M. CHAILLOU Antoine

Le Centre d'Etudes et de Développement Informatiques du Matériel de l'Armée de Terre

NOTE DE SYNTHESE

Projet :

Mise en place d'un Proxy
Avec traçabilité et filtrage des stations Internet

mai/juin 2009

Sommaire :

I. Introduction

J'ai réalisé mon stage au **C**entre d'**E**tudes et de **D**éveloppement **I**nformatiques du **M**atériel de l'**A**rmée de **T**erre (C.E.D.I.M.A.T).
Au sein de cet établissement de l'armée de terre, la sécurité des accès au système d'information doit être strictement réglementée, ce qui aura été l'un des objectifs de mon projet.
Le réseau principal du C.E.D.I.M.A.T., était séparé physiquement du réseau INTERNET. Il y avait une connexion INTERNET pour le personnel sur 14 postes dédiés.
Le C.E.D.I.M.A.T. avait souhaité, pour améliorer la sécurité du bâtiment et par obligation d'un décret, « tracer » et « limiter » les accès Internet des utilisateurs. Cependant l'architecture existante n'était pas adaptée aux besoins de l'établissement et aux exigences de la direction.

Mon projet consistait donc à étudier et à mettre en place une solution permettant de **« tracer »** et de **« limiter »** les accès Internet.

La note de synthèse est organisée en plusieurs parties. Dans un 1er temps, je ferai une présentation de l'établissement public. Dans un second temps, j'évoquerai l'architecture existante des accès Internet au C.E.D.I.M.A.T., avant mon arrivée, la problématique du projet, l'étude des différentes solutions et le choix de la solution retenue.
La mise en œuvre de cette solution a consisté en deux étapes principales :

- La mise en place d'un annuaire Active Directory indispensable pour « historiser » les comptes utilisateurs qui accèdent à INTERNET
- La mise en place d'un serveur PROXY

Dans une dernière partie, je préciserai les aspects juridiques concernant la traçabilité des accès INTERNET de l'établissement avec la mise en place de la solution.

Présentation :

L'Ecole Supérieure et d'Application du Matériel (E.S.A.M) est un établissement d'enseignement spécialisé de l'Armée de Terre française, créée en 1945, à Bourges. Sur une superficie de 75 hectares, l'école possède l'ensemble des matériels terrestres en service dans l'Armée et forme des officiers et des sous-officiers pour la maintenance des matériels militaires ; elle dispose d'équipements et de moyens de hautes technologies.

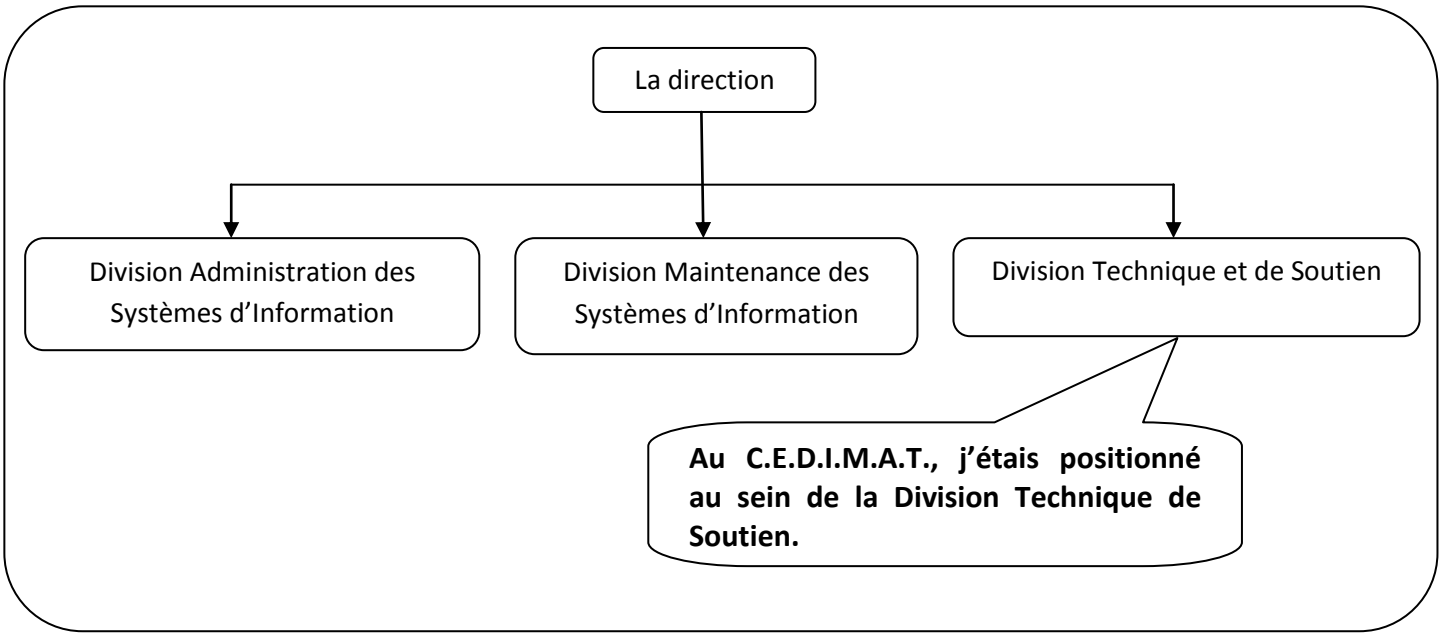
Le Centre d'Etudes et de Développement Informatiques du Matériel de l'Armée de Terre (C.E.D.I.M.A.T.) est implanté à Bourges dans l'enceinte de l'E.S.A.M., depuis 1998. C'est un service qui s'occupe de la gestion des matériels militaires, du développement et de la maintenance de son logiciel SIMAT (c'est une application fonctionnant avec le Système de Gestion de Base de Donnée Relationnelle INGRES) afin de recenser le matériel de l'armée de terre.

Le personnel est constitué d'une centaine de personnes militaires et civiles.

L'établissement est partagé en 4 divisions :

- la Direction,
- la Division Administration des Systèmes d'Information assure le déploiement et l'administration du logiciel SIMAT,
- la Division Maintenance des Systèmes d'Information s'occupe essentiellement de la maintenance et le développement du logiciel SIMAT
- la Division Technique et de Soutien gère l'infrastructure réseau et met en place des plateformes techniques de tests.

Organigramme :

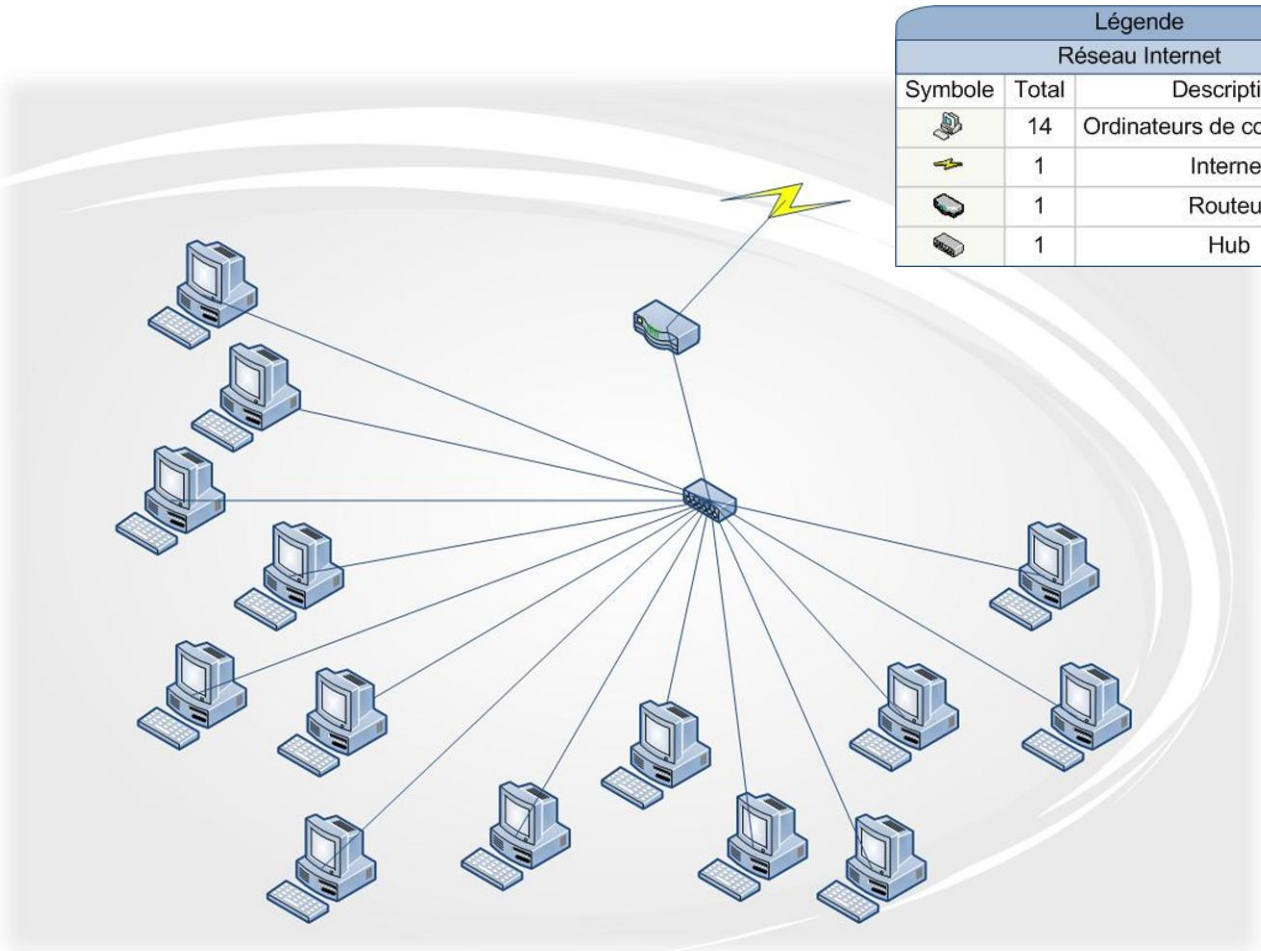


II. Etude de l'existant

Schéma du réseau au début du stage :

Le C.E.D.I.M.A.T. possède 80 Serveurs, 150 Ordinateurs de Bureau, 15 Ordinateurs Portables et 70 Périphériques. Parmi les ordinateurs de bureau, on compte treize postes qui sont sous Windows XP SP3 et un sous Linux, dédiés uniquement aux accès Internet. Ces machines sont coupées « physiquement » du reste du réseau interne de l'entreprise et donc toute autre machine que ces 14 postes n'est pas connectée à INTERNET.
Le routeur est une « LiveBox » de chez « Orange » et la connexion « Wi-Fi » n'est pas active pour des mesures de sécurité.
A l'origine il y avait 9 postes destinés à la sécurité du réseau interne, appelé « stations blanches », et qui ne sont pas également sur le réseau Internet du C.E.D.I.M.A.T. Celles-ci servaient donc à ce qu'un utilisateur puisse transférer des données d'un poste Internet à une machine sur le réseau Intranet de l'établissement en toute sécurité.

Réseau Internet du C.E.D.I.M.A.T. le 18/06/2009



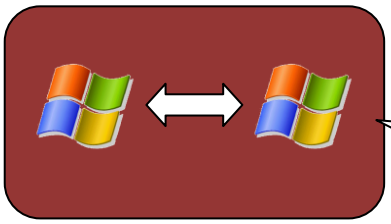
Légende		
Réseau Internet		
Symbole	Total	Description
	14	Ordinateurs de consultations
	1	Internet
	1	Routeur
	1	Hub

Problématique et solution à déployer :

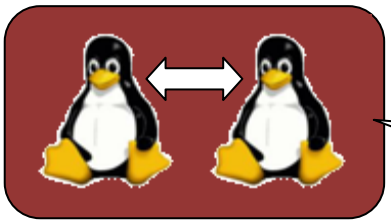
La multiplication des postes internet nécessite la mise en place d'une administration centralisée permettant une gestion plus simple des utilisateurs grâce à un contrôleur de domaine et de l'Active Directory. Le CEDIMAT se doit de conserver dans un délai d'un an toutes traces des connexions effectuées pendant cette période (Il est juridiquement obligatoire d'avoir une traçabilité d'un an d'après le décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques).

La situation actuelle des stations connectées à Internet est également inadaptée pour une bonne gestion des comptes et des profils utilisateurs. Sur chaque machine un compte est créé pour chaque personne (le nombre de compte « locaux » correspond au nombre d'utilisateurs par le nombre de postes dédiés à Internet). Les utilisateurs ont également accès à tous types d'informations circulant sur la toile, la direction souhaite donc aussi mettre en place un filtrage sur certains sites INTERNET (interdire les sites de jeux…).

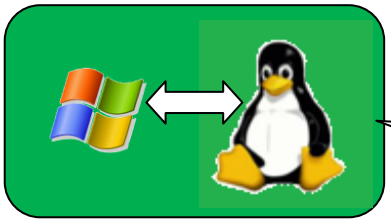
Pour réaliser ce projet les solutions logicielles m'ont été imposées pour des raisons techniques. Les solutions possibles étaient les suivantes :



Deux plateformes <u>Windows</u> était possibles avec « Active directory » sur le premier serveur et une application Microsoft « ISA SERVER » sur le deuxième serveur. Mais je devais utiliser obligatoirement l'application A.L.C.A.S.A.R.



Deux plateformes <u>Linux</u> était possibles avec « SAMBA » et « SQUID ». Mais la mise en place de stratégies de groupe se fait uniquement sous une plateforme Windows.



Une plateforme <u>Windows</u> et <u>Linux</u> convenait tout à fait aux attentes et aucune autre contrainte ne s'opposait alors à la mise en place du projet.

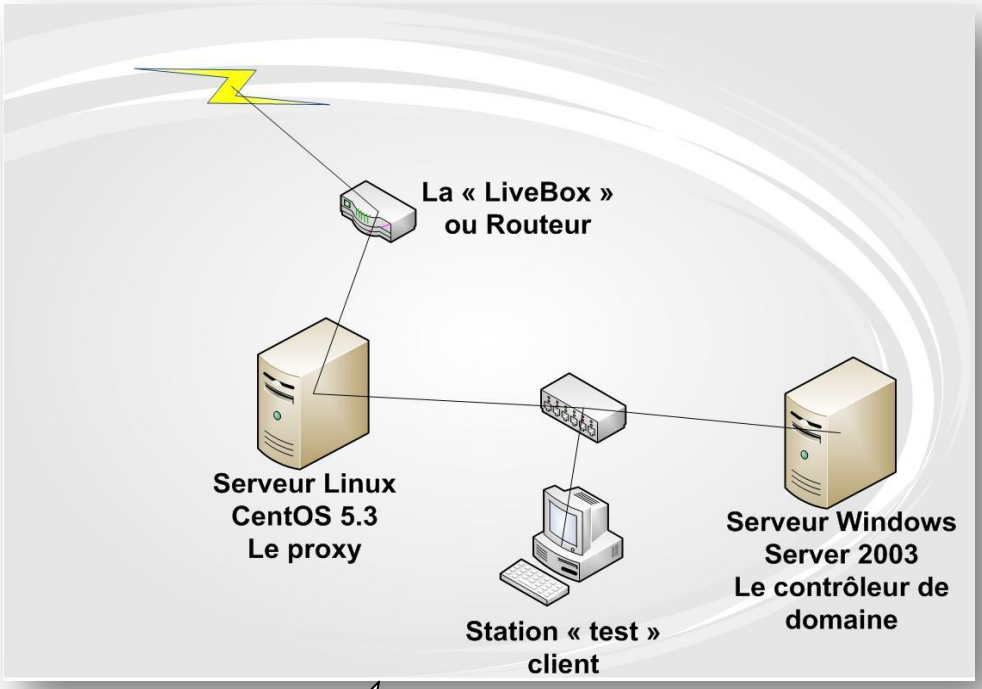
Donc il m'était impossible de préparer les deux serveurs à ma disposition sous un même système d'exploitation.

(Pour le projet, il n'y avait aucune contrainte de coût car des licences Microsoft étaient disponible et les administrateurs réseaux s'occupant de la maintenance pouvaient intervenir sous ces deux environnements)

III. Mise en œuvre de la solution retenue

Initialisation du projet

Pour débuter le projet, je ne devais pas perturber les utilisateurs dans leurs travaux et consultations sur le web. Pour cette raison, il était nécessaire de simuler l'environnement futur sur 3 machines (2 serveurs + 1 client). Je devais donc rester sur un réseau fermé avec une connexion Internet pour réaliser tous les tests nécessaires. Cela a nécessité trois adresses DNS, deux pour la connexion au Fournisseur d'Accès Internet dont le domaine est « oleane.net » et une pour la connexion au contrôleur de domaine (un serveur DNS est à mettre obligatoirement en place pour créer un nouveau contrôleur de domaine). J'ai commencé tout d'abord par installer 2 serveurs et 1 poste « test » client sur mon emplacement de travail.



Ce schéma réseau représente mon plan de travail.

1 Mise en place du contrôleur de domaine

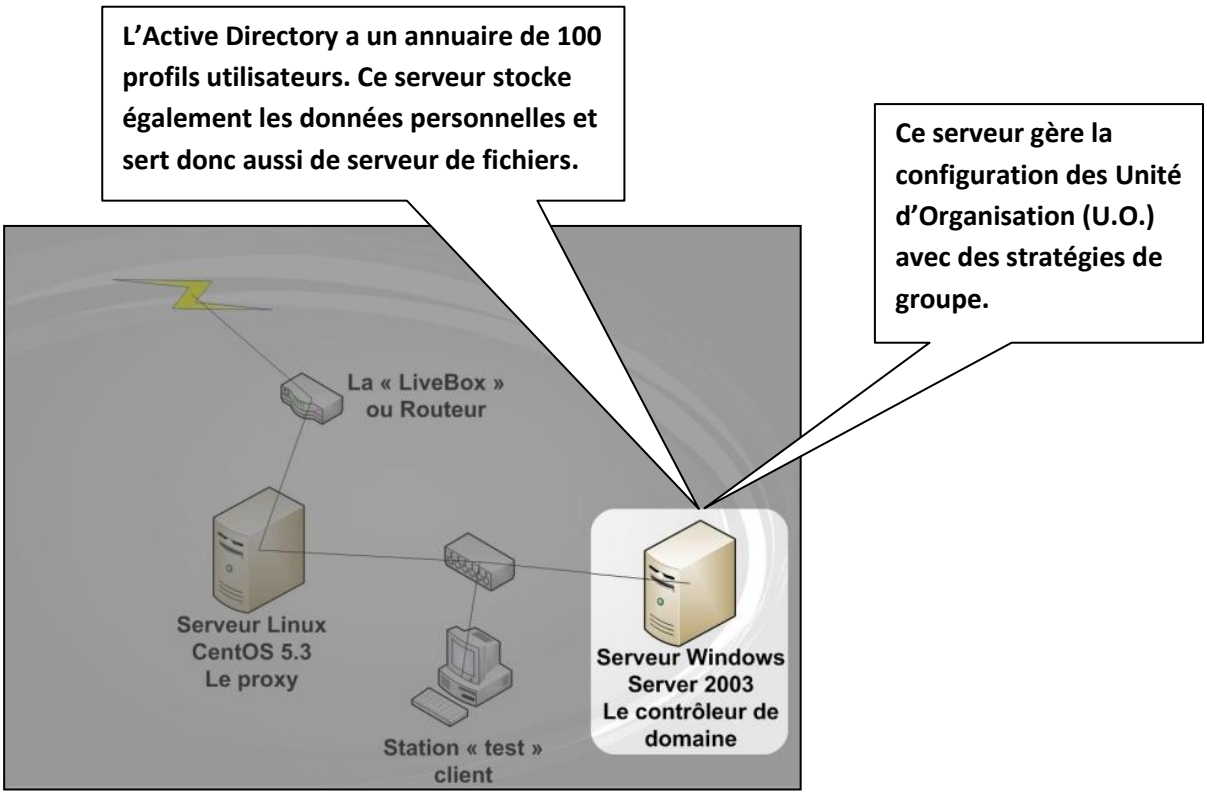
Pour le serveur contrôleur de domaine, dont le rôle est de gérer les comptes utilisateurs j'ai initialisé des produit de base Windows Server 2003 Service Pack 1. Lors de son installation, des pilotes étaient manquants pour un des composants de la machine. Les drivers des connexions « SCSI » de la carte « ADAPTEC » ont été immédiatement transférés sur une disquette grâce au CD d'installation de cette carte.

- **Annuaire du C.E.D.I.M.A.T. - Active directory**

Ici le serveur a joué le rôle de contrôleur de domaine. Grâce à la commande « DCPROMO » qui a permis de conduire à l'assistant d'installation de « l'Active Directory », le contrôleur de domaine a été paramétré suivant une configuration recommandée par Windows Server 2003.
Des comptes utilisateurs étaient déjà créés sur chaque poste Internet existant ; j'avais envisagé un transfert des annuaires des 14 postes sur le nouveau contrôleur de domaine. Cependant, les commandes « LDIFDE » et « CVCDE » ne fonctionnaient pas parce qu'il y avait une incompatibilité des versions Windows (Server 2003 SP1 / XP SP3). Donc, les comptes ont été créés manuellement car il n'y avait que 100 utilisateurs à créer mais un script aurait été une solution possible.

- **Les profils itinérants**

Des profils itinérants pour les utilisateurs ont été également créés dans leur dossier partagé personnel : les membres du C.E.D.I.M.A.T. sont maintenant chacun propriétaire de leur dossier profil. Ils ont accès uniquement à leur dossier lorsqu'ils se connectent à leur session d'utilisateur.

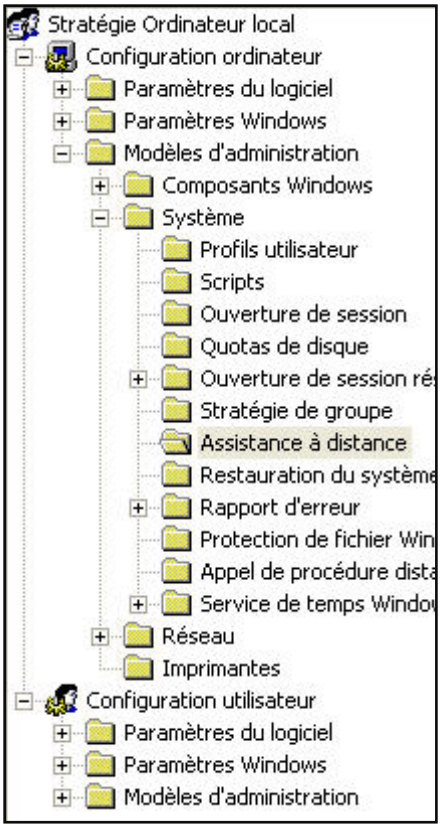


- **Serveur de fichier - racine « Distributed File System » (DFS)**

Ce serveur sert également de stockage pour les données des utilisateurs ; c'est-à-dire que des dossiers ont été partagés sur le réseau pour les 14 postes. Il a été nécessaire de créer un dossier pour chaque utilisateur ce qui a représenté en globalité une centaine de dossiers partagés. Les propriétés sur les sécurités des dossiers ont été paramétrées de façon à ce que l'utilisateur puisse seulement « créer », « lire » et « modifier » le contenu de son répertoire personnel et qu'il en soit le propriétaire.
Pour encore plus de sécurité, une « racine DFS » est créée en prévention d'une éventuelle panne ; c'est un moyen simple d'accéder à des données réparties et distribuées sur un réseau. Cela a servi de point d'accès aux dossiers du réseau. Les utilisateurs devaient avoir accès uniquement à leur dossier lors de la connexion à leur session.

- **Stratégies de groupes**

Nous avons structuré par la suite la liste des utilisateurs et des ordinateurs « Unité d'Organisation » (U.O.). Ces dernières peuvent contenir des groupes, des utilisateurs, des ordinateurs ou d'autres U.O. Elles étaient nécessaires pour mettre en place des stratégies de groupes



J'ai donc paramétré au total 4 GPO (Group Policy Object) :

- Activation des profils itinérants
- Quotas maximum sur les profils des utilisateurs
- Paramétrage d' « Internet Explorer » pour le Proxy
- Extraction du dossier « Mes documents » du profil

- **La gestion des quotas**

Les dossiers « profil » ont été limités en taille (au maximum de 30 Mo) afin que le dossier « mes documents » puisse accueillir un volume plus conséquent. Grâce à la stratégie de groupe, nous avons pu transférer ce dossier à la racine du dossier personnel des utilisateurs et donc il n'était plus limité en taille ; cette action a été bien évidement transparente à l'utilisateur. Puis, pour un partage équitable du volume sur le disque, la gestion des quotas a été activée sur les dossiers personnels ; une limite de 5 Go et une alerte à 4.5 Go ont été définies.

Le contenu des dossiers profils sont mis en place lors de la première utilisation de la session pour les utilisateurs. Pour finaliser la configuration du serveur, il a été installé un antivirus nommé « Office Scan ».

2 Mise en place du serveur Proxy SQUID

Pour commencer, sur le serveur jouant le rôle de proxy, il était nécessaire d'avoir deux cartes réseaux avant que le Système Exploitation soit installé ; donc une deuxième carte a été insérée sur la machine. Un **serveur mandataire** a plusieurs fonctions :

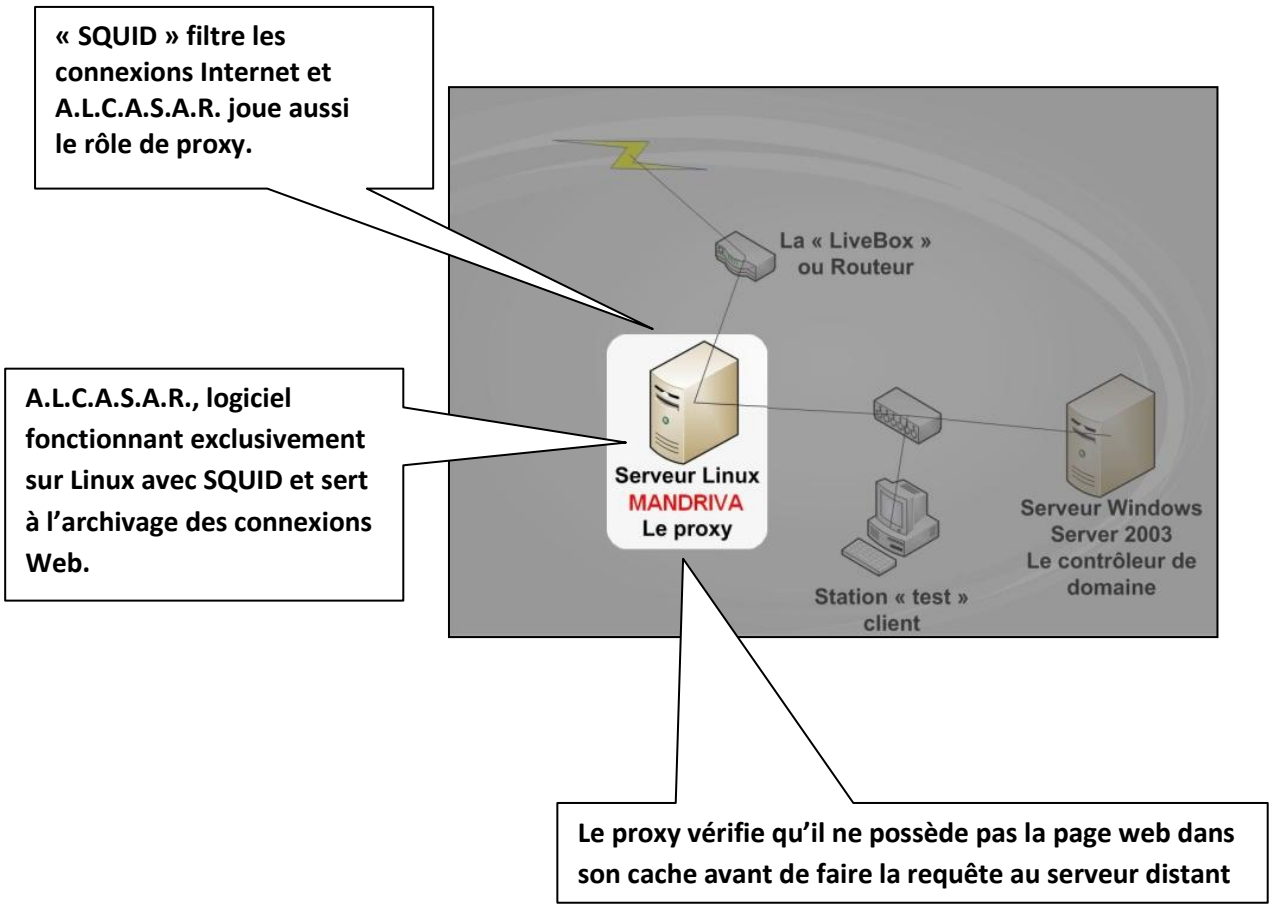
- La mise en cache d'élément pour limiter l'utilisation de la bande passante (débit sur le réseau) et accélérer l'accès aux pages web (proxy cache)
- Le partage et la centralisation d'une connexion INTERNET
- Le filtrage des données (proxy filtre)

- **Linux « MANDRIVA 2009»**

Il a été initialisé Linux free MANDRIVA 2009 avec un partitionnement adapté aux besoins du C.E.D.I.M.A.T. Au total 5 partitions ont été créées, une « SWAP », une « / », une « /TMP », une « /HOME » et une « /VAR ». Ce partitionnement m'était imposé par le C.E.D.I.M.A.T.. SQUID était déjà intégré dans la distribution MANDRIVA, il n'y avait donc pas à le rajouter (il faut savoir que sous d'autres distributions tel Linux UBUNTU il faut le télécharger).

- **Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau**

J'ai installé ensuite un logiciel s'initialisant exclusivement sur Linux et faisant partie de la distribution « MANDRIVA », l'application « ALCASAR ».

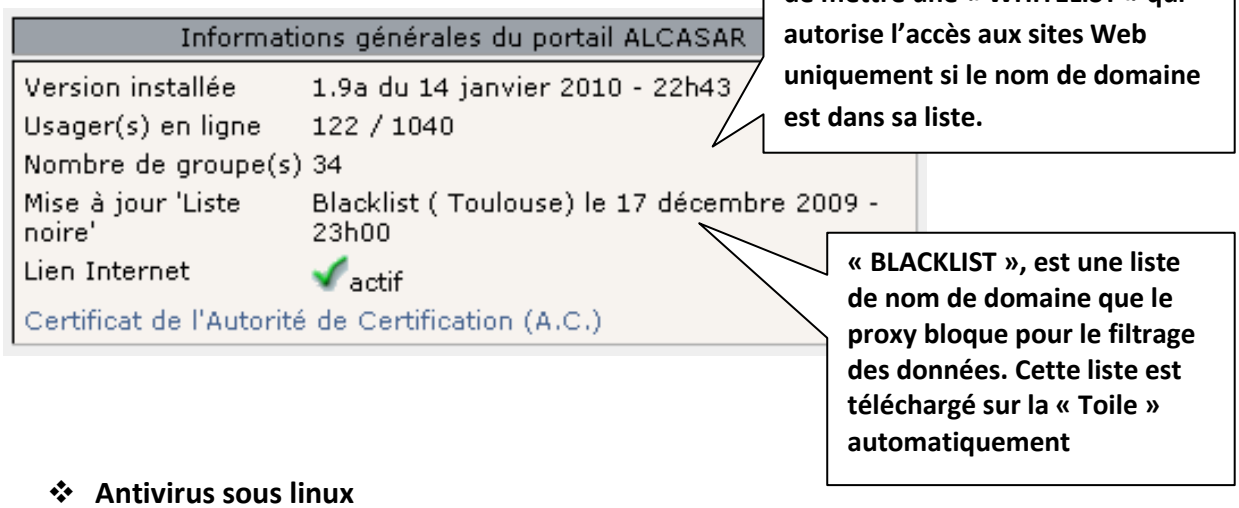


« ALCASAR » est un Logiciel gérant l'archivage des connections effectuées et la traçabilité de celles-ci ; il possède un rôle secondaire qui est celui de « Proxy ». Lors de son installation qui se déroula en ligne de commande (pas de mode graphique), celui-ci a mis en erreur le Système d'Exploitation car il désinstalla une multitude de packages pour en installer de nouveaux inattendus.
Nous avons alors téléchargé et installé une nouvelle version de Linux MANDRIVA 2009.
« ALCASAR » s'initialisa ensuite correctement tout en refaisant la même manipulation sur les packages.

Sa configuration a lieu en mode graphique via un navigateur (le serveur Linux est donc serveur WEB sous « APACHE»). Cependant, il y a bien évidement un login et un mot de passe « d'administrateur » à fournir.

- **Paramétrage « A.L.C.A.S.A.R. » et « SQUID » (Proxy)**

Le proxy sur Linux étant « SQUID », son fichier de configuration « SQUID.CONF » a été modifié pour l'accès au Web (Il existe des « BLACKLIST » et des « WHITELIST » gérés sous « ALCASAR »). Il est configuré pour bloquer l'accès Internet aux utilisateurs qui ne seraient pas authentifiés et qui n'appartiendraient pas au réseau. Des adresses « DNS » ont été attribuées manuellement afin d'avoir une communication avec le routeur Internet, et, en même temps avec le contrôleur de domaine. Une mise en place de listes « d'URL » a été réalisée afin de les autoriser à passer sans authentification comme les mises à jour de l'antivirus ou de Windows par exemple.



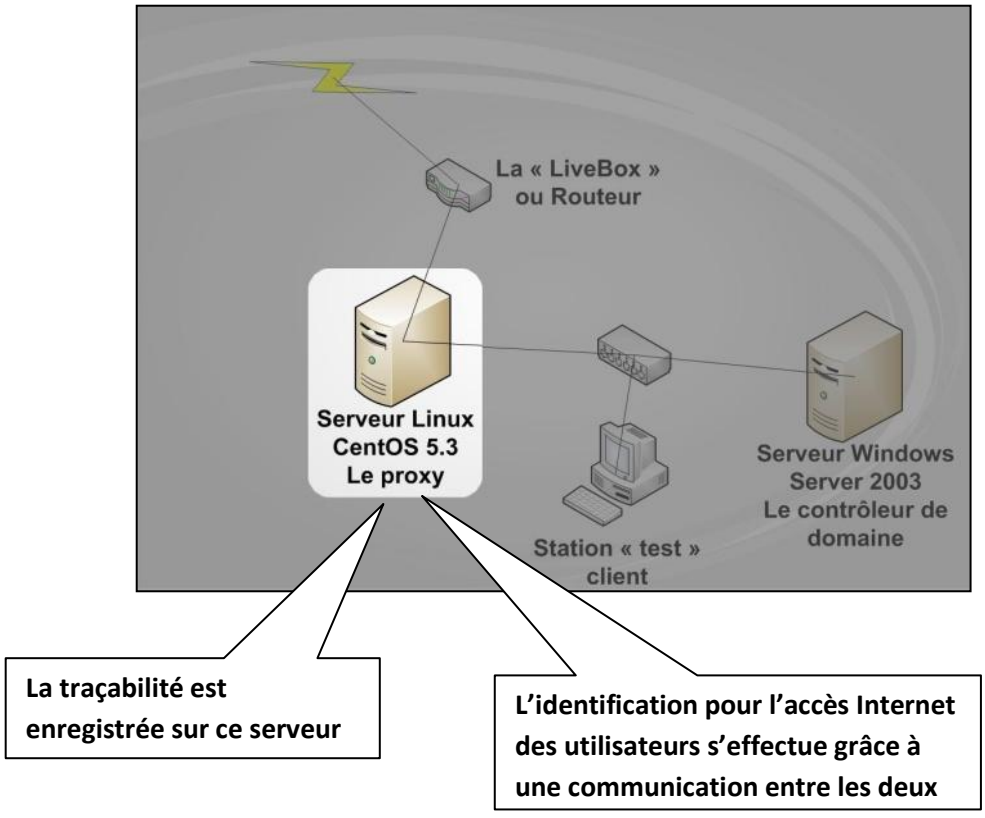
- **Antivirus sous linux**

Ensuite, lors de l'installation de l'antivirus « Server Project », conseillé sur le réseau Intranet, un problème est survenu. Cette application a été créée uniquement pour la distribution de Linux « RED-HAT » et le noyau du Système d'Exploitation ne correspondait pas avec celui que nous possédions. Nous avons décidé alors d'installer l'antivirus « CLAMAV » mais l'initialisation « d'ALCASAR » a désinstallé dans les packages l'option de compilation.

- **Changement de la solution Initiale**

Suite à l'installation de l'antivirus, nous avons remarqué que sur les postes de consultation des utilisateurs, lorsqu'ils voulaient aller sur Internet, devaient renseigner une seconde fenêtre d'authentification et cela n'était vraiment pas pratique. Il était donc nécessaire de rendre cette authentification transparente pour l'utilisateur et également d'attribuer une garantie de sa traçabilité.

Nous avons donc réalisé ensuite une étude qui consistait à trouver un système permettant d'aller chercher l'utilisateur dans l'annuaire de l'Active Directory et de faire sa comparaison avec son mot de passe, de manière invisible pour l'utilisateur.
Après avoir trouvé une solution adéquate qui nous faisait avoir une transparence de l'authentification et un seul annuaire, nous devions développer une autre architecture où l'identification de la connexion Internet se faisait par l'ouverture de la session de l'utilisateur.



Nous avons décidé alors de prendre une autre distribution de Linux, la « CENTOS », qui descend de la « RED-HAT » et d'abandonner totalement le logiciel «ALCASAR » puisqu'il ne répondait pas aux exigences attendues.

- **Linux « CENTOS »**

Le partitionnement réalisé a été identique à la version Linux MANDRIVA 2009 pour l'installation de Linux « CENTOS 5.3».

Puis, des recherches sur Internet nous ont permis d'obtenir des tutoriels pour la configuration des fichiers « .CONF ». Les fichiers de configuration de «SAMBA », «KERBEROS», «WINBIND» et «SQUID» ont été adaptés et modifiés à la version Linux « CENTOS » et aux exigences attendues.

❖ **« WINBIND » et « KERBEROS »**

«WINBIND »a servi à joindre le serveur Linux « CENTOS » au domaine sous « Windows Server 2003 », afin d'authentifier le système d'exploitation. Il était désormais possible de conserver des comptes utilisateurs sur le premier serveur. La synchronisation entre les deux machines se faisait automatiquement, d'où résultait une plus grande facilité de gestion des comptes.
«KERBEROS» est un protocole de sécurité utilisé par « SAMBA » et « Windows Server 2003 ». Donc par le biais de WINBIND, il s'effectuait une authentification par rapport à « l'Active Directory ». Elle est transparente pour l'utilisateur et permet également de l'identifier pour la traçabilité mise en place.

❖ **« SQUID »**

Le Proxy «SQUID» a été également remis pour bloquer l'accès Internet aux utilisateurs qui ne seraient pas authentifiés ou qui n'appartiendraient pas au réseau. Il devait néanmoins autoriser l'antivirus des machines clientes à télécharger les mises à jour sans qu'ils s'authentifient.

LOG de SQUID d'une station allant sur msn.com et www.google.com :

```
1245190910.038   2801 192.168.10.254 TCP_MISS/200 7347 GET http://runonce.msn.co
m/images/tabbed-2.png - DIRECT/213.199.181.20 image/png
1245190910.689   2901 192.168.10.254 TCP_MISS/200 7852 GET http://runonce.msn.co
m/images/advanced-printing.png - DIRECT/213.199.181.20 image/png
1245190910.989    947 192.168.10.254 TCP_MISS/200 623 GET http://runonce.msn.com
/images/bg_ylo_bot_1px.gif - DIRECT/213.199.181.20 image/gif
1245190911.419   3057 192.168.10.254 TCP_MISS/200 7800 GET http://runonce.msn.co
m/images/tighter-security.png - DIRECT/213.199.181.20 image/png
1245190912.548   1855 192.168.10.254 TCP_MISS/200 3788 GET http://runonce.msn.co
m/images//bg_def3fa_curve_leftbot.png - DIRECT/213.199.181.20 image/png
1245190912.577   4494 192.168.10.254 TCP_MISS/200 7628 GET http://runonce.msn.co
m/images/easier-search.png - DIRECT/213.199.181.20 image/png
1245195570.566   1095 192.168.10.254 TCP_MISS/200 665 GET http://m.webtrends.com
/dcsjwb9vb00000c932fd0rjc7_5p3t/dcs.gif? - DIRECT/63.88.212.184 image/gif
1245195583.094   1675 192.168.10.254 TCP_MISS/302 586 GET http://www.google.com/
 - DIRECT/74.125.43.99 text/html
1245195584.348   1194 192.168.10.254 TCP_MISS/200 3830 GET http://www.google.de/
 - DIRECT/74.125.43.103 text/html
1245195586.466   1579 192.168.10.254 TCP_MISS/204 291 GET http://clients1.google
.de/generate_204 - DIRECT/74.125.43.113 text/html
1245195587.540   3181 192.168.10.254 TCP_MISS/200 25214 GET http://www.google.de
/logos/stravinsky09.gif - DIRECT/74.125.43.103 image/gif
1245195588.289    745 192.168.10.254 TCP_MISS/204 381 GET http://www.google.de/c
si? - DIRECT/74.125.43.103 text/html
_
```

❖ **WEBALIZER**

Les calculs des statistiques et la traçabilité des utilisateurs peuvent être consultés par un logiciel s'intitulant «WEBALIZER». Celui-ci permet à l'administrateur d'avoir une interface graphique pour consulter ces résultats (Nécessité d'avoir un serveur «APACHES»). Les statistiques concernant un utilisateur ne peuvent être consultées sans avoir eu l'autorisation de la personne, en raison des droits de la «CNIL» (Avant la mise en place de ce réseau, les utilisateurs ont été informés que la traçabilité était maintenant effective lors de leur navigation sur Internet).

La traçabilité a été enregistrée en «LOG» avec sauvegarde programmée une fois par jour. Ces fichiers sont conservés avec un délai de 52 semaines, selon le décret en vigueur. Ces documents constituant un volume assez important, nous avons donc conçu une compression des «LOG» toutes les semaines.

Le C.E.D.I.M.A.T. ne m'a pas autorisé à prendre un exemple de traçabilité des comptes utilisateurs, pour des raisons de confidentialité.

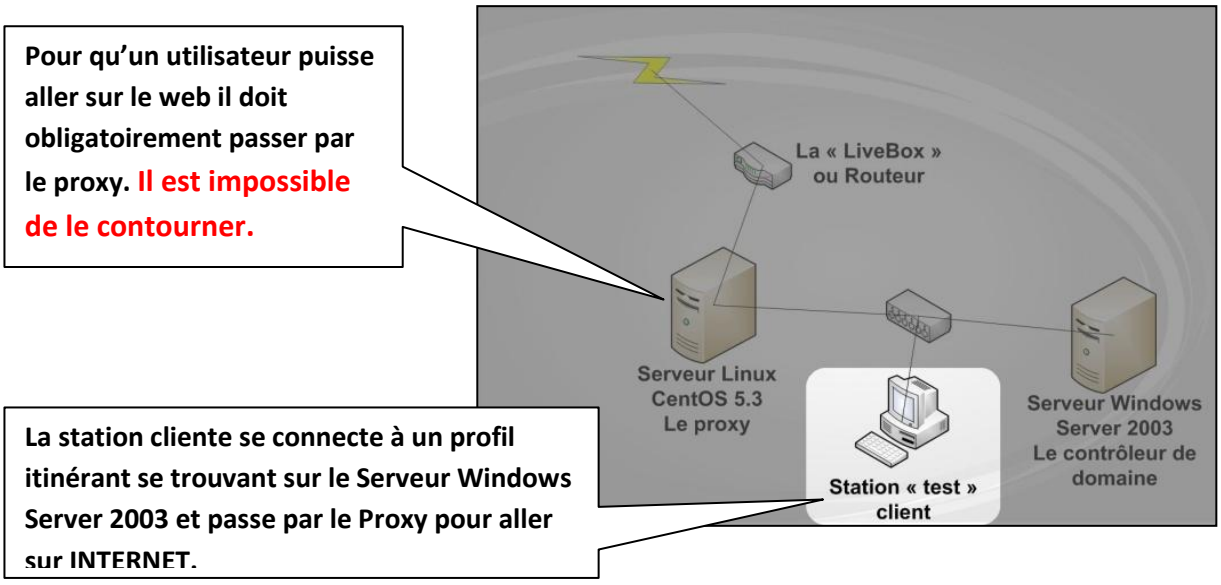
3 Installation d'une station Internet

- **configuration du poste et son paramétrage réseau**

Sur le poste « test » client, il a été installé le Système d'Exploitation Windows XP avec le Service Pack 3. Il a été nécessaire de modifier simplement la configuration IP, DNS et la passerelle car l'adressage se fait, non pas avec un « DHCP » mais de façon « statique ».

Les propriétés du système ont aussi été changées afin que le domaine soit enregistré sur l'ordinateur. Lors de la connexion des utilisateurs, leur profil se charge immédiatement, ainsi ils peuvent profiter de l'ensemble de leurs documents et cela sur n'importe quel poste connecté au réseau Internet. Dans le navigateur Internet, il a été nécessaire d'inscrire dans les paramètres de connexion, l'adresse du proxy (adresse IP du serveur Linux) et son port dédié. En étant connecté à une session d'utilisateur, la connexion à Internet s'est faite de manière transparente sur les 2 navigateurs de l'ordinateur (Internet Explorer et FIREFOX).

Le serveur mandataire était donc transparent pour tous les utilisateurs.



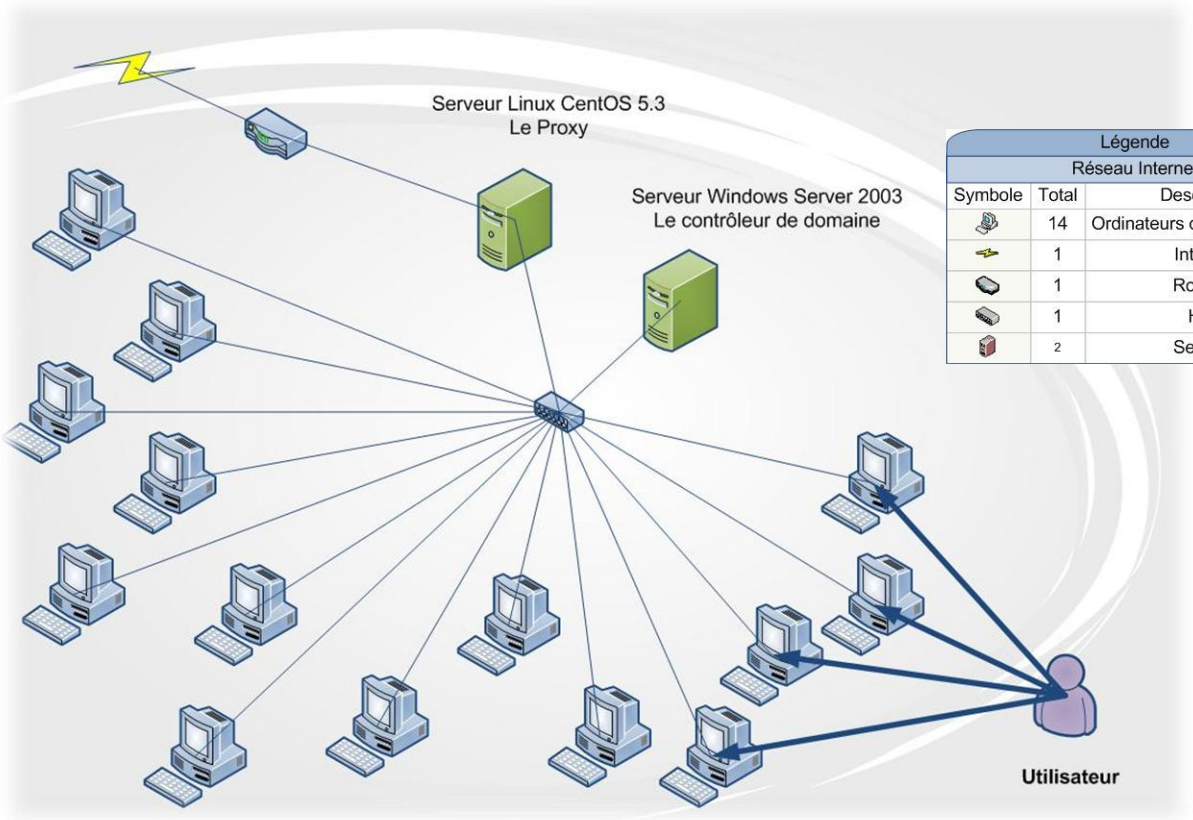
- **« GHOST » du poste test**

Après l'installation de divers logiciels et utilitaires, une image du poste « test » client a été créée. Cette machine a été configurée de telle sorte qu'une image de celle-ci soit projetée ensuite sur seulement 8 nouveaux ordinateurs en remplacement des anciens. Les 6 ordinateurs restants ont eu des modifications au niveau de l'intégration au domaine et de leur nom. L'image a été réalisée grâce au logiciel « Drive Image » se trouvant sur 2 disquettes.

Pour terminer, la dernière protection antivirus est le logiciel « PC CILLIN » qui peut effectuer ses mises à jour sans passer par une authentification d'utilisateur. Celles-ci ont été installées individuellement sur chaque poste Internet.

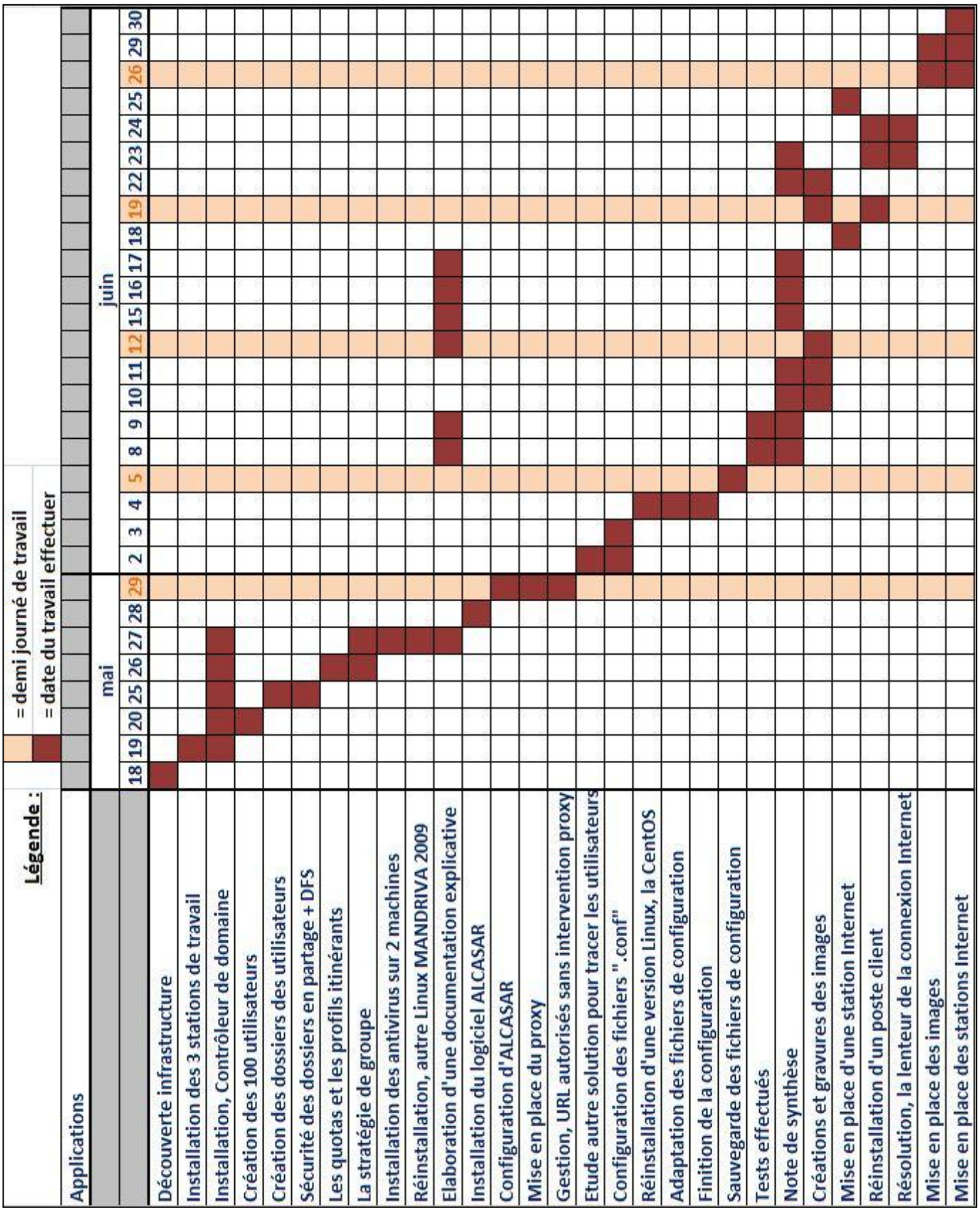
Schéma du Projet à la fin du stage :

Réseau Internet du C.E.D.I.M.A.T. le 30/06/2009



Légende		
Réseau Internet		
Symbole	Total	Description
	14	Ordinateurs de consultations
	1	Internet
	1	Routeur
	1	Hub
	2	Serveur

Le diagramme de « GANTT »



IV. Problèmes et solutions

Problèmes rencontrés :

Premier problème rencontré : Installation du serveur avec Windows Server 2003 ; les drivers pour les connexions SCSI sont manquants et aucun package sur le Web ne fonctionne.
Résolution du problème : Transfert des drivers SCSI du CD d'installation de la carte ADAPTEC à une disquette pour l'installation sur le serveur Windows Server 2003.

Deuxième problème rencontré : Impossibilité de transférer les utilisateurs créés sous les postes des stations Internet pour les mettre sur la machine Windows Server 2003.
Résolution du problème : Création des 100 comptes utilisateurs manuellement sur Windows Server 2003 car les commandes « LDIFDE » et « CVCDE » ne fonctionnent pas, un script VB aurait pu être créé pour l'édition automatique des comptes.

Troisième problème rencontré : Les profils itinérants étant créés, ils sont limités en taille à 30 Mo. Il a été nécessaire de placer les documents des utilisateurs dans un dossier à part entière au même titre que le dossier profil. La station cliente ne trouve pas la destination donnée pour le nouveau dossier contenant « mes documents ».
Résolution du problème : L'option a du être activée dans la stratégie de groupe qui est d'exclure un répertoire.

Quatrième problème rencontré : Concernant le serveur sous Linux MANDRIVA, l'antivirus « Server Project » n'est pas compatible avec le noyau de l'OS installé et l'antivirus est destiné pour des S.E. Linux « RED-HATE ».
Résolution du problème : Le système d'exploitation a reçu l'antivirus « CLAMAV ».

Cinquième problème rencontré : La version de Linux MANDRIVA 2009 installée est incompatible avec le logiciel « ALCASAR » ; lors de l'installation de celui-ci, le logiciel a fait « planter » le S.E.
Résolution du problème : Installation d'une autre version de Linux MANDRIVA 2009 correspondant mieux à « ALCASAR ».

Sixième problème rencontré : « ALCASAR » a supprimé des packages lors de sa mise en place et donc l'installation de l'antivirus « CLAMAV» n'a pu se faire car la compilation était impossible.
Résolution du problème : Les packages manquant sont téléchargés, l'antivirus est installé et un scan toute les heures est programmé.

Septième problème rencontré : Lors de l'authentification pour une connexion Internet un utilisateur devait faire plusieurs clics en plus, et se loguer une seconde fois.

Résolution du problème : abandon du logiciel « ALCASAR », pour une solution sous le S.E. Linux « CENTOS 5.3 ».

Huitième problème rencontré : Pas de « PING » sur les machines alors que les adresses IP attribuées en statique sont correctes.

Résolution du problème : il suffit simplement de désactiver les services concernant le « pare feu ».

Neuvième problème rencontré : Multitude de problèmes rencontrés sur les fichiers de configurations « conf ».

Résolution du problème : Etude des problèmes grâce à des tutoriels et des forums sur le web.

Dixième problème rencontré : Impossible de graver l'image du poste « test » client.

Résolution du problème : Le problème vient du système de fichier, « NTFS » ; celui-ci ne convient pas, nous avons formaté la partition en « FAT32 ».

V. Le droit à la traçabilité

Le Décret 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques.

Les données doivent être conservées pendant un an à compter du jour de leur enregistrement. La nature des données de connexion est également à conserver. Tout organisme public qui offre une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau doit tracer ses utilisateurs. L'obligation ne vise que les « données de trafics » définies par le décret comme étant « des informations rendues disponibles par les procédés de communication électronique ». Donc celles-ci peuvent être enregistrées en des « logs de connexion ». Pour mettre en place l'application de ce décret, il faut penser aux droits des usagers de la connexion.

Commission Nationale de l'Informatique et des Libertés, une autorité administrative indépendante française que l'Armée de Terre se doit de respecter. Avant de mettre en place le projet, les utilisateurs des postes Internet devront être prévenus que tous les accès à INTERNET seront enregistrés dans un cadre juridique. La sauvegarde de l'ensemble des « LOG » ne sera accessible qu'à l'administrateur réseau de l'établissement. La lecture de ces enregistrements est interdite pour tous, y compris l'administrateur réseau, seule une dérogation juridique peut permettre cela.

Tous les « LOG » enregistrés ne peuvent être lu uniquement pour des raisons juridiques par des référés

Conclusion :

En raison de la C.N.I.L., toutes les personnes travaillant dans le C.E.D.I.M.A.T. ont été obligatoirement prévenues qu'une nouvelle solution du réseau Internet est mise en place et que cette architecture enregistre tous les accès au Web.
Désormais, le C.E.D.I.M.A.T. dispose d'un réseau Internet sur lequel toutes les connexions au Web sont automatiquement tracées et enregistrées pour une période de 52 semaines, comme la loi l'exige. Aujourd'hui, la gestion des utilisateurs est devenue plus simple pour l'administrateur du réseau. L'utilisateur a maintenant un profil itinérant qui lui permet de retrouver son environnement sur n'importe quel poste lié à sa division et toutes ces modifications apportées sont transparentes pour lui.