PRÉCONISATIONS SÉCURITÉ	Produit : Arlequin Comm Topkapi Description : préconisations de sécurité de mise en œuvre de filezilla server

Table des matières

1 INTRODUCTION

Les produits comme le P400XI et le Smartlog peuvent déposer leur données sous formes de fichier ftpmodbus dans un serveur ftp. Ce serveur ftp doit être accessible depuis internet pour les produits utilisant le réseau TCP/IP via GPRS.

L'accès à ce serveur ne peut pas être restreint à une liste d'adresses IP par un routeur/firewall intermédiaire entre le serveur ftp et internet car les produits ont une adresse IP privée et dynamique affectée par l'opérateur du réseau GPRS.

Les produits P400XI et Smartlog n'intègrent pas encore la fonctionnalité d'utiliser le protocole FTPS qui permettrait de crypter la communication et d'authentifier les accès. Cependant un ensemble de règles applicables au serveur ftp et à son environnement immédiat permet de renforcer sa sécurité.

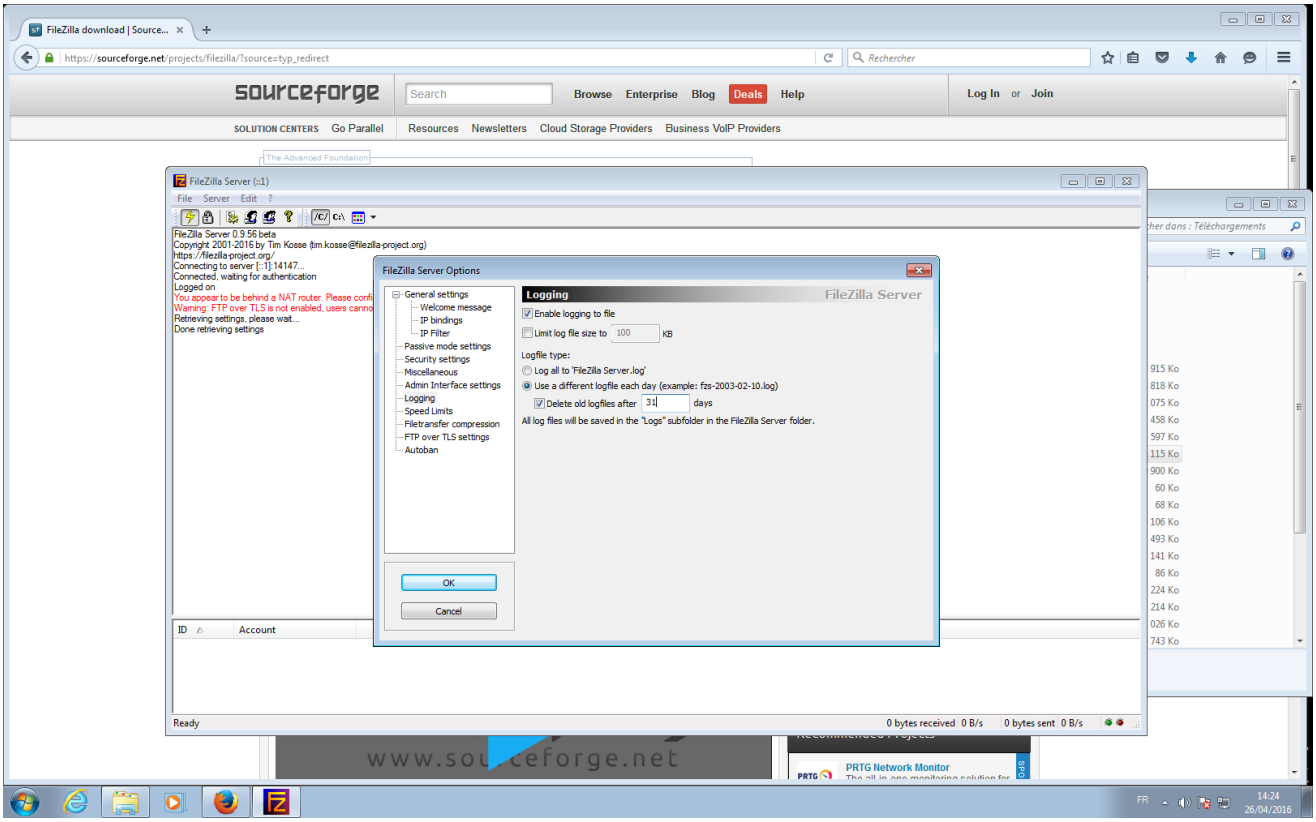
La solution proposée pour Arlequin Comm et Topkapi est FileZilla Server

ⓘ l'ensemble de ces règles ne constitue pas une protection absolue mais une protection contre les attaques triviales.

2 RÈGLES OBLIGATOIRES

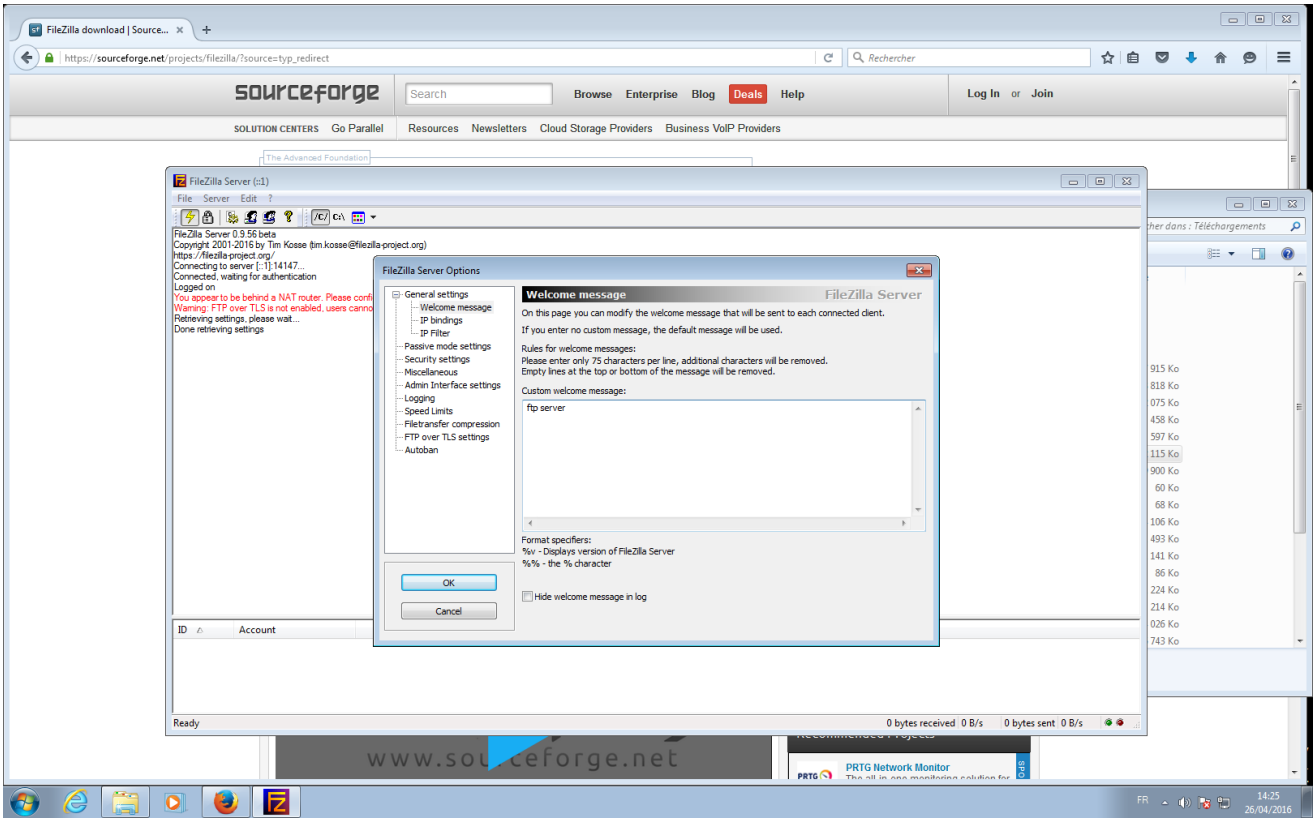
2.1 ACTIVER LES LOGS

Pour pouvoir trouver l'origine d'un problème et pouvoir identifier des tentatives d'accès, il faut activer les logs du logiciel. La solution choisie est d'avoir un fichier de log par jour et d'effectuer une rotation sur 31 jours.



2.2 REMPLACER LA BANNIÈRE DE LOGIN

Pour éviter que les personnes malveillantes identifient facilement le logiciel de serveur ftp et sa version afin de trouver des informations sur ses éventuelles vulnérabilités, il faut modifier la bannière par défaut par un message neutre ne donnant aucune informations :



2.3 UTILISER DES MOTS DE PASSES NON TRIVIAL POUR LES CLIENTS FTP

Pour les clients P400XI et Smartlog se connectant au serveur ftp , il faut définir un mot de passe

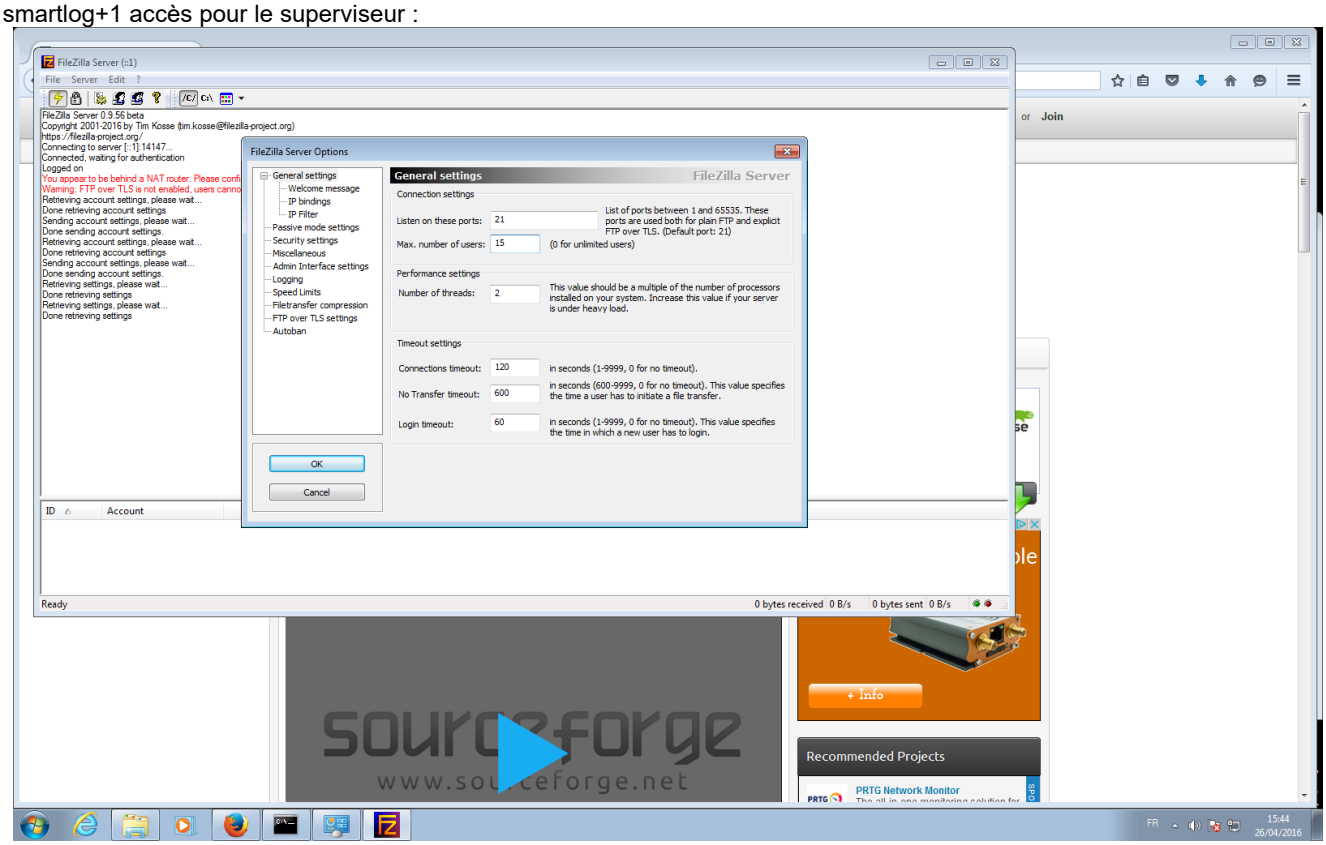
- ➔ qui soit spécifique à l'installation
- ➔ dont la longueur soit supérieure à 10
- ➔ qui est composée de chiffres et de lettres

2.4 CHANGER LES MOTS DE PASSE

A chaque disparition d'un produit ou d'une suspicion de l'ouverture d'un produit, il faut changer les mots de passe de tous les clients ftp,

2.5 LIMITER LE NOMBRE D'ACCÈS CONCURRENTS

Il faut limiter le nombre d'accès concurrents au nombre de produits composant l'installation. Ici par exemple, 14 smartlog+1 accès pour le superviseur :



2.6 SÉCURISER L'ACCÈS À LA CONSOLE D'ADMINISTRATION DU SERVEUR FTP

Cet accès doit être sécurisé en

- ➔ activant la protection avec un mot de passe non trivial
- ➔ n'autorisant l'accès que depuis le PC hébergeant le serveur ftp

2.7 RESTREINDRE L'UTILISATION DU PC

L'utilisation du PC hébergeant le serveur ftp et la supervision doit être restreint qu'à ces deux fonctionnalités. La consultation de site internet par exemple doit être proscrit.

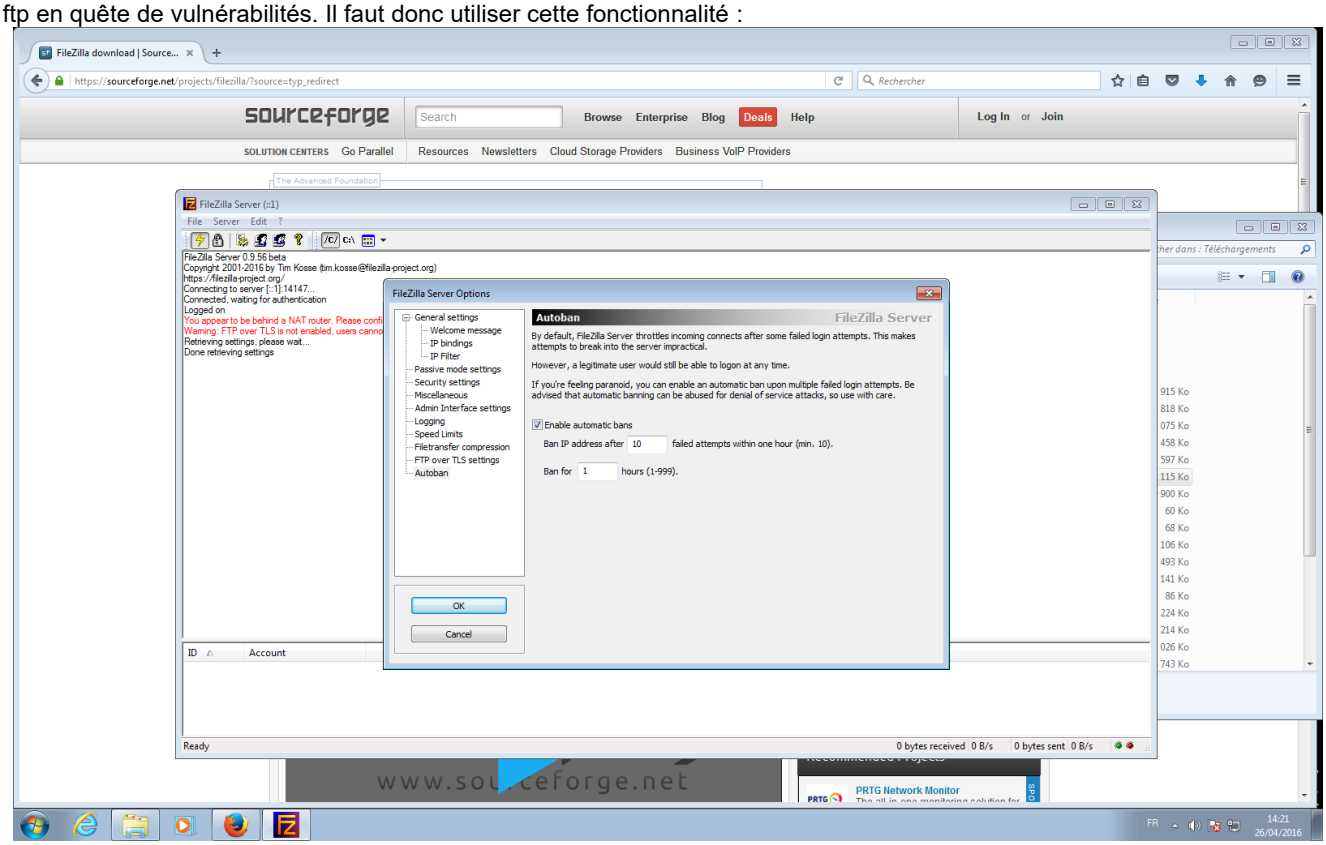
2.8 MAINTENANCE

L'installation doit être maintenue :

- ➔ le logiciel filezilla server doit être mis à jour dès une parution d'une faille critique
- ➔ le système d'exploitation windows doit être mise à jour automatiquement
- ➔ les logs du serveur filezilla doivent être examinés avec une périodicité qui soit inférieure à la rotation des logs. Un événement qui n'est pas de l'ordre du fonctionnement nominal doit provoquer un examen immédiat des logs.

2.9 METTRE AU PURGATOIRE LES ADRESSES IP DES CLIENTS FTP QUI SCANNENT

Le logiciel filezilla server offre la possibilité de bannir pendant un temps déterminé un client ftp qui a généré des erreurs d'ouverture de la connexion pendant un laps de temps court. Ce qui caractérise les clients ftp qui scannent des serveurs ftp en quête de vulnérabilités. Il faut donc utiliser cette fonctionnalité :

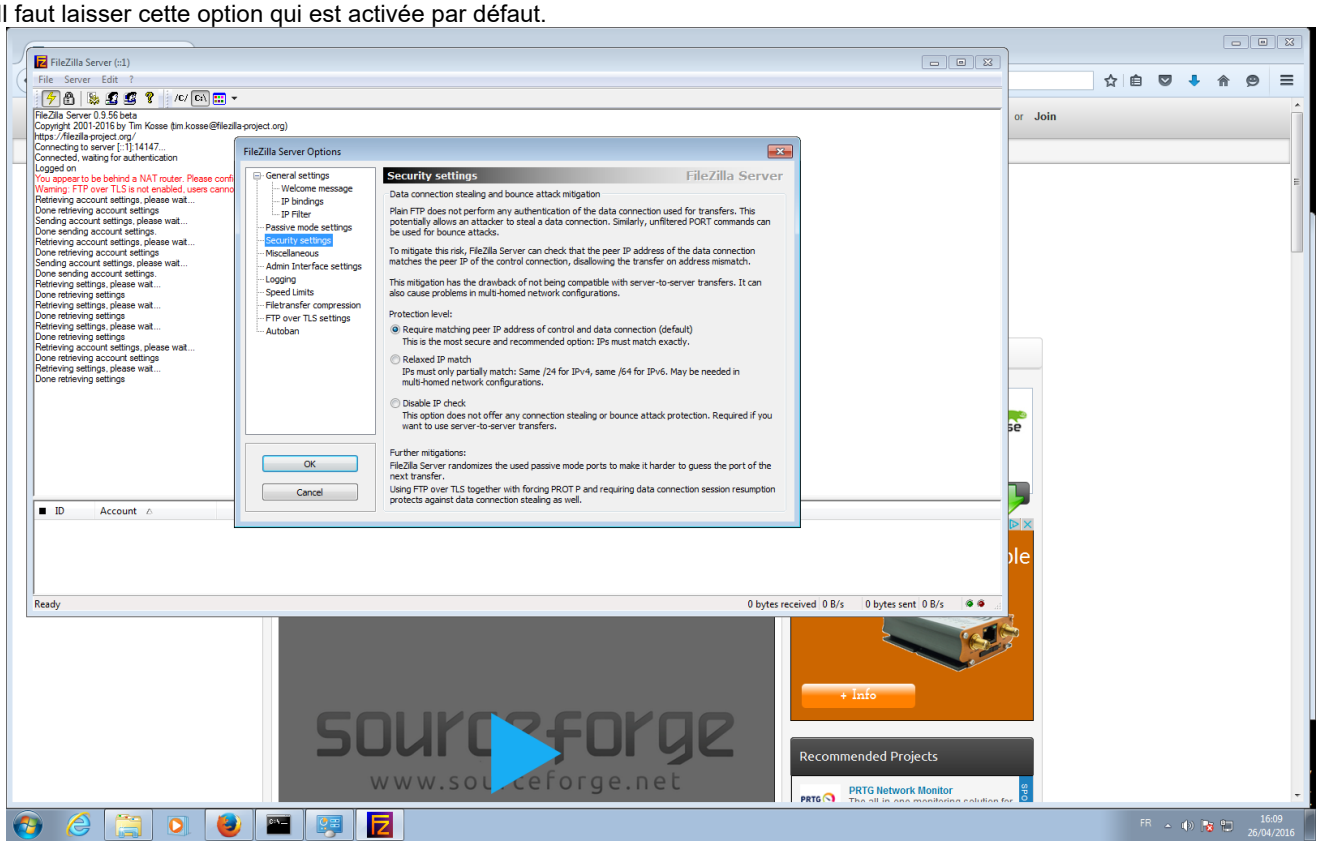


2.10RÉPERTOIRE DE STOCKAGE DES FICHIERS DÉPOSÉS

Le répertoire utilisé pour les dépôts des fichiers ftpmodbus et des sémaphores doit être dédié à cet usage

2.11 VÉRIFICATION DE L'UTILISATION DE LA MÊME ADRESSE IP POUR LE CANAL DE DONNÉES ET DE COMMANDE

Il faut laisser cette option qui est activée par défaut.



3 RÈGLES FACULTATIVES

Ces règles permettent de renforcer la sécurité de l'installation.

3.1 UTILISER UN ROUTEUR/FIREWALL

L'utilisation d'un routeur/firewall qui soit distinct de celui du PC Windows et de l'éventuel box internet permet de ne pas être tributaires de leur fonctionnalité pour la sécurité. Il faut cependant que ce routeur/firewall puisse effectuer une gestion de la connexion entrante en ftp passif en modifiant les adresses ip dans les commandes et réponses ftp,

3.2 RESTREINDRE LA PLAGE D'ADRESSES IP DES CLIENTS FTP POUVANT SE CONNECTER AU SERVEUR

Si les clients ftp sur gprs ont les mêmes fournisseur de réseau GPRS, il faut demander à ce fournisseur la plage d'adresses IP qu'il attribue aux postes GPRS et de restreindre l'accès ftp à cette plage.