Compte-rendu de CA ResEl

2 février 2011

par Erwan PILLET

Membres présents
Membres du CA : Emmanuel Caillé, Pillet Erwan, Xavier Corbillon, Hamed Ky, Simon Recher
Autres membres : Grégoire Payen De La Garanderie,

Ordre du Jour

Début de la réunion à 08h00.

Cordialité sur IRC

Suite à certains évenements, il est mentionné le fait qu'il faudrait rester correct sur les canals IRC.

Problème du P2P

Nous avons fait le point sur le fait que le P2P est interdit par Renater.
La question est alors de savoir si le P2P doit être bloqué ou simplement détecté.
La détection est beaucoup moins lourde que le bloquage. Elle peut se faire à postériori et n'implique d'attendre la réponse de l'analyse pour laisser passer ou non le paquet.
Cela permet aussi de s'adapter à tous les cas particuliers et éviter les échecs.

Problème de communication quand au P2P

Il faut mettre les utilisateurs au courant à la fois du fait que le P2P est interdit sur le réseau, et aussi que nous avons reçu des avertissements de la part de MediaSentry. Emmanuel a l'intention d'envoyer un mail à utilisateur.

Quelle réaction à un avertissement de MediaSentry

Shape ou coupure ?
Il faudrait, face à une détection, on coupe direct, l'avertissement aura été réalisé par le mail sur utilisateurs.
Il faudra faire attention aux faux positifs, mais cependant, une découpure n'aura lieu que si il y a une réelle vérification de la nature du trafic.

Pour réaliser celà, un outil tel que celui déjà mis en place avec IPFM, semble nécessaire.
Pour la durée de la coupure, la durée d'une première coupure sera de 4 jours, la deuxième coupure sera de un mois.
Pour éviter les faux positifs, pourquoi ne pas installer un client qui contacte la personne concernée par l'alerte pour connaitre son client et eventuellement le nom du fichier incriminé.

Efficacité du SNORT

Il faut améliorer les protocoles détectés par SNORT car tous les protocoles ne sont pas tous actuellement détectés.
Il faut donc ajouter des règles dans le SNORT et analyser les différents protocoles concernés.

Questions des quotas

Adapter les quotas à l'horaire de téléchargement pour que les gens puissent télécharger pendant la nuit les fichiers dont ils ont besoin pendant les heures creuses mais il y a le risque de rendre ces règles obscures.
Faire de la QOS afin de faire du shape en fonction des protocoles, pour faire en sorte que le réseau ne sature pas et garde des performances correctes.

Fin de la réunion 11h30