Distribution EOLE - Tâche #36801

Scénario # 36761 (Terminé (Sprint)): EOLE 2.10 : La navigation authentifiée avec filtrage web désactivé ne rapporte pas les utilisateurs dans les logs

Étude

24/04/2025 16:06 - Benjamin Bohard

Statut:	Fermé	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Version cible:	Livraison Cadoles - MEN 31/05/2025 (40)	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 24/04/2025 16:06 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#2 - 24/04/2025 16:14 - Benjamin Bohard

On observe deux successions types de logs.

Dans le premier cas, où le login est récupéré rapidement après requête http :

1. TCP_DENIED/407
2. TCP_DENIED/407
3. NONE_NONE/000 suivi du login

Ce cas est rencontré depuis les clients Linux et Windows, avec le navigateur Firefox, dans le cas du filtrage web activé, et seulement depuis le client Linux dans le cas du filtrage web désactivé.

Le second cas est observé depuis le client Windows dans le cas du filtrage web désactivé :

1. TCP_DENIED/407
2. TCP_DENIED/407
   …
   Rafraîchissement de la page dans le navigateur nécessaire
3. TCP_TUNNEL/200 suivi du login

Dans les deux cas, les deux premiers TCP_DENIED/407 sont attendus avec l'utilisation de NTLM.

#3 - 28/04/2025 11:28 - Benjamin Bohard

Si on considère que la note du pas 6 du test squash PROXY-T16-001 est légitime (rechargement de la page acceptable), il ne semble pas y avoir de problème.

Il y a bien une différence de comportement entre les deux OS cependant. Si on ne recharge pas la page mais qu'on navigue sur un autre site, ~~l'association utilisateur URL est perdue (les logs contiennent pas le résultat TCP_TUNNEL/200 avec le login).~~ le résultat TCP_TUNNEL/200 avec le login peut arriver plus tard dans les logs :

```
avril 28 11:26:01 proxy squid[9250]: 1745832361.892     32 192.168.0.153 TCP_DENIED/407 4020 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:26:01 proxy squid[9250]: 1745832361.897      0 192.168.0.153 TCP_DENIED/407 4366 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.004      1 192.168.0.153 TCP_DENIED/407 4024 CONNECT www.googl
e.fr:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.018      0 192.168.0.153 TCP_DENIED/407 4370 CONNECT www.googl
e.fr:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.043     19 192.168.0.153 TCP_DENIED/407 4068 CONNECT www.googl
etagmanager.com:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.054      0 192.168.0.153 TCP_DENIED/407 4414 CONNECT www.googl
etagmanager.com:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.454     19 192.168.0.153 TCP_DENIED/407 4068 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.461      0 192.168.0.153 TCP_DENIED/407 4414 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.623     19 192.168.0.153 TCP_DENIED/407 4084 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:26:02 proxy squid[9250]: 1745832362.626      0 192.168.0.153 TCP_DENIED/407 4430 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:26:09 proxy squid[9250]: 1745832369.142      0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-b
efore-headers - HIER_NONE/- -
avril 28 11:26:09 proxy squid[9250]: 1745832369.233     19 192.168.0.153 TCP_DENIED/407 4028 CONNECT www.googl
e.com:443 - HIER_NONE/- text/html
avril 28 11:26:09 proxy squid[9250]: 1745832369.236      0 192.168.0.153 TCP_DENIED/407 4374 CONNECT www.googl
e.com:443 - HIER_NONE/- text/html
avril 28 11:26:18 proxy squid[9250]: 1745832378.804     30 192.168.0.153 TCP_DENIED/407 4040 CONNECT www.wikip
edia.org:443 - HIER_NONE/- text/html
avril 28 11:26:18 proxy squid[9250]: 1745832378.810      0 192.168.0.153 TCP_DENIED/407 4386 CONNECT www.wikip
edia.org:443 - HIER_NONE/- text/html
avril 28 11:28:04 proxy squid[9250]: 1745832484.159      0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-b
efore-headers - HIER_NONE/- -
avril 28 11:28:46 proxy squid[9250]: 1745832526.230 147416 192.168.0.153 TCP_TUNNEL/200 83041 CONNECT www.wiki
pedia.org:443 prof.6a HIER_DIRECT/185.15.58.224 -
avril 28 11:28:46 proxy squid[9250]: 1745832526.307 170707 192.168.0.153 TCP_TUNNEL/200 12506 CONNECT ads.mozi
lla.org:443 prof.6a HIER_DIRECT/34.36.137.203 -
avril 28 11:28:52 proxy squid[9250]: 1745832532.327 170298 192.168.0.153 TCP_TUNNEL/200 5167 CONNECT www.googl
e.fr:443 prof.6a HIER_DIRECT/142.251.37.35 -
avril 28 11:28:53 proxy squid[9250]: 1745832533.333 171268 192.168.0.153 TCP_TUNNEL/200 222368 CONNECT www.goo
gletagmanager.com:443 prof.6a HIER_DIRECT/172.217.19.136 -
avril 28 11:29:28 proxy squid[9250]: 1745832568.342 206440 192.168.0.153 TCP_TUNNEL/200 8763 CONNECT www.perl.
org:443 prof.6a HIER_DIRECT/146.75.117.55 -
```

#4 - 28/04/2025 11:52 - Benjamin Bohard

Test complémentaire avec une session ouverte localement sur le poste Windows (pcadmin) et la configuration manuelle du proxy (comme pour le poste Linux) :

```
avril 28 11:38:56 proxy squid[9250]: 1745833136.589     17 192.168.0.153 TCP_DENIED/407 4020 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.594      0 192.168.0.153 TCP_DENIED/407 4366 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.598      1 192.168.0.153 TCP_DENIED/407 4700 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.602      0 192.168.0.153 TCP_DENIED/407 4366 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.746     19 192.168.0.153 TCP_DENIED/407 4024 CONNECT www.googl
e.fr:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.749      0 192.168.0.153 TCP_DENIED/407 4370 CONNECT www.googl
e.fr:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.752      1 192.168.0.153 TCP_DENIED/407 4710 CONNECT www.googl
e.fr:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.762      0 192.168.0.153 TCP_DENIED/407 4370 CONNECT www.googl
e.fr:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.965     19 192.168.0.153 TCP_DENIED/407 4068 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.967      0 192.168.0.153 TCP_DENIED/407 4414 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.971      1 192.168.0.153 TCP_DENIED/407 4778 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:38:56 proxy squid[9250]: 1745833136.976      0 192.168.0.153 TCP_DENIED/407 4414 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:38:57 proxy squid[9250]: 1745833137.333      0 192.168.0.153 TCP_DENIED/407 4084 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:38:57 proxy squid[9250]: 1745833137.335      0 192.168.0.153 TCP_DENIED/407 4430 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:38:57 proxy squid[9250]: 1745833137.339      1 192.168.0.153 TCP_DENIED/407 4808 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:38:57 proxy squid[9250]: 1745833137.345      0 192.168.0.153 TCP_DENIED/407 4430 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:39:01 proxy squid[9250]: 1745833141.398 170758 192.168.0.153 TCP_TUNNEL/200 5116 CONNECT aus5.mozi
lla.org:443 prof.6a HIER_DIRECT/35.244.181.201 -
avril 28 11:39:24 proxy squid[9250]: 1745833164.353      1 192.168.0.153 TCP_DENIED/407 4032 CONNECT ads.mozil
la.org:443 - HIER_NONE/- text/html
avril 28 11:39:24 proxy squid[9250]: 1745833164.364      0 192.168.0.153 TCP_DENIED/407 4378 CONNECT ads.mozil
la.org:443 - HIER_NONE/- text/html
avril 28 11:39:24 proxy squid[9250]: 1745833164.368      2 192.168.0.153 TCP_DENIED/407 4718 CONNECT ads.mozil
la.org:443 - HIER_NONE/- text/html
avril 28 11:39:24 proxy squid[9250]: 1745833164.372      0 192.168.0.153 TCP_DENIED/407 4378 CONNECT ads.mozil
la.org:443 - HIER_NONE/- text/html
avril 28 11:39:34 proxy squid[9250]: 1745833174.143      0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-b
efore-headers - HIER_NONE/- -
avril 28 11:41:29 proxy squid[9250]: 1745833289.143      0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-b
efore-headers - HIER_NONE/- -
avril 28 11:41:42 proxy squid[9250]: 1745833302.399 170778 192.168.0.153 TCP_TUNNEL/200 544327 CONNECT firefox
-settings-attachments.cdn.mozilla.net:443 prof.6a HIER_DIRECT/34.107.152.202 -
avril 28 11:41:42 proxy squid[9250]: 1745833302.400 170885 192.168.0.153 TCP_TUNNEL/200 17392 CONNECT firefox.
settings.services.mozilla.com:443 prof.6a HIER_DIRECT/34.149.100.209 -
avril 28 11:41:47 proxy squid[9250]: 1745833307.413 170649 192.168.0.153 TCP_TUNNEL/200 5168 CONNECT www.googl
e.fr:443 prof.6a HIER_DIRECT/142.251.37.35 -
avril 28 11:41:47 proxy squid[9250]: 1745833307.414 170809 192.168.0.153 TCP_TUNNEL/200 5326 CONNECT www.perl.
org:443 prof.6a HIER_DIRECT/146.75.117.55 -
```

Le délai entre le début de l'authentification (TCP_DENIED/407) et la trace associant URL et login est de l'ordre de 3 min, comme dans le test précédent.

En fait, on observe la même chose depuis le client Linux :

```
avril 28 11:45:20 proxy squid[9250]: 1745833520.938      0 192.168.0.154 TCP_DENIED/407 4004 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:45:20 proxy squid[9250]: 1745833520.939      0 192.168.0.154 TCP_DENIED/407 4336 CONNECT www.perl.
org:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.094      0 192.168.0.154 TCP_DENIED/407 4008 CONNECT www.googl
```

```
e.fr:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.100      0 192.168.0.154 TCP_DENIED/407 4052 CONNECT www.googl
etagmanager.com:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.112      0 192.168.0.154 TCP_DENIED/407 4340 CONNECT www.googl
e.fr:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.114      0 192.168.0.154 TCP_DENIED/407 4384 CONNECT www.googl
etagmanager.com:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.483      0 192.168.0.154 TCP_DENIED/407 4052 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.488      0 192.168.0.154 TCP_DENIED/407 4384 CONNECT www.googl
e-analytics.com:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.675      0 192.168.0.154 TCP_DENIED/407 4068 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.677      0 192.168.0.154 TCP_DENIED/407 4400 CONNECT region1.a
nalytics.google.com:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.677      0 192.168.0.154 TCP_DENIED/407 4048 CONNECT stats.g.d
oubleclick.net:443 - HIER_NONE/- text/html
avril 28 11:45:21 proxy squid[9250]: 1745833521.679      0 192.168.0.154 TCP_DENIED/407 4380 CONNECT stats.g.d
oubleclick.net:443 - HIER_NONE/- text/html
avril 28 11:47:14 proxy squid[9250]: 1745833634.144      0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-b
efore-headers - HIER_NONE/- -
avril 28 11:48:05 proxy squid[9250]: 1745833685.355 171008 192.168.0.154 TCP_TUNNEL/200 13957 CONNECT merino.s
ervices.mozilla.com:443 prof.6b HIER_DIRECT/34.110.138.217 -
avril 28 11:48:05 proxy squid[9250]: 1745833685.355 171018 192.168.0.154 TCP_TUNNEL/200 18107 CONNECT ads.mozi
lla.org:443 prof.6b HIER_DIRECT/34.36.137.203 -
avril 28 11:48:09 proxy squid[9250]: 1745833689.355 175043 192.168.0.154 TCP_TUNNEL/200 2303 CONNECT incoming.
telemetry.mozilla.org:443 prof.6b HIER_DIRECT/34.120.208.123 -
avril 28 11:48:11 proxy squid[9250]: 1745833691.356 170232 192.168.0.154 TCP_TUNNEL/200 2577 CONNECT www.googl
e.fr:443 prof.6b HIER_DIRECT/142.251.37.35 -
avril 28 11:48:11 proxy squid[9250]: 1745833691.356 170415 192.168.0.154 TCP_TUNNEL/200 8653 CONNECT www.perl.
org:443 prof.6b HIER_DIRECT/146.75.117.55 -
```

Le fonctionnement "normal" semble bien être celui-ci : un délai assez long entre la trace de l'authentification et la trace associant l'URL et le login. Le cas du code de résultat NONE_NONE/000 qui sert dans le test squash est-il pertinent ?

#5 - 28/04/2025 13:09 - Benjamin Bohard

Finalement, la trace dans les logs de Squid qui associe l'URL et le login est écrite à la fermeture de la connexion. Logiquement, c'est cette trace qu'il faudrait attendre (ou déclencher en rechargeant la page) dans le test squash.

L'origine de la trace supplémentaire qui est parfois observée, et sur laquelle s'appuyait le test, n'est pas identifiée pour l'instant.

#6 - 28/04/2025 13:12 - Benjamin Bohard

- Fichier http.pcap ajouté

#7 - 28/04/2025 13:12 - Benjamin Bohard

- Statut changé de En cours à À valider

#8 - 29/04/2025 10:06 - Benjamin Bohard

Le problème semblant davantage lié à la manière de tester, est-ce qu'on le résoud en modifiant le test squash ?

La proposition est soit d'attendre (environ 3 minutes) la fermeture de la connexion, soit d'interrompre la connexion en rechargeant la page (Maj-F5).

#9 - 05/05/2025 11:17 - Joël Cuissinat

OK pour modifier le test squash, si Maj-F5 fonctionne, je prendrais cette solution afin de ne pas faire attendre le testeur...

#10 - 10/06/2025 09:58 - Laurent Gourvenec

- % réalisé changé de 0 à 100

#11 - 08/07/2025 13:56 - Ludwig Seys

- Statut changé de À valider à Résolu

#12 - 08/07/2025 14:56 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

OK

Fichiers

http.pcap	47,8 ko	28/04/2025	Benjamin Bohard