République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/MIRA de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de Cycle

En vue de l'obtention d'un Master professionnelle en Informatique

Option

Administration et Sécurité des Réseaux
ASR

Thème

Réseau Social de communication Surveillance domestique des mineurs.

Présenté par :
M^{elle} **BELMEHDI Dania** M^{elle} **BROURI Amel**

Devant le jury composé de :

Président	M^{r} **SAADI Mustapha**	**Enseignant Permanent**
Examinateur	M^{r} **BAADACHE Abderrahmane**	**Enseignant Permanent**
Examinatrice	M^{elle} **BENMARBI Samah**	**Doctorante LMD en Informatique**
Encadreur	M^{r} **TOUAZI Djoudi**	**Maître Assistant**

Promotion 2014/2015

⁂ ⁂ ⁂⁂ *Remerciements* ⁂ ⁂ ⁂⁂

Nous souhaitons vivement remercier notre encadreur Monsieur TOUAZI Djoudi pour l'assistance qu'il nous a témoignée, pour sa disponibilité, son orientation et conseils sans lesquels ce travail n'aurait pas vu le jour, qu'il trouve ici l'expression de notre gratitude.

Nous souhaitons également remercier Mme SALAMI qui nous a orienté dans la réalisation de notre projet.

Nous remercions tout particulièrement les membres de jury qui ont accepté de juger notre travail.

Enfin, Nous remercions aussi toutes nos familles respectives et tous nos amis et collègues qui nous ont soutenus. Ainsi que tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

⁂ ⁂ ⁂⁂ *Dédicace* ⁂ ⁂ ⁂⁂

Je dédie ce modeste travail,

A la mémoire de mes très chers parents,
A ma chère Tata Fadila,
A mon cher grand frère Elias et sa fiancée Lydia,
A mes valeureuses petites sœurs Sara et Katia,
A toute la famille,
A mes meilleures amies Farida, Lydia, Fiika, Meriem,
A mon binôme et à toute sa famille
A tous mes amis,

BELMEHDI Dania

⁂ ⁂ ⁂⁂ *Dédicace* ⁂ ⁂ ⁂⁂

A ce qui est toujours mon meilleur exemple dans la vie : mes très cher parents, pour les sacrifices qu'ils ont consentis pour mon éducation et pour l'avenir qu'ils n'ont cessé d'offrir.

Au symbole de douceur, de tendresse, d'amour et affection : ma mère. A mes très chers frère et sœurs : Tayeb, Houda et Nassrine.

A mes oncles : Larbi, Khelifa, Lyes, Abdenour, et leurs familles, cousins et cousines. A ma belle famille.

A ceux qui m'ont crée un milieu d'ambiance : mes amies : Seline, Nabil, Asmaa, Fahima, Nadjim, Hamza, Nassim.

A mes amis de l'association Raj, et l'école de musique l'association Naciria

A Ma binôme Dania et sa famille.

A toute la promotion informatique 2015

BROURI Amel

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

Admin : Administrateur.

Apps : Applications.

DHCP : Dynamic Host Configuration Protocol.

DMZ :zone démilitarisée.

DNS :Domain Name System.

IDS :Intrusion Detection System.

LAN : Local Area Network.

NAT : Network Address Translation.

RPV : Réseau privé virtuel.

SSH :Secure Shell.

WAN : Wide Area Network.

Wow : World of Warcraft.

Introduction générale

Dans n'importe quelle structure, mettre en place une architecture du réseau informatique est indispensable pour le bon fonctionnement et la communication entre les équipements le composant, mais cela ne suffit pas. La partie la plus importante et sensible est sa sécurité et surveillance. Superviser son réseau cela permet d'avoir une vue globale de son bon fonctionnement et d'anticiper les éventuels problèmes (failles).

De nos jours, les réseaux domestiques sont de plus en plus vulnérables. La réflexion à la mise en place d'une politique de sécurité est nécessaire : le contrôle parental.

Le grand défi des parents est de protéger leurs enfants d'Internet qui surfent librement sans surveillance et sans protection. Alors comment faire pour protéger ses enfants pour qu'ils ne tombent sur des sites inappropriés et interdit ?

De nombreux systèmes et outils existent pour justement répondre à cette question que tout le monde se pose. Il suffit de l'intégrer au système et de le surveiller.

•Problématique et objectif : Ce présent travail a pour but de mettre en place une surveillance sur un réseau domestique, qui permettra aux parents de mener à bien la surveillance de leur réseau, notamment leurs enfants.

•Présentation des chapitres :

Le mémoire est organisé en 4 chapitres :

Dans le premier chapitre, nous donnons quelques concepts et notions liés aux réseaux et la surveillance.

Le deuxième chapitre, nous avons fait une étude des existants.

Le troisième chapitre, nous avons présenté l'outil de surveillance IP Cop.

Le quatrième chapitre expose la configuration d'IP Cop et quelques scénarios.

Une conclusion et perspectives termine le mémoire.

Chapitre I

Généralités

I.1 Introduction

Dans ce chapitre, nous aborderons les différents concepts liés aux réseaux et surveillance en donnant quelques généralités.

I.2 La surveillance

I.2.1 La définition de la surveillance

En informatique, la supervision est une technique de suivi qui permet de surveiller, analyser, rapporter et d'alerter les fonctionnements normaux et anormaux des systèmes informatiques.[1]

Elle consiste en outre à indiquer et/ou commander l'état d'un serveur, d'un équipement réseau ou d'un service software pour anticiper les plantages ou diagnostiquer rapidement une panne.

I.2.2 Objectifs

Il est aujourd'hui de plus en plus difficile d'administrer un réseau. En effet le nombre d'équipements à gérer est souvent de plus en plus important : stations, serveurs, imprimantes. Le plus grand souci d'un administrateur est la maintenance des équipements, des systèmes et leur disponibilité. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires.

Il faut pouvoir surveiller de manière continu l'état des systèmes d'information afin d'éviter un arrêt d'activité de trop longue durée. C'est là où la supervision intervient. Elle doit permettre d'anticiper les problèmes et de faire remonter des informations sur l'état des équipements.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils indispensables.

I.3 Réseau local

I.3.1 Définition

Un réseau local est défini comme l'ensemble des ressources télé-informatiques permettant l'échange à haut débit de données entre équipements dans une zone géographique privée (entreprise, hôpital, campus, ...)[2]

I.3.2 Avantages

- Le partage de ressources communes : matériel et logiciel (critère économique).
- Une meilleure fiabilité puisqu'on dispose de plusieurs machines (redondance).
- Les possibilités d'évolution : ajout de machine en cas de besoin.
- Plus d'indépendance vis à vis des constructeurs.

I.3.3 Inconvénients

Ce type d'architecture est plus complexe à mettre en œuvre, les principaux problèmes rencontrés sont :

- Une plus grande difficulté à contrôler l'ensemble du système notamment pour la gestion des ressources.
- La nécessité des mécanismes qui assurent l'intégrité des données et leur confidentialité.
- Les risques d'incompatibilité entre matériels.
- Le coût des équipements supplémentaires de communication (câbles, cartes, logiciels, etc.) et des services (formation).

I.3.4 But d'un réseau local

Le but d'un réseau local est de partager entre membres de la famille, fichiers, photos, films, imprimantes, dossiers et d'installer éventuellement une surveillance vidéo en cas d'absence via une ou plusieurs caméras. Tout ceci étant paramétrable. Le minimum est d'avoir au moins deux ordinateurs reliés en réseau pour partager entre ordinateurs.[3]

I.3.5 Composants et Statistiques

Le marché des réseaux locaux subit une croissance annuelle de 35%, et ce de la façon suivante [2] :

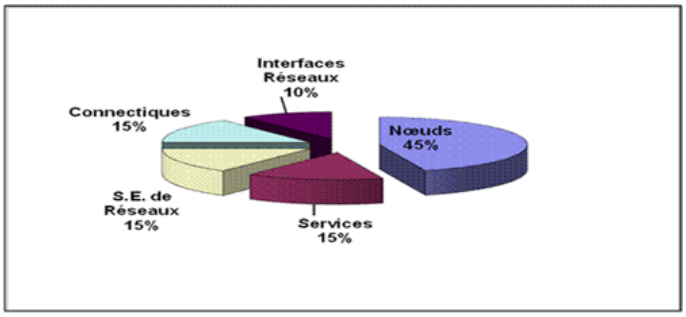


FIGURE I.1 – Composant et statistique des réseaux locaux

a)Nœuds

On distingue :

- Les ordinateurs qui exécutent les applications accessibles depuis les autres micros (serveurs de stockage, d'impression et de messagerie).
- Les serveurs d'interconnexion : ponts, commutateurs, routeurs et passerelles.
- Les micro-ordinateurs.

b)Interfaces Réseaux

Cartes coupleurs permettant la connexion des micros et des stations à un réseau local. Ils assurent la gestion de l'accès à la ligne et la transformation des signaux (tendance vers l'intégration). On ajoute aussi les répéteurs qui permettent de répéter et d'amplifier le signal en reliant les différentes parties du réseau.

b)Les services :

Maintenance des équipements de réseau, conseil et formation des utilisateurs.

c)Les systèmes d'exploitation de réseau :

Windows NT, Linux, Netware de Novell, Lan Manager de Microsoft, etc.

d)Connectiques :

Câbles (cat. 5, coaxial, fibre), prises (BNC, RJ45), panneau de brassage, moulures, armoires, etc.

- Autres : imprimantes, équipements audio ou vidéo, etc.

I.3.6 Caractéristiques d'un réseau local

Un réseau local se caractérise par[2] :

- La courte distance entre les nœuds (<10 km)
- Haut Débit (Une vitesse de transmission élevée : 10 Mbit/s à 10 Gbit/s)
- Un faible taux d'erreur
- La nature privée du réseau
- Des équipements diversifiés : connectiques, média, ordinateurs, périphériques, ...
- La Topologie logique de connexion : bus, étoile ...
- La méthode de partage des accès : droit de parole.
- Format des trames : Plusieurs types d'informations.

I.4 Réseau WAN

un WAN (Wide Area Network) interconnecte plusieurs réseaux LANs à travers de grandes distances géographiques de l'ordre de la taille d'un pays.

Les débits disponibles sur un WANr ésultent d'un arbitrage avec le coût des liaisons et peuvent être faibles.

Les WANs fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un noeud.[4]

I.5 Proxy

- Un proxy est un intermédiaire dans une connexion entre le client et le serveur
- Le client s ?adresse toujours au proxy
- Le proxy est spécifique à une application donnée HTTP,FTP... [5]

I.6 Les réseaux sociaux

Les réseaux sociaux font partie de ce que l'on appelle plus largement les médias sociaux (ou social média) comme le montre bien la figure ci-dessous.

Les médias sociaux englobent tous les outils ou applications qui permettent une interaction entre internautes.

Au sein de cette galaxie des médias sociaux, nous trouverons de nombreuses planètes des outils de publication de textes (blog, wiki), d'échange et de partage (youtube pour les vidéos, slideshare pour les présentations powerpoint), les outils de discussion (skype), de microblog (twitter).[6]

FIGURE I.2 – La galaxie des médias sociaux

I.6.1 Pourquoi considérons-nous que les réseaux sociaux puissent être un danger ?

Les réseaux sociaux peuvent être des dangers pour les enfants à deux titres : ils peuvent être abordés par des prédateurs sexuels et ils peuvent être victimes de harcèlement (injures, photos obscènes...) de la part d'autres mineurs. Cela étant, ces réseaux constituent

des outils intéressants pour se faire des amis, garder le contact avec des connaissances qui déménagent. De plus, l'utilisation de ces réseaux par des pré-adolescents ou des adolescents peut les former à l'utilisation d'outils dont ils vont avoir besoin dans leur future vie professionnelle.[7]

I.6.2 Quels sont les dangers que représentent les réseaux sociaux pour les enfants selon la typologie et comment les en protéger ?

Les principaux dangers sont comme suite :

- Être victime d'un prédateur sexuel.
- Le harcèlement de la part d'autres enfants.
- Le vol d'identité numérique.
- Passer trop de temps.

Le premier danger est réel, mais ne doit pas être exagéré. Il n'y a pas plus de risques de rencontrer un pédophile sur Internet qu'à la sortie de l'école, et il faut savoir que 95 % des enfants qui ont été victimes de violences sexuelles de la part d'un pédophile ont rencontré ce délinquant sexuel dans leur cercle familial, au sens large. Cela étant, le risque existe.

1). Le harcèlement : les réseaux sociaux permettent d'échanger des messages. Certains se servent de ces outils de communication pour insulter leurs contacts ou pour leur envoyer des photos obscènes.

2). Le vol d'identité : ce phénomène comporte plusieurs degrés. Le premier degré est le détournement de photo. Une photo récupérée sur un réseau social du style MySpace ou Facebook peut être modifiée, détournée à l'insu de son propriétaire. Le second degré est le vol pur et simple d'identité. Certains petits malins créent des profils à la place d'autres personnes et se font passer pour elles sur Internet.

3). Passer trop de temps : comme tout outil interactif (le surf, les jeux vidéo...), les réseaux sociaux sont extrêmement chrono-phages. Il est alors tentant pour un enfant d'y consacrer plus de temps qu'à la lecture, à ses devoirs... et surtout de se plonger dans ce genre d'activité au lieu de faire marcher son imagination.[7]

I.6.3 Comment se protéger de ces dangers

- La pédophilie : les réseaux sociaux du type Facebook permettent de préciser les règles de confidentialité de son profil. Par exemple, on peut empêcher toute personne qui ne fait pas partie de son réseau d'amis de nous envoyer un message.

- Le harcèlement : il ne faut pas hésiter à faire comprendre à son interlocuteur qu'il a dépassé les limites lorsqu'il nous envoie des messages à répétition que l'on n'a pas sollicités. Et s'il n'obtempère pas, il ne faut pas hésiter à l'enlever de sa liste d'amis.

- Vol d'identité : il ne faut pas hésiter de temps en temps à rechercher son propre nom sur les moteurs de recherche pour voir les informations qui circulent sur soi sur Internet.

- Le temps passé sur cette activité : là, c'est aux parents d'intervenir et de surveiller discrètement ce que font leurs enfants sur Internet. Pour cela, la meilleure solution reste encore d'installer l'ordinateur dans une pièce commune où la famille peut jeter un coup d'œil sur ce qui se passe.[7]

I.7 Conclusion

Dans ce chapitre, nous avons abordé le thème de la surveillance dans un réseau plus précisément un réseau local. Nous avons vu quelles sont les raisons qui nous à pousser à protéger les enfants du danger des réseaux sociaux et comment leur éviter ces dangers.

Chapitre II

Etat de l'art

II.1 Introduction

Dans ce deuxième chapitre, nous allons présenter le contrôle parental, les catégories et définir quelques logiciels de contrôle parental. Ensuite nous allons faire une comparaison de ces logiciels.

II.2 Contrôle parental

C'est un logiciel que les parents installent sur l'ordinateur que ce soit enfant ou familial, protégé par un mot de passe qui va tourner en permanence dés le démarrage sur la machine.[8]

II.3 Logiciels de surveillance

Pour surveiller les enfants, il n'y a pas mieux que les outils de contrôle parental soient donc les compagnons favoris des parents. Aujourd'hui, le contrôle parental doit faire face à de nouveaux défis et s'exercer sur de nouvelles applications telles que les messageries instantanées, les réseaux sociaux ou les outils multimédias de consultation de contenus.

Le contrôle parental peut être généralement configuré sur 3 niveaux[9] :

1- Possibilité de fixer des limites horaires

2- Possibilité d'interdire l'accès à des sites sensibles du web

3- Possibilité de limiter l'accès à des jeux ou à d'autres logiciels

II.3.1 Possibilité de fixer des limites horaires

Ces limites horaires peuvent être de plusieurs ordres et varient suivant les logiciels de contrôle comme par exemple : Net Addict Free et PC TimeWatch.

Elles peuvent porter sur[10] :

- L'utilisation de tel ou tel logiciel (internet explorer, mozilla, msn messenger, jeux vidéo...)

- L'utilisation de la connexion internet (efficacité très variable suivant notre type de connexion et le logiciel de contrôle parental utilisé)

- L'utilisation de l'ordinateur (l'ordinateur s'éteint automatiquement quand l'enfant a dépassé le temps imparti où quand il est en dehors de la plage horaire autorisée par les parents)

II.3.1.1 PC TimeWatch

a) Description

PC TimeWatch est un programme de contrôle parental d'accès à l'ordinateur. Il nous permet de spécifier pour chaque utilisateur quand et pour combien de temps l'accès à Windows, à Internet et aux applications est autorisé.

Nous définissons les règles d'accès à l'ordinateur tout en laissant l'utilisateur libre de ses choix à l'intérieur des créneaux horaires autorisés. Cette approche désamorce les conflits parents-enfants car une fois les règles horaires acceptées par tous, le PC TimeWatch qui se charge de les faire appliquer.

PC TimeWatch est également adapté à une utilisation en milieu scolaire, éducatif ou professionnel. Le contrôle parental n'implique pas nécessairement l'intrusion dans l'espace privé des enfants.

Il n'est pas un programme "espion" qui enregistre les actions de l'utilisateur. En dehors du temps d'utilisation de Windows et de chaque programme restreint, PC TimeWatch n'enregistre aucune activité utilisateur.[11]

b)Qu'est-ce qui rend PC TimeWatch différent de ses concurrents ?

- Nous n'avons pas à gérer des profils ou des mots de passe séparés.

- PC TimeWatch verrouille vraiment les programmes.

- Il est très sécurisé.
- Son interface utilisateur est beaucoup plus simple.

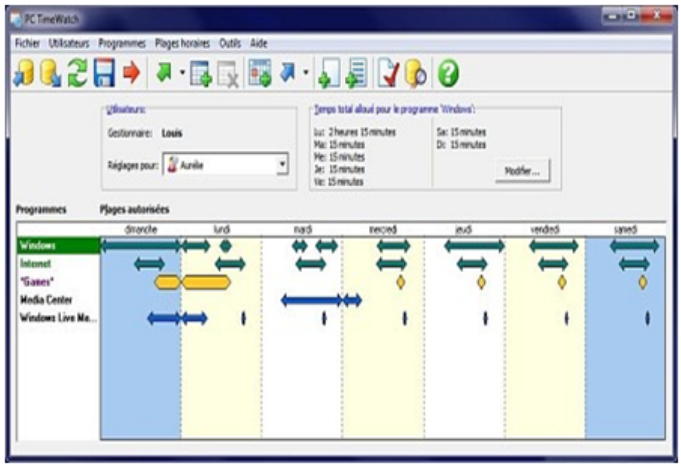


FIGURE II.1 – Interface d'accueil de PC TimeWatch

c)Les points fort de PC Timewatch

- Contrôle automatique du lancement et de la durée d'exécution des programmes via un service spécialisé et un pilote.
- Contrôle de l'accès à Internet via l'interface utilisateur (plages horaires, allocation globale de temps).
- Accès au programme de configuration par mot de passe.
- Réglages, par programme, par utilisateur et par jour, des durées maximum d'utilisation des programmes.
- Accès bloqué à tous les utilisateurs non autorisés par le gestionnaire du logiciel.
- Avertissements configurables (avant la fermeture des programmes, de la connexion Internet ou de la session Windows).
- Statistiques d'utilisation.
- Système de contrôle et de verrouillage de l'heure système.
- Protection contre les tentatives de modification des fichiers de configuration :. [12]

d)Fonctionnalités

PC TimeWatch possède une interface utilisateur très simple et ne perturbe ni le fonctionnement normal du système ni ses performances. En effet, une fois que nous avons

défini les règles, le logiciel se fait complètement oublié. Toutefois, nous nous rappellerons son existence quand les limites seront dépassées.

II.3.1.2 Net Addict Free

a)Description

NetAddictFree facilite la protection parentale en intégrant à la fois des fonctions de contrôle parental et de blocage horaire. Son utilisation est identique sous Windows, Androïd et sur le site internet d'administration à distance, rendant facile sa prise en main par les parents. Toutes les fonctions présentées sont disponibles pour PC windows. Le contrôle parental NetAddictFree ne ralentit pas l'ordinateur ou la navigation Internet.[13]

b)Limiter la durée et les horaires d'utilisation

1) Limiter le temps d'utilisation quotidien ou hebdomadaire de l'ordinateur et de l'Internet : Nous définissons des limitations de temps pour l'ordinateur et pour Internet pour chaque jour de la semaine et/ou pour toute la semaine. Si nos enfants partagent un ordinateur ou une tablette, nous attribuons un temps d'utilisation équitable à chacun et évitons les disputes. Selon les âges ou nos besoins, nous pouvons attribuer des limitations de temps différentes pour chaque enfant.

2)Définir les plages horaires d'accès à certains sites ou programmes et Applications : Nos enfants accèdent à internet pour leurs devoirs scolaires. Pendant cette période ils ne doivent pas aller sur les réseaux sociaux ou messagerie instantanée. Nous limitons facebook ou msn selon des plages horaires que nous maîtrisons. Nous bloquons certains programmes de jeux en réseau tel que wow (World of Warcraft). Ces programmes Windows ou Apps Android ne pourront s'exécuter que dans des plages horaires autorisées. Pendant la durée de leur utilisation, le temps alloué à l'Internet sera décompté.

3)Bloquer l'ordinateur et internet : La nuit, Internet peut être complètement bloquée par le contrôle parental : chaque enfant peut avoir son temps quotidien autorisé d'utilisation d'Internet avec une interdiction totale sur une plage horaire. Par exemple, l'enfant a droit à une heure d'Internet par jour mais une interdiction d'accès entre 21h00 et 7h00 du matin. De même, la session de l'enfant peut être inactivée à certaines heures de la journée avec un temps d'utilisation maximum alloué sur les plages horaires autorisées.[13]

c)Filtre Internet

1)Liste blanche du contrôle parental : Nos enfants doivent aussi pouvoir accéder en toute liberté à certains sites internet pédagogiques. La fonction liste blanche nous permet de définir des sites pour lesquels aucune limitation de temps ou d'accès ne sera imposée. A l'inverse, la liste noire contient un million de sites interdits.

2)Liste noire : Nous pouvons activer le filtrage internet par la liste noire intégrée. Cette liste noire de plus d'un million de sites "adultes" est mise à jour automatiquement.

3)Mots clés : Le contrôle parental NetAddictFree nous permet de définir nos propres mots clés d'interdiction.

d)Statistiques d'utilisation et types de statistiques pour chaque enfant

1)Temps passés sur l'ordinateur et Internet dans son ensemble.

2)Applications et sites consultés :

- Les applications surveillées (pour Windows) et toutes les Apps utilisées sous Android.
- Les sites internet visités.

3)Modes de consultation des statistiques :

- Directement sur l'ordinateur.
- A partir du site d'administration à distance.
- Par email : Nous pouvons régler la fréquence d'envoi des mails de statistiques : tous les jours, une fois par semaine... Nous connaissons pour chaque enfant la durée quotidienne d'utilisation de l'ordinateur et de l'Internet. Nous savons sur quels sites navigue notre enfant avec l'historique détaillé sur les 7 derniers jours et la synthèse des sites visités sur les 30 derniers jours. Ensuite nous déciderons ou non de limiter le temps d'utilisation quotidienne ou hebdomadaire, ou de restreindre l'accès à certains sites internet ou programmes.

e)Administration à distance ou locale

1) Configuration à partir de l'ordinateur de l'enfant :

NetAddictFree pour Windows est configurable directement sur l'appareil de l'enfant. Cela peut contribuer à instituer un dialogue constructif parents/enfants.

2) Configuration à distance :

Si nos enfants nous interdisent l'accès à leur ordinateur, ou si nous ne sommes pas chez nous pour effectuer les modifications de paramétrage, le contrôle parental NetAddictFree intègre la fonction d'administration à distance : par internet, nous intervenons sur les réglages du contrôle parental de nos enfants.

Si nous devons surveiller plusieurs ordinateurs, possédant chacun plusieurs comptes utilisateurs, grâce à l'administration à distance, nous gérons tout à partir d'un seul point d'accès via le site internet de NetAddictFree.

3)Cumul des temps consommés sur plusieurs appareils :

Un enfant utilisant plusieurs ordinateurs, même avec des comptes différents, pourra voir la totalité de son temps comptabilisé et contrôlé par NetAddictFree.

f)Sécurité

1)Mot de passe : Le contrôle parental est protégé par un mot de passe. La connaissance du mot de passe est nécessaire pour modifier les plages horaires et limitations de temps. Sans mot de passe, l'enfant peut suivre sa consommation.

2)Blocage de fonctions d'accès aux paramètres Windows : Pour les adolescents ou enfants experts en informatique, le contrôle parental fonctionne efficacement, même lorsque l'enfant possède un compte administrateur.

Avec le contrôle des fonctions avancées de windows, nous pouvons interdire l'accès au gestionnaire de tâches, à la désinstallation du logiciel ou au panneau de configuration. Notre enfant peut donc être administrateur pour installer librement ses logiciels, sans pouvoir contourner le contrôle parental.

3)Navigateurs supportés : Windows ()Internet Explorer, Chrome, Firefox, Opera :.)

II.3.2 Possibilité d'interdire l'accès à des sites sensibles du web

Le contrôle parental nous permet de filtrer différentes catégories de sites Web en fonction de trois groupes d'âge : 3-7 (enfant), 8-12 (pré-adolescent) et 13-17 (adolescent).

Il y a principalement trois façons de procéder selon les logiciels :

- Interdictions de mots clés : Le logiciel interdit l'accès toute page contenant un ou plusieurs mots clés établis dans une liste (par exemple : sexe, xxx...).

- liste noire : C'est simplement une liste de sites interdits, généralement mise à jour à chaque connexion par le logiciel. C'est évidemment peu sûr, étant donné le nombre de sites

lancés sur le net chaque jour, n'espérons pas avoir une liste exhaustive de tous les sites sensibles par le biais d'un logiciel de contrôle parental.

- Liste blanche : C'est une solution sûre mais très restrictive. Il s'agit de définir une liste des sites autorisés. Tous les sites qui ne figurent pas dans la liste blanche seront bloqués par le logiciel. C'est certainement le mieux à faire pour de jeunes enfants, mais beaucoup trop restrictif pour des collégiens par exemple, qui auront besoin de pouvoir naviguer librement pour faire des recherches, que ce soit pour le collège ou pour leurs loisirs.[10]

II.3.2.1 Control Kids

a)Définition

Control Kids est un logiciel de contrôle parental qui filtre le contenu des sites web inadéquats : la pornographie, la violence, la pédophilie, les sectes. C'est un logiciel compatible avec tout système d'exploitation Windows (win98/Me/XP/Vista/7) et avec tout navigateur Internet (Internet explorer, Firefox, Chrome, Safari, Opera...)[14]

b)Exécution

Control Kids s'exécute de manière transparente près de l'horloge (en bas à droite du bureau). Pour accéder au panneau de contrôle, nous avons besoin de cliquer sur l'icône situé près de l'horloge, Control Kids nous demandera de saisir un mot de passe, qui nous permettra par la suite de désinstaller le programme, accéder à l'administration... nous ne pouvons pas désinstaller le programme par le moyen classique supprimer/désinstaller un programme.[14]

c)Administration et Historique

Control kids est totalement transparent pour l'utilisateur : nous n'avons rien à configurer. Il détecte automatiquement les sites jugés dangereux ou offensants. Aucun paramétrage n'est à faire.

d)Sites web interdits

Lorsque nous naviguerons sur une page interdite, nous verrons alors s'afficher une page de control kids suivante :

FIGURE II.2 – Page de Control Kids

e)Désinstallation le programme

La seule manière est d'appuyer sur le bouton 'désinstaller' à partir du programme. Nous ne pouvons pas le faire de la manière classique.

On ne peut pas ouvrir une nouvelle page avec Internet explorer avec le bouton droit Ceci est dû au fait que Control Kids empêche tout ouverture de nouvelle page (pop ups). Nous pouvons forcer l'ouverture de la nouvelle page en laissant la touche que nous avons choisie précédemment appuyée.

II.3.2.2 Qustodio

a)Description

Qustodio est un outil de contrôle parental conçu pour les parents d'aujourd'hui, très occupés et familiers avec l'Internet. Aucun matériel, aucune installation compliquée ne sont nécessaires, mais juste l'accès à un simple tableau de bord en ligne qui nous permet d'analyser toutes les informations nécessaires en un coup d'œil. Que nos enfants utilisent l'ordinateur familial ou un ordinateur portable personnel. [15]

b)Principales fonctionnalités

- Surveillance : Qustodio permet de savoir sur quels sites internet se sont connectés les personnes surveillées. Il permet aux parents de connaître tous les contacts de leurs enfants sur les réseaux sociaux et les sites de discussion instantanés. Le temps passé sur chaque

FIGURE II.3 – Interface d'accueil de Qustodio

plateforme peut aussi être récupéré.

- Filtre : ce logiciel est en mesure de bloquer certains sites web pour les rendre inaccessibles depuis l'ordinateur des enfants. Pour ce faire, il met une interface de saisie à la disposition de l'utilisateur pour enregistrer les adresses URL qui seront bannies de la navigation.

- Alerte : Qustodio dispose d'une fonction permettant d'alerter instantanément l'utilisateur en cas de connexions non autorisées. Le programme peut de ce fait envoyer un message par courrier électronique à une adresse préalablement spécifiée. Un rapport quotidien est également consultable en vue d'améliorer le suivi.[16]

c)Les avantages

1) Bloquez les sites et contenus dangereux : Le filtre internet intelligent analyse le contenu web en temps réel, pour qu'aucun site n'échappe à notre examen minutieux, et ce même s'il est récent. Pour tous les sites, toutes les pages, et tous les navigateurs.

2)Contrôlez l'activité sur les réseaux sociaux Permet de contrôler l'activité de notre enfant sur les réseaux sociaux comme Facebook, Twitter ou Yahoo.

3)Contrôlez leur utilisation de l'ordinateur : Nous pouvons définir des limites quotidiennes de durée d'utilisation de l'ordinateur et de temps navigation sur internet pour les jours de la semaine et les week-ends.

4)Contrôlez l'utilisation des jeux et logiciels : Nous pouvons accéder à des données statistiques sur l'utilisation de différents logiciels par nos enfants. Nous pouvons également bloquer l'utilisation de certaines applications.[17]

II.3.3 Possibilité de limiter l'accès à des jeux ou à d'autres logiciels

Il s'agit d'interdire l'exécution d'un programme, que ce soit un jeu vidéo, un logiciel de téléchargement (peer to peer), de messagerie instantanée ou autre, par exemple : SpyMykeyboard.[10]

III.3.3.1 SpyMykeyboard

a)Description

Totalement invisible SpyMyKeyboard enregistre ce qui est saisi et prend des captures d'écran. De cette façon, les familles et les entreprises peuvent surveiller les activités sur leur réseau sans connaissance directe des utilisateurs.[18]

b)Pourquoi choisir SpyMyKeyboard ?

Sophistiqué et pourtant très facile à utiliser, SpyMyKeyboard offre de multiples fonctionnalités. Il enregistre tout ce qui est tapé sur le clavier, indépendamment de l'application (logiciel de messagerie, programme de messagerie instantanée, navigateur web, etc.). L'interface utilisateur est simple et il suffit d'une minute pour le mettre en fonctionnement. Les autres utilisateurs n'auront pas accès au logiciel. Le keylogger est invisible et n'aura pas de fenêtre ou de message qui afficherons. En outre, l'interface est sécurisée avec une combinaison de touche que vous pouvez paramétrer.[18]

c)Principales fonctionnalités

- Rapport par e-mail : il nous est possible de savoir tout ce que l'utilisateur a effectué sur notre machine pendant que nous étions absents. Pour ce faire, SpyMykeyboard va travailler en toute discrétion, et va nous envoyer par e-mail un rapport complet dans lequel s'affichent les parcours de l'utilisateur.

- Les éléments sauvegardés : son efficacité réside sur sa capacité de tout enregistrer y compris les mots de passe, les conversations et autres, et peut même effectuer une capture d'écran pour les accompagner.

- Configurable : SpyMykeyboard est totalement configurable puisque nous pouvons ajuster la fréquence d'envoi des e-mails ainsi que les captures d'écran selon nos préférences. Ainsi, notre surveillance sera optimisée.

Sans installation : c'est un logiciel pratique qui peut être transporté partout et dans n'importe quelle forme de support que ce soit flash disque, ou autres périphériques amovibles. Il ne nécessite aucune installation, il nous suffit de double cliquer et le logiciel fonctionne.[19]

d)Avantages

- Ce logiciel se lance automatiquement au démarrage de Windows.
- Il est très facile à utiliser et indétectable par les anti-virus.
- L'interface est intuitive, ce qui rend la mise en œuvre facile.

II.3.4 IPCop

II.3.4.1 Description

IPCop est un projet Open Source dont le but est d'obtenir une distribution Linux complètement dédiée à la sécurité et aux services essentiels d'un réseau. Il fonctionne à part entière sur une machine dédiée, et utilise très peu de ressources systèmes (un ordinateur PC équipé de 64 Mo de mémoire vive et d'un processeur à 233 MHz suffit).

IPCop a le rôle d'intermédiaire entre un réseau considéré comme non sûr (Internet) et un réseau que l'on souhaite sécuriser (le réseau local par exemple), tout en fournissant des services permettant la gestion et le suivi de celui-ci.[20]

II.3.4.2 Caractéristiques d'IPCop

- Une distribution de pare-feu basée sur Linux, stable, sécurisée et hautement configurable.

- Une administration facile depuis un navigateur par l'intégration d'un serveur web.

- Un client DHCP permettant éventuellement à IPCop d'obtenir une adresse IP de votre FAI.

- Un serveur DHCP vous permettant de configurer facilement les machines de votre réseau interne.

- Un serveur mandataire DNS pour accélérer la résolution des requêtes de nom de domaine.

- Un serveur mandataire web (proxy) pour accélérer l'accès au web.

- Un système de détection d'intrusion pour identifier les attaques externes sur votre réseau.[21]

II.4 Comparaison des logiciels

	Filtrage des sites	Limiter les horaires	Limiter l'accès à Applications et logiciels	Capacités
PC Time Watch			✓	18.48 Mo
Net Addict Free	✓	✓		1,60 Mo
Control Kids	✓			1.70 Mo
Qustodio	✓			14 Mo
Spy My Keyboard			✓	16 Mo
IPCop	✓	✓	✓	64 Mo

Table II.1 – Comparaison des logiciels

Dans ce tableau ci dessus,nous remarquons qu'IPCop est le plus performants que les autres logiciels cités précédemment.

II.5 Synthèse

Comme nous avons vu il existe donc des catégories de contrôle parental :

- Possibilité de fixer des limites horaires
- Possibilité d'interdire l'accès à des sites
- Possibilité limité l'accès à des jeux ou à d'autres logiciels

La figure regroupe sous forme schématique les principaux qui ont été présentés.

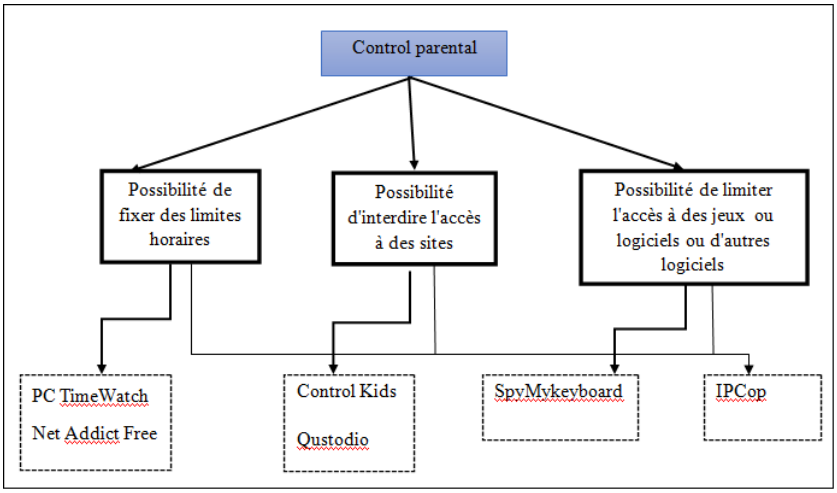


FIGURE II.4 – Catégories du contrôle parental

II.6 Conclusion

Le contrôle parental est opté pour surveiller les enfants qui surfent sur le web. Dans ce chapitre, nous avons présenté un état de l'art sur le contrôle parental en citant quelques logiciels de chaque catégorie. Nous avons fait une comparaison des logiciels ainsi qu'une synthèse.

Chapitre III

Déploiement de l'architecture

III.1 Introduction

Dans ce chapitre, nous allons présenter le logiciel choisi, l'architecture de notre réseau, ainsi que quelques fonctionnalités d'IPCop que nous avons présenté grâce à des diagrammes.

III.2 Description de notre travail

Comme évoqué dans la phase précédente, le but du projet consiste à sécuriser et surveiller un réseau domestique. C'est de permettre à des parents de mettre en place des politiques de sécurité et restrictions à leurs enfants.

Après étude, la solution choisie est IPCop. Cet outil possède une interface ergonomique assez simple à utiliser avec des fonctionnalités très avancées, permettant de sécuriser et cloisonner un réseau.

III.3 Architecture global

Le schéma ci-dessus représente le réseau domestique. Il se compose de trois PCs clients, un serveur IPCop avec le rôle de proxy/firewall et d'un point d'accès (modem). Chaque PC est connecté à un Switch.

Dans cette architecture, le réseau est scindé en deux parties : la zone verte (réseau LAN) et la zone rouge (internet) - La zone verte : C'est une partie qu'IPCop doit protéger, il s'agit d'un réseau local où se trouvent les clients.

- La zone rouge : C'est la partie qui correspond à l'Internet ou un réseau non sûr.

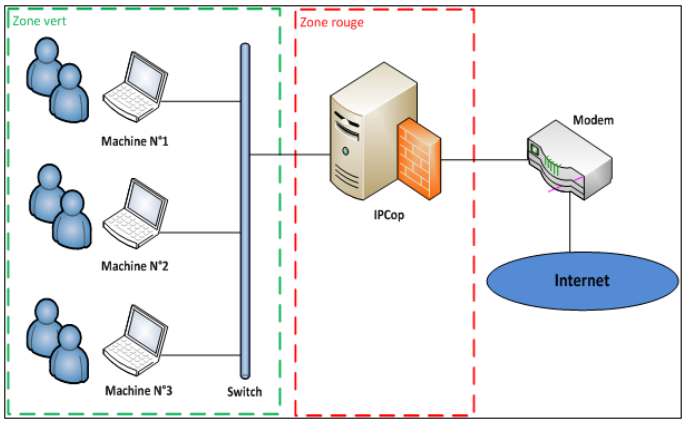


FIGURE III.1 – Architecture du réseau domestique

Le routage s'effectue de manière automatique, au niveau d'IPCop, entre l'interface d'entrée du trafic (vert) et les interfaces de sortie (rouge).

III.4 Présentation de l'outil IPCop

C'est un outil pouvant avoir plusieurs rôle dans un réseau local : Firewall, routeur, proxy ... , Il se compose de plusieurs interfaces dont chacune peut être utilisée ou non. Elles sont distinguées par des codes couleurs ou zones :

- Zone rouge c'est le réseau qui est relié à internet. Cette zone est obligatoire lors de la configuration

- Zone vert c'est le réseau local LAN utilisateur. Cette zone est à protéger et obligatoire

- Zone bleu elle est spécifique pour les sans fil. Il n'est possible de faire communiquer l'interface Verte et l'interface Bleu avec tunnel VPN.

- Zone orange nommée aussi zone démilitarisée (DMZ). Elle est considérée comme publique, elle est accessible de l'extérieur mais ne possède aucun accès sortant (ex. serveurs web, caméras IP...}. Ce réseau est facultatif[21]

III.5 Service d'IPCop

Divers services sont disponibles avec IPCop, certains peuvent être désactivés tandis que d'autres qui sont nécessaires ne peuvent l'être :

- Système : Cette section regroupe tous les utilitaires systèmes : mise à jour, accès SSH, modification du mot de passe, sauvegarde ... etc.

- Etat : regroupant les résumé de l'état système ainsi que des outils de surveillance graphique : services actifs, utilisation de mémoire, du processeur, du disque dur ... etc.

- Réseau : Cette section n'est utile que si vous avez connecté directement un modem à l'interface rouge (en non un routeur/modem) dans ce cas elle vous permet de paramétrer directement le modem.

- Services : Vous retrouvez ici les options de paramétrages des différent services installé sur le pare feu. Bien sûr au plus vous ajoutez de Plugins, au plus cette interface sera fournie.

Par défaut vous y trouverez : serveur mandataire (serveur proxy), serveur DHCP, serveur DNS Dynamique, serveur de temps, fonction de lissage de trafic ...etc.

- Pare feu : voici la section dédiée au paramétrage fin du firewall : transfert de ports, accès externe, option du pare feu ... etc.

- RPVs : Cette section vous permet de créer un VPN (réseau privé virtuel) entre deux firewall IPCOP.

- Journaux : Configuration des journaux, Résumé des journaux, Journaux du serveur mandataire, Journaux du pare-feu, Journaux IDS si ce dernier est actif et Journaux Système.[22]

III.6 Plug-ins

Des plug-ins (modules supplémentaires) peuvent être installés afin d'améliorer des services existants ou afin d'ajouter des rôles supplémentaires au serveur IPCop.[23]

- AdvProxy Advanced Proxy est, comme son nom l'indique, un serveur proxy avancé. Il enrichit ainsi les options existantes au niveau du proxy d'IPCop, son installation est nécessaire pour pouvoir utiliser et activer le plug-in URL Filter.

- URL Filter Ce plug-in vous permettra d'effectuer un filtrage d'Url afin d'interdire l'accès à certaines catégories de sites web.

III.7 Le fonctionnement d'IPCop

IPcop a pour rôle d'un pare feu, ce qui permet de bien mener la surveillance dans un réseau domestique. Les diagrammes cités ci-dessous nous montrent les fonctionnalités que peut nous servir IPCop dans notre configuration.

III.7.1 Diagramme de cas d'utilisation

Les cas d'utilisation permettent d'identifier les fonctionnalités qui peuvent être fournies par le système en interagissant avec les acteurs.[24]

Dans notre cas, nous avons uniquement un acteur qui utilise le système pour accomplir plusieurs tâches.

Les cas d'utilisation

Les cas d'utilisations sont déterminés à partir des manipulations que peut effectuer l'administrateur, d'où notre système sera présenté par les cas d'utilisation suivants :

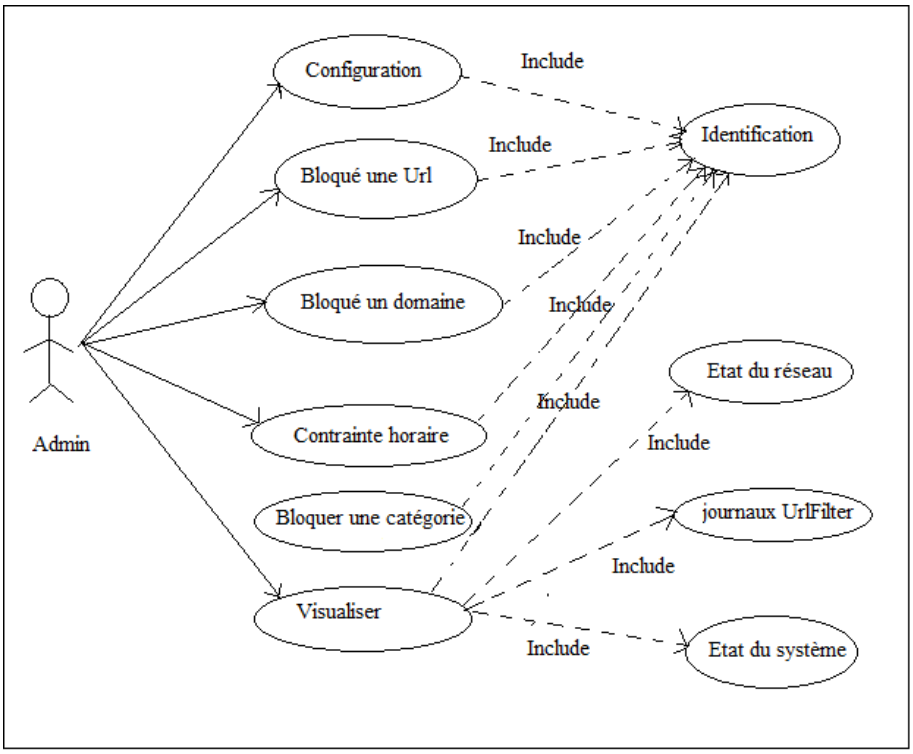


FIGURE III.2 – Diagramme de cas d'utilisation

III.7.2 Diagramme de séquence

Ces diagrammes permettent de lire les messages inter-changés entre les différents objets du haut vers le bas.[25]

Les différents diagrammes de séquences pour le cas d'utilisation sont donnés sur les figures.

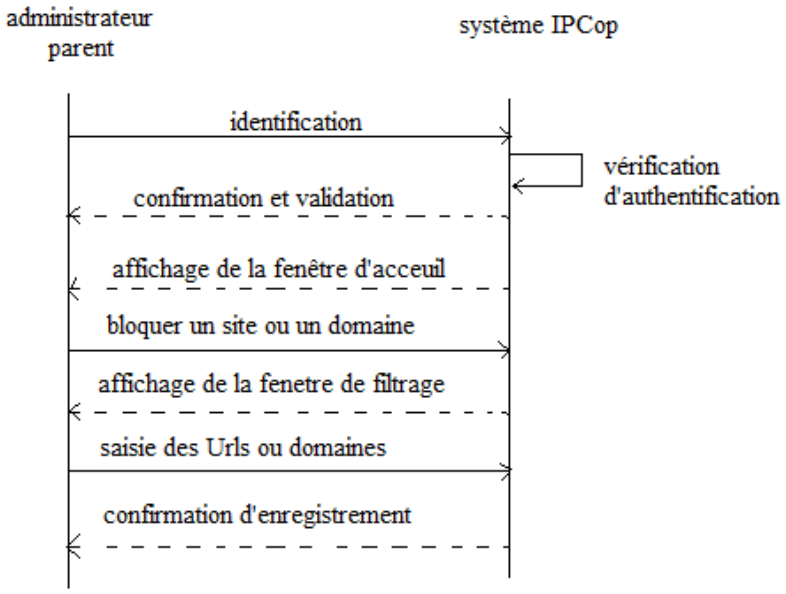


FIGURE III.3 – Diagramme de séquence « filtrer un site ou un domaine »

le diagramme ci-dessus montre les interactions qui se réalisent entre les objets dans le cas de filtrage d'un site ou d'un domaine dans la mesure où chaque requête émise par l'admin , IPCop répond. Après identification, l'utilisateur demande de bloquer, le système IPCop lui affiche la fenêtre. ensuite l'administrateur va cocher.

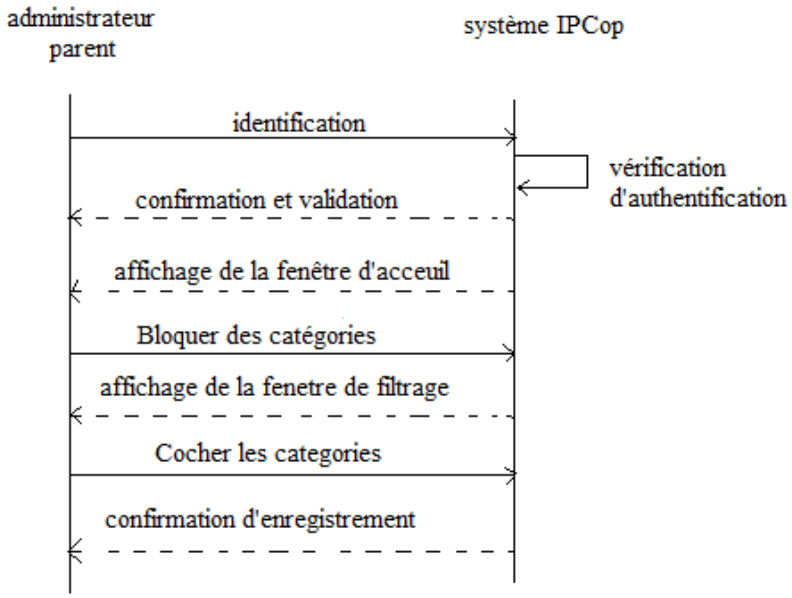


FIGURE III.4 – Diagramme de séquence « Bloquer une catégorie »

Le diagramme (ci-dessus) montre les interactions qui se réalisent entre les objets dans le cas d'un blocage d'une catégorie dans la mesure où chaque requête émise par l'administrateur, le système IPCop répond. Après identification, l'utilisateur demande de bloquer une ou plusieurs catégories, le système lui affiche la fenêtre de filtrage. Ensuite l'administrateur choisie et coche les catégories, enfin le système met à jour et enregistre.

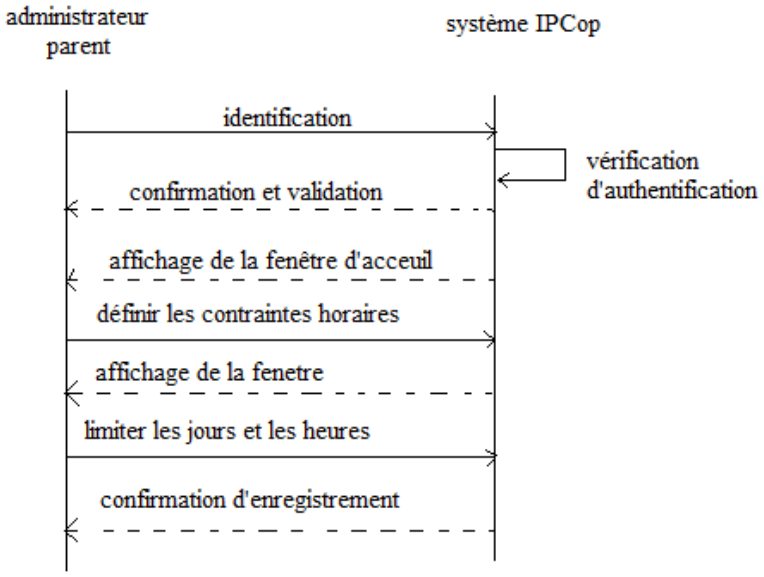


FIGURE III.5 – Diagramme de séquence « Contrainte horaire »

III.7.3 Diagramme d'activité

Ce diagramme montre tout les comportements internes d'un objet vis-à-vis des messages reçus.[25]

a)Diagramme d'activité : « Identification »

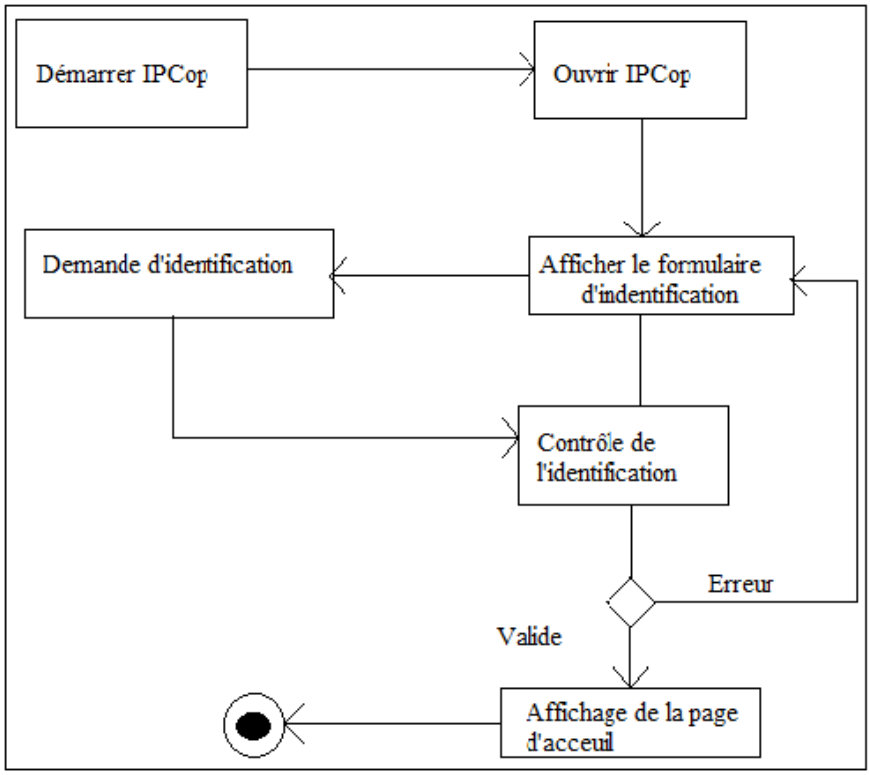


FIGURE III.6 – Diagramme d'activité « Identification »

Ce diagramme d'activité d'identification permet surtout de montrer les comportements du système. Lorsque l'utilisateur démarre l'application, le système lui répond en lui affichant un formulaire d'identification. Suite à cela, l'administrateur sais les données et le système vérifie si les informations saisîtes sont valides ou non. Si elles le sont, le système répond par un affichage de la page d'accueil sinon il lui renvoi un message d'erreur.

b)Diagramme d'activité « Filtrer des Urls ou domaines »

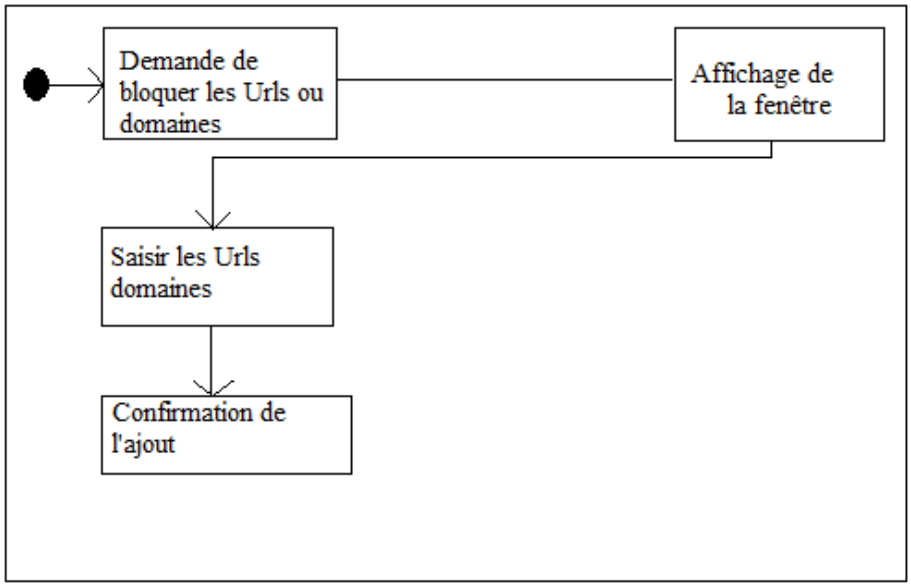


FIGURE III.7 – Diagramme d'activité « Filtrer des Urls ou domaines »

c)Diagramme d'activité « Bloquer une(les) catégorie(s) »

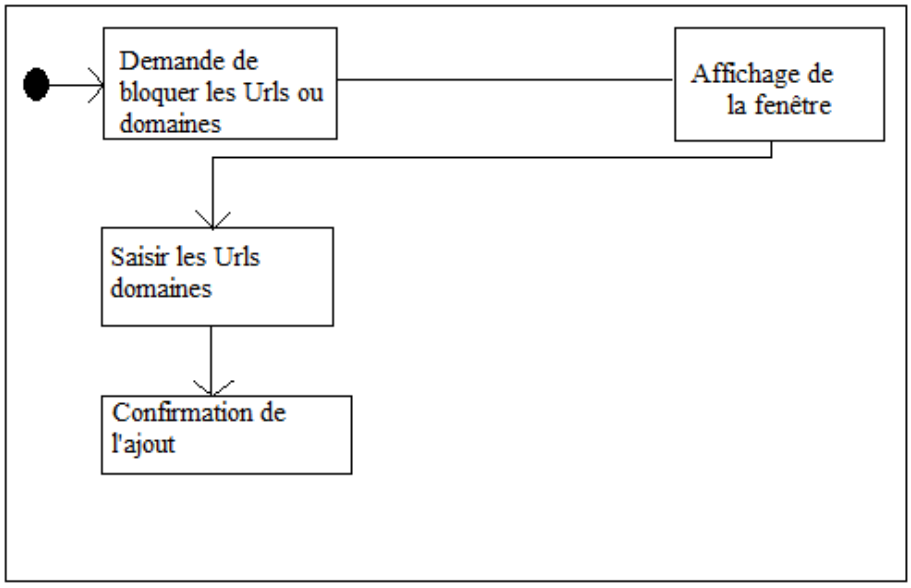


FIGURE III.8 – Diagramme d'activité «Bloquer une(les) catégorie(s) »

d)Diagramme d'activité : Interdire/Autoriser un accès à un client

La figure III.9 Représente un client(Enfant) qui veut accéder à une page web par exemple yahoo.fr, donc cette requête doit passer par IPCop pour vérifier si ce domaine est bloqué par l'utilisateur (parent) ou non. Lorsque ce domaine est bloqué et que l'enfant y accède, le message de blocage apparait.

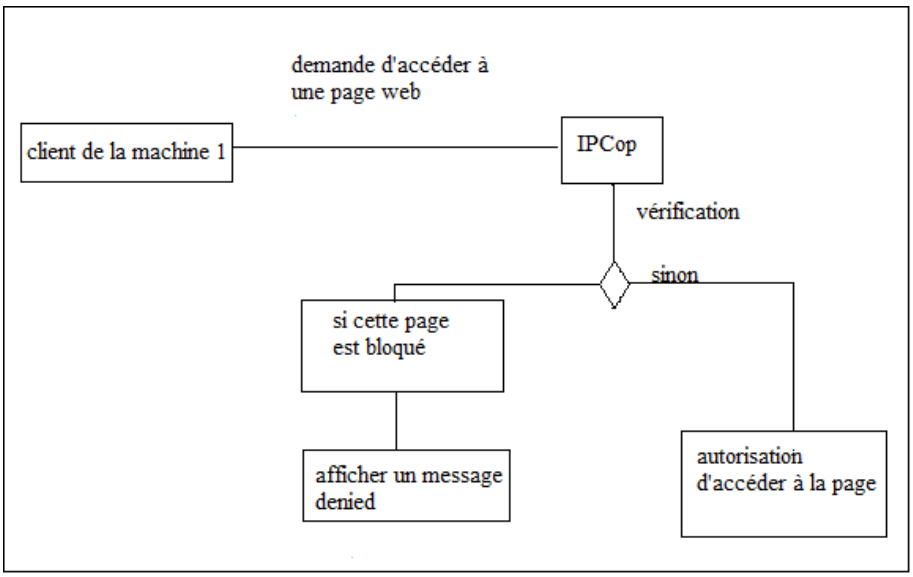


FIGURE III.9 – Diagramme d'activité «Interdire/autoriser un accès à un client»

III.8 Conclusion

Dans ce chapitre, nous avons d'abord présenté IPCop en donnant l'architecture globale de notre système ainsi que son fonctionnement en utilisant des diagrammes. Cette phase nous permet de bien mener les phases de configuration et de test dans le chapitre suivant.

Chapitre IV

Implémentation et configuration

IV.1 Introduction

Après avoir donné, dans le chapitre précédent, l'architecture de notre système, nous aborderons dans ce qui suit la phase de la réalisation de notre projet, nous présenterons les pré-requis et les étapes d'installation de IPCop, ensuite nous présenterons notre configuration représentatifs de notre application avec des explications sur l'utilisation et les fonctionnalités pour chaque capture.

IV.2 Pré-requis

Notre configuration est implémentée sous le système d'exploitation Windows 7 (professionnel) sur un micro portable de 2Go de RAM (Random Access Memory) et 150Go de Disque Dur (DD).

Version d'IPCop	2.1.8
Plateforme d'installation	Oracle VirtuelBox 4.3.20

TABLE IV.1 – pré-requis IPCop

Pour une configuration domestique, nous aurons besoin de :

- Mémoire vive 256 Mo.

- Disque Dur virtuel 8 Go.

- 2 cartes réseau en mode (reseau interne et NAT).

- Connexion internet (Modem, Câble).

- Nous utiliserons une architecture simple, nous opterons pour la technologie de virtualisation.

- Une machine virtuel « IPCop » sous linux disposant de deux cartes réseaux.

- Une machine virtuel« client » sous windows 7 pour configurer IPCop à distance et faire les tests.

IV.3 Les étapes d'installation de IPCop

- Télécharger le fichier "ipcop-2.1.8-install-cd-i486.iso" [22]

- Démarrer la machine virtuelle en insérant l'image iso d'IPCop.

- Choisir la langue.

- Choisir 'fr' pour le clavier français, AZERTY standard.

- Choisir fuseau horaire.

- Sélectionnez le support.

- Indiquer quel est le type du support que vous avez choisit précédemment.

Remarque : Le port à utiliser pour accéder à l'interface web d'IPCOP, qui est un port non standard pour le HTTPS : 8443.

Entrer le nom d'hôte de la machine ainsi que le nom du domaine.

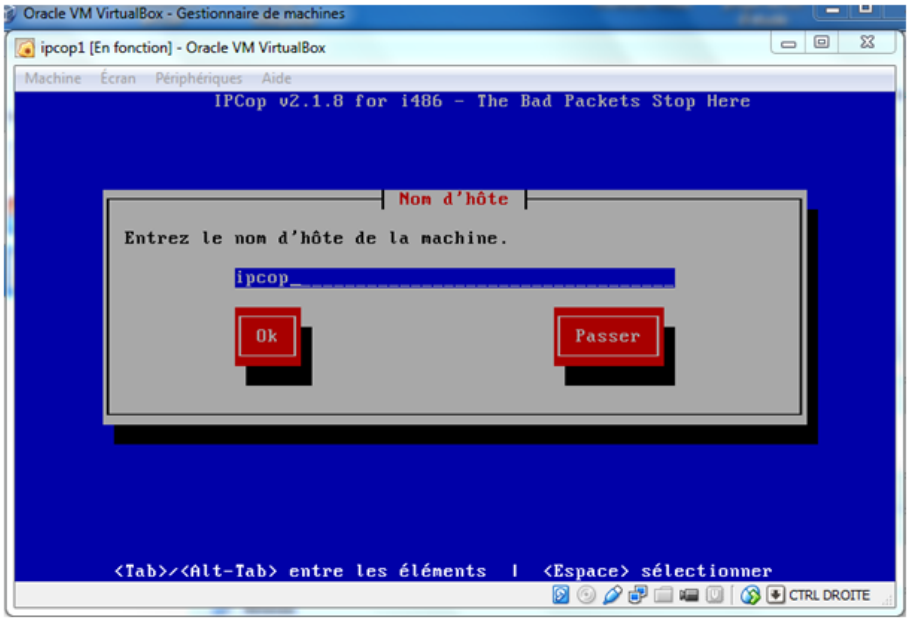


FIGURE IV.1 – Nom d'hôte de la machine IPCop

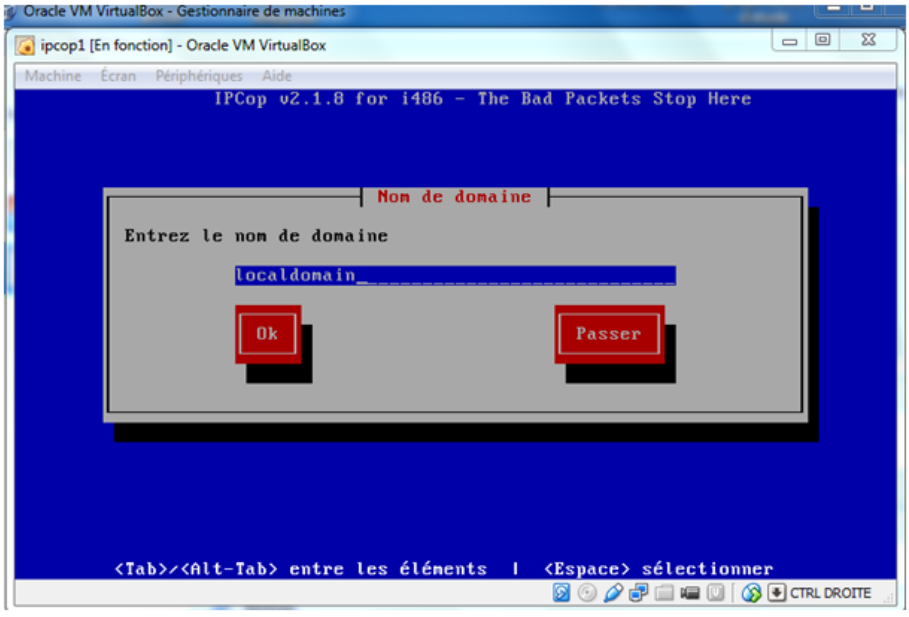


FIGURE IV.2 – Nom du domaine de la machine IPCop

L'interface ROUGE, c'est à dire l'interface côté internet, peut être de plusieurs types (voir figure IV.3). Pour attribuer une configuration statique à l'interface, sélectionnez 'S-

tatique' dans la liste en utilisant la barre d'espace pour sélectionner.

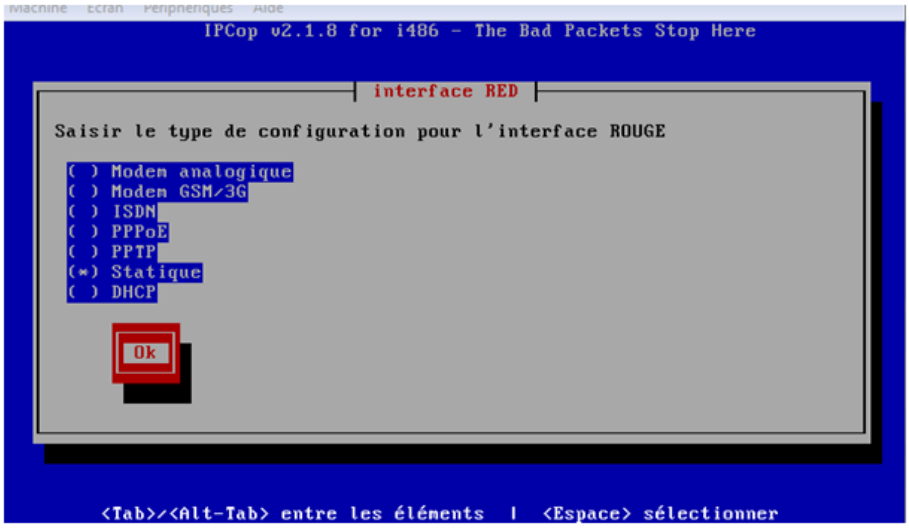


FIGURE IV.3 – Interface RED

IPCop fonctionne avec des couleurs pour identifier le WAN et le LAN, voici la correspondance : WAN= RED et LAN=GREEN (figure IV.4 et IV.5)

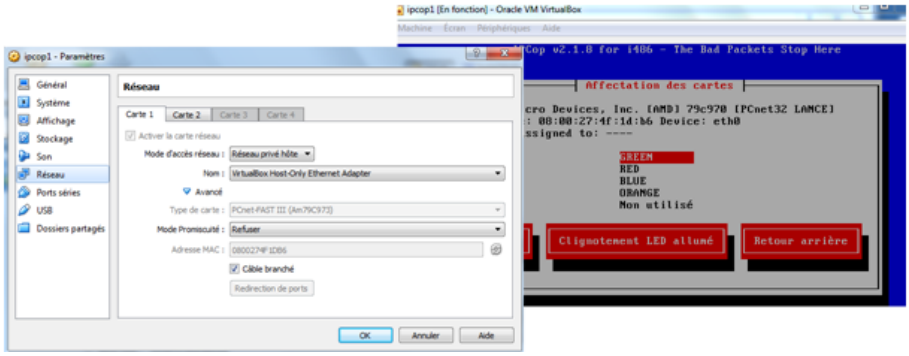


FIGURE IV.4 – Affectation de la carte GREEN

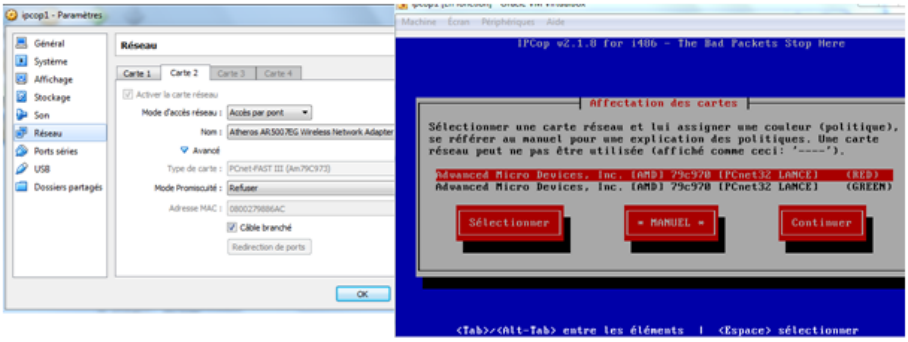


FIGURE IV.5 – Affectation de la carte RED

Affectation de l'adresse IP pour l'interface verte

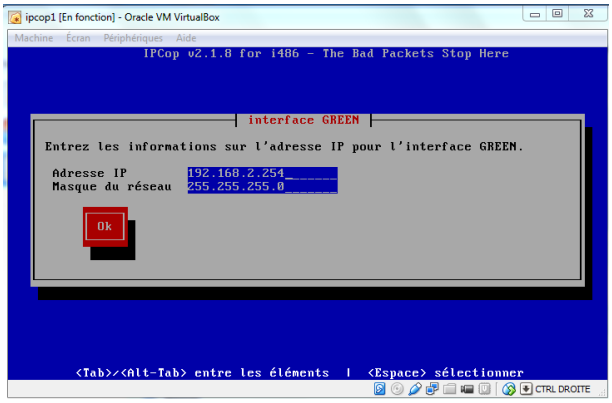


FIGURE IV.6 – Affectation des @ IP pour l'interface green

Affectation de l'adresse IP pour l'interface rouge(Figure IV.7)

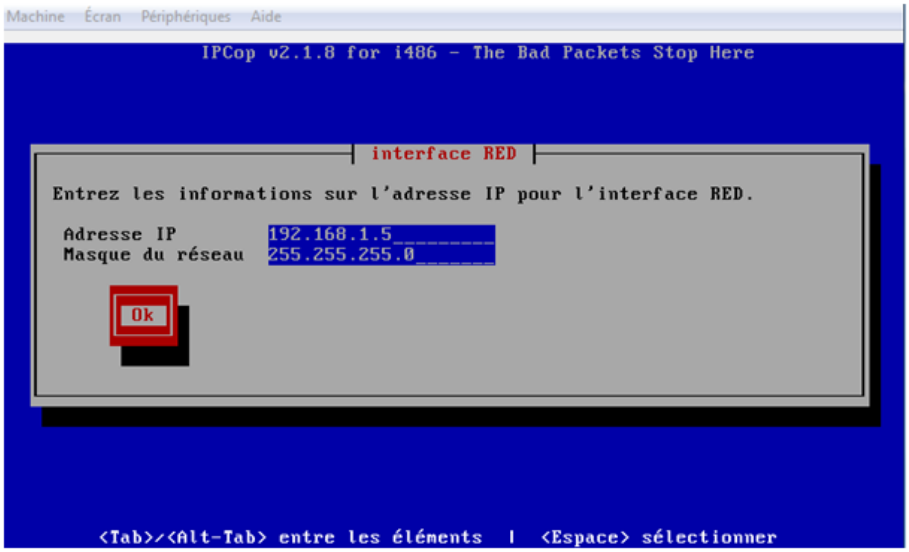


FIGURE IV.7 – Affectation des @ IP pour l'interface red

Indiquez les serveurs DNS (Primaire et secondaire) que doit utiliser l'IPCOP, et également, la passerelle par défaut pour sortir du réseau.(Figure IV.8)

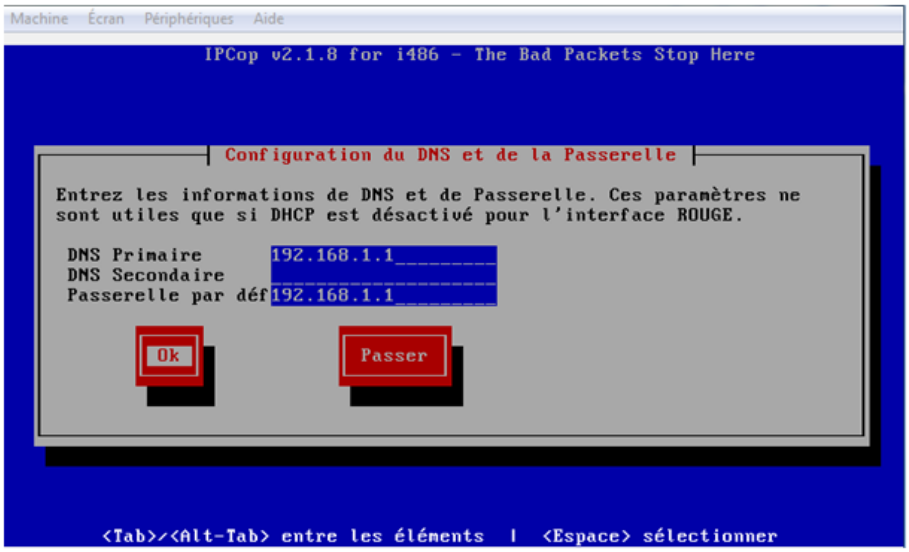


FIGURE IV.8 – Configuration de DNS et de la passerelle

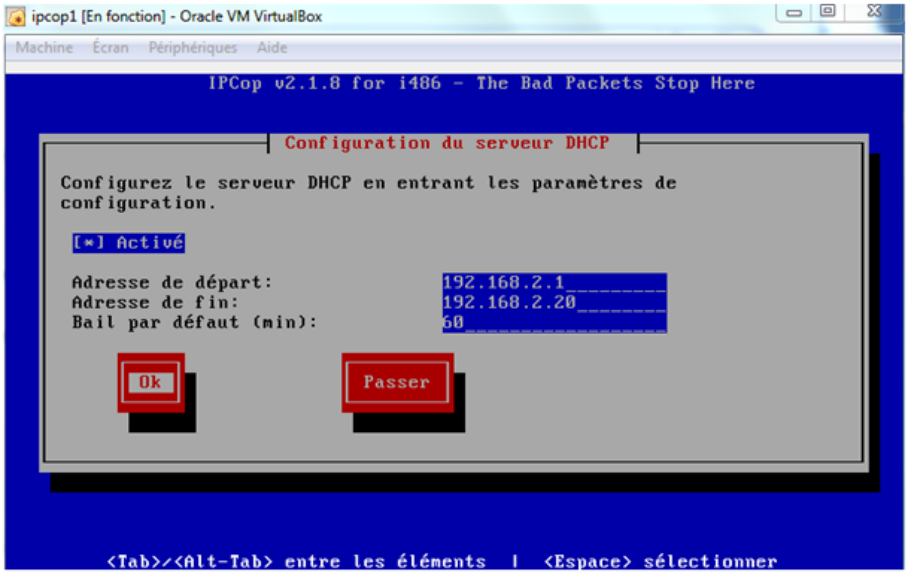


FIGURE IV.9 – Configuration du serveur DHCP

Les trois prochaines étapes concernant la définition des mots de passes, le premier mot de passe est celui pour l'utilisateur root, ensuite l'utilisateur admin qui permet l'accès à l'interface web, puis celui à utiliser pour les clés de cryptage de sauvegardes.

IV.4 Configuration de IPCop

IV.4.1 Méthodes d'accès à IPCop

Pour accéder à IPCOP, nous avons disposé de deux possibilités requises par ce système : Ouverture d'une session avec le compte root (voir figure IV.10).

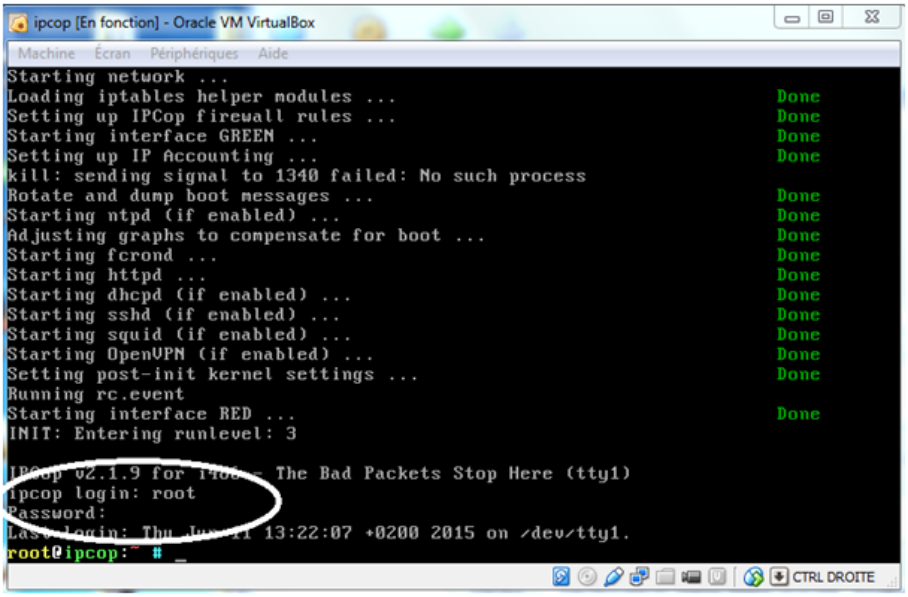


FIGURE IV.10 – Accès local en mode terminal

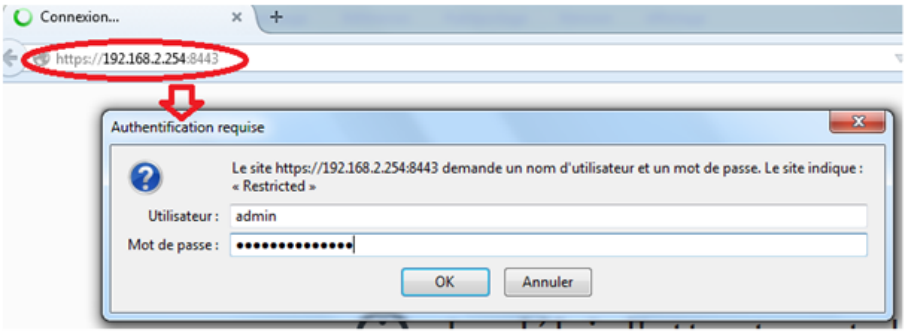


FIGURE IV.11 – Accès en mode interface graphique

A travers une interface graphique tout en saisissant dans un navigateur l'adresse IP de l'interface VERTE suivi du numéro de port :8443 (voir figure IV.11).

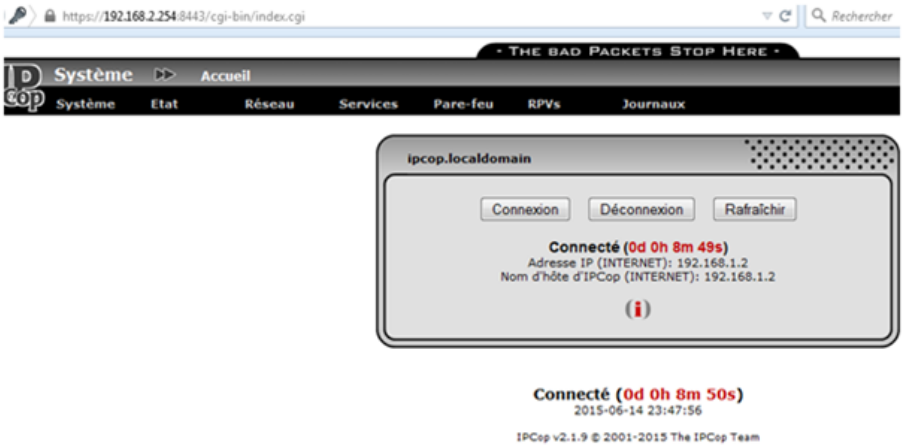


FIGURE IV.12 – Page d'accueil de IPCop

Après avoir saisi le nom d'utilisateur et le mot de passe, la page d'accueil d'IPCop s'affiche (voir la figure IV.12)

IV.4.2 Configuration du serveur mandataire

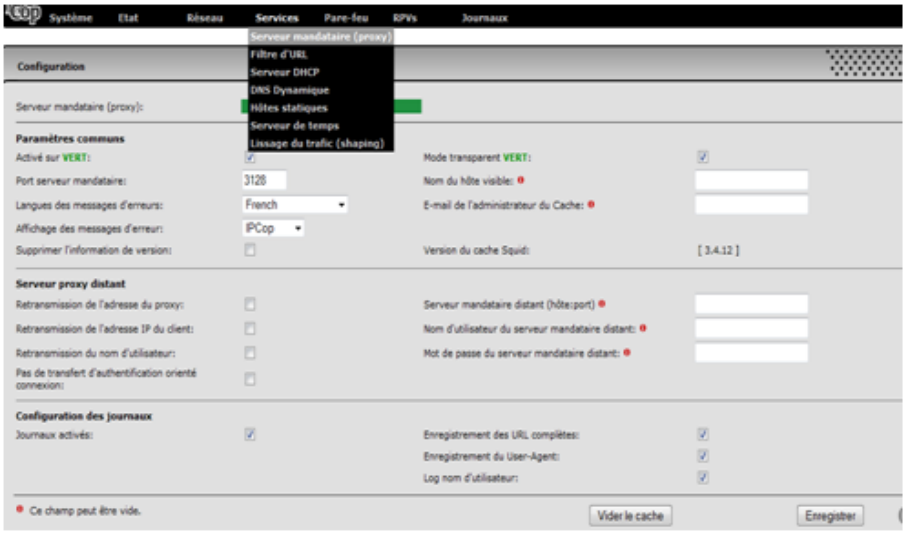


FIGURE IV.13 – Serveur mandataire

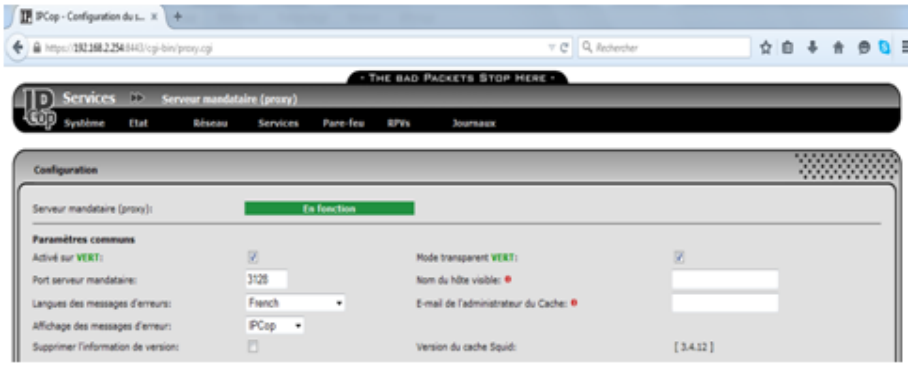


FIGURE IV.14 – Activation du Serveur mandataire

a)Activation du serveur mandataire (proxy)

Afin d'utiliser le proxy dans sa configuration initiale, il est impératif de l'activer.

Le mode transparent permet de se passer de toute configuration sur les postes clients au niveau des navigateurs internet (paramétrage du proxy). Tout trafic passant par la passerelle IPCOP sera analysé par le proxy.

b)Activation des Logs

les Logs nous permet de voir de tout ce qui passe par IPCOP (Figure IV.15)

FIGURE IV.15 – Activation des Logs

c)Contrôle des accès par le réseau

La section Contrôle d'accès par le réseau permet de définir les réseaux et sous réseau permit pour utiliser IPCOP.

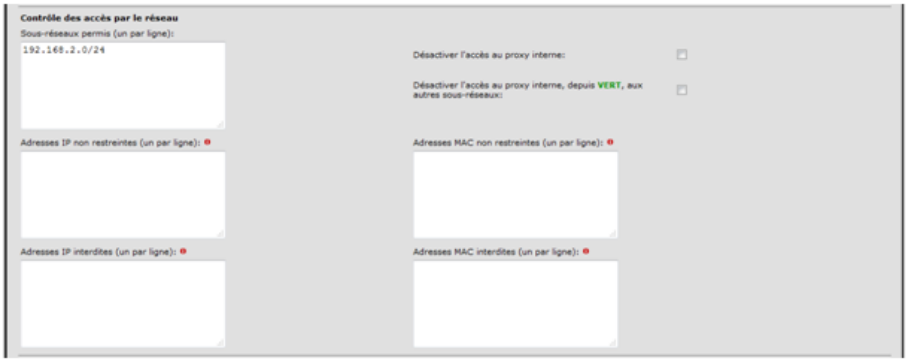


FIGURE IV.16 – Contrôle d'accès par le réseau

d)Les restrictions de temps

FIGURE IV.17 – Restriction de temps

Nous verrons lors de la configuration d'UrlFilter une méthode de restriction plus poussée.

e)Les limites de transfert

La section Limites de transfert permet de donner une limite sur la taille des fichiers en réception et en émission.

FIGURE IV.18 – Limite de transfert

f)Réduction de téléchargement

La section réduction du téléchargement, permet d'allouer de la bande passante globale et/ou par poste client.

FIGURE IV.19 – Réduction de téléchargement

IV.4.3 Configuration de l'UrlFilter

a) Activation du Filtrer d'URL

Nous voyons ici que le filtrer d'URL est bien disponible, cependant pour l'activer nous devons passer par le serveur mandataire.

- Section UrlFilter

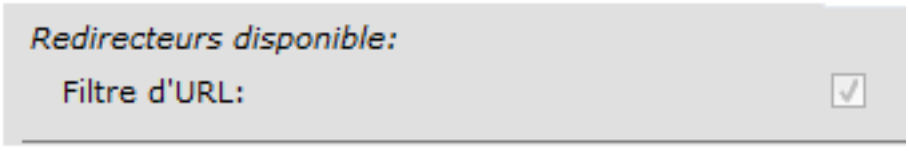


FIGURE IV.20 – Section d'UrlFilter

b) Catégorie de blocage

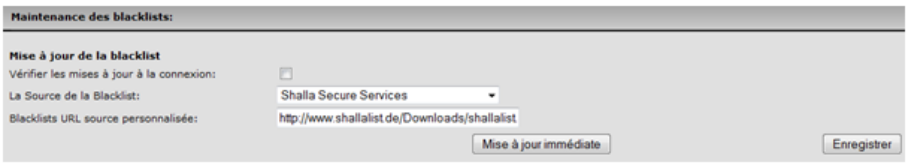


FIGURE IV.21 – Maintenance des blacklists

Installation de Blacklist Shalla Secure Services :

http ://www.shallalist.de/Downloads/shallalist.tar.gz,il permet un filtrage assez poussé, comme le démontre la figure ci-dessous :

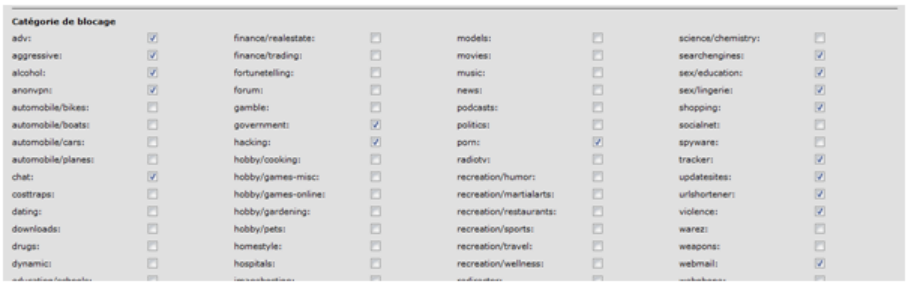


FIGURE IV.22 – Catégorie de blocage

Les catégories de blocage sont des listes de domaines et URL qu'il est possible de bloquer simplement en cochant la case correspondante.

c)Blacklists personnalisées

FIGURE IV.23 – Blacklists personnalisées

Dans cette section il est possible d'ajouter rapidement un domaine ou une URL à bloquer. Un domaine est de la forme par exemple : www.yahoo.fr

Une URL sera de la forme http ://www.monsite.com/index.php

d)Whitelists personnalisées

FIGURE IV.24 – Autoriser un domaine ou Url dans Whitelists

Dans cette section il est possible d'ajouter rapidement un domaine ou une URL qui serait bloqué par les blacklists par défaut.

e)Liste d'expressions personnalisées

FIGURE IV.25 – Liste d'expressions personnalisées

Les listes d'expressions personnalisées permettent de bloquer des termes apparaissant dans une URL sans pour autant bloquer un domaine complet.

f)Contrôle des accès sur le réseau

Cette section permet de définir les adresse IP qui ne doivent pas être filtrées (serveurs) et celle qui doivent être bannies.

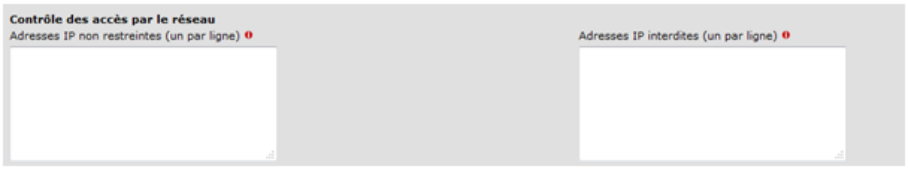
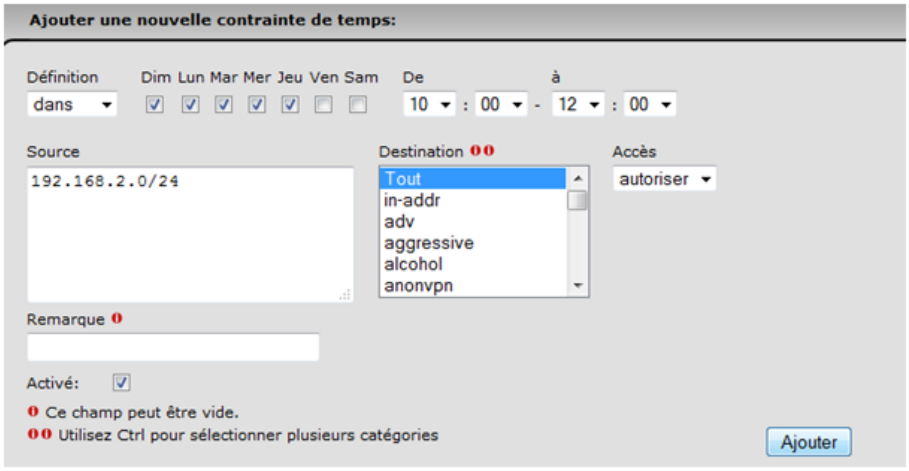


FIGURE IV.26 – Contrôle des accès sur le réseau

g)Contrôle d'accès basé sur le temps

Cliquer sur "définir les contraintes horaires" (voir figure)



Définir qui peut accéder à quoi et à quel moment de la semaine ou de la journée (ici les postes du réseau 192.168.2.0/24 peuvent accéder sans restrictions au contenu internet de 10h00 à 12h00 du lundi au vendredi.)

h)Paramètres des pages bloquées

Il est possible de paramétrer l'affichage de l'utilisateur lorsque ce dernier se voit être bloqué.

i)Configuration de l'authentification

Il est possible dans IPCOP de procéder à l'identification des utilisateurs d'Internet.

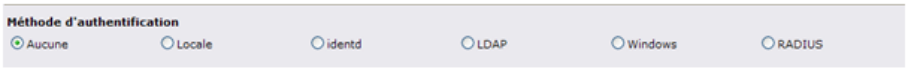
Cependant pour activer cette fonction, plusieurs points sont à prendre en considération :

- Le mode Proxy Transparent doit être désactivé.
- Les postes clients doivent donc être configurés pour passer à travers le proxy.

Plusieurs méthodes d'authentification sont disponibles sous IPCOP.

Dans le bas de la fenêtre de configuration du Proxy Avancé nous avons (figure) :

Dans notre cas nous utiliserons l'authentification none.

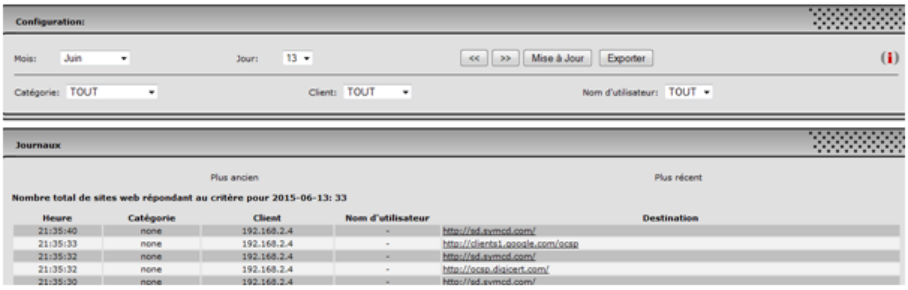


IV.4.4 Visualisation de journaux IPCOP

a)Journaux Url filter

Au bout de 24 heures (rotation et enregistrement de log par défaut).

Il permet à l'administrateur d'avoir l'historique du client quand il a l'accès à internet.

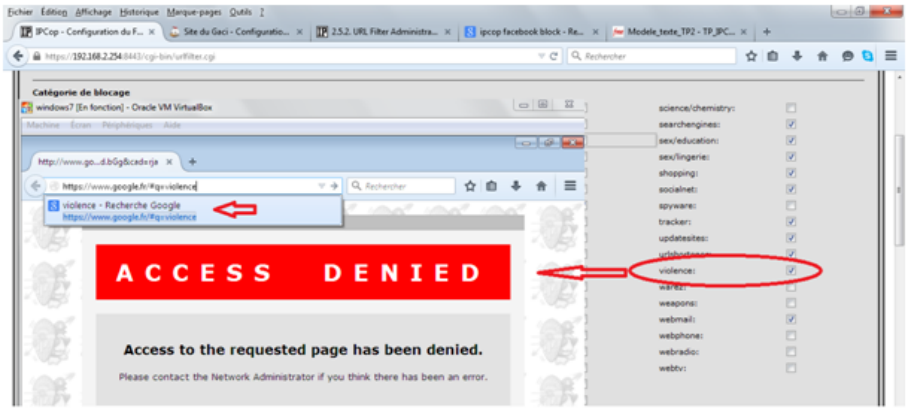


IV.5 Test

Dans cette section, nous considérons quelques exemples de tests effectués sur IPCop et le client. Nous avons choisi des exemples illustrés ci dessus :

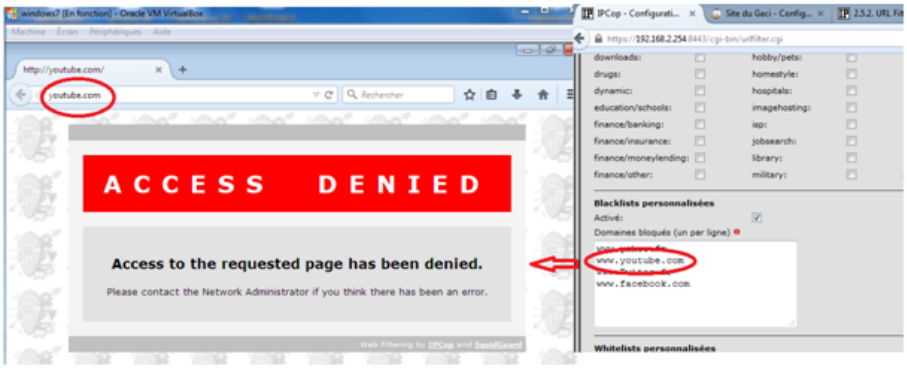
Test N°1 : Catégorie bloqué

La figure ci-dessous nous montre quand un client (enfant) accède à une catégorie, par exemple « violence », et que cette dernière est déjà bloquée par l'administrateur (parent), il lui affiche un message Denied.



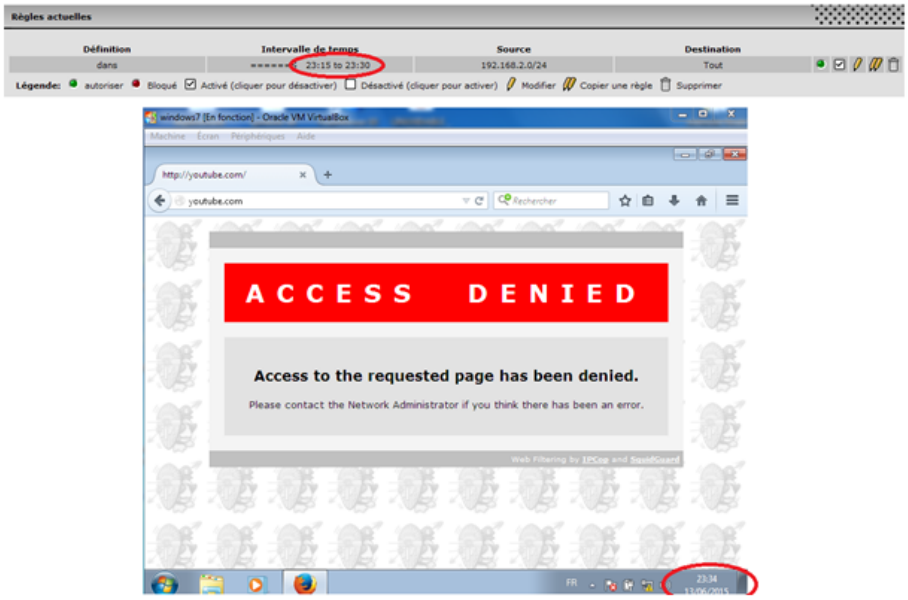
Test N°2 : Url ou Domaine bloqué

La figure ci-dessous nous montre quand un client (enfant) accède à une Url ou à un domaine, par exemple : www.youtube.com et que ce dernière est déjà bloqué par l'administrateur (parent), il lui affiche un message Denied.

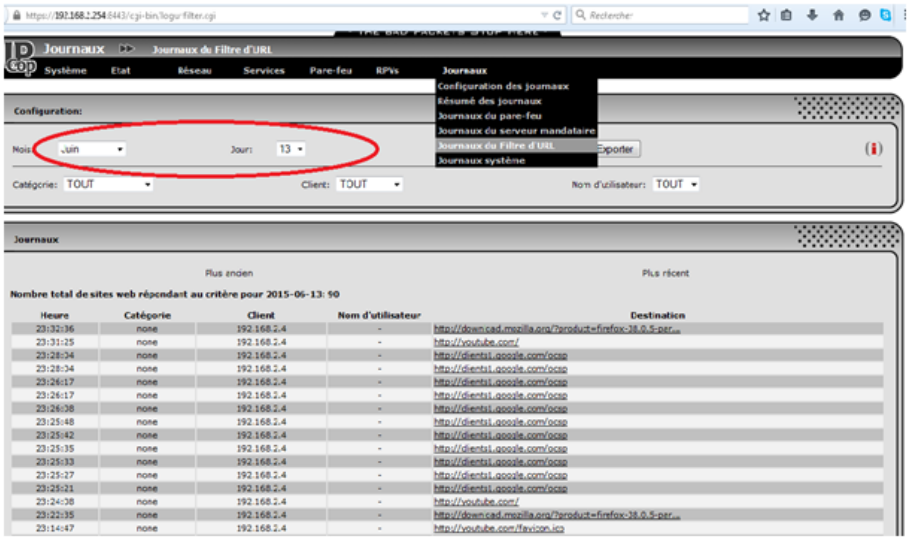


Tests N°3 : Contrainte horaire

Dans cette figure, le client n'a plus d'accès a certain domaine, vu que l'administrateur a posé des contrainte horaire.



Test N°4 : Journaux de UrlFilter



IV.6 Conclusion

A travers ce chapitre, nous avons présenté les pré-requis utilisés pour la configuration de IPCop.

Quelques scénarios été présentés qui permettent d'avoir une vision globale sur les tâches que peut réaliser IPCop sur les clients.

Conclusion générale

Au terme de cette étude, nous rappelons que notre travail porte sur la surveillance des mineurs dans un réseau domestique. En d'autres termes, réaliser une architecture afin de permettre aux parents de sécuriser et superviser leur réseau informatique.

Au cours de la réalisation de notre projet, nous avons rencontré de nombreux problèmes, parmi lesquels :

- Utilisation de la technologie de virtualisation à cause de la non disponibilité du matériel physique adéquat :

Effectivement, l'un des pré-requis de la machine qui héberge l'outil IPCop est de posséder deux cartes réseau. Or, nous n'avons pas pu avoir cette machine. La technique de virtualisation a été choisie pour palier à ce problème en utilisant des cartes réseau virtuelles.

- Utilisation des adresses IP statiques sur les machines clients :

IPCop peut avoir le rôle d'un serveur DHCP mais vu que les tests se sont fait dans un environnement déjà possédant son propre serveur DHCP, l'activation du rôle engendrera un conflit et une instabilité du réseau sur lequel nos tests ont été réalisés.

L'architecture mise en œuvre permet de bien intégrer et gérer les différentes sécurités souhaitées. Toutefois, plusieurs améliorations peuvent être ajoutées comme :

- Installation d'antivirus avec licence sur les postes pour plus de sécurité virale.

- Mise en place d'un pare-feu complet qui implémente des règles assez poussées et affinées. Enfin, nous espérons que ce travail sera complété et deviendra l'objet et la réflexion d'autres projets.

Annexe A

Annexes

Dans cette section, nous présenterons l'installation de quelques logiciels cités précédemment dans le chapitre 2.

A.1 PC TimeWatch

- Exécuter le programme d'installation PC TimeWatch
- Cliquez sur « suivant » jusqu'à la fin de l'installation. C'est terminé !

FIGURE A.1 – Page D'accueil Dans L'assistant De PC TimeWatch

FIGURE A.2 – Sélection De L'administration

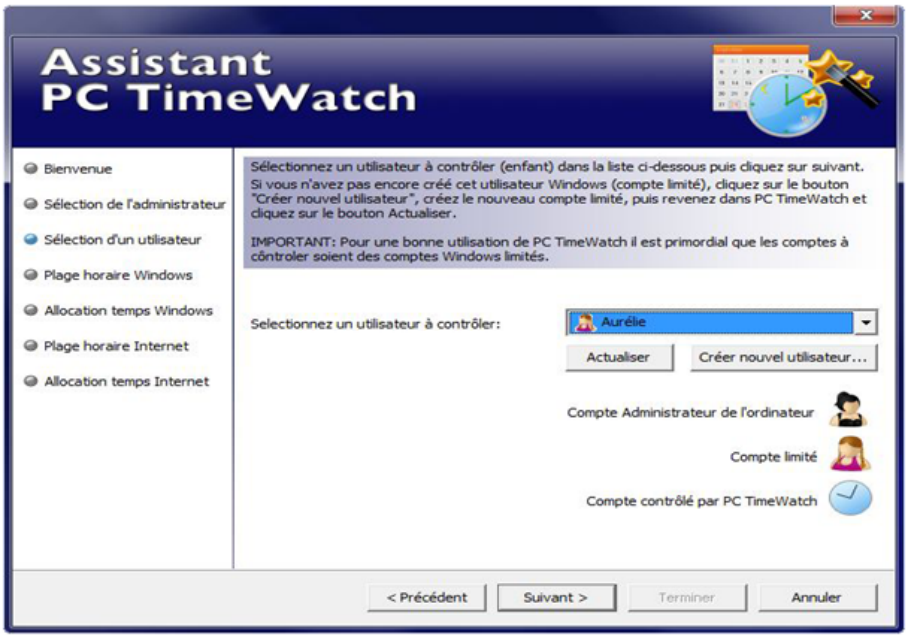


FIGURE A.3 – Sélection d'un Utilisateur

FIGURE A.4 – Plage Horaire Windows

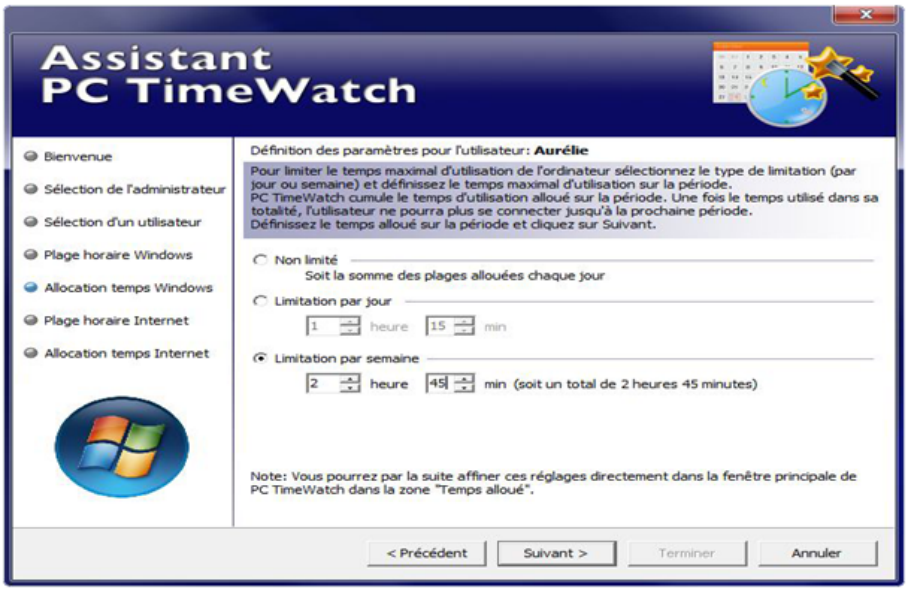


FIGURE A.5 – Allocation Temps Windows

FIGURE A.6 – Plage horaire internet

FIGURE A.7 – Allocation Temps Internet

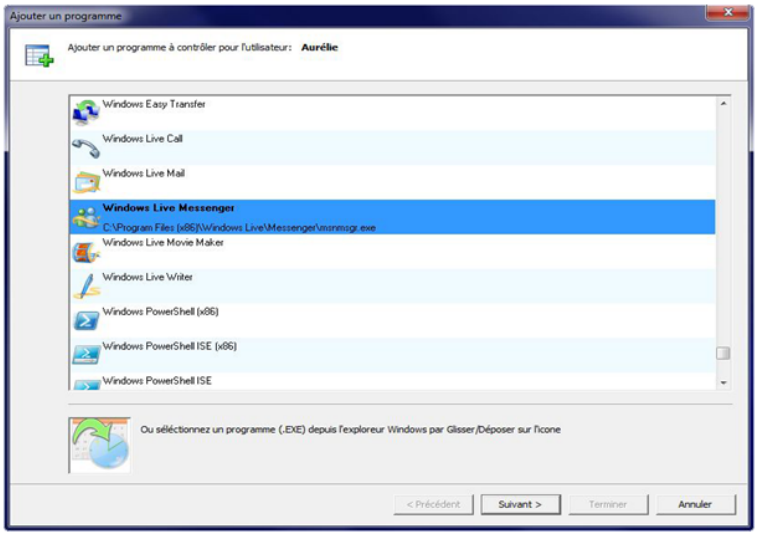


FIGURE A.8 – Ajouter Un Programme à Contrôler Pour L'utilisateur

- Dans cette étape on va ajouter une plage pour limiter le temps d'utilisation, on doit fixer les horaires et les jours après on clique sur OK

FIGURE A.9 – Ajouter une Plage

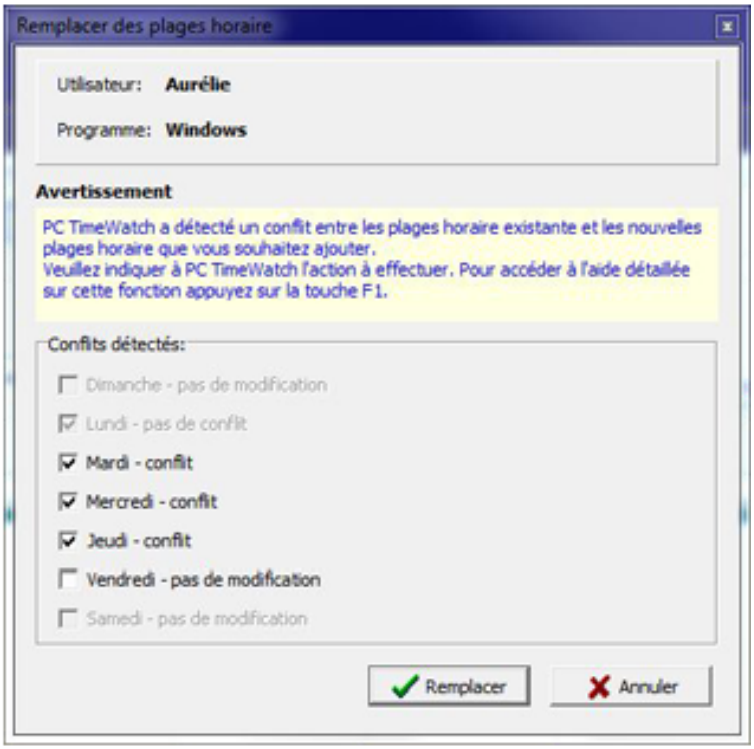


FIGURE A.10 – Remplacer des Plages Horaire

Figure(A.10) représente remplacement des plages horaire lorsque il trouve un conflit entre les plages horaire existe et les nouvelles plages horaire que nous souhaitons ajouter cliquer sur Remplacer pour confirmer notre plages horaire que nous souhaitons.

Dans cette fenêtre nous pouvons allouer des plages horaires.

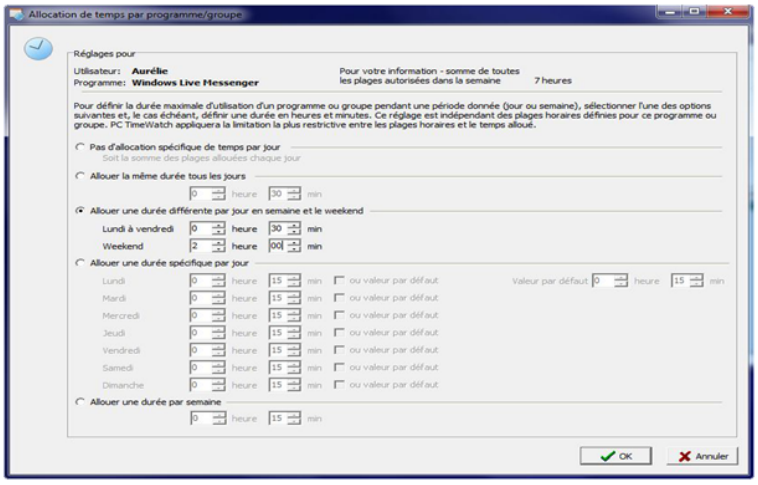


FIGURE A.11 – Allocation de Temps Par Programme/Groupe

Cette figure (A.12) défini les utilisateurs administrateur et inviter, on choisit le nom du gestionnaire de PC TimeWatch comme administrateur et le nom d'utilisateurs autorisés sur la machine et on clique sur Actualiser après sur OK.

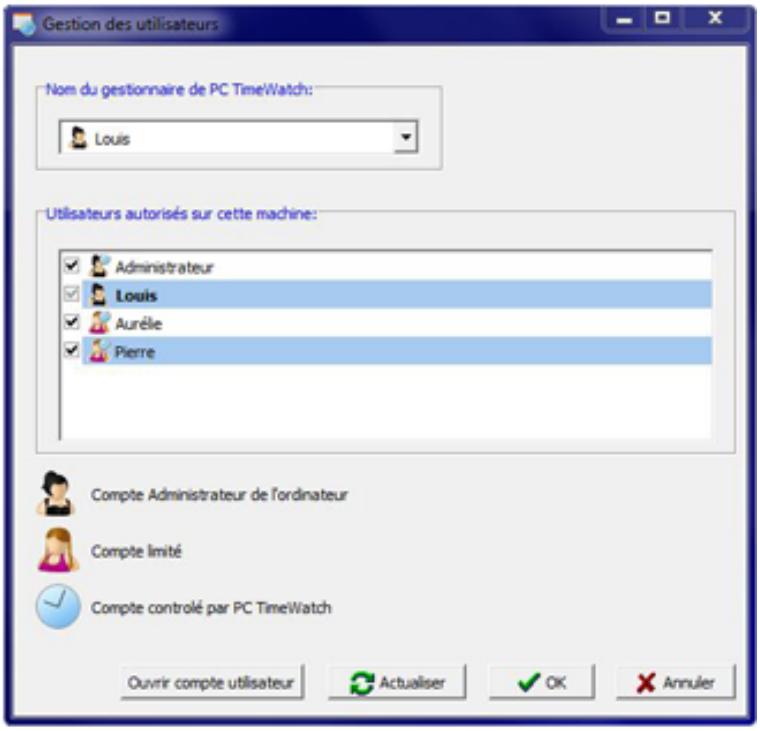


FIGURE A.12 – Gestion des Utilisateurs

Enfin, nous aurons une page d'accueil de PC Time Watch

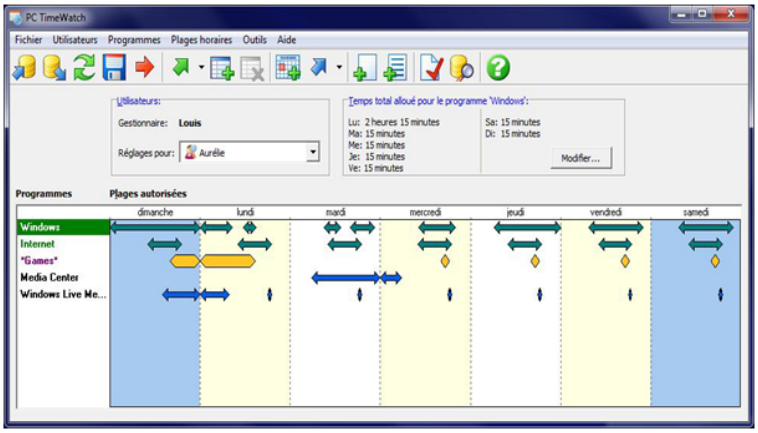


FIGURE A.13 – PC TimeWatch

A.2 Net Addict Free

Exécuter le programme d'installation NetAddictFree_Install.exe, Cliquons sur « suivant » jusqu'à la fin de l'installation. C'est terminé.

Le programme « contrôle parental » se lance automatiquement.

Premier lancement cliquons sur OK.

Le programme du contrôle parental nous demande de saisir notre mot de passe, Saisissons notre mot de passe (2 fois).

Cliquons sur « enregistrer le mot de passe », Fermer la fenêtre pour quitter le programme

Arrêter et redémarrer l'ordinateur. C'est terminé.

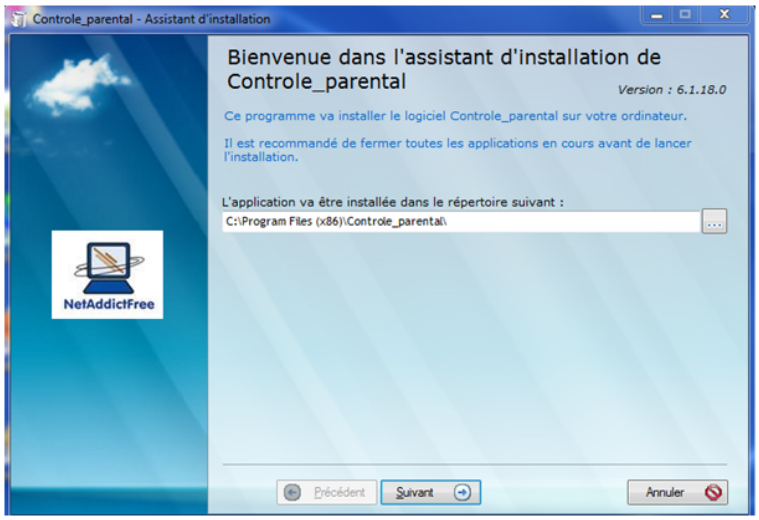


FIGURE A.14 – Le Choix de répertoire pour installer

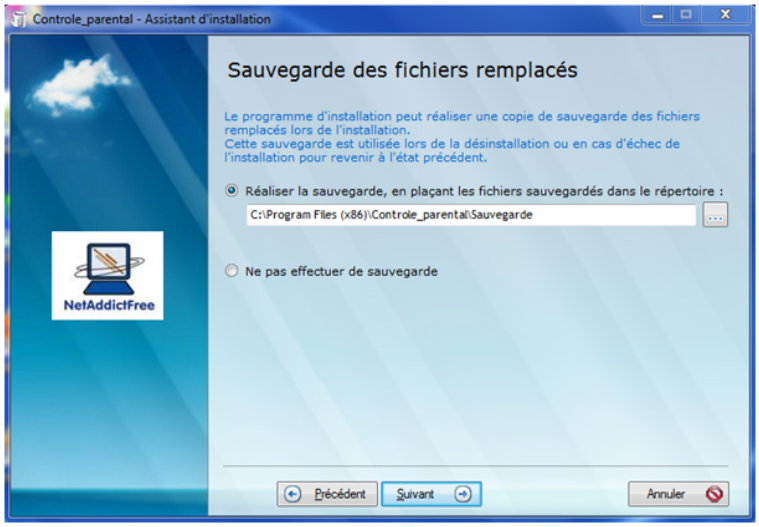


FIGURE A.15 – Sauvegarde des anciens fichiers

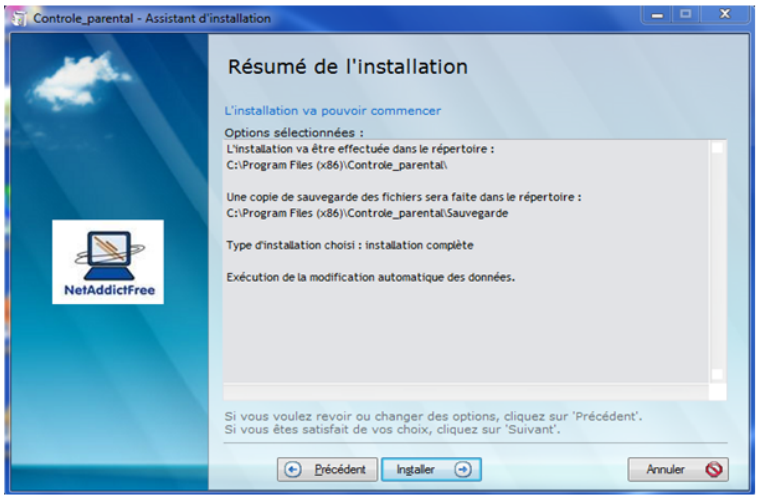


FIGURE A.16 – Résumé de l'installation

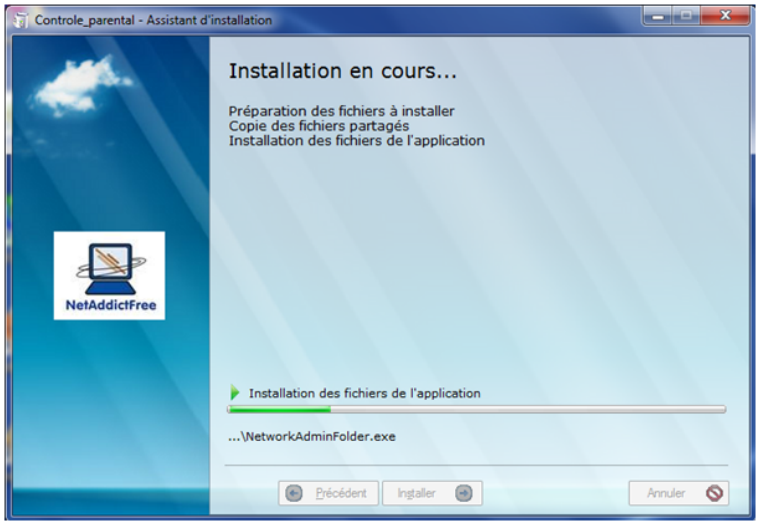


FIGURE A.17 – Installation en cours

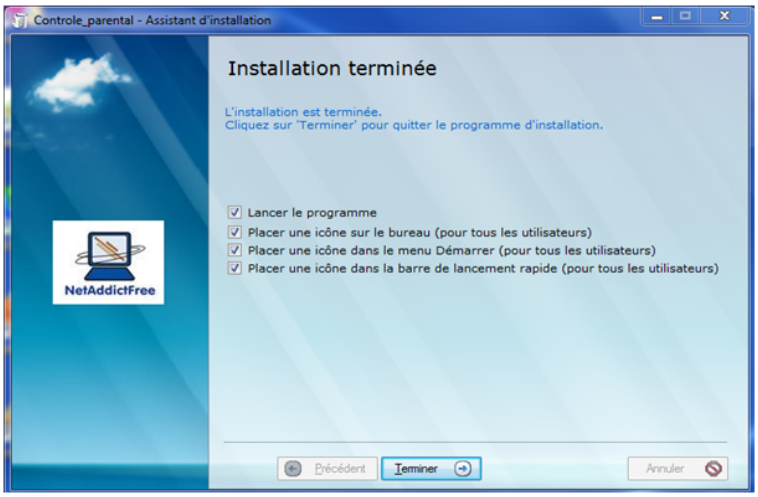


FIGURE A.18 – Fin D'installation

A.3 Control Kids

Double clique sur le programme ControlKidsInstall.exe, Le programme s'installe automatiquement sur notre PC.

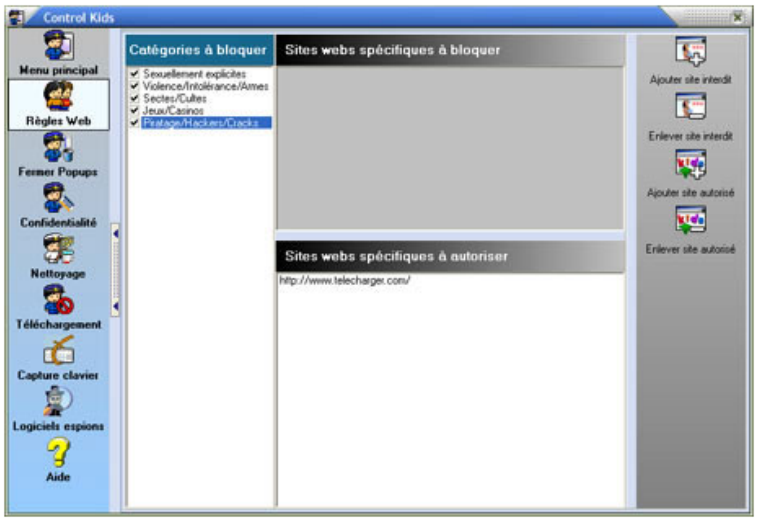


FIGURE A.19 – Control Kids

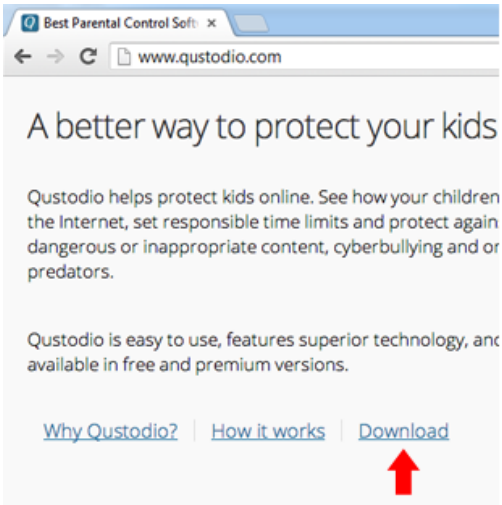
A.4 SpyMykeyboard

Le logiciel fonctionne en arrière-plan, et aucune installation n'est nécessaire.

A.5 Qustodio

Sur navigateur, allez sur le site de Qustodio à www.qustodio.com

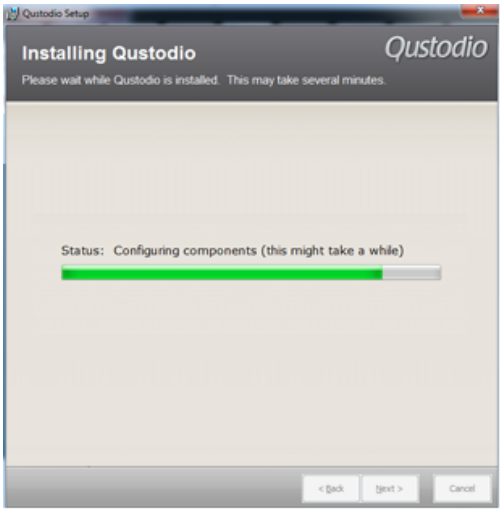
Cliquez sur le lien Télécharger.



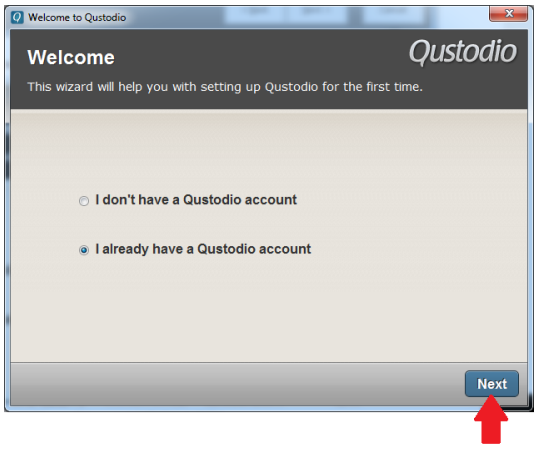
Patientez lors du téléchargement de l'installateur de Qustodio.

Cliquez sur le fichier QustodioInstaller.exe, au bas de votre fenêtre de navigation.
Cliquez sur Accepter et Installer.

Patientez quelques minutes pendant le téléchargement et l'installation du logiciel.



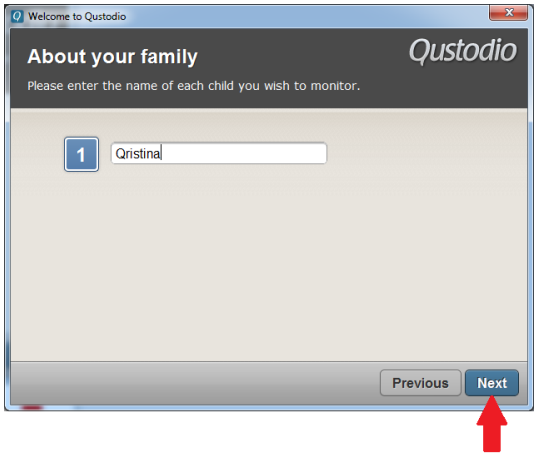
Dans la fenêtre d'accueil, sélectionnez Je n'ai pas de compte . Cliquez sur Suivant.



Entrez votre nom, votre adresse email et votre mot de passe. Cliquez sur Suivant.

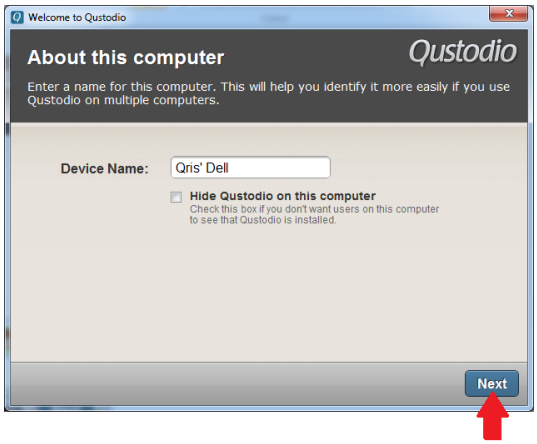
Cliquez sur le nombre d'enfants que vous souhaitez protéger. Cliquez sur Suivant.

Entrez le nom de chaque d'enfant que vous souhaitez protéger. Cliquez sur Suivant.

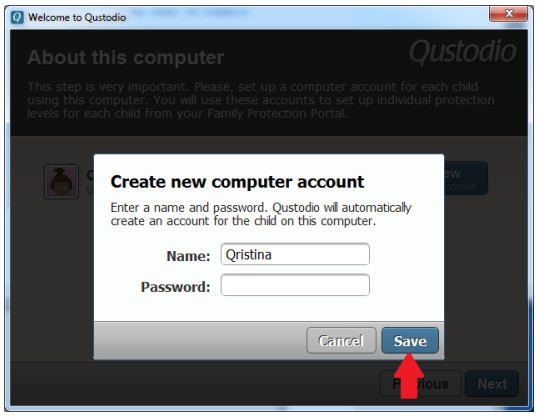


Entrez l'année de naissance et le sexe de chaque enfant, et sélectionnez un avatar. Cliquez sur Suivant.

Entrez le nom que vous souhaitez assigner au PC. Choisissez ou non de cacher Qustodio sur l'ordinateur. Cliquez sur Suivant.

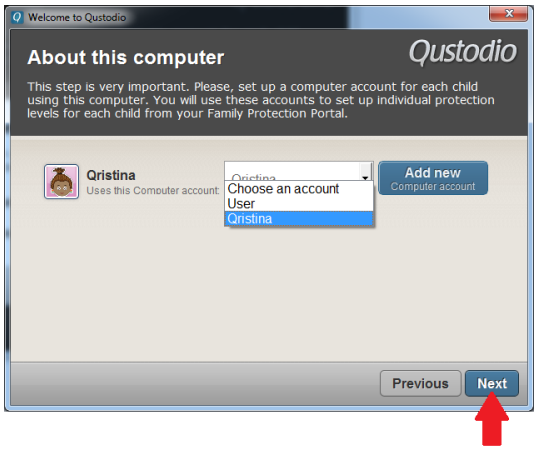


Créez un compte d'utilisateur pour votre enfant sur cet ordinateur, en cliquant sur Ajouter un compte d'utilisateur.



Entrez un nom et mot de passe (optionnel) pour l'enfant. Cliquez sur Sauvegarder.

Sélectionnez le compte utilisateur de votre enfant dans le menu déroulant. Cliquez sur Suivant.



Installation complète.

Bibliographie

[1] BELKHOUCHE Souheyla. Etude et Administration des Systèmes de Supervision dans un Réseau Local. Mémoire pour l'Obtention du Diplôme D'Ingénieur d'Etat en Informatique, Option « Système d'Information ». Tlemcen : Université Abou Bakr Belkaid, 2011.

[2] http ://www.technologuepro.com/reseaux/Chapitre1-reseaux-locaux.htm

[3] HUBERT Eric .COURS RESEAU DOMESTIQUE - 3 parties. CoinNumérique. Association de fait sans but lucratif. Loisirs - Seniors - Bénévolat.

[4] http ://www.commentcamarche.net/ contents/515-types-de-reseaux

[5] Guermouche A. Administration réseau Réseaux privés. Département Informatique, France, Université de Bordeaux.

[6] BONDU Jérôme, GARNIER Alain. Livre blanc « L'IMPACT DES RESEAUX SOCIAUX ». Montreuil .février 2009 Jamespot et Inter-Ligere.

[7] http ://www.lemonde.fr/technologies/chat/2009/02/09/reseaux-sociaux-de-nouveaux-dangers-pour-nos-enfants_1151995_651865.html

[8] http ://www.controle-parental.net/

[9] http ://www.mana.pf/_cli/espaceclients.php ?r3=parental

[10] http ://www.logitheque.com/logiciels/windows/antivirus_securite/controle_parental/telecharger/pc_timewatch_18398.htm

[11] http ://www.entelechargement.com/ anti-virus-et-securite/autres-outils-de-securite/pc- timewatch.html

[12] http ://netaddictfree.com/FR/PAGE_Controle_Parental.php

[13] https ://www.controlkids.com/caracteristiques-controle-parental.php

[14] https ://www.qustodio.com/fr/family/why-qustodio/

[15] http ://www.commentcamarche.net/download/telecharger-34099798-qustodio .

[16] https ://www.qustodio.com/fr/

[17] http ://www.logitheque.com/logiciels/windows/antivirus_securite/keylogger/telecharger/spymykeyboard_keylogger_45912.htm

[18] http ://www.commentcamarche.net/download/telecharger-34085162-spymykeyboard

[19] http ://ipcopfr.free.fr/

[20] WALKER Pete, GOLDSCHMITT Harry, PIELSCHMIDT Stephen. Manuel d'Installation d'IPCop v1.4.0. Copyright 2002-2004.

[21] http ://www.ipcop.org/1.4.0/fr/ install/html/decide-configuration.html#network-configuration-types

[22] http ://nilz.fr/configuration-d E2 80 99un-firewall-ipcop

[23] http ://www.generation-nt.com/ firewall-ipcop-securiser-son-reseau- avec-article-24818-3.html

[24] STEFFE Jérôme, 'cours UML', Université Bordeaux - France, janvier 2003.

Résumé

Ce présent travail porte sur la surveillance des mineurs dans un réseau domestique, qui permettra aux parents de mener à bien la surveillance de leur réseau, notamment leurs enfants.

Il s'agit de mettre une configuration sur le réseau domestique grâce à IPCop qui a pour rôle d'un pare feu afin de bien mener la surveillance.

VirtuelBox a été utilisé pour mener l'installation d'IPCop virtuellement.

Quelques tests illustratifs de la validité du système terminent le mémoire.

Mots clés **:** réseaux domestique, contrôle parental, IPCop, VirtuelBox.

Abstract

This present work deals with the supervision of minors in a home network, which will allow parents to carry out the monitoring of their network, especially their children.

This is putting a setup on the home network through which IPCop has the role of a firewall to properly conduct surveillance.

VirtuelBox was used to conduct the IPCop installation virtually.

Some illustrative test of the validity of the complete system memory.

Keywords **:** Domestic network, parental control, IPCop, VirtuelBox.