Distribution EOLE - Tâche #21686

Scénario # 21300 (Terminé (Sprint)): Traitement express MEN (40-42)

Ajout d'algorithme dans la liste de ceux proposés

12/10/2017 12:02 - Jean-Marc MELET

Statut:	Fermé	**Début:**	12/10/2017
Priorité:	Normal	**Echéance:**	
Assigné à:	Fabrice Barconnière	**% réalisé:**	100%
Version cible:	sprint 2017 40-42 Equipe MENSR	**Temps estimé:**	2.00 heures
		Temps passé:	1.50 heure

Description

Afin d'étendre l'interopérabilité avec des systèmes tiers, nous proposons l'ajout des algorithmes d'encryption/authentication **aes128-sha256** pour esp pour être utilisés dans les connections ipsec.
Nous avons récemment eu ce besoin en voulant établir des tunnels ipsec entre Sphynx et un équipement Stormshield basé également sur strongswan. Malheureusement, les modifications apportées au fichier ipsec.conf pour permettre le fonctionnement lors de l'échange mutuel des algorithmes supportés ne sont pas persistantes et la conf d'origine est écrasée à chaque modification faite dans ARV.
Voici la modification dont nous avons eu besoin dans notre cas:

esp = aes128gcm128,aes192gcm128,aes128-sha256

Logs de charon avant la modification:

```
2017-10-09T12:11:05.629735+02:00 sphynx01.agr.ac-aix-marseille.fr charon: 25[IKE] no acceptable pr
oposal found
2017-10-09T12:11:15.623953+02:00 sphynx01.agr.ac-aix-marseille.fr charon: 61[CFG] received proposa
ls: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SEQ
2017-10-09T12:11:15.623972+02:00 sphynx01.agr.ac-aix-marseille.fr charon: 61[CFG] configured propo
sals: ESP:AES_GCM_16_128/NO_EXT_SEQ, ESP:AES_GCM_16_192/NO_EXT_SEQ, ESP:AES_CBC_128/AES_CBC_192/AE
S_CBC_256/3DES_CBC/BLOWFISH_CBC_256/HMAC_SHA1_96/AES_XCBC_96/HMAC_MD5_96/NO_EXT_SEQ
```

Merci

Révisions associées

Révision b513342d - 12/10/2017 13:13 - Fabrice Barconnière

Ajout de l'algorithme de chiffrement aes128-sha256 pour ESP

ref #21686

Révision cf463d06 - 07/11/2017 15:05 - Benjamin Bohard

Passer les machines ldapma et dns-banshee en dépendance dans ModeleReseauTestEole.yaml

Ref #21686

Historique

#1 - 12/10/2017 13:14 - Fabrice Barconnière

- Tracker changé de Demande à Tâche

- Temps estimé mis à 2.00 h

- Tâche parente mis à #21300

- Restant à faire (heures) mis à 2.0

#2 - 12/10/2017 13:14 - Fabrice Barconnière

- Projet changé de Sphynx à Distribution EOLE

- Statut changé de Nouveau à En cours

#3 - 12/10/2017 13:14 - Fabrice Barconnière

- Description mis à jour

- Assigné à mis à Fabrice Barconnière

#4 - 12/10/2017 13:34 - Fabrice Barconnière

- Statut changé de En cours à Résolu

- % réalisé changé de 0 à 100

- Restant à faire (heures) changé de 2.0 à 1.0

#5 - 12/10/2017 15:40 - Fabrice Barconnière

- Statut changé de Résolu à En cours

- % réalisé changé de 100 à 80

Ne pas oublier de merger dans le projet arv de merger la branche feature/new-algo-esp en 2.6.0, 2.6.1 et master.

#6 - 15/10/2017 16:27 - Jean-Marc MELET

Testé fonctionnel sur Sphynx et Amon apres avoir regénéré les conf dans ARV et renvoyé une sur un serveur.

Merci

#7 - 16/10/2017 08:20 - Fabrice Barconnière

- Statut changé de En cours à Résolu

- % réalisé changé de 80 à 100

- Restant à faire (heures) changé de 1.0 à 0.0

merge dans 2.6.0, 2.6.1 et master.
Journaux modifiés.

#8 - 16/10/2017 15:23 - Fabrice Barconnière

- Statut changé de Résolu à Fermé