

Amon - Scénario #36200

Le filtrage WEB ne fonctionne pas (2.8.1)

08/10/2024 10:01 - Klaas TJEBBES

Statut:	Terminé (Sprint)	Début:	01/10/2022
Priorité:	Normal	Echéance:	01/01/2026
Assigné à:	Benjamin Bohard	% réalisé:	100%
Catégorie:		Temps estimé:	0.00 heure
Version cible:	Livraison Cadoles - MEN 31/12/2024 (100)	Temps passé:	0.00 heure
Description			
En 2.8.1 les sites blacklistés ne sont pas bloqués.			
Nous n'avons pas activé de ssl bump.			
2024-10-01T09:34:04.102462+04:00 a-clg-0072k.9740072k.ad.in.ac-reunion.fr squid[251265]: optional ICAP service is down after an options fetch failure: icap://127.0.0.1:1340/response [down,!opt]			
2024-10-01T09:34:05.921556+04:00 a-clg-0072k.9740072k.ad.in.ac-reunion.fr squid[251265]: optional ICAP service is down after an options fetch failure: icap://127.0.0.1:1340/request [down,!opt]			
- /var/log/squid/cache.log (ou 172.19.80.4 est l'ip de ma machine de test)			
2024/09/26 21:57:22 kid1 kick abandoning local=172.19.80.1:3128 remote=172.19.80.4:49419 FD 725 f lags=1			
2024/09/26 21:57:23 kid1 kick abandoning local=172.19.80.1:3128 remote=172.19.80.4:49422 FD 726 f lags=1			
2024/09/26 21:57:24 kid1 kick abandoning local=172.19.80.1:3128 remote=172.19.80.4:49427 FD 710 f lags=1			
2024/09/26 21:57:28 kid1 suspending ICAP service for too many failures			
2024/09/26 21:57:28 kid1 optional ICAP service is suspended: icap://127.0.0.1:1340/request [down, susp, fail2]			
2024/09/26 21:57:38 kid1 optional ICAP service is up: icap://127.0.0.1:1340/request [up]			
2024/09/26 21:57:39 kid1 Starting new ntlmauthenticator helpers...			
2024/09/26 21:57:39 kid1 helperOpenServers: Starting 1/75 'ntlm_auth' processes			
2024/09/26 21:57:39 kid1 Starting new ntlmauthenticator helpers...			
2024/09/26 21:57:39 kid1 helperOpenServers: Starting 1/75 'ntlm_auth' processes			
2024/09/26 21:57:40 kid1 kick abandoning local=172.19.80.1:3128 remote=172.19.80.4:49482 FD 665 f lags=1			
2024/09/26 21:57:42 kid1 kick abandoning local=172.19.80.1:3128 remote=172.19.80.4:49489 FD 688 f lags=1			
Dès que le service ICAP tombe, je n'ai plus de trace de la requête sur le nom de domaine dans le log du guardian, je ne vois que les redirections effectuées par l'accès au domaine en question (static-XXXX.cdn.com) en mode CONNECT, et du coup j'accède au contenu interdit.			
Exemple: netflix			
Domaine interdit: netflix.com			
traces dans le log du guardian:			
e2guardian0[589986]: "2024.09.25 08:34:57","admin","172.21.16.4","https://netflix.com:443","*Accès interdit* Site interdit : netflix.com","CONNECT","0","0","-", "1","403","-", "172.21.16.4","politiquedefaut","-", "-", "-", "-", "-", "-"			

Message d'erreur sur la page web: La connexion a échoué - Une erreur est survenue pendant une connexion à netflix.com. => ce n'est pas le message du guardian classique

Et un peu plus tard, je relance et la ça passe sans souci.

C'est toujours indiqué , "admin", "172.21.16.4", "https://netflix.com:443", "*Accès interdit* Site interdit : netflix.com", "CONNECT", "0", "0", "-", "1", "403", "-", "172.21.16.4", "politiquedefaut", "-", "-", "-", "-", "-", "-"

Mais sur mon navigateur j'ai bien accès à la ressource Web.

Dans les autres traces je constates: suspending ICAP service for too many failures, même après avoir augmenté le nombre de workers à 10 000 ...

Nous (EOLE) disposons du fichier config.eol du serveur à problème, je ne le mets pas en ligne pour des raisons de sécurité des données personnelles. Nous contacter pour avoir une copie. Email sur la liste eole@ac-dijon.fr du 08/10/2024 10h03.

Sous-tâches:	
Tâche # 36216: Étude	Fermé
Tâche # 36349: Modifier la configuration de squid	Fermé
Tâche # 36350: Documenter	Fermé
Tâche # 36351: Tester	Fermé

Historique

- #1 - 08/10/2024 14:57 - Joël Cuissinat
- Tracker changé de Demande à Scénario
 - Début 08/10/2024 supprimé
 - Release mis à Carnet de produit Cadoles - MEN
 - Points de scénarios mis à 2.0

- #2 - 14/10/2024 11:12 - Benjamin Bohard
- Echéance mis à 01/01/2026
 - Assigné à mis à Benjamin Bohard
 - Version cible mis à Carnet Cadoles - MEN
 - Début mis à 01/10/2022

- #3 - 17/12/2024 10:28 - Joël Cuissinat
- Points de scénarios changé de 2.0 à 3.0

+1 pour rétro-portage jusqu'en 2.8.1

- #4 - 18/02/2025 10:41 - Joël Cuissinat
- Points de scénarios changé de 3.0 à 4.0

+1 pour documenter les 8 variables

- #5 - 25/04/2025 17:21 - Joël Cuissinat
- Release changé de Carnet de produit Cadoles - MEN à EOLE 2.8.1

#6 - 05/05/2025 16:54 - Joël Cuissinat

- Statut changé de Nouveau à Terminé (Sprint)

- Version cible changé de Carnet Cadoles - MEN à Livraison Cadoles - MEN 31/12/2024 (100)