

STANISLAS Veronical

BTS **SIO** (1) Services informatiques aux organisations

SLAM Solutions Logiciels et Applications Métiers

Lycée Jean-Jacques ROUSSEAU - MONTMORENCY



Tuteur : SALVADOR Enrique

Stage de Première année du 29 Mai 2017 au 23 Juin 2017

Mairie de Montmorency - Service Systèmes d'Information et Télécommunications

Remerciements

Je souhaite remercier Enrique SALVADOR pour la confiance qu'il m'a accordée.

Je souhaite également remercier l'ensemble du personnel du service informatique pour m'avoir intégré dans l'équipe, leur accueil et leur aide tout au long du stage.

I. Présentation



STATUT JURIDIQUE

Le **statut juridique** en droit français est un ensemble de textes qui règlent la situation d'un groupe d'individus, leurs droits, leurs obligations. Il sert à distinguer les indépendants des autres catégories d'actifs qui sont essentiellement composées de salariés.

En France, il existe différents **statuts juridiques** possibles pour une **entreprise**. Comme :

- Les *entreprises individuelles* (85% des entreprises aujourd'hui en France). Elle est la propriété d'une seule personne responsable. En s'inscrivant au Registre du Commerce et des Sociétés/Répertoire des Métiers, elle a un statut de petite entreprise.
- Les *sociétés civiles* (SC) : qui peuvent être immobilière (SCI), professionnelle (SCP) ou de moyen (SCM). Elles regroupent artisans, exploitants agricoles, professions libérales, immobilier à titre familial.
- *EIRL* (Entrepreneur Individuel à Responsabilité Limitée), *EURL* (Entreprise Unipersonnelle à Responsabilité Limitée), *SARL* (Société à Responsabilité Limitée)
- *SAS* ou *SASU* (Société par Actions Simplifiée (Unipersonnelle))
- *SA* (Société Anonyme).

Le choix entre ces différents statuts est fait en fonction de critères comme la volonté ou non de s'associer, la protection du patrimoine personnel, du régime social ou fiscal de l'entrepreneur, des besoins financiers, etc.

La Mairie est une **Collectivité territoriale** (*Administration publique*).

ACTIVITE(S)

La Mairie a des **obligations de services** comme l'Etat civils, l'Enseignement, l'Entretien et la protection de la commune, l'Aide sociale, le Centre Communal d'Actions Sociales (CCAS) etc.

Elle propose également des **services facultatifs** comme les loisirs etc.

TYPE D'ACTEUR DU SECTEUR INFORMATIQUE

La Mairie est **acteurs de la demande**. L'organisme va se payer les services ou bien les solutions du marché.
Elle va, par ailleurs, également fournir services à la ville.

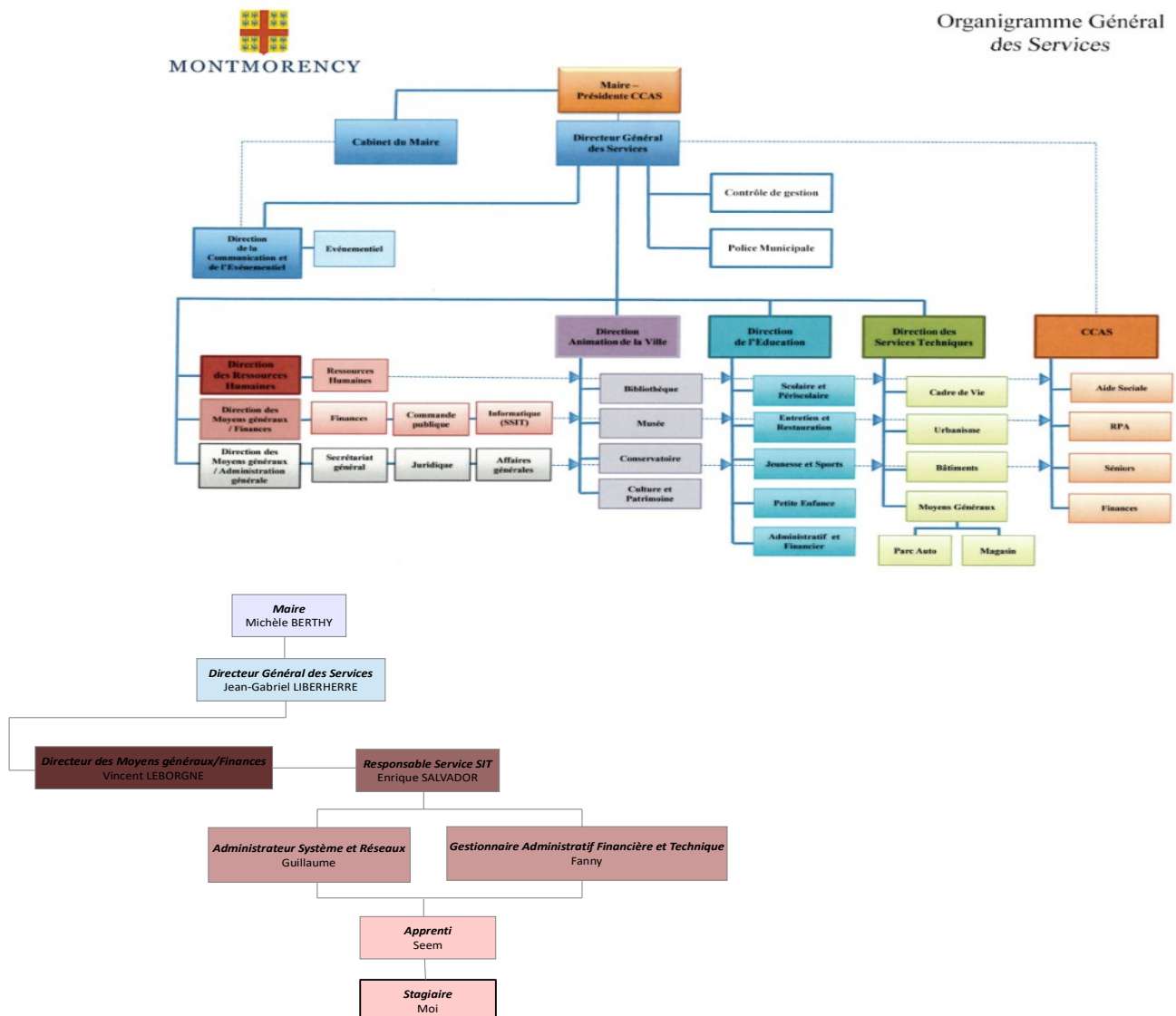
RESSOURCES TANGIBLES ET INTANGIBLES

Les **ressources tangibles** sont imitables et ne procurent pas vraiment d'avantages durables.

Les **ressources intangibles** sont distinctives, spécifiques et constituent le capital immatériel de l'entreprise.

- ✓ Ressources tangibles (ou matérielles)
 - **Physiques** : La mairie (le bâtiment), le matériel disponible aux personnels ...
 - **Financières** : Capacité financière (budget de la ville)
- ✓ Ressources intangibles (ou immatérielles)
 - **Technologiques** : savoir-faire ...
 - **Commerciales** : Réputation, notoriété, relations avec la ville ...
 - **Humaines** : dynamisme du personnels/ des équipes, flexibilité, capacité à échanger des informations ...
 - **Organisationnelles** : Système d'information, base de données, mécanismes de coordination ...

ORGANIGRAMME



II. *Le Marché*

MARCHE DE L'ENTREPRISE

Le **marché** est le lieu de rencontre entre l'offre et la demande, lieu où se déterminent les prix et les quantités échangés. **Offreurs et demandeurs** viennent échanger des biens et des services moyennant paiement.

L'offre c'est l'ensemble des producteurs, des distributeurs, des vendeurs.

La Demande c'est l'ensemble des consommateurs sur le marché.

L'objet principal du marché concerné est le service.

L'Offre est représenté par l'ensemble des services rendus par la mairie en elle même.

Les demandeurs sont des établissements publics notamment dans le secteur de l'éducation de l'aide social etc.

On peut donc conclure qu'il s'agit d'un monopole (un seul offreur).

Nous n'avons pas de chiffres permettant d'analyser le marché.

ZONE D'INTERVENTION

La **Mairie** intervient sur la Ville de Montmorency.

PLACE SUR LE MARCHE

Une **place de marché** est un lieu où se rencontre des multiples acteurs des marchés financiers.

La mairie est le cœur de la ville, elle dirige la ville. Aucun concurrent direct ne peuvent être identifiés. En effet, elle fournit des services à moindre coût pour les habitants de la ville. En revanche, des entreprises privées peuvent essayer de rivaliser avec celle-ci.

PRINCIPAUX CONCURRENTS

Les entreprises exerçant la même activité et offrant des produits ou services plus ou moins similaires sont des **entreprises concurrentes**.

Les **concurrents d'une mairie** peuvent être locaux/nationaux. Le but des Mairies : Attirer les habitants (Environnement) et les entreprises (taxes professionnelles) qui permettent d'assurer les **services** municipaux, améliorer l'image de la ville, développer son attractivité, et relancer son activité économique.

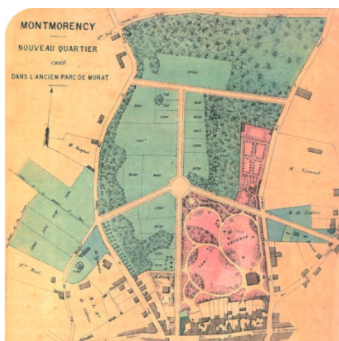
RECOURS A L'EXTERNALISATION

Externalisation est le fait de transférer à l'extérieur certain de ses activités.

Pour une entreprise externaliser consiste à se séparer d'une activité réalisée jusque-là en interne et de faire appel à une société de services spécialisés.

La Mairie a recours à des prestataires extérieurs pour la réalisation de son site web ou encore la réalisation d'une application mobile.

III. *Historique*



1788 : Construction de la propriété de Louis Nicolas Goix (Actuel hôtel de ville)

Cet ancien hôtel particulier a été construit dans un parc de 13 hectares à la fin du XVIII^e siècle par Nicolas-Louis Goix, commis de la Marine royale. De cet illustre propriétaire, restent les ornements marins – une ancre est encore visible le long de la grille du côté de la rue Théophile Vacher. Emilien Rey De Foresta achète l'ensemble en 1859. Il divise alors son domaine, créant ainsi de nouveaux quartiers. Il conserve une partie du parc et l'hôtel particulier pour son usage privé. L'état actuel du bâtiment et du parc a conservé l'aménagement de Rey

De Foresta, avec ses petites allées, son kiosque, sa pelouse centrale, et sa grille ouvragée. Rey De Foresta devient maire de Montmorency en 1865. La ville fait l'acquisition de la propriété en 1906, le bâtiment devient alors l'hôtel de Ville, et son parc un jardin public.

Par ailleurs, les initiales « RF » que l'on retrouve sur la grille de l'entrée principale rue Théophile Vacher, renvoient à son dernier occupant, et non pas à la fonction actuelle du bâtiment, contrairement à celles des façades.

IV. *Développement Durable*

Le **développement durable** est un développement qui répond aux besoins du présent sans compromettre la possibilité, pour les générations à venir, de pouvoir répondre à leurs propres besoins.

En faveur au développement durable, La Mairie a mis en place un Plan Local d'Urbanisme (il s'agit d'un document réglementaire spécifique à la ville, régi par les dispositions du code de l'Urbanisme. Il remplace l'ancien Plan d'Occupation des Sols (POS). Il a aussi pour enjeu de déterminer à quoi ressemblera la ville de demain). Elle a également mis en place un Projet d'Aménagement et de Développement Durables.

V. *Système d'Information*

CONTRAT INFORMATIQUE TYPE DE L'ENTREPRISE

Un **contrat informatique** fait référence à une vente ou la location d'objets appartenant au domaine de l'informatique comme du matériel (ordinateur, disque dur externe ...) ou des logiciels.

Le **contrat de maintenance** est un **contrat** fondamental en informatique notamment qui régit notamment le contenu des prestations et les obligations des parties en matière de maintenance.

✓ Version papier du contrat également disponible.

CHARTRE INFORMATIQUE

La **charte informatique** est un document interne établissement, en accord avec la législation, les responsabilités des utilisateurs, des installations informatiques d’une entreprise, d’une administration, d’une association ... Elle établit les règles minimales de courtoisie et de respect d’autrui pour un usage correct des ressources informatiques et des services réseaux. Elle fait également connaître aux utilisateurs les mesures de sécurité adoptées.

✓ Version informatisé (pdf) également disponible

REPUBLIQUE FRANÇAISE
 Montmorency
 PÔLE RESSOURCES INTERNES
 Service Systèmes d'information et télécommunications
 CHARTRE DU BON USAGE ET DE LA SECURITE
 DE L'INFORMATIQUE ET DES RESEAUX
 I. REGLES D'USAGE DE L'EQUIPEMENT INDIVIDUEL.....2
 L'utilisateur doit prendre soin des outils mis à sa disposition2
 Il doit assurer la protection de ses propres informations2
 Il ne doit pas porter atteinte à la sécurité par négligence2
 Il ne doit pas se procurer les droits d'un autre utilisateur3
 II. REGLES D'USAGE DES RESSOURCES COMMUNES3
 Contrôle des accès aux dossiers4
 Contrôle de l'accès internet4
 Respect du principe d'équité4
 Respect de la confidentialité4
 Respect de la déontologie d'Internet5
 III. MISE EN ŒUVRE DE LA MAINTENANCE6
 Conduite des opérations d'exploitation6
 Demandes d'intervention7
 IV. RÉGIME JURIDIQUE DES LIMITES D'UTILISATION7
 Utilisation extra-professionnelle7
 Respect de la loi Informatique et Liberté8
 Violation de la protection du logiciel8
 Téléchargement et propriété intellectuelle9
 V. SANCTIONS9
 Sanctions administratives9
 Sanctions pénales9

La Mairie met à la disposition de ses agents divers moyens informatiques, qu'il s'agisse d'équipements individuels, comme les postes de travail, ou de ressources partagées comme l'accès à Internet.

La présente charte vise à faire connaître les règles régissant l'usage de ces moyens informatiques, à présenter le rôle et les responsabilités de ceux qui interviennent dans la gestion de ces moyens et à explorer les procédures mises en œuvre afin d'en assurer l'utilisation la plus efficace.

Elle vise également à faire prendre conscience de certains risques encourus à l'occasion de l'utilisation des outils informatiques.

Elle présente en outre l'état actuel de la législation française en matière de délits informatiques, ainsi que les sanctions encourues.

I. REGLES D'USAGE DE L'EQUIPEMENT INDIVIDUEL

On entend par « utilisateur » toute personne ayant accès à des moyens informatiques mis à sa disposition par la collectivité.

Tout utilisateur est responsable de l'usage qu'il fait de son équipement individuel, l'attention qu'il porte à se conformer à quelques principes simples contribuant à la sécurité générale.

L'utilisateur doit prendre soin des outils mis à sa disposition

- Il doit participer aux sessions de formation proposées par la collectivité et employer correctement les matériels et logiciels avec lesquels il travaille ; l'assistance ne doit normalement être sollicitée que sur des fonctionnalités non courantes ;
- Il ne doit pas détourner ces outils vers un usage pour lequel ils n'auraient pas été prévus ;

- Il ne doit pas procéder, en dehors du contrôle du responsable du service informatique, à l'installation de logiciels sur son poste, l'équipement devant demeurer, pour des raisons d'efficacité de la maintenance dans la configuration standard.

Il doit assurer la protection de ses propres informations

- Il lui appartient de protéger ses données professionnelles en utilisant les différents moyens de sauvegarde disponibles, notamment l'espace mis à sa disposition sur le réseau ;
- Il doit signaler au responsable informatique toute tentative de violation de son compte, et de façon générale, toute anomalie qu'il peut constater.

Il ne doit pas porter atteinte à la sécurité par négligence

- S'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes

REPUBLIQUE FRANÇAISE
 Montmorency
 ou aux réseaux dont il a l'usage ;
 • il doit garder secret ses mots de passe, et en aucun cas, les communiquer à des tiers ou les noter sur un support visible par d'autres ;
 • il doit verrouiller sa session lorsqu'il quitte son poste de travail (Ctrl+Alt+Supr) afin de ne pas laisser d'informations accessibles ;
 • il ne doit pas laisser en évidence tous supports amovibles susceptibles d'être dérobés (disquettes, cédéroms, clés USB ou équivalents). Il lui appartient de placer en lieu sur ces éléments amovibles ;
 • il doit faire preuve de vigilance concernant les fichiers qu'il télécharge, les supports magnétique ou électronique d'origine douteuse ou les messages qu'il reçoit s'il ne connaît pas leur provenance. Les virus qu'ils seraient susceptibles de contenir constituent, en effet, un danger pour ses données personnelles comme pour le réseau en général. En cas de détection d'un virus, l'utilisateur doit immédiatement informer un agent du service informatique, afin que ce dernier puisse exercer au mieux sa fonction de protection du parc informatique et minimiser les dysfonctionnements éventuels ou potentiels.
 Il ne doit pas se procurer les droits d'un autre utilisateur
 • il ne doit pas utiliser ou essayer d'utiliser les mots de passe autre que le sien ;
 • il ne doit pas chercher à obtenir des droits d'accès plus larges que ceux qui lui ont été attribués, dont les limites sont justifiées par un impératif de sécurité ;
 • il ne doit pas tenter de lire, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement.
 II. REGLES D'USAGE DES RESSOURCES COMMUNES
 On entend par « ressources communes » tout ce qui est accessible par le réseau (accès internet, fichiers partagés, ...)
 L'utilisation de ressources communes au travers du réseau s'accompagne d'une augmentation des risques d'atteinte à la sécurité et implique certaines règles.
 Contrôle des accès aux dossiers
 L'utilisation des ressources informatiques partagées est toujours, par mesure de protection, soumise à autorisation. En pratique cette autorisation se traduit par une déclaration de l'utilisateur sur un serveur et par l'attribution d'un mot de passe. Chaque utilisateur bénéficie ainsi d'un accès à certaines ressources, en particulier l'internet à haut débit.

REPUBLIQUE FRANÇAISE
 Montmorency
 Comme il est d'usage, un second mot de passe dit « administrateur » est conservé par les agents du service informatique. Il permet d'installer les logiciels et d'assurer la maintenance du système.
 L'autorisation ainsi accordée est strictement personnelle et ne doit en aucun cas être cédée à un tiers par divulgation du mot de passe.
 Elle peut être retirée à tout moment, par mesure de sécurité, le temps d'une investigation technique, s'il est constaté un usage anormal.
 Cette autorisation d'accès prend fin lors de la cessation définitive de l'activité au sein de la collectivité (retraite, mutation) et est suspendue en cas d'absence longue (congé maternité, longue maladie, ...).
 Contrôle de l'accès internet
 Techniquement, le filtrage de l'accès internet s'appuie sur l'utilisation du logiciel de contrôle « Webfilter ».
 Conformément à l'article R. 10-13 –I du Code des postes et des communications électroniques, pris en application du II de l'article L. 34-1 du même code, la Mairie est tenue de conserver pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :
 Les informations permettant d'identifier l'utilisateur ;
 Les données relatives aux équipements terminaux de communication utilisés ;
 Les caractéristiques techniques ainsi que la date, l'heure et la durée de chaque communication ;
 Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
 Les données permettant d'identifier le ou les destinataires de la communication.
 Ces informations sont conservées durant un an, conformément à la loi.
 Respect du principe d'équité
 L'utilisation d'une ressource commune doit se faire de manière équitable. Aucun utilisateur n'a le droit de monopoliser cette ressource de façon abusive pour ses propres besoins.
 En particulier, il convient de faire un usage raisonnable de la possibilité de sauvegarder des fichiers sur les disques partagés, en procédant régulièrement à un nettoyage de son armoire, qu'il transfère la partie définitivement liée de celui-ci sur cédérom (les CD sont fournis pas le service financier comme les fournitures administratives).
 Respect de la confidentialité
 Les fichiers d'un utilisateur sont réservés à son propre usage (même s'ils comportent certaines possibilités d'utilisation par des tiers). Partant de ce principe, la possibilité de lire un fichier n'équivaut pas à l'autorisation de le lire.
 Il est interdit de prendre connaissance d'informations translat sur le réseau ou détenues par

REPUBLIQUE FRANÇAISE
 Montmorency
 d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux courriers électroniques dont l'utilisateur n'est destinataire ni directement ni en copie.
 Dans le cas où un utilisateur s'aperçoit que les données ne lui appartenant pas lui sont accessibles, il doit en aviser un agent du service informatique, afin que celui-ci puisse prendre les dispositions nécessaires.
 Il est rappelé qu'il est pénalement sanctionné le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système informatique, même s'il n'en résulte aucune suppression ou modification des données, ni aucune altération du fonctionnement du système.
 Respect de la déontologie d'Internet
 L'interconnexion à travers les réseaux d'internet met à la disposition des utilisateurs de la Mairie des ressources considérables. L'utilisateur doit faire usage de ces services Internet en respectant certaines règles de bonne conduite.
 • il ne doit pas se connecter, ou essayer de connecter par des manœuvres de contournement, à un serveur d'accès restreint dont l'entrée ne lui est pas autorisée ;
 • il ne doit pas se livrer à des actions mettant en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
 • il ne doit pas, par manipulation de paramètres d'identification, usurper l'identité d'une autre personne ou intercepter une communication entre tiers ;
 • il ne doit pas exécuter ou réaliser un programme informatique ou utiliser l'accès Internet mis à sa disposition pour proposer, ou rendre accessible aux tiers, des informations confidentielles ou contraires à la législation en vigueur, notamment celle relative aux publications à caractère inouïeux, raciste, pornographique, diffamatoire, terroriste ;
 • il doit faire preuve de courtoisie à l'égard de ses interlocuteurs dans les échanges électroniques par courrier ou dans les forums de discussions ; l'utilisateur doit être conscient que les échanges par messagerie électronique ne sont pas anonymes et, en particulier, qu'ils sont faits avec l'adresse indiquant l'appartenance de l'utilisateur aux services municipaux. Les prises de position doivent être conformes aux intérêts de la mairie ;
 • il doit se montrer vigilant vis-à-vis de la réception de pièces attachées à des courriers électroniques, afin d'éviter la propagation des virus informatiques. En cas de doute, en particulier sur l'expéditeur, il ne doit jamais ouvrir les fichiers joints ni exécuter les programmes envoyés par celui-ci et contacter le service informatique ;
 • il doit éviter de monopoliser à son seul profit les capacités techniques de la connexion Internet,

REPUBLIQUE FRANÇAISE
 Montmorency
 excédant cinquante personnes, le spamming (diffusion massive et non désirée de messages) à destination des agents ou d'usagers externes et le transfert de messages d'alerte sur les virus. En cas de doute ou d'interrogation sur l'existence de virus, seuls les agents du service informatique sont autorisés à communiquer avec l'ensemble des utilisateurs de l'informatique de la Ville.
 III. MISE EN ŒUVRE DE LA MAINTENANCE
 La maintenance de l'équipement informatique et des ressources auxquelles il est raccordé est assurée par les agents du service informatique. Ces derniers engagent leur responsabilité quant à la qualité du service rendu et disposent en contrepartie de prérogatives techniques leur donnant les moyens d'assurer le bon fonctionnement des outils mis à la disposition des utilisateurs. De leur côté les utilisateurs doivent solliciter le service informatique à bon escient afin de préserver l'efficacité de sa capacité d'intervention.
 Conduite des opérations d'exploitation
 En vue d'assurer le bon fonctionnement des outils mis à la disposition des utilisateurs, les agents du service informatique disposent de certains moyens d'action, relevant soit des opérations courantes d'exploitation, soit des mesures conservatoires pour faire face à un incident ; ils s'appuient techniquement sur l'utilisation du logiciel de contrôle « Webseense ».
 Les agents du service informatique peuvent :
 • surveiller régulièrement l'utilisation du système pour pouvoir détecter les anomalies et les intrus ;
 • procéder aux ajustements de capacité des outils, conformément aux décisions prises par la Direction, eu égard à l'évolution des besoins ;
 • imposer temporairement, pour faire face à une surcharge, des limitations, sous forme de quotas, à l'ensemble des utilisateurs (un temps maximal de connexion ou une place maximale sur un disque par exemple) ;
 • interrompre une procédure suspecte violant manifestement les règles de fonctionnement courantes ;
 • modifier temporairement certains droits ou certaines priorités pour l'ensemble ou une partie des utilisateurs ;
 • accéder, dans un but d'investigation, aux ressources d'utilisateurs susceptibles d'avoir été, sciemment ou involontairement, à l'origine d'un dysfonctionnement.
 Les agents du service informatique respectent en contrepartie un certains nombre de règles :

REPUBLIQUE FRANÇAISE
 Montmorency
 • la confidentialité, l'accès aux données des utilisateurs (fichiers, messages) devant se faire strictement dans le cadre du diagnostic d'un dysfonctionnement ;
 • informer les utilisateurs des arrêts prévus, au moyen du courrier électronique notamment, chaque fois qu'une anticipation est possible ;
 • minimiser les durées d'indisponibilités ;
 • informer la hiérarchie de toute investigation en cours.
 Demandes d'intervention
 Une application extranet destinée à la saisie des demandes d'intervention informatique sera mise en place sous peu.
 En attendant, les demandes d'intervention sont à adresser à un des agents du service informatique (par message électronique ou téléphone), qui analyse le problème, le résout éventuellement ou décide de faire appel à la maintenance extérieure.
 IV. RÉGIME JURIDIQUE DES LIMITES D'UTILISATION
 Dans un souci de bonne information des utilisateurs, il paraît opportun de présenter, ci-après, les principales dispositions relatives aux usages illicites de l'informatique.
 L'utilisateur s'engage à utiliser les services :
 • dans le respect des lois relatives à la propriété littéraire et artistique ;
 • dans le respect des lois relatives à l'informatique, aux fichiers et aux libertés ;
 • dans le respect des règles relatives à la protection de la vie privée et notamment du droit à l'image d'autrui ;
 • en s'assurant de ne pas envoyer de messages à caractère raciste, pornographique, pédopédophile, injurieux, diffamatoire, et, de manière générale, à ne pas diffuser d'informations présentant le caractère d'un délit.
 Utilisation extra-professionnelle
 Toutes les ressources informatiques mises à la disposition des utilisateurs sont par définition destinées à un usage professionnel. Un usage personnel raisonnable de ces moyens est admissible dans la mesure où l'activité professionnelle ne s'en trouve aucunement affectée, et s'il n'est pas contraire à la loi.
 L'accès à certains sites (radios, chats, jeux, ...) dont l'utilisation perturbe l'activité des utilisateurs et l'efficacité du réseau pourra être limité ou interdit.

REPUBLIQUE FRANÇAISE
 Montmorency
 Respect de la loi Informatique et Liberté
 Si dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers contenant des informations nominatives, la Commission Nationale de l'Informatique et des Libertés (CNIL) doit au préalable être saisie sous forme d'une demande d'avis ou d'une déclaration simplifiée pour les traitements les plus courants. La seule entité à la mairie habilitée à effectuer ces formalités auprès de la CNIL est le service des Affaires Juridiques.
 Violation de la protection du logiciel
 En vertu de la loi n°85-660 du 3 juillet 1985 et de la loi n° 92-597 du 1er juillet 1992 relatives à la protection des logiciels et à la propriété intellectuelle, le logiciel bénéficie des mêmes protections que toute œuvre intellectuelle. Seule une copie de sauvegarde est autorisée pour un logiciel officiellement acheté. Toute autre copie est illicite et assimilée à un acte de vol. Le code source d'une application ne peut être inclus dans une application qui va être utilisée ailleurs.
 Le contournement des restrictions d'utilisation d'un logiciel est considéré comme un délit, dont la sanction peut aller jusqu'à deux ans de prison ferme et 150 000 euros d'amende.
 En particulier, sont sanctionnées les délits suivants :
 • contrefaçon d'une œuvre de l'esprit (y compris d'un logiciel) (Art. 335-2 et 335-3 du code de la propriété intellectuelle) ;
 • contrefaçon d'un dessin ou d'un modèle (Art. 521-4) ;
 • contrefaçon de marque (Art. 716-2 et suivants).
 Tout utilisateur auteur ou responsable de reproduction illicite devra seul supporter les condamnations pénales encourues, même s'il n'a pas agit dans son intérêt personnel.
 Téléchargement et propriété intellectuelle
 Les données circulant sur Internet peuvent être réglementées en termes d'utilisation ou être protégées par un droit de propriété intellectuelle. L'utilisateur est responsable de l'utilisation des données qu'il consulte et transfère et doit notamment, à cet effet, disposer de toutes les autorisations nécessaires (telles que licences d'autorisation, droit de reproduction des images, textes et sons, etc...).
 Tous les téléchargements de logiciels, même s'ils sont gratuits, doivent respecter les droits de propriété intellectuelle et de protection des logiciels et ne peuvent être effectués en dehors du contrôle d'un agent du service informatique.

REPUBLIQUE FRANÇAISE
 Montmorency
 V. SANCTIONS
 Le non respect des règles de bonne conduite fixées par cette charte, ainsi que les textes de loi en vigueur, conduit à des sanctions administratives ou pénales.
 Sanctions administratives
 Elles sont prises par le Maire qui jugera de la gravité de l'acte et prendra les sanctions adéquates.
 Sanctions pénales
 Par ailleurs, l'utilisateur responsable d'une violation constatée pourra être poursuivi pénalement.
 Fait à Montmorency, le
 Le Maire
 Vice-Président
 De la Communauté d'Agglomération
 De la Vallée de Montmorency
 François Deltion

NOM DE DOMAINE/PROTECTION DE L'ENTREPRISE

Un **nom de domaine** est une chaîne de caractères (ex : google) associée à une extension (ex : .com, .fr ...). Il constitue ainsi un nom familier associé à une adresse IP.

Le *nom de domaine* de la ville de Montmorency : <http://www.ville-montmorency.fr/>

Les *collectivités territoriales* ne disposent pas d'un droit d'exploitation exclusif mais elles peuvent le protéger préventivement (déposition du nom auprès de l'INPI). En effet, elles sont protégées seulement s'il y a atteinte à des intérêts publics.

La *collectivité territoriale* ne représente pas l'intérêt général, mais en principe, l'intérêt d'une fraction du public, ses administrés. En conséquence, les droits qui lui sont confiés doivent être limités aux missions de service public, car le maire pourrait être tenté d'utiliser ces droits à des fins personnelles.

Les *noms des collectivités territoriales* ont une place spécifique dans le droit des marques.

En effet, la **collectivité territoriale** s'est vue accorder, non pas un monopole, mais des droits sur son nom afin de préserver ses intérêts qui sont en fait ceux de ses administrés et donc d'une section du public.

La marque n'est qu'une protection fugace, car au-delà des cinq années suivant son enregistrement la marque est ouverte à la déchéance pour non usage. Ce qui est problématique, car la marque n'est pas forcément utilisée par la collectivité pour tous les services déposés.

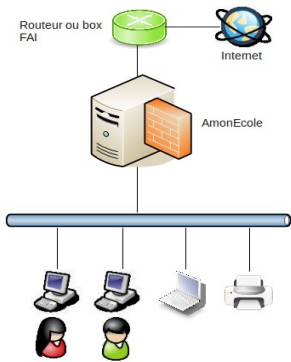
PROBLEME(S) JURIDIQUES RENCONTRES (LITIGES)

Un **problème/litige juridique** est un désaccord entre deux ou plusieurs personnes (physiques ou morales) concernant l'exercice d'un droit. Ce désaccord peut naître d'un contrat ou d'une situation de fait.

La Mairie de Montmorency n'a rencontrées aucuns litiges liée au nom de domaine jusqu'à présent.

OBJECTIF

Remplacer une **solution de filtrage** de l’Education Nationale (**AmonEcole**) par un autre produit gratuit et répondant aux mêmes exigences de sécurité **IPFire**.

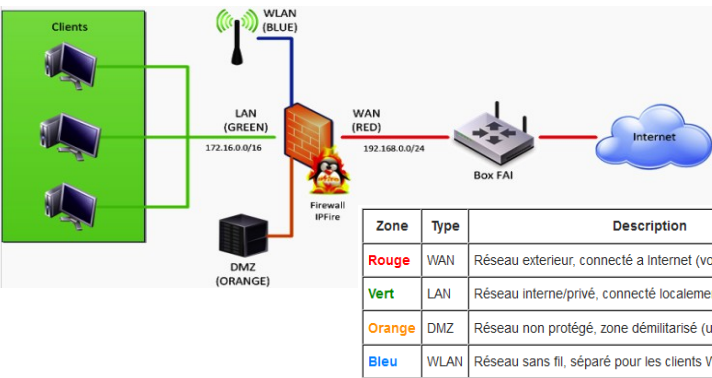


AMONECOLE

AmonEcole est un serveur utilisé comme pare-feu, contrôleur de domaine et comme serveurs de fichiers.

Il permet le filtrage d’accès et la navigation web. Il permet également de gérer le partage de fichiers et la messagerie élèves ainsi que l’Installation du portail ENVOLE (ENT).

IPFIRE

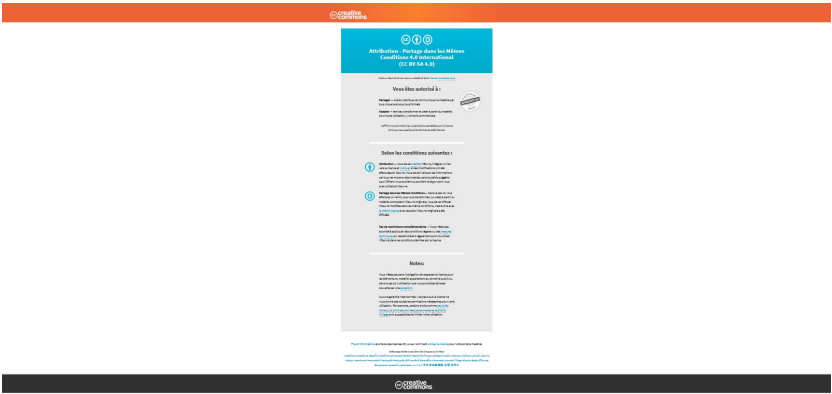


IPFire est un logiciel OpenSource libre. C’est un pare-feu permettant de sécuriser le réseau à l’aide du filtrage d’accès notamment.

SOLUTION DE FILTRAGE

L’Académie de Toulouse utilise une Blacklist que l’Education nationale elle-même recommande. Le **Filtrage d’URL** est par logiciel une comparaison entre la requête d’un utilisateur et une liste préétablie.

La Blacklist de l’Académie de Toulouse est sous **licence Creative Common**.



GUIDE IPFire



I° Installation

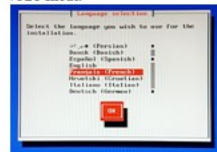
1° Télécharger ipfire.iso
<http://www.ipfire.org/download>
 2° Graver l'image iso sur un CD

Rappel Clavier Linux : Tab (se déplacer),
 Espace (sélectionner), Entrée (Valider)

3° Insérer le CD d'installation – L'écran d'accueil s'affiche – Démarrer l'installation.



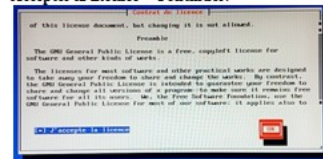
4° Sélectionner la langue pour l'installation – Français (French) - Valider votre choix.



5° Un message d'accueil s'affiche – Démarrer l'installation – Valider.



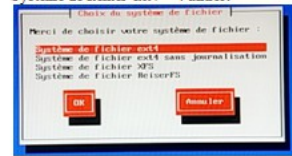
6° Le contrat de Licence s'affiche – Accepter la Licence – Continuer.



7° Formatage du disque pour l'installation (Attention à vos données, faites les nécessaires avant) - Suppression de toutes les données présentes – Valider.



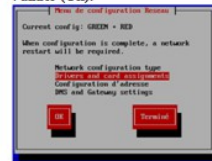
8° Sélectionner le système de fichiers – Système de fichier ext4 – Valider.



9° IPFire a été installé avec succès – Enlever le CD – Redémarrer.



16° On arrive de nouveau sur le menu de configuration réseau – On s'occupe maintenant de l'Attribution des cartes - Se placer sur 'Drivers and card assignments' – Valider (Ok).



On va devoir choisir une carte réseau pour chaque interface – On commence avec la 'GREEN' – Sélectionner.



Dans notre cas, On choisira pour celle-ci 'pci : Marvell Technology [...]' – Sélectionner.



On vient d'attribuer à la 'GREEN' une carte réseau – On va ensuite définir la 'RED' – Se placer sur 'RED' - Sélectionner.



On choisira pour celle-ci 'pci : 3Com Corporation [...]' – Sélectionner.



On vient de définir à chaque interface une carte réseau – Sélectionner Terminé.



17° Se placer à présent sur 'Configuration d'adresse' – Valider (Ok).



On va commencer par configurer l'interface 'GREEN' (Correspond à l'Adresse IP Interne) – Valider (Ok).



Un message d'avertissement s'affiche – Continuer (Ok).



II° Configuration

10° Sélectionner le type de clavier vous correspondant au mieux – fr (Azerty) – Valider.



11° Sélectionner le fuseau horaire – Europe/Paris – Valider.



12° Définir le nom d'hôte de la machine – Valider.



13° Définir le nom de domaine – Valider.



14° Définir un mot de passe pour 'root' et 'admin' (Majuscules, minuscules et caractères spéciaux) – Si le mot de passe n'apparaît, tout est normal - Valider.



15° On va démarrer la Configuration du réseau – On commence par définir le type – Se placer sur 'Network configuration type' – Valider (Ok).



Dans notre cas, on choisira 'GREEN + RED' – Valider.



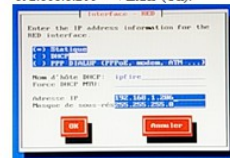
On attribue à 'GREEN' une adresse Ip et un masque de sous-réseau – Dans notre cas, on donne à GREEN '10.0.1.254' – Continuer (Ok).



On va ensuite configurer l'interface 'RED' (Correspond à l'Adresse IP Externe) – Se placer sur 'RED' - Valider (Ok).



Dans notre cas, la carte 'RED' est paramétrée Statique – Sélectionner STATIQUE – Attribuer à RED '192.168.1.206' – Valider (Ok).



On va finir par paramétrer le DNS et la Passerelle – Valider (Ok).



Dans notre cas, on attribue au DNS primaire '8.8.8.8' et à la passerelle par défaut '192.168.1.1' – Valider (Ok).



La configuration du réseau est Terminée.



18° Activer le Serveur DHCP – Définir une adresse de début (10.0.1.2) et une adresse de fin (10.0.1.200) – Valider (Ok).



19° L'Installation d'IPFire est à présent terminée.



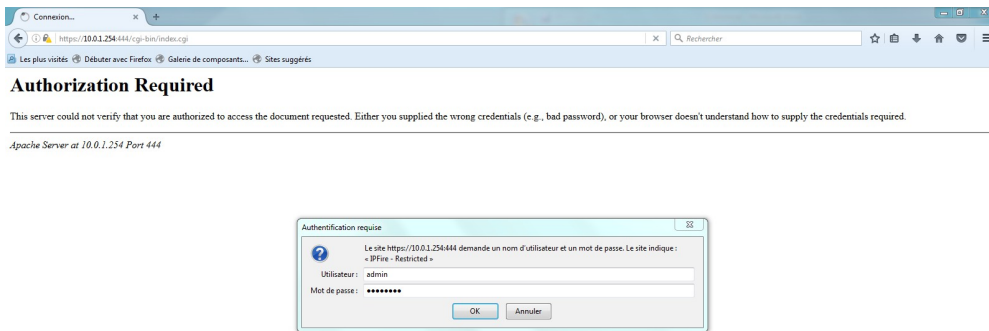
20° Identification requise (root) – C'est à vous !



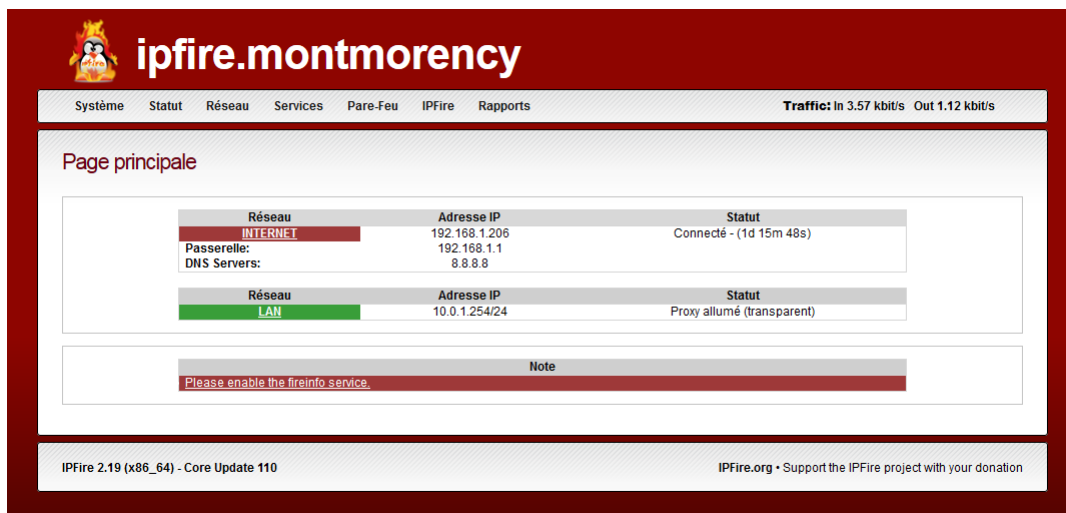
CONFIGURATION IPFIRE

On accède à IPFire via l'adresse suivante : <https://10.0.1.254:444/> (SNPP-Simple Network Paging Protocol)

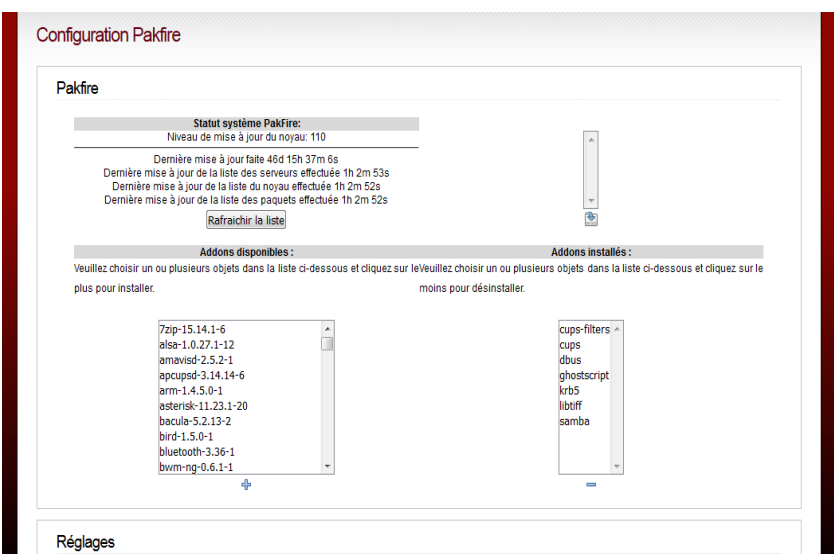
Adresse IPFire IP Interne suivi du port 444 (port 444 est un protocole SNPP permettant d'envoyer des paquets IP en direction d'un programme permettant de basculer d'un bureau virtuel à un autre).



Après authentification, on arrive alors sur la page d'accueil IPFire.



On va configurer Pakfire.



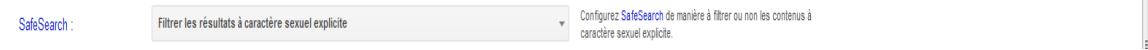
On a installée les addons **samba** (pour le partage de fichiers), **guardian** (pour la sécurisation), **clamAV** et **Squidclamav** (anti-virus), **Iperf** (serveur d'analyse de bande passante), **cacti** (outils de visualisation des données réseau avec RRDTool/SNMP), **sarg** (outil d'analyse graphique des rapports proxy, pouvant être utilisés sur l'interface web), **OpenMailAdmin** (serveur mail).

On configure ensuite les addons qu'on vient d'installer.

De nombreux addons sont disponibles, pouvant être installé/enlevé facilement selon les besoins : <http://wiki.ipfire.org/en/addons/all>

Dans notre cas, on veut : Filtrer les URL, Sécuriser et pouvoir créer un système de partage de fichiers.

On peut activer le Mode SafeSearch sur Google (paramètres (coin en bas à droite) puis recherche avancée). Réaliser les modifications nécessaires.



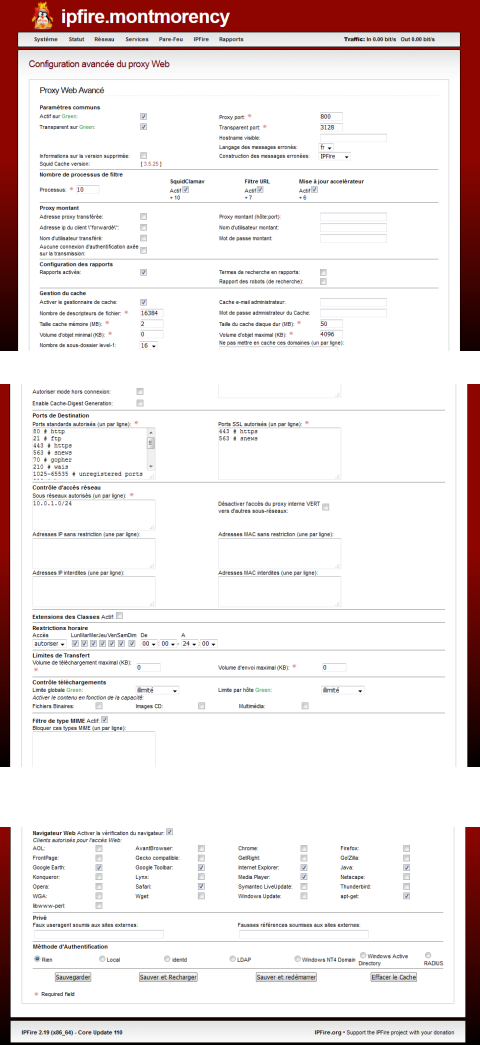
Egalement activer le Mode SafeSearch sur Google (paramètres puis paramètres de recherche). Enregistrer.

Filtres Safe Search

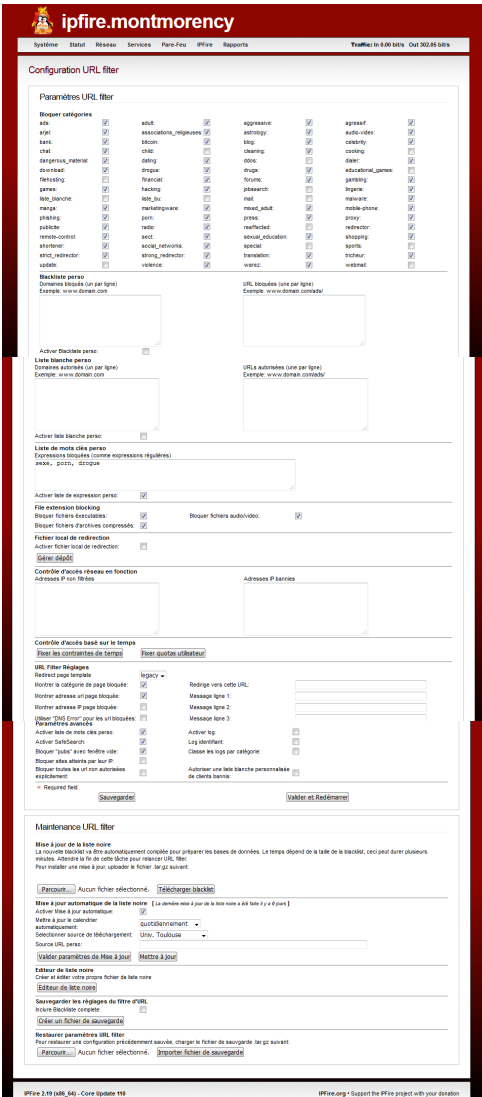
SafeSearch peut vous aider à bloquer les images inappropriées ou explicites dans les résultats de recherche Google. Le filtre SafeSearch n'est pas précis à 100 %, mais il vous permet d'éviter le contenu violent et réservé aux adultes dans la grande majorité des cas.

☒ Activer SafeSearch ☒ Verrouiller SafeSearch

1/ On doit, ensuite, activer le Proxy sur IPFire.



2/ On continue par configurer le filtreur d'URL.

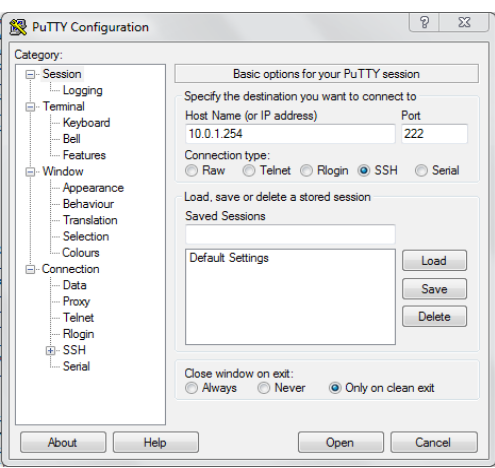


Le Pare-feu est à présent complet, modifiable selon les contraintes spécifiques à l'Education nationale.
Pour finaliser les configurations, on redémarre IPFire.

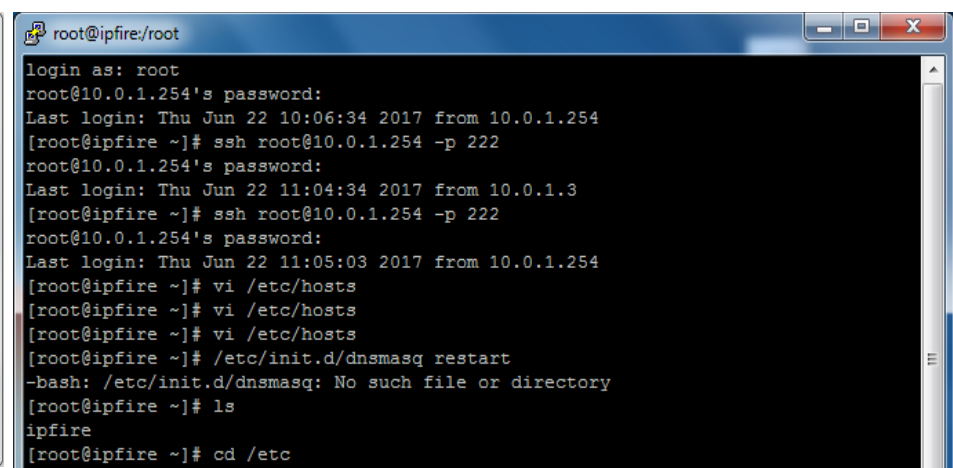


Blocage des sites. Tous ne sont pas bloquer notamment les images avec Google (mode SafeSearch sur Google pouvant être désactivé facilement).

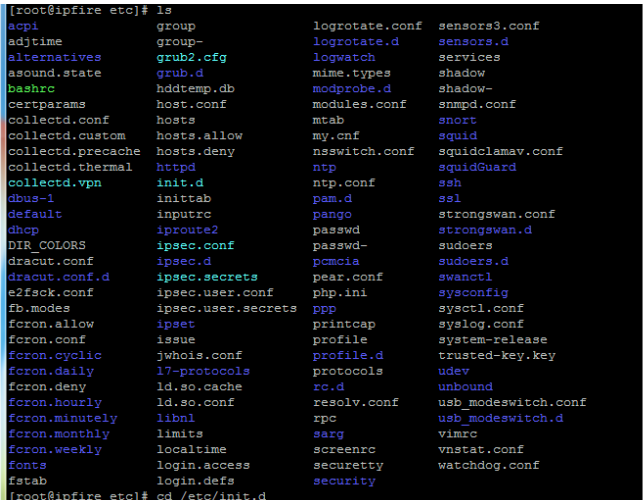
Pour cela, on va essayer le contrôle parental par les DNS.



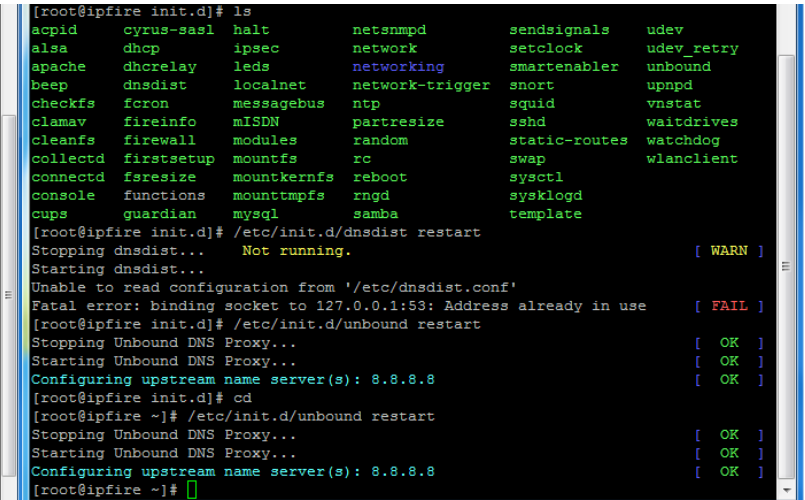
The PuTTY Configuration window shows the 'SSH' connection type selected. The host name is '10.0.1.254' and the port is '222'. The 'Close window on exit' option is set to 'Only on clean exit'.



```
root@ipfire:/root
login as: root
root@10.0.1.254's password:
Last login: Thu Jun 22 10:06:34 2017 from 10.0.1.254
[root@ipfire ~]# ssh root@10.0.1.254 -p 222
root@10.0.1.254's password:
Last login: Thu Jun 22 11:04:34 2017 from 10.0.1.3
[root@ipfire ~]# ssh root@10.0.1.254 -p 222
root@10.0.1.254's password:
Last login: Thu Jun 22 11:05:03 2017 from 10.0.1.254
[root@ipfire ~]# vi /etc/hosts
[root@ipfire ~]# vi /etc/hosts
[root@ipfire ~]# vi /etc/hosts
[root@ipfire ~]# /etc/init.d/dnsmasq restart
-bash: /etc/init.d/dnsmasq: No such file or directory
[root@ipfire ~]# ls
ipfire
[root@ipfire ~]# cd /etc
```

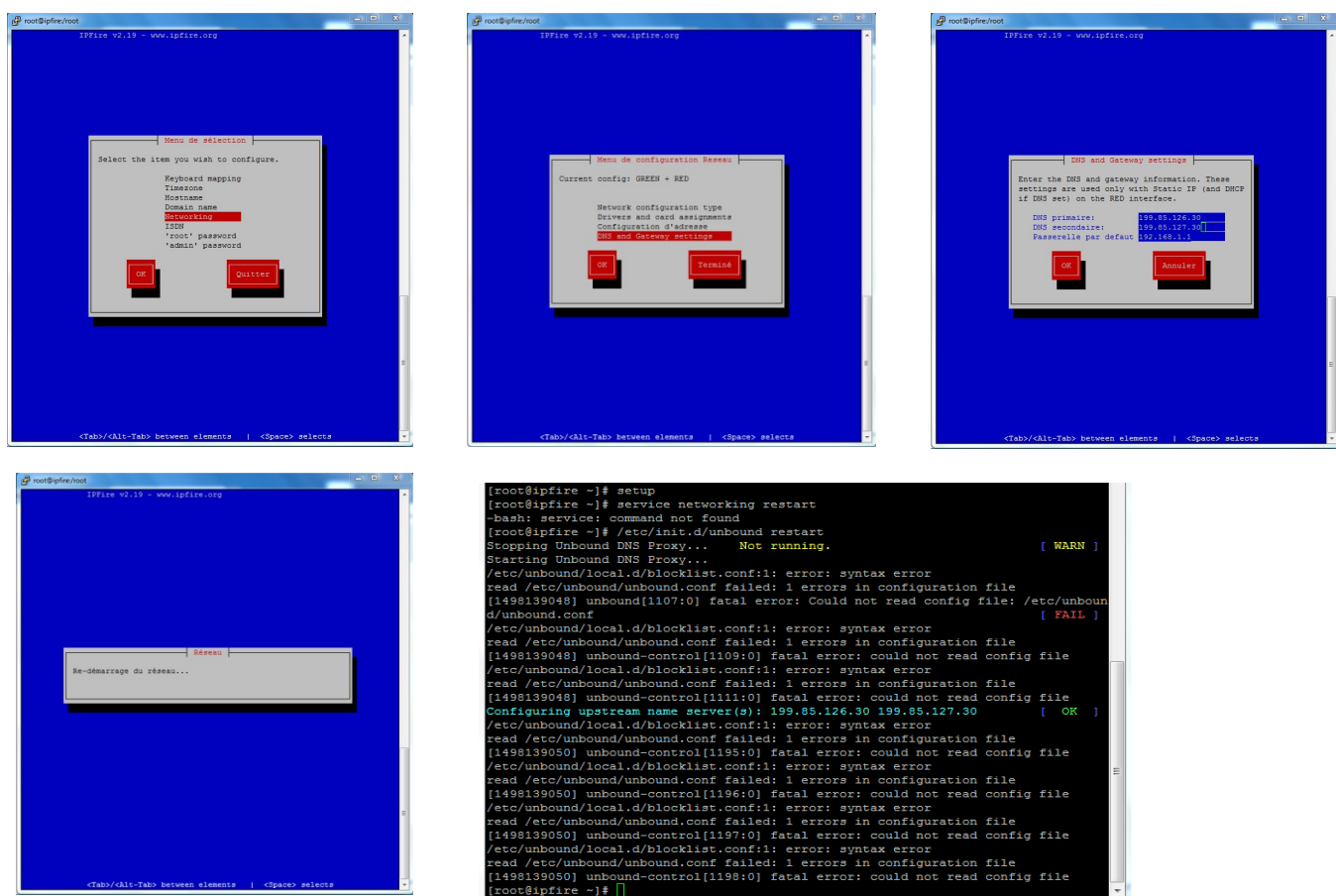


```
[root@ipfire etc]# ls
acpid      group      logrotate.conf  sensors3.conf
adjtime    group-     logrotate.d      sensors.d
alternatives grub2.cfg    logwatch          services
asound.state grub.d      mime.types        shadow
bashrc     hddtemp.db modprobe.d        shadow-
certparams host.conf   modules.conf      snmpd.conf
collectd.conf hosts      mtab              snort
collectd.custom hosts.allow my.cnf             squid
collectd.precache hosts.deny nsswitch.conf     squidclamav.conf
collectd.thermal httpd      ntp               squidGuard
collectd.vpn init.d      ntp.conf          ssh
dbus-1     inittab    pam.d             ssl
default    inputrc    pango             strongswan.conf
dhcp       iproute2   passwd            strongswan.d
DIR_COLORS ipsec.conf pcmcia            sudoers
dracut.conf ipsec.d     pear.conf         swanctl
dracut.conf.d ipsec.secrets php.ini           sysconfig
e2fsck.conf ipsec.user.conf printcap          syslog.conf
fb.modes   ipsec.user.secrets ppp              system-release
fcron.allow ipset      profile           trusted-key.key
fcron.conf jwhois.conf protocols        udev
fcron.cyclic 17-protocols rc.d              unbound
fcron.daily  ld.so.cache resolv.conf       usb_modeswitch.conf
fcron.deny   ld.so.conf rpc               usb_modeswitch.d
fcron.hourly libnl       rsyslogd          vmare
fcron.minutely limits      screenrc          vnstat.conf
fcron.monthly localtime  security          watchdog.conf
fcron.weekly login.access securityty
fonts        login.defs security
fstab
```






```
[root@ipfire init.d]# ls
acpid      cyrus-sasl  halt              netsnmpd        sendsignals    udev
alsa        dhcp        ipsec             network         setclock       udev_retry
apache      dhcprelay  leds             networking      smartenabler   unbound
beep        dnsdist    localnet         network-trigger snort           upnpd
checkfs     fcron      messagebus       ntp             squid           vnstat
clamav      fireinfo   mISDN            partsize        sshd            waitdrives
cleanfs     firewall   modules          random          static-routes  watchdog
collectd    firstsetup mountfs           rc              swap            wlanclient
connectd    fsresize   mountkernfs      reboot          sysctl          syslogd
console     functions  mounttmpfs       rngd            template
cups        guardian   mysql            samba

[root@ipfire init.d]# /etc/init.d/dnsmasq restart
Stopping dnsmasq...      Not running.
Starting dnsmasq...
Unable to read configuration from '/etc/dnsmasq.conf'
Fatal error: binding socket to 127.0.0.1:53: Address already in use
[root@ipfire init.d]# /etc/init.d/unbound restart
Stopping Unbound DNS Proxy...
Starting Unbound DNS Proxy...
Configuring upstream name server(s): 8.8.8.8
[root@ipfire init.d]# cd
[root@ipfire ~]# /etc/init.d/unbound restart
Stopping Unbound DNS Proxy...
Starting Unbound DNS Proxy...
Configuring upstream name server(s): 8.8.8.8
[root@ipfire ~]#
```



Quelques liens pour poursuivre la recherche

-  <http://blog.info16.fr/index.php?article63/controle-parental-avec-opendns-une-solution-alternative-au-proxy>
-  <https://cyrille-borne.com/article2378/le-retour-du-controle-parental-ou-le-filtrage-delicat-de-https-en-action>
-  <http://forum.ipfire.org/viewtopic.php?t=17633>

Conclusion

IPFire bloque les sites voulus (selon la configuration). Par ailleurs, il ne bloque pas les images Google (mode SafeSearch sur Google non activé, facilement désactivable par des enfants) et, ou ne fonctionnent pas correctement. Nous poursuivons nos recherches, il nous reste à présent à tester.