



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 :

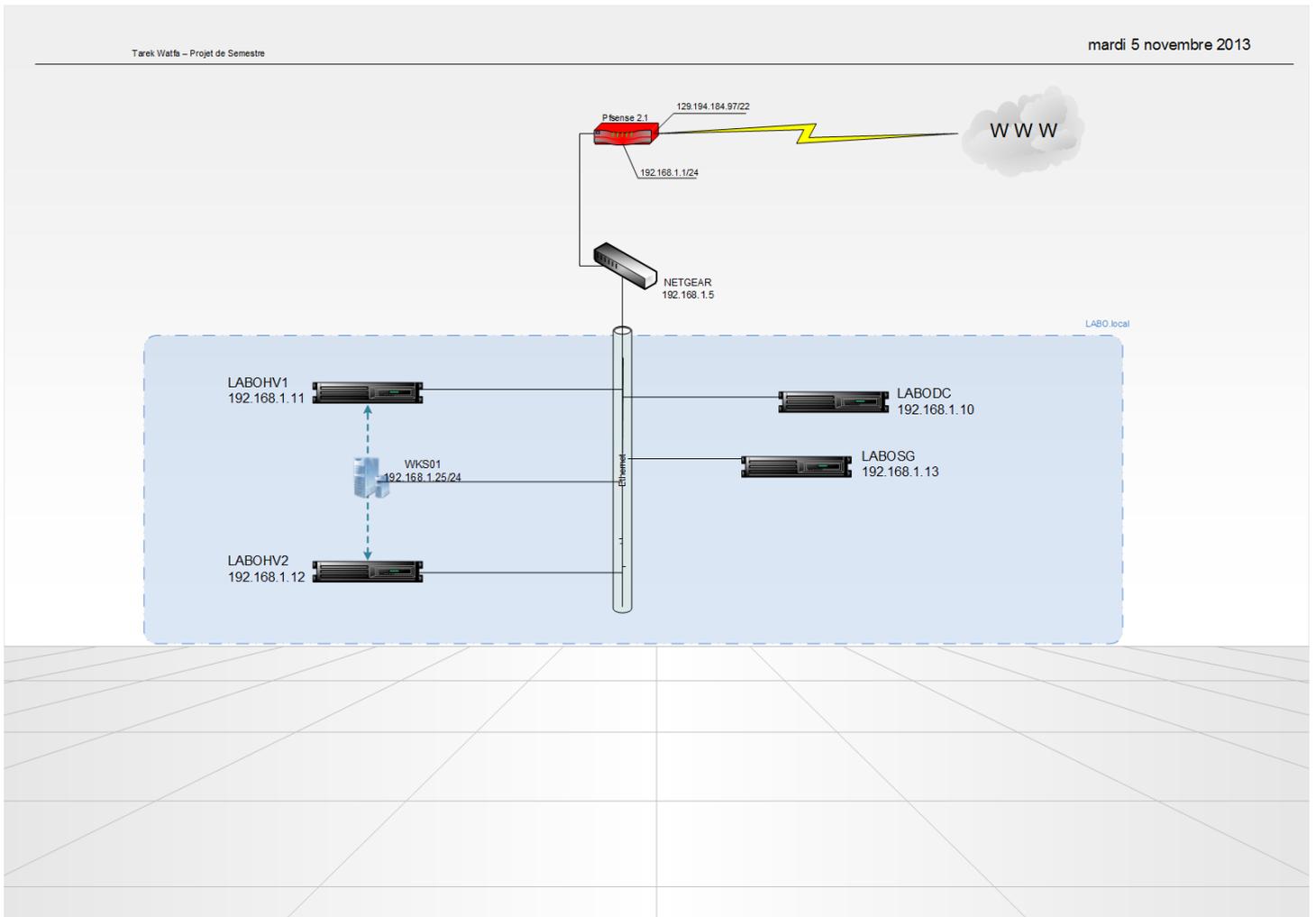
Table des matières

Schéma réseau du projet.....	2
Installation du package OpenVPN Client Export Utility	2
Création de l'autorité de certification.....	4
Création d'utilisateur openVPN et certificat privé pour l'utilisateur	6
Configuration interface WAN OpenVPN	7
Ajouter la route pour accéder au réseau	11
Export du client openVPN et la configuration.....	12
Test de connexion	12

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 installed 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.

System: Package Manager: Install Package

Available packages | Installed packages | **Package Installer**

```
Installing OpenVPN Client Export Utility and its dependencies.
Beginning package installation for OpenVPN Client Export Utility...
Downloading package configuration file... done.
Saving updated package information... done.
Downloading OpenVPN Client Export Utility and its dependencies...
Checking for package installation...
Downloading http://files.pfsense.org/packages/amd64/8/All/p7zip-9.13.tbz ... 12%
```

Et se termine comme suit :

System: Package Manager: Install Package

Available packages | Installed packages | **Package Installer**

```

OpenVPN Client Export Utility installation completed.

Beginning package installation for OpenVPN Client Export Utility...
Downloading package configuration file... done.
Saving updated package information... done.
Downloading OpenVPN Client Export Utility and its dependencies...
Checking for package installation...
  Downloading http://files.pfsense.org/packages/amd64/8/All/zip-3.0.tbz ...
(extracting)
Loading package configuration... done.
Configuring package components...
Additional files... done.
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Custom commands...
Executing custom_php_install_command()...done.
Integrated Tab items... done.
Writing configuration... done.

Installation completed.  Please check to make sure that the package is configured
from the respective menu then start the package.
  
```

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 :

Descriptive 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**

System: Certificate Authority Manager

CAs
Certificates
Certificate Revocation

Descriptive name

Method

Internal Certificate Authority

Key length bits

Digest Algorithm
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime days

Distinguished name

Country Code :	<input style="width: 50px;" type="text" value="CH"/>	
State or Province :	<input style="width: 150px;" type="text" value="Geneva"/>	<small>ex: Texas</small>
City :	<input style="width: 150px;" type="text" value="Geneva"/>	<small>ex: Austin</small>
Organization :	<input style="width: 150px;" type="text" value="Geneva"/>	<small>ex: My Company Inc.</small>
Email Address :	<input style="width: 150px;" type="text" value="tarek@watfa.ch"/>	<small>ex: admin@mycompany.com</small>
Common Name :	<input style="width: 150px;" type="text" value="VPNCA"/>	<small>ex: internal-ca</small>

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

System: User Manager



Users Groups Settings Servers

Defined by **USER**

Disabled

Username

Password
 (confirmation)

Full name
 User's full name, for your own information only

Expiration date
 Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy

Group Memberships

Not Member Of		Member Of
admins	 	

Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Certificate Click to create a user certificate.

Authorized keys Click to paste an authorized key.

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

Certificate	Descriptive name	<input type="text" value="VPNTarekCert"/>
	Certificate authority	<input type="text" value="VPN Server CA"/>
	Key length	<input type="text" value="2048"/> bits
	Lifetime	<input type="text" value="3650"/> days
Authorized keys	<input type="checkbox"/> Click to paste an authorized key.	
IPsec Pre-Shared Key	<input type="text"/>	
<input type="button" value="Save"/>		

Certificate	Descriptive name	VPNTarekCert
	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.



OpenVPN Remote Access Server Setup Wizard

Select an Authentication Backend Type

Type of Server:

NOTE: If you are unsure, leave this set to "Local User Access."

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 Authentication : **Enable authentication 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)**

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information	
Interface:	WAN <input type="button" value="v"/> The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol:	UDP <input type="button" value="v"/> Protocol to use for OpenVPN connections. If you are unsure, leave this set to UDP.
Local Port:	<input type="text" value="1194"/> Local port upon which OpenVPN will listen for connections. The default port is 1194. Leave this blank unless you need to use a different port.
Description:	<input type="text" value="WanOpenVPN Udp port"/> A name for this OpenVPN instance, for your reference. It can be set however you like, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff").
Cryptographic Settings	
TLS Authentication:	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Generate TLS Key:	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key:	<input type="text"/> Paste in a shared TLS key if one has already been generated.
DH Parameters Length:	1024 bit <input type="button" value="v"/> Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. As with other such settings, the larger values are more secure, but may be slower in operation.
Encryption Algorithm:	AES-128-CBC (128-bit) <input type="button" value="v"/> The method used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however you like. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.

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.**

Hardware Crypto:	<input type="text" value="No Hardware Crypto Acceleration"/> The hardware cryptographic accelerator to use for this VPN connection, if any.
Tunnel Settings	
Tunnel Network:	<input type="text" value="192.168.2.0/24"/> This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway:	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network:	<input type="text" value="192.168.1.0/24"/> This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Concurrent Connections:	<input type="text" value="10"/> Specify the maximum number of clients allowed to concurrently connect to this server.
Compression:	<input checked="" type="checkbox"/> Compress tunnel packets using the LZO algorithm.
Type-of-Service:	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-Client Communication:	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections:	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

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).**

Client Settings	
Dynamic IP:	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Address Pool:	<input checked="" type="checkbox"/> Provide a virtual adapter IP address to clients (see Tunnel Network).
DNS Default Domain:	<input type="text"/> Provide a default domain name to clients.
DNS Server 1:	<input type="text"/> DNS server to provide for connecting client systems.
DNS Server 2:	<input type="text"/> DNS server to provide for connecting client systems.
DNS Server 3:	<input type="text"/> DNS server to provide for connecting client systems.
DNS Server 4:	<input type="text"/> DNS server to provide for connecting client systems.
NTP Server:	<input type="text"/> Network Time Protocol server to provide for connecting client systems.
NTP Server 2:	<input type="text"/> Network Time Protocol server to provide for connecting client systems.
NetBIOS Options:	<input type="checkbox"/> Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

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

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall Rules control what network traffic is permitted. You must add rules to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule: Add a rule to permit traffic from clients on the Internet to the OpenVPN server process.

Traffic from clients through VPN

OpenVPN rule: Add a rule to allow all traffic from connected clients to pass across the VPN tunnel.

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

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

Your configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

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';

Advanced configuration

Advanced

```
push "route 192.168.1.0 255.255.255.0";
```

Enter any additional options you would like to add to the OpenVPN server configuration here, separated by a semicolon
EXAMPLE: push "route 10.0.0.0 255.255.255.0";

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

Client Install Packages		
User	Certificate Name	Export
Tarek	VPNTarekCert	<ul style="list-style-type: none"> - Standard Configurations: Archive Config Only - Inline Configurations: Android OpenVPN Connect (iOS/Android) Others - Windows Installers: 2.2 2.3-x86 - Mac OSX: Viscosity Bundle

NOTE: If you expect to see a certain client in the list but it is not there, it is usually due to a CA mismatch between the OpenVPN server instance and the client certificates found in the User Manager.

Links to OpenVPN clients for various platforms:

- [OpenVPN Community Client](#) - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers
- [OpenVPN For Android](#) - Recommended client for Android
- [FEAT VPN For Android](#) - For older versions of Android
- [OpenVPN Connect: Android \(Google Play\) or iOS \(App Store\)](#) - Recommended client for iOS
- [Viscosity](#) - Recommended client for Mac OSX
- [Tunnelblick](#) - Free client for OSX

On télécharge le client qui correspond à notre Système.

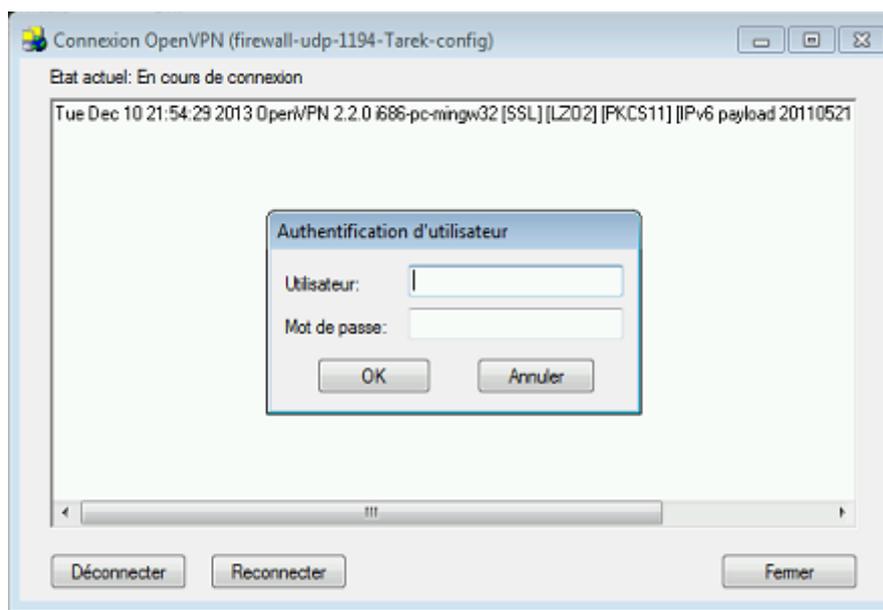
Test de connexion

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 :



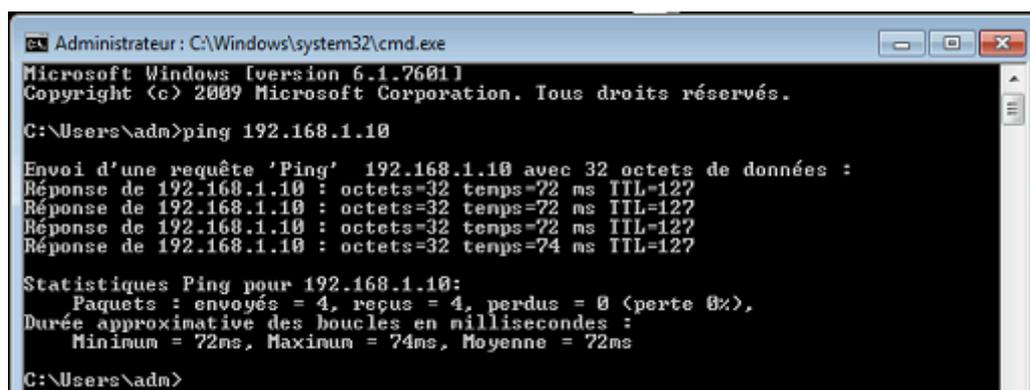
La connexion est établie.



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 :



```
Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\adm>ping 192.168.1.10

Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps=72 ms TTL=127
Réponse de 192.168.1.10 : octets=32 temps=72 ms TTL=127
Réponse de 192.168.1.10 : octets=32 temps=72 ms TTL=127
Réponse de 192.168.1.10 : octets=32 temps=74 ms TTL=127

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 72ms, Maximum = 74ms, Moyenne = 72ms

C:\Users\adm>
```

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