EOLE AD DC - Proposition Scénario #19317

Evolution du filtrage IPTABLE mise en place sur le SETH en 2.6.1

22/02/2017 15:26 - Emmanuel IHRY

Statut:	Fermé	**% réalisé:**	0%
Priorité:	Normal	**Temps estimé:**	0.00 heure
Assigné à:		**Temps passé:**	0.00 heure
Catégorie:	Version mineure		
Version cible:			

Description

La solution mise en oeuvre en 2.6.1 n'est pas tout à fait satisfaisante. Le module peut être diffusé en l'état mais une évolution doit être envisagée pour la version 2.6.2.

Dans la solution mise en place en 2.6.1, le filtrage des flux AD (on ne parle pas des flux spécifiques EOLE) est basé sur la saisie ou non de ces trois familles de clients du serveur :

- Adresses IP des serveurs autorisés à se connecter
- Réseaux autorisés à se connecter aux services samba
- Adresses IP autorisées à se connecter au service LDAP

Fonctionnement en 2.6.1 :

- lorsqu'aucune IP n'est définie pour ces trois familles, les flux sont open avec comme source any --> OK

- lorsque ces trois familles sont saisies, cela revient à n'ouvrir les flux nécessaires que pour chacune des plages IP sources des trois familles. Le SETH n'autorise plus les connexions entrantes que pour les seuls serveurs et PC identifiés --> OK, ceci permet de diffuser la version 2.6.1 en l'état car le filtrage fin est possible.

- lorsque seule l'une des deux familles "Réseaux autorisés à se connecter aux services samba" ou "Adresses IP des serveurs autorisés à se connecter" est saisie :

La plupart des flux restent ouverts pour source any, alors qu'on pourrait s'attendre à ce que seuls les flux nécessaires à la famille pour laquelle on a saisi des IP sources soient ouverts (pour les seules IP sources désignées). Mais comme les flux entre les deux familles sont assez similaires (sauf le port 464) le pare-feu reste ouvert en any alors qu'on pensait avoir une limitation aux seules IP sources saisies --> KO

Dans cette situation, le fait de saisir des "Adresses IP autorisées à se connecter au service LDAP" ne sert a rien puisque les flux sont déjà ouverts en any.

- d'autre part, des flux sont ajoutés en cas de saisie de "Adresse IP des contrôleurs de domaine faisant partie du même domaine Active Directory". J'ai l'impression que cela fait double emploi avec "Adresses IP des serveurs autorisés à se connecter" ?

Evolution proposée pour la 2.6.2 :

- faire en sorte que dès lors que l'on renseigne des valeurs pour une seule des trois familles, il n'y ait plus aucun flux AD ouvert en any. On considère alors que le serveur ne peut accepter comme flux entrants que ceux correspondant aux familles pour lesquelles les IP sources sont explicitement identifiées (donc saisies).

- voir les liens avec "Adresse IP des contrôleurs de domaine faisant partie du même domaine Active Directory"

Demandes liées:

Lié à EOLE AD DC - Tâche #18221: Faire évoluer les règles FW à mettre en plac...	**Fermé**	**01/12/2016**	
Lié à EOLE AD DC - Scénario #20777: Seth : revoir/clarifier le fonctionnement...	**Terminé (Sprint)**	**01/09/2017**	**29/09/2017**

Historique

#1 - 22/02/2017 16:14 - Benjamin Bohard

- Lié à Tâche #18221: Faire évoluer les règles FW à mettre en place sur un ROCD/RWDC ajouté

#2 - 22/02/2017 16:21 - Benjamin Bohard

Fonctionnement en 2.6.1

Pour les ports utilisés par les postes clients et les serveurs (c'est-à-dire l'ensemble des ports utilisés par les serveurs selon la liste établie dans la demande liée), les ip autorisées sont déterminées comme l'*union* des deux ensembles.

Fonctionnement attendu en 2.6.2

Les ip autorisées devront être déterminées comme :

- **any**, si aucune plage n'est précisée nulle part (c'est-à-dire tous les ensembles sont vides) ;
- l' **union** de TOUS les ensembles définis.

En partant du principe que les ensembles ne sont pas *any* par défaut si aucune plage n'est précisée mais bien *vide*.

La grande différence par rapport à la spécification précédente est donc qu'il n'y a pas de valeur par défaut pour les différents ensembles (serveurs, postes clients, clients ldap).

#3 - 23/02/2017 13:16 - Emmanuel IHRY

NB : pour le Seth membre, je ne sais pas si la famille "Adresses IP autorisées à se connecter au service LDAP" a bien un sens

#4 - 14/06/2017 08:49 - Emmanuel IHRY

- Lié à Scénario #20777: Seth : revoir/clarifier le fonctionnement des autorisations réseau ajouté

#5 - 04/08/2017 09:24 - Emmanuel IHRY

- Statut changé de Nouveau à Fermé

remplacé par #20777: