Démarqué en NON PROTÉGÉ
par décision n°15699/ANSSI/SDE/ST/LAM
du 18 juillet 2018

Documentation CLIP

2101a

Guide de l'utilisateur CLIP-RM

Version	Date	Auteur	Commentaires
1,4	13/11/2009	Olivier Levillain Yves-Alexis Perez	Mise à jour pour CLIP4 ! Corrections de typos, mise à jour de la procédure Wifi pour inclure la sélection de l'ESSID dans la list. Supression de la description des services de RM_H SGDN. Déplacement configuration firewall et audit vers les annexes. Ajout schéma d'architecture.
1.3.2	13/02/2009	Vincent Strubel	Prise en compte des remarques AQL (FDC18) : listing complet des fichiers de journaux, consultation des archives de journaux, et de la version CLIP.
1.3.1	11/02/2009	Vincent Strubel	Prise en compte des remarques AQL (FDC17). Ajout de la remarque 2 : utilisation d'un démarrage verbeux après une modification de configuration. Précisions dans la remarque 4.
1.3	09/02/2009	Olivier Levillain	Amélioration de l'introduction sur le démarrage du poste et mise à jour du guide suivant les modifications de *userclt*.
1.2.1	03/02/2009	Vincent Strubel	Prise en compte des remarques AQL (FDC16).
1.2	29/09/2008	Vincent Strubel	Ajout des conditions d'emploi (chapitre rédigé par EADS D&S). Renommage et renumérotation du document, pour permettre la rédaction d'autres guides pour les autres types de systèmes CLIP.
1.1	29/08/2008	Olivier Levillain	Ajout de photos décrivant le matériel
1.0	05/08/2008	Olivier Levillain	Version initiale

Table des matières

Introduction

Ce guide a pour vocation de donner les éléments indispensables à la prise en main et à la personnalisation d'un système CLIP dans une configuration multi-niveau, permettant l'accès sur un même poste à deux réseaux de sensibilités différentes de manière sécurisée (CLIP-RM). En l'absence d'agrément, le système CLIP n'est cependant pas destiné à être exploité pour traiter des niveaux de classifications différents.

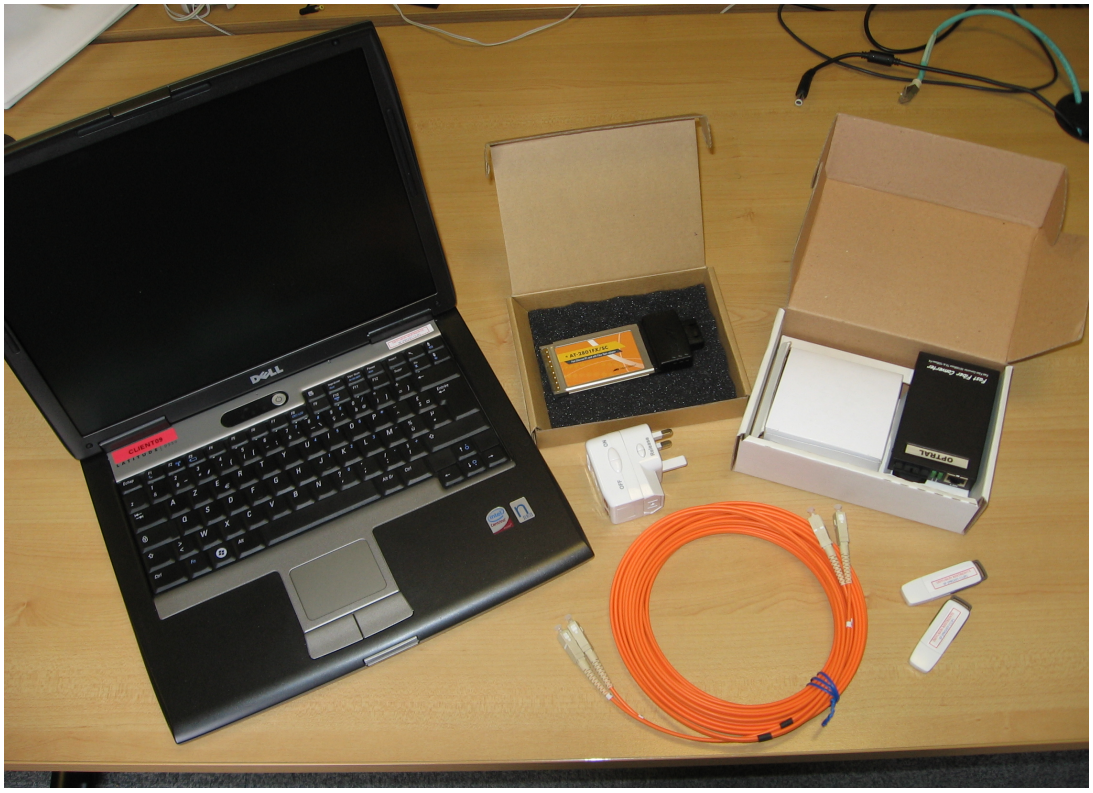
Les points abordés par le présent document sont les suivants :

- le démarrage du poste client CLIP-RM ;
- la création de comptes utilisateurs, administrateurs et auditeurs ;
- la configuration du réseau, pour pouvoir utiliser les services présents sur les deux réseaux considérés ;
- l'utilisation des différents comptes ;
- l'utilisation des supports amovibles ;
- la configuration des services sur le réseau RM_H.

1 Matériel fourni

La photo ci-dessous indique l'ensemble du matériel fourni avec un poste client CLIP standard (modèle DELL D530) :

- une carte réseau optique, qui s'insèrera dans le port PCMCIA ;
- un convertisseur réseau optique / réseau cuivre (boîtier noir à droite de la photo) ;
- une fibre optique ;
- un adaptateur secteur international.



Remarque 1 : présence des équipements optiques

Au départ, l'utilisation des équipements optiques était obligatoire pour faire fonctionner le poste CLIP. Depuis la version 4 du système CLIP, il est également possible d'utiliser directement l'interface cuivre (prise RJ45) ou l'interface Wifi si celle-ci a été activée dans le BIOS.

Remarque 2 : compatibilité avec d'autres équipements

Le poste CLIP standard décrit ci-dessus n'est pas la seule configuration matérielle apte à accueillir CLIP. Généralement, il est possible d'adapter CLIP à du matériel supporté par une distribution Linux standard. L'adaptation à de nouvelles plate-formes peut être discutée avec l'équipe de développement du

projet.

2 Présentation du système CLIP

CLIP-RM est un système d'exploitation sécurisé qui s'auto-protège de différents vecteurs d'attaques : les attaques par le réseau, les failles logicielles et dans une certaine mesure, l'utilisateur du poste lui-même. La version dont vous disposez sur les postes portables s'appelle CLIP-RM, pour « Réseaux de Messagerie ». Cette version permet l'accès à deux réseaux de sensibilité différentes de manière simultanée. Pour cela, l'utilisateur a à sa disposition deux environnements bureautiques isolés, chacun étant relié à un réseau différent.

Le cas d'emploi typique de votre poste est l'utilisation du réseau internet comme réseau de messagerie bas (RM_B), et un réseau à accès limité, comportant des données « Diffusion Restreinte », opéré par l'équipe projet CLIP (RM_H). Votre poste est directement connecté au réseau internet, et l'accès au réseau RM_H est réalisé à l'aide d'un VPN sécurisé au-dessus du réseau internet.

L'utilisation d'internet se fait de manière classique à travers un navigateur (Firefox) et un client de courrier électronique (Thunderbird). Ces deux applications sont également disponibles sur l'environnement RM_H, afin de pouvoir accéder à certains services (messagerie DR entre les utilisateurs de CLIP, *wiki*, gestion de tickets d'incidents[1]) à travers un VPN sécurisé. Chacun de ces deux environnements offre également une suite bureautique (OpenOffice.org), ainsi que d'autres applications optionnelles (lecteur multimédia, éditeur d'images, etc.).

Voici les principales caractéristiques du poste CLIP-RM :

- les mises à jour du poste sont automatiques, dès qu'une connexion est disponible (le poste vérifie régulièrement la présence de mises à jour sur un serveur opéré par l'équipe projet CLIP, à travers un second VPN sécurisé) ;
- le poste garantit un cloisonnement fort entre les deux environnement, RM_B et RM_H. Il est cependant possible de faire « monter » de l'information depuis la cage RM_B vers la cage RM_H à l'aide d'une diode[2];
- le poste s'auto-protège contre les attaques réseau, les vulnérabilité logicielles et certains comportements des utilisateurs. Pour cela, les utilitaires du poste ont été durcis et une démarche de défense en profondeur a été adoptée pour empêcher de nombreuses classes d'attaque, et limiter l'impact des attaques restantes ;
- une fois éteint, le poste ne contient plus de données utilisateur en clair. L'ensemble des partitions utilisateurs est chiffré à l'aide d'une clé dérivée du mot de passe de l'utilisateur. Celui-ci est ainsi à l'abri de la divulgation de ses données en cas de perte ou de vol[3];
- le poste peut être multi-utilisateur. Dans ce cas, chaque utilisateur ne voit que les partitions lui appartenant. Il est de plus possible de réaliser une séparation des rôles (administration, audit et utilisation) à l'aide de divers types d'utilisateurs. Il est à noter que les opérations

[1] Les services disponibles dans RM_H sont du ressort de l'administrateur réseau. La liste n'est qu'indicative et sera sans doute différente pour chaque déploiement de CLIP.

[2] Une application de chiffrement en coupure compatible avec ACID Cryptofiler v7 a également été développée et est déjà présente sur les postes. Elle permet la descente d'information avec chiffrement, et la montée d'archives avec déchiffrement. Cependant, elle ne sera réellement fonctionnelle que lorsque les clés ACID v7 seront déployées.

[3] Il est cependant essentiel, en cas de perte ou de vol, de prévenir au plus vite l'équipe projet CLIP, afin qu'elle puisse prendre les mesures de révocation de nécessaires.

d'administration autorisées à un opérateur sont extrêmement limitées (il s'agit essentiellement de la configuration réseau), et ne peuvent menacer que la disponibilité du poste.

Toutes ces caractéristiques permettent donc une utilisation nomade du poste CLIP de façon sereine, puisque l'utilisateur est à l'abri de la majorité des attaques possibles.

3 Démarrage du poste

Lorsque vous recevez votre poste CLIP, il se peut que sa batterie soit totalement déchargée. Il est donc conseillé de commencer par brancher le câble d'alimentation du poste avant son utilisation.

Vous pouvez à présent allumer votre poste CLIP. À sa mise sous tension, un menu de démarrage apparaît, proposant le choix entre la version courante du système, ou la version précédente. Démarrer la version précédente permet une reprise sur erreur lors de la mise à jour du système. Ce cas n'est pas décrit dans cette documentation qui se veut un guide succint. Quant à la gestion des mises à jour dans le système CLIP, elle est réalisée de manière automatique, généralement non perceptible pour l'utilisateur, qui ne constate qu'un allongement de la séquence de démarrage (avec un éventuel redémarrage) lorsque ces mises à jour ont lieu.

Nous démarrons donc la version courante du système ; c'est celle-ci qui sera sélectionnée par défaut au bout de 10 secondes. Une fois le choix effectué, le système se charge, en affichant quelques lignes de texte, puis un écran avec un indicateur de l'avancement de la procédure de démarrage. À la fin de celle-ci, un écran invite l'utilisateur à s'identifier.

4 Création des comptes utilisateurs

4.1 Les différents types de comptes

Un système CLIP connaît cinq sortes de comptes :

- les utilisateurs réels, qui auront accès à des applications de bureautique, à un navigateur Internet, et à un client de messagerie, dans deux environnement, appelés *cages RM*, l'un correspondant au niveau bas RM_B (dans notre cas, Internet), l'autre au niveau haut RM_H (typiquement, un réseau à Diffusion Restreinte) ;
- les administrateurs, responsables de la configuration nécessaire au bon fonctionnement du coeur du système (paramètres réseaux, clés cryptographiques pour les VPN) ;
- les auditeurs, qui ont accès au paramètres du poste et aux journaux systèmes, en lecture seule ;
- les utilisateurs privilégiés, qui cumulent les trois rôles précédents ;
- les utilisateurs nomades enfin, qui sont des utilisateurs ayant la possibilité de configurer les paramètres réseaux (il s'agit d'utilisateurs aux privilèges limités).

Il est essentiel de comprendre que les droits des comptes administrateurs sont extrêmement limités, puisque ceux-ci ne peuvent pas directement installer de logiciels, ni accéder aux données des autres utilisateurs sans leur mot de passe. Les seules attaques qu'un administrateur peut mener concernent la disponibilité du poste (si des paramètres réseau erronés sont entrés par exemple).

Il existe deux usages typiques d'un poste CLIP :

- poste mono-utilisateur, avec un seul utilisateur privilégié, capable de gérer lui-même les paramètres réseau et de surveiller les journaux en cas de problème ;
- poste multi-utilisateur, avec différents comptes utilisateurs, un ou plusieurs administrateurs, et un ou plusieurs auditeurs. Il est alors possible de réaliser une séparation des rôles.

En pratique, nous allons créer un compte de type « utilisateur privilégié » dans la présente section.

4.2 Généralités sur la création de comptes

À chaque compte est associé un identifiant (*login*), un type et un mot de passe. De plus, la création de chacun des comptes nécessite l'allocation d'une partie du disque dur afin de stocker les fichiers correspondant au compte. Pour les comptes de type administrateur ou auditeur, la taille de cette partition est fixée automatiquement au minimum afin de réserver un maximum d'espace disque aux comptes utilisateurs (privilégiés ou non). Pour la création de ces derniers, il faudra spécifier l'espace disque qui leur sera réservé, ainsi que la répartition entre les environnements RM_B et RM_H.

Une fois les paramètres saisis par l'administrateur pour créer un nouveau compte, l'espace disque chiffré du nouveau compte est initialisé, ce qui peut prendre un certain temps pour les partitions des utilisateurs (il faut compter environ une minute par tranche de 2 Go). Il est important de ne pas interrompre le programme durant cette phase ; dans le cas contraire, il est possible que de l'espace disque soit perdu.

Par ailleurs, les mots de passes saisis lors de la création d'un compte, ainsi que lors de la modification d'un compte existant, sont soumis à un certain nombre de contraintes :

- taille minimale de 6 caractères ;
- mot de passe suffisamment différent du nom de l'utilisateur ;
- pas de suite triviale, comme *"abcdef"* ;
- pas de mots du dictionnaire.

Les mots de passes ne respectant pas ces conditions sont rejetés par la boîte de dialogue de création ou de modification de compte, qui demande alors la saisie d'un nouveau mot de passe.

Remarque 3 : impact des erreurs dans la gestion des comptes

Une suppression de compte est irrévocable : les données utilisateur de ce compte sont définitivement perdues, sauf éventuellement pour les fichiers ayant fait l'objet de copies sur un support amovible.

De même, une erreur (double, puisque le mot de passe est demandé deux fois) dans la saisie du nouveau mot de passe lors de la modification d'un compte existant est irrévocable, entraînant la perte des données de ce compte s'il se révèle impossible de retrouver le mot de passe effectivement saisi. Dans ce cas, la seule solution consiste à faire intervenir un administrateur du socle afin de supprimer le compte, et d'en créer un nouveau du même nom.

Remarque 4 : impact de la perte du mot de passe et absence de séquestre

Le mot de passe d'un compte local est dérivé pour obtenir la clé de chiffrement des données associées à ce compte. C'est la raison pour laquelle il est demandé d'utiliser un mot de passe fort, seul gardien de la confidentialité des données une fois le poste éteint. En contrepartie, la perte de ce mot de passe rend la récupération des données impossible.

La solution CLIP n'offre à l'heure actuelle aucune fonction de séquestre de ce mot de passe ou de la clé qui en est dérivée. La gestion d'un tel séquestre, si elle est nécessaire, sera donc réalisée par l'utilisateur du poste lui-même (par exemple en recopiant le mot de passe en question sur un papier mis au coffre).

4.3 Ouverture d'une session administrateur

Après l'installation du poste, il existe un unique compte présent sur le poste. Il s'agit d'un compte administrateur du socle, nommé *config*. Nous allons voir ici comment utiliser ce compte adminsitrateur pour créer un compte de type « utilisateur privilégié ». Puis, nous supprimerons le compte *config*.

Commençons par lancer une session pour l'administrateur *config*. Pour cela, il faut entrer l'identifiant temporaire *config* et le mot de passe *config* à l'invite de bienvenue du système.

Une fois la session lancée, deux menus sont accessibles en haut à gauche de l'écran. Le menu principal (une icône représentant une cage) contient des informations sur les derniers changements, les commandes de manipulation des supports amovibles et des paramètres concernant la session (changement de mot de passe, verrouillage et fermeture). Le second menu, dont l'icône représente une clé plate, contient l'ensemble des opérations d'administration. Nous aborderons dans la présente section

la gestion des utilisateurs. La gestion du réseau fera l'objet de la section suivante. Notons enfin l'entrée du menu intitulée « Configurer la date et l'heure », qui permet de mettre l'horloge système à l'heure à travers deux boîtes de dialogue successives. D'autres opérations sont décrites dans l'annexe A.

4.4 Création d'un compte « utilisateur privilégié »

L'application « Gérer les utilisateurs », disponible dans le sous-menu « Avancé » du menu adminsitration (l'icône figurant une clé plate en haut de l'écran) permet de créer les nouveaux utilisateurs.

Lorsque l'application démarre, vous devriez obtenir une liste des comptes réduites à un utilisateur « config », de type administrateur.

Afin de créer un nouveau compte, cliquez sur « Ajouter ». Il faut ensuite remplir les différents champs contenus dans la fenêtre d'ajout. Tout d'abord, le nom du nouveau compte vous est demandé. L'identifiant peut comporter jusqu'à 8 caractères et ne doit contenir que des minuscules. On pourra par exemple choisir un identifiant à partir du prénom et du nom de l'utilisateur, comme jdupont pour Jean Dupont, ou tdlparti pour Thomas de la Particule.

Ensuite, il faut choisir le mot de passe de l'utilisateur (à saisir deux fois), puis le type d'utilisateur que nous souhaitons créer, ici « Utilisateur privilégié ». Après cela, il faut choisir la quantité totale d'espace en méga-octets que vous souhaitez allouer à l'utilisateur (pour les deux environnement, haut et bas) ; puis, sur cet espace, il vous faudra choisir la répartition de cette quantité entre les réseaux de messagerie RM_B et RM_H. Une fois l'ensemble des paramètres validés, cliquez sur « Ajouter ».

Les partitions sont alors créées, ce qui nécessite un certain temps (il faut compter une minute pour 2 Go environ) durant lequel une boîte de dialogue vous invite à patienter. Il est important de ne pas éteindre le poste ou fermer la session avant la fin de l'opération. Lorsque les partitions sont générées correctement, une boîte de dialogue vous annonce le succès de l'opération : la liste des comptes utilisateurs contient désormais deux noms dans la liste : *config* et le compte que vous venez de créer.

Nous allons terminer la configuration des comptes en supprimant le compte temporaire *config*, maintenant qu'un nouveau compte est présent. Cependant, il est impossible de supprimer le compte *config* à partir d'une session ouverte par l'utilisateur *config*. Il est donc nécessaire de se déconnecter de la session courante, à l'aide du menu fléché bleu, et de se connecter à l'aide de l'identifiant du nouveau compte et du mot de passe associé.

Ce compte ayant accès aux fonctions d'administration, le menu avec la clé plate est également présent en haut à gauche de l'environnement. Le programme « Gérer les utilisateurs » se trouve là encore dans le sous-menu « Avancé ».

Cliquez sur la ligne « config » dans la liste des comptes, puis sur le bouton « Supprimer ». Une confirmation vous est demandée.

4.5 Changement du mot de passe d'un compte

Comme indiqué plus haut, le changement de mot de passe s'effectue en cliquant sur le menu principal, en haut à gauche de l'écran, puis en choisissant l'entrée « Configuration » et « Changer de mot de passe » de ce menu. L'ancien mot de passe vous est alors demandé, ainsi que le nouveau (deux fois, pour éviter les erreurs de frappe).

5 Présentation d'une session utilisateur privilégié

Lancer une session pour un utilisateur privilégié se fait tout simplement en entrant le nom du compte correspondant et le mot de passe associé. Au moins trois boutons sont alors disposés en haut à gauche de l'écran. Le coin en haut à droite est quant à lui occupé par différents indicateurs concernant respectivement les supports amovibles USB, la connexion réseau, l'état des mises à jour du socle, la charge de la batterie, et l'horloge.

Le premier bouton en forme de cage en haut à gauche est le menu principal. Il contient :

- un sous-menu « Information » permettant de se renseigner sur les mises à jour récentes ;
- un sous-menu « Supports amovibles » concernant les clés USB (voir plus bas) ;
- un sous-menu « Configuration » permettant de changer de mot de passe et le temps d'activation du verrouillage de l'écran ;
- une option « Retirer un support USB », qui permet à l'utilisateur de demander la désactivation des supports actuellement disponibles (également accessible en cliquant sur l'indicateur des supports amovibles en haut à droite) ;
- « Verrouiller la session », qui enclenche l'économiseur d'écran, et ne permet l'accès à la machine qu'après saisie du mot de passe de l'utilisateur ;
- « Fermer la session », qui permet de revenir à l'invite de bienvenue, ou d'arrêter le poste.

Le menu d'administration, représenté par une clé plate, et le menu d'audit, représenté par une loupe, se trouvent à droite du menu principal. Les principales actions disponibles dans ces menus sont décrites dans la suite du document.

Les deux derniers boutons, RM_H en rouge, et RM_B en vert, permettent de lancer une session utilisateur dans chacune des cages. Une telle session consiste en une fenêtre occupant tout l'écran à l'exclusion de la barre de menu décrite ci-dessus. Il est possible de lancer les deux environnements en parallèle, permettant l'accès simultané à des environnements de niveaux différents.

Le système CLIP garantit le cloisonnement des informations entre ces deux environnements. De plus, afin d'éviter les confusions, la couleur des bandeaux de fenêtre définit sans ambigüité la cage RM étant en cours d'utilisation : un bandeau rouge pour RM_H, et un vert pour RM_B.

Chaque environnement correspond à un bureau avec une barre d'état en bas de l'écran. Cette barre d'état contient un bouton K, équivalent du menu Démarrer des environnements Windows pour les environnements KDE utilisés dans CLIP, ainsi que quelques raccourcis vers des applications, telles que le navigateur *Firefox* ou le client de messagerie *Thunderbird*. D'autres applications sont installées dans chacun des environnements RM_X telles que la suite *OpenOffice.org* pour l'édition de document bureautique, et sont disponibles dans le menu K.

Lorsque l'utilisateur ferme la session à l'aide du menu principal, les cages encore ouvertes sont fermées, et l'invite de bienvenue réapparaît. Cette invite de bienvenue permet, comme nous l'avons vu, de démarrer les sessions des différents comptes présents sur le poste, mais également de redémarrer ou d'arrêter la machine (avec les boutons en haut à gauche).

6 Configuration du réseau

6.1 Profils réseau

La configuration réseau du poste CLIP regroupe un certain nombre de paramètres (adresse IP, adresses de passerelles, configuration du *firewall*, etc.) qui varient d'une connexion à une autre. Afin de rendre le nomadisme plus pratique, il est possible de gérer des profils réseau regroupant ces informations pour des situations différentes.

Par défaut, il n'existe qu'un seul profil, nommé « default », qui sera pris en compte par le système. Si par la suite vous créez d'autres profils, il vous faudra indiquer au démarrage du poste quel profil activer. Un menu avec tous les profils vous est ainsi proposé lors du démarrage, et le profil « default » est choisi automatiquement au bout de quelques secondes si vous n'avez saisi aucun choix. Une fois le poste démarré, il est alors possible de changer le profil courant depuis un compte administrateur, utilisateur privilégié ou utilisateur nomade.

Ces profils se configurent depuis une session administrateur (ou utilisateur privilégié) à l'aide du programme « Configurer le réseau » du menu d'administration. La première ligne de la fenêtre contient une liste des profils existants, un bouton « + » pour ajouter un nouveau profil, un bouton « - » pour supprimer le profil sélectionné[4], un bouton « Activer » pour activer le profil sélectionné et un bouton « Sauver » pour enregistrer les modifications effectuées au profil en cours d'édition.

En dessous de cette première ligne se trouvent un certain nombre d'onglets (« Socle », « Wifi », « RM_H » et « RM_B »). Des onglets supplémentaires peuvent également être affichés en cochant la case « Mode avancé ». Le contenu de ces onglets seront abordés dans l'annexe A.

6.2 Configuration de l'accès à Internet

6.2.1 Choix de l'interface

Le système d'exploitation CLIP peut utiliser différents types d'interfaces réseau pour se connecter à Internet : une carte réseau optique, une carte réseau cuivre (prise RJ 45), une interface sans fil (Wifi) ou une carte 3G, sous certaines hypothèses matérielles.

Si la carte optique fournie avec le poste est enclenchée dans le port PCMCIA, elle masquera la carte réseau cuivre. Ensuite, le dispositif utilisé dépend du profil activé : l'onglet « Interface » vous permet de choisir entre une interface filaire, une interface Wifi ou un accès téléphonique 3G.

Remarque 5 : Absence de l'onglet « Wifi »

Il est possible que l'onglet « Wifi » ne soit pas visible sur votre poste CLIP. Cela signifie, soit que le poste que vous utilisez ne contient pas de carte Wifi, soit que cette carte n'est pas activée dans le BIOS, soit enfin que la carte n'est pas reconnue par le système CLIP.

[4] Le profil « default » étant le profil particulier activé par défaut, il ne peut pas être supprimé.

Si l'interface utilisée est l'interface sans fil, il vous faut ensuite entrer les paramètres de votre point d'accès Wifi. La démarche complète est la suivante :

- Cocher la case « Utiliser l'interface Wifi » dans l'onglet « Interface », puis passez à l'onglet « Wifi » ;
- Cliquer sur le bouton « Choisir un identifiant parmi les réseaux actifs » ou bien entrer manuellement le nom du réseau sans fil auquel il faut se connecter dans le champ « ESSID » ;
- Choisir la méthode de chiffrement (« Aucun », « WEP » ou « WPA »), et le cas échéant, saisir le mot de passe ou la clé dans le champ « Clé ».

6.2.2 Paramètres réseau du socle

Il faut à présent entrer les paramètres réseau du socle, en choisissant l'onglet du même nom. Deux cas de figure peuvent se présenter :

- l'adresse IP est attribuée automatiquement par le routeur, le modem ADSL ou le point d'accès. Il faut alors choisir l'option « DHCP » ;
- l'adresse IP est à saisir manuellement et vous a été remise par l'administrateur du réseau. Dans ce cas, choisissez l'option « Manuel » et entrez les paramètres suivants :
  - l'adresse IP (il s'agit de 4 nombres entre 0 et 255 séparés par des points), à saisir dans les 4 premiers champ de l'adresse IP,
  - le masque de sous réseau. Il vaut généralement 255.255.255.0[5] si on ne vous l'a pas indiqué. Dans ce cas il faut entrer « 24 » dans le dernier champ de l'adresse IP (après le « / »),
  - l'adresse IP de la passerelle par défaut, à saisir dans le champ « Passerelle par défaut ».

Remarque 6 : Désactivation de l'onglet « Socle » dans le cas d'une interface 3G

L'utilisation d'une interface 3G implique l'obtention automatique d'une adresse IP. Il est dès lors impossible de spécifier celle-ci de manière manuelle.

6.2.3 Configuration des DNS

Il reste deux onglets à décrire, qui concernent la résolution de nom de domaine dans les cages RM_H et RM_B. La résolution de nom consiste en l'association d'une adresse IP à un nom de domaine (de la forme « www.ssi.gouv.fr »).

En ce qui concerne RM_H, les adresses vous seront donnés par l'administrateur du réseau correspondant.

Pour l'onglet RM_B, la situation dépend de votre connexion Internet, car RM_B est relié directement à Internet. Si vous avez choisi DHCP plus haut, l'adresse des serveurs DNS pour RM_B sera envoyée automatiquement au poste lors de l'attribution de votre adresse IP. Dans le cas manuel, il vous faudra saisir le (ou les) serveur(s) DNS dont l'adresse vous aura été fournie avec le reste des paramètres réseau.

[5] Si le masque de sous-réseau vaut 255.255.0.0, il faut saisir 16. S'il vaut 255.0.0.0, il faut saisir 8. Pour tout autre valeur, contactez votre administrateur pour qu'il vous indique comment faire la conversion entre le masque de sous-réseau et le nombre à placer derrière le « / ».

7 Utilisation des clés USB

Nous allons décrire ici la gestion d'une clé USB sur un système CLIP. Il existe différents niveaux pour les supports amovibles : les niveaux RM_B et RM_H pour les utilisateurs réels, le niveau CLIP pour les administrateurs et auditeurs du socle, ainsi que pour les mises à jour. Il existe plusieurs types de supports USB que nous allons détaillés ici.

7.1 Les supports standards

Les clés USB standards peuvent être utilisées sous CLIP. En les branchant au cours d'une session, vous obtenez une boîte de dialogue qui vous propose de monter le support dans un des environnements disponibles. Pour un utilisateur privilégié, il vous sera possible de choisir entre :

- RM_B, en lecture / écriture[6] ;
- RM_H, en lecture seule ;
- différents emplacement du socle en lecture seule (la cage ADMIN pour importer des paramètres de configuration, la cage AUDIT ou la cage UPDATE pour effectuer des mises à jour depuis ce support).

Lorsque vous souhaitez débrancher le périphérique, il vous faut cliquer sur l'icône représentant une clé USB en haut à droite de l'écran. Il vous faut alors choisir quel périphérique vous souhaitez débrancher (en effet, vous pouvez brancher simultanément un périphérique à chacun des emplacements énumérés ci-dessus).

7.2 Les supports associés à un niveau

L'autre grande famille de supports amovibles est celle des supports associés à un niveau donné (parmi RM_B, RM_H et CLIP). Une fois initialisé, un tel support est également associé à un utilisateur et à un poste CLIP. Ce cloisonnement des supports amovibles, assuré par le système CLIP, prolonge le cloisonnement des environnements RM_H et RM_B pour l'utilisateur final.

L'utilisation des supports amovibles se fait à l'aide d'un menu contenant quatre options décrites en détails ci-dessous. En réalité, il existe un menu par niveau, dans le choix « Supports amovibles » du menu principal : un pour le niveau CLIP, un pour RM_H et un pour RM_B. Les quatre sous-menus composant ces menus sont les mêmes, et ont les noms suivants :

- « Initialiser un support USB chiffré » ;
- « Initialiser un support USB non chiffré » ;
- « Générer les clés cryptographiques » ;
- « Exporter les clés cryptographiques ».

[6] Les possibilités de montage (lecture seule ou lecture / écriture) dans les différents environnement peuvent différer d'un déploiement à l'autre. Nous donnons ici la configuration par défaut.

7.2.1 Création du matériel cryptographique nécessaire

Avant de pouvoir créer des supports pour un niveau et un utilisateur donné, il est nécessaire d'initialiser les clés cryptographiques associées. C'est le rôle de l'entrée « Générer les clés cryptographiques ». Ces clés permettent le chiffrement des informations (cas des supports chiffrés), et la signature du support (cas de tous les supports associés). Il faut un jeu de clés cryptographique différent pour chaque compte et pour chaque niveau (RM_H, RM_B, CLIP).

La procédure de génération demande un mot de passe (avec double saisie). Ce mot de passe sera nécessaire lors de la création d'un nouveau support, ainsi que pour le montage d'un support chiffré.

Si des clés existent déjà, l'option « Générer les clés cryptographiques » demandera confirmation avant d'écraser les clés existantes par une re-génération. En effet, si les clés cryptogaphiques sont écrasées, il ne sera plus possible de monter un support amovible initialisé avec les anciennes clés, et les données des supports chiffrés seront perdues, à moins d'avoir au préalable exportées les anciennes clés cryptographiques à l'aide de la fonction « Exporter les clés cryptographiques » (voir plus loin).

7.2.2 Détails de l'utilisation d'un support amovible

Les fonction « Initialiser une clé USB » d'un niveau donné permet de formater un support amovible et de le rendre utilisable au niveau considéré pour l'utilisateur qui lance la commande. Pour cela, il faut brancher le support sur un des ports USB du poste CLIP, et cliquer sur le bouton « Initialiser une clé USB ». Le mot de passe correspondant à la clé cryptographique de l'utilisateur et du niveau considéré sera alors demandé.

Par la suite, le branchement de cette clé provoquera l'ouverture d'une boîte de dialogue invitant l'utilisateur à monter la clé à l'endroit adéquat (en fonction de son niveau). La clé aparaîtra :

- dans le répertoire */mnt/usb* de la cage RM_B si le niveau de la clé est RM_B ; ce répertoire est accessible par un raccourci sur le bureau de l'environnement RM_B ;
- dans le répertoire */mnt/usb* de la cage RM_H si le niveau de la clé est RM_H ; là aussi, le répertoire est accessible par un raccourci sur le bureau de l'environnement RM_H ;
- dans le répertoire */mnt/usb* du socle, accessible dans les consoles d'administration et d'audit du socle.

Lorsque le support n'est plus utilisé, il faut le démonter, afin de pouvoir le retirer en toute sécurité. Pour cela, il faut cliquer sur l'icône représentant une clé USB en haut à droite de l'écran, et confirmer le démontage du support au niveau considéré.

7.2.3 Utilisation des supports associés sur d'autres postes

Un support USB non chiffré pourra être utilisé tel quel sur tout autre poste informatique qu'un poste CLIP. Il est donc du ressort de l'utilisateur de vérifier qu'il branche son support sur un poste de niveau adéquat.

Le cas des supports USB chiffrés est différent. En effet, leur déchiffrement implique la connaissance des clés cryptographiques du niveau considéré. Il est donc nécessaire de suivre la démarche suivante :

- exporter les clés cryptographiques sur une clé standard (à l'aide du sous-menu de même nom

dans le menu « Supports Amovibles » du niveau considéré ;

- installer les clés cryptographiques sur le poste non CLIP ;
- installer les outils de montage des supports USB chiffrés CLIP sur le poste non CLIP ;
- monter la clé chiffrée en utilisant les outils et les clés cryptographiques précédemment installés.

A l'heure actuelle, des scripts existent pour des systèmes Linux. Les outils équivalents sous Windows n'ont pas été mis à jour lors de la modification du format des supports USB survenue dans la version 4 de CLIP.

8 Diode

Un système de diode montante permet de transférer des fichiers du niveau bas vers le niveau haut. Un utilisateur peut donc faire passer des fichiers de RM_B vers RM_H. L'inverse n'est pas possible, ni le passage d'information d'un utilisateur à un autre.

Pour utiliser la diode, on se place dans la cage RM_B et on lance l'utilitaire, via son entrée dans le menu KDE « Client diode niveau bas ». On peut alors choisir le fichier à exporter (via le bouton [+]), puis on confirme l'export via le bouton « Exporter » (ou bien « Exporter et quitter » si l'on ne souhaite exporter qu'un seul fichier et fermer directement la fenêtre). Une alternative est de cliquer avec le bouton droit sur le fichier à exporter, puis de choisir « Action » et « Importer dans la diode » pour afficher la fenêtre de la diode côté bas.

On se place ensuite dans la cage RM_H pour lancer l'utilitaire homologue via l'entrée de menu « Client diode niveau haut ». La liste des fichiers disponibles est affichée dans la partie haute, et il faut alors choisir le répertoire de destination (via le bouton [+]), où seront déposés les fichiers sélectionnés. On confirme l'import via le bouton « Importer » (ou bien « Importer et quitter » si c'est le dernier fichier).

Annexe A Admin

Cette annexe donne plus d'informations sur certaines opérations d'administration non décrites dans le corps du document.

A.1 Configuration du pare-feu du socle

Si l'administrateur du socle souhaite autoriser ou interdire certains flux réseaux pour l'environnement RM_B, il est possible de le faire en se connectant comme administrateur du socle ou utilisateur privilégié.

Lorsque l'utilisateur privilégié est connecté il a accès via le menu « clé plate » à l'option « Configurer le réseau ». En passant en mode avancé (via la case à cocher prévue à cet effet), de nouveaux onglets deviennent disponibles, et en particulier les onglets « Flux du socle », « Flux des MàJ », « Flux de RM_B » et « Flux de RM_H ». Ces différents onglets correspondent à la configuration du pare-feu des différentes cages.

Pour chacun des protocoles (*TCP* et *UDP*), on peut ajouter des ports à autoriser de deux façon :

•sans condition ;

•à condition que les ports *source* et *destination* soient identiques.

Supposons que la navigation Internet pour RM_B se fasse à travers un *proxy* pour les protocoles HTTP et HTTPS, et que ce *proxy* soit à l'écoute sur le port TCP 8080. Nous devons alors interdire les ports TCP 80 et 443 (correspondants aux connexions directes pour HTTP et HTTPS) et autoriser le port TCP 8080 à la place. Dans l'onglet « Flux de RM_B », on choisit alors le protocole *TCP* et on s'occupe de la première ligne (le port de destination n'est pas forcément identique au port source). On retire (en sélectionnant, puis à l'aide du bouton [-]) les ports 80 et 443, puis on ajoute (en tapant le numéro dans la case, puis à l'aide du bouton [+]) le port 8080.

Pour que la nouvelle configuration du pare-feu soit fonctionnelle, il est nécessaire, comme pour les paramètres réseau décrits plus haut, de réactiver le profil réseau (ou de redémarrer le poste).

A.2 Configuration de la rotation des journaux

Les fichiers de journaux consultables par l'administrateur local font l'objet d'une "rotation" au démarrage du système : pour chaque fichier de journaux */log/<fichier>* dépassant une certaine taille limite, le fichier est archivé (compressé) dans */log/keep* et un nouveau fichier */log/<fichier>* vide est créé. Un certain nombre d'archives est conservé pour chaque fichier dans */log/keep*, chaque archive étant numérotée en fonction de son ancienneté : *<fichier>.gz.1* désigne l'archive la plus récente, *<fichier>.gz.2* la deuxième plus récente, et ainsi de suite. Le nombre d'archives étant limité pour chaque fichier, l'archive la plus ancienne est supprimée au besoin lors de la création d'une nouvelle archive.

Deux paramètres de cette rotation sont modifiables par l'administrateur du socle CLIP : la taille limite au delà de laquelle les fichiers sont archivés au démarrage, et le nombre d'archives à conserver pour chaque fichier. Ces deux paramètres sont modifiables à travers le menu administration, « Gestion de l'audit », « Configurer l'archivage des journaux » :

- *« Nombre d'archives »* : définit le nombre maximum d'archives qui peuvent être conservées simultanément pour un même fichier de journaux. Cette variable peut prendre pour valeur un nombre compris entre 5 et 99. La valeur par défaut à l'installation est de 6, tandis que la valeur par défaut appliquée en cas d'erreur dans les paramètres est 5.
- « Taille maximale » : définit la taille limite (inférieure) en kilo-octets des fichiers déclenchant leur archivage au démarrage du système. Cette variable peut prendre pour valeur un nombre compris entre 1 et 99 999. La valeur par défaut est 20.

Lorsque l'une de ces variables est définie de manière incorrecte (valeur hors de la plage autorisée, ou erreur de syntaxe), l'erreur est signalée au démarrage, et la valeur par défaut est utilisée. Par construction, une modification de ces valeurs n'est prise en compte qu'au démarrage suivant.

Remarque 7 : impact d'une erreur de configuration de la rotation de journaux

Une erreur de configuration de la rotation de journaux peut entraîner une suppression trop fréquente des journaux, par rapport à la périodicité de consultation de ces derniers par l'auditeur du socle, ou au contraire la conservation de trop de fichiers de journaux, risquant d'entraîner une saturation de la partition de journaux.

Annexe B Audit

La connexion à la console d'audit du socle se fait de manière similaire à la connexion à la console d'administration du socle : en donnant le nom du compte auditeur et le mot de passe associé.

Il est aussi possible d'accéder aux journaux à partir de la session d'un *utilisateur privilegié*. Le menu « Loupe » permet d'accéder aux fonctions d'audit.

A partir de là, il est possible d'accéder en lecture seule aux paramètres d'administration décrits en Error: Reference source not found et Error: Reference source not found, afin d'auditer la configuration du socle. Ceux-ci sont disponibles au même emplacement que pour l'administration, dans des sous-répertoires du répertoire */etc*.

Les journaux sont répartis entre plusieurs fichiers prédéfinis de */log*, en fonction du type d'événement auquel ils se rapportent et de leur origine. Certains sont accessibles par des liens du menu audit, à travers le sous-menu « Journaux CLIP » (nom donné entre parenthèses) . Ces fichiers sont les suivants :

- *audit.log* : journaux du sous-système d'audit du noyau, non utilisé à ce jour.
- *auth.log* (Journaux d'authentification) : journaux des actions d'authentification, contenant notamment les succès et échecs des traitements par les modules PAM *pam_tcb* et *pam_exec_pwd*, ainsi que ceux des démons *sshd* des cages $ADMIN_{clip}$ et $AUDIT_{clip}$, et du démon *pwcheckd* utilisé pour déverrouiller les sessions graphiques dans $USER_{clip}$.
- *clsm.log* (Violations CLIP-LSM) : journaux du LSM CLIP, issus du noyau et identifiés par leur préfixe *"CLSM:"*.
- *cron.log* (Journaux des tâches périodiques) : journaux du démon *cron* de $UPDATE_{clip}$.
- *daemon.log* (Journaux des démons CLIP) : journaux des différents démons du système, notamment :
  - *iked* et *spmd* : établissement et expiration d'associations et de politiques de sécurité IPsec, erreurs de négociation IKEv2.
  - *pwcheckd* : authentifications ou échecs d'authentification des utilisateurs.
  - *xdm* : ouvertures et fermetures de sessions.
  - *usbadmin_*, useradmin*, databackupd, backupd* et *mdadmd* : journaux des erreurs de traitement.
- *debug* : journaux utilisateur de niveau de priorité *debug.*
- *fw.log* (Journaux du pare-feu) : journaux des paquets rejetés par le pare-feu réseau local
- *grsec.log* (Journaux GRsecurity) : journaux *Grsecurity*, hors opérations de montage.
- *grsec_mount.log* (Journaux des montages) : journaux *Grsecurity* des opérations de montage et de démontage VFS.
- *kern.log* : ensemble des journaux du noyau.
- *mail.log* : journaux d'un éventuel serveur de *mail* local. Non utilisé à ce stade.
- *messages* (Journaux divers CLIP) : journaux divers du système, notamment :

  - opérations de téléchargement réussies ou échouées dans UPDATE$_{clip}$ (journaux *clip-download*).
  - opérations de mise à jour des paquetages primaires et secondaires de la distribution CLIP (respectivement dans le socle et dans UPDATE$_{clip}$).
  - journaux des commandes lancées à l'ouverture et à la fermeture de session utilisateur par *pam_exec_pwd*.
- *pax.log* (Violations PaX) : journaux des violations PaX.
- *ssp.log* (Viloations Propolice CLIP) : journaux des violations SSP dans le socle et les cages CLIP uniquement.
- *syslog* : journaux internes de *syslog* (non utilisé à ce stade).
- *user.log* (Journaux d'utilisation) : journaux de la *facility syslog "user"*, en particulier ceux des scripts *hotplug* associés à la gestion de supports amovibles sécurisés.
- *veriexec.log* : journaux *veriexec*
- *vserver.log* (Journaux Vserver) : journaux *vserver* (avertissements concernant notamment les opérations bloquées par *vserver*)

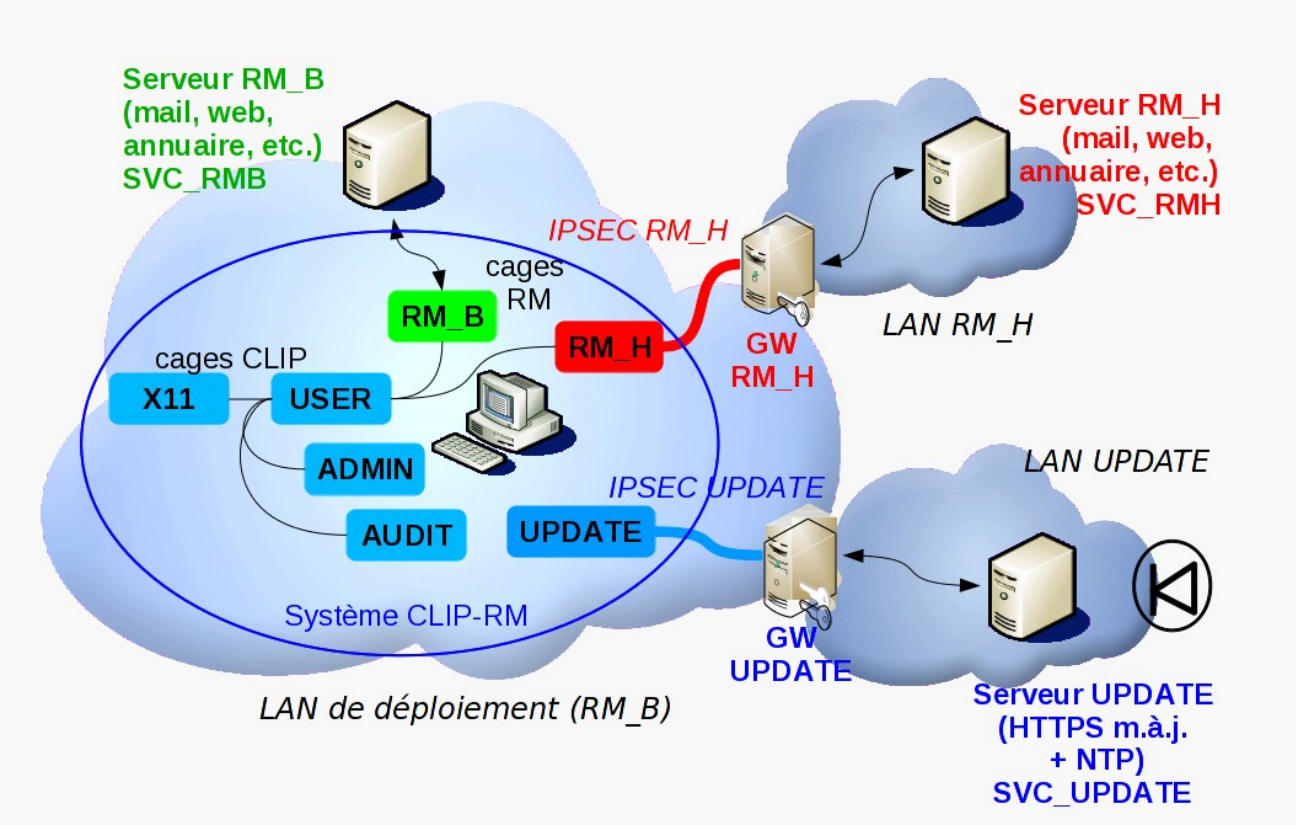
S'y ajoutent pour chaque cage RM *rm_X*, dont certains sont présents dans les sous-menus « Journaux RM_H » et « Journaux RM_B » du menu audit (leur intitulé est donné entre parenthèses) :

- *rm_X_auth.log* : journaux d'authentification au sein de la cage RM_X, contenant principalement les authentifications réussies ou échouées vis-à-vis du démon *sshd* de la vue ADMIN de la cage.
- rm_X_cron.log (Journaux des tâches périodiques RM_X) : journaux du démon crond de la vue UPDATE de la cage.
- rm_X_daemon.log (Journaux des démons RM_X) : journaux des autres démons de la cage, composés principalement des messages d'ouverture de session du démon jailmaster.
- rm_X_messages.log (Journaux divers RM_X) : autres journaux de la cage, notamment ceux des mises à jour de la cage.
- *rm_X_ssp.log* (Violations Propolice dans RM_X) : violations SSP au sein de la cage.

Les versions plus anciennes de ces différents journaux sont conservées compressées dans */log/keep/*. Les fichiers compressés sont numérotés en fonction de leur ancienneté, par exemple *fw.log.gz.1* désigne la plus récente archive de *fw.log*, *fw.log.gz.2* la précédente, etc. Ces fichiers sont consultables par des commandes *zcat* ou *zless*.

Annexe C Architecture

Trois réseaux composent l'architecture de CLIP-RM :
•RM_H (réseau de messagerie haut) ;
•RM_B (réseau de messagerie bas) ;
•UPDATE (réseau de mise à jour du socle et des cages RM).



Les réseaux RM_H ou RM_B peuvent être optionnels (dans le cas d'un déploiment simple-niveau), mais le réseau UPDATE est forcément présent. Le réseau RM_B ne possède pas de sécurité particulière (autre que sa sécurité intrinsèque), tandis que les réseaux RM_H et UPDATE sont accessibles (au travers du réseau RM_B) en passant par un tunnel chiffré et authentifié (IPSEC).

Annexe D Conditions d'usage du poste CLIP

Afin de maintenir les propriétés de sécurité apportées par un poste CLIP, les utilisateurs doivent veiller à ce que les conditions d'usage suivantes soient respectées :

1. L'installation du poste doit avoir été réalisée sur un site de confiance, en suivant la procédure détaillée dans le document de référence [CLIP_2001]. Si une réinstallation du poste s'avère nécessaire, l'utilisateur ne doit pas le réinstaller lui-même mais le retourner afin qu'il soit réinstallé dans les mêmes conditions.
2. Le poste doit être utilisé conformément à la catégorisation TEMPEST du poste et au niveau de classification des informations traitées (cf. [CLIP_2003])
3. Une référence de temps externe doit être utilisée pour la configuration de la date et de l'heure du système. Comme détaillé en Error: Reference source not found, l'utilisation d'un serveur NTP dans la zone de service UPDATE est préférable. A défaut, toute autre référence fiable peut être utilisée pour une configuration manuelle.
4. L'environnement réseau doit permettre au poste de communiquer avec deux passerelles IPsec CLIP (UPDATE et RM_H). Ces passerelles doivent être protégées en intégrité, et leurs éléments secrets d'authentification protégés en confidentialité.
5. Un auditeur doit exploiter les journaux dans les délais appropriés, en l'occurrence inférieurs à la période de rotation des journaux (cf. Error: Reference source not found).
6. Le BIOS doit être configuré selon les recommandations définies dans le guide correspondant (document de référence [CLIP_2002]).
7. Les composants du poste jugés superflus doivent être retirés physiquement ou désactivés au niveau du BIOS (e.g. cartes sans-fil…).
8. Au moins deux comptes administrateur du socle doivent être configurés pour des raisons de redondance, afin que le poste puisse continuer à être administré si les éléments d'authentification d'un administrateur sont inutilisables (perdus, détruits…).
9. Le poste doit être livré et installé de manière à respecter la politique de sécurité et les contraintes applicables à l'organisme pour le traitement d'informations de niveau RM_H.
10. Le poste doit se trouver dans un local de niveau de sécurité en adéquation avec celui défini pour son usage selon le mode : en fonctionnement (poste allumé) et en mode stockage (poste éteint, pas de données utilisateur en clair).
11. Les usagers doivent être formés (formations, guides) à l'utilisation du poste. Ils doivent être sensibilisés à la sécurité et à la nécessité de signaler tout comportement anormal du système, ainsi qu'aux risques d'erreur liés au traitement simultané de deux niveaux de sensibilité sur un même poste. La formation des usagers inclut une sensibilisation au choix des mots de passe. Chaque utilisateur doit changer son mot de passe immédiatement après la création de son compte. Les modalités de choix et de renouvellement des mots de passe sont précisées par la politique de sécurité.
12. Des mesures organisationnelles doivent être mises en oeuvre pour permettre la détection de vol du poste.

13. Une étiquette de sécurité doit être collée sur le poste afin de détecter toute intrusion physique.
14. Des mesures organisationnelles doivent définir comment détecter l'indisponibilité du poste par exemple à la suite d'une mauvaise configuration de la part d'un administrateur, du socle ou des cages RM. Elles précisent comment un utilisateur peut remonter des problèmes liés à l'indisponibilité de son poste, ces problèmes étant dus à des erreurs, volontaires ou non, de la part d'un administrateur.

Annexe E Références

[CLIP_2001] *Documentation CLIP – 2001 – Procédure d'installation*

[CLIP_2002] *Documentation CLIP – 2002 – Guide de configuration du BIOS (document 2002x correspondant au matériel considéré)*

[CLIP_2003] *Documentation CLIP – 2003 – Guide TEMPEST (document 2003x correspondant au matériel considéré)*