Distribution EOLE - Tâche #13114

Scénario # 13068 (Partiellement Réalisé): Permettre au MEDDE d'accéder à squashTM

Monter une connexion VPN entre eSSL MEDDE et FW-EOLE

09/22/2015 02:31 PM - Fabrice Barconnière

Status:	Fermé	**Start date:**	09/21/2015
Priority:	Normal	**Due date:**	
Assigned To:	Fabrice Barconnière	**% Done:**	100%
Target version:	Sprint 2015 39-41 - Équipe MENESR	**Estimated time:**	6.00 hours
		Spent time:	5.00 hours

Description

Maintenant que la fonctionnalité tunnel entre une réseau et une adresse IP a été vérifiée, trouver pourquoi on n'arrive pas à le faire entre FW-EOLE et FW-MEDDE.
Quelques pistes :

- Passerelle VPN EOLE : serveur Debian Wheezy avec le serveur cible sur une interface VLAN
- Passerelle VPN MEDDE : serveur eSBL NATTÉ derrière une livebox

On constate que la connexion ne s'établit qu'à l'initiative de la passerelle du MEDDE.
Aucun trafic ne passe.

On pourrait vérifier les règles IPtables sur la passerelle EOLE (au minimum ceci) :

```
-A INPUT -i eth0 -j eth0-root
-A INPUT -i vlan300 -j vlan300-root
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -o vlan300 -j eth0-vlan300
-A FORWARD -i vlan300 -o eth0 -j vlan300-eth0
-A OUTPUT -o lo -j ACCEPT
-A eth0-eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A eth0-vlan300 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A eth0-vlan300 -m policy --dir in --pol ipsec --proto esp -j ACCEPT
-A eth0-vlan300 -j DROP
-A eth0-root -p udp -m udp --dport 500 -j ACCEPT
-A eth0-root -p udp -m udp --dport 4500 -j ACCEPT
-A eth0-root -p esp -j ACCEPT
-A eth0-root -m policy --dir in --pol ipsec --proto esp -j ACCEPT
-A eth0-root -m state --state RELATED,ESTABLISHED -j ACCEPT
-A eth0-root -j DROP
-A vlan300-eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A vlan300-eth0 -m policy --dir out --pol ipsec --proto esp -j ACCEPT
-A vlan300-eth0 -j DROP
-A vlan300-root -m policy --dir in --pol ipsec --proto esp -j ACCEPT
-A vlan300-root -m state --state RELATED,ESTABLISHED -j ACCEPT
-A vlan300-root -j DROP
-A root-eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A root-eth0 -m state --state NEW -j ACCEPT
-A root-eth0 -m policy --dir out --pol ipsec --proto esp -j ACCEPT
```

- Pour info, il n'y a pas besoin de route spécifique à ce tunnel côté FW-EOLE

Vérifier également la livebox:

- http://assistance.orange.fr/livebox-modem/toutes-les-livebox-et-modems/installer-et-utiliser/piloter-et-parametrer-votre-materiel/la-creation-d-un-reseau/creer-un-reseau-vpn/livebox-pro-v2-configurer-le-pare-feu-pour-l-utilisation-du-vpn_26590-27230
- autorisation UPD/500, UDP/4500, ESP
- peut-être NAT des paquets provenant venant d'IP eth0 EOLE UDP/500 et 4500 vers IP eth0 eSSL

History

#1 - 09/22/2015 02:34 PM - Fabrice Barconnière

- Status changed from En cours to Nouveau

- % Done changed from 100 to 0

#2 - 09/22/2015 02:34 PM - Fabrice Barconnière

- Remaining (hours) changed from 0.0 to 6.0

#3 - 09/22/2015 02:36 PM - Fabrice Barconnière

- Tracker changed from Tâche to Anomalie

- Assigned To deleted (Fabrice Barconnière)

- Target version deleted (Sprint 2015 39-41 - Équipe MENESR)

#4 - 09/22/2015 02:38 PM - Fabrice Barconnière

- Tracker changed from Anomalie to Tâche

#5 - 09/22/2015 02:42 PM - Fabrice Barconnière

- Parent task set to #13068

#6 - 09/22/2015 02:49 PM - Fabrice Barconnière

- Description updated

#7 - 09/22/2015 03:09 PM - Fabrice Barconnière

- Description updated

#8 - 09/22/2015 03:33 PM - Daniel Dehennin

- Description updated

#9 - 09/23/2015 10:54 AM - Fabrice Barconnière

- Status changed from Nouveau to En cours

#10 - 09/23/2015 10:54 AM - Fabrice Barconnière

- Assigned To set to Fabrice Barconnière

#11 - 09/23/2015 02:46 PM - Fabrice Barconnière

- % Done changed from 0 to 50

On avance :

```
barco> teebee44: je viens de voir Sam, de notre coté, la conf semble correcte. Les ping issues de Squash sorte
nt bien chiffrés de notre FW, mais il n'y a pas de réponse.
<barco> la box doit certainement les bloquer.
<teebee44> ok
<barco> il doit falloir rediriger UDP/500, UDP/4500 et le protocol ESP (protocol 50) vers l'IP eth0 de ton
```

#12 - 09/23/2015 04:08 PM - Fabrice Barconnière

Pour le suivi des opérations :

```
<teebee44> barco, pour info, j'ai baissé le niveau de fw de la box et créé le nat qui va bien, pas mieux
<teebee44> faut voir avec Sam
```

#13 - 09/24/2015 11:27 AM - Fabrice Barconnière

- % Done changed from 50 to 70

- Remaining (hours) changed from 6.0 to 3.0

Le tunnel fonctionne. On verra à 13h après un reconfigure si c'est ok.

#14 - 09/24/2015 03:08 PM - Fabrice Barconnière

- % Done changed from 70 to 100

- Remaining (hours) changed from 3.0 to 0.0

Après un dernier réglage sur eSSL du MEDDE + reconfigure, les machines sur leur réseau accèdent bien à la machine "jessie" (ping). Ça passe pas depuis eSSL, mais ça ne pose pas de problème particulier.

#15 - 09/24/2015 05:28 PM - Thierry Bertrand

- Status changed from En cours to Résolu

#16 - 09/25/2015 09:46 AM - Scrum Master

- Status changed from Résolu to Fermé