Agence Nationale
de la Sécurité des
Systèmes d'Information

Mémo : Guide de démarrage du client Clip

Mots-clés : démarrage,premiers pas, client Clip

Table des matières

DIFFUSION LIMITÉE

DIFFUSION LIMITÉE

1 Pré-requis

Ce guide a pour but de permettre à un utilisateur de se familiariser rapidement avec son nouveau environnement de travail Clip (poste client). Il ne nécessite aucun pré-requis. D'autres guides détaillent l'utilisation avancée du poste.

2 Présentation générale de Clip

2.1 Multiniveau et le poste client

Le poste Clip, pour « Client Protégé », est tout d'abord un ordinateur portable multiniveau, ce qui permet à son utilisateur de manipuler des données et de rejoindre des réseaux de niveaux de sensibilités différents, en toute sécurité. Le système sur lequel s'appuie Clip emploie à cet effet des mécanismes de cloisonnement robustes, qui permettent d'isoler entre eux des compartiments logiciels. Le système Clip distingue notamment deux compartiments appelés compartiments «RM» (Réseau de Messagerie). L'un correspondant au niveau bas, appelé RMB, peut être connecté au réseau local, ou forcer tout ou une partie des communications à passer par IPsec. L'autre au niveau haut, appelé RMH, fait lui toujours passer ses connexions via un tunnel IPsec. Ces deux niveaux cohabitent sur la machine Clip tout en restant cloisonnés.

La machine Clip peut ainsi être l'extension de deux réseaux de niveaux de classification différents correspondants à « RMB » (typiquement, internet) et « RMH » (un réseau de niveau diffusion restreinte). Des machines DR peuvent importer et exporter des données vers la machine Clip. De même, la machine Clip peut importer et exporter des données vers des machines connectées à l'internet. L'accès à ces réseaux se fait par l'intermédiaire d'une interface indifférenciée (connexion filaire – ethernet ou optique –, ou sans fil – wifi ou cellulaire –).

Au niveau de l'interface graphique du poste, les niveaux « RMB » et « RMH » se matérialisent par les deux bureaux distincts auxquels l'utilisateur peut accéder en cliquant sur le bouton de la barre dite « de confiance », située à gauche de l'écran, et dont l'apparence change en fonction du niveau actif (les couleurs étant définies à l'installation du poste, ou laissé par défaut : rouge/vert). Chacun des deux compartiments « RMH » et « RMB » disposent des capacités habituelles d'un poste informatique : outil de messagerie, navigateur, suite logicielle bureautique, etc.

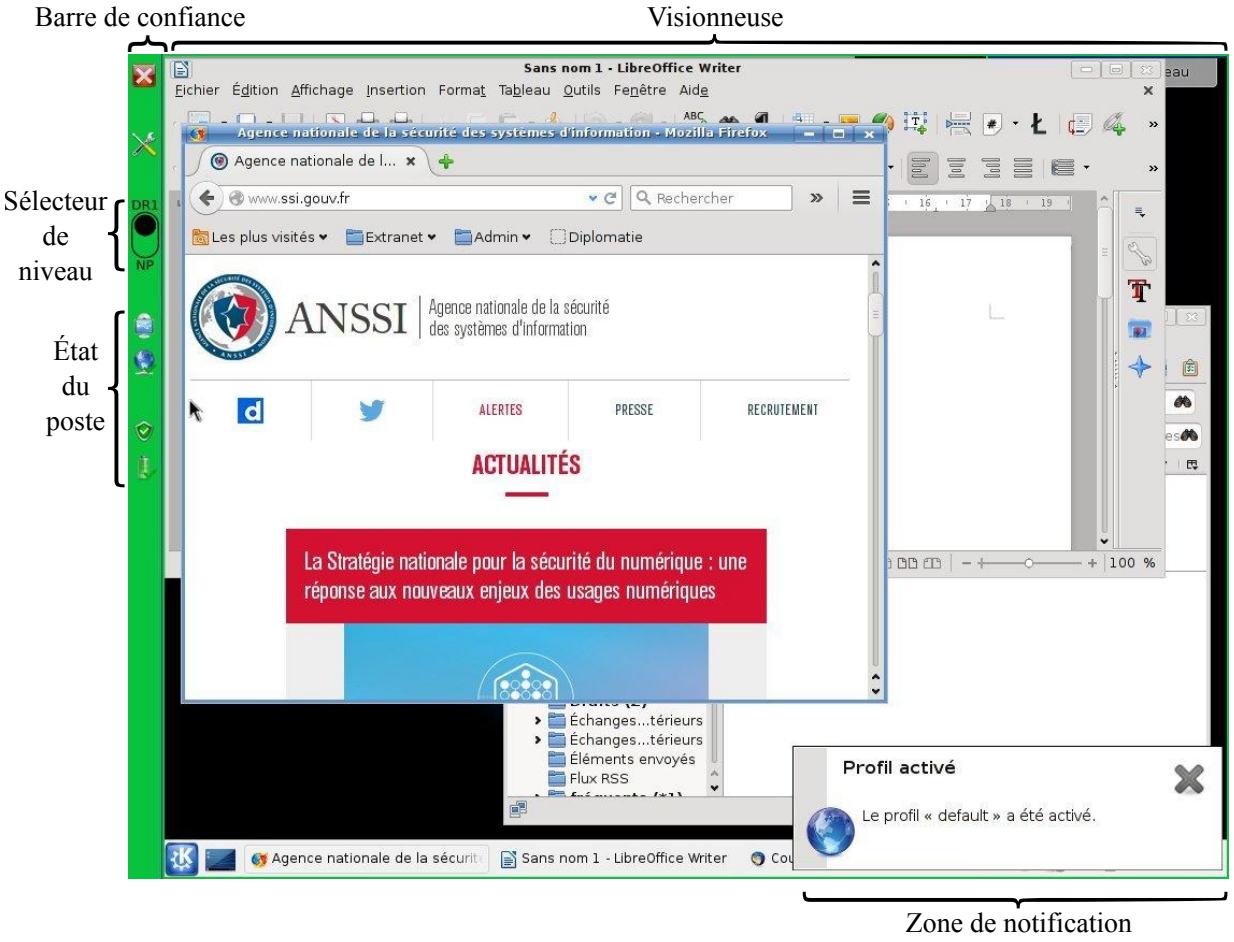

FIGURE 1 – Présentation du bureau CLIP

La Figure 1 présente la vue utilsateur après le démarrage du poste.

2.2 Fonctions et mécanismes de sécurité

Le système d'exploitation CLIP généralise tout d'abord l'emploi du mécanisme de cloisonnement évoqué précédemment à l'ensemble du système. Ce cloisonnement concourt à une meilleure séparation et à une réduction des privilèges des programmes qui s'exécutent dans des compartiments distincts, et limite ainsi la portée de l'exploitation d'une vulnérabilité, y compris dans un service privilégié.

Ce cloisonnement sert également à séparer rigoureusement les rôles des différents intervenants sur le poste :

- l'administrateur ne peut pas accéder aux données de l'utilisateur ni interférer avec les processus de journalisation du système ;
- l'auditeur a exclusivement accès aux journaux d'activité du poste ;
- l'utilisateur standard ne dispose ni des privilèges de l'administrateur ni de ceux de l'auditeur.

La Section 3 donne de plus amples détails sur ces différents rôles.

Le système d'exploitation du poste CLIP est **durci** : c'est un noyau Linux minimaliste spécialement adapté au matériel constituant le poste de travail et équipé de dispositifs de sécurité supplémentaires. Le système d'exploitation constitue ainsi le socle de confiance du poste. Ce durcissement réduit très fortement les risques d'injection de code malveillant depuis les réseaux auxquels le poste est connecté.

Les données utilisateurs de « RMB » et « RMH » sont chiffrées à la volée sur le disque du poste CLIP (généralement en utilisant le mot de passe de l'utilisateur) afin de protéger leur confidentialité.

Si l'accès au réseau « RMH » est protégé par une connexion IPsec, au sein de laquelle sont routés l'intégralité des flux destinés à ce réseau, l'accès au réseau « RMB » est plus flexible. Il permet notamment (selon le déploiement) de « débrayer » l'utilisation du tunnel IPsec et de choisir sa portée (toutes les communications, ou un ensemble de destinations seulement). En outre, il est possible de protéger les flux réseaux en plus du tunnel IPsec, application par application, via l'utilisation de tunnels TLS (configurables indépendamment pour chaque niveau).

Le socle de confiance du système d'exploitation du poste Clip, de même que tout l'environnement applicatif des compartiments « RMH » et « RMB » sont automatiquement mis à jour avec des paquetages logiciels dont l'authenticité est vérifiée. Cette mise à jour peut être locale (par ex. CD-ROM ou USB) ou distante (via l'utilisation d'un canal IPsec dédié).

Le système rend les droits d'exécution et d'écriture mutuellement exclusifs. Ceci signifie en particulier qu'il est impossible pour l'utilisateur d'exécuter des programmes (ou des scripts) qui seraient importés dans son environnement de travail personnel (par exemple par le biais d'une clé USB ou d'une pièce jointe à un email). Seuls les logiciels fournis avec le poste Clip peuvent être exécutés. Cette protection vise à empêcher l'exécution de code arbitraire ou non maîtrisé.

Le poste est protégé contre l'insertion de supports USB malveillants. Le poste peut être configuré pour que seules des clés USB préalablement enregistrées sur le poste puissent être rendues accessibles en écriture dans les différents compartiments. Il reste en revanche toujours possible d'exposer une clé USB non enregistrée en lecture seule dans un compartiment. Par ailleurs, le contenu des clés USB peut être automatiquement chiffré (voir le document « Clés USB »).

L'échange d'informations entre les réseaux « RMH » et « RMB » est possible et maîtrisé par l'emploi d'une diode « logicielle » dans le sens montant et d'une diode chiffrante dans le sens descendant.

3 Rôles, comptes et privilèges des utilisateurs

3.1 Rôles

La sécurité d'un poste informatique plaide en faveur de la séparation des privilèges des utilisateurs autorisés à utiliser le poste. En application de ce principe, le système Clip distingue plusieurs sortes de comptes organisés autour de trois **rôles** principaux :

- le rôle **utilisateur** a accès à des applications de bureautique, à un navigateur Internet, et à un client de messagerie, dans les deux environnements RM évoqués dans la section précédente ;
- le rôle **administrateur** a la possibilité de gérer la configuration nécessaire au bon fonctionnement du système ;
- le rôle **auditeur** donne accès aux paramètres du poste, ainsi qu'aux journaux systèmes, mais uniquement en lecture.

Les privilèges associés au rôle administrateur sont très limités. Ces privilèges permettent exclusivement à celui qui en bénéficie de modifier les paramètres réseau, d'ajouter ou supprimer des utilisateurs, de gérer les éléments cryptographiques, de modifier la date et l'heure du poste, d'ajouter ou supprimer des logiciels optionnels et de changer l'attribution des périphériques aux environnements RM. Les privilèges associés au rôle administrateur dans le cas d'un poste Clip ne correspondent donc pas à ceux de l'Administrateur Windows ou root UNIX.

3.2 Comptes

Le système Clip distingue cinq types de **comptes** :

- le compte **utilisateur**, qui correspond au rôle utilisateur ci-dessus ;
- le compte **administrateur du socle**, qui correspond au rôle administrateur ci-dessus ;
- le compte **auditeur du socle**, qui correspond au rôle auditeur ci-dessus ;
- le compte **utilisateur privilégié**, qui cumule les prérogatives des trois profils ;

– le compte **utilisateur nomade**, qui a la capacité de modifier au cours de l'utilisation la configuration réseau d'un poste CLIP.

Visuellement, l'interface de chaque compte est distinguable par la présence ou non des différents menus dans la barre du socle CLIP.

Le compte utilisateur privilégié offre une ergonomie accrue dans le cas où un seul utilisateur est configuré sur le poste car il confère à ce dernier des privilèges dont il a l'habitude de disposer (notamment, installer des logiciels optionnels ou modifier la configuration réseau). Compte tenue de la portée très limitée des privilèges associés aux rôles administrateur et auditeur, le cumul des trois rôles ne présente pas de risque majeur sur la sécurité (sauf considérations organisationnelles lorsque plusieurs utilisateurs sont définis sur le poste). Rappelons par ailleurs qu'un utilisateur privilégié ne peut pas accéder aux données d'un autre utilisteur du poste.

Les Figures 2 et 3 illustrent l'interface graphique pour un compte administrateur et pour un compte utilisateur privilégié.

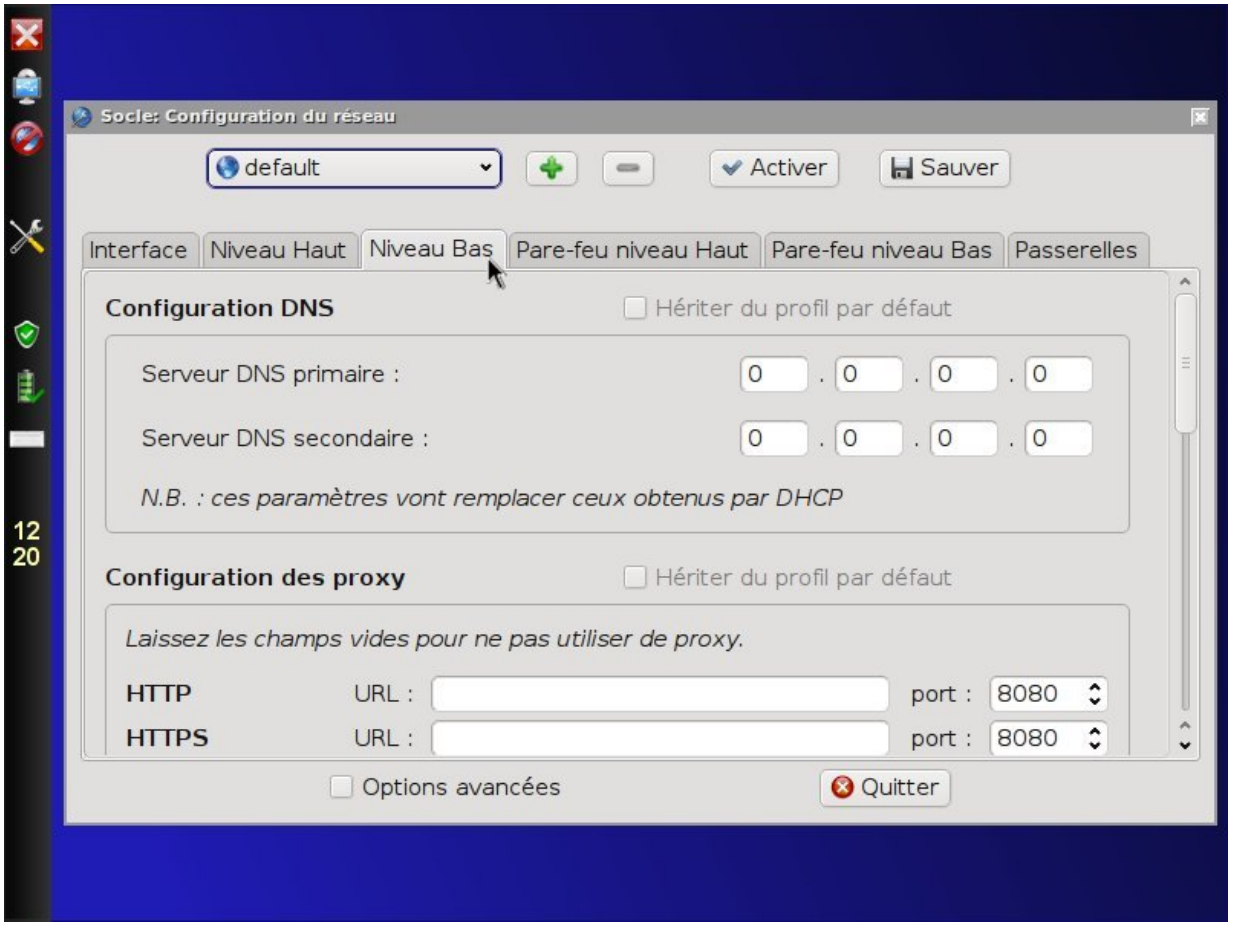

FIGURE 2 – Bureau CLIP du rôle administrateur (fenêtre du gestionnaire de réseau ouverte)

FIGURE 3 – Bureau CLIP du rôle utilisateur privilégié

4 Configuration du poste

Les éléments de configuration du poste CLIP sont minimaux. La plupart des opérations d'administration usuelles (installation et configuration d'applications) se font à l'échelon central, au niveau de l'élaboration des mises à jour de CLIP.

4.1 Changement de mot du passe de l'utilisateur

Le changement du mot de passe de l'utilisateur se fait depuis la barre de confiance via le menu « Configuration et administration » → « Compte » → « Mot de passe ».

4.2 Verrouillage automatique du poste

Le verrouillage du poste est obligatoire et ne peut pas être désactivé par l'utilisateur. Seul le délai peut être modifié de manière temporaire, pour la durée de la session de l'utilisateur (ceci sert notamment à empêcher le verrouillage intempestif du poste qui peut s'avérer gênant, par exemple lors d'une présentation devant un auditoire). La modification du délai de verrouillage se fait depuis la barre de confiance via le menu « Configuration et administration » → « Compte » → « Verrouillage de session (temporaire) ».

Seul les comptes avec le rôle administrateur ont le droit de modifier de manière permanente le délai de verrouillage de manière définitive, via le menu « Configuration et administration » → « Compte »

→ « Verrouillage de session (permanent) ».

4.3 Paramètres de saisie du poste

Les paramètres de saisie du poste (disposition du clavier, configuration de la souris, du clavier et du pavé tactile) peuvent être modifiés via le menu « Configuration et administration » → « Périphériques » → « Clavier et souris ».

5 Bureau virtuel

L'environement de bureau fournit par défaut sous Clip est KDE. Il s'agit d'un ensemble de logiciel libre et bien documenté sur Internet. Nous ne décrirons donc pas son fonctionnement dans cette section.

6 Logiciels

6.1 Logiciel de messagerie

Le logiciel de message fournit avec Clip est Mozilla Thunderbird. Il permet les accès classiques au mail par IMAP et POP. Sa documentation est disponible depuis le logiciel et sur le site de l'éditeur.

6.2 Navigateurs Web

Clip fournit deux navigateurs Web : Mozilla Firefox et Chromium (version libre de Google Chrome). Ceux-ci sont fournis avec certaines fonctionalités désactivées (chargement manuel de « plugin », lien de remontée de bug avec l'éditeur, etc) afin d'améliorer leur sécurité.

6.3 Logiciels bureautiques

Clip est fourni avec la suite LibreOffice. Pour la rédaction de documents scientifiques, TexLive est également disponible (en tant que paquetage optionnel).

6.4 Logiciels spécifiques Clip

6.4.1 ACID Cryptofiler

L'outil ACID Cryptofiler de la DGA-MI, permettant de manipuler des archives au format ACID, est disponible uniquement pour le niveau haut du poste.

6.4.2 Diodes logicielles

L'échange d'informations entre les compartiments « RMB » et « RMH » est possible. Dans le sens montant, une diode permet l'import de données depuis le niveau bas (possiblement internet) vers le niveau haut (potentiellement de catégorie Diffusion Restreinte). Dans le sens descendant, une diode chiffrante (illustrée Figure 4) permet de noircir des données du niveau « RMH » pour permettre leur acheminement sur un réseau « Non Protégé ». Ce chiffrement est compatible de celui du logiciel ACID v7 développé par DGA-MI et peut donc réutiliser les mêmes clés. Inversement, à la réception, des données chiffrées peuvent être directement importées au niveau « RMH ».

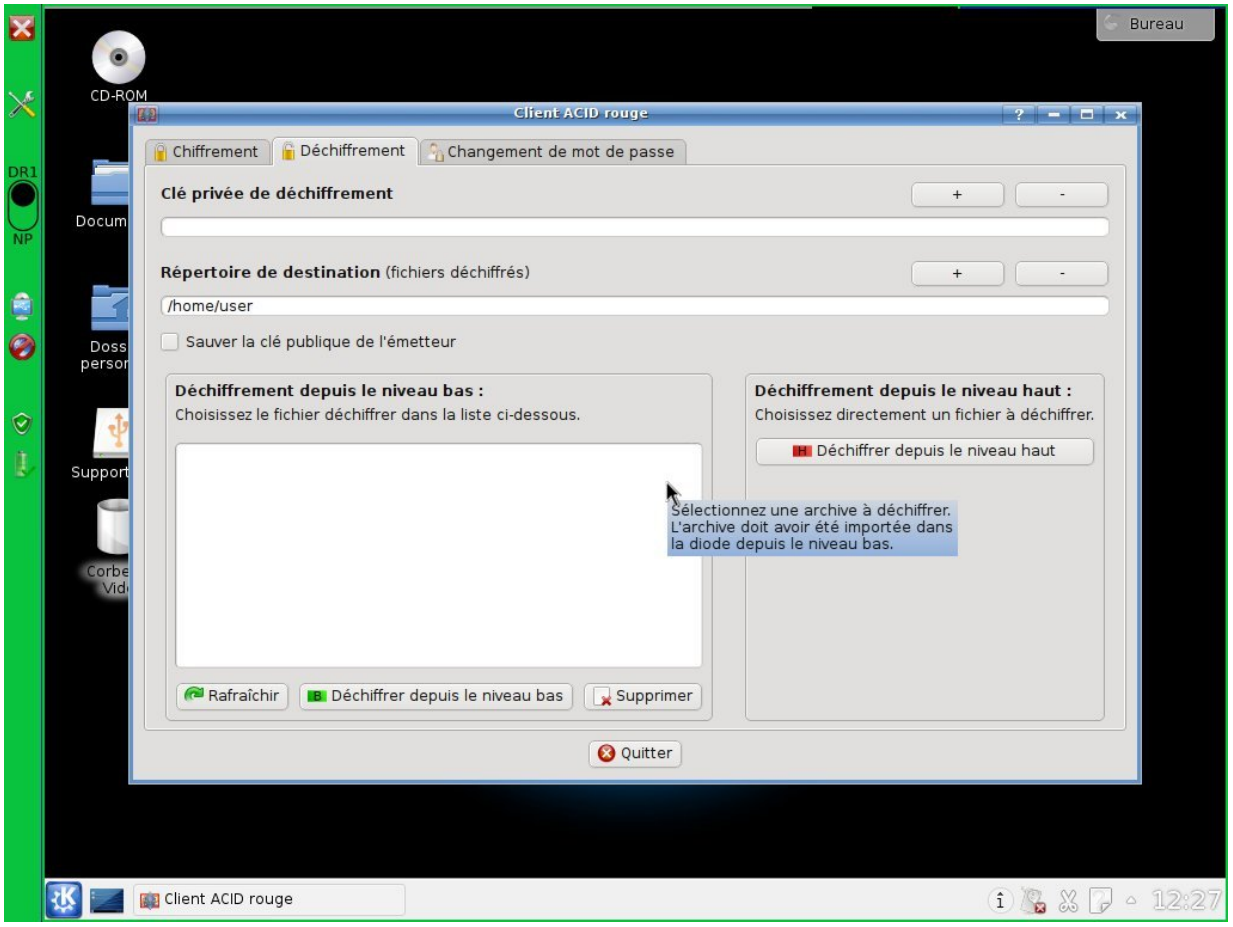

FIGURE 4 – Diode (ACID) chiffrante descendante

6.5 Paquetages logiciels additionnels

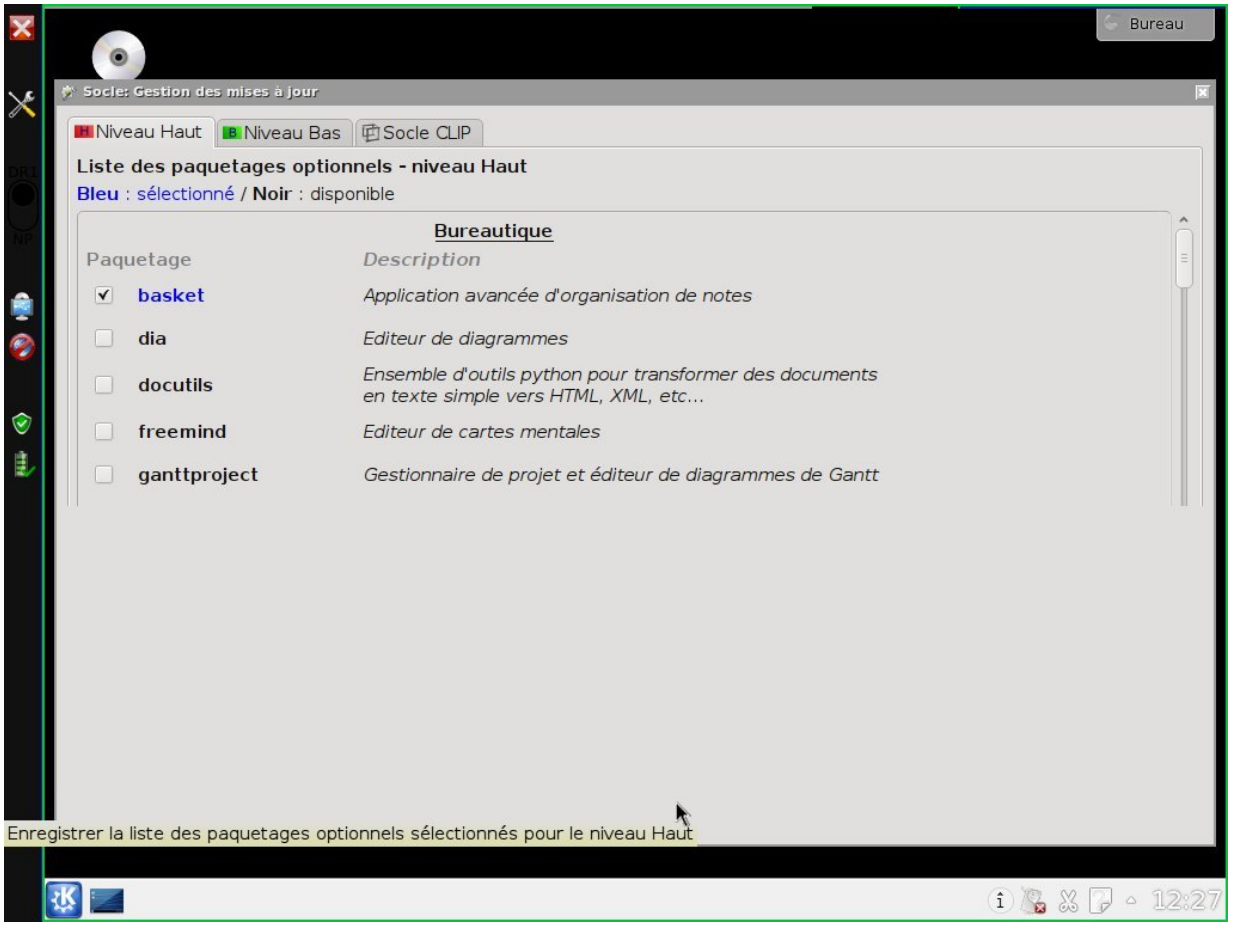

FIGURE 5 – Application d'ajout de logiciels additionnels

Le poste CLIP fournit l'équivalent d'un « store » d'application. Il s'agit d'applications supplémentaires qui peuvent aller jusqu'à modifier le fonctionnement du poste (par exemple, le bureau par défaut KDE peut être remplacé par XFCE). L'ajout de ces applications se fait de manière graphique depuis la barre de confiance via le menu « Configuration et administration » → « Mises à jour » → « Paquetages optionnels ». L'application est illustrée Figure 5. Plusieurs onglets sont disponibles, en fonction du niveau où l'application devra être installée (« RMH », « RMB » ou le socle), car la liste des applications disponibles varie en fonction des niveaux. Par ailleurs, l'installation d'un paquetage à un niveau ne signifie pas que le paquetage sera installé automatiquement à un autre niveau.

7 Configuration du réseau

L'accès à la configuration du réseau se fait via l'entrée du menu « Gestion du réseau » accessible via le bouton « Réseau » de la barre du socle. L'icône de ce bouton dépend de la nature et de l'état de la connexion réseau sous-jacente.

7.1 Notion de profil réseau

L'organisation de la configuration réseau se fait par *profil*. Par exemple, il est possible de définir un profil Bureau, un profil Domicile, un profil Wifi-train, etc. L'utilisateur peut définir autant de profils

qu'il le souhaite (sous réserve qu'il dispose des privilèges requis, voir section 3, p. 3).

Le bouton « + » de la fenêtre de gestion du réseau sert à créer un nouveau profil réseau. Il suffit ensuite de lui attribuer un nom et de renseigner les paramètres du nouveau profil. Le profil courant sera pris comme base du nouveau profil.

Une fois un profil configuré et sauvegardé, il est nécessaire de l'activer en cliquant sur le bouton « Activer ». La bascule d'un profil à un autre est réalisée d'une manière sécurisée qui exclut l'existence d'états intermédiaires (ou d'états résultant d'erreurs) non sûrs (par exemple, une interface réseau activée sans filtrage ou chiffrement, ou avec un filtrage inadapté à ses adresses). Il en résulte que l'accès à tout réseau est suspendu pendant la durée d'activation du profil. Le réseau ne sera à nouveau disponible qu'une fois toutes les protections de type pare-feu correctement reconfigurées.

7.2 Profil par défaut

Le profil activé au démarrage, et présent sur tous les systèmes, est nommé « profil par défaut ». Il sert de base à un système d'héritage des profils réseaux. Ainsi, chaque profil peut décider ou non d'hériter d'une ou plusieurs parties du profil par défaut (c.-à-d. les champs de ces parties ne seront pas défini par le profil en cours d'édition, mais par le profil par défaut). La seul partie qui ne peut être hérité est le type de connexion (décrit à la section suivante).

Lorsque l'ajout d'un nouveau profil est réalisé depuis le profil par défaut (celui-ci est en cours d'édition dans l'interface graphique), il est possible de créé un profil complètement hérité. Cela permet par exemple de partager les mêmes paramètres (par ex. DHCP) entre un réseau Wifi et un réseau Ethernet filaire.

L'héritage ajoute une flexibilité dans la gestion des profils réseaux, son utilisation est donc souvent recommandée.

7.3 Types de connexion

Le choix du type de connexion se fait dans le premier onglet « Interface ». Trois types de connexion réseau sont supportées :

- Connexion filaire : la connexion filaire peut utiliser l'interface Ethernet native du poste ou une interface optique supportée. Aucune configuration spécifique n'est requise pour cet accès physique. Seule la configuration TCP/IP est nécessaire. La gestion des certificats d'accès RADIUS n'est pas encore supportée pour l'accès filaire ;
- Connexion WiFi : l'onglet WiFi permet de configurer les paramètres d'accès à un réseau sans fil WiFi. Tous les modes d'accès possibles sont actuellement supportés. Saisissez tout d'abord l'identifiant ESSID du réseau WiFi ou sélectionnez le en cliquant sur « Choisir un identifiant parmi les réseaux actifs » ;
- Connexion UMTS : la connexion UMTS ou 3G suppose l'utilisation d'un matériel particulier de marque Option ou Sony Ericsson. Il est déconseillé, pour une première utilisation de Clip, de se connecter par ce biais, car les aléas des réseaux de télécommunication 3G sont encore importants. Entrez tout d'abord le code PIN de votre carte SIM, puis les informations de connexion de votre fournisseur d'accès.

Il est possible également de spécifier « pas d'accès réseau » pour avoir un profil où le réseau n'est pas activé.

7.4 Configuration TCP/IP

- **Obtention automatique d'adresse IP :** la plupart des réseaux proposent une obtention automatique de l'adresse IP. Dans l'onglet Socle sélectionnez DHCP. Ceci suffit généralement à réaliser la totalité de la configuration réseau. Dans certains cas, il peut toutefois être nécessaire

de configurer le DNS et les proxy. La partie DNS surcharge les valeurs qui peuvent être envoyer par le DHCP ;

- **Configuration manuelle de l'adresse IP :** si le réseau ne fournit pas automatiquement la configuration IP, sélectionner « Attribution manuel » dans l'onglet « Adresse du socle ». Consultez votre administrateur réseau pour connaître les paramètres à renseigner aux deux lignes « Adresse IP » et « Passerelle par défaut ».
  Par exemple, si votre adresse locale est `192.168.3.23`, que votre réseau local est en `192.168.0.0/16` et que votre passerelle a pour adresse `192.168.254.254`, renseignez les valeurs suivantes :
  - Adresse IP : `192.168.3.23/16`
  - Passerelle par défaut : `192.168.254.254` [1]

7.5 Configuration DNS

Si le réseau ne fournit pas automatiquement les adresses des serveurs DNS et des proxy, consultez votre administrateur réseau pour obtenir ces informations et renseignez les dans l'onglet « RMB » et « RMH ».

7.6 Configuration du pare-feu local

Les onglets « Pare-feu niveau Haut » et « Pare-feu niveau Bas » de la fenêtre de configuration du réseau permettent de modifier les règles de filtrage des flux autorisés à sortir des compartiments « RMH » et « RMB », respectivement. Aucun flux entrant n'est autorisé sur le poste (à l'exception des flux IPsec entrant pour la cage *_audit* et *_admin* si ces services sont activés).

7.7 Accès au réseau « RMH »

Le poste Clip se connecte à un réseau support donnant l'accès à internet.

Pour disposer de l'accès aux serveurs du réseau niveau haut (et également niveau bas dans certaines configurations), le poste Clip doit pouvoir établir un tunnel chiffrant. Ce tunnel chiffrant utilise les protocoles standards IPsec et IKEv2. Pour un fonctionnement correct, l'accès à l'internet ne doit donc pas filtrer ces protocoles [2].

8 Supports de stockage amovibles

Le fonctionnement du support des clés USB est détaillé dans le document « Clés USB ».

8.1 Supports de type CD/DVD ROM

Un CD-ROM ou un DVD-ROM peut être monté en lecture sur l'un des compartiments « RMH » ou « RMB ». Il apparaît alors dans le répertoire `/mnt/cdrom` du niveau sur lequel il a été monté. Pour cela, depuis la barre de confiance, utiliser le menu « Périphériques amovibles » → « Monter un CD-ROM ».

Pour éjecter un CD-ROM ou un DVD-ROM, utiliser le menu « Périphériques amovibles » → « Éjecter le CD-ROM ».

Il n'est pas possible à ce stade de graver un CD/DVD-ROM sur un poste Clip.

1. Attention, votre passerelle par défaut doit appartenir à votre réseau local.
2. Techniquement, les flux IPsec utilisent des connexions UDP sur les ports 500 et 4500 et des paquets IPsec ESP.

9 La sauvegarde : une précaution d'usage

Le poste Clip est un poste nomade dont l'utilisation ne requiert pas d'être connecté en permanence au réseau. La sauvegarde des informations de l'utilisateur n'est donc pas assurée et **il convient de prévoir un mécanisme de sauvegarde locale**.

La sauvegarde de données doit autant que possible limiter les risques de compromission des données de l'utilisateur. Rappelons que celles-ci sont chiffrées sur le disque (au sein de « RMH » et de « RMB ») et que les mécanismes de durcissement du système réduisent le risque d'une compromission des données suite à une intrusion ou un virus. Il convient donc de protéger convenablement le support de stockage externe utilisé pour sauvegarder les données.

Pour la sauvegarde des données, il est recommandé d'utiliser un support USB chiffré pour chaque compartiment. Pour peu que les clés de chiffrement du support aient bien été exportées et récupérées cette synchronisation constitue donc une sauvegarde récupérable. On s'assurera de cela en montant le support sur une autre machine.

10 Périphériques externes

10.1 Attribution des périphériques du poste

Il est possible d'attribuer un périphérique à un au plusieurs niveaux (carte son, Webcam, carte à puce, ...). Afin de garantir le cloisonnement du poste, l'utilisation de briques logicielles intermédiaire est parfois utilisée.

Pour démarrer la boite de dialogue : menu de la barre de confiance « Configuration et administration » → « Périphériques » → « Attribution des périphériques ».

10.2 Écran externe ou vidéoprojecteur

La connexion d'un écran externe ou d'un vidéoprojecteur active automatiquement un clonage de l'affichage sur le périphérique concerné. La résolution choisie pour l'affichage devient alors la plus grande résolution commune à tous les écrans connectés sur le système.

Il est parfois souhaitable d'aller plus loin, notamment lorsque le but est d'attribuer un niveau par écran. La configuration de l'affichage externe se fait via l'outil accessible depuis le menu de la barre de confiance « Configuration et administration » → « Périphériques » → « Paramètres d'affichage ». Pour plus d'information, voir la documentation « Écran étendu ».

10.3 Imprimantes

Le gestionnaire d'impression accessible depuis l'intérieur des visionneuses dans le « Menu K » → « Application » → « Configuration » → « Système » → « Configuration du système » → « Imprimantes » permet de réaliser la plupart des opérations de configuration des imprimantes.

10.3.1 Types d'imprimantes

Clip permet d'utiliser des imprimantes réseau et des imprimantes USB. Dans la configuration par défaut du poste, les imprimantes USB ne sont accessibles que depuis le contexte « RMH ».

10.3.2 Ajout d'imprimante

Pour ajouter une imprimante, il suffit d'exécuter le gestionnaire d'impression, de cliquer sur le menu « Ajouter », de choisir « Ajouter une imprimante/une classe », puis de répondre aux questions posées.

Lorsqu'on ajoute une imprimante, le système demande la marque de celle-ci, puis demande à choisir son modèle. Si celui-ci existe dans la liste, on peut le sélectionner, puis prendre le pilote recommandé. Si le modèle n'existe pas, un modèle approchant peut être sélectionné.

Une imprimante USB doit être préalablement alimentée et connectée au poste pour être ajoutée. Le choix du mode de communication avec une imprimante réseau (SMB/Windows, TCP, CUPS distant ou IPP) dépend du type d'imprimante et/ou de la façon dont elle est configurée. Le choix de TCP fonctionne généralement (il est nécessaire de connaître l'adresse IP de l'imprimante et le port –9100 par défaut–).

10.3.3 Modification des propriétés d'une imprimante

Depuis l'interface principale du gestionnaire d'impression, une imprimante peut-être définie comme imprimante par défaut (clic droit sur l'imprimante, « Choisir par défaut pour l'utilisateur » et « Choisir par défaut localement »).

Depuis l'interface principale du gestionnaire d'impression, en sélectionnant l'imprimante et en choisissant « Configurer... », il est possible de modifier les paramètres de l'imprimante (résolution, format de papier par défaut, etc.).

10.3.4 Suppression d'une imprimante

Depuis l'interface principale du gestionnaire d'impression, sélectionner l'imprimante (clic droit) puis « Supprimer ».

10.3.5 Problèmes d'impression

Voici quelques suggestions pour vous aider à résoudre d'éventuels problèmes d'impression :
- vérifier que l'imprimante est connectée ;
- vérifier que l'imprimante est bien accessible (dans le cas d'une imprimante réseau) ou connectée au poste (dans le cas d'une imprimante USB) ;
- vérifier que le contexte « RMB »/« RMH » depuis lequel l'impression est lancée correspond à celui auquel l'imprimante est associée ;
- vérifier que l'imprimante est en marche du point de vue du poste Clip (l'imprimante ne doit pas être marquée comme «arrêtée» dans l'interface du gestionnaire d'impression ; si c'est le cas, faire un clic droit sur l'imprimante et choisir «démarrer l'imprimante») ;
- vérifier que le système d'impression utilisé par défaut est CUPS (cette information est accessible depuis la fenêtre principale de l'interface du gestionnaire d'impression).

10.4 Scanners

Un scanner (en connectique USB) peut être utilisé directement sur le compartiment « RMB ». Aucune commande de montage n'est a priori nécessaire.

Après avoir connecté et allumé le scanner, vous pouvez l'utiliser :
- soit par le biais d'un outil bureautique : par exemple, dans LibreOffice, vous pouvez insérer une image provenant directement de votre scanner (pour la configuration, par le menu « Insertion/Image/Scanner/Sélectionner la source » ; pour acquérir l'image par le menu « Insertion/Image/Scanner/Acquérir) » ;
- soit par le biais de l'outil dédié Skanlite.

11 Mise à jour du poste

Comme évoqué dans la présentation générale du poste, le socle de confiance du système d'exploitation du poste CLIP, de même que tout l'environnement applicatif des compartiments « RMH » et « RMB » sont **automatiquement mis à jour**, à distance, par un réseau dédié, au moyen de paquetages logiciels dont l'authenticité est vérifiée.

L'icône en forme de bouclier située dans la barre de confiance indique la présence ou non de mise à jour. Ces mises à jour sont appliquées au redémarrage du système.

Le téléchargement des mises à jour est réalisé en arrière plan et l'utilisateur ne peut empêcher leur application ; il peut seulement la retarder. L'installation d'une mise mise à jour pouvant être assez longue, la possibilité pour l'utilisateur de retarder sa réalisation sert à limiter d'éventuels désagréments dûs au besoin de disponibilité immédiate du poste.

Le poste dispose en permanence de la version courante du système et de la version précédente, de sorte que l'utilisateur puisse toujours utiliser une version fonctionnelle de son poste, dans l'hypothèse où une mise à jour poserait problème. Le choix de la version se fait lors du démarrage du poste, voir Figure 6.

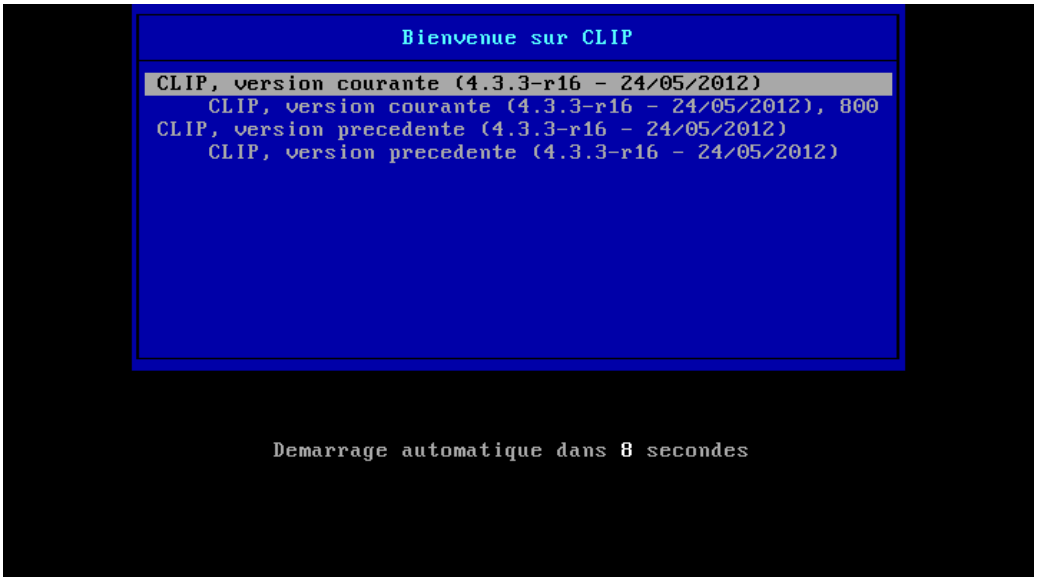

FIGURE 6 – Menu de démarrage de séléction du système (ici, les systèmes sont identiques car le système est fraichement installé)