Distribution EOLE - Scénario #19715

Vérifier qu'e2guardian utilise bien X-Forwarded-For pour les Groupe de machine

15/03/2017 14:29 - Joël Cuissinat

Statut:	Terminé (Sprint)	**Début:**	06/03/2017
Priorité:	Normal	**Echéance:**	24/03/2017
Assigné à:		**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	sprint 2017 10-12 Equipe MENSR	**Temps passé:**	0.00 heure

Description

Test : Correction PROXY-T10-001 - Groupe de machine avec politique "interdits" (2.6.1-b4 - Amon)

http://squash-tm.eole.lan/squash/executions/4899

La navigation est possible sous Linux (Cntlm) alors qu'elle devrait être interdite.

Voir avec upstream.

Sous-tâches:

Tâche # 19773: Correction PROXY-T10-006 - Groupe de machine avec politique "mode liste ...	**Ne sera pas résolu**
Tâche # 19774: Correction PROXY-T10-007 - Groupe de machine avec politique de filtrage ...	**Ne sera pas résolu**

Historique

#1 - 15/03/2017 15:13 - Joël Cuissinat

- Tâche parente changé de #19507 à #19508

#2 - 15/03/2017 15:19 - Joël Cuissinat

À rapprocher de :

- PROXY-T10-006 - Groupe de machine avec politique "mode liste blanche" : http://squash-tm.eole.lan/squash/executions/4936
- PROXY-T10-007 - Groupe de machine avec politique de filtrage personnalisée : http://squash-tm.eole.lan/squash/executions/4955/executions/4955

#3 - 16/03/2017 15:11 - Daniel Dehennin

- Sujet changé de PROXY-T10-001 - Groupe de machine avec politique "interdits" (beta4 - Amon) à Correction PROXY-T10-001 - Groupe de machine avec politique "interdits" (2.6.1-b4 - Amon)

#4 - 17/03/2017 11:07 - Scrum Master

- Sujet changé de Correction PROXY-T10-001 - Groupe de machine avec politique "interdits" (2.6.1-b4 - Amon) à Vérifier qu'e2guardian utilise bien X-Forwarded-For pour les Groupe de machine

- Description mis à jour

- Tâche parente #19508 supprimé

#5 - 17/03/2017 11:07 - Scrum Master

- Tracker changé de Tâche à Scénario

- Echéance mis à 24/03/2017

#6 - 20/03/2017 15:36 - Daniel Dehennin

Le problème vient du fait que le permier plugin d'authentification qui identifie l'utilisateur défini le groupe de filtrage.

La différence de fonctionnement visible entre un poste client intégrée au domaine Scribe et un poste utilisant cNTLM tient de la différence de

traitement de l'authentification.

Une machine client utilisant cNTLM

1. Le navigateur se connecte au proxy cNTLM
2. Le proxy négocie l'authentification avec le navigateur
3. Le proxy envoit le paquet authentifié à e2guardian avec l'entête **Proxy-Authorization**
4. e2guardian voit une nouvelle connexion et joue les plugins d'authentification
    1. Le plugin **proxy-ntlm** détecte l'entête **Proxy-Authorization** et valide l'authentification
    2. Le plugin **proxy-ntlm** détermine le groupe de filtrage basé sur le nom d'utilisateur (dans mon cas aucun)
    3. Aucun autre plugin d'authentification n'est joué
5. e2guardian applique le filtrage déterminé par son groupe de filtrage (dans mon cas aucun)
6. La connexion est transmise à squid et la connexion continue

Une machine client intégrée au domaine ne correspondant pas à un groupe de machine déclaré dans l'EAD

1. Le navigateur se connecte à e2guardian
2. e2guardian voit une une nouvelle connexion et joue les plugins d'authentification
    1. Le plugin **proxy-ntlm** ne détecte pas l'entête **Proxy-Authorization**

    ```
    50241 -Not got persistent credentials for this connection - querying auth plugins
    50241 -Querying next auth plugin...
    No auth negotiation currently in progress - making initial request persistent so that proxy will advert
    ise NTLM
    ```

    2. Le plugin **proxy-basic** ne prend pas en charge la connexion

    ```
    Auth plugin did not find a match; querying remaining plugins
    50241 -Querying next auth plugin...
    ```

    3. Le plugin **ip** ne trouve pas de correspondance entre l'IP de la station cliente et un groupe de machine
3. e2guardian transmet la connexion à squid
4. squid demande une négociation d'authentification qui est transmise au navigateur
5. Le navigateur se reconnecte à e2guardian en ajoutant l'entête **Proxy-Authorization**
6. e2guardian voit une nouvelle connexion et joue les plugins d'authentification
    1. Le plugin **proxy-ntlm** détecte l'entête **Proxy-Authorization** et valide l'authentification
    2. Le plugin **proxy-ntlm** détermine le groupe de filtrage basé sur le nom d'utilisateur (dans mon cas aucun)
    3. Aucun autre plugin d'authentification n'est joué
7. e2guardian applique le filtrage déterminé par son groupe de filtrage (dans mon cas aucun)
8. La connexion est transmise à squid et la connexion continue

Une machine client intégrée au domaine correspondant à un groupe de machine déclaré dans l'EAD

1. Le navigateur se connecte à e2guardian
2. e2guardian voit une une nouvelle connexion et joue les plugins d'authentification
    1. Le plugin **proxy-ntlm** ne détecte pas l'entête **Proxy-Authorization**

    ```
    50241 -Not got persistent credentials for this connection - querying auth plugins
    50241 -Querying next auth plugin...
    No auth negotiation currently in progress - making initial request persistent so that proxy will advert
    ise NTLM
    ```

    2. Le plugin **proxy-basic** ne prend pas en charge la connexion

    ```
    Auth plugin did not find a match; querying remaining plugins
    50241 -Querying next auth plugin...
    ```

    3. Le plugin **ip** trouve une correspondance entre l'IP de la station cliente et le groupe de machine **squash** et détermine le groupe de filtrage associé
3. e2guardian applique le filtrage déterminé par son groupe de filtrage → **interdit** bloque toutes les connexions

#7 - 22/03/2017 09:29 - Joël Cuissinat

- Points de scénarios mis à 1.0

#8 - 24/03/2017 15:18 - Scrum Master

- Statut changé de Nouveau à Terminé (Sprint)