FILEZILLA sous UBUNTU

Réalisé par :

Nezha BENMOUSSA

Master ISIF

proposé par :

Pr RAJI

Année Universitaire : 2012/2013

SOMMAIRE

INTRODUCTION

FileZilla est un client FTP (**File Transfer Protocol**) libre (**GNU**) convenant aussi bien au débutant qu'à l'utilisateur confirmé. C'est un logiciel libre qui permet de charger ou télécharger les fichiers sur un serveur. Par exemple les éléments du site web chez ou depuis un hébergeur. Il possède une interface utilisateur graphique intuitive. Rapide et fiable, *Filezilla* est gratuit et multi-plateforme. En effet, il fonctionne sur tout système d'exploitation et supporte plusieurs types de connexion : client FTP, FTPS et SFTP (mode normal ou sécurisé). Il cible surtout les **webmasters, blogueurs, graphistes et intégrateurs web.**

I. Aperçu historique

C'est au tout début de l'année 2001 que FileZilla a commencé à trotter dans la tête de Tim Kosse et de deux de ses collègues de Computer Science. Conscients de la concurrence des clients ftp déjà disponibles, ils ont décidé de réaliser le leur en open source. Leur idée était de concevoir un client simple avec une interface simple tout en supportant l'ensemble des fonctions de base pour transférer des fichiers sur un serveur. Très rapidement, les versions s'enchaînent. Depuis la Alpha 1, sortie le 27 février 2001, des versions sortent de semaine en semaine pour atteindre la Bêta 1 le 11 avril de la même année. D'autres Bêta sortent pour corriger les bogues. Ainsi, le 12 juin 2001, voit arriver la version 1.0 de FileZilla. Il y a eu en tout pas moins de 26 versions 1.xxx avant d'arriver à une première Bêta de la version 2. La première version 2.0.0 est sortie le 2 septembre 2002. La dernière version en date est la 3.0.4.1 sortie début décembre 2007.

II. Définition

FTP signifie File Transfer Protocol ou Protocole de Transfert de Fichiers. C'est un protocole de communication qui permet l'échange de fichiers sur internet avec un réseau TCP/IP.

Le FTP est régit selon le modèle client-serveur :

1. Un client depuis lequel on envoie les fichiers

2. Un serveur appelé plus communément *serveur FTP*, sur lequel sont envoyés des fichiers.

Un client FTP est donc un logiciel qui permet de faire la liaison entre le client et le serveur.

III. Caractéristiques

FileZilla présente les caractéristiques suivantes **:**

- Facile à utiliser
- Prise en charge FTP, FTP over SSL / TLS (FTPS) et SSH File Transfer Protocol (SFTP)
- Multi-plateforme. Fonctionne sur Windows, Linux, BSD, Mac OS X et plus
- Prend en charge IPv6
- Disponible dans de nombreuses langues
- Reprise lors d'un transfert de gros fichiers de plus de 4Go
- Capacité à reprendre les mises à jour et téléchargements interrompus (si le serveur le supporte)
- Gestionnaire de site puissant et file d'attente de transfert
- Configuration limites de vitesse de transfert
- Annuaire de comparaison
- Réseau assistant de configuration
- Édition de fichiers à distance
- Exploration des répertoires synchronisés
- Recherche de fichiers à distance
- Commandes et interface personnalisables
- Explorateur local/distant permettant d'éditer les fichiers en ligne et de changer les permissions d'accès
- Système anti-déconnexion
- Détection des temps de pause pare-feu
- Support de SOCKS4/5 et proxy HTTP1.1
- Connexions SSL sécurisées SFTP supporté et FTPS (SSL/TLS)
- File d'attente
- Gestion de la bande passante
- Import et export de paramètres de connexion
- Mise à jour / téléchargement
- Glisser & Déposer (*Drag and Drop*)

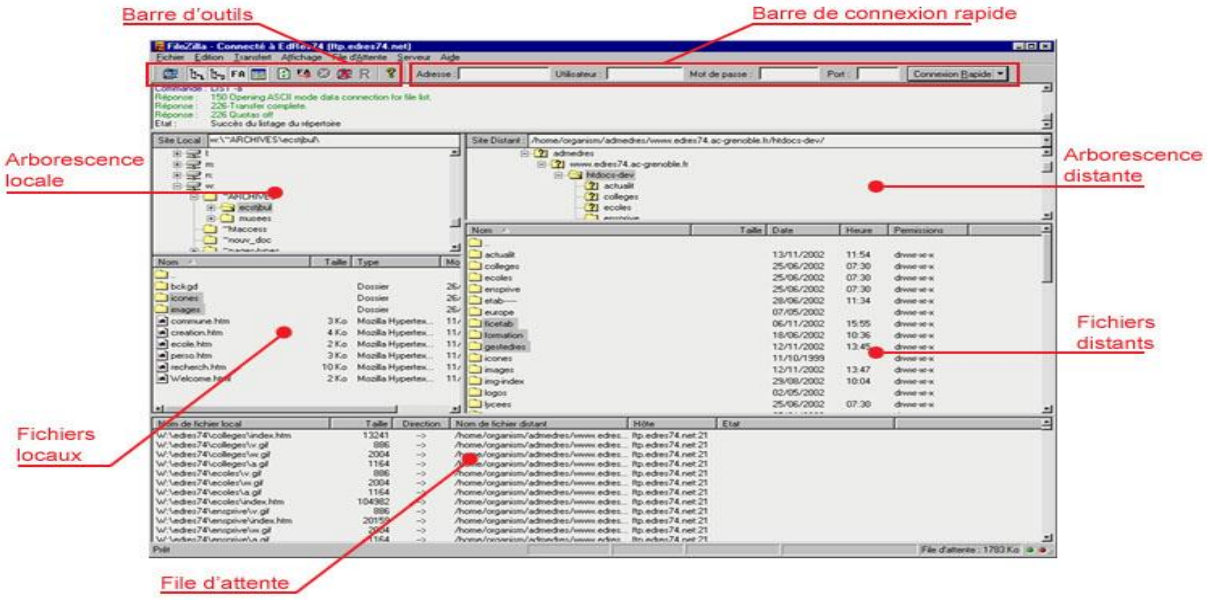
IV. FONCTIONS

Pour des raisons de sécurité, FileZilla propose un mode dans lequel il ne conserve aucune trace des mots de passe sur votre ordinateur. Ainsi, une authentification est nécessaire à chaque connexion aux serveurs, même en utilisant les favoris du gestionnaire de site. Le programme permet également de se connecter aux serveurs distants sécurisés en utilisant le protocole SSH (Secure Shell -> impose un échange de clés de chiffrement en début de connexion). FileZilla est capable de compresser les données en cours de téléchargement, ce qui améliore les vitesses de transfert. Le niveau de compression est paramétrable, ce qui lui donne une grande flexibilité. **Les fonctions principales de FileZilla sont** :

* Capacité à reprendre les mises à jour/téléchargements interrompus (si le serveur le supporte)
* Commandes personnalisables
* Gestionnaire de site avec ses dossiers
* Système anti-déconnexion
* Détection des temps de pause pare-feu
* SOCKS4/5 et proxy HTTP1.1 supportés
* Connexions SSL sécurisées SFTP supportées
* File d'attente
* Mise à jour/téléchargement
* Glisser-déposer
* Support multi-langues
* Authentification et cryptage GSS utilisant Kerberos
* Pare-feu supporté
* Réglage de la bande passante
* Répertoire de liens déjà visités

V. Description

La page écran de FileZilla est la suivante :



1-Menu/Barre d'outils/Connexion rapide :

Différentes options proposées par FileZilla. Les détails sont dans les menus Edition / Configuration

2-Journal des messages :

C'est la liste des échanges entre le serveur FTP et FileZilla. Chaque message apparaît avec une couleur significative :

Statut : Message "normal" traitant de l'échange en cours. Par exemple : Résolution de l'adresse IP pour developpez.com
Erreur : Ce sont les messages signalant une erreur survenant pendant l'échange. Par exemple : Déconnecté du serveur
Commande : Ce sont les commandes envoyées par FileZilla au serveur FTP. Par exemple : USER adrien-artero
Réponse : Ce sont les réponses transmises à FileZilla par le serveur FTP. Elles sont toutes précédées par un nombre commençant par 2, 3, 4 ou 5. 2 et 3 indiquent une réussite de la commande. 4 et 5 indiquent un échec de la commande. Un échec de la commande ne signifie pas forcément une erreur. Par exemple : 501 Option not recognized.

Le journal des messages comprend un menu contextuel accessible par un simple clic-droit dans le journal. Ainsi on peut :
* Entrer une commande à envoyer au serveur FTP
* Copier le contenu du journal (si vous voulez le coller dans une balise [CODE] de developpez.com ^^)
* Effacer le contenu du journal

3-Affichage du site en local :
C'est une opération qui permet d'explorer le contenu de votre site local. Celui-ci se présente quasiment comme le site distant.
Un menu contextuel permet d'envoyer les fichiers sur le serveur ou les placer en file d'attente :

Egalement glisser-déposer les fichiers d'un site à l'autre.

4-Affichage du site distant :

Permet d'explorer le contenu de votre site distant et possibilité de télécharger les fichiers depuis le site distant.
Un menu contextuel permet de télécharger les fichiers depuis le serveur ou les placer en file d'attente :

Le glisser-déposer fonctionne également dans ce sens.

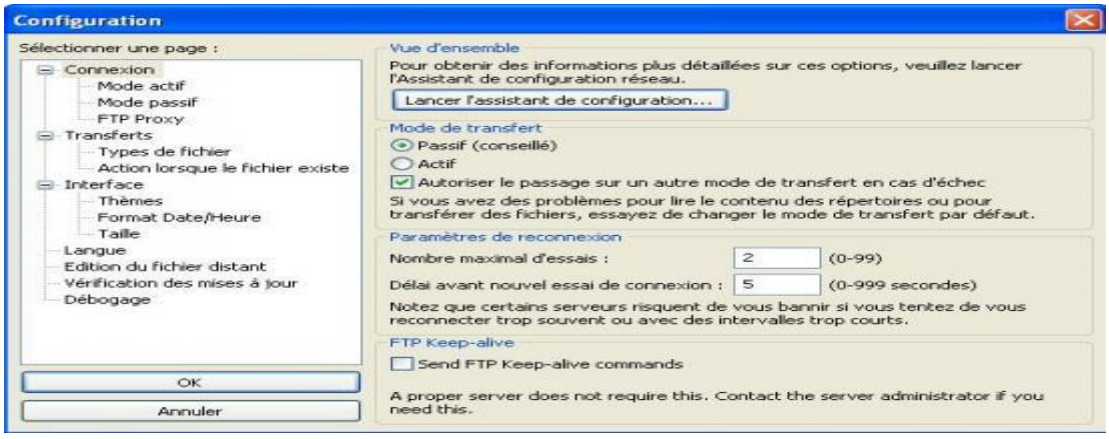
Il est à signaler que les fichiers et dossiers du site distant ont des droits qui leur sont attribués : Ces droits se composent de 10 caractères. Un premier qui indique si c'est un fichier ou dossier puis de 3 groupes de 3 caractères.

Le premier groupe indique les droits de propriété.
Le deuxième groupe indique les droits de groupe.
Le troisième groupe indique les droits publics.

R (read) indique un droit de lecture
W (write) indique un droit d'écriture
X (Xcute) indique un droit d'exécution

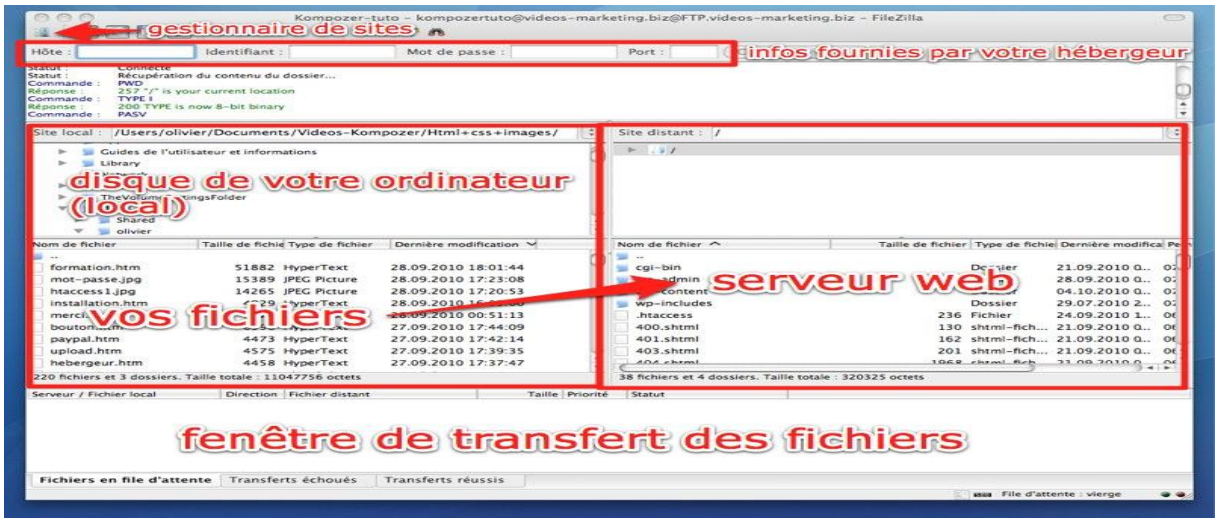
5-File d'attente :
Liste des fichiers ou dossiers présents dans la file d'attente quand l'envoi comporte plus d'une entité.

Il est possible d'optimiser FileZilla en le configurant à ses besoins.
Pour le configurer, allez dans Edition / Configuration. Affichage de cet écran :



Pour bien configurer le routeur et les pare-feux, cliquez sur "Lancer l'assistant de configuration" et laissez vous guider. Ainsi régler les modes Actifs et Passifs même **s'il est déconseillé d'activer les pare-feux.**

Il faut donc retenir les zones essentielles de travail qui sont :



VI. Paramétrage du site

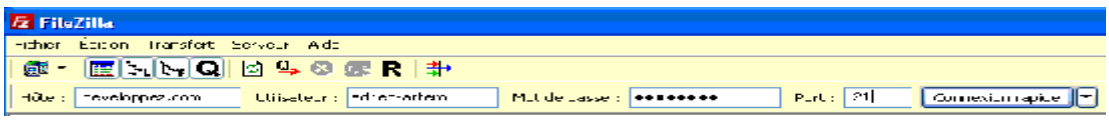
Afin de pouvoir commencer à transférer les fichiers sur un serveur, il faut préalablement paramétrer le site. Afin d'avoir un accès rapide les fois suivantes, il existe 2 options pour le faire :

- ✓ entrer ponctuellement les données de connexion au serveur
- ✓ créer votre site dans le gestionnaire.

A. Pour entrer ponctuellement les données de connexion :

1-Hôte : Entrez ici l'adresse du serveur ftp à laquelle vous souhaitez vous connecter. **N'entrez le protocole que s'il s'agit d'un serveur SFTP.**
2-Utilisateur : A entrer si besoin
3-Mot de passe : A entrer si besoin
4-Port : Par défaut, 21 pour FTP et 22 pour SFTP

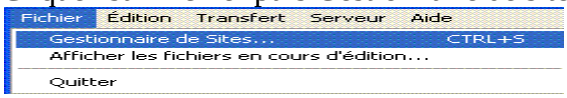
Ainsi, pour le site sur développez.com :



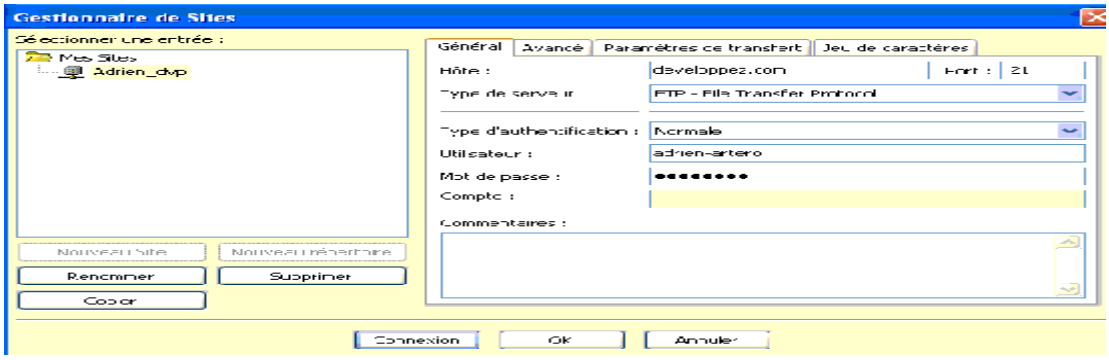
Il n'y a plus qu'à cliquer sur Connexion rapide.

VII. Gestionnaire de site

Le gestionnaire de site est très pratique. Il permet de "jongler" entre les différents sites :
Cliquez sur Fichier puis Gestionnaire de site



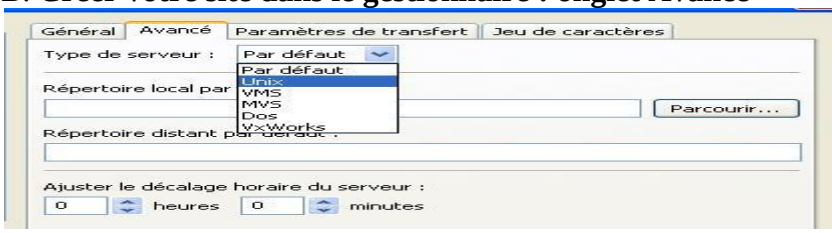
Cliquez sur Nouveau site et entrez les mêmes informations que pour une connexion ponctuelle :



Indiquer le **type de serveur** à utiliser :

FTP (par défaut)
SFTP (SSH): A utiliser lorsque la connexion au SFTP est cryptée.
FTPS (cryptage implicite): A utiliser lors de la connexion à des serveurs sécurisés SSL (Secure Sockets Layer) et que l'obtention du canal sécurisé est établi **avant** la connexion.
FTPES (cryptage explicite): A utiliser lors de la connexion à des serveurs sécurisés SSL (Secure Sockets Layer) et que l'obtention du canal sécurisé est établi **au moment de** la connexion.
Egalement définir **le type d'authentification** : le mode *anonyme* ne demande pas d'entrer d'identifiants, *Mot de passe* juste un MDP, etc.

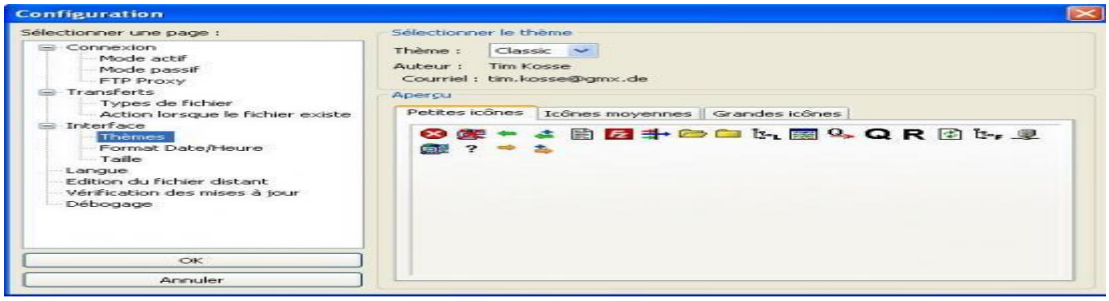
B. **Créer votre site dans le gestionnaire : onglet Avancé**



Définir un type de serveur UNIX, VSM, MVS, Dos, etc.
Il est également possible de déterminer un répertoire local et un distant par défaut:
Cela signifie qu'au moment de la connexion au site, FileZilla prendra ces deux répertoires automatiquement.

Avec les derniers onglets, il est possible de définir le nombre de connexions simultanées possibles ou le type d'encodage des caractères pour les noms de fichiers.

VIII. Configuration



Il suffit d'ouvrir le gestionnaire de sites et de mettre vos informations données par le serveur FTP :

- l'adresse du serveur
- le port (par défaut le port 21)
- le login
- le mot de passe

Ne pas afficher les dossiers cachés

Un problème qui peut rapidement vous gâcher la vie, c'est l'affichage des dossiers et fichiers cachés par défaut. Pour pallier cela, il va falloir configurer un « Filtre » :

Version francisée : Cliquer sur l'icône *Gestion des filtres* → *Éditer les règles de filtrages…* → *Nouveau*. Choisir un nom (« Cachés » c'est très bien…). Cliquer sur le bouton "En ajouter plus". Dans le menu déroulant, sélectionner "Nom du fichier" puis « commence par ». Dans le champ le plus à droite mettre un « . ». Vérifier que les deux cases «Fichiers» et «Répertoires», à la section « Le filtre s'applique à :» sont cochées puis Valider. De retour dans la section "Jeu de filtres", cocher la case placée devant le nom du nouveau filtre « Cachés » pour les filtres locaux et/ou les filtres distants.

Version originale : Cliquer sur l'icône *Filter the directory listings* → *Edit Filters…* → *New*. Choisir un nom (« hidden » c'est très bien…). Mettre "Filename" et « begins with » et mettre « . ». Puis « Filter applies to Directories ». Valider.

La fenêtre est scindée en deux : à gauche pour votre disque-dur, à droite pour le serveur auquel vous vous connectez. Cochez donc celle de gauche. Et enfin, Validez

IX. **Méthodes de sécurité**

FileZilla et la sécurité des sites enregistrés

FileZilla ne chiffre pas son dossier de configuration (*~/.filezilla*) mais on n'y fait pas toujours attention car dans le logiciel, les mots de passe n'apparaissent pas. Cependant la simple commande suivante affichera tout : **cat ~/.filezilla/sitemanager.xml**

Apparemment il n'existe pas de fonctions de chiffrement dans filezilla. Il suffirait d'ajouter un chiffrement dans le code source mais encore faudrait-il avoir le temps d'analyser le code source.

Il existe deux méthodes pour sécuriser le répertoire de configuration de FileZilla contre les utilisateurs indiscrets de votre ordinateur et contre les logiciels espions. La première est simple, la seconde est plus sûr et pratique.

1. **Méthode cryptkeeper à 2 niveaux de chiffrement**

Utiliser **cryptkeeper** pour chiffrer le répertoire de configuration de FileZillaet **zenity** afin d'afficher une alerte bloquante :

installer les paquets apt://cryptkeeper apt://zenity.

ajoutez un répertoire à chiffrer dans cryptkeeper, (le chemin du répertoire déchiffré est ~/.filezilla.

Si cryptkeeper ne se lance pas au démarrage d'Ubuntu, il suffit de l'ajouter dans la liste des applications au démarrage (sa commande est simplement cryptkeeper). Une fois lancé, un trousseau de clés apparait parmi les icones de minimisation de la barre Ubuntu. Un simple clic gauche sur cette icone affiche la liste des répertoires chiffrés/déchiffrés et de quoi créer/importer des dossiers chiffrés.

Ensuite le petit souci, c'est évidemment de démarrer filezilla avant d'avoir déchiffré le répertoire de configuration. Résultat : filezilla va créer un nouveau répertoire *~/.filezilla* et il faudra le supprimer à la main avant de déverrouiller notre répertoire chiffré (sinon cryptkeeper affichera un message disant que le répertoire cible existe déjà) et de relancer filezilla. C'est ici que zenity sera utile.

2. **Méthode truecrypt**

Une seconde méthode pour sécuriser les sites enregistrés avec FileZilla c'est utiliser un fichier chiffré avec **truecrypt**. D'après wiki, TrueCrypt est gratuit et open-source mais non-libre. C'est donc une histoire de licence qui m'échappe

Cette méthode a 2 avantages majeurs par rapport à cryptkeeper :

- elle nécessite un seul clic pour ouvrir Filezilla avec son fichier chiffré

- elle permet d'avoir un répertoire de configuration ~/*.filezilla* factice.

Installation et création du fichier chiffré

alltray permet de réduire une application dans la barre de minimisation et **truecrypt** permet de chiffrer notre répertoire de configuration :

1. installez alltray ainsi que **truecrypt** disponible sur le site officielhttp://www.truecrypt.org/downloads.
2. créer notre fichier chiffré qui contiendra ce qu'il y a normalement dans ~/.filezilla/ lancez **TrueCrypt** en mode graphique via le menu de Gnome *Accessoires* > *TrueCrypt*.
3. Créez un nouveau volume chiffré (ici pas besoin d'une partition chiffrée). Truecrypt permet 2 niveaux de chiffrement : un seul niveau de chiffrement (pas de *volume hidden*) utiliser aussi une taille réduite (1Mo est largement suffisant) et le chiffrement *Serpent-Twofish-AES* qui est plus lent que AES simple (mais sans impact visible sur un si petit volume) mais plus sûr. Par la suite, appeller le fichier chiffré FZ_CHIFFRE (un autre nom, nécessite de modifier les chemins en conséquence) et il contiendra tous les fichiers contenus dans ~/*.filezilla*.

Le fichier chiffré créé, montez-le (par défaut, en mode graphique, il sera monté typiquement dans /media/truecrypt1), et copiez-y vos fichier contenus dans ~/*.filezilla*. Pour s'assurez que vous ayez bien mis les fichiers au bon endroit, vous devez avoir la hiérarchie /media/truecrypt1/sitemanager.xml et PAS /media/truecrypt1/.filezilla/sitemanager.xml

Script personnalisé de lancement de FileZilla

Ensuite, créez un script de lancement (donnez-lui le nom de votre choix, moi je l'ai nommé *filezilla_p*) dans votre répertoire personnel (ou ailleurs si ça vous chante mais adaptez les chemins dans ce cas), ce script remplacera la commande originel *filezilla*. Collez ceci dans votre script :

```
echo "Montage du répertoire..."
truecrypt --mount /home/USER/FZ_CHIFFRE /home/USER/.filezilla
echo "Exécution de FileZilla..."
filezilla;
echo "Démontage du répertoire..."
truecrypt --dismount /home/USER/.filezilla
exit 0
```

Explications :

- les affichages **echo** ne sont pas indispensables mais peuvent être utile en cas de blocage quelconque pour savoir où le blocage survient.
- ensuite pour la ligne truecrypt –mount /home/USER/FZ_CHIFFRE /home/USER/.filezilla : remplacez**USER** par votre nom d'utilisateur ; remplacez **FZ_CHIFFRE** par le nom donné au fichier chiffré. Cette ligne permet de déchiffrer et monter FZ_CHIFFRE comme étant ~/.filezilla/. Truecrypt demandera le

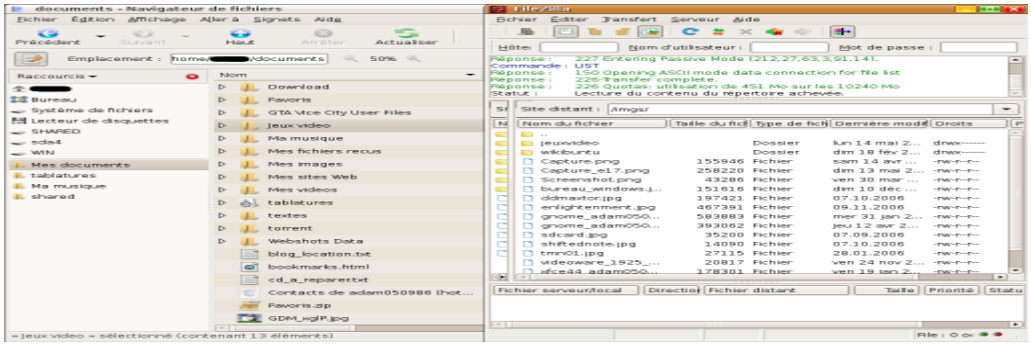
mot de passe administrateur si besoin (cf la note d'introduction à la méthode truecrypt).

- enfin pour la ligne truecrypt –dismount /home/USER/.filezilla : remplacez **USER** par votre nom d'utilisateur ; Cette ligne permet de démonter et rechiffrer le répertoire ~/.filezilla/ en FZ_CHIFFRE. Elle ne sera exécutée qu'une fois FileZilla fermé évidemment.

Il est possible d'ajouter le mot de passe de votre fichier chiffré dans la ligne de commande. Ceci présente l'avantage de ne pas avoir à l'entrer à chaque fois mais affaiblit la sécurité.

X. Interface plus conviviale

En utilisant Nautilus ou Thunar les raccourcis personnels ne sont pas pris en compte, ce qui peut être génant et handicapant pour travailler efficacement. FileZilla supporte le **"drag'n'drop"** (glisser/déposer) pour utiliser un bureau spécifique :



La solution est de modifier le raccourci dans la barre de raccourcis (et éventuellement le menu de Gnome Applications > Internet > Filezilla) comme suit.

On crée un petit script que l'on appelle *.filezilla_p* et que l'on mettra dans notre répertoire personnel (sinon, adaptez les chemins dans la suite). Ensuite il suffit de remplacer la commande filezilla dans le raccourci par /home/USER/.filezilla_p (**USER** est à remplacer par votre nom d'utilisateur).
Contenu de **/home/USER/.filezilla_p** :
zenity --title 'FileZilla' --info --text='Le répertoire est-il déverrouillé ?' ; filezilla
Quand on lance filezilla avec notre raccourci, une boite de dialogue bloquante s'affiche (avant le lancement même de filezilla) et ainsi on peut déchiffrer notre répertoire *~/.filezilla* avec cryptkeeper si c'est pas déjà fait. Ensuite on clique sur Valider et filezilla se lance.
Après avoir fermé filezilla, il faut rechiffrer le répertoire *~/.filezilla* en le "démontant" avec cryptkeeper.

CONCLUSION

La sécurité est importante dans tous les systèmes informatiques. FileZilla en dispose et est en constante évolution avec les nouvelles versions.

Il est à signaler qu'un attaquant pourrait envoyer des paquets FIN usurpés au client. Même si GnuTLS détecte avec GNUTLS_E_UNEXPECTED_PACKET_LENGTH, FileZilla n'enregistre pas un échec de transfert dans tous les cas.

Malheureusement, tous les serveurs exécutent un ordre SSL / TLS arrêt. Étant donné que ce ne peut être distingué d'une attaque, FileZilla ne sera pas en mesure de télécharger des listes ou des fichiers à partir de ces serveurs. Les versions qui sont affectées sont celles antérieures à 3.1.0.1. Cette vulnérabilité a été corrigée dans le 3.1.0.1.

Webographie :

http://www.ordi-netfr.com/tutorialafilezilla.php

http://www.framasoft.net/IMG/pdf/tutorial_installation_configuration_serveur_ftp_filezilla_server_version_fr.pdf

http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail

http://filezilla-project.org/

http://www.framasoft.net/article1941.html

http://www.authorstream.com/Presentation/imtoolsguide-761017-filezilla-review/

http://filezilla-project.org/download.php