horizon-default-settings - Bug #3465

horizon-squid-default-settings : gestion du proxy filtrant SSL

27/03/2014 18:42 - Eric Seigne

Statut:	Fixed - Corrigé - Implémenté	**Début:**	27/03/2014
Priorité:	Haute	**Echéance:**	
Assigné à:	Eric Seigne	**% réalisé:**	80%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:			

Description

À ajouter pour éviter que https://google.fr ne soit trop utilisé pour aller regarder des images p*rn*

Ça fait quelques mois que je creuse la question en arrière plan, là c'est l'étape mise en prod de la solution, tout se concentre dans ce paquet horizon-squid-default-settings qui sera accompagné dans son déploiement de

- squid3 version 3.3 minimum
- squidguard version 1.4 minimum

La doc produite au long cours est disponible ici https://secure.ryxeo.com/doku.php/workinprogress/ssl-bump -> http://redmine.abuledu.org/projects/horizon-default-settings/wiki/Squid_33_pour_SSL-Bump

Historique

#1 - 30/03/2014 22:29 - Eric Seigne

- % réalisé changé de 0 à 80

Bon,
ça passe bien pour moi, reste à valider dans une école réelle & a faire la documentation ...

En attendant que les paquets soient validés:

```
dpkg -i horizon-squid-default-settings_11.08.8_all.deb squid_3.3.1-1lucid1~ryxeo5_amd64.deb squid3_3.3.1-1luci
d1~ryxeo5_amd64.deb squid3-common_3.3.1-1lucid1~ryxeo5_all.deb squidclient_3.3.1-1lucid1~ryxeo5_amd64.deb squi
d-common_3.3.1-1lucid1~ryxeo5_all.deb squidguard_1.4-2ryxeo2_amd64.deb
```

#2 - 17/06/2014 17:26 - Eric Seigne

Bon,
le script HST qui ajoute les certificats dans les trousseaux des utilisateurs, c'est gentil mais ça ne permet pas de gérer les futurs utilisateurs :

- création d'un compte
- lancement de firefox -> création du répertoire de stockage du profil et du porte clé
- lancement des HST pour ajouter le certificat

ça n'est pas satisfaisant, il faut donc trouver le moyen d'ajouter le certificat racine sur le poste / le navigateur / l'OS ... bref, "au dessus" des comptes utilisateurs !

#3 - 24/06/2014 10:04 - Eric Seigne

Une piste,

```
mkdir /usr/share/ca-certificates/local/
cp /etc/squid3/keys/serveur.pem /usr/share/ca-certificates/local/serveur.crt
update-ca-certificates --fresh
```

à faire sur tous les postes clients ... à mon avis c'est la même chose que d'ajouter le certificat dans la racine de sécurité windows.

#4 - 17/07/2014 07:57 - Eric Seigne

Après avoir cherché des solutions hyper compliquées ...

> Voilà ou j'en suis:
>
> <VirtualHost *:443>
> ServerAdmin webmaster@chezmoi
> DocumentRoot /home/webs/chezmoi/htdocs
> ServerName fake
> ErrorLog /tmp/error.log
> CustomLog /tmp/access.log combined
> SSLEngine on
> SSLCertificateFile /tmp/fake.crt
> SSLCertificateKeyFile /tmp/fake.key
> </VirtualHost>
>
> Mon problème c'est que fake.crt n'est pas modifié et donc si mon utilisateur essaye d'aller sur https://banque1.fr/ ou sur https://banque2.fr/ il ne faut pas que mon apache se présente en tant que fake ... mais en tant que banque1.fr ou banque2.fr
>
> pour celà il faudrait que j'ai
>
> <VirtualHost *:443>
> ServerAdmin webmaster@chezmoi
> DocumentRoot /home/webs/chezmoi/htdocs
> ServerName banque1.fr
> ErrorLog /tmp/error.log
> CustomLog /tmp/access.log combined
> SSLEngine on
> SSLCertificateFile /tmp/fake-banque1.crt
> SSLCertificateKeyFile /tmp/fake-banque1.key
> </VirtualHost>
>
> et
>
> <VirtualHost *:443>
> ServerAdmin webmaster@chezmoi
> DocumentRoot /home/webs/chezmoi/htdocs
> ServerName banque2.fr
> ErrorLog /tmp/error.log
> CustomLog /tmp/access.log combined
> SSLEngine on
> SSLCertificateFile /tmp/fake-banque2.crt
> SSLCertificateKeyFile /tmp/fake-banque2.key
> </VirtualHost>
>
> mais je te laisse imaginer si je veux pouvoir capter "la terre entière" ça n'est pas possible, donc en fait je cherche un micro serveur web qui pourrait écouter sur le port 443, capter dans les 1eres échanges (SNI mon amour bonjour) le hostname demandé et zoup il charge le faux-certificat qui correspond à ce que je client lui demande et ensuite

il lui pousse la page web adaptée

Finalement la solution est vraiment simple, il suffit d'avoir des redirect 302 dans squidGuard.conf:

```
dest porn {
  domainlist porn/domains
  urllist    porn/urls
  redirect   302:http://servecole.abuledu/proxy/stop.php?clientaddr=%a&clientnam
e=%n&clientuser=%i&clientgroup=%s&url=%u
  log squidGuard.log
}
```

#5 - 01/02/2015 16:19 - Eric Seigne

Bon, c'était une fausse joie, on ne peut pas faire un redirect d'un https vers un http, c'est une faille du protocole et tous les navigateurs qui se respectent interdisent ça.

Il faut donc reprendre la R&D vers un serveur web qui ferait du fake ssl via SNI.

À mon avis on trouvera ça dans la malette du parfait pirate qui fait du ManInTheMiddle ... donc à chercher du côté sombre du web international.

#6 - 25/07/2019 22:52 - Eric Seigne

- Description mis à jour

#7 - 17/12/2020 10:04 - Eric Seigne

- Statut changé de Assigned - En cours à Fixed - Corrigé - Implémenté