire active directory est à configurer et nécessite l'ouverture de ports complémentaires sur le pare-feu et donc une faille de sécurité potentielle. Une surveillance de ces tâches est également à effectuer. La console de centralisation « Triton », non évaluée, apporterait plus d'ergonomie, de souplesse et des rapports plus aboutis par rapport à la version hébergée, peu ergonomique. De plus, un serveur virtuel, même d'une criticité faible, resterait à gérer. Enfin, il est impératif de comptabiliser une licence par utilisateur susceptible d'accéder à Internet. Le coût en licence peut alors très vite devenir important.

Enfin, la solution Olfeo en appliance est la solution qui a le mieux répondue aux attentes du CH de Montbert. L'exploitation de base de réputations françaises correspond aux habitudes de navigations des utilisateurs. Le moteur de règles est entièrement personnalisable, mais peu se montrer complexe par un trop grand nombre de règles. Le cache optimise les temps de réponses. La qualité de service offre la possibilité de prioriser des flux métiers (Agirh Planning, ATIH, …) par rapport à des flux de navigation d'importance moindre. Le support de proxy (http, ou autre) permettrait à l'établissement de supprimer son serveur proxy actuel, pour les mêmes fonctionnalités. La solution répond parfaitement aux contraintes de gestion des services spécifiques (addictologie, suicide, activités) et la traçabilité d'un an intégrée à l'appliance est appréciable. Le module de statistique est entièrement personnalisable et fourni des graphiques immédiatement prêts pour diffusion. Pour la mise en cluster, Olfeo propose d'installer une version logicielle sur une machine virtuelle afin d'éviter l'acquisition d'une seconde appliance. Enfin, la solution Olfeo est la seule qui offre la possibilité de signer informatiquement la charte informatique avant le premier accès à Internet. Cette fonctionnalité répond parfaitement à la problématique de diffusion de cette charte vers les utilisateurs du CH de Montbert. Les responsabilités de chacun sont alors décrites et connues de tous.

En conclusion, le choix technique se porte sur les fonctionnalités de la solution Olfeo et la capacité d'adaptation du produit à l'environnement du CH de Montbert.

8.3 Choix d'une solution de sécurisation des flux messagerie

Afin de sécuriser les flux de messagerie, plusieurs produits ont fait l'objet d'une période d'évaluation. La passerelle IMSVA de Trend Micro sous forme de serveur virtuel et la solution Vade Retro MailCube2 également en serveur virtuel mais qui dispose des mêmes fonctionnalités

en appliance. Les produits Websens hosted Email Security et Mail In Black, non évalués en production, ont tout de même été étudiés.

Tout d'abord, la solution IMSVA de Trend Micro a été déployée en production sur le CH de Montbert. L'antivirus, comme pour le filtrage des flux Internet, est extrêmement performant et embarque de nombreuses options de configuration. Le principe d'un filtrage en amont du CH de Montbert parait intéressant. Cependant, une double administration est à mettre en place, pour gérer à la fois le serveur virtuel et les règles de filtrage distantes. Le module de filtrage des adresses IP est une licence complémentaire non intégrée dans la licence de base, ce qui est regrettable par rapport aux concurrents. Pendant l'évaluation, il n'a pas été recensé d'attaques depuis l'extérieur. La question de l'acquisition de ce module doit être posée. L'anti spam, quant à lui, nécessite une longue période d'apprentissage pour remplir sa fonction. En effet, il a été impératif de construire des listes de mots-clés pour trier les spams et les publicités illégitimes, des newsletters légitimes. La configuration devient vite complexe car chaque client a accès au moteur de règles, qu'il peut administrer lui-même. Ceci est un avantage en terme de personnalisation, mais peu devenir un inconvénient, car les administrateurs doivent régulièrement vérifier l'efficacité des filtres mis en place. Enfin, il n'existe pas de filtre « anti-pubs » ce qui pour le CH de Montbert peut être un inconvénient majeur car une grande part des courriels réceptionnés sont de la publicité. La solution IMSVA, est d'un bon rapport qualité/prix mais doit faire l'objet d'analyses régulières pour optimiser le filtrage.

Une demande d'évaluation de la solution Websense Hosted Email Security avait été demandée, mais n'a pas été effectuée. Une modification de l'enregistrement MX était nécessaire pour rediriger tous les flux de messageries vers les serveurs Websense et non vers ceux du CH de Montbert. Cependant, il a été possible d'accéder à l'interface de gestion sans basculer les flux. Celle-ci est identique à celle utilisée pour la partie de filtrage Internet, peu ergonomique, non attrayante. Un système de listes blanches et noires est à administrer. Il n'y a pas d'accès direct au moteur de règles. Enfin, les services de rapports disponibles ne sont pas personnalisables. L'utilisation de la console « Triton » parait indispensable pour pouvoir gérer ses logs et ses listes. La version logicielle déployée en mode hébergé n'est pas la même que celle déployée dans les appliances et dispose par conséquent de moins de fonctionnalités. La société internationale Websense cherche cependant à harmoniser ses versions pour offrir un meilleur service aux clients qui font le choix du mode hébergé.

Le CH de Saint Nazaire a fait l'acquisition de la solution Mail In Black, en mode hébergé. La philosophie appliquée pour le filtrage est la mise en œuvre du test de Turing, qui consiste à demander à l'expéditeur de s'authentifier manuellement avant d'être placé en liste blanche. Le déploiement d'une telle solution implique de remettre à plat tous les carnets d'adresses des utilisateurs et d'y associer une communication importante, internet et externe. En effet, l'anti spam du CH de Montbert classait toujours les messages d'authentification comme spams. Les « utilisateurs expéditeurs » ne pouvaient s'authentifier. Par conséquent, les destinataires ne pouvait le recevoir. Les fonctionnalités offertes en mode hébergé sont restreintes, voire nulles.

Figure 76 : Page d'accueil de Mail In Black (CHSN)

Les statistiques fournies sont sous forme de tableaux et réduites au minimum. Il n'existe pas d'option de personnalisation.

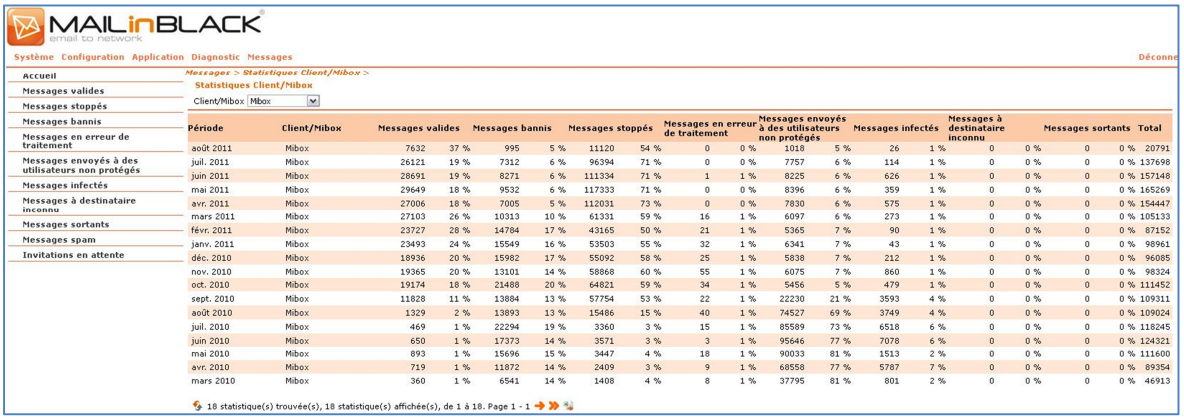


Figure 77 : Exemple de statistiques disponibles avec Mail In Black (CHSN)

En cas de problème sur une adresse email spécifique, un ticket doit être ouvert auprès de la société pour étudier les solutions à apporter. L'intervention ne peut donc être immédiate. De plus, cette technique de filtrage ne prend pas en compte le cas du piratage de l'adresse électronique d'un utilisateur déjà enregistré en liste blanche. Il serait alors possible de continuer

à recevoir des spams via cette faille. La quarantaine, réservée à chaque utilisateur, est intuitive ce qui est utile pour l'utilisation au quotidien par les agents :

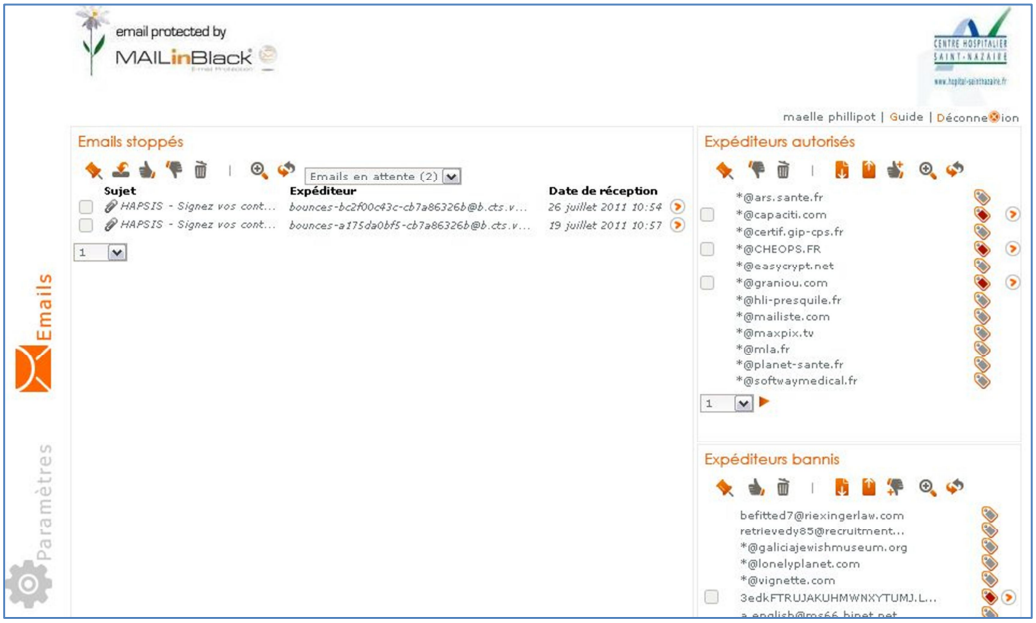


Figure 78 : Exemple d'une quarantaine utilisateur avec Mail In Black (CHSN)

Le CH de Saint Nazaire a souhaité conserver son antivirus Trend Micro en complément de cette solution de filtrage. Après un an de mise en place, le retour d'expérience parait positif car « ils n'ont rien à faire » sur cette solution.

Enfin, l'offre MailCube2 de la société Vade Retro a été évaluée sur une période de 15 jours. Cette solution est très intuitive, simple à administrer et surtout performante. En effet, elle dispose d'un filtre anti spams, antivirus heuristique et viral, mais aussi d'un filtre anti-publicités. Le message réceptionné subit des analyses en cascade (enveloppe, contenu, pièce jointe, …) afin de déterminer sa légitimité. Le filtrage réalisé se montre concluant, même s'il est nécessaire de débloquer certaines listes de diffusion reconnues. Le principal défaut de cette solution est la pauvreté de son module de statistique et les options réduites pour les analyses antivirus. L'accès au moteur de règles est impossible car il est entièrement géré par les équipes de Vade Retro qui sont chargées d'évaluer en continu les performances du moteur et de les optimiser. En effet, un mode « super-admin » pourrait être créé de façon à personnaliser certaines règles. La gestion de la quarantaine utilisateur est facile et certaines options, comme l'utilisation des alias, sont illimitées. Globalement cette solution sait se faire oublier et propose une alternative séduisante entre le mode hébergé et la complexité du produit Trend Micro. L'utilisation d'un cluster

d'appliances augmente encore cette simplicité. Des améliorations sont cependant attendues, notamment sur l'authentification des administrateurs et les rapports.

Les évaluations de tous ces produits ont aidé à déterminer quelle serait la solution de filtrage la plus appropriée à installer. La solution Vade Retro parait être la plus adaptée car elle répond aux besoins et reste facilement administrable. Le choix technique réalisé, les éléments financiers de chaque solution sont à prendre en considération.

8.4 Bilan financier

Les informations financières pour ces solutions ont été fournies par les intégrateurs en lien avec les éditeurs. Les coûts précisés sont fonction du mode de déploiement de chaque solution : en version matérielle, logicielle ou hébergé. La comparaison est difficile car les produits évalués ne proposent pas tous les mêmes fonctionnalités.

8.4.1 Bilan pour les solutions de filtrage Internet

L'annexe N présente un tableau récapitulatif des coûts d'acquisition de chaque solution.

Il est intéressant de constater que l'investissement à court terme, c'est-à-dire sur une période de 3 ans maximum, dans une solution en mode hébergé, parait avantageux sur le plan financier. En effet, il n'y a pas à maintenir de matériels, pas de contrat de support, ni de notion de disponibilité du service car tout l'environnement est géré par l'hébergeur. Cependant, sur une durée de 5 ans, ce constat est remis en cause, principalement en raison du mode de calcul appliqué. Généralement, la facturation en mode SaaS est établie sur la base d'un coût annuel par agent susceptible d'accéder à Internet. L'acquisition de 480 licences peut se montrer onéreuse. Or dans le cas d'un déploiement sur site avec du matériel, le poste client sert de base, soit 250 ordinateurs, près de deux fois moins que d'agents ! Globalement, au-delà de 4 ans, le choix d'un fonctionnement en mode hébergé est toujours plus coûteux que celui d'une version matérielle ou logicielle. En effet, il s'agit de la location d'un service (logiciel et coût de fonctionnement de l'hébergeur) et non d'un investissement.

Dans le cadre d'un déploiement sur site, il est nécessaire de déterminer si une appliance matérielle ou logicielle sera installée. Le choix d'une version logicielle, déployée sur la baie de stockage comme n'importe quel autre serveur virtuel supprime les coûts d'acquisition de l'appliance matérielle et la garantie associée. L'offre est donc moins coûteuse. Cependant, il faudrait ajouter à ces tarifs une part relative de l'investissement matériel engagé sur les serveurs physiques et la baie de stockage pour effectuer une comparaison plus juste. Enfin, l'offre en

appliance matérielle est la plus coûteuse, mais la plus adaptée aux besoins de performances, puisque la solution est autonome.

Les tarifs proposés par Trend Micro sont à considérer avec précaution. En effet, le CH de Montbert est déjà client et les coûts indiqués sont uniquement ceux pour le renouvellement et la migration vers IWSVA de la licence IWSS en place. L'éditeur refuse de préciser les prix publics. De plus, seul l'antivirus est déployé, car les licences de filtrage IP et d'URL n'ont pas été acquises. Seule la solution Olfeo affiche des prix publics, sans négociation, d'où le coût supérieur au produit Websense. Il est aussi à noter que les coûts pour les années 4 et 5, pour le renouvellement du support est moindre pour Olfeo et Websense que pour Trend Micro.

En conclusion, il faut prévoir une augmentation des coûts, liée au déploiement d'une solution de filtrage des flux Internet performante, de deux fois supérieurs ceux engagés à ce jour. Cependant les coûts de support seuls paraissent après la 4ème année, moins onéreux. Sur le même principe, des coûts indicatifs pour le déploiement des solutions de filtrage de flux de messagerie ont été demandés.

8.4.2 Bilan pour les solutions de filtrage de messagerie

L'annexe O présente un tableau récapitulatif des coûts d'acquisition de chaque solution de sécurisation pour la messagerie.

Tout d'abord, pour la sécurisation des flux de messagerie, il convient de prendre en compte que seules les adresses électroniques nominatives sont considérées. Les listes de diffusion ne sont pas protégées, pour les raisons déjà évoquées. Que ce soit en mode hébergé ou en local, les devis fournis protègent 250 boîtes aux lettres utilisateurs. Les protections intégrées de base sont un antivirus, un anti-spam et une quarantaine utilisateur par adresse protégée. Certains éditeurs intègrent aussi un antivirus heuristique et un filtre anti-publicités.

A l'image de la sécurisation des flux Internet en hébergé, l'externalisation de la solution de protection des messages est largement plus coûteuse, pour des raisons identiques aux frais de fonctionnement. Le principal avantage de cette architecture est de disposer d'un délai de conservation des messages en cas de coupure du lien réseau avec l'établissement, variant de 3 à 5 jours selon les éditeurs. Mais, le fournisseur d'accès Internet peut aussi proposer ce service à moindre coût, avec l'activation d'un relai SMTP. Le déploiement sur le site local est donc le plus avantageux.

Le choix d'architecture entre serveur virtuel ou matériel est ici plus aisé. En effet, la différence est faible voir même à l'avantage de la solution physique, suivant le mode de licences. La solution Vade Retro est la plus intéressante sur le plan financier et technique car elle intègre dans les coûts présentés, une architecture haute disponibilité avec l'installation de deux appliances et de toutes les protections offertes par l'éditeur. De plus, la mise à disposition de la « quarantaine administrative » permet d'assurer aussi le filtrage sur les listes de diffusion, même si cet espace doit être géré par les administrateurs de la solution. Cette option n'est pas disponible pour tous les produits et peut imposer de conserver une solution tierce de filtrage uniquement pour le cas particulier des listes de diffusion, comme cela est le cas au CH de Saint Nazaire.

Pour conclure, le déploiement d'une solution de filtrage des flux de messagerie beaucoup plus performante implique une augmentation des coûts par un facteur 2 par rapport à ceux engagés à ce jour avec la solution IMSS et la maintenance du serveur proxy. A la vue des évaluations effectuées, les messageries des utilisateurs ne seraient pas mieux protégées au niveau antivirus, mais beaucoup plus au niveau du filtrage des spams et publicités, offrant ainsi un gain de temps dans la gestion de la boîte aux lettres de chaque utilisateur. Le gain financier reste difficile à évaluer.

8.4.3 Bilan financier du projet de sécurisation

L'annexe P présente un comparatif des coûts entre un renouvellement de la solution actuelle et l'acquisition de nouveaux services.

Ce tableau illustre les investissements supplémentaires nécessaires à mettre en œuvre pour l'acquisition des deux solutions retenus à la suite de mes évaluations. L'association des solutions Olfeo et Vade Retro doublerait l'investissement financier dégagé à ce jour sur cinq ans, par rapport à la solution de Trend Micro IWSVA et IMSVA.

Ces éléments financiers sont à considérer avec précaution car le CH de Montbert est déjà client des produits Trend Micro et les tarifs présentés dans ce document tiennent compte de cette « fidélité ». Des négociations de prix sont néanmoins possibles avec les éditeurs Olfeo et Vade Retro, car les prix présentés sont les prix publics. Ils devraient être beaucoup plus compétitifs dans le cadre des réponses aux futures consultations.

L'acquisition de ces solutions, après validations des éléments techniques et financiers doit être associée à un planning de déploiement.

8.5 Proposition de plannings de déploiement

8.5.1 Pour une solution de filtrage des flux Internet

Le déploiement d'une solution de sécurisation des flux Internet s'instaure dans le temps. L'annexe Q propose un planning de mise en œuvre incluant les phases de consultation et d'intégration.

Ce planning se découpe en deux parties : la consultation publique et l'intégration. Le nombre de jour de mise en œuvre peut paraître élevé, mais il inclut une phase d'observation des comportements utilisateurs. En effet, il est impératif de connaître les habitudes de navigation pour élaborer les règles de filtrages les plus pertinentes. Ces optimisations seront chronophages car les comportements évoluent avec les technologies et les contenus disponibles.

Enfin, une communication poussée à destination de tous les personnels est impérative. Celle—ci apportera une meilleure vision des responsabilités de chacun et permettra d'insister sur les aspects réglementaires à l'origine du déploiement d'une solution de filtrage. La charte informatique revue dernièrement sur le CH de Montbert devra prendre en compte les spécificités de la solution retenue et les mentionner le cas échéant.

Pour conclure, la date de mise en production finale pourrait intervenir six mois après le début du projet, soit 75 jours après le début de la phase d'intégration. Le contrat de maintenance de la solution actuelle arrive à son terme le 31/12/2012. Le projet devrait être lancé à la fin du premier semestre 2012 pour respecter la date de fin de maintenance de la solution actuelle.

8.5.2 Pour une solution de filtrage des flux de messagerie

Le déploiement d'une solution de sécurisation des flux de messagerie nécessite aussi une supervision dans le temps. L'annexe R propose un planning de mise en œuvre incluant les phases de consultation et d'intégration.

De la même manière, le planning est découpé entre la phase de consultation publique et la phase d'intégration. Sur cette dernière, le temps de mise en œuvre est extrêmement variable et dépend de la solution retenue. Ainsi, pour Trend Micro ou Vade Retro, l'installation de la solution peut-être transparente aux utilisateurs. Dans le cas de la solution Mail In Black, cette période peut-être plus longue car elle implique de réinitialiser tous les carnets d'adresses utilisateurs et de surveiller les flux pour éviter des pertes de messages.

En complément de l'intégration, le déploiement d'une quarantaine utilisateur nominative doit être associé à une communication forte, des supports et si besoin des formations pour illustrer le

fonctionnement global. Ce changement peut intervenir boîte aux lettres par boîtes aux lettres. Ce mode de migration sera plus long, car personnalisé mais permettra de mieux accompagner les utilisateurs à ce changement, afin que chacun gère sa propre quarantaine, sans intervention du service informatique. Quelques semaines sont suffisantes pour s'approprier les solutions, celles-ci étant très intuitives.

Enfin, la date de mise en production de la solution pourrait être effective en moins de six mois, répartie entre une phase de consultation de quatre mois et une phase d'intégration et de formation de deux mois. A l'image de la solution de filtrage Internet en place, le contrat de maintenance arrive à son terme le 31/12/2012. Le projet devrait aussi être initié au plus tard à la fin du premier semestre 2012 pour respecter cette date de fin de maintenance de la solution actuelle.

9 Conclusion

Les solutions déployées sur le CH de Montbert ne permettent plus de répondre aux exigences de sécurité minimum et ainsi de faire face à l'évolution des besoins et de la réglementation. Ainsi, l'antivirus Trend Micro associé à un proxy squid pour la gestion des listes de réputation ne permet pas d'assurer la traçabilité, l'authentification et les spécificités par unité de soins, du moins dans un temps limité, avec une équipe informatique réduite. Pour les flux de messageries, l'antivirus couplé avec la solution libre spam assassin montre les mêmes difficultés de performances, pour la lutte contre le spam et les publicités, mais aussi de maintenance. Or les actualités présentent régulièrement des piratages ou attaques dans le but de dérober des informations. La préservation du secret médical est une règle d'or et tous les moyens doivent être mis en œuvre pour limiter au maximum ou rendre impossible le vol de données sur l'établissement.

Dans ce contexte, le CH de Montbert montre une détermination forte à sécuriser ses communications dans un environnement en permanente mutation. Le respect de la législation en vigueur est aussi capital. La mise en œuvre d'outils de filtrage n'a pas pour but d'instaurer un espionnage des salariés, mais de leur offrir plus de services et d'accès, tout en cherchant à responsabiliser les usages et par conséquent à inciter les agents à modifier leurs comportements. En complément de ces outils, des communications spécifiques doivent être mises en place pour informer, sensibiliser et former les agents. Ainsi la révision de la charte informatique, ou la création d'une charte Internet plus simple et d'une charte de connexions des prestataires extérieurs sont des exemples des démarches parallèles à accomplir. Le succès du déploiement de ces solutions est impossible sans une implication forte de la direction de l'établissement. En effet, le service informatique ne doit pas être ni l'instigateur, ni le décisionnaire des politiques de filtrage.

Pour réaliser ces objectifs, différents produits ont été évalués. La comparaison point par point est impossible car chacun ne dispose pas des mêmes fonctionnalités ou services. Cependant, la solution de filtrage des flux Internet Olfeo semble être la plus pertinente à la vue des exigences du CH de Montbert. De même, l'offre MailCube2 de Vade Reto pour la messagerie apporte la meilleure réponse. Ces deux solutions, sous forme d'appliance, ne nécessitent pas de temps d'administration importants et libèrent le service informatique de ces contraintes, tout en répondant aux critères de disponibilités et de performance. En contrepartie, les coûts

d'acquisition et de maintenance sont d'un tout autre ordre que ceux engagés ces dernières années. Toutes les problématiques de sécurisation ne sont pas pour autant résolues.

En effet, seule la sécurisation des flux Internet et de messagerie depuis le CH de Montbert a été traitée. Or, le développement des communications mobiles de 3ème et 4ème génération offre la possibilité de consulter Internet ou ses messageries personnelles directement sur le terminal mobile. Par conséquent, il est impossible de contrôler l'ensemble des flux. La communication, l'information et l'appel aux responsabilités de chacun sont les clés pour sécuriser un environnement dans lequel la technique seule ne peut pas tout résoudre.

10 Glossaire

ARM : Advanced Reporting Manager, solution Trend Micro qui, associée à IWSVA, permet de fournir un module de rapports et de statistiques plus performant.

Cloud computing est un concept informatique qui consite à déporter l'exécution d'applications sur des serveurs accessible depuis Internet au lieu de conserver ses applications en interne ou bien sur des postes de travail.

Bots : Un bot informatique est un agent logiciel automatique ou semi-automatique qui interagit avec des serveurs informatiques. Un bot se connecte et interagit avec le serveur comme un programme client utilisé par un humain, d'où le terme « *bot* », qui est la contraction de « *robot* ».

CHSCT : Comité d'Hygiène et de Sécurité des Conditions de Travail est une institution représentative du personnel au sein de l'entreprise.

CNIL : Commission Nationale Informatique et Liberté est une autorité administrative consultative et indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

DADVSI : **Droit d'Auteur et Droits Voisins dans la Société de l'Information** est une loi française issue de la transposition en droit français de la directive européenne 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

DKIM : **Domain Keys Indentified Mail** est une norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique. Elle constitue une protection efficace contre le spam et l'hameçonnage.

DOS : **Denial Of Service**, ou déni de service est une attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser, en saturant le réseau, en bloquant les accès ou en perturbant le dialogue entre des machines.

DMZ : **Zone DéMilitarisée** est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

FAI : Fournisseur d'Accès à Internet

GPO : Group Policy Object ou stratégies de groupes, sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory.

HWS : **Hosted Web Security** est la solution hébergée de filtrage des flux Internet de la société Websense.

IMSS : **Interscan Messaging Security Server** est une ancienne solution de filtrage des flux de messagerie. Elle est remplacée à ce jour par IMSVA.

IMSVA : **InterScan Messaging Security Virtual Appliance** est la solution de passerelle logicielle pour la sécurisation des flux de messagerie de la société Trend Micro.

IWF : **Internet Watch Foundation** est une organisation anglaise indépendante qui cherche à lutter contre les contenus illégaux sur Internet. L'IWF travaille en collaboration avec les services de police et les FAI, à qui elle transmet une liste noire de contenus potentiellement illégaux, ensuite utilisée pour en censurer l'accès à leurs clients.

IWSS : **Interscan Web Security Server** est une ancienne solution de filtrage des flux Internet. Elle est remplacée à ce jour par IWSVA.

IWSVA : **InterScan Web Security Virtual Appliance** est la solution de passerelle logicielle pour la sécurisation des flux Internet de la société Trend Micro.

LDAP : **Lightweight Directory Access Protocol** est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire.

Nagios : application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes vont mal et quand ils vont mieux. C'est un logiciel libre sous licence GPL.

NTIC : Nouvelles Technologies de l'Information et de la Communication

OCLCTIC : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

Open source : logiciels dont la licence respecte des critères précisément établis par l'*Open Source Initiative*, c'est-à-dire la possibilité de libre redistribution, d'accès au code source et aux travaux dérivés.

OSSIR : **Observatoire de la Sécurité des Systèmes d'Information et des Réseaux** est une association à but non lucratif (loi de 1901) existant depuis 1996 qui regroupe les utilisateurs intéressés par la sécurité des systèmes d'information et des réseaux.

PHF : **Predictive Heuristic Filter** : moteur de filtrage heuristique développé par la société Vade Retro afin de protéger les comptes de messageries des utilisateurs des spams et autres attaques.

Phishing ou **hameçonnage** : technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

Pharming (ou **dévoiement**) : technique de piratage informatique exploitant des vulnérabilités DNS. Cette technique consiste à rediriger une requête DNS pour un nom de domaine vers un site frauduleux et non pas vers l'IP réelle du nom de domaine.

RBL : **Realtime Blackhole List** est une liste de serveurs réputés comme grands envoyeurs de spams qui sont aussi charger de « ficher » les spammeurs.

Rootkit : ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible.

RTSP : **Real Time Streaming Protocol** est un protocole de communication de niveau applicatif (niveau 7 du modèle OSI) destiné aux systèmes de streaming média.

SaaS : **Software As A Service** est un concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence.

SAN : Stockage Area Network est un réseau spécialisé permettant de mutualiser des ressources de stockage.

SMB : **Server Message Block** est un protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows.

SPF : **Sender Policy Framework** est une norme de vérification du nom de domaine de l'expéditeur d'un courrier électronique, normalisé dans la RFC 4408. L'adoption de cette norme est de nature à réduire le spam.

SPN : **Smart Prevention Network** est un réseau de protection dans le Cloud fournit par Trend Micro pour sécuriser les échanges en amont des serveurs clients.

Spyware : logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.

SOCKS : protocole réseau qui permet à des applications client-serveur d'employer d'une manière transparente les services d'un pare-feu. SOCKS est l'abréviation du terme anglophone « *sockets* » et « *Secured Over Credential-based Kerberos* ».

SSL : Secure Sockets Layer est un protocole de sécurisation des échanges sur Internet

ThreatSeeker constitue le fondement technologique des solutions de sécurité du Web, de la messagerie et des données de Websense. Ce réseau permet de récupérer des informations sur l'évolution du web afin de mieux préparer les solutions de sécurisations.

Thor : est un réseau mondial décentralisé de routeurs, organisés en couches, appelés *nœuds* de l'oignon, dont la tâche est de transmettre de manière anonyme des paquets TCP. C'est ainsi que tout échange Internet basé sur TCP peut être rendu anonyme en utilisant Tor.

TLS : **Transport Layer Security**, protocole qui remplace aujourd'hui le SSL.

Virus : logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans les programmes légitimes appelés « hôtes »

Ver : logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

11 Références bibliographie

11.1 Ouvrages

[**DEIBERT-AD**] : DEIBERT R, PALFREY J., ROHOZINSKI R., ZITTRAIN J., 2008 eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press : cet ouvrage permet de découvrir et d'analyser les différentes pratiques de filtrage dans le monde.

[**DEIBERT-AC**] DEIBERT R, PALFREY J., ROHOZINSKI R., ZITTRAIN J., 2010, eds., *Access Controlled: The shapping of power, rights and rule in cyberspace*, Cambridge: MIT Press : cet ouvrage présente les moyens de contrôles des flux mis en oeuvre dans le monde.

[**FERRARI**] : FERRARI H., 31 Octobre 2005, *Web and Information Security*, p 112 : Suite de chapitres décrivant l'état de l'art sur des sujets liés à la sécurité de l'information sur le Web.

[TANENBAUM] TANENBAUM A, 2003, *La couche application In Réseaux* 4ème édition. HALL P., Pearson, Education

11.2 Etudes, guides, rapports et livres blancs

[**CNIL-EMPSAL**] : Guide pratique de la CNIL « pour les employeurs et les salariés », édition 2010, fiche n°6.

[**CNIL-CYB**] : Rapport de la CNIL « *La cybersurveillance sur les lieux de travail* », édition mars 2004, p. 12.

[**ESPERN1**] : Christophe Espern, « *Principe, intérêts, limites et risques du filtrage hybride à des fins de blocage de ressources pédopornographiques hébergées sur des serveurs étrangers* », La quadrature du net, 2008, [en ligne], http://www.laquadrature.net/files/note-quadrature-filtrage-hybride.pdf

[**MARPIJ**] : Cabinet d'étude Marpij & Insight, 3 juillet 2009, « *Etude d'impact du blocage des sites pédopornographiques* »,

11.3 Revues et périodiques

[**MISC-TOR**] : BIDOU R., mars/avril 2011, *Multi-System & Internet Security Cookbook*, numéro 54, , p38-43.

[**MISC-HADOPI**] : BIDOU R., mars/avril 2011, *Multi-System & Internet Security Cookbook*, p35-37.

11.4 Presse écrite et radios

[**COLOMBAIN**] : COLOMBAIN J., 26/07/2011 ,« *Les botnets : ces réseaux d'ordinateurs zombies* », France info rubrique high-tech, http://www.france-info.com/chroniques-pirates-du-nouveau-monde-2011-07-26-les-botnets-ces-reseaux-d-ordinateurs-zombies-551996-29-35.html

[**LE POINT**] : NEUER L., 20/09/2010, « *HADOPI, Quel impact juridique pour les entreprises ?* », [en ligne], http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/hadopi-quel-impact-juridique-pour-les-entreprises-20-09-2010-1238560_56.php

[**LE MONDE 1**]. http://www.lemonde.fr/economie/article/2011/03/07/bercy-victime-d-une-vaste-operation-de-piratage-informatique_1489228_3234.html

[**MARPIJ**] : cabinet Marpij, cabinet Inside, juillet 2009, « *Rapport 'impact sur le filtrage* »

[**NYTIMES**] : BILTON N., STELTER B., 26/04/2011, Sony says Playstation hacker got personal data, [en ligne], http://www.nytimes.com/2011/04/27/technology/27playstation.html

11.5 Editeurs de solutions informatique

[**MAILINBLACK**] : MailInBlack, *Spam – Le livre blanc*, [en ligne], 2006, http://assiste.com.free.fr/ftp/livre_blanc_le_spam.pdf

[**SYMANTEC**] : Symatec, 2009, « *rapport d'étude sur l'évolution du spam* ».

[**TREND MICRO**] : Trend Micro, documentation technique d'installation de la solution IMSVA ou IWSVA

[**TMIWSVA1**] : Trend Micro, « *Sizing guide* », 16 février 2011, [en ligne], http://downloadcenter.trendmicro.com/index.php?regs=fr&clk=latest&clkval=1747&lang_loc=7

[**WEBSENSE**] : solution Hosted Web Security de l'éditeur Websense.

[**WEBSENSE1**] : Jon Crotty, « *2010, Rapport sur les menaces* », décembre 2010, [en ligne], http://www.websense.com/assets/reports/report-security-labs-threat-report-2010-

fr.pdf?cmpid=EmailSocialWebBirdsFRApr11&wsid=0032000000VH8aHAAT&linkid=Rapport+Websense+2010+sur+les+menaces

[**ZEROSPAM**] : Editeur de solution Zerospam, « *Architecture de filtrage* », [en ligne], http://www.zerospam.ca/1/Services/La_solution_ZEROSPAM/Architecture_de_filtrage

11.6 Articles sur Internet

[**ALTOSPAM**] : Altospam, 09/2008, « *Configuration des serveurs de messagerie et filtrage des destinataires* », http://www.altospam.com/actualite/2008/09/configuration-des-serveurs-de-messagerie-et-filtrage-des-destinataires/

[BECHETOILLE] : BECHETOILLE B., 26/02/2011, « *Le deep packet inspection est-il une arme ?* », [en ligne], http://reflets.info/deep-packet-inspection-qosmos-techtoctv/

[CLAYTON1] : CLAYTON R., 2006, *Filtrage sur l'URL par injection de paquet RST*, Murdoch, Watson : Ignoring the Great Firewall of China. University of Cambridge, Computer Laboratory, http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

[CLAYTON2] : CLAYTON R., 2006, Filtrage hybride (Cleanfeed, WebMinder, NetClean), *Failures in a Hybrid Content Blocking System*. 2005, University of Cambridge, Computer Laboratory, http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf

[DORNSEIF] : DORNEISIF M., 2003, *Government mandated blocking of foreign Web content*, http://md.hudora.de : techniques de blocage de flux

[**EDELMAN1**] : EDELMAN B., 2003, *Web Sites Sharing IP Addresses: Prevalence and Significance*, Berkman Center for Internet and Society at Harvard Law School, http://cyber.law.harvard.edu/archived_content/people/edelman/ipsharing

[**EDELMAN2**]: EDELMAN B., 04/2003, *Internet Filtering in China*, http://www.benedelman.org/publications

[**ENFANTS-NET3**] : BAUP L., MELISON D., 29/12/2008, *Les enfants du Net III, Conditions nécessaires à la mise en place du filtrage des sites pédopornographiques par les FAI*, [en ligne], http://www.foruminternet.org/institution/espace-presse/communiques-de-presse/IMG/pdf/reco-enfantsIII_finale.pdf : Recommandations portant sur la mise en place de solutions de filtrage et sur les solutions administratives et judiciaires pour filtrer les sites pédopornographiques.

[**GALLOT**] : GALLOT K., 03/2005, « *Les méthodes anti-spam* », [en ligne], http://www.secuser.com/dossiers/methodes_antispam.htm

[**GRAHAM1**] : GRAHAM P., 08/2002, « *A plan for spam* », [en ligne], http://www.paulgraham.com/spam.html

[**GRAHAM2**] : GRAHAM P., 09/2002, « *Filters vs Blacklists* », [en ligne], http://www.paulgraham.com/falsepositives.html

[**HASSANE**] : HASSANE O., 10/2009, « *Étude des techniques. de classification et de filtrage automatique de Pourriels* », Ecole Polytechnique de Montreal, [en ligne], http://www.slideshare.net/guest3a44d425/tude-des-techniques-de-classification-et-de-filtrage-automatique-de-pourriels-3644963

[**KWAN**] : KWAN P., 08/2009 « Trend Micro Software Virtual Appliance, Best Practices for VMware", [en ligne], http://trendedge.trendmicro.com/pr/tm/te/document/VMWare_Best_Practices_for_SVAs_090803.pdf

[**LAGADEC**] : LAGADEC P., 2005, « *Filtrage de messagerie et analyse de contenu* », [en ligne], http://actes.sstic.org/SSTIC04/Filtrage_messagerie/SSTIC04-article-Lagadec-Filtrage_messagerie.pdf

[**OSSIR**] : Groupe de travail de l'OSSIR, Livre blanc sur les logs, 06/11/2009, [en ligne], http://www.ossir.org/uploads/media/OSSIR_Livre-blanc_Logs_v1.pdf

[**MANENTI**] : MANENTI B., 03/2011, Le Nouvel Observateur, « *Bercy victime d'un pdf piégé* », [en ligne], http://tempsreel.nouvelobs.com/actualite/societe/20110307.OBS9242/bercy-victime-d-un-pdf-piege.html

[**NSP**] : Cabinet de consulting Network Strategy partners, « *Next generation DPI : an overview of requirements an applications*», mars 2007, [en ligne], http://0299d3f.netsolhost.com/NewPages/DPI.pdf

[**QUADRATURE1**] : La quadrature du Net, 2009, « *Riposte graduée » : inefficace, inapplicable et dangereuse* », [en ligne], http://www.laquadrature.net/files/LaQuadratureduNet-20090207_Riposte-Graduee_inefficace-inapplicable-dangereuse_2pages.pdf

[**RFC821**] : Jonathan B. Postel, « *Simple Mail Transfert Protocol* », août 1982, [en ligne], http://www.ietf.org/rfc/rfc0821.txt

[**SET**] : Scunthorpe Evening Telegraph, Tuesday, 9 avril 1996,

[**SQUID**] :site Internet de la solution, mis à jour le 23/07/2011, http://www.squid-cache.org/

[**SQUIDGUARD**] : site Internet de la solution http://www.squidguard.org/index.html

[**HARNETT**] : Dermot Harnett, "*State of spam*", septembre 2009, [en ligne], http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_09-2009.en-us.pdf

12 Liste des illustrations

13 Annexes

Annexe A - Rappels sur les réseaux

Annexe B – Architecture WAN actuelle du CH de Montbert

Annexe C – Architecture de filtrage actuelle des flux Internet

Annexe D – Architecture de filtrage des flux Internet en mode appliance logicielle avec Trend Micro IWSVA et ARM

Annexe E – Architecture de filtrage des flux Internet en mode SaaS Websense Hosted Web Security

Annexe F – Architecture de filtrage des flux Internet en mode appliance matérielle Olfeo

Annexe G – Liste des catégories d'url de l'éditeur Olfeo

Annexe H – Liste des filtrages protocolaires supportés par l'éditeur Olfeo

Annexe I – Rapports d'activités de l'évaluation de la solution Olfeo

Annexe J - Architecture de filtrage actuelle des flux de messagerie

Annexe K - Architecture de filtrage des flux de messagerie en appliance logicielle avec Trend Micro IMSVA

Annexe L - Architecture de filtrage des flux de messagerie en mode hébergé

Annexe M - Architecture de filtrage des flux de messagerie en appliance logicielle avec Vade Retro MailCube2

Annexe N – Bilan financier des solutions de filtrage des flux Internet

Annexe O – Bilan financier des solutions de filtrage des flux de messagerie

Annexe P – Bilan financier total du projet

Annexe Q – Planning de déploiement d'une solution de filtrage des flux Internet

Annexe R – Planning de déploiement d'une solution de filtrage des flux de messagerie

Annexe S : Organigramme de la direction générale du CH de Montbert.

Annexe A – Rappel sur les réseaux

1. Le modèle en couche OSI

Le modèle OSI (Open Systems Interconnection), « modèle de référence d'interconnexion de systèmes ouverts » a été créé à la fin des années 1970 par l'ISO (Organisation Internationale de Normalisation) afin de mettre en place un standard de communications entre ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre ordinateurs. En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire). Ainsi de nombreux réseaux incompatibles coexistaient. C'est la raison pour laquelle l'établissement de normes communes a été nécessaire.

Le rôle du modèle OSI consiste à standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles (pour peu qu'ils respectent scrupuleusement le modèle OSI).

Dans ce modèle, l'ensemble des protocoles d'un réseau informatique est décomposé en 7 parties appelées couches OSI ou niveaux, numérotées de 1 à 7. Les couches OSI respectent les principes suivants :

- Chaque couche décrit un protocole indépendamment des autres couches
- Chaque couche procure des services à la couche immédiatement supérieure
- Chaque couche requiert les services de la couche immédiatement inférieure

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, un entête (ensemble d'informations qui garantit la transmission) est ajouté au paquet de données, ce procédé s'appelle l'encapsulation. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'entête est lu, puis supprimé selon un procédé de décapsulation. Ainsi, à la réception, le message est dans son état originel...

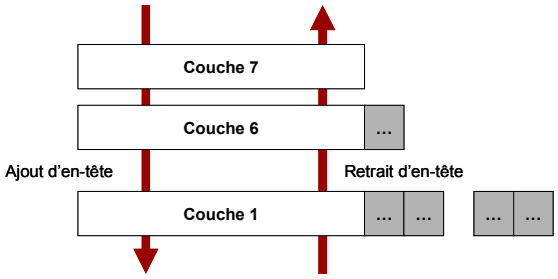


Figure 79 : Encapsulation des données (Marpij)

Les 7 couches du modèle OSI se décomposent en deux groupes. Le groupe « applicatif » ou les 3 couches supérieures définissent la façon dont les applications vont communiquer entre elles et avec les utilisateurs finaux. Le groupe « transport » ou les 4 couches inférieures définissent la façon dont les données sont transmises d'un point à un autre.

Numéro	Nom	Rôle
Couche 7	Application	C'est à ce niveau que sont les logiciels : navigateur, email, FTP, chat...
Couche 6	Présentation	Elle est en charge de la représentation des données (de telle sorte qu'elle soit indépendante du type de microprocesseur ou du système d'exploitation par exemple) et - éventuellement - du chiffrement.
Couche 5	Session	En charge d'établir et maintenir des sessions (c'est à dire débuter le dialogue entre 2 machines: vérifier que l'autre machine est prête à communiquer, s'identifier, etc.)
Couche 4	Transport	En charge de la liaison d'un bout à l'autre. S'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.
Couche 3	Réseau	En charge du transport, de l'adressage et du routage des paquets.
Couche 2	Liaison de	En charge d'encoder (ou moduler) les données pour qu'elles soient transportables par la couche physique, et

	données	fournit également la détection d'erreur de transmission et la synchronisation.
Couche 1	Physique	C'est le support de transmissions lui-même: un fil de cuivre, une fibre optique, les ondes hertziennes...

Tableau 1 : Description des couches du modèle OSI (Marpij)

Ce modèle a fait l'objet d'implémentations chez divers constructeurs, mais sans succès commercial, le marché s'étant largement orienté vers le modèle à 4 couches 'TCP/IP' de Internet, plus facile à comprendre et pour lequel existaient déjà des implémentations et une communauté d'utilisateurs précurseurs : le monde académique.

2. Le modèle de l'Internet

L'ensemble des protocoles utilisés par Internet est souvent appelé TCP/IP, d'après le nom de deux de ses protocoles : TCP (Transmission Control Protocol) et IP (Internet Protocol), qui ont été les premiers à être définis.

Le modèle TCP/IP, inspiré du modèle OSI, reprend son approche en couches.

2.1. La couche réseau – Niveau 3

Chaque fichier (ou donnée) transitant sur Internet est décomposé en paquets. Cette couche s'occupe de l'acheminement de ces paquets de données à travers les réseaux. Elle gère le routage (mécanisme par lequel les données d'un équipement expéditeur sont acheminées jusqu'à leur destinataire, même si aucun des deux ne connaît le chemin complet que les données devront suivre.), l'adressage, le traitement des congestions et l'interconnexion de réseaux hétérogènes. Le principal protocole utilisé dans cette couche est le protocole IP. IP gère la transmission des informations sur Internet. IP associe l'adresse IP de l'émetteur et celle du destinataire à chaque paquet transmis. Le destinataire est ainsi capable de connaître l'adresse IP de l'émetteur.

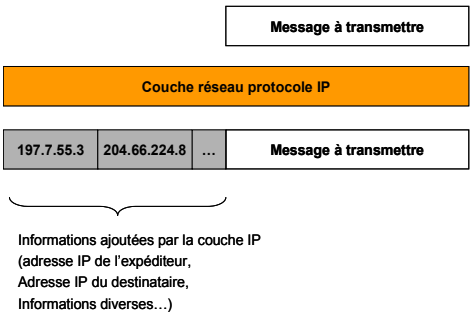


Figure 80 : Encapsulation par le protocole IP (Marpij)

2.2. La couche transport – Niveau 4

Les protocoles de la couche de transport peuvent résoudre des problèmes comme la fiabilité des échanges (« est-ce que les données sont arrivées à destination ? ») et assurer que les données arrivent dans l'ordre correct. Les protocoles de transport déterminent aussi à quelle application chaque paquet de données doit être délivré. Les deux principaux protocoles de cette couche sont UDP et TCP.

2.3. UDP (User Datagram Protocol)

UDP est un protocole simple qui ne vérifie pas que les paquets sont arrivés à destination, et ne garantit pas leur arrivée dans l'ordre. UDP est généralement utilisé par des applications de diffusion multimédia à temps réel (audio et vidéo, etc) pour lesquelles le temps requis pour gérer les retransmissions et l'ordonnancement des paquets n'est pas disponible, ou pour des applications basées sur des mécanismes simples de questions/réponses.

2.4. TCP (Transmission Control Protocol)

TCP est un protocole de transport « fiable » qui fournit un flux d'octets fiable assurant l'arrivée des données sans altérations et dans l'ordre, avec retransmission en cas de perte, et élimination des données dupliquées. Il gère aussi les données « urgentes » qui doivent être traitées dans le désordre. TCP essaie de délivrer toutes les données correctement et en séquence - c'est son but et son principal avantage sur UDP.

2.5. Le concept de ports

Aussi bien TCP qu'UDP sont utilisés simultanément par de nombreuses applications sur Internet (exemple ouvrir plusieurs navigateurs ou bien naviguer sur des pages HTML tout

en téléchargeant un fichier par FTP). Chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données.

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine : un port (la combinaison adresse IP + port est alors une adresse unique au monde, elle est aussi appelée socket).

L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau tandis que le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante. Il existe des dizaines de milliers de ports (65 536).

2.6. La couche application – niveau 7

C'est dans la couche application que se situent la plupart des programmes réseau.

Les applications fonctionnent au-dessus de TCP ou d'UDP, et sont souvent associées à un port bien connu. Les principales applications sont : POP, IMAP et SMTP pour le courrier électronique, HTTP pour l'accès aux sites Web, FTP pour le transfert de fichiers, SSH qui permet de chiffrer les communications, DHCP qui assigne automatiquement les adresses IP, IRC utilisé par les messageries instantanées, DNS qui fait correspondre adresse IP et nom de domaine.

Il existe ainsi des centaines de protocoles différents qui s'appuient sur TCP/IP ou UDP/IP. Si les protocoles publics sont publiés dans des RFC, il existe également des protocoles propriétaires connus ou non qu'il est probablement impossible de décoder sans en connaître les implémentations et/ou les algorithmes de chiffrement.

2.7. Les adresses

Il existe plusieurs types et formats d'adresses permettant d'accéder à des machines physiques, des applications ou à des contenus hébergés sur des machines en fonction du type d'application.

2.8. L’adresse IP

Une adresse IP est le numéro qui identifie chaque ordinateur connecté à Internet, ou plus généralement et précisément, l'interface avec le réseau de tout matériel informatique (routeur, imprimante) connecté à un réseau informatique utilisant le protocole Internet (IP).

Il existe des adresses IP de version 4 (IPv4) et de version 6 (IPv6). La version 4 est actuellement la plus utilisée. Elle est généralement notée avec quatre nombres compris entre 0 et 255, séparés par des points ; exemple : 212.85.150.134.

Dans chaque paquet envoyé à l'aide du protocole IP, l'en-tête spécifie le couple (adresse IP du destinataire, adresse IP de l'émetteur) afin de permettre au protocole de routage de router le paquet correctement et à la machine destinataire de connaître l'origine des informations qu'elle reçoit, donc d'y répondre si besoin est.

2.9. Masque de sous-réseau

Un masque de sous-réseau est une chaîne de caractères indiquant le nombre de bits d'une adresse IPv4 utilisés pour identifier le sous-réseau, et le nombre de bits caractérisant les hôtes (ce qui indique aussi le nombre d'hôtes possibles dans ce sous-réseau).

Les masques de sous-réseau utilisent la même représentation que celle des adresses IPv4. En IPv4, une adresse IP est codée sur 4 octets, soit 32 bits (représentés en notation décimale à point). Un masque de sous-réseau possède lui aussi 4 octets. Cependant, seules certaines valeurs sont autorisées : 0, 128, 192, 224, 240, 248, 252, 254, 255. Le masque 255.255.224.0 est donc valide. On utilise en pratique des masques constitués d'une suite de 1 suivie d'une suite de 0.

La notation 212.85.150.134/19 désigne donc l'adresse IP 212.85.150.134 avec le masque 255.255.224.0, et signifie que les 19 premiers bits de l'adresse sont dédiés à l'adresse du réseau et du sous-réseau, et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous-réseau.

2.10. Le nom de domaine

Dans le système de nom de domaine, il s'agit d'un identifiant de domaine, un domaine étant un ensemble d'ordinateurs reliés à Internet et possédant une caractéristique commune.

Le système de nom de domaine est une hiérarchie permettant la définition de sous-domaines. Il est composé d'au moins un mot, le label. S'il y a plusieurs labels, on doit séparer deux labels par un point. Dans un nom de domaine, le label d'extrême droite doit être choisi dans la liste des noms de domaine de premier niveau, appelé aussi domaine de tête. Il y a peu de restrictions dans la composition des labels précédant le label d'extrême droite.

Il existe deux types de domaine de premier niveau. Les domaines nationaux de premier niveau sont composés de deux lettres identifiant un pays ou un territoire indépendant (exemple : fr pour France, uk pour le Royaume-Uni). Les domaines de premier niveau génériques sont composés de trois lettres ou plus, identifiants généralement le secteur d'activité dans lequel opèrent les individus ou les organisations qui les utilisent (exemple : com pour commercial, org pour organisation à but non commercial) ;

Chaque domaine (ou sous-domaine) est peuplé d'hôtes, c'est-à-dire d'ordinateurs. Le nom de l'ordinateur apparaîtra avant le premier point en partant de la gauche. Par exemple, www.exemple.com désigne l'ordinateur www dans le domaine exemple.com.

2.11. L'URL

Une URL (pour Uniform Resource Locator), littéralement « localisateur uniforme de ressource », est une chaîne de caractères utilisée pour adresser les ressources du World Wide Web : document HTML, image, son, forum Usenet, boîte aux lettres électroniques, etc. Elle est informellement appelée adresse web.

Une URL absolue permet d'indiquer comment accéder à une ressource indépendamment de tout contexte où elle peut être précisée ou transmise. Elle commence par l'indication d'un schéma de représentation (spécifique au protocole de communication utilisé pour accéder à cette ressource), suivi de l'ensemble des paramètres permettant de localiser sur le réseau le service hébergeant la ressource, puis permet de préciser à ce service le nom d'une ressource à traiter, transmettre des données de traitement, acheminer et récupérer les résultats, puis de préciser éventuellement quelle partie de ce résultat sera utilisée.

Voici un exemple d'url : http://www.exemple.com/Dictionnaire/Url où www désigne la machine hôte dans le domaine exemple.com, Dictionnaire le chemin absolu sur le service contenant la page web et Url le nom de la page recherchée.

3. Les principaux éléments de réseau

Il s'agit ici de décrire la chaîne d'accès internet et les différents nœuds du réseau au travers desquels la connexion internet est établie et les paquets acheminés.

3.1. Carte d'accès - interface réseau

Une carte réseau est une carte d'extension d'ordinateur. Elle assure le rattachement d'un équipement informatique à un ensemble d'autres ressources connectées sur le même réseau. Les équipements communiquent sur le réseau au moyen de signaux qui doivent absolument respecter des normes.

Chaque carte réseau dispose d'une adresse MAC (Media Access Control address). Cette adresse est un identifiant physique utilisé pour attribuer mondialement une adresse unique au niveau de la couche de liaison (couche 2 du modèle OSI). C'est la partie inférieure de celle-ci (sous-couche d'accès au média – Media Access Control) qui s'occupe d'insérer et de traiter ces adresses au sein des paquets de données qui sont transmis.

3.2. Modem ou routeur d'accès

Le modem est un périphérique servant à connecter un réseau local, généralement domestique, avec un réseau distant par l'intermédiaire d'une ligne téléphonique, d'un câble coaxial ou d'une fibre optique. Il permet par exemple de se connecter à Internet, d'échanger des e-mails, de téléphoner ou de recevoir la télévision. Il est considéré comme le premier nœud de réseau car il est situé au plus près de l'utilisateur. Les modems modernes sont aujourd'hui équipés d'accès sans fil Wifi, de fonctionnalités de routeur d'accès permettant d'agréger le trafic de plusieurs machines locales et d'effectuer des fonctions de DHCP et NAT.

Le DHCP est un protocole permettant d'allouer dynamiquement des adresses IP aux machines locales en fonction de leur état d'activité. Le NAT est un protocole de translation d'adresse qui permet d'agréger sur une même adresse IP (en l'occurrence celle du modem ou routeur d'accès) les requêtes provenant de différentes machines locales identifiées par des adresses IP différentes.

3.3. Nœud d'accès réseau

Le nœud d'accès est un équipement de terminaison du réseau de l'opérateur qui assure la collecte et la distribution des flux de données des utilisateurs à travers la boucle locale : paire de cuivre, câble coaxial, fibre optique, interface radio…

3.4. DSLAM

Le DSLAM (Digital Subscriber Line Access Multiplexer) est un multiplexeur qui permet d'assurer sur les lignes téléphoniques un service de type DSL (ADSL, ADSL 2+, SDSL, …).

Techniquement, le DSLAM récupère le trafic de données, issu de l'utilisation des technologies DSL (internet haut débit, télévision par ADSL, VoIP …), transitant sur les lignes téléphoniques qui lui sont raccordées, après que ce trafic a été séparé du trafic de voix issu de la téléphonie classique, grâce à un filtre. Ensuite le DSLAM regroupe le trafic des différentes lignes qui lui sont raccordées et le redirige vers le réseau de l'opérateur ou du fournisseur d'accès selon le principe du multiplexage temporel où les données sont transportées en IP ou en ATM.

Géographiquement, le DSLAM se situe à la terminaison de la boucle locale (partie entre la prise téléphonique et le répartiteur).

3.5. CMTS

Le CMTS (Cable Modem Termination System) est l'équipement de tête de ligne utilisé par les « câblo-opérateurs » pour offrir des services (internet haut débit, télévision par ADSL, VoIP …) aux utilisateurs à travers un réseau Hybride Fibre-Câble (HFC). Il est équivalent du DSLAM en technologie DSL.

Pour offrir ces services, le CMTS est connecté en aval à la boucle locale HFC et en amont au réseau IP du câblo-opérateur. Il possède donc deux types d'interfaces : les interfaces RF (radio fréquences) du côté du réseau d'accès HFC, et les interfaces Ethernet (permettant le transporter le trafic IP) du côté du réseau IP d'agrégation.

3.6. BTS et Node B

La BTS (Base Transceiver Station) est un élément de base du système cellulaire de téléphonie mobile GSM. Elle est composée essentiellement d'un élément d'interface avec la

station de contrôle (BSC), d'un émetteur/récepteur (transceiver, *TRX*) et d'une antenne : elle forme ainsi une cellule (base du maillage du réseau). La BTS désigne le nœud d'accès dans les réseaux mobiles de deuxième génération (GSM ou 2G).

Dans la troisième génération de téléphonie mobile UMTS (3G), l'équivalent de la BTS est appelé NodeB. Il assure la transmission de la voix et des données à des débits bien supérieurs au GSM ce qui a permis de développer considérablement les applications sur mobile comme l'accès internet à haut débit ou encore la télévision mobile.

3.7. Réseau IP

Le réseau IP, est la partie du réseau de l'opérateur où les différents flux de données émanant des utilisateurs sont agrégés et transportés au moyen du protocole IP. Un réseau IP est constitué d'un ensemble de routeurs IP interconnectés entre eux.

Un routeur est un équipement de communication de réseau destiné à acheminer un trafic entre un émetteur et un destinataire. Son rôle est de déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé, afin que ce dernier atteigne sa destination finale le plus rapidement possible. Un routeur doit être connecté à au moins deux réseaux informatiques pour être fonctionnel. Le routeur crée et maintient une table dite de routage, qui contient les meilleures routes vers d'autres réseaux via les métriques associées à ces routes. Pour router les paquets, un routeur a besoin de:

- Connaître les adresses de destination,
- Identifier les sources par lesquelles il apprend,
- Découvrir les routes possibles pour atteindre une destination,
- Choisir la meilleure route,
- Maintenir et vérifier les informations de routage.

Le routeur gère la couche 3 du modèle OSI (donc IP). Il ne traite pas les données appartenant aux couches supérieures, couches transport et application. Il ne peut donc pas connaître les applications utilisées par les internautes.

Il existe différents types de routeurs en fonction de leur emplacement dans le réseau et de leur taille.

3.8. Les routeurs d'agrégation

Ils sont chargés de collecter le trafic provenant d'un ensemble de nœuds d'accès (DSLAM, CMTS…) et d'agréger ce trafic sur des interfaces de plus grande capacité afin de le router vers sa destination. Les routeurs d'agrégation sont caractérisés par un grand nombre et une forte granularité des interfaces physiques qui ne dépassent pas en général le 1 Gbit/s par interface.

3.9. Les routeurs de cœur

Les routeurs de cœur sont des équipements IP qui disposent d'une grande capacité de traitement et de routage. Leur capacité est multiple de 100 Gbit/s. Dans un réseau d'opérateurs, les routeurs de cœur sont moins nombreux que les routeurs d'agrégation et servent à fédérer les trafics de ces derniers. Ils sont également positionnés à la frontière avec les autres réseaux et servent à échanger le trafic internet entre pairs. On parle alors de « peering ». Cette technique consiste à établir des liaisons point-à-point à très haut débit entre les routeurs des différents FAI situés dans un même centre de co-localisation. Le protocole de peering utilisé est BGP.

3.10. Le protocole de routage BGP

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'au(x) destinataire(s). Le routage est effectué entre les *hôtes* qui émettent ou reçoivent les messages par l'intermédiaire des *routeurs*.

Il existe plusieurs types de protocoles de routage dans les réseaux IP. Les protocoles internes, capables de router des données à l'intérieur d'un système autonome, et les protocoles de routages externes qui sont utilisés entre systèmes autonomes. Le plus connu des protocoles de routage externes est le protocole BGP.

Sur Internet, un Système Autonome (Autonomous System ou AS) est un ensemble de réseaux IP sous le contrôle d'une seule et même entité, typiquement un fournisseur d'accès à Internet ou une plus grande organisation qui possède des connexions avec le reste du réseau Internet.

BGP (Border Gateway Protocol) est un protocole d'échange de route utilisé sur le réseau Internet. Son objectif est d'échanger des adresses réseaux (adresse IP + masque) avec ses voisins par le biais de sessions TCP sur le port 179.

BGP est utilisé pour transporter des paquets IP entre systèmes autonomes (AS) car il est le seul protocole à supporter de très grands volumes de données.

Les connexions entre voisins BGP (neighbours ou peers) sont configurées manuellement entre deux routeurs. Ils communiquent alors entre eux via une session TCP sur le port 179. BGP est le seul protocole de routage à utiliser TCP comme protocole de transport. Ces deux systèmes s'échangent des informations sur les réseaux qu'ils connaissent et sur le moyen de les atteindre. Ils ne connaissent pas l'intégralité des routeurs du réseau mais juste leurs voisins.

BGP est constitué de deux parties : Interior BGP (iBGP) et Exterior BGP (eBGP). iBGP est utilisé à l'intérieur d'un autonomous system alors que eBGP est utilisé pour relier deux AS.

BGP supporte l'agrégation de routes afin de limiter la taille de la table de routage. Depuis 1994, la version 4 du protocole est utilisée sur Internet, les précédentes étant considérées comme obsolètes. Ses spécifications sont décrites dans la RFC 4271 *A Border Gateway Protocol 4 (BGP-4)*.

3.11. Serveur

Un serveur est une machine ou un programme informatique qui partage un service. Ce service peut être, par exemple, de partager des ressources - comme ses périphériques et ses disques durs - avec d'autres ordinateurs clients sur un réseau. Le serveur communique avec les clients à l'aide de protocoles de communication, par exemple TCP/IP, qui est le protocole le plus utilisé sur Internet.

Un serveur HTTP ou serveur Web est un logiciel servant des requêtes et respectant le protocole de communication client-serveur HyperText Transfer Protocol (HTTP), qui a été développé pour le World Wide Web. Une machine sur laquelle tourne un serveur HTTP est appelée serveur Web. Le terme « serveur Web » peut aussi désigner le serveur HTTP (le logiciel) lui-même. Les deux termes sont utilisés pour le logiciel car le protocole HTTP a

été développé pour le Web et les pages Web sont en pratique toujours servies avec ce protocole.

Un serveur FTP (pour File Transfer Protocol) permet, comme son nom l'indique, de transférer des fichiers par Internet. Si vous en avez l'autorisation, vous pouvez télécharger et envoyer des fichiers sur un ordinateur distant faisant fonctionner un tel serveur.

Un serveur Mail est un logiciel de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client e-mail, soit un webmail, qui se charge de contacter le serveur pour envoyer ou recevoir les messages. La plupart des serveurs de messagerie possèdent ces deux fonctions (envoi/réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs.

3.12. Proxy

Au sens le plus général du terme, un proxy est un serveur mandataire qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Un serveur proxy peut offrir d'autres fonctionnalités comme le contrôle d'accès. Il peut agréger les demandes d'accès à une ressource partagée. Il offre la possibilité de filtrer et rejeter les demandes selon des critères fixés par l'administrateur du réseau, comme des demandes d'accès non autorisées à des fichiers propriétaires. Son rôle peut aussi être d'identifier et d'authentifier les utilisateurs.

Les serveurs proxy sont notamment utilisés pour assurer les fonctions suivantes :

- Mémoriser des contenus – on parle alors de serveur Cache
- Relayer les requêtes internet – on parle alors de proxy http
- Relayer les requêtes DNS – on parle alors de proxy DNS

La plupart des FAI ont abandonné les serveurs proxy web et les serveurs Cache. Ces serveurs étaient généralisés à l'époque où les débits étaient peu élevés. Avec le développement du haut débit, cette solution est apparue inutile aux FAI, voire nuisible à la fluidité du réseau.

3.13. DNS

Le DNS (pour Domain Name System) est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine. Dans la hiérarchie DNS, il existe deux type de serveurs, les serveurs DNS dits autoritaires et les serveurs DNS dits récursifs.

Les serveurs de noms de domaine autoritaires ou serveurs DNS autoritaires sont des équipements chargés de publier les données DNS, autrement dit des tables de correspondance entre noms de domaine et adresses IP des serveurs hébergeant les noms de domaine. Il s'agit là d'une base de données distribuée qui est le plus souvent tenue par les opérateurs ou leurs partenaires. Les personnes qui ne sont pas impliquées dans la gestion des réseaux n'ont généralement aucun contact direct avec ces serveurs.

Les serveurs récursifs, parfois appelés solveurs récursifs sont des serveurs mandataires qui interrogent les serveurs de nom de domaine à la place des utilisateurs. La translation de nom de domaine en adresse IP est habituellement faite à travers une requête des serveurs DNS autoritaires par l'intermédiaire des serveurs récursifs. Les serveurs récursifs font également office de cache, en ce sens qu'ils stockent les adresses IP des noms de domaines les plus demandés.

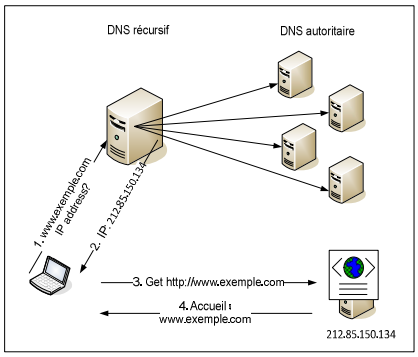


Figure 81 : Fonctionnement du système DNS (Marpij)

Quand un hôte a besoin de résoudre un nom de domaine (c'est-à-dire trouver l'adresse IP correspondant à un nom de domaine), il doit connaître l'adresse IP d'un ou plusieurs serveurs de noms récursifs qui vont éventuellement faire suivre la requête à un ou plusieurs autres serveurs de noms pour fournir une réponse. Les adresses IP de ces serveurs récursifs sont souvent obtenues dynamiquement ou encore configurées en dur sur la machine hôte.

Les fournisseurs d'accès à Internet mettent normalement à disposition de leurs clients ces serveurs récursifs.

3.14. DPI

Le DPI (pour Deep Packet Inspection ou Inspection en profondeur des paquets), est une technique d'inspection de paquets qui examine le contenu d'un paquet IP (à la fois l'entête et les données) lorsqu'il traverse un point particulier du réseau. L'inspection des paquets vise à rechercher des informations selon les critères prédéfinis dans le but de les router vers une autre destination ou de collecter des informations statistiques. Le DPI désigne la technique de blocage et par extension le serveur qui opère cette fonction dans le réseau.

3.15. L'architecture réseau d'un opérateur internet

A partir des éléments de réseau présentés ci-dessus, nous schématiser l'architecture technique d'un opérateur internet, et ce quelle que soit sa technologie d'accès.

Les principaux nœuds mis en jeu sont : les nœuds d'accès, les routeurs d'agrégation et de cœur, les serveurs DNS et les DPI et pare-feux lorsqu'ils sont utilisés.

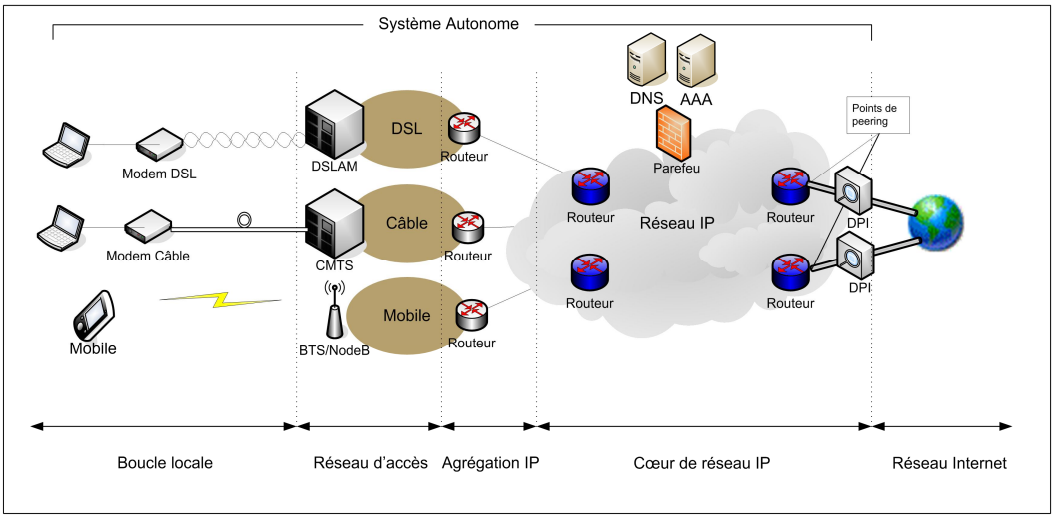


Figure 82 : Architecture technique d'un réseau d'opérateur Internet (Marpij)

L'usage de ces technologies réseaux et de ces transferts d'informations sont soumis à des réglementations de plus en plus fortes qui doivent répondre aux problématiques rencontrées face à leur développement très rapide.

Résumé

Les technologies de la communication évoluent rapidement et apportent de nouveaux services. Les problématiques de sécurité liées à l'accès aux données, aux flux de navigation Internet et de messagerie suivent une progression parallèle.

Le Centre Hospitalier de Montbert dispose de solutions de sécurisation anciennes qui ne permettent plus de sécuriser les flux et encore moins leur contenu. Les usages et comportements ont évolué et les besoins d'interconnexions, de recherches et d'échanges d'informations se sont multipliés.

Ce mémoire pose la problématique du respect du cadre légal et des solutions techniques de filtrage à mettre en œuvre.

L'objectif de cette étude est de déterminer les solutions de filtrage des flux Internet et des flux de messagerie qui répondent aux contraintes de la réglementation tout en prenant en compte les besoins professionnels des usagers et les spécificités de certains services de soins.

Mots-clés : Filtrage, Flux, Messagerie électronique, Internet, Intégration, Spams

---

Abstract

Communication technologies are evolving rapidly and providing new services. Security issues related to access data, Internet browsing and email stream follow a parallel progression.

The Montbert Hospital Center has old security solutions that can not secure flows, neither contents. Uses and behaviors have changed and needs of interconnections, research and exchange of information have multiplied.

This brief raises the issue of compliance with laws and technical solutions to implement filtering.

The study objective is to determine the filtering solutions for Internet and mail flows to match the regulatory constraints and needs of users and the specificities of particular health care.

Key words : Filtering, flows, Internet, Mails, Integration, Spams