Distribution EOLE - Tâche #13093

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

Monter une infra VPN Amon-Sphynx avec un tunnels vers une IP coté Amon.

09/22/2015 10:29 AM - 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:	3.00 hours

Description

History

#1 - 09/22/2015 10:29 AM - Fabrice Barconnière

- Status changed from Nouveau to En cours

#2 - 09/22/2015 10:29 AM - Fabrice Barconnière

- Assigned To set to Fabrice Barconnière

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

- Subject changed from Monter une infra VPN Amon-Sphynx avec un tunnels vers une IP coté Sphynx. to Monter une infra VPN Amon-Sphynx avec un tunnels vers une IP coté Amon.

- % Done changed from 0 to 100

- Remaining (hours) changed from 6.0 to 0.0

- Sphynx correspondant à la passerelle VPN du MEDDE : réseau cible sur carte eth1
- Amon correspondant à la passerelle VPN EOLE : serveur Horus sur eth1 comme serveur cible
  La connexion VPN s'établit sans problème et seul le traffic entre le réseau eth1 Sphynx et l'adresse IP Horus passe en chiffré (but recherché).

La situation réelle :

- 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
```

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

#4 - 09/22/2015 02:37 PM - Fabrice Barconnière

- Remaining (hours) changed from 0.0 to 1.0

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

- Remaining (hours) changed from 1.0 to 0.0

#6 - 09/23/2015 09:51 AM - Scrum Master

- Status changed from En cours to Résolu

#7 - 09/25/2015 09:45 AM - Scrum Master

- Status changed from Résolu to Fermé