

Fiche   
pfsense 2.4.1 – Document de base

Dans cette fiche …

[Pfsense 2.4.1 – squid et squidguard 1](#_Toc496770943)

[Installation de pfsense 2](#_Toc496770944)

[Ouverture de session 3](#_Toc496770945)

[Installation des paquetage squid et squidguard 4](#_Toc496770946)

[Configuration de base de squid proxy server 5](#_Toc496770947)

[Mise en place des filtres à l’aide des listes noires (*blacklists*) 6](#_Toc496770948)

[Ajout de règles avec *easyrule* 8](#_Toc496770949)

Département d’informatique  
Collège de Maisonneuve  
3800 est, rue Sherbrooke,  
Montréal (Québec) H1X 2A2  
514.251-7131 poste 4800

Document proposé par Louis Savard, M. Ing. TI  
Dernière révision : Octobre 2017

## Introduction

|  |  |
| --- | --- |
|  | pfsense est une distribution logicielle permettant de réaliser une passerelle réseau à partir d'un serveur x86.  Il date de 2004 à partir d’un fork de m0n0wall par Chris Buechler et Scott Ullrich. |

Très fréquemment rencontré dans les PME et les petites structures, pfsense offre une solution complète de routage, filtrage, VPN et partage de connexion. Il est basé sur pf, et intègre un grand nombre de composants tiers : serveur DHCP/DNS, serveur de temps, proxy web, monitoring... La configuration se fait entièrement via une interface web.

pfsense est disponible sous licence BSD. Un support officiel est proposé par la société   
*BSD Perimeter*.

pfsense peut être installé sur un simple ordinateur personnel comme sur un serveur.   
Basé sur PF (*packet filter*), comme *iptables* sur GNU/Linux, il est réputé pour sa fiabilité.

Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q).

## Présentation

pfsense ne fait pas seulement un pare-feu, il offre également toute une panoplie de services réseaux.

* **Pare-feu**  
  Le pare-feu est celui de *FreeBSD*, à savoir PacketFilter.
* **Table d'état**  
  La table d'état (*State table*) contient les informations sur les connexions réseaux.   
  Cela permet d'avoir un aperçu des connexions et surtout de créer des règles comme par exemple sur le nombre de connexion maximum pour un hôte.
* **Translation d'adresses réseaux** (NAT)  
  Permet de joindre un réseau privé vers l'extérieur.
* **VPN**  
  Permet la création de VPN IPsec, OpenVPN ou PPTP.
* **Serveur DHCP**.
* **Serveur DNS et DNS dynamiques**.
* **Portail Captif**.
* **Redondance et équilibrage de charge**.
* **Graphes pour la charge système et réseaux**
* …

Des logiciels complémentaires s'installent grâce à un système d’ajout. Ces derniers sont configurés pour s'intégrer à l'interface web.

Comme exemple d’ajout on trouve *nut* (pour le monitoring des onduleurs) et FreeRADIUS.

Le nombre d’ajout augmente régulièrement.

Il est aussi possible d'installer d'autres paquets que ceux proposés par l'interface, en ligne de commande.

La version 2.4 finale de *pfsense* est arrivée fin septembre 2017.

## Installation du service

pfsense est un pare-feu à état (*statefull firewall*) basé sur FreeBSD, gratuit et à code ouvert comme pare-feu ou aiguilleur (*router*). En plus de sa puissance et flexibilité, la distribution inclut beaucoup de fonctionnalités.

**Mise en place de la machine virtuelle**

Lors de la création de la machine virtuelle…

Inscrire *pfsense* comme nom de la machine virtuelle et Virtalbox fera le reste.

Accepter les paramètres par défaut.

Avant de démarrer la machine virtuelle une première fois...

Modifier les paramètres suivants :

* Interface 1 (carte 1)   
  Mode d'accès réseau = Accès par pont (cela sera notre interface du réseau interne (LAN)).
* Interface 2 (carte 2)   
  Mode d'accès réseau = Accès par point (cela sera notre interface du réseau externe (WAN)).

Note:

Ne pas oublier d'insérer l'image iso dans le lecteur CD/DVD.

## Mise en place de *pfsense*

Démarrer la machine virtuelle.

Note:

Les touches de déplacement et la touche TAB permettent de se déplacer entre les éléments)

* Au démarrage, laisse démarrer le service

À l'aide de l'interface texte

* Accepter les termes de copyright et de license ;
* Sélectionner l'installation (*Install pfsense*) ;
* Sélectionner le clavier (*keymap selection*) ;
* Sélectionner le partitionnement par défaut (*Auto UFS* – *Guided Disk Setup*) ;
* Sélectionner **No** pour une configuration manuelle ;
* Redémarrer.

Avant le redémarrage

Retirer de la machine virtuelle l'image iso du lecteur cd/dvd.

Au redémarrage

* Entrer n (pour non) à la demande de la configuration VLAN
* Sélectionner la première interface *em0* comme interface interne (Réseau interne (LAN))  
  Nommer l'interface em0
* Sélectionner le second interface *em1* comme interface externe (Réseau externe (WAN))  
  Laisser le nom de l'interface vide  
  *pfsense* confirme vos deux interfaces
* Entrer *y* (pour oui) pour confirmer

## Utilisation de pfsense

À l'aide d'une seconde machine virtuelle

* Modifier les paramètres de la machine virtuelle:  
  Mode d'accès réseau = Accès par point (cela sera notre interface du réseau local (LAN)).

Démarrer un fureteur et entrer l’URL suivante  
<http://192.168.1.1> (adresse de l’interface interne par défaut)

Pour se connecter à l'interface graphique

Nom d'usager: *admin*

Mot de passe: *pfsense*

**Personnalisation de *pfsense***

Sélectionner *System – General setup*

Modifier les paramètres si désiré

**Principales configurations**Outils offert sous le menu *firewall*

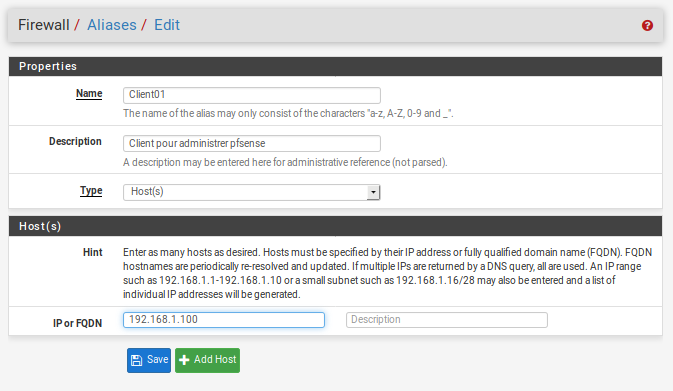
**Création d’un alias**

Dans *pfsense* un alias est utilisé pour associer ou regrouper des éléments sous un nom commun. Ce nom est utilisable dans certaines zones, lors de la création de règles par exemple. Un alias (ou “groupe”) peut être constitués de ports, d'adresses IP ou de réseaux.

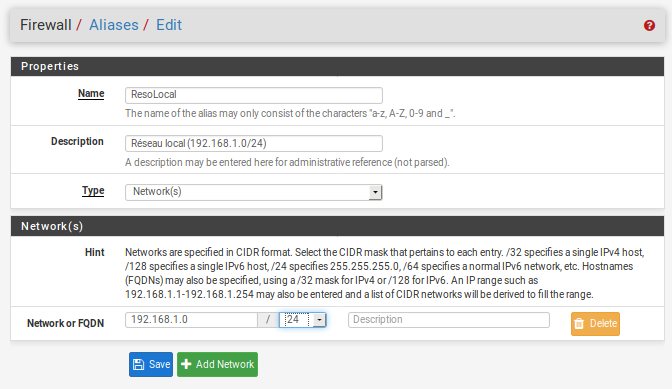
Ces éléments, de différentes natures, ne peuvent pas être mélangés au sein d'un même alias.

**Création d’un alias pour un hôte**

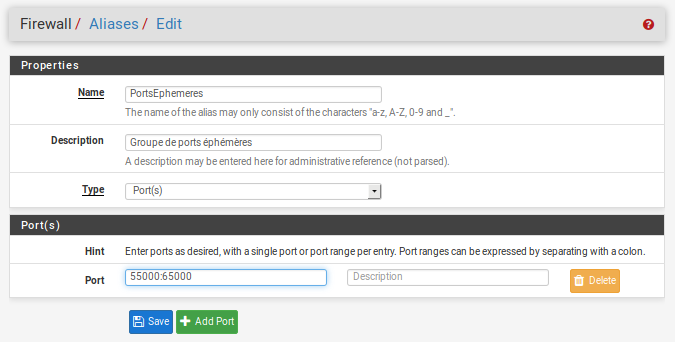
Hôte ayant le nom de computer1

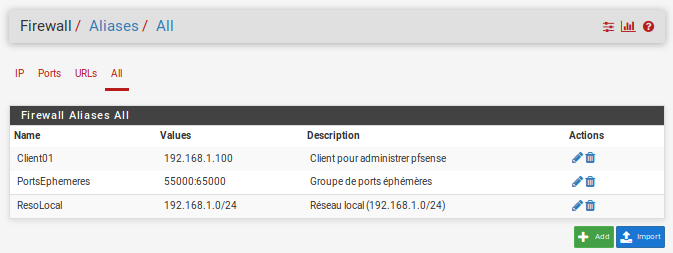


**Création d’un alias de réseau ou de groupe de réseau**



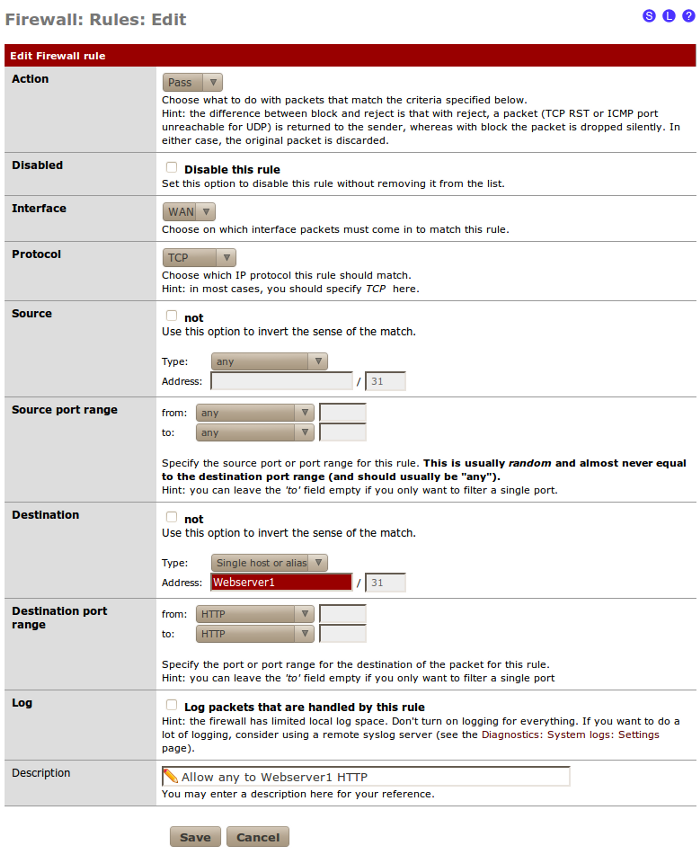
**Création d’un alias de port ou de groupe de ports**





*Résultats de la création d’alias*

**Création d’une règle de pare feu**



**Ordre des règles du pare-feu**

Les règles avec pfsense sont toujours évaluées de haut en bas.

La première règle qui correspond est exécutée et le reste des règles sont ignorées.

De manière générale, il est de bon usage de placer les règles les plus restrictives en premier et les règles les plus génériques en dernier.

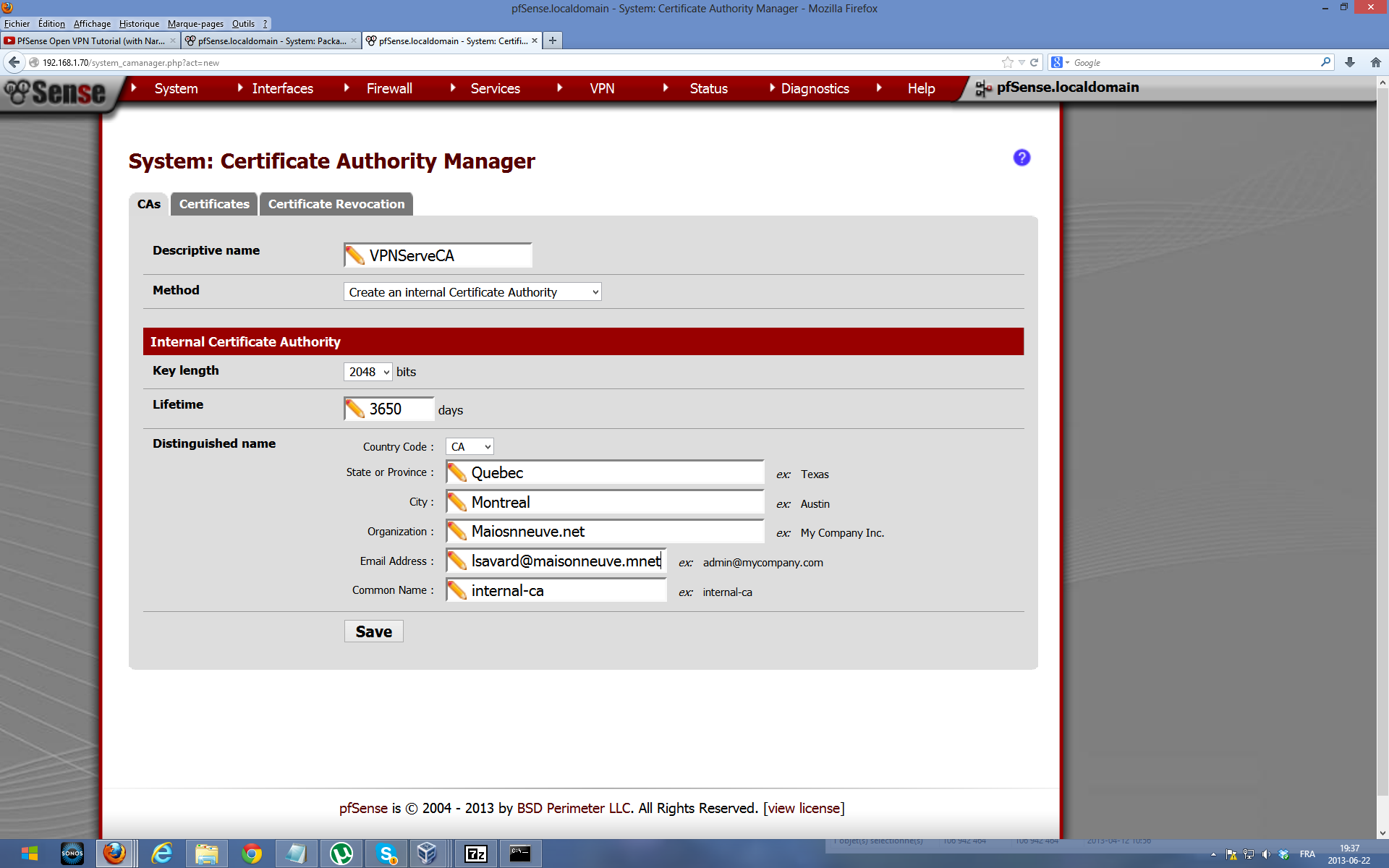
Pour réorganiser l’ordre des règles, sélectionner une règle et cliquez sur le bouton de déplacement appropriés.

**Installation du client VPN**

System – Packages  
Available packages  
OpenVPN Client Export Utility

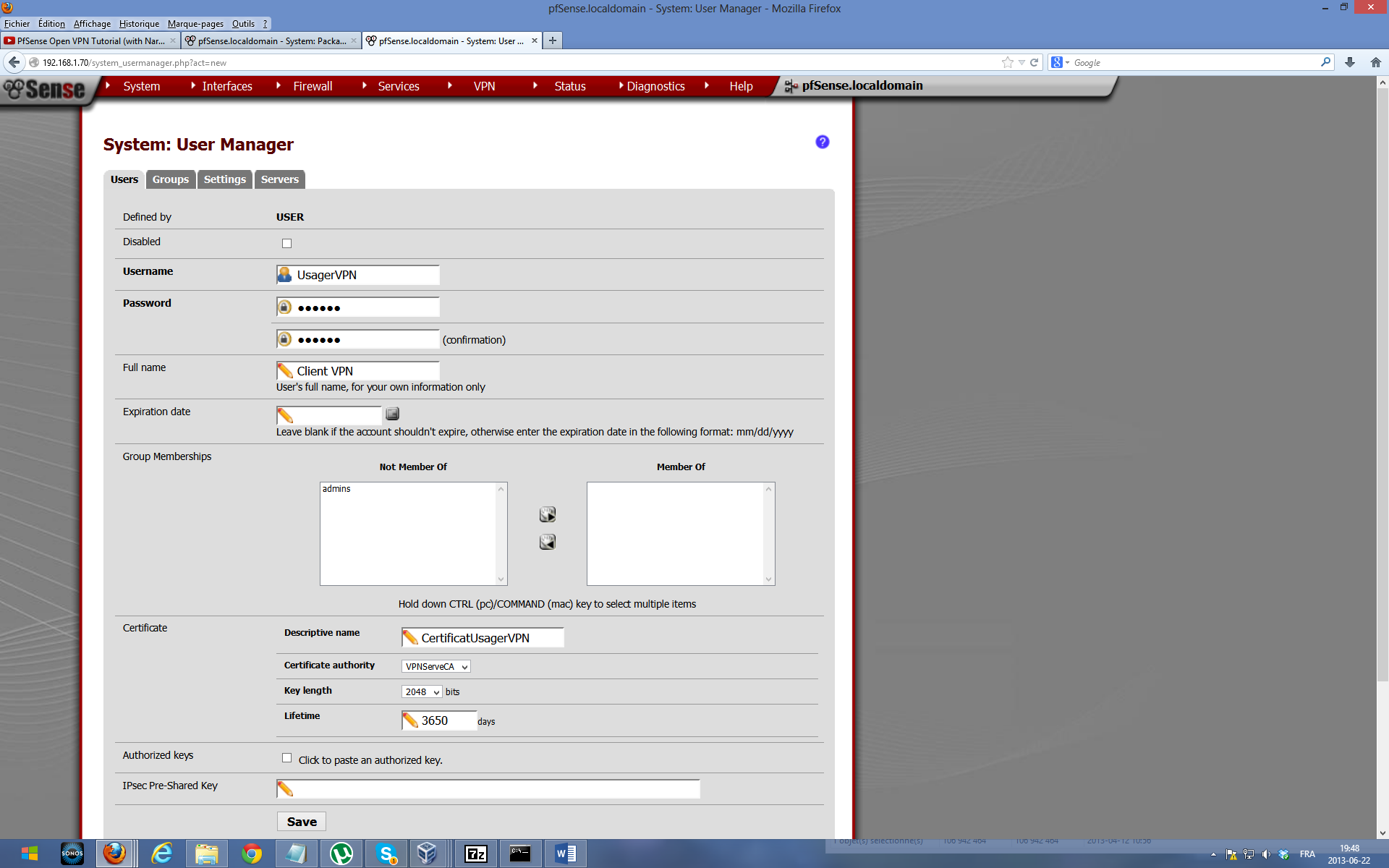
**Installation de l’autorité de certification**

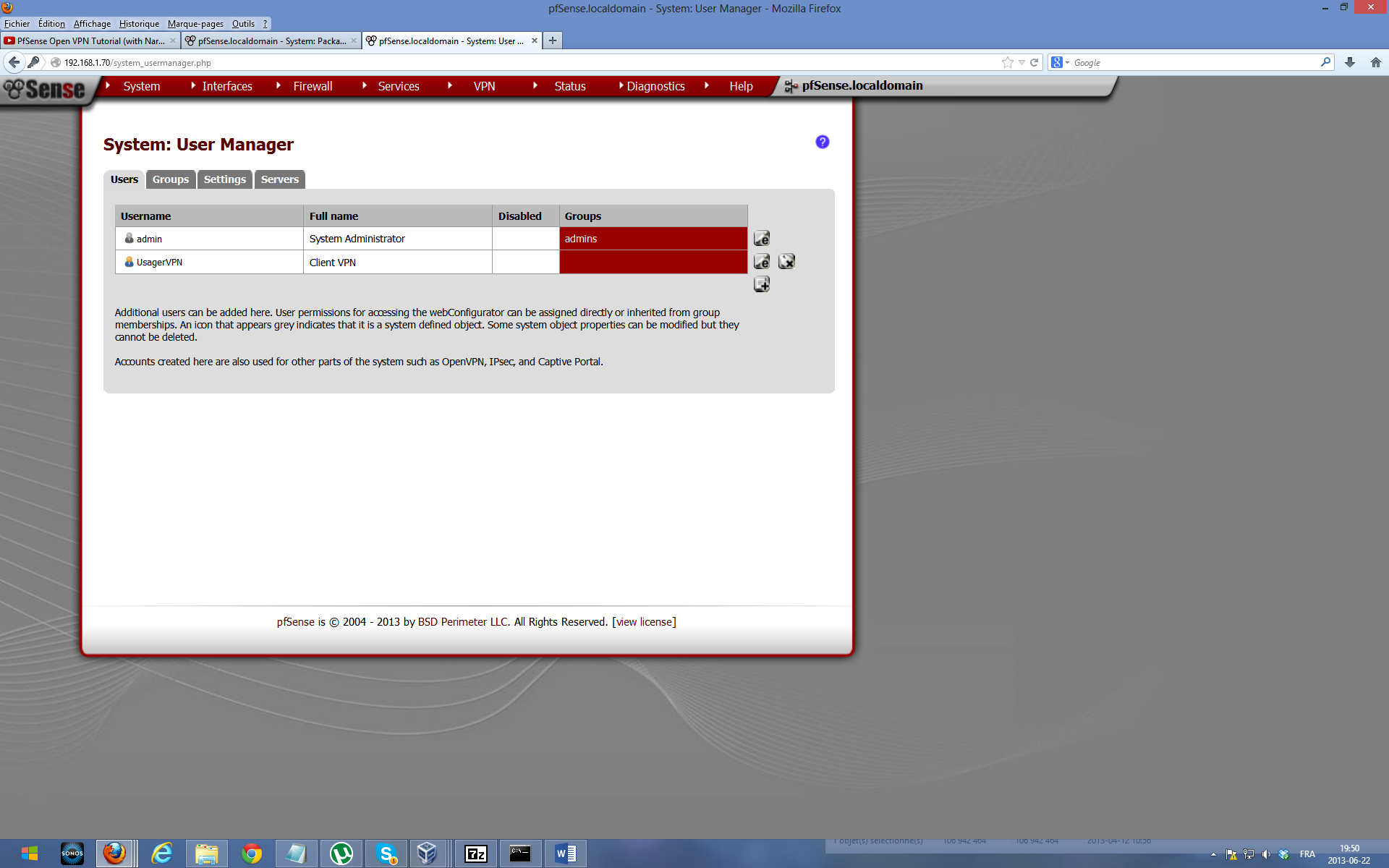
System – CertManager



**Création d’un usager**

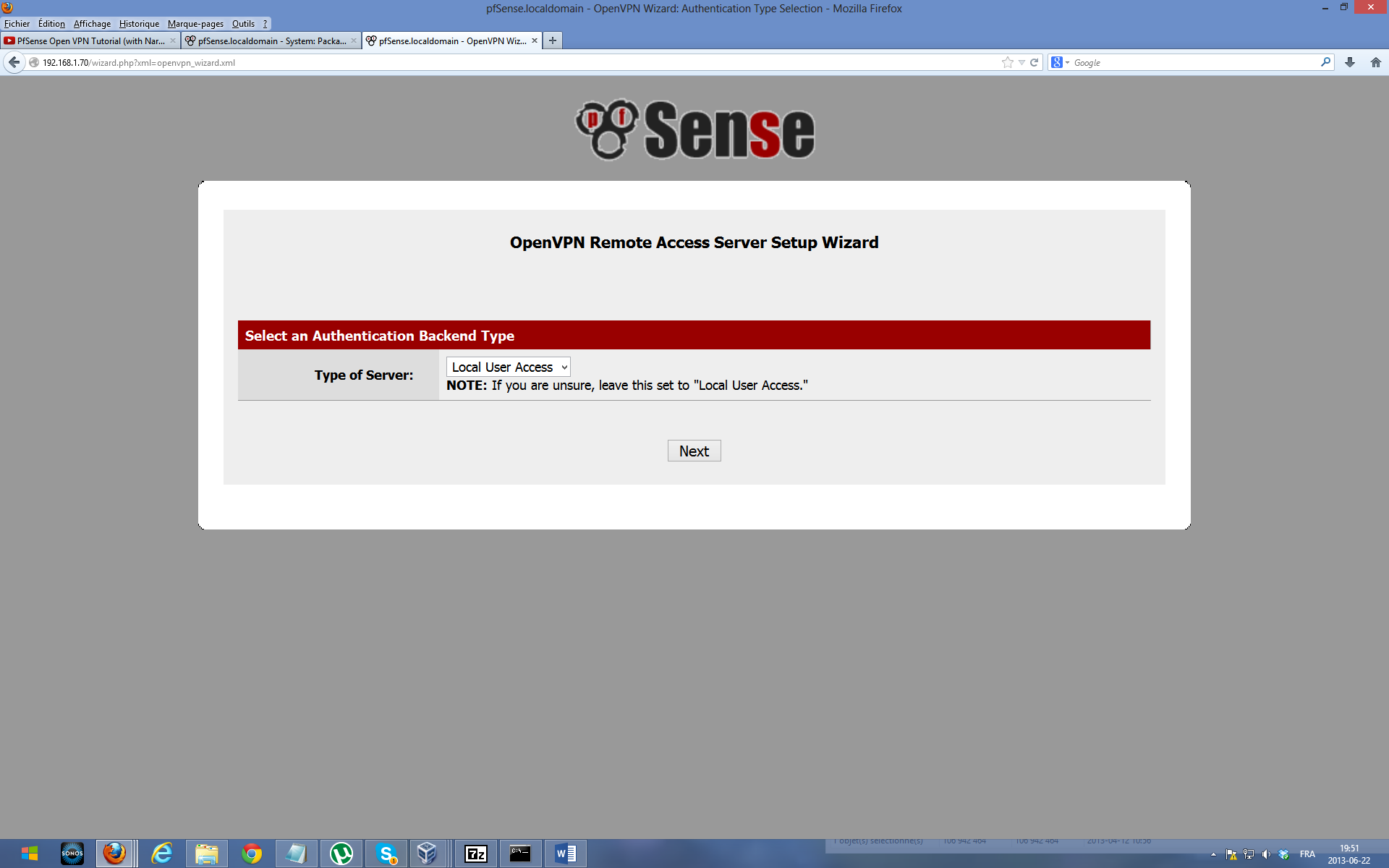
System – User Manager

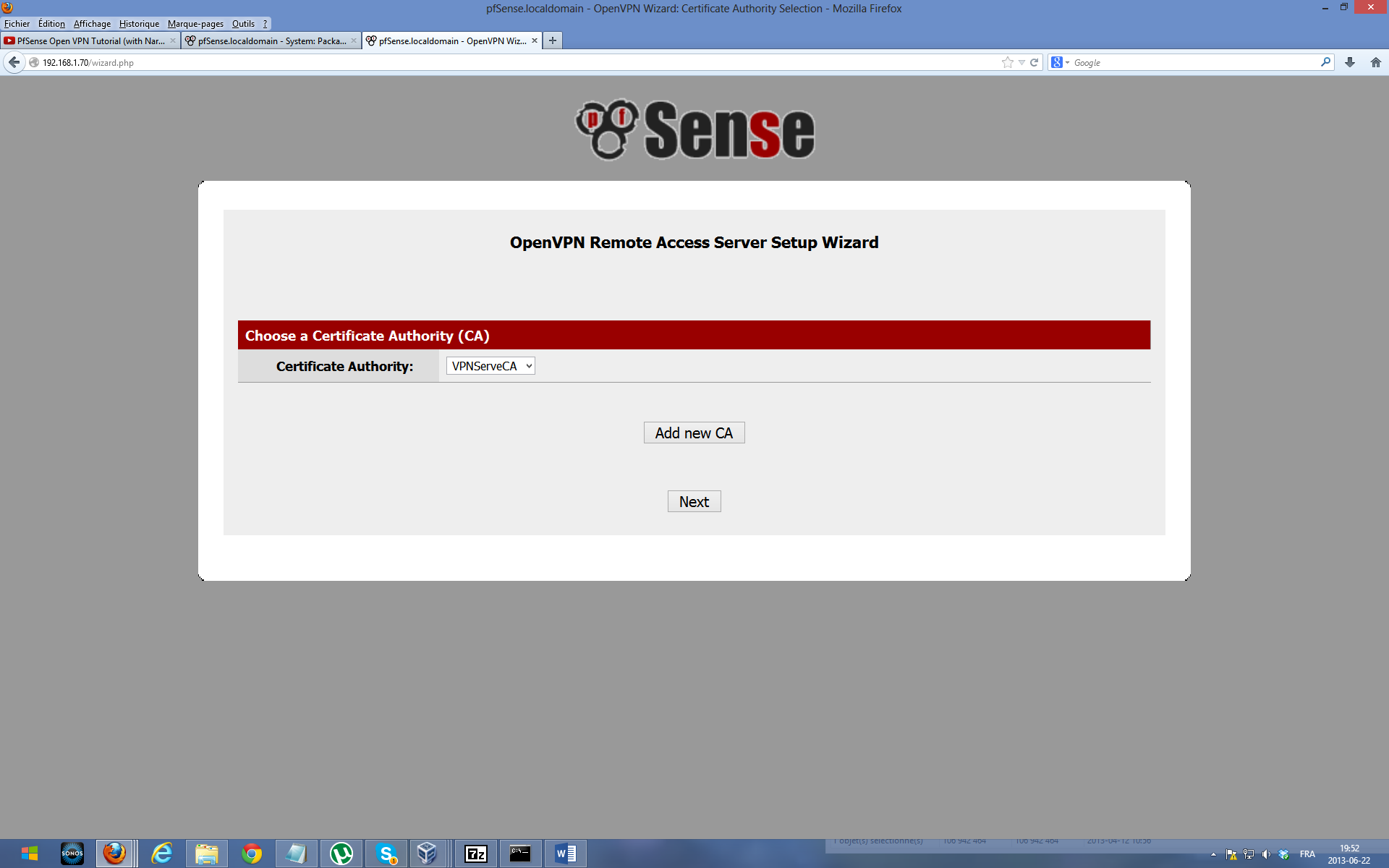




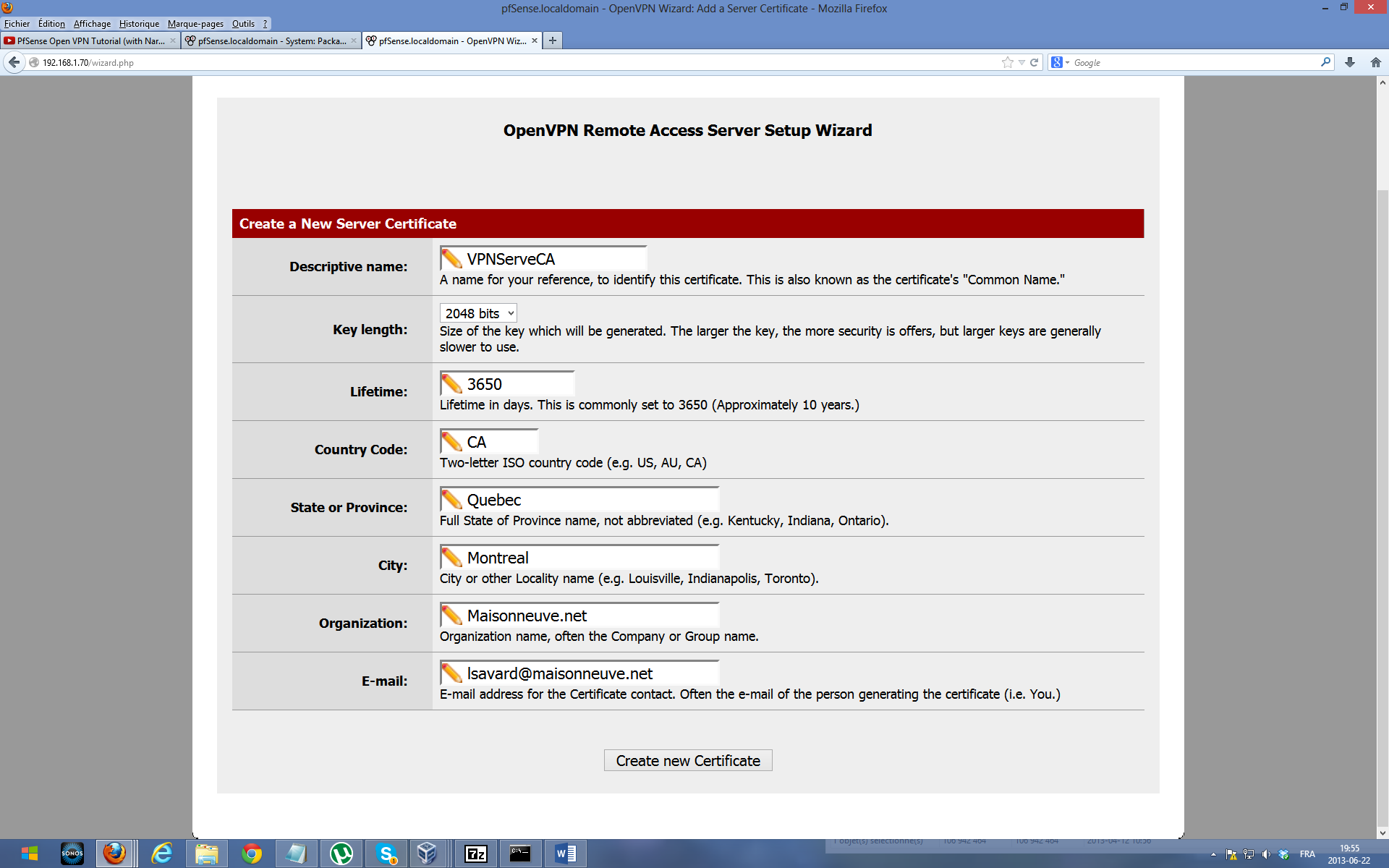
Mise en place du VPN

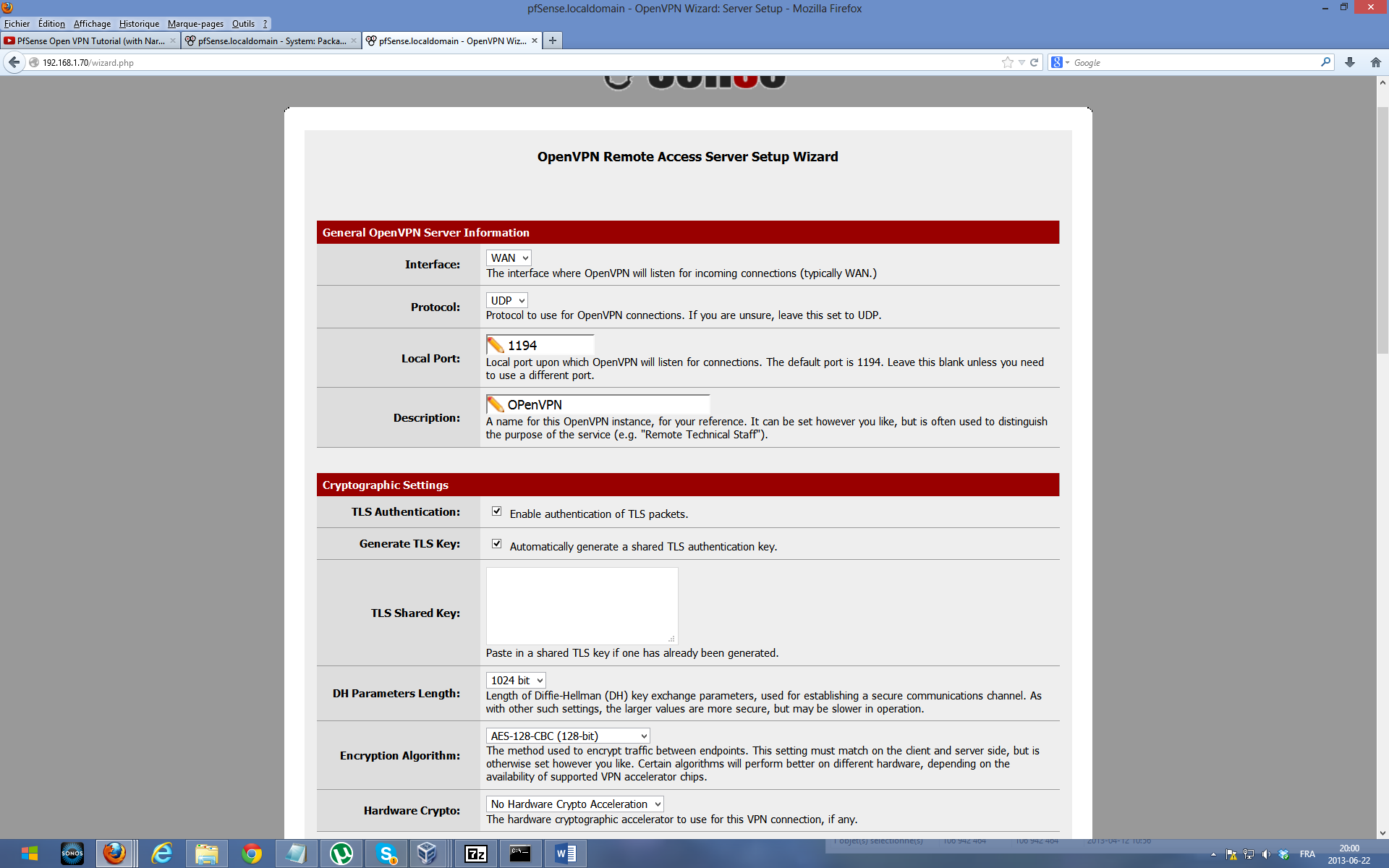
VPN – OpenVPN… Wizzard



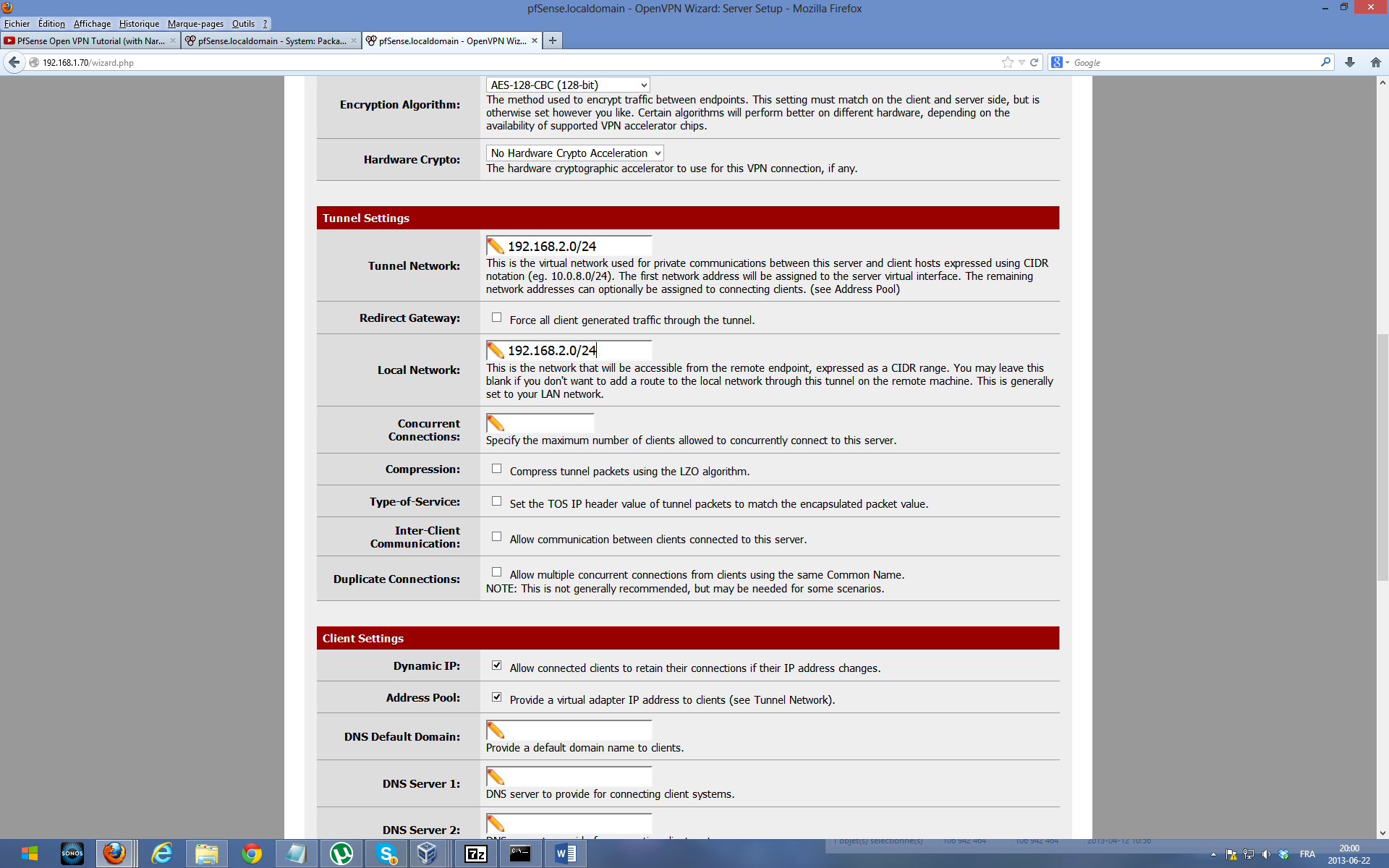


Add new certificate

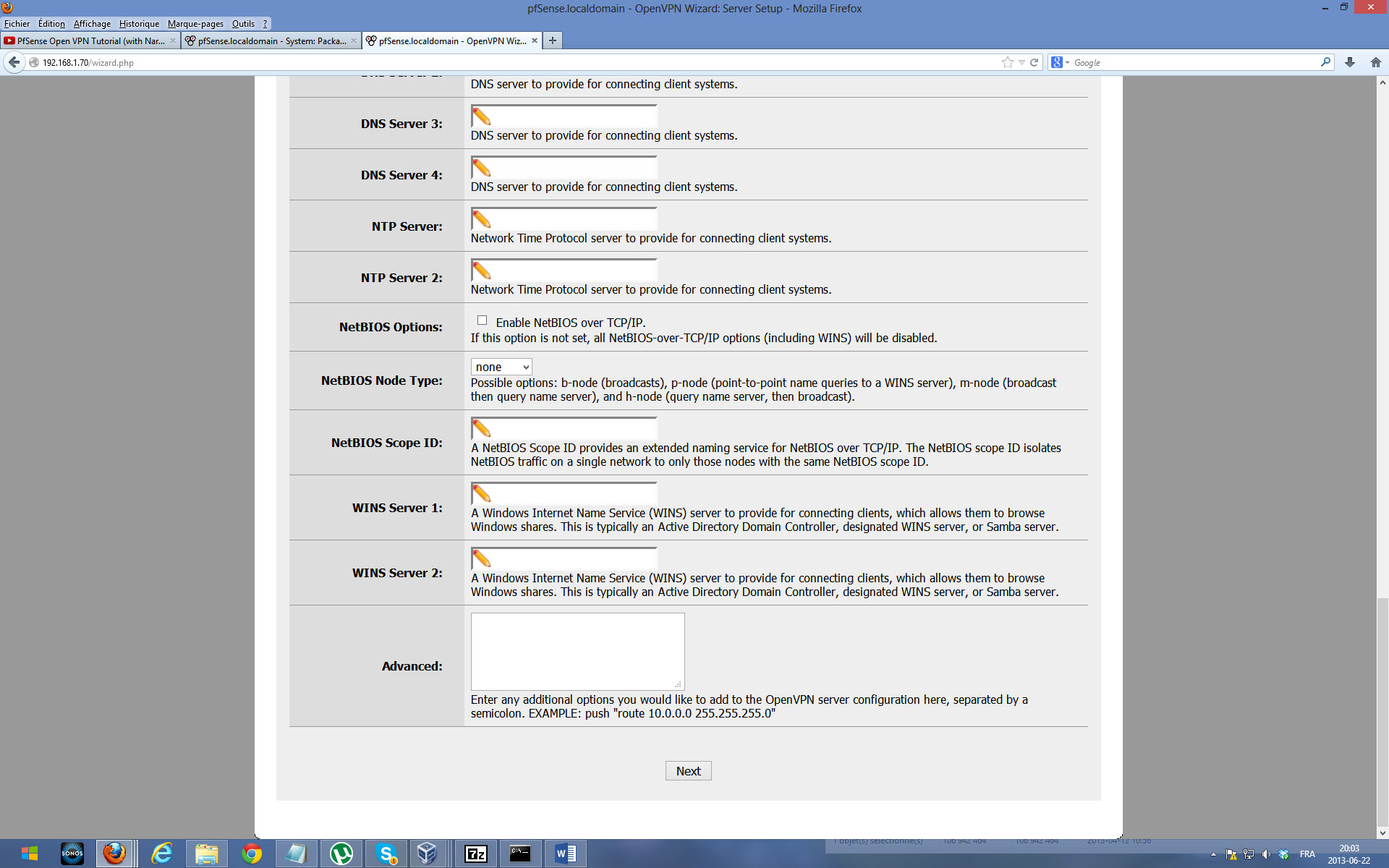




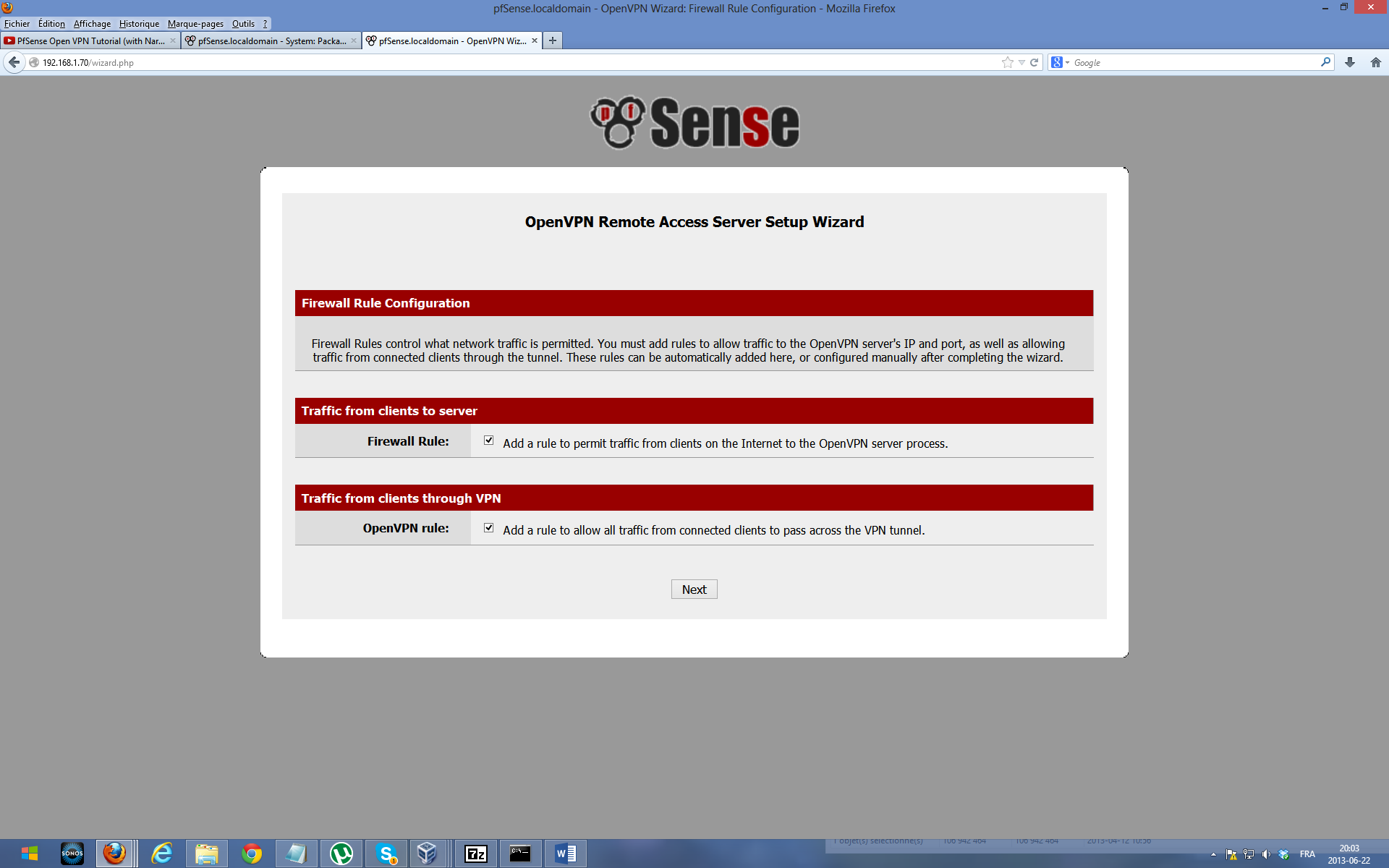
…



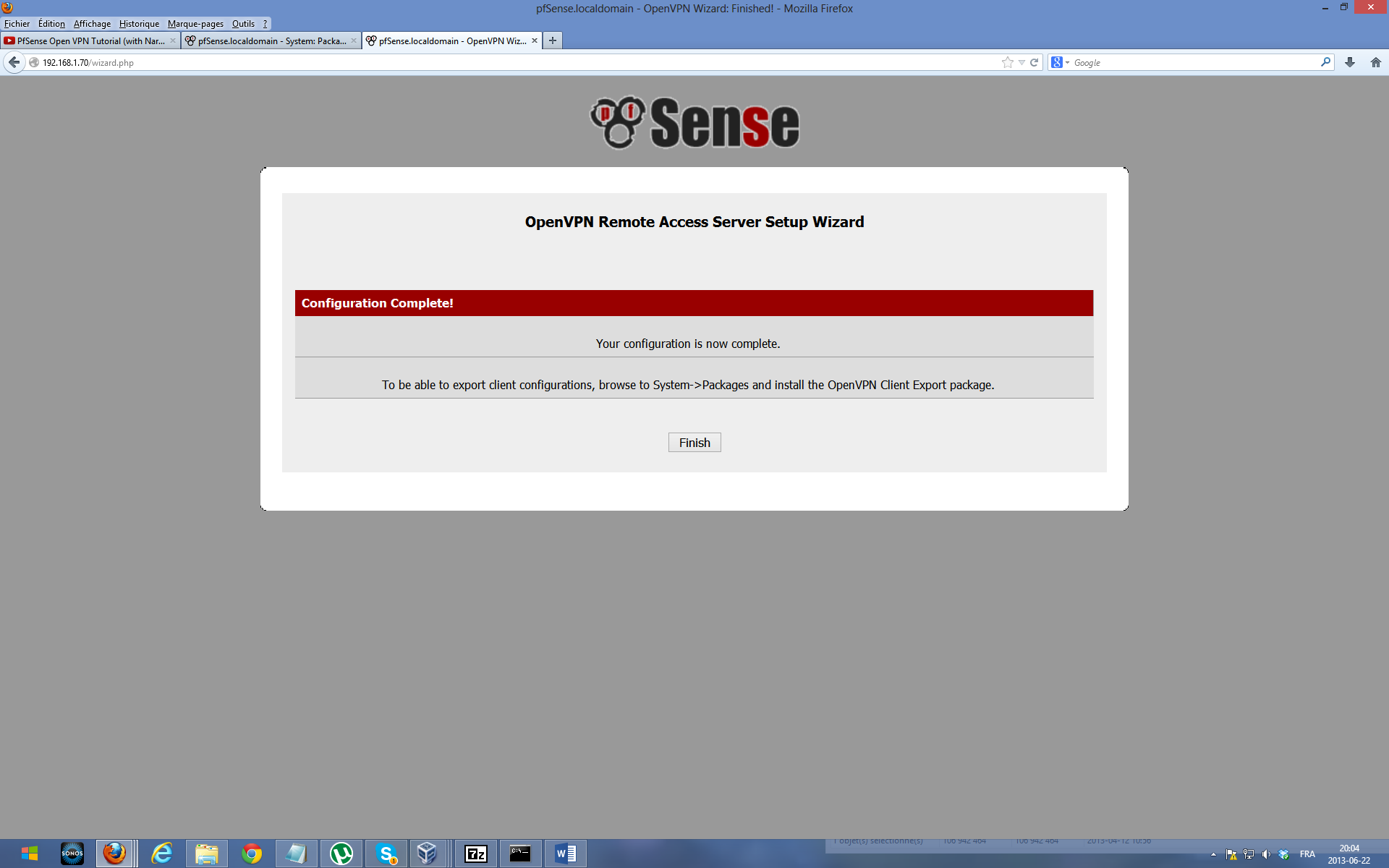
…

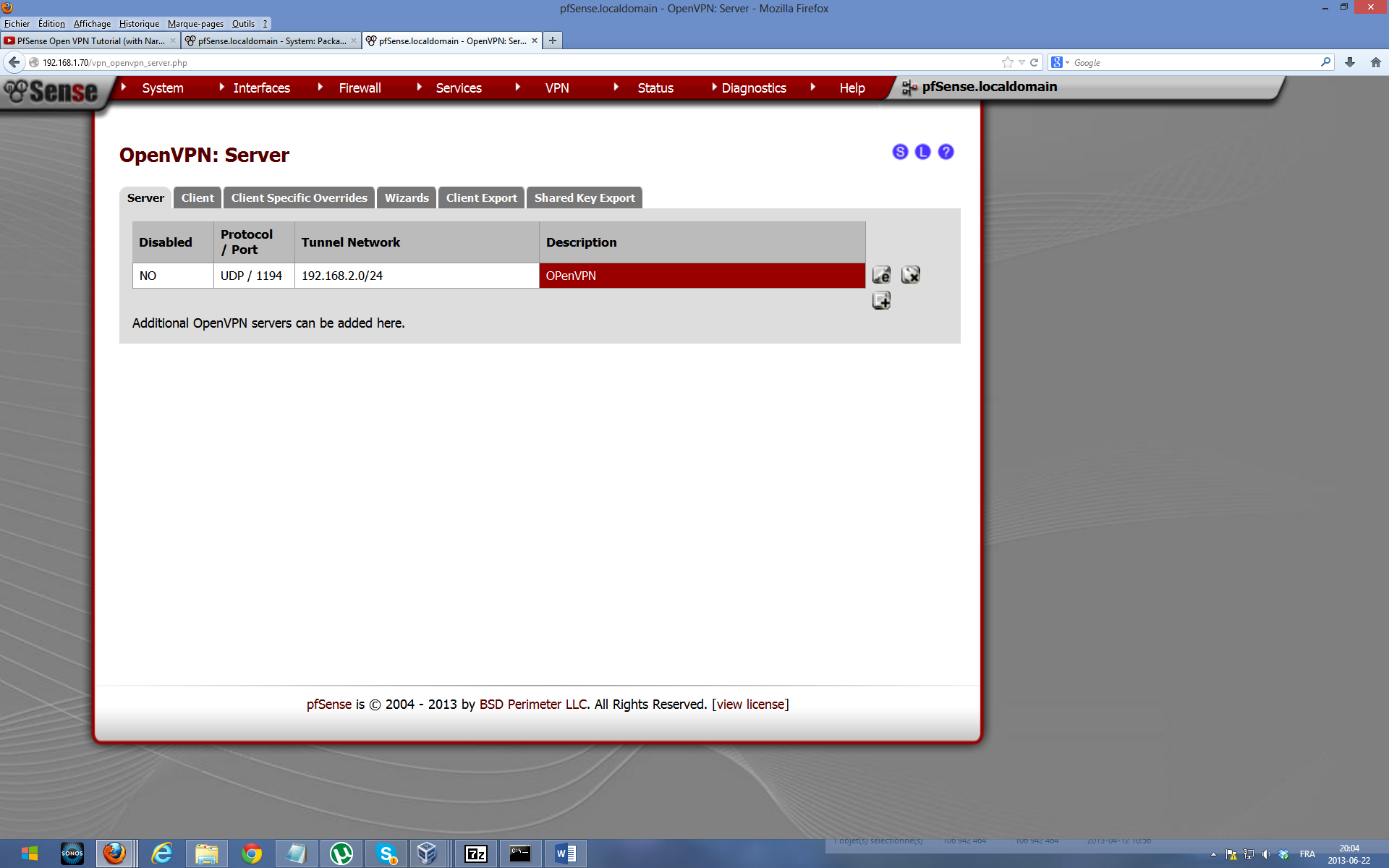


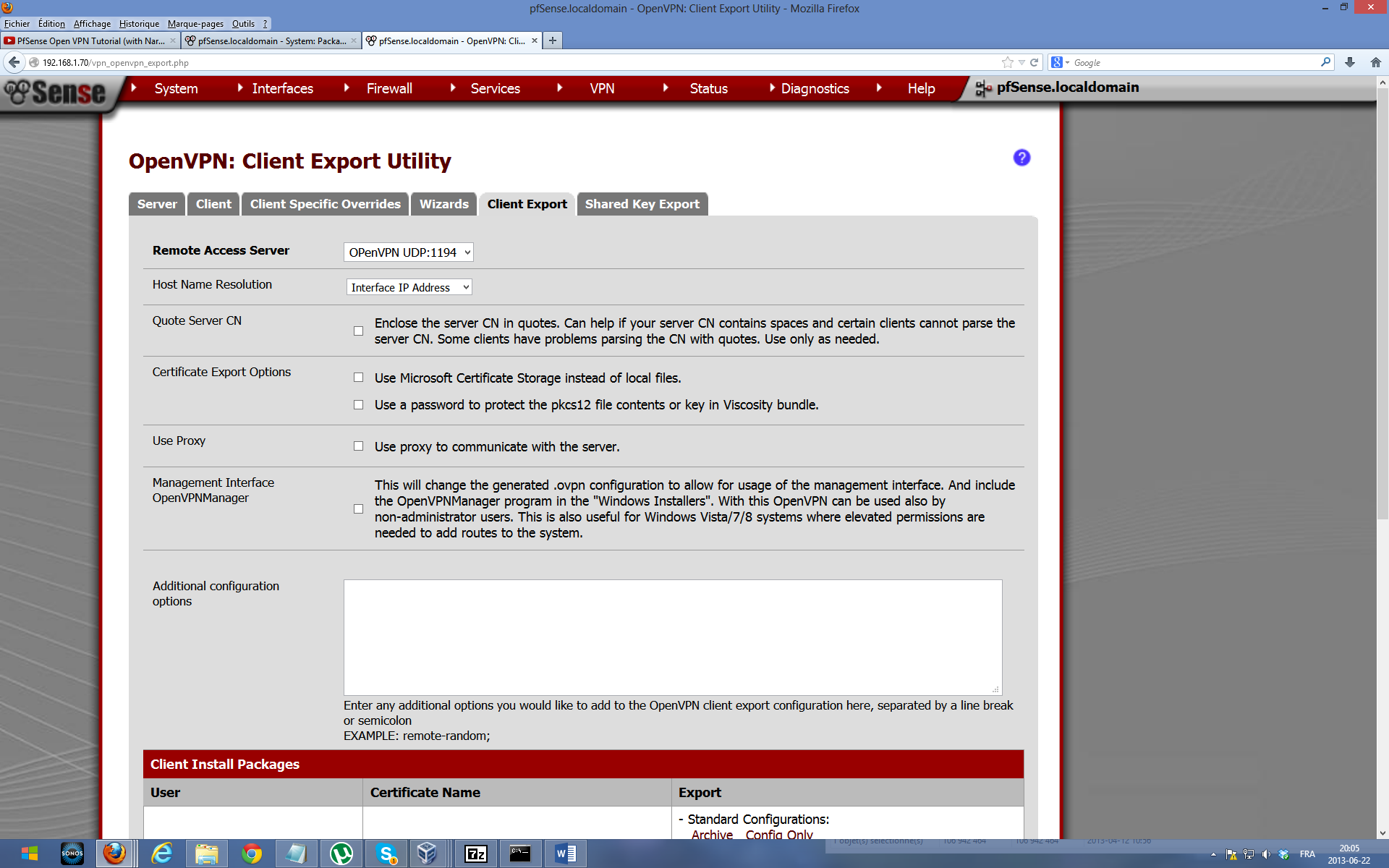
Next…



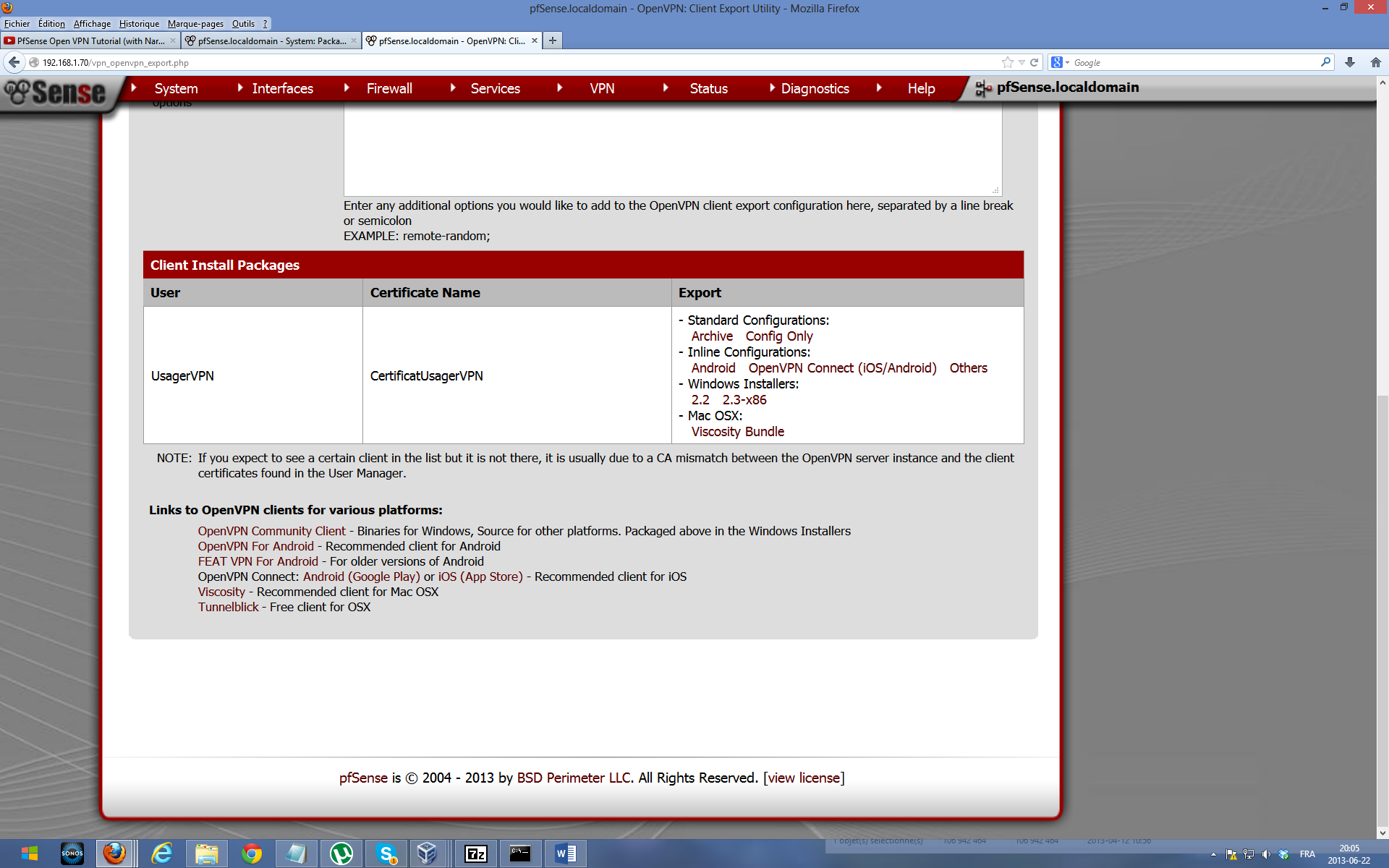
Next…



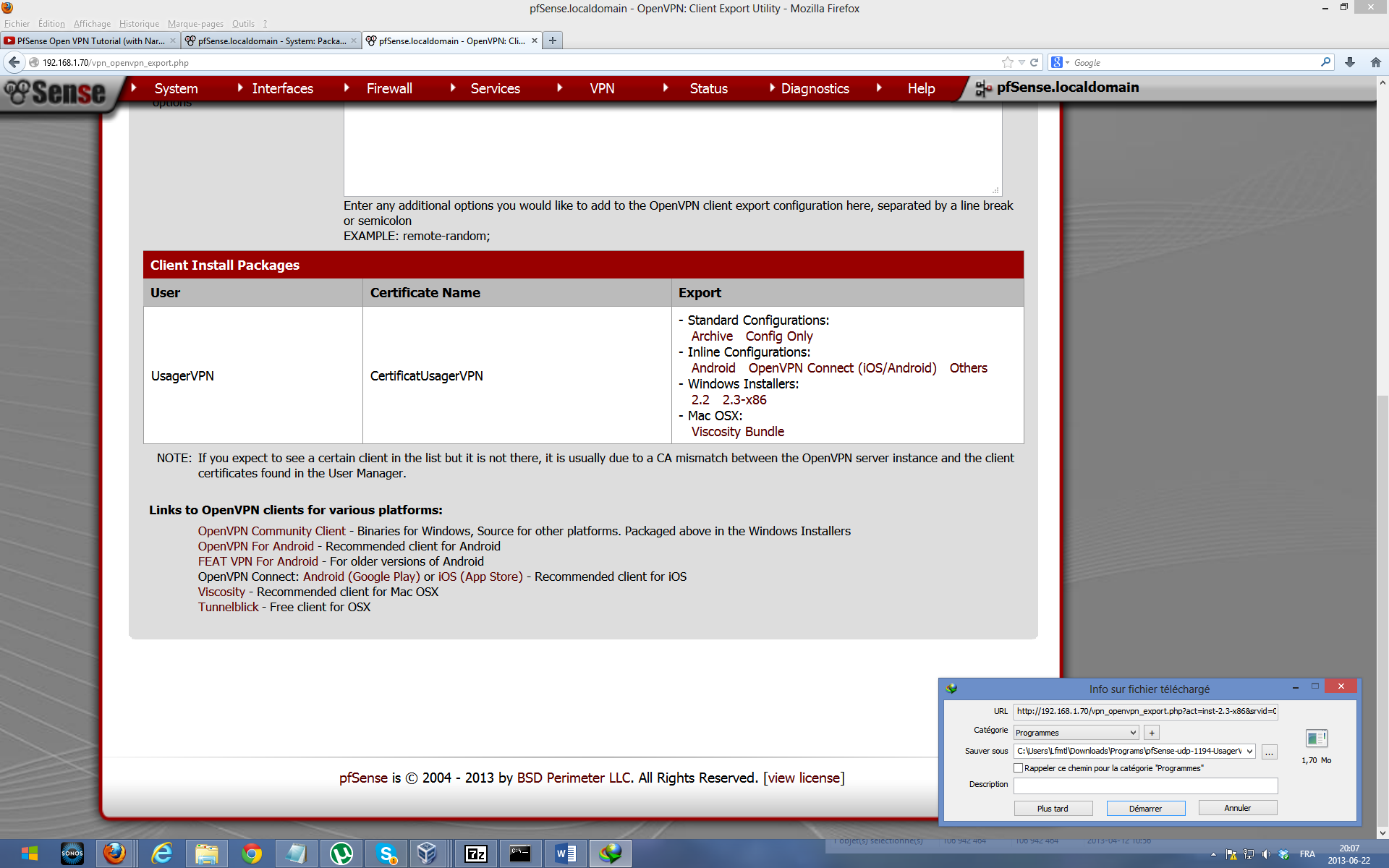




…



**Installation du client (suite)**



Vidéos YouTube

<http://www.youtube.com/watch?v=VdAHVSTl1ys>  
<http://www.youtube.com/watch?v=02vlrVNbe70>  
<http://www.youtube.com/watch?v=odjviG-KDq8>