Distribution EOLE - Tâche #13326

Scénario # 13325 (Terminé (Sprint)): Mettre en place une infrastructure de connexion VPN roadwarrior sur le réseau EOLE (postes nomades domicile, clé 3G, ...)

Monter une maquette sur ONE pour mettre en place les configuration strongSwan

10/02/2015 09:27 AM - Fabrice Barconnière

Status:	Fermé	**Start date:**	10/02/2015
Priority:	Normal	**Due date:**	
Assigned To:	Fabrice Barconnière	**% Done:**	100%
Target version:	Sprint 2015 42-44 - Équipe MENESR	**Estimated time:**	4.00 hours
		Spent time:	4.00 hours

Description

- Un serveur **etb1.amon** sera le FW-EOLE
- Un poste **etb1.scribe** sera le serveur DHCP du réseau EOLE
- Un poste **aca.pc-lxde** sera le poste nomade
- Un serveur **aca.sphynx** sera utilisé pour mixer VPN roadwarrior et VPN MEDDE et pour générer la base des configurations ipsec.

History

#1 - 10/12/2015 02:51 PM - Fabrice Barconnière

- Status changed from Nouveau to En cours

#2 - 10/12/2015 02:52 PM - Fabrice Barconnière

- Description updated

- Assigned To set to Fabrice Barconnière

#3 - 10/13/2015 09:41 AM - Fabrice Barconnière

- % Done changed from 0 to 100

Côté FW EOLE :

- si nécessaire, installer le plugin strongSwan farp (paquet strongswan-plugin-farp) sur le FW EOLE.
- si nécessaire, modifier la configuration, strongSwan pour que les plugin farp se charge
- modèle de connexion ipsec à déclarer sur le firewall (fichier ipsec.conf complet) :

```
#configuration is in ipsec.conf file
config setup
    uniqueids = yes
    cachecrls = yes
    strictcrlpolicy = no

conn %default
    keyingtries = 3
    keyexchange = ike
    authby = pubkey
    dpdaction = restart
    dpddelay = 120s
    ike = aes128-sha256-modp2048,aes192-sha384-modp3072
    esp = aes128gcm128,aes192gcm128
    forceencaps = no
    mobike = no

#DEB:etb1.amon-default-2.5.1-aca-xubuntu_1-RW_tunnel
conn "etb1.amon-default-2.5.1-aca-xubuntu_1-RW_tunnel"
    leftid = "C=FR, L=Dijon, O=Education Nationale, OU=0002 110043015, CN=amon.ac-test.fr"
    leftcert = "amon.ac-test.fr.pem"
    left = 192.168.0.31
    leftsubnet = "10.1.2.0/24"
```

```
    leftupdown = /etc/ipsec.d/ipsec_updown
    rightid = "C=FR, L=Dijon, O=Education Nationale, OU=0002 110043015, CN=aca-xubuntu.ac-test.fr"
    right = %any
    rightsourceip = 10.1.2.99
    rightdns = 10.1.2.1
    auto=add
#FIN:etb1.amon-default-2.5.1-aca-xubuntu_1-RW_tunnel
```

Côté poste roadwarrior (exemples de commandes sur Ubuntu >= 14.04):

- installer strongSwan (version 5.0.x mini). La configuration de base suffit.
- désactiver le lancement automatique de strongSwan :

```
[ ! -f /etc/init/strongswan.override ] && echo "manual" > /etc/init/strongswan.override
```

Le lancement du VPN se fera manuellement
Sur un poste xubuntu 15.04, il a fallu modifier la configuration apparmor :

- **/etc/apparmor.d/usr.lib.ipsec.stroke** :
ajouter

```
  /var/run/charon.ctl           rw,
```

- **apparmor_parser -r /etc/apparmor.d/usr.lib.ipsec.stroke** pour prendre en compte la modification.

- **ipsec.secrets**

```
#DEB:/C=FR/L=Dijon/O=Education Nationale/OU=0002 110043015/CN=aca-xubuntu.ac-test.fr
: RSA "privaca-xubuntu.ac-test.fr.pem" %prompt
#FIN:/C=FR/L=Dijon/O=Education Nationale/OU=0002 110043015/CN=aca-xubuntu.ac-test.fr
```

Le **%prompt** permet de saisir la passphrase de la clé chiffrée de manière interactive.

- modèle de connexion ipsec roadwarrior (fichier ipsec.conf complet) :

```
#configuration is in ipsec.conf file
config setup
    uniqueids = yes
    cachecrls = yes
    strictcrlpolicy = no

conn %default
    keyingtries = 3
    keyexchange = ike
    authby = pubkey
    dpdaction = restart
    dpddelay = 120s
    ike = aes128-sha256-modp2048,aes192-sha384-modp3072
    esp = aes128gcm128,aes192gcm128
    forceencaps = no
    mobike = no

#DEB:aca-xubuntu-etb1.amon-default-2.5.1_1-RW_tunnel
conn "aca-xubuntu-etb1.amon-default-2.5.1_1-RW_tunnel"
    leftid = "C=FR, L=Dijon, O=Education Nationale, OU=0002 110043015, CN=aca-xubuntu.ac-test.fr"
    leftcert = "aca-xubuntu.ac-test.fr.pem"
    leftsourceip = %config
    leftdns = %config
    rightid = "C=FR, L=Dijon, O=Education Nationale, OU=0002 110043015, CN=amon.ac-test.fr"
    right = 192.168.0.31
    rightsubnet = "10.1.2.0/24"
    auto=start
#FIN:aca-xubuntu-etb1.amon-default-2.5.1_1-RW_tunnel
```

- montage du VPN :

```
root@pc:~# service strongswan start
root@pc:~# ipsec rereadall
Private key '/etc/ipsec.d/private/privaca-xubuntu.ac-test.fr.pem' is encrypted.
Passphrase: ****************
root@pc:~# ipsec reload
Reloading strongSwan IPsec configuration...
```

#4 - 10/13/2015 09:42 AM - Fabrice Barconnière

- Remaining (hours) changed from 4.0 to 0.0

#5 - 10/13/2015 09:46 AM - Scrum Master

- Status changed from En cours to Résolu

#6 - 10/30/2015 10:48 AM - Daniel Dehennin

- Status changed from Résolu to Fermé