Agence Nationale
de la Sécurité des
Systèmes d'Information

Mémo : Guide d'utilisation d'une passerelle Clip

Mots-clés : utilisation, administration, premiers pas, passerelle

Table des matières

~~DIFFUSION LIMITÉE~~

1 Pré-requis

Liste des pré-requis :

- Passerelle CLIP installée ;
- Média d'insllation CLIP (optionel).

2 Utilisation standard

2.1 Démarrage du système

Le démarrage de la passerelle IPsec est une étape d'utilisation assez simple. Vérifiez bien qu'aucun média d'installation n'est inséré dans la machine pour être certain de démarrer sur le système présent sur le(s) disque(s) dur(s).

Un écran similaire à celui du Dessin 4 apparaît. Les différentes possibilités sont, dans l'ordre :

- démarrer sur la version de la passerelle la plus à jour avec le meilleur mode vidéo possible (choix par défaut) ;
- démarrer sur la version de la passerelle la plus à jour avec un mode vidéo forcé en 800x600 (en cas de problème d'affichage) ;
- démarrer sur la version de la passerelle avant la dernière mise à jour (en cas de problème majeur lors d'une mise à jour) ;
- démarrer sur la version de la passerelle avant la dernière mise à jour en mode vidéo forcé en 800x600.

Si aucune touche n'est pressée, au bout de quelques secondes le choix par défaut est validé. Notez que deux systèmes sont présents en parallèle sur la machine, ce qui permet en cas d'erreur majeure lors d'une mise à jour de revenir à une version précédente fonctionnelle en attendant que le problème soit corrigé. Dans le cas d'un démarrage sur une installation neuve, les deux versions (courante et précédente) sont bien entendu identiques.

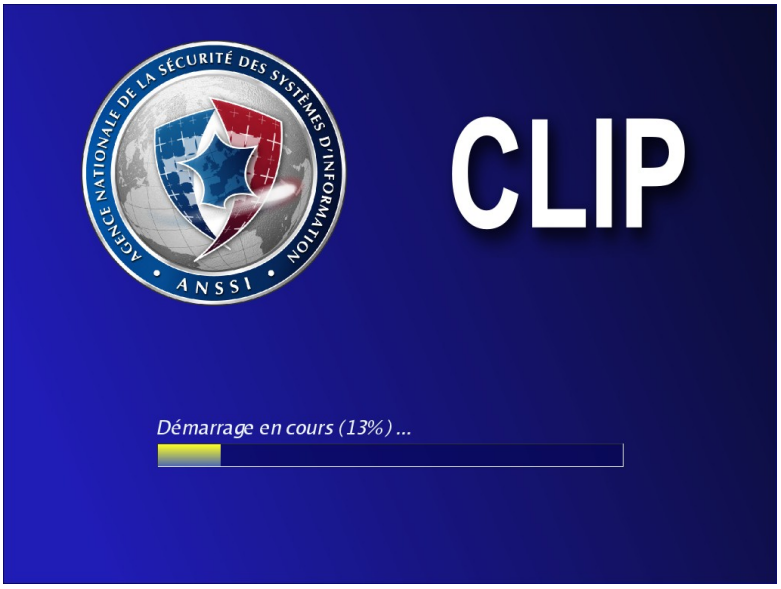

FIGURE 1 – Démarrage en cours de la passerelle IPsec

Une fois un choix validé, le démarrage va se poursuivre, symbolisé par une barre de chargement (voir Figure 1).

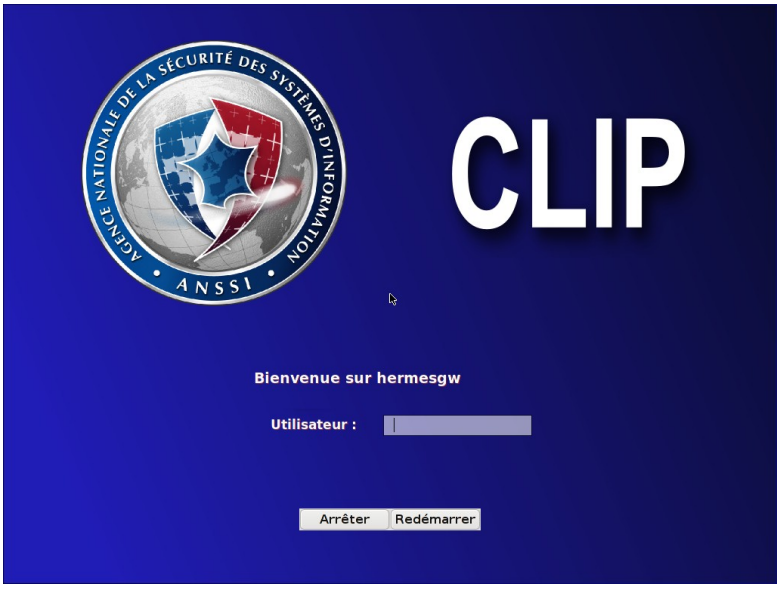

FIGURE 2 – Écran de *login* de CLIP

Le démarrage une fois achevé, l'écran de *login* s'ouvre (voir Figure 2) et vous propose d'entrer un nom d'utilisateur puis un mot de passe. Lors d'un premier démarrage, les utilisateurs disponibles sont ceux spécifiés dans le fichier du profil d'installation « `users.list` » (cf documentations sur la préparation de profil d'installation).

Figure : Écran de login de la passerelle IPsec

Entrez votre nom d'utilisateur et votre mot de passe (validez chaque étape par un appuie sur la touche « Entrée »), vous accédez maintenant à l'interface d'administration de la passerelle IPsec.

3 Utilisation avancée

3.1 Adresses virtuelles

Le fonctionnement d'IPsec (et plus précisément d'IKEv2) fait appel à une plage d'adresses virtuelles, ou adresses privées, correspondant aux adresses prises par les terminaux distants sur le réseau local. Dans le cas de la passerelle IPsec, cette plage d'adresses peut se retrouver sous la dénomination « sous-réseau des clients ».

Ces adresses ne seront vues que par les équipements d'infrastructure. Il faut donc prendre garde à ne pas créer de conflits d'adresses IP à ce niveau là en choisissant l'adressage du réseau. Il est surtout important de noter que la taille de la plage d'adresses limite directement le nombre de connexions simultanées à la passerelle, et donc le nombre de terminaux qu'il est possible de déployer. La plage choisie est divisée en deux parties égales pour les terminaux à adressage statique et dynamique. Ainsi, un sous réseau de classe B pour les adresses virtuelles (masque « `255.255.0.0` ») permettra de connecter environ 30 000 terminaux client simultanément (s'ils ne montent qu'un seul tunnel à destination de cette passerelle).

3.2 Adressage statique et dynamique

Le protocole IKE permettant l'établissement du tunnel, IPsec peut sélectionner les adresses privées des équipements d'extrémité selon deux modes : une adresse statique, définie sur le terminal et dont l'attribution est confirmée par la passerelle, ou bien une adresse attribuée dynamiquement par la passerelle parmi une plage d'IP disponibles. Pour permettre le fonctionnement selon ces deux modes,

la passerelle IPsec divise en deux parties égales la plage d'adresses IP qui lui est donnée dans sa configuration réseau. La première moitié est réservée aux clients se connectant avec un adressage statique, la seconde aux clients se connectant avec un adressage dynamique.

3.3 Changement des certificats IPsec

La modification des certificats IPsec peut se faire depuis un terminal ADMIN (disponible pour les utilisateurs disposant du rôle « admin »).

Dans le cas où il s'agit de modifier le certificat serveur ou sa clef, ces deux fichiers sont contenus dans le répertoire « `etc/admin/ike2/cert/` ». L'utilisateur *_admin* ne dispose pas des droits suffisants afin de pouvoir lire les fichiers de certificats et des clés privées (afin de ne pas pouvoir les extraire d'une passerelle en cours de fonctionnement). L'outil « `install_ccsd` » en ligne de commande permet d'injecter de nouveaux fichiers dans le répertoire de certificats. Le certificat doit être encodé au format PEM, non-chiffré. La clef doit être encodée en PEM et son éventuel mot de passe renseigné dans le fichier « `ipsec.secrets` », dans le même répertoire. À noter que l'utilisation de mot de passe ne présente aucun avantage. Attention à bien respecter ici le nom des fichiers : « `gw.pem` » pour la partie publique (certificat), « `gw.key` » pour la clef privée. Avant de procéder au remplacement de la clef privée, il est important de vérifier que celle-ci n'est pas enregistrée au format PKCS#8. Une méthode rapide pour le vérifier consiste à afficher le fichier dans un éditeur de texte. Les délimiteurs autour du bloc codant la clef doivent être « `---BEGIN RSA PRIVATE KEY---` » et « `--END RSA PRIVATE KEY---` ». Toute autre valeur (et notamment « `---BEGIN PRIVATE KEY---` ») indique que le format n'est pas celui attendu).

3.4 Modification des clefs publiques pour l'accès SSH

Voir documentation « Mise en place de l'administration à distance des passerelles Clip ».

3.5 Accès à l'ensemble du système de fichiers

3.5.1 Boot sur un média d'installation

Pour des raisons de sécurité, le système d'exploitation Clip n'autorise pas l'accès à l'ensemble du système de fichiers de la machine durant son fonctionnement. Pour les même raisons, il est également impossible de se connecter en tant qu'utilisateur *root*. Il est de plus difficile d'accéder aux partitions via un *live cédérom* standard étant donné que celles-ci sont chiffrées. Pour effectuer des modifications avancées à la passerelle IPsec (changement d'autorité de certifications, ...) il est alors nécessaire de redémarrer sur un média d'installation Clip, d'ouvrir un terminal et d'utiliser la commande :

```
# clip-disk mount all
```

Cette outil, disponible sur le média d'installation, permet de déchiffrer et monter les deux systèmes de fichiers de la passerelle (système courant et système de secours) dans les répertoires « `/clip1` » et « `/clip2` ».

Notez que tout changement par cette méthode doit être fait avec les plus extrêmes précautions et peut conduire à un dysfonctionnement de la passerelle à son redémarrage en cas de mauvaise manipulation.

Il est alors possible d'appliquer les modifications voulues à la passerelle avant de démonter les partitions via la commande :

```
# clip-disk umount all
```

Notez également que tout changement fait de cette manière doit être appliqué à la fois au système monté sur « `/clip1` » et à celui monté sur « `/clip2` ». Les système courant et de secours inversant leur rôle lors d'une mise à jour, il serait fâcheux de perdre des modifications importantes.

3.6 Modification des certificats

Le changement des certificats des autorités de certifications sur une machine installée n'est pour l'instant possible que via le média d'installation. Il est donc nécessaire de rebooter sur le média d'installation comme indiqué Section 3.5.1, puis d'effectuer les manipulations suivantes dans les répertoires « `/clip1` » et « `/clip2` ». Dans le cas où il s'agit de modifier les certificats autorités (CA), ces derniers sont contenus dans le répertoire « `etc/ike2/cert/` ». Ils doivent être insérés au format PEM, non-chiffrés. Le nom des fichiers n'a pas d'importance.

3.6.1 Modification du filtre des certificats client

Le changement des filtres des certificats sur une machine installée n'est pour l'instant possible que via une modification avancée. Il est donc nécessaire de rebooter sur le média d'installation comme indiqué Section 3.5.1, puis d'effectuer les manipulations suivantes dans les répertoires « `/clip1` » et « `/clip2` ». Le fichier de configuration IPsec contenant les filtres se trouve dans le répertoire « `etc/conf.d/` ». Modifiez-le suivant vos besoins et les instructions données en XXX avant de redémarrer la passerelle.