HAUTE DISPONIBILITÉ DE MACHINE VIRTUELLE AVEC HYPER-V 2012 R2 – PARTIE CONFIGURATION OPENVPN SUR PFSENSE

Projet de semestre ITI soir 4ème année

Résumé

configuration OpenVpn sur pfsense 2.1

Etudiant :Tarek Watfa

tarek@watfa.ch

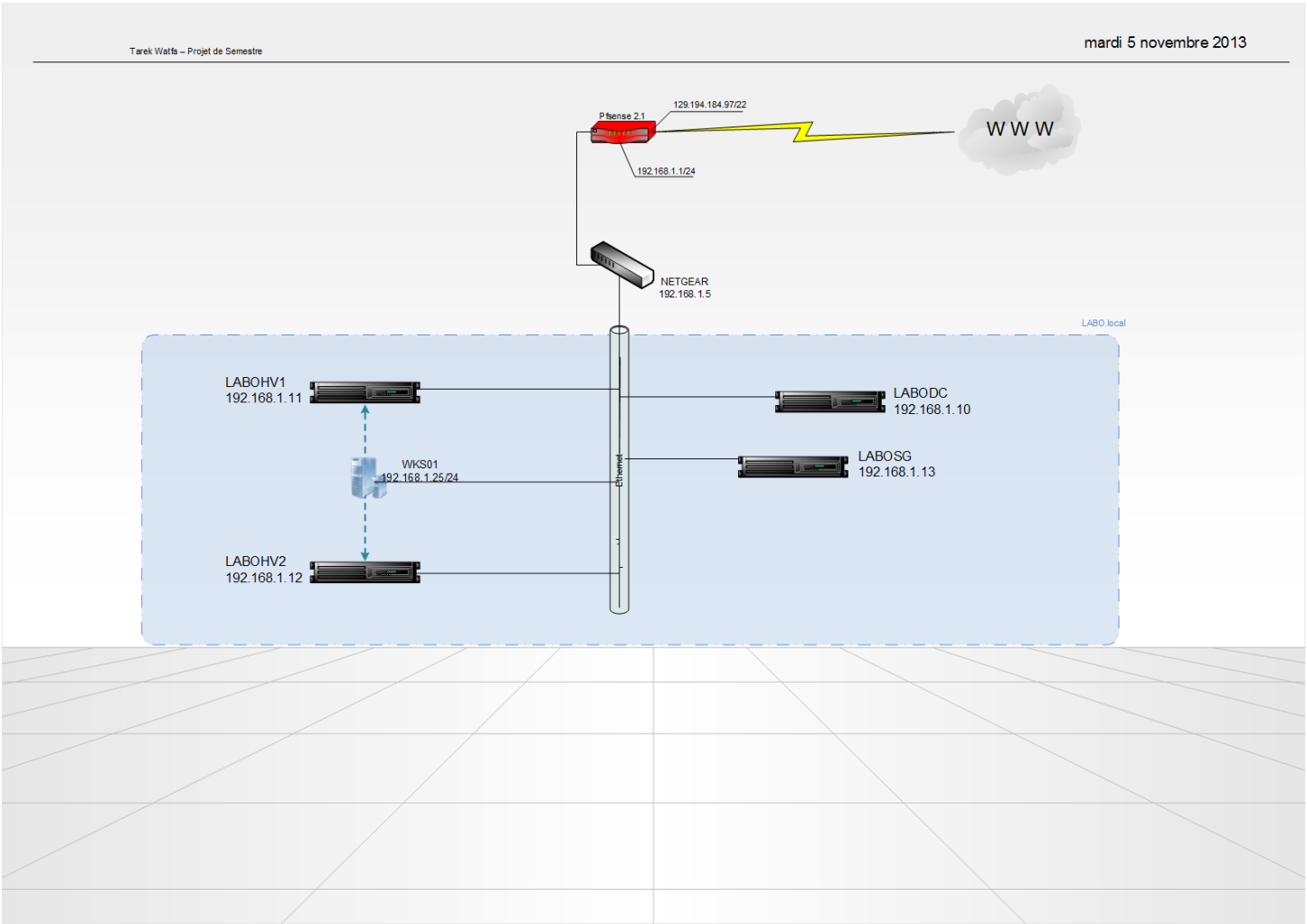
Sommaire :

Table des matières

Introduction :

Configuration d'une connexion OpenVpn sur pfsense 2.1 afin de permettre une connexion à distance vers le réseau privé du laboratoire. C'est succinct non ?

Schéma réseau du projet :



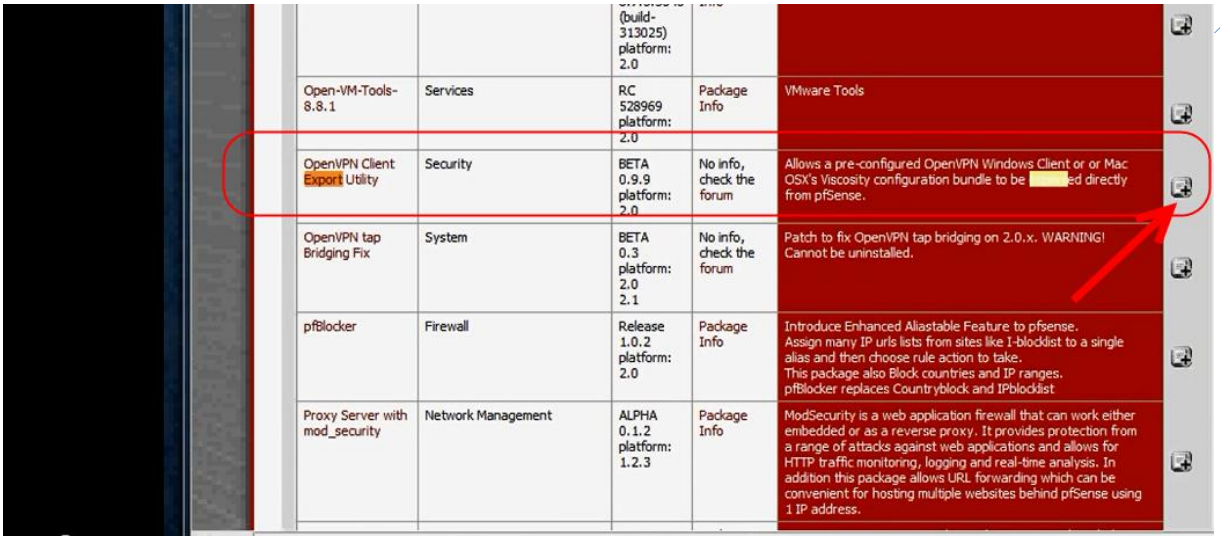
Installation du package OpenVPN Client Export Utility

Il convient de commencer par télécharger un package qui va nous permettre de simplifier par la suite l'installation du client OpenVpn ainsi que l'export de la configuration vers les postes mobiles.

Depuis l'interface de gestion du firewall :

System→packages →Available Packages.

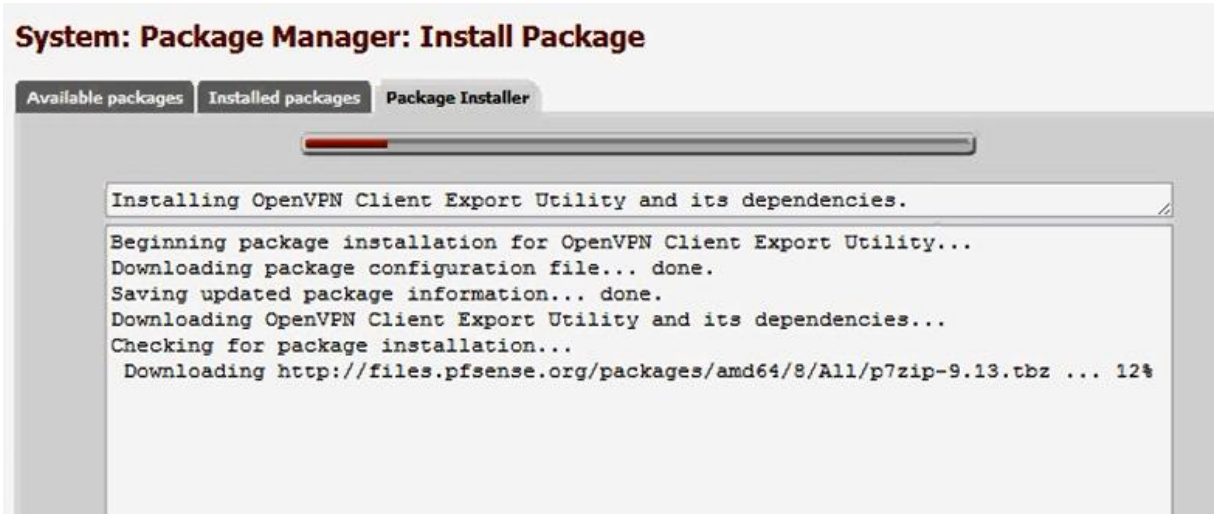
Sélectionner Open Vpn Client Export Utility et cliquer sur + pour l'installer.



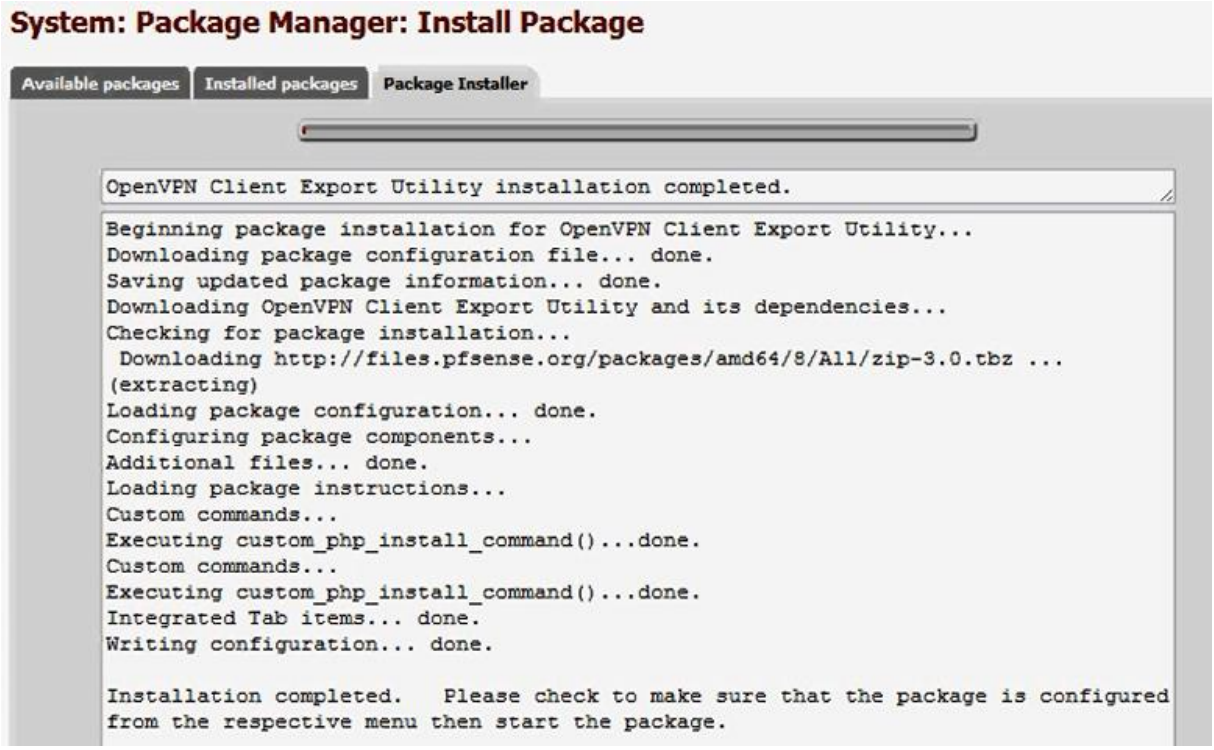
		(build-313025) platform: 2.0		
Open-VM-Tools-8.8.1	Services	RC 528969 platform: 2.0	Package Info	VMware Tools
OpenVPN Client Export Utility	Security	BETA 0.9.9 platform: 2.0	No info, check the forum	Allows a pre-configured OpenVPN Windows Client or or Mac OSX's Viscosity configuration bundle to be [redacted]ed directly from pfSense.
OpenVPN tap Bridging Fix	System	BETA 0.3 platform: 2.0 2.1	No info, check the forum	Patch to fix OpenVPN tap bridging on 2.0.x. WARNING! Cannot be uninstalled.
pfBlocker	Firewall	Release 1.0.2 platform: 2.0	Package Info	Introduce Enhanced Aliastable Feature to pfsense. Assign many IP urls lists from sites like I-blocklist to a single alias and then choose rule action to take. This package also Block countries and IP ranges. pfBlocker replaces Countryblock and IPblocklist
Proxy Server with mod_security	Network Management	ALPHA 0.1.2 platform: 1.2.3	Package Info	ModSecurity is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis. In addition this package allows URL forwarding which can be convenient for hosting multiple websites behind pfSense using 1 IP address.

Confirmer l'installation.

L'installation se lance.



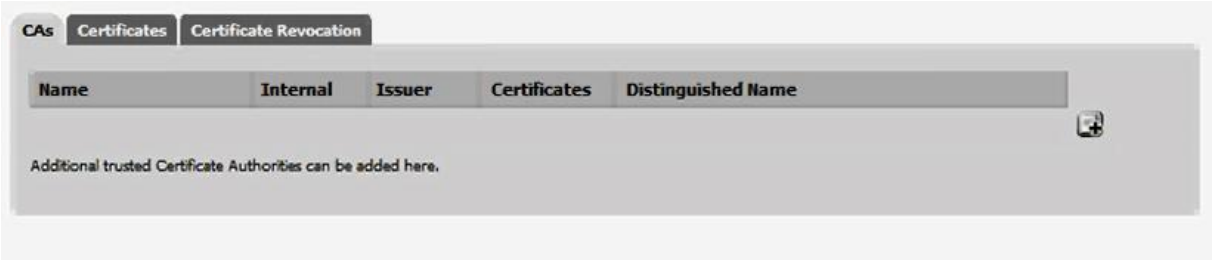
Et se termine comme suit :



Création de l'autorité de certification

Depuis l'interface de gestion du firewall faites:

System→Cert Manager



Dans l'onglet « Cas » cliquer sur « + » pour créer une nouvelle autorité de certification serveur VPN.

On remplit comme suit :

Desciptive name : **VPN Server CA**

Method : **Create an internal Certificate Authority**

Key length : **2048 bits**

Digest Algorithm : **SHA256**

Lifetime : **3650** (10 ans)

Country Code : **CH**

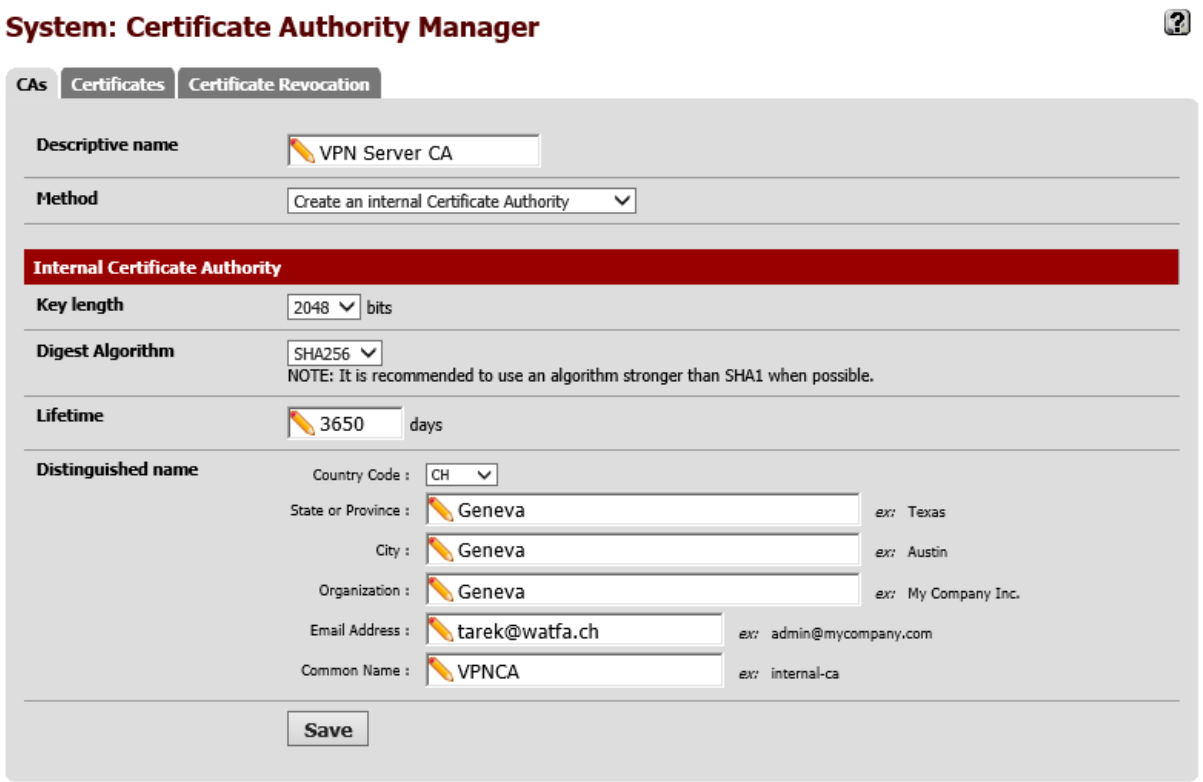
State or Province : **Geneva**

City : **Geneva**

Organization : **Geneva**

Email Address : **tarek@watfa.ch**

Common Name : **VPNCA**



Et on enregistre.

Notre certificat CA est créé.

Création d'utilisateur openVPN et certificat privé pour l'utilisateur

Depuis l'interface de gestion du firewall faites:

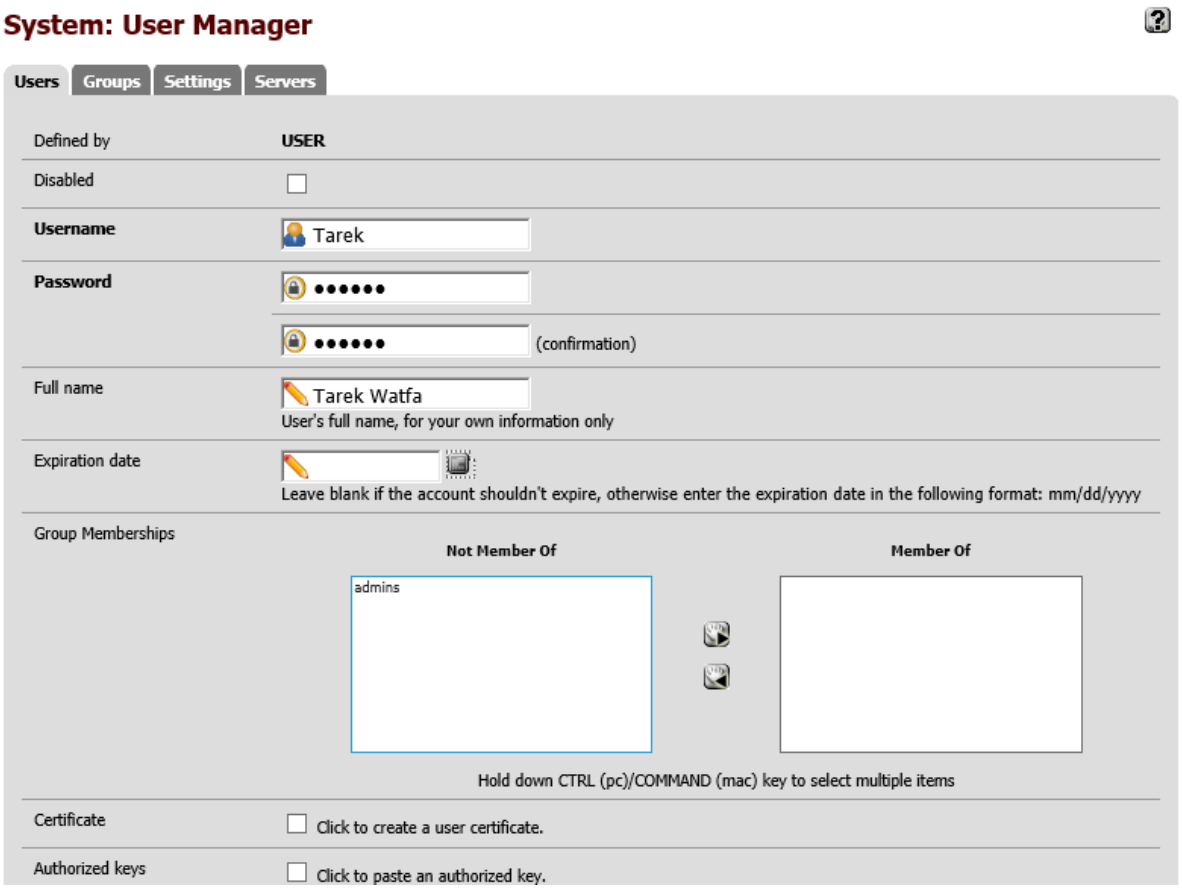
System→User Manager

Dans l'onglet Users cliquer sur + pour créer un nouvel utilisateur.

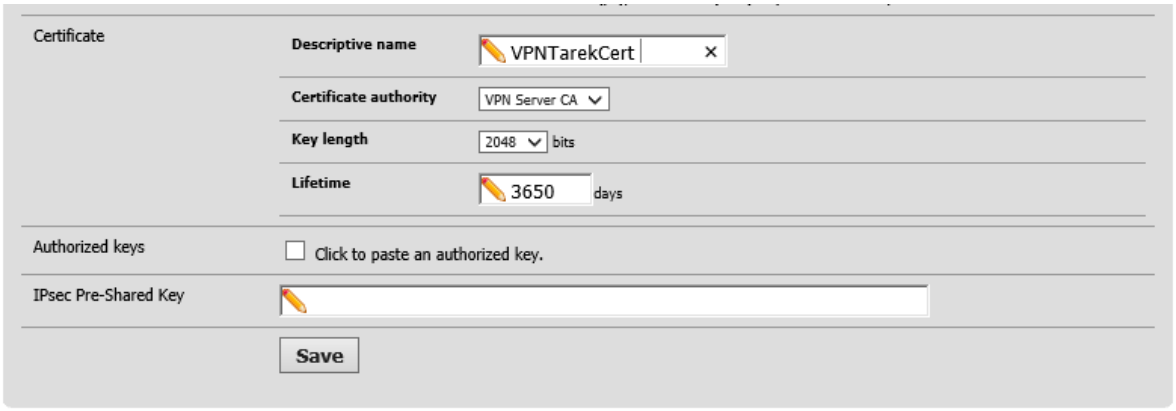
Username : Tarek

Password : ******

Full name : Tarek Watfa



Cliquer sur « *click to create a user certificate* » à partir du CA créé plus haut.



Certificate	Descriptive name	VPN**TarekCert**
	Certificate authority	**VPN Server CA**
	Key length	**2048 bits**
	Lifetime	**2650 days**

Enregistrer.

Configuration interface WAN OpenVPN

Il faut qu'on configure le firewall afin qu'il écoute sur le port WAN.

Depuis l'interface de gestion du firewall faites:

VPN→OpenVPN

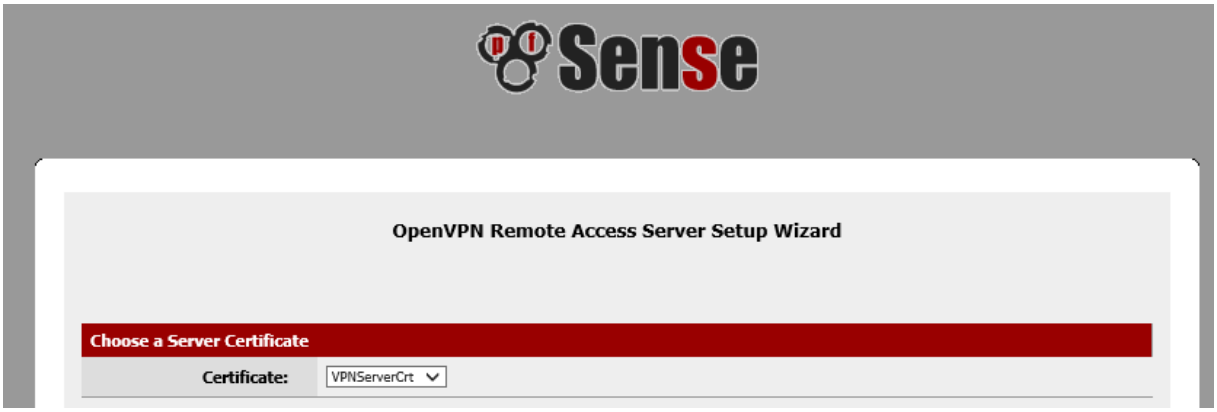
Onglet Wizard

On définit le type d'authentification.

Dans notre cas des comptes locaux, mais sinon on peut faire du LDAP ou du RADIUS comme authentification.

A l'étape suivante, on choisit le certificat CA qu'on a créé bien plus haut et qui va valider le certificat donné au PC mobile.

On sélectionne le certificat du serveur.



Interface : **WAN** c'est l'interface sur laquelle le serveur OpenVPN écoutera.

Port : **UDP**

Local Port : **1194**

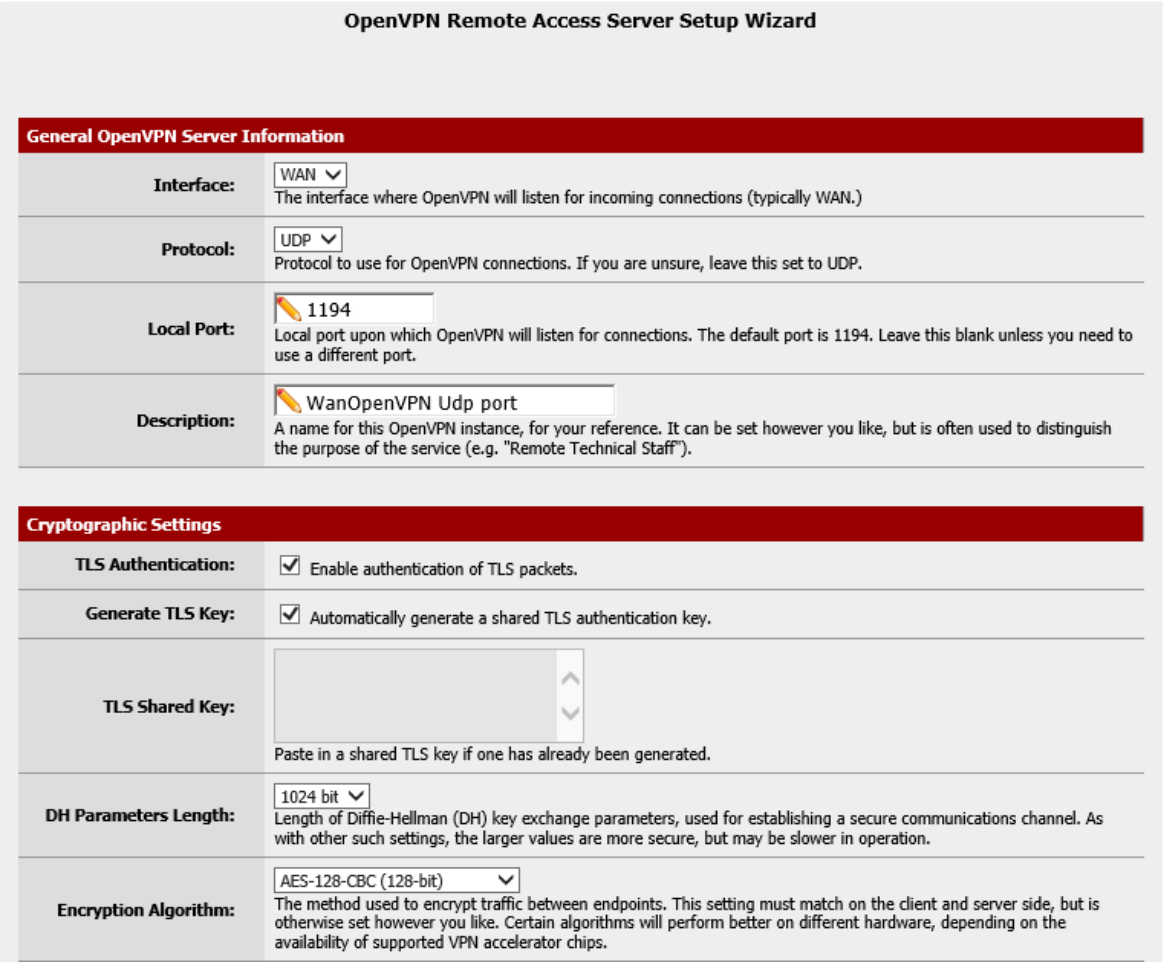
Description : **WanOpenVpn UDP port**

TLS Authentification : **Enable authentification of TLS packets.**

Generate TLS Key : **Automatically generate a shared TLS authentication key**

DH Parameters Length : **1024 bits.**

Encryption Algorithm : **AES-128-CBC (128 bits)**



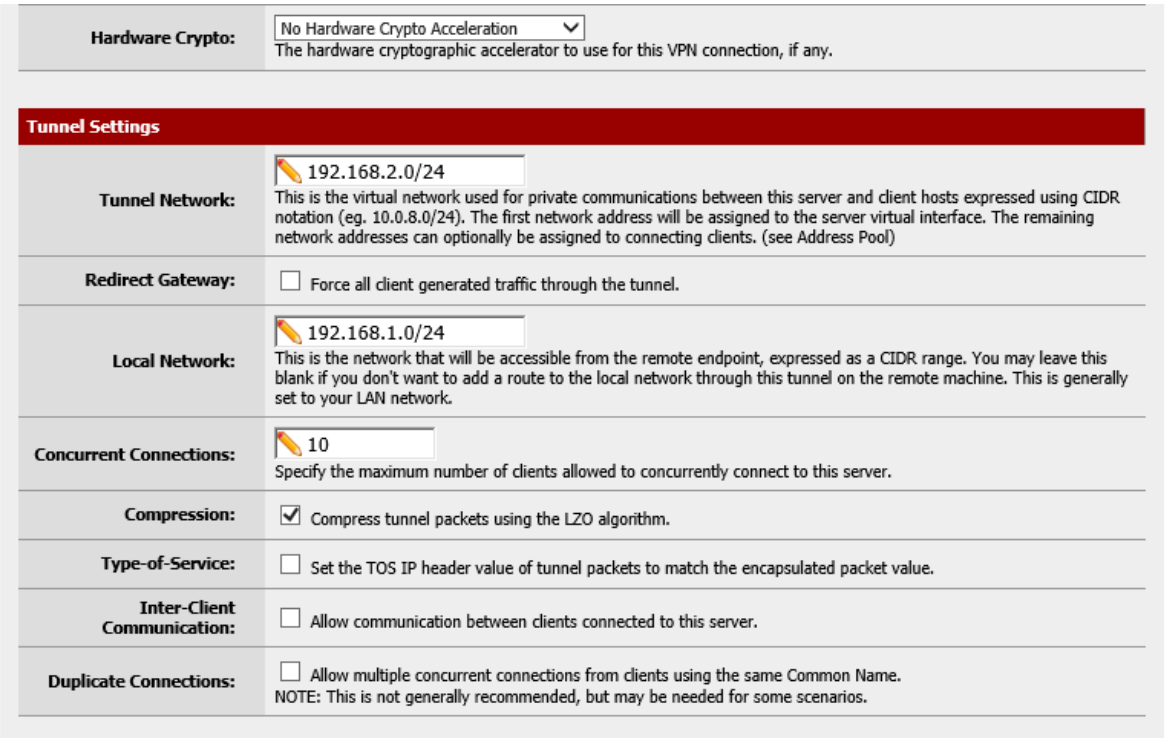
Hardware crypto : **no Hardware Crypto Acceleration**

Tunnel Network : **192.168.2.0/24** (le réseau virtuel au quel le pc distant sera connecté)

Redirect Gateway : **décocher Force all client generated traffic the tunnel**

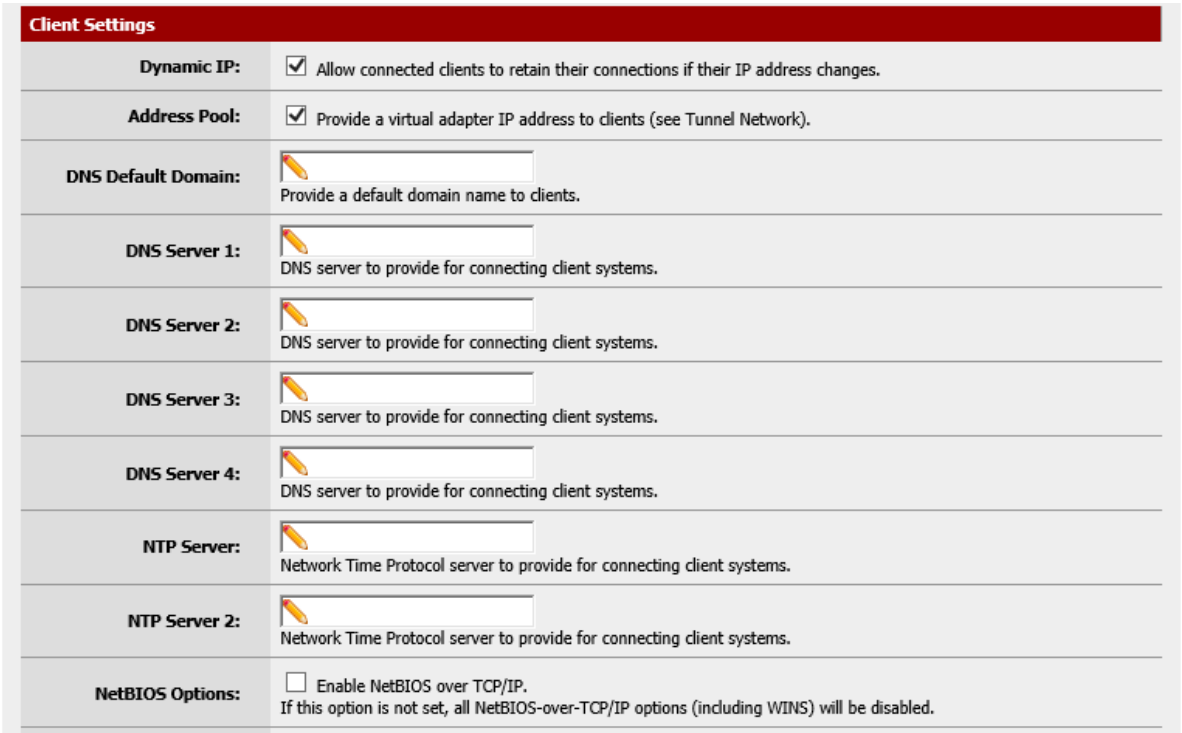
Local Network : **192.168.1.0/24** (le réseau local du labo)

Compression : **cocher Compress tunnel packets using the LZO algorithm.**

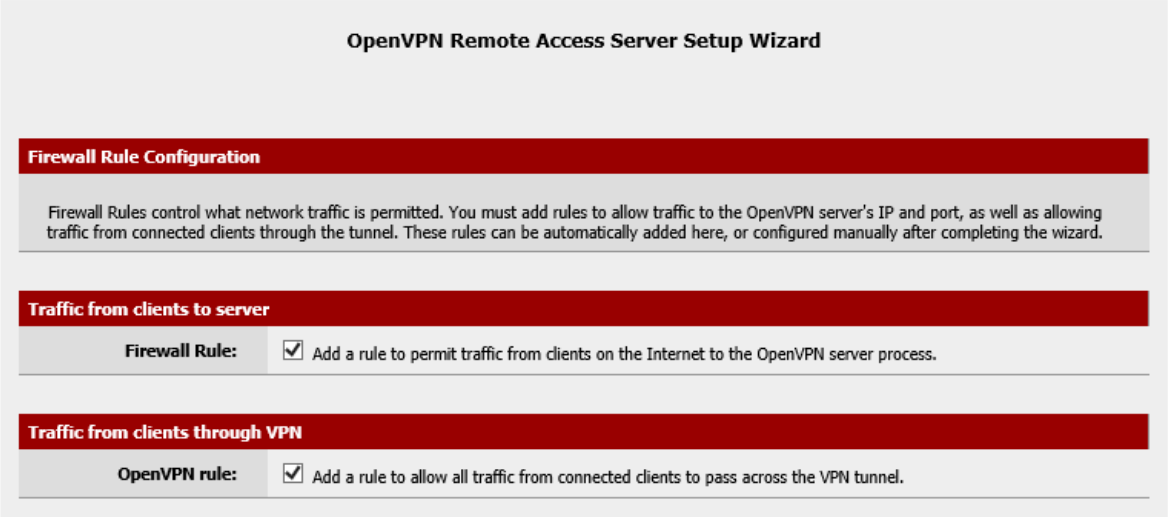


Dynamic IP : **cocher Allow connected clients to retain their connections if their IP address changes.**

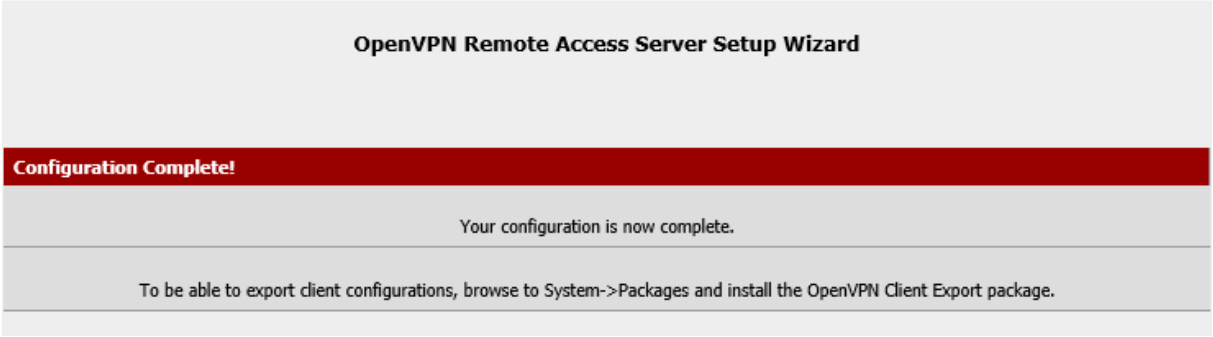
Address Pool : **Provide a virtual adapter IP address to clients (see Tunnel Network).**



Le reste on laisse, par défaut, vide et on valide.



Le wizard ajoute les règles dans le firewall et on valide.



Ajouter la route pour accéder au réseau

Il faut ajouter une route dans la configuration du serveur VPN afin de pousser les clients à accéder au lan donc du réseau virtuel 192.168.2.0 jusqu'à 192.168.1.0.

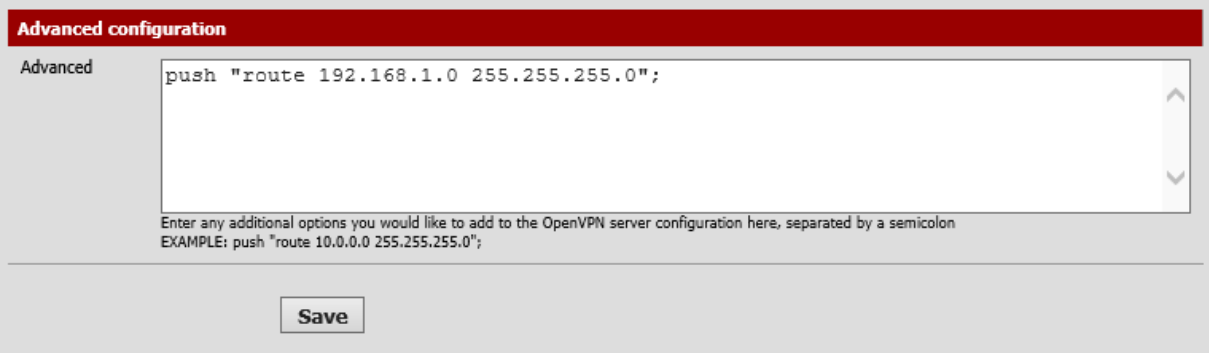
Depuis l'interface de gestion du firewall:

VPN→OpenVPN

Dans l'onglet server, sélectionner la connexion server qu'on vient de créer et cliquer sur « e » pour éditer.

Tout en bas dans « advanced configuration » ajouter.

Push ''route 192.168.1.0 255.255.255.0 '';



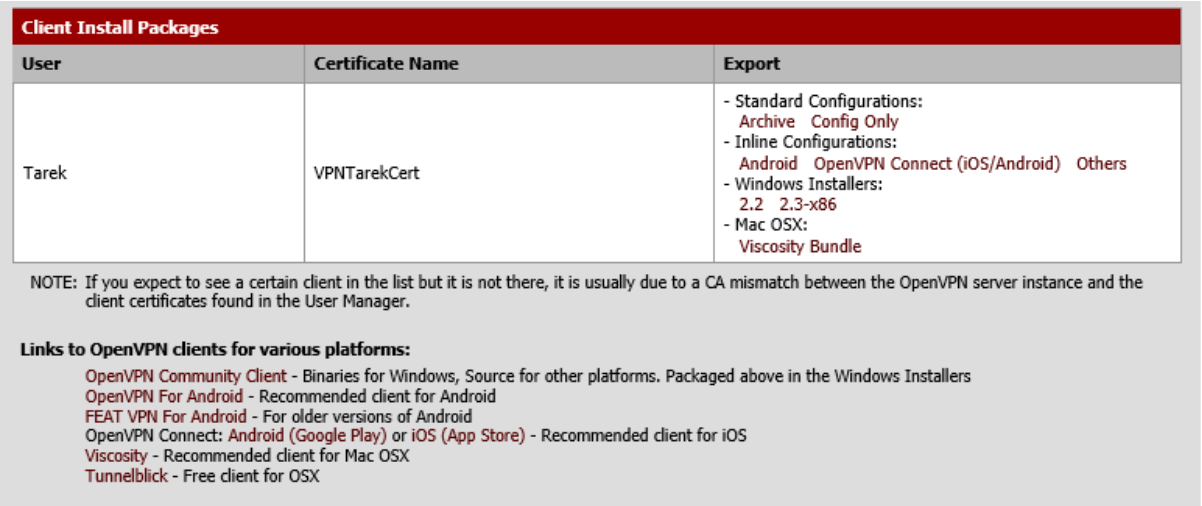
La configuration du serveur est dorénavant terminée.

Export du client openVPN et la configuration

Depuis l'interface de gestion du firewall faites:

VPN→OpenVPN

Onglet client Export



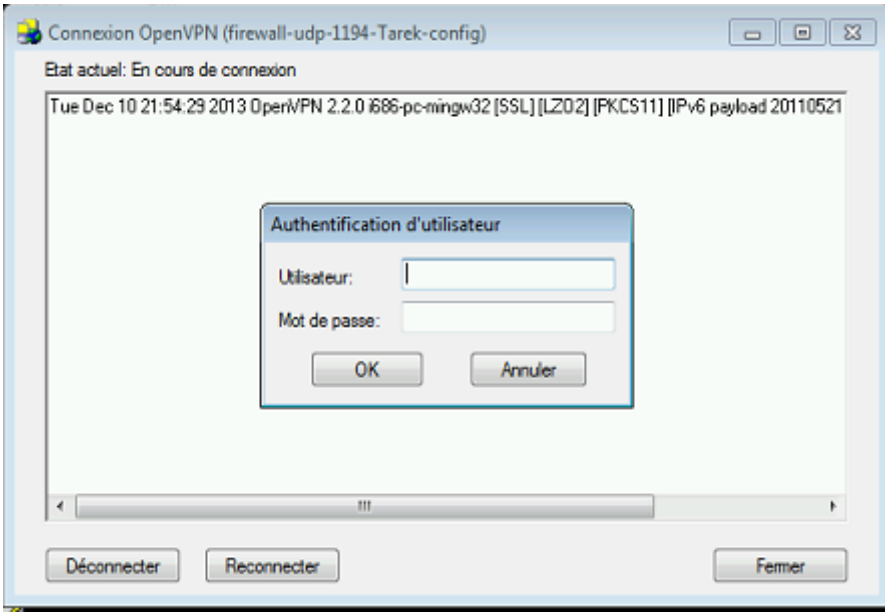
On télécharge le client qui correspond à notre Système.

Test de connexion

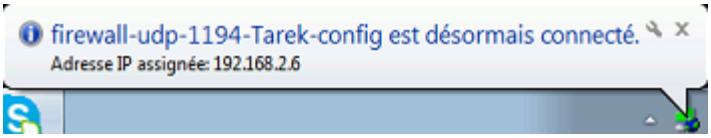
On installe le package téléchargé depuis le site qui contient le client OpenVPN avec la configuration intégrée.

Remarque sur un windows 7 ou 8 : il faut exécuter le client « OPENVPN GUI » en tant qu'administrateur !

Login :



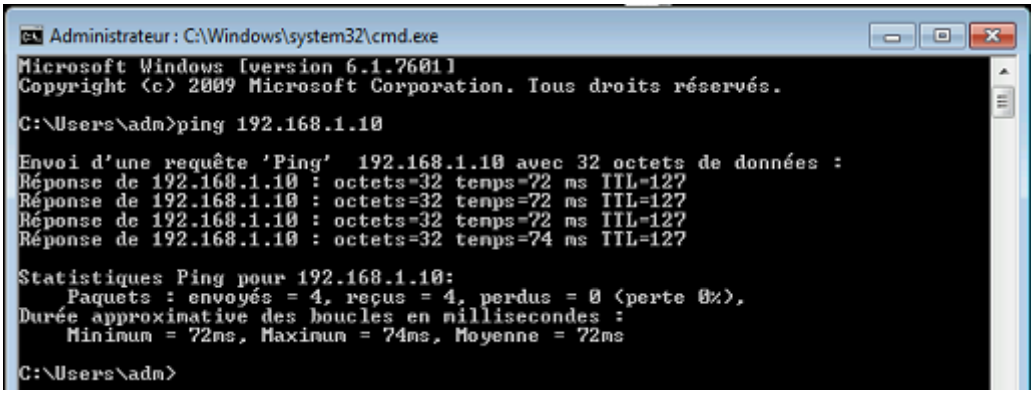
La connexion est établie.



Log :

Tue Dec 10 21:51:17 2013 OpenVPN 2.2.0 i686-pc-mingw32 [SSL] [LZO2] [PKCS11] [IPv6 payload 20110521-1 (2.2.0)] built on May 21 2011
Tue Dec 10 21:51:22 2013 IMPORTANT: OpenVPN's default port number is now 1194, based on an official port number assignment by IANA. OpenVPN 2.0-beta16 and earlier used 5000 as the default port.
Tue Dec 10 21:51:22 2013 WARNING: Make sure you understand the semantics of --tls-remote before using it (see the man page).
Tue Dec 10 21:51:22 2013 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or executables
Tue Dec 10 21:51:22 2013 Control Channel Authentication: using 'firewall-udp-1194-Tarek-tls.key' as a OpenVPN static key file
Tue Dec 10 21:51:22 2013 LZO compression initialized
Tue Dec 10 21:51:22 2013 UDPv4 link local (bound): [undef]:1194
Tue Dec 10 21:51:22 2013 UDPv4 link remote: 129.194.184.97:1194
Tue Dec 10 21:51:22 2013 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Tue Dec 10 21:51:29 2013 [VPNServerCrt] Peer Connection Initiated with 129.194.184.97:1194
Tue Dec 10 21:51:31 2013 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Tue Dec 10 21:51:31 2013 open_tun, tt->ipv6=0
Tue Dec 10 21:51:31 2013 TAP-WIN32 device [Connexion au réseau local] opened: \\.\Global\{9675E6D2-F35A-4C14-8027-5345658634C6}.tap
Tue Dec 10 21:51:31 2013 Notified TAP-Win32 driver to set a DHCP IP/netmask of 192.168.2.6/255.255.255.252 on interface {9675E6D2-F35A-4C14-8027-5345658634C6} [DHCP-serv: 192.168.2.5, lease-time: 31536000]
Tue Dec 10 21:51:31 2013 Successful ARP Flush on interface [30] {9675E6D2-F35A-4C14-8027-5345658634C6}
Tue Dec 10 21:51:36 2013 ROUTE: route addition failed using CreateIpForwardEntry: L'objet existe déjà. [status=5010 if_index=30]
Tue Dec 10 21:51:36 2013 env_block: add PATH=C:\Windows\System32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
Tue Dec 10 21:51:37 2013 Initialization Sequence Completed

Test de ping vers le serveur distant :



Le temps de 72 ms correspond à un débit correct de la connexion vpn.