

## eole-vpn - Anomalie #6956

### gestion des xfrm policy

01/06/2014 01:52 PM - Karim Ayari

<b>Status:</b>	Fermé	<b>Start date:</b>	
<b>Priority:</b>	Normal	<b>Due date:</b>	01/10/2014
<b>Assigned To:</b>	Fabrice Barconnière	<b>% Done:</b>	100%
<b>Category:</b>		<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	Mises à jour 2.3.12	<b>Spent time:</b>	3.17 hours
<b>Distribution:</b>	EOLE 2.3		
<b>Description</b>			
La génération des règles "ip xfrm policy" prend tout en compte de ce fait nous rencontrons un problème d'accès au serveur amon dans les tunnels depuis un serveur de supervision (sur un réseau 10 non connu de l'amon) au rectorat lorsque l'amon a une route statique pointant sur eth0.			
pour que cela fonctionne on doit supprimer une règle xfrm:			
<b>ip xfrm policy delete src 10.169.254.240/28 dst reseau_eth1 dir in</b>			
Vu avec Fabrice, il faut revoir le script pour ne pas prendre en compte les routes sur eth0.			
<b>Related issues:</b>			
Related to eole-vpn - Anomalie #6949: ip_xfrm_policy n'est pas mis à jour aut...		<b>Fermé</b>	<b>01/10/2014</b>
Related to eole-vpn - Evolution #6965: ip_xfrm_policy : gérer les alias		<b>Fermé</b>	<b>01/10/2014</b>
Related to Amon - Scénario #22836: Correction dans la gestion des xfrm policy		<b>Terminé (Sprint)</b>	<b>01/30/2018 03/09/2018</b>

### Associated revisions

#### Revision e752c04a - 01/06/2014 04:12 PM - Fabrice Barconnière

Templatisation du script ip\_xfrm\_policy et ajout de tests sur les routes statiques pour exclure eth0  
fixes #6949 fixes #6956 @3h

#### Revision 11c1e2f1 - 01/06/2014 04:45 PM - Fabrice Barconnière

Portage en 2.4 des modifs 2.3 : templatisation ip\_xfrm\_policy  
ref #6949 ref #6956 ref #6965 @15m

### History

#### #1 - 01/06/2014 02:52 PM - Fabrice Barconnière

- Project changed from Amon to eole-vpn
- Due date set to 01/10/2014
- Status changed from Nouveau to Accepté
- Assigned To set to Fabrice Barconnière
- Target version set to Mises à jour 2.3.12

#### #2 - 01/06/2014 04:15 PM - Fabrice Barconnière

- Status changed from Accepté to Résolu
- % Done changed from 0 to 100

Appliqué par commit [e752c04a6d71580a5d2f6042ad74244beb48942e](#).

**#3 - 01/06/2014 06:49 PM - Karim Ayari**

- test ok, les routes pointant sur eth0 ne sont plus traitées.

**#4 - 02/06/2014 09:57 AM - Fabrice Barconnière**

- *Status changed from Résolu to Fermé*

Testé et validé par Karim

**#5 - 01/26/2018 09:52 AM - Jean-Marc MELET**

Bonjour,

Je déteure un vieux signalement car nous nous sommes aperçu d'un effet de bord qui nous pose problème maintenant.

En effet, nous avons découvert que ce changement engendre maintenant un problème inverse qui à mon sens est plus gênant: Si pour une raison quelconque (typiquement chez nous besoin d'exclure du VPN une route RFC1918 d'une collectivité reliée en VPN niveau 3 opérateur aux établissements sur eth0) nous devons déclarer une route statique sur eth0, celle-ci n'est plus exclue des tunnels dans ip\_xfrm\_policy, ce qui empêche tout bonnement les communications avec ces réseaux dans ces cas là.

Il me semble que le cas décrit à l'origine de ce changement peut être contourné autrement, en tout cas à mon avis il ne doit pas justifier de "pénaliser" la gestion globale des routes sur la passerelle Amon.

**#6 - 01/26/2018 01:09 PM - Gérald Schwartzmann**

- *Related to Scénario #22836: Correction dans la gestion des xfrm policy added*