Agence Nationale
de la Sécurité des
Systèmes d'Information

Mémo : Administration en ligne de commande d'une passerelle Clip

Mots-clés : configuration, passerelle, ligne de commande, CRL

Table des matières

~~DIFFUSION LIMITÉE~~

1 Pré-requis

Liste des pré-requis :

- une passerelle Clip installé ;
- un accès SSH aux cages « AUDIT » et « ADMIN » (optionnel).

2 Configuration du réseau

Une seconde partie de la configuration réseau est située dans le répertoire « conf/netconf.d ». Chaque sous-répertoire de ce chemin représente une arborescence de « profil réseau ».

Le profil nommé « default » est le seul profil dont la présence est obligatoire. Il s'agit du profil qui est chargé par le système lors du démarrage.

Ce profil est la base du système d'héritage : pour chaque profil nouvellement crée, il est possible d'hériter (c'est à dire de recopier automatiquement) un ensemble de variables du profil par défaut. Cet héritage est basé dans la pratique sur un ensemble de liens symboliques. Chaque fichier d'un profil réseau qui est hérité est, en réalité, un lien symbolique vers le fichier régulier de même nom du profil par défaut.

Dans la pratique, tous les média d'installation Clip ne disposent pas d'un système de fichiers supportant les liens symboliques (FAT en est un bon exemple). Pour parer à cette limitation, il est possible d'ajouter dans le répertoire « conf/netconf.d » du profil d'installation, une archive au format "tar" contenant un ou plusieurs profils réseaux. En effet, ce format d'archive est capable de contenir des liens symboliques et pourra les restituer lors l'installation de Clip.

Listing 1 – Listes des fichiers d'un profil réseau

```
netconf.d
+-- * [need at least a "default" profile]
    +-- admin [vpn]
    +-- hostname
    +-- hosts
    +-- net
    +-- ipsec
    +-- ipsec.* [vpn]
    +-- netfilter
    +-- resolv.conf
    +-- umts
    +-- wireless
```

Le Listing 1 fournit la liste des fichiers qui composent un profil réseau. Ceux-ci remplissent les rôles suivants :

- *hostname* : le nom d'hôte de la machine ;
- *hosts* : il s'agit du fichier « /etc/hosts » qui sera utilisé sur le « socle » ; il est notamment visible depuis les cages « UPDATE », « ADMIN » et « AUDIT » et permet, par exemple, de définir un nom de domaine pour le miroir de mise à jour si aucun DNS n'est disponible ;
- *net* (illustré Listing 2) : renseigné les adresses IP assignées aux interfaces réseaux, les routes supplémentaires et l'utilisation de NATT.
  - *USE_NATT* : utilisation du NAT-Traversal (port 4500) ;
  - *ETHX_ADDR*, *ETHX_MASK* et *ETHX_MTU* (où X prend la valeur de 0 à 2) permet de configurer respectivement les adresses IP, masque sous-réseau et MTU du lien de chaque interface. L'interface *ETH0* est connectée au réseau externe, l'interface *ETH1* est connectée au réseau interne et l'interface *ETH2* est connectée au réseau d'administration ;
  - *UPDATE_GW* : l'adresse de la passerelle IPsec avec laquelle monter le tunnel « UPDATE » (mise à jour) entre la cage *UPDATE* et une passerelle IPsec distante. Si la variable *UPDATE_NOIPSEC* a été renseignée à *yes* dans le fichier « params/conf.d/net » du profil d'installation, cette variable est ignorée ;

  - *ADMIN_GW* : comme à *UPDATE_GW*, permet de définir un tunnel IPsec depuis la cage « ADMIN » vers une passerelle distante ;
  - *AUDIT_GW* : comme à *UPDATE_GW*, permet de définir un tunnel IPsec depuis la cage « AUDIT » vers une passerelle distante. Il n'existe pas de variable *AUDIT_NOIPSEC* correspondante ;
  - *ADMIN_NETWORKS* et *ADMIN_TARGETS* identifient respectivement les réseaux clients et les IP des clients pour lesquels la fonctionnalité d'administration à distance a été activée (flux SSH depuis l'intérieur du SI vers les clients) ;
  - *CLIENT_NETWORKS* : *pool* d'adresses qui peuvent être attribués aux clients IPsec ;
  - *DOWNLOAD_LOCKED* : quand mis à *yes*, empêche la mise à jour via le réseau ;
  - *NO_NETWORK* : quand mis à *yes*, le profil devient un profil sans réseau (aucun trafic ne passe, même les flux d'administration) ;
  - *ROUTE_EXTRA* : défini des routes spécifiques ; il s'agit de couple de la forme « RESEAU :ADRESSE », séparé par un espace ;
  - *PEER_ADDR* : permet de restreindre, au niveau pare-feu, l'IP des clients qui sont autorisés à se connecter à la passerelle ;
  - *DYNAMIC_CLIENT_IPS* : alloue aux clients IPsec une adresse IP de manière dynamique depuis un *pool* d'adresse.
- *ipsec* : permet de reprendre et de surcharger les paramètes de configuration IPsec (« UPDATE_GW », « ADMIN_GW », « AUDIT_GW »), comme illustré dans le Listing 3 qui se trouvent dans le fichier « net » ;
- *netfilter* : permet de définir les autorisations dans le pare-feu. Les ports autorisés doivent être séparés par une virgule, comme illustré Listing 4 ;
- *resolv.conf* : liste des serveurs DNS utilisés par le système pour faire de la résolution de noms ; ce fichier est exposé sur les cages « AUDIT », « ADMIN » et « UPDATE » .

Listing 2 – Contenu du fichier net

```
# Note : pas de " ni ‘ dans ce fichier

# Mettre a 'yes' pour activer le support NATT
# (si une NAT est realisee entre le poste et les passerelles)
# Laisser a 'no' sinon
USE_NATT=yes

# Adresse externe
# Doit etre routable sur le reseau local.
ETH0_ADDR=192.168.1.2
ETH0_MASK=24
ETH0_MTU=1500

# Adresse interne
ETH1_ADDR=192.168.2.2
ETH1_MASK=24

# Route par defaut sur le reseau local
DEFAULT_ROUTE=192.168.1.1

# Passerelle UPDATE
UPDATE_GW=0.0.0.0

# Reseau Client
CLIENT_NETWORKS=172.16.0.0/16

# Adresse supervision/administration
ETH2_ADDR=10.0.1.2
ETH2_MASK=24

DOWNLOAD_LOCKED=yes
NO_NETWORK=
ROUTE_EXTRA=-
ADMIN_GW=
ADMIN_NETWORKS=-
ADMIN_TARGETS=-
PEER_ADDR=
DYNAMIC_CLIENT_IPS=yes
```

Listing 3 – Exemple de contenu de fichier ipsec

```
UPDATE_GW=
AUDIT_GW=
ADMIN_GW=
```

Listing 4 – Exemple de contenu de fichier netfilter

```
# NOTE : pas de " ni ' dans ce fichier
# Pas non plus de commentaires ou d'espaces en fin de ligne, pour le moment...

ILLEGAL_LOGLEV=info
ILLEGAL_LOGLIM=10/minute

## CORE : interface externe ##
# Services autorises : IKE + NATT
ETH0_OUT_TCP=-
ETH0_OUT_UDP=-
ETH0_OUT_SAME_UDP=500,4500
ETH0_OUT_SAME_TCP=-
ETH0_IN_TCP=-
ETH0_IN_UDP=500,4500
ETH0_IN_SAME_TCP=-
ETH0_IN_SAME_UDP=500,4500
ETH0_DEST=0.0.0.0/0

## CORE : interface interne ##
ETH1_OUT_TCP=-
ETH1_OUT_UDP=-
ETH1_OUT_SAME_TCP=-
ETH1_OUT_SAME_UDP=-
ETH1_DEST=0.0.0.0/0

## UPDATE ##
# Services autorises : HTTPS
UPDATE_OUT_TCP=443
UPDATE_OUT_UDP=-
UPDATE_OUT_SAME_TCP=-
UPDATE_OUT_SAME_UDP=-
UPDATE_DEST=0.0.0.0/0

## FORWARD ##
# Premier paquet eth0 -> eth1
# Services autorises : stunnel-http[12090],stunnel-imap[12143],stunnel-smtp[12025],stunnel-activesync[12073],
    stunnel-caldav[14000],stunnel-addrbook[14001]
FWD_IN_TCP=12180,12150,12110,12143,12025,9999,8888,8889
FWD_IN_UDP=-
FWD_IN_SAME_TCP=-
FWD_IN_SAME_UDP=-
```

Les fichiers suivants ne sont pas utilisés sur un profil passerelle :

- *utms*
- *wireless*

3 Application des mises à jour

3.1 Configuration de la mise à jour par le réseau

La mise à jour distante passe obligatoirement par le protocole HTTPS. Cela implique que les autorités de certifications du ou des serveurs contenant les mises à jour doivent être présentes sur le poste. Celles-ci se trouvent dans le répertoire « /etc/admin/clip_download/cacerts ». Il ne suffit pas seulement de déposer les autorités de certification, il faut également que celles-ci soient accessibles (droit de lecture pour tous) et exécuter la command « c_rehash » avec comme argument le répertoire contenant les certificats de mise à jour, afin de créér des liens symboliques nécessaire au bon fonctionnement du système de mise à jour (APT). Le Listing 5 illustre un fichier « /etc/admin/-clip_download/sources.list » tel qu'il peut être vu depuis une cage « ADMIN ».

Listing 5 – Exemple de fichier conf/clip_download/sources.list.clip

```
deb      https://clip.miroir:39999/update-v1/mac-@ETH0@/name-@HOSTNAME@/clip-gtw-dpkg/clip/clip-core-conf clip
    main
deb      https://clip.miroir:39999/update-v1/mac-@ETH0@/name-@HOSTNAME@/clip-gtw-dpkg/clip/clip-apps-conf clip
    main

deb      copy:///mnt/usb/mirrors/clip-gtw-dpkg/clip/clip-core-conf clip main
deb      copy:///mnt/usb/mirrors/clip-gtw-dpkg/clip/clip-apps-conf clip main
```

L'authentification du client (ici la passerelle CLIP) est activée dès lors qu'un certificat et une clé privée sont déposés respectivement aux chemins « /etc/admin/clip_download/private/apt.cert.pem » et « /etc/admin/clip_download/apt.key.pem » de la cage « ADMIN ».

3.2 Forcer le téléchargement immédiat d'une mise à jour

Le système de mise à jour recherche automatiquement des mises à jour toutes les heures. Il est possible de forcer une mise à jour en utilisant la commande « downloadrequest » (comme illustré Listing 6). La commande peut mettre quelques secondes à être exécutée, et indique si le téléchargement de la mise à jour s'est bien déroulé.

Listing 6 – Commande permettant de forcer la mise à jour du système depuis un terminal « ADMIN »

```
downloadrequest launch clip
```

L'application de la mise à jour nécessitera un redémarrage et donc une coupure du service.

3.3 Mise à jour des listes de révocations

La passerelle CLIP peut prendre en compte des *Certificate Revocation Lists* (CRLs) pour la partie IPsec. Celles-ci doivent se trouver dans le répertoire « /etc/admin/ike2/crl » de la cage « ADMIN ». La ou les CRLs doivent être au format PEM. Si le nom n'a pas d'importance, il faut bien faire attention aux droits associés au fichier : ses permissions doivent permettre la lecture pour les « autres » (les fichiers CRLs étant lus par l'utilisateur *racoon* associé au démon *strongswan*). La prise en compte se fait lorsqu'une nouvelle CRL est déposée dans le répertoire.

La méthode la plus simple pour mettre à jour les CRLs consiste à les *pousser* par SSH.

3.4 Redémarrage à distance

À noter l'appuie sur le bouton power n'a aucun effet, et en particulier ne provoque pas l'extinction du système. Ainsi, si un reboot local et en aveugle est envisagé, il faut connecter un clavier, aller sur le premier terminal virtuel (appuie « Ctrl+Alt+F1 ») et envoyer la séquence clavier « Ctrl+Alt+Suppr. ».

À venir. Depuis la cage « ADMIN », il est possible d'utiliser la commande « clip-device-request » pour effectuer un arrêt ou redémarrage du système (comme illustré dans le Listing 7).

Listing 7 – Exemple d'utilisation de la commande « clip-device-request »

```
clip-device-request -p h # arrêt du système
clip-device-request -p r # rédémarrage du système
clip-device-request -p s # mise en veille du système (si supporté)
```