Amon - Scénario #37474

Second filtre web e2guardian inopérant sur les Amons

22/05/2026 10:23 - Valérian M

Statut:	Terminé (Sprint)	**Début:**	20/07/2026
Priorité:	Normal	**Echéance:**	20/07/2026
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Livraison Cadoles - MEN 31/07/2026 (45)		

Description

Bonjour,

comme constaté avec le collègue de l'Académie de la Réunion, il semblerait que le second filtre web ne soit pas pris en compte, rendant le filtrage différencié inopérant, où seul le premier filtrage est réellement actif, peu importe la valeur de la variable %%dansguardian_ethX.

Pour reproduire le problème sur un Amon 2.8, 2.9 ou 2.10 :

- Configurer dans le gen_config :
  - dansguardian_eth1 = "1" (Filtre admin)
  - dansguardian_eth2 = "2" (Filtre pédagogique)
- Reconfigurer l'amon
- Tester sur une machine se situant sur le réseau eth2 : les requêtes passant par cette interface (authentifiée) contournent le Filtre web 2

Faits observés :

- Les processus e2guardian sont actifs sur les ports 1340 ET 1341:

```
root@amon:~# netstat -lntp | grep e2guardian
tcp        0      0 0.0.0.0:1340            0.0.0.0:*               LISTEN      160500/e2guard
ian
tcp        0      0 0.0.0.0:1341            0.0.0.0:*               LISTEN      161508/e2guard
ian
tcp        0      0 127.0.0.1:9990          0.0.0.0:*               LISTEN      160500/e2guard
ian
tcp        0      0 127.0.0.1:9991          0.0.0.0:*               LISTEN      161508/e2guard
ian
```

- Aucune erreur dans les logs e2guardian
- Problème identifié : Le template 01squid.conf ne génère que la configuration pour le port 1340

Impact :
Le filtrage différencié ne fonctionne pas :

- Toutes les requêtes utilisent le Filtre web 1
- Le Filtre web 2 est totalement ignoré

Solution de contournement actuelle apportée par l'Académie de la Réunion :
Patch manuel de fichier 01squid.conf avec ACLs par interface et services ICAP distincts pour chaque port.

Nous vous remercions d'avance pour nous apporter une correction officielle à notre problème.

Sous-tâches:

Tâche # 37557: Utiliser les deux instances de e2guardian	**Fermé**
Tâche # 37577: Tester	**Fermé**

Historique

#1 - 26/05/2026 09:39 - Joël Cuissinat

- Tracker changé de Demande à Scénario

- Début 22/05/2026 supprimé

- Release mis à Carnet de produit Cadoles - MEN

- Points de scénarios mis à 1.0

#2 - 23/06/2026 10:34 - Benjamin Bohard

- Assigné à mis à Benjamin Bohard

#3 - 29/06/2026 09:39 - Benjamin Bohard

- Echéance mis à 01/01/2026

- Version cible mis à Carnet Cadoles - MEN

- Début mis à 01/10/2022

#4 - 29/06/2026 09:54 - Benjamin Bohard

La perte de la fonctionnalité semble bien lié au passage à ICAP et à squid en frontal.

Auparavant, la distinction était gérée dans la configuration de e2guardian.

La configuration de squid doit être modifiée comme suggérée dans le scénario.

L'ajout du patch serait un plus pour avoir une correction déjà testée en production. Il est toutefois possible que des adaptations soient à effectuer.

L'activation selon les valeurs de la configuration creole doit être dérivée (pas de variable explicite mais présence dans une liste de variables). Les ACL sont à revoir également.

#5 - 29/06/2026 10:25 - Joël Cuissinat

- Points de scénarios changé de 1.0 à 2.0

#6 - 29/06/2026 10:26 - Joël Cuissinat

+1 pour vérification et application des patches

#7 - 29/06/2026 10:34 - Benjamin Bohard

Pour mémoire, le patch qui a été référencé dans la discussion sur la liste :

```
icap_enable on
%if %%dansguardian_eth1 != %%dansguardian_eth2
%for nbeth in %%range(1, %%int(%%nombre_interfaces))
acl %%getVar('nom_machine_eth' + %%str(%%nbeth))  src %%getVar('adresse_network_eth' + %%str(%%nbeth))/%%getVa
r('adresse_netmask_eth' + %%str(%%nbeth))
%end for
icap_service service_admin_req reqmod_precache bypass=on icap://127.0.0.1:1340/request
icap_service service_admin_resp respmod_precache bypass=on icap://127.0.0.1:1340/response
%for nbeth in %%range(1, %%int(%%nombre_interfaces))
%if %%getVar('dansguardian_eth' + %%str(%%nbeth)) == "1"
adaptation_access service_admin_req allow %%getVar('nom_machine_eth' + %%str(%%nbeth))
adaptation_access service_admin_resp allow %%getVar('nom_machine_eth' + %%str(%%nbeth))
%end if
%end for
icap_service service_pedago_req reqmod_precache bypass=on icap://127.0.0.1:1341/request
icap_service service_pedago_resp respmod_precache bypass=on icap://127.0.0.1:1341/response
%for nbeth in %%range(1, %%int(%%nombre_interfaces))
```

```
%if %%getVar('dansguardian_eth' + %%str(%%nbeth)) == "2"
adaptation_access service_pedago_req allow %%getVar('nom_machine_eth' + %%str(%%nbeth))
adaptation_access service_pedago_resp allow %%getVar('nom_machine_eth' + %%str(%%nbeth))
%end if
%end for
%else
icap_service service_req reqmod_precache bypass=on icap://127.0.0.1:1340/request
icap_service service_resp respmod_precache bypass=on icap://127.0.0.1:1340/response
%end if
```

Il semble nécessaire de faire quelques généralisations pour la prise en charge d'autres combinaisons d'interfaces et d'instances de e2guardian et de vérifier si les ACL créées dans common-squid1.conf ne pourraient pas servir (fichier chargé après la déclaration de la configuration ICAP toutefois).

#8 - 29/06/2026 11:26 - Valérian M

Bonjour,
si ça peut vous aider, je me suis penché sur un patch un peu plus élégant et qui semble fonctionner (voir PJ).
Mais je préfère tout de même que les experts (vous) le vérifient car il y a probablement des subtilités que je n'aurais pas vus, qui doivent peut-être rester ou qui pourraient peut-être compromettre la sécurité.

Au final, ça pourrait ressembler à cela :

```
%if %%activer_filtrage_proxy == 'oui'
icap_enable on
icap_service service_req_1 reqmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.1:1340/reque
st
icap_service service_resp_1 respmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.1:1340/res
ponse
%if %%dansguardian_eth1 == '2' or %%dansguardian_eth2 == '2' or %%dansguardian_eth3 == '2' or %%dansguardian_e
th4 == '2'
icap_service service_req_2 reqmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.1:1341/reque
st
icap_service service_resp_2 respmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.1:1341/res
ponse
%end if
icap_service_revival_delay 10
icap_send_client_ip on
icap_send_client_username on
icap_service_failure_limit %%icap_service_failure_limit
icap_connect_timeout 10 seconds
icap_io_timeout 15 seconds
#33136
#icap_persistent_connections on
#icap_preview_enable on
#icap_preview_size 4096
icap_client_username_encode off
#icap_client_username_header X-Authenticated-User
adaptation_masterx_shared_names X-ICAP-E2G
icap_log syslog:LOG_LOCAL1|LOG_INFO squid
%end if
```

Merci à vous de vous pencher sur notre demande.

#9 - 29/06/2026 11:37 - Benjamin Bohard

La déclaration des directives adaptation_access dans common-squid2.conf ne semble pas justifiée.

#10 - 29/06/2026 11:45 - Valérian M

Et dans le common-squid2.conf (merci Benjamin pour le rappel), j'avais modifié comme cela :

```
%for numero_interface in %%range(1, %%int(%%nombre_interfaces))
%if %%getVar('dansguardian_eth' + %%str(%%numero_interface)) == '1'
adaptation_access service_req_1 allow %%getVar('nom_machine_eth' + %%str(%%numero_interface))
adaptation_access service_resp_1 allow %%getVar('nom_machine_eth' + %%str(%%numero_interface))
%end if
%if %%getVar('dansguardian_eth' + %%str(%%numero_interface)) == '2'
adaptation_access service_req_2 allow %%getVar('nom_machine_eth' + %%str(%%numero_interface))
adaptation_access service_resp_2 allow %%getVar('nom_machine_eth' + %%str(%%numero_interface))
%end if
%end for
adaptation_access service_req_1 deny all
adaptation_access service_resp_1 deny all
adaptation_access service_req_2 deny all
adaptation_access service_resp_2 deny all
```

#11 - 29/06/2026 11:56 - Benjamin Bohard

Valérian M a écrit :

> Bonjour,
> si ça peut vous aider, je me suis penché sur un patch un peu plus élégant et qui semble fonctionner (voir PJ).
> Mais je préfère tout de même que les experts (vous) le vérifient car il y a probablement des subtilités que je n'aurais pas vus, qui doivent peut-être rester ou qui pourraient peut-être compromettre la sécurité.
>
> Au final, ça pourrait ressembler à cela :
> [...]
>
> Merci à vous de vous pencher sur notre demande.

Le patch que je teste pour l'instant tente de s'affranchir des tests sur des listes de valeurs fixes et de s'appuyer sur les ACL créées par ailleurs. Ça implique un chargement plus précoce des fichiers annexes. J'ai conservé les adaptation_access dans la même partie que le reste de la configuration ICAP. La répartition entre les différents fichiers pourrait être discutée.

Voici le patch que j'ai généré en 2.9.0 pour l'instant :

```
--- distrib/01squid.conf    2026-04-28 10:13:03.000000000 +0200
+++ modif/01squid.conf    2026-06-29 11:27:18.821828894 +0200
@@ -1010,16 +1010,24 @@
 access_log syslog:LOG_LOCAL1|LOG_INFO squid
 pid_filename /var/run/squid.pid

-# ICAP OPTIONS INSTANCE 1 (Port 1340)
+%if %%activer_squid_1_mitm == 'oui'
+acl step1 at_step SslBump1
+acl step2 at_step SslBump2
```

```
+acl step3 at_step SslBump3
+
+ssl_bump bump all
+%end if
+
+include /etc/squid/common-squid1.conf
+include /etc/squid/01inc-squid.conf
+include /etc/squid/common-squid2.conf
+#
+# ICAP OPTIONS INSTANCES (Port 1340: instance 1, port 1341: instance 2)
 # ------------------------------------------------------------------------------
 %if %%activer_filtrage_proxy == 'oui'

 icap_enable on
-icap_service service_req reqmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.1:1340/reques
t
-icap_service service_resp respmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.1:1340/resp
onse
 icap_service_revival_delay 10
-adaptation_access service_req allow all
-adaptation_access service_resp allow all
 icap_send_client_ip on
 icap_send_client_username on
 icap_service_failure_limit %%icap_service_failure_limit
@@ -1034,19 +1042,34 @@
 adaptation_masterx_shared_names X-ICAP-E2G
 icap_log syslog:LOG_LOCAL1|LOG_INFO squid

-adaptation_access service_req allow all
-adaptation_access service_resp allow all

-%end if
-
-%if %%activer_squid_1_mitm == 'oui'
-acl step1 at_step SslBump1
-acl step2 at_step SslBump2
-acl step3 at_step SslBump3
+  %set %%e2g_int_map = {}
+  %for %%interface in range(1, %%int(%%nombre_interfaces)):
+    %set %%current_interface = 'eth' + str(%%interface)
+    %set %%e2g_instance = %%getVar('dansguardian_' + %%current_interface)
+    %silent %%e2g_int_map.setdefault(%%e2g_instance, [])
+    %silent %%e2g_int_map[%%e2g_instance] += [%%current_interface]
+  %end for
+
+  %if '1' in %%e2g_int_map
+    %set %%serv_suffix = '_instance1'
+icap_service service_req%%serv_suffix reqmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.
1:1340/request
+icap_service service_resp%%serv_suffix respmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.
0.1:1340/response
+    %for %%interface in %%e2g_int_map['1']
+adaptation_access service_req%%serv_suffix allow reseau%%interface
+adaptation_access service_resp%%serv_suffix allow reseau%%interface
+    %end for
+  %end if
+
+  %if '2' in %%e2g_int_map
+    %set %%serv_suffix = '_instance2'
+icap_service service_req%%serv_suffix reqmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.0.
1:1341/request
+icap_service service_resp%%serv_suffix respmod_precache bypass=%%bypass_icap_service_if_failure icap://127.0.
0.1:1341/response
+    %for %%interface in %%e2g_int_map['2']
+adaptation_access service_req%%serv_suffix allow reseau%%interface
+adaptation_access service_resp%%serv_suffix allow reseau%%interface
+    %end for
+  %end if

-ssl_bump bump all
 %end if

-include /etc/squid/common-squid1.conf
-include /etc/squid/01inc-squid.conf
-include /etc/squid/common-squid2.conf
```

#12 - 29/06/2026 15:50 - Benjamin Bohard

La réelle difficulté est dans le choix des ACL à utiliser.

Une interface est associée à un réseau principal mais peut également être associée à des VLAN.

La zone est déclarée au niveau d'une interface et il n'est pas proposé de spécifier si ça inclut les VLAN.

Les ACL déclarées distinguent le réseau principal des VLAN. La question porterait donc sur le choix suivant :
- le filtrage est associé à tous les réseaux d'une interface (principal + VLAN, ACL reseauethX + reseauethX_Y) ;
- le filtrage est associé uniquement au réseau princpal (uniquement l'ACL reseauethX correspondante).

La configuration actuelle (ACL all) n'est sans doute pas un bon indicateur de la configuration souhaitée.

En pratique, qu'est-ce qui semblerait le plus pertinent ?

#13 - 15/07/2026 12:02 - Klaas TJEBBES

J'ai posé la question à divers utilisateurs Amon. Les VLANs ne semblent pas être utilisés pour séparer des parties des réseau PEDAGO ou ADMIN.

Donc un filtre Web par interface est une solution valide.

Si des utilisateurs souhaitent un filtre Web par VLAN, nous pourrons toujours étudier une solution.

#14 - 22/07/2026 14:45 - Joël Cuissinat

- Points de scénarios changé de 2.0 à 3.0

+1 pour finaliser les corrections

#15 - 31/08/2026 10:52 - Laurent Gourvenec

Bonjour Valérian M, pourriez-vous tester la correction svp ? Un paquet est disponible pour les versions suivantes :
- 2.8.1 : https://test-eole.ac-dijon.fr/eole/pool/main/e/eole-proxy/eole-proxy_2.8.1-66_all.deb
- 2.9 : https://test-eole.ac-dijon.fr/eole/pool/main/e/eole-proxy/eole-proxy_2.9.0-25_all.deb
- 2.10 : https://test-eole.ac-dijon.fr/eole/pool/main/e/eole-proxy/eole-proxy_2.10.0-11_all.deb

#16 - 08/09/2026 16:36 - Valérian M

Bonjour,
désolé pour l'attente de ma réponse, je souhaitais quelques jours de fonctionnement afin de vous faire un retour avec un peu plus de recul.

J'ai donc pu tester brièvement sur mon amon de test en version 2.10, puis mis en place sur un établissement en version 2.9 depuis le milieu de la semaine dernière.
Il semblerait en effet que votre correctif soit fonctionnel, les filtres 1 et 2 que nous utilisons respectivement pour les réseaux administratif et pédagogique sont bien à nouveau appliqués distinctement.

Merci à vous !

#17 - 09/09/2026 11:27 - Joël Cuissinat

- Statut changé de Nouveau à Terminé (Sprint)

- Version cible changé de Carnet Cadoles - MEN à Livraison Cadoles - MEN 31/05/2026 (30)

- Release changé de Carnet de produit Cadoles - MEN à EOLE 2.8.1

#18 - 10/09/2026 15:23 - Joël Cuissinat

- Version cible changé de Livraison Cadoles - MEN 31/05/2026 (30) à Livraison Cadoles - MEN 31/07/2026 (45)