eole-common - Anomalie #8271

plus de traffic dans les tunnels apres un reconfigure

27/05/2014 17:06 - Christophe Dezé

Statut:	Fermé	**Début:**	
Priorité:	Haut	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	4.00 heures
Version cible:		**Temps passé:**	0.00 heure
Distribution:	Toutes		

Description

vu avec barco
les tunnels mettent trop de temsp à monter ???
il manque

-A POSTROUTING -s 172.21.163.0/24 -d 192.168.0.0/16 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 172.21.163.0/24 -d 192.168.0.0/16 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 10.172.254.0/24 -d 192.168.0.0/16 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 10.172.254.0/24 -d 192.168.0.0/16 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 172.21.163.0/24 -d 10.0.0.0/8 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 172.21.163.0/24 -d 10.0.0.0/8 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 10.172.254.0/24 -d 10.0.0.0/8 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 10.172.254.0/24 -d 10.0.0.0/8 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 172.21.163.0/24 -d 172.16.0.0/12 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 172.21.163.0/24 -d 172.16.0.0/12 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 10.172.254.0/24 -d 172.16.0.0/12 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 10.172.254.0/24 -d 172.16.0.0/12 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 192.168.0.0/16 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 192.168.0.0/16 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 161.48.0.0/19 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 161.48.0.0/19 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 10.0.0.0/8 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 10.0.0.0/8 -o eth0 -m state --state NEW -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 172.16.0.0/12 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A POSTROUTING -s 10.72.254.0/24 -d 172.16.0.0/12 -o eth0 -m state --state NEW -j ACCEPT

Demandes liées:

Lié à Amon - Anomalie #8376: bastion ne démarre pas	**Fermé**		
Lié à eole-common - Tâche #5897: creole_serv non fonctionnel après reboot	**Fermé**	**09/10/2014**	**20/06/2014**

Historique

#1 - 27/05/2014 17:15 - Fabrice Barconnière

- Projet changé de Amon à eole-common

- Statut changé de Nouveau à Accepté

- Temps estimé mis à 4.00 h

Lors d'un reconfigure, networking lance bastion qui relance rvp. Or bastion est relancé pas loin derrière et relance rvp. Cela conduit à cette situation lorsque les tunnels mettent un certain temps à monter. L'exécution des scripts /etc/ipsec.d/ipsec_updown semble se chevaucher.
Sur ma VM, je ne reproduit pas le problème.
Le problème à régler est donc le double lancement de bastion au reconfigure.

#2 - 27/05/2014 18:01 - Christophe Dezé

Le problème survient lors d'un start de bastion après un restart.
Pas forcément dans la foulée. Donc ça ne doit pas être du à un ifup -a simultané

#3 - 28/05/2014 11:55 - Fabrice Barconnière

En fait, je reproduis bien le problème sur ma VM, les règles disparaissent.
Le problème est au niveau de l'action bastion start lorsque les tunnels sont déjà montés :

- le script /sbin/lance.firewall appelé fait un flush des tables
  - les règles liées aux tunnels disparaissent
- le script d'init rvp est appelé avec un start uniquement
  - les tunnels étant déjà montés, strongSwan ne tente pas de les remonter et n'appelle donc pas le script /etc/ipsec.d/ipsec_updown (qui met en place les règles iptables liées aux tunnels)

#4 - 28/05/2014 15:02 - Fabrice Barconnière

- Distribution changé de EOLE 2.4 à Toutes

Le problème est le même en 2.3 !!!

#5 - 12/06/2014 09:08 - Fabrice Barconnière

- Echéance mis à 20/06/2014

- Priorité changé de Normal à Haut

On peut masquer le pb en ajoutant "stopother" avant "start" dans le case "start)" du script d'init bastion.
Cela n'empêchera pas le double lancement de bastion mais au moins, les tunnels seront arrêtés et strongSwan remettra les règles liées aux tunnels.

#6 - 12/06/2014 15:39 - Fabrice Barconnière

- Assigné à mis à Fabrice Barconnière

- Version cible mis à sprint 2014 36-37

#7 - 23/06/2014 15:20 - Daniel Dehennin

- Echéance 20/06/2014 supprimé

- Assigné à Fabrice Barconnière supprimé

- Version cible sprint 2014 36-37 supprimé

#8 - 16/11/2015 13:52 - Fabrice Barconnière

- Statut changé de Accepté à Fermé

Le script d'init bastion a été réécrit à partir d'EOLE 2.4.x. Si bastion est déjà lancé, l'action start ne fera rien. On ne perdra donc plus les règles iptables liées aux tunnels