arv - Tâche #8545

Scénario # 8772 (Terminé (Sprint)): VPN - ARV

gerer leftsendcert = never

07/04/2014 09:15 AM - Christophe Dezé

Status:	Fermé	**Start date:**	
Priority:	Normal	**Due date:**	09/12/2014
Assigned To:	Fabrice Barconnière	**% Done:**	100%
Target version:	sprint 2014 36-37	**Estimated time:**	7.00 hours
		Spent time:	29.00 hours

Description

La solution de Fabrice fonctionne

Le 02/07/2014 22:09, Laurent Haeffelé a écrit :

> Le 02/07/2014 21:55, cd a écrit :
>
> > Le passage en IKEv2 de strongswan (sphynx 2.3) lié a des soucis
> > de gestion de la fragmentation par ces modems empêchent
> > l'établissement des tunnels. Avez vous aussi constaté cela ?
>
> Oui. J'ai constaté cela sur un établissement de l'académie de
> Strasbourg aussi, mais je n'ai pas trouvé de solution pour le
> moment ...
>
> Cordialement,

Bonjour,

IKEV2 ne supporte pas la fragmentation. Il existe juste quelques recommandations pour éviter au maximum cette fragmentation[1], mais dans certain cas, cela reste un problème.

Vous pouvez tenter une solution[2] qui est proposée sur la liste strongSwan Users.
Le but est de diminuer la taille des paquets lors de l'authentification en stockant les certificats des serveurs distant localement et en indiquant à strongSwan de ne pas les envoyer.
En cas de retour positif, on pourrait envisager d'intégrer cette méthode (en mode fichier plat uniquement).

Mise en oeuvre :

- Configuration de Sphynx :
  - Les fichiers certificats **sphynx.pem** et **amon.pem** doivent être dans le répertoire /**etc**/**ipsec.d**/**certs**/
  - Exemple de configuration ipsec (**ipsec.conf**) à modifier pour chaque tunnel (--> sont les lignes à ajouter):

```
#DEB:amon-sphynx-reseth1_adm
conn "amon-sphynx-reseth1_adm"
    leftid = "C=fr, O=gouv, OU=education, OU=ac-academie, CN=sphynx"
    leftcert = "sphynx.pem"
- --> leftsendcert = never
    left = adresse_ip_publique_sphynx
    leftsubnet = "172.x.y.0/24"
```

```
    leftupdown =
    rightid = "C=fr, O=gouv, OU=education, OU=ac-academie, CN=amon"
- --> rightcert = "amon.pem"
    right = adresse_ip_publique_amon
    rightsubnet = "10.d.e.0/24"
    auto=start
#FIN:amon-sphynx-reseth1_adm
```

- Lancer **ipsec rereadall** puis **ipsec update**
  (ou **/etc/init.d/ipsec restart** mais ça coupe les autres tunnels)

- Configuration d'Amon :
  - Les fichiers certificats **sphynx.pem** et **amon.pem** doivent être dans le répertoire **/etc/ipsec.d/certs/**
  - Exemple de configuration ipsec (**ipsec.conf**) à modifier pour chaque tunnel (--> sont les lignes à ajouter):

```
#DEB:amon-sphynx-reseth1_adm
conn "amon-sphynx-reseth1_adm"
    leftid = "C=fr, O=gouv, OU=education, OU=ac-academie, CN=amon"
    leftcert = "amon.pem"
- --> leftsendcert = never
    left = adresse_ip_publique_amon
    leftsubnet = "10.d.e.0/24"
    leftupdown =
    rightid = "C=fr, O=gouv, OU=education, OU=ac-academie, CN=sphynx"
- --> rightcert = "sphynx.pem"
    right = adresse_ip_publique_sphynx
    rightsubnet = "172.x.y.0/24"
    auto=start
#FIN:amon-sphynx-reseth1_adm
```

  - Lancer **/etc/init.d/rvp restart**

Footnotes :
[1] http://tools.ietf.org/html/draft-ietf-ipsecme-ikev2-fragmentation-05
[2] https://www.mail-archive.com/users@lists.strongswan.org/msg07143.html

- --
Cordialement,
Fabrice Barconnière
Equipe EOLE

Related issues:

Related to Documentations - Evolution #8841: Documentation ARV : documenter l...	**Fermé**	**09/12/2014**
Duplicated by arv - Evolution #8733: solution de contournement aux pbs de vpn...	**Fermé**	
Copied to arv - Tâche #8838: gerer leftsendcert = never pour EOLE 2.4.1	**Fermé**	**11/07/2014**

Associated revisions

Revision 4c3151c8 - 09/11/2014 01:24 PM - Fabrice Barconnière

Gestion de l'envoi ou non des certificats à l'établissement des tunnels
fixes #8545 @28h

History

#1 - 07/04/2014 09:37 AM - Fabrice Barconnière

- Description updated

#2 - 07/04/2014 03:19 PM - Fabrice Barconnière

Il serait plus prudent coté Sphynx d'utiliser l'option **leftsencert = ifasked**. Ça permettra au serveur Sphynx d'envoyer son certificat aux serveurs Amon qui n'ont pas encore cette configuration.

#3 - 08/27/2014 01:20 PM - Laurent HAEFFELE

L'idéal serait de pouvoir sélectionner ce mode de configuration par Lien sécurisé ou par Modèle de lien sécurisé dans ERA plutôt que d'avoir une option de configuration globale.

#4 - 08/27/2014 02:05 PM - Emmanuel GARETTE

Dans Era ou ARV ?

#5 - 08/29/2014 03:20 PM - équipe eole Academie d'Orléans-Tours

Bonjour, je ne sais pas à quoi faisait allusion Laurent HAEFFELE (je pense que c'est ARV), mais du point de vue d'Orléans, ça serait au niveau d'ARV, ou l'on pourrait choisir de créer un modele de serveur rvp avec ce type de conf. (pas d'envoi de certificat)
Peux être mieux, comme l'évoque aussi Laurent, ne pas avoir un modèle de serveur dédié mais seulement le choisir cette option sur le type lien sécurisé.

Nicolas

#6 - 09/03/2014 02:59 PM - Fabrice Barconnière

- Due date set to 09/12/2014

- Status changed from Nouveau to Accepté

- Assigned To set to Fabrice Barconnière

- Target version set to sprint 2014 36-37

- Estimated time set to 7.00 h

À discuter :

- Est-ce une bonne idée de proposer cette option globalement pour le modèle (tous les serveur en hériterons) ?
  - Cela pourrait alonger le temps de génération des archives VPN et alourdir leur taille.
  - Si on met la valeur ***ifasked*** sur Sphynx, il faut les certificats de tous les serveurs dans ***/etc/ipsec.d/certs/*** car Sphynx ne les demandera pas et cela allongera d'autant plus le temps de gérération des archives VPN mais il ne sera pas nécessaire de repasser sur tous les Amon.
  - Si on met la valeur ***never*** sur Sphynx, ça veut dire qu'il faut relancer la procédure "active_rvp" sur tous les Amon suite à cette modif (pas viable).
- Sinon, on peut proposer cette option par serveur :
  - Ainsi, on oublie la valeur ***ifasked*** sur Sphynx pour n'avoir que ***never*** ou ***always***
  - Pas besoin de repasser sur tous les Amon.

#7 - 09/04/2014 10:58 AM - Fabrice Barconnière

- Parent task set to #8765

#8 - 09/05/2014 11:31 AM - Luc Bourdot

- Parent task changed from #8765 to #8772

#9 - 09/11/2014 01:27 PM - Fabrice Barconnière

- Status changed from Accepté to Résolu

- % Done changed from 0 to 100

Appliqué par commit 4c3151c8211f4c7559bd2ef3113da566912f725a.

#10 - 09/11/2014 03:54 PM - Bruno Boiget

- Distribution changed from Toutes to EOLE 2.3

#11 - 09/11/2014 04:22 PM - Bruno Boiget

- Status changed from Résolu to Fermé

testé sur la candidate 2.3.14