# conf-amon - Evolution #4803

## leftsourceip en 2.3

01/31/2013 07:34 AM - Guillaume PITARD

| | | | |
|---|---|---|---|
| **Status:** | Fermé | **Start date:** | |
| **Priority:** | Haut | **Due date:** | 04/12/2013 |
| **Assigned To:** | Fabrice Barconnière | **% Done:** | 100% |
| **Category:** | | **Estimated time:** | 0.25 hour |
| **Target version:** | Mises à jour 2.3.9 | **Spent time:** | 1.33 hour |
| **Distribution:** | EOLE 2.3 | | |

**Description**

Bonjour,

J'ai découvert un bug problématique en 2.3 lorsqu'on gère les tunnels agriates.

On ne peut pas imposer dans la conf vpn avec quelle adresse IP l'amon va rentrer dans les tunnels.
Ainsi si un proxy parent existe et nécessite le passage par les tunnels, ou lors des requêtes DNS à destination des serveurs en in.ac-quelque-chose, on ne maîtrise l'adresse IP source.
Cela peut-être une ip 10.dep (admin) ou une en 10.1dep (peda), dans mon cas j'ai également des IP en 172 pour des réseaux péda.
Du coup, s'il existe des règles de filtrage pour que des stations pédagogiques n'aillent pas sur nos réseaux centraux, cela va provoquer des dysfonctionnements.

Pouvez-vous faire en sorte que lorsque les paquets sont émis par l'amon, il le soit avec l'IP admin de l'amon.

Cordialement,

**Related issues:**

| | | |
|---|---|---|
| Related to arv - Evolution #4036: adresse source aléatoire | **Fermé** | **09/11/2012** |

### Associated revisions

**Revision a79eb240 - 04/04/2013 04:56 PM - Fabrice Barconnière**

rvp/tmpl/ipsec_updown : routes gérées ici -> ip eth1 src par defaut
rvp/tmpl/strongswan.conf : désactiver gestion routes par Strongswan
fixes #4803 @1h

### History

**#1 - 01/31/2013 08:34 AM - Guillaume PITARD**

Bonjour,

C'est même pire que ce que je pensais, l'ip source de l'amon change en fonction du réseau de la destination.
Voici un exemple obtenu pour 4 réseaux différents, les ping son lancé du même amon.

root@pf-amon.crid72.in.ac-nantes.fr:~# ping 10.10.10.10
...
root@pf-amon.crid72.in.ac-nantes.fr:~# ping 172.30.30.30
...
root@pf-amon.crid72.in.ac-nantes.fr:~# ping 192.168.1.1
...
root@pf-amon.crid72.in.ac-nantes.fr:~# ping 161.48.0.1

résultats sur le sphynx:
root@xxxxxxxxx:~# tcpdump -ni eth0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
08:18:19.973259 IP 10.72.254.4 > 10.10.10.10: ICMP echo request, id 11376, seq 1, length 64
...
08:18:33.789489 IP 10.172.254.126 > 172.30.30.30: ICMP echo request, id 12144, seq 1, length 64
...
08:18:48.376163 IP 10.172.254.126 > 192.168.1.1: ICMP echo request, id 15216, seq 1, length 64
...

08:19:07.353470 IP 10.72.254.4 > 161.48.0.1: ICMP echo request, id 16496, seq 1, length 64

On vois l'amon utiliser des IP différentes en fonction des réseau de destination.

Ce qui est cohérent avec l'ordre dans lequel les tunnels ce sont montés.

amon crid72-sphynx RECTORAT ACADEMIE DE NANTES[1]: ESTABLISHED 8 minutes ago, 10.172.253.254[C=fr, O=gouv, OU=education, OU=ac-nantes, CN=0721572T-02]...195.83.xx.xx[C=fr, O=gouv, OU=education, OU=ac-nantes, CN=AGRIATES-NANTES-02]
APA_admin_10{1}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c6e9ba90_i cc3fd008_o
APA_admin_10{1}:   10.72.254.0/24 === 10.0.0.0/8
APA_peda_192{2}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c71d98bb_i cd6288eb_o
APA_peda_192{2}:   10.172.254.0/24 === 192.168.0.0/16
APA_peda_172{3}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c07de140_i c9f786da_o
APA_peda_172{3}:   10.172.254.0/24 === 172.16.0.0/12
APA_peda_10{4}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c621c035_i ce367b71_o
APA_peda_10{4}:   10.172.254.0/24 === 10.0.0.0/8
APA_admin_ader{5}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c3c82818_i c8ab342f_o
APA_admin_ader{5}:   10.72.254.0/24 === 161.48.0.0/19
APA_admin_172{6}:  INSTALLED, TUNNEL, ESP in UDP SPIs: cb09a80d_i cca36fe6_o
APA_admin_172{6}:   10.72.254.0/24 === 172.16.0.0/12
APA_admin_192{7}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c899ba54_i c0447f63_o
APA_admin_192{7}:   10.72.254.0/24 === 192.168.0.0/16

Le problème est que ce n'est pas satisfaisant du point de vue de la sécurité.
Le comportement n'est pas prédictive.

Cordialement,

#### #2 - 01/31/2013 09:18 AM - Guillaume PITARD

Re-bonjour,

```
Je pense avoir trouver la solution pour fixer l'IP source des trames émises par l'amon, mais je ne sais pas co
mment intégrer ça.
```

```
ip route add 10.0.0.0/8 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
  ip route add 172.16.0.0/12 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
  ip route add 192.168.0.0/16 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
  ip route add 161.48.0.0/19 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
```

Cordialement,

#### #3 - 01/31/2013 10:36 AM - Guillaume PITARD

En creusant un peu je pense vous avoir trouver une piste.

1) modif de /etc/strongswan.conf dans le paragraphe charon
Remplacer install_routes = yes
par install_route = no

2) modifier le script /etc/init.d/rvp
Ajouter dans le paragraphe start:
if [ $RETVAL -eq 0 ]; then
ip route add 10.0.0.0/8 via 10.172.253.253 dev eth0 proto static src 10.72.254.4
ip route add 172.16.0.0/12 via 10.172.253.253 dev eth0 proto static src 10.72.254.4
ip route add 192.168.0.0/16 via 10.172.253.253 dev eth0 proto static src 10.72.254.4
ip route add 161.48.0.0/19 via 10.172.253.253 dev eth0 proto static src 10.72.254.4
fi

```
Ajouter dans le paragraphe stop:
    ip route del 10.0.0.0/8
    ip route del 172.16.0.0/12
    ip route del 192.168.0.0/16
    ip route del 161.48.0.0/19
```

C'est un peu brute de fonderie, il faudrait que ce soit en cohérence avec ARV.

Bon courage.

#### #4 - 01/31/2013 11:04 AM - Guillaume PITARD

La modif peut encore être plus light.
C'est même tellement light qu'on pourrait appeler ça du zéro.

Modifier uniquement le script /etc/init.d/rvp
en ajoutant simplement dans le paragraphe start:
if [ $RETVAL -eq 0 ]; then
ip route replace 10.0.0.0/8 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
ip route replace 172.16.0.0/12 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
ip route replace 192.168.0.0/16 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
ip route replace 161.48.0.0/19 via 'IP de ETH0' dev eth0 proto static src 'IP de ETH1'
fi

Bon maintenant, il faut arriver mettre ça en cohérence avec les modèles de liens sécurisés dans ARV, mais là je ne sais pas faire, à vous de jouer...

Cordialement,

#### #5 - 02/08/2013 10:21 AM - Joël Cuissinat

*- Target version changed from Mises à jour 2.3.8 to Mises à jour 2.3.9*

#### #6 - 03/14/2013 02:17 PM - Guillaume PITARD

Bonjour,

Fabrice m'a proposé par mail une solution qui me semble fonctionnelle, et qui me convient. Je la mets dans ce fil, ça permettra peut-être de l'avoir à la prochaine mise à jour Amon.

Cordialement.

MAIL de FABRICE :

**Salut Guillaume,**

**Peux-tu me dire si ceci te convient :**
**À faire sur Amon uniquement.**
**Dans /etc/ipsec.d/ipsec_updown :**
**ligne 349 : décommenter #uproute**
**ligne 369 : décommenter #downroute**
**Dans /etc/strongswan.conf :**
**Remplacer la ligne 19 par : install_routes = no**

**Relancer rvp.**

**Le script ipsec_updown est lancé à chaque montée/descente de tunnel et installera/supprimera les routes forcée par IP eth1.**
**Les routes ne sont plus gérées par Strongswan (install_routes = no)**

**Attention, un reconfigure annulera les modifs. Si ça te convient, on pourra intégrer ceci.**

**--**
**Cordialement,**
**Fabrice Barconnière**
**Equipe EOLE**

#### #7 - 03/26/2013 08:44 AM - Fabrice Barconnière

*- Status changed from Nouveau to En attente d'informations*

*- Estimated time set to 0.25 h*

Attente d'infos pour savoir si Guillaume est satisfait de cette solution et si il n'y a pas d'effets indésirables.

#### #8 - 03/26/2013 08:45 AM - Fabrice Barconnière

*- Tracker changed from Anomalie to Evolution*

#### #9 - 03/26/2013 04:15 PM - Fabrice Barconnière

*- Project changed from arv to conf-amon*

#### #10 - 03/27/2013 11:30 AM - Fabrice Barconnière

*- Due date set to 03/29/2013*

#### #11 - 03/29/2013 10:13 AM - Redmine Admin

*- Due date changed from 03/29/2013 to 04/05/2013*

#### #12 - 04/02/2013 09:46 AM - Luc Bourdot

*- Due date changed from 04/05/2013 to 04/04/2014*

#### #13 - 04/02/2013 09:51 AM - Guillaume PITARD

Salut Luc,

```
2014 c'est une erreur de frappe, rassures moi !!!
```

Cordialement,

#### #14 - 04/04/2013 03:41 PM - Guillaume PITARD

Salut,

Après tests et re-test, je peux dire que la modification proposer par Fabrice est satisfaisante.

Désolé pour le retard, je pensais avoir déjà répondu.

Cordialement.

#### #15 - 04/04/2013 03:49 PM - Gérald Schwartzmann

*- Status changed from En attente d'informations to Accepté*

#### #16 - 04/04/2013 04:58 PM - Fabrice Barconnière

*- Status changed from Accepté to Résolu*

*- % Done changed from 0 to 100*

Appliqué par commit a79eb240302c4b3d1e1db96d0d22bff725e37ac5.

#### #17 - 04/10/2013 10:23 AM - Fabrice Barconnière

*- Due date changed from 04/04/2014 to 04/12/2013*

#### #18 - 04/10/2013 11:38 AM - Fabrice Barconnière

*- Status changed from Résolu to Fermé*