> Introduction :

Tout au long de ce tutoriel nous allons voir comment installer un serveur VPN avec OpenVPN sous Debian Squeeze commençons tout d'abord à les définir et voir leurs fonctions.

Debian : est une distribution libre du système d'exploitation libre Linux, développée par plusieurs milliers de volontaires dans le monde entier, qui collaborent via Internet. **Debian Squeeze étant la version 6.**

<u>VPN</u>: Un VPN (de l'anglais Virtual Private Network) est un Réseau Privé Virtuel. Il permet, lorsque vous êtes sur un site distant (à votre domicile par exemple), d'avoir accès au réseau local de votre entreprise à travers une connexion internet sécurisée. Ainsi, vous avez accès aux ressources de votre réseau local (fichiers partagés, intranet, extranet...) comme si vous étiez sur votre lieu de travail.

OpenVPN : est un logiciel libre permettant de créer facilement une liaison VPN site à site. OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance ou de certificats. Il fonctionne sur un mode client/serveur, ce qui implique son installation sur les 2 sites distants, l'un côté client, l'autre côté serveur.

Nous allons donc travailler sur l'environnement Debian Squeeze, nous allons suivre toutes les étapes de l'installation de cette distribution, puis l'installation d'OpenVPN ainsi que la création des certificats, pour en finir avec la configuration du serveur et la configuration de clients.

> <u>Sommaire :</u>

I) Installation de Debian Squeeze

II) Installation d'OpenVPN et Création de certificats

III) Configuration du Serveur

IV) Configuration des Clients

I) Installation de Debian Squeeze

Dans cette partie nous utiliserons Workstation, un outil de virtualisation de système d'exploitation, pour installer Debian sur une machine virtuel.

Dans le menu « File » on sélectionne « New Virtual Machine » pour créer une machine virtuel



On sélectionne Typical et on passe à l'étape suivante.



Ont choisir l'option de l'iso, où est contenue Debian 6 et on passe à l'étape suivante.



Dans cette étape ont choisis seulement le nom de la machine virtuel.

lew Virtual Machine Wizard	×
Name the Virtual Machine What name would you like to use for this virtual machine?	
Virtual machine name:	10 m
ServeurVPN	
Location:	
C: \Users \NGUYEN \Documents \Virtual Machines \Serveur VPN	Browse
< Back Next >	Cancel

On laisse par défaut et on passe à l'étape suivante.



Puis on termine en cliquant sur « Finish »



C'est vraiment à partir de ce moment, qu'on va commencer à installer Debian. On démarre la machine virtuelle et on sélectionne « Install ».



On choisit la langue désiré.

Nagios-Centreon - VMware Workstation		
<u>File Edit View VM Tabs H</u> elp		
🖩 + 🕹 🏷 🛇 🗳 🖬 🚍 🖼		
🔓 Home 🗙 🙀 Nagios-Centreon 🗙		
	[11] Select a language Choose the language to be used for the installation process. The selected language will also be the default language for the installed system. Language: C - No localization Albanian - Shqip Arabic - マラン Asturian - Asturianu Basque - Euskara Belarusian - Ebarapcrua Bosnian - Bosanski Bulgerian - Català Chinese (Simplified) - 中文(商作) Chinese (Irmditined) - 中文(商作) Chinese (Traditional) - 中文(商作) Chinese (Traditional) - 中文(商作) Chinese (Traditional) - 中文(商作) Chinese (Traditional) - Estina Dutch - Nederlands English - English Esperanto - Esperanto Estonian - Galego German - Deutsch Greek - EXAnyıků +	E
	<go back=""> NGUY</go>	'EN
	Eródó	rie
<	Tab> moves: <space> selects: <enter> activates buttons</enter></space>	
To direct input to this VM, click inside or press Ctrl+G.	이 같은 것 같은	6 🔯 🖻

On choisit notre situation géographique.



En passant à l'étape suivant, on rencontre un problème de réseau.



Rien de très inquiétant on a seulement à branché notre carte réseau en « Bridged » Pour cela « on clique-droit » et on sélectionne « Settings …»



Puis on sélectionne en « Bridged » et là on aura plus de problème de connexion réseau .



Pour le nom de la machine on met « ServeurVPN ».



Pour le domaine on met « lprs.local »

🗐 Nagios-Centreon - VMware Workstation	
Eile Edit <u>View VM</u> Iabs <u>H</u> elp	
Home X B Nagios-Centreon X	
	·
[1] Configurer 1e réseau	
Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il	
se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvers mattre ce que vous vous explanations d'aventueurs la pôme propre réseau.	
les machines.	
Domaine :	E
<pre></pre>	
	NGUYEN
(Tah) dénlacement: (Esnace) sélection: (Entrée) activation des houtons	Frederic
To direct input to this VM, click inside or press Ctrl+G.	

On va définir un mot de passe pour le compte super-utilisateur, donc le compte « root », ainsi son mot de passe sera « admin »



Puis on reconfirme le mot de passe saisi précédemment



On créer maintenant un nouveau compte, dans ce cas le nom du compte sera « nguyen » et le mot de passe « frederic ».

On saisit donc le nom du compte « nguyen ».

Sagios-Centreon - VMware Workstation	
Eile Edit View VM Iabs Help	
Home × i i Ragios-Centreon ×	
	Â
[1] Créer les utilisateurs et choisir les mots de passe	
veuinez choisir un identifiants doivent commencer par une lettre minuscule, suivie d'un	
nombre quelconque de chiffres et de lettres minuscules.	
Identifiant pour le compte utilisateur :	E
Inguyen	
(Revenin en annière)	
	NGUYEN
	Frédéric
Control input to this VM, click inside or press CH+G.	

To direct input to this VM, click inside or press Ctrl+G.

On définit le mot de passe « frederic ».



On re-tape le mot de passe « frederic »

Nagios-Centreon - VMware Workstation	
Eile Edit View VM Iabs Help	
H ▼ ≟ も c) c) i = = = i = i = i	
C Home × G Nagios-Centreon ×	
[!!] Créer les utilisateurs et choisir les mots de passe Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte. Confirmation du mot de passe : ververe ∢Revenir en arrière> Continuers	E
	NGUTEN
	Erádária
<tab> déplacement: <espace> sélection: <entrée> activation des boutons</entrée></espace></tab>	Frederic .
To direct input to this VM, click inside or press Ctrl+G.	

To direct input to this VM, click inside or press Ctrl+G.

On sélectionne « Assisté – utiliser un disque entier ».



On choisit le disque à partitionner.



On choisit tout dans une seule partition.



On sélectionne « Terminer le partitionnement et appliquer les changements ».



On sélectionne « Oui ».



On sélectionne « Non ».



On sélectionne « Oui » pour pouvoir utiliser le miroir du réseau



On choisit « France ».



On choisit le premier miroir.



On laisse vide et on passe à l'étape suivante en sélectionnant « Continuer »

On sélectionne « Non ».

Ont sélectionne les logiciels à installer et on passe à l'étape suivant en sélectionnant « Continuer »

On met pour le nom de domaine « lprs.local »

On installe le programme de démarrage GRUB sur le secteur d'amorçage en sélectionnant « Oui ».

On termine l'installation en sélectionnant « Continuer »

L'installation de Debian 6 est maintenant terminer.

II) Installation d'OpenVPN et Création de certificats

Dans cette partie nous allons d'abord commencé par installer OpenVPN puis créer les certificats.

A) Installation d'OpenVPN :

On démarre notre machine virtuelle et on se connecte en « root » avec le mot de passe « admin »

Starting kerneloops: Starting mpt-status monitor: mpt-statusd. Starting internet superserver: inetd. Starting PostgreSQL 8.4 database server: mainsaned disabled; edit /etc/default/s aned SpamAssassin Mail Filter Daemon: disabled, see /etc/default/spamassassin Starting Samba daemons: nmbd smbd. Starting OpenBSD Secure Shell server: sshd. Starting the Winbind daemon: winbind. Starting MTA: exim4. Debian GNU/Linux 6.0 ServeurVPN tty1 ServeurVPN login: root Password: Linux ServeurVPN 2.6.32-5-amd64 #1 SMP Mon Sep 23 22:14:43 UTC 2013 x86_64 The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright. Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. root@ServeurVPN:~# _

On va installer OpenVPN avec cette commande :

> apt-get install openvpn

Ce qui nous donne :

7 974 ko réceptionnés en 32s (248 ko/s) Préconfiguration des paquets... Sélection du paquet openss1-blacklist précédemment désélectionné. (Lecture de la base de données... 129039 fichiers et répertoires déjà installés.) Dépaquetage de openss1-blacklist (à partir de .../openss1-blacklist_0.5-2_all.de b... Sélection du paquet liblzo2-2 précédemment désélectionné. Dépaquetage de liblzo2-2 (à partir de .../liblzo2-2_2.03-2_amd64.deb) ... Sélection du paquet liblexs11-helper1 précédemment désélectionné. Dépaquetage de liblzo2-2 (à partir de .../liblkcs11-helper1_1.07-1_amd64 ... Sélection du paquet openvpn-blacklist précédemment désélectionné. Dépaquetage de openvpn-blacklist précédemment désélectionné. Dépaquetage de openvpn-blacklist précédemment désélectionné. Dépaquetage de openvpn précédemment désélectionné. Dépaquetage de openvpn précédemment désélectionné. Dépaquetage de openvpn liacklist (à partir de .../openvpn-blacklist_0.4_all.deb) ... Faitement des actions différées (« triggers ») pour « man-db »... Paramétrage de liblzo2-2 (2.03-2) ... Paramétrage de liblzo2-2 (2.03-2) ... Paramétrage de liblzo2-2 (2.03-2) ... Paramétrage de openvpn-blacklist (0.4) ...

Installation d'OpenSSL pour la sécurisation des données :

Généralement, OpenSSL est installé par défaut sur les machines et ne nécessite donc pas d'être réinstallé.

> apt-get install openssl

Ce qui nous donne :

```
root@ServeurVPN:~# apt-get install openssl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
openssl est déjà la plus récente version disponible.
openssl passé en « installé manuellement ».
O mis à jour, O nouvellement installés, O à enlever et O non mis à jour.
root@ServeurVPN:~# _
```

Donc, dans notre cas OpennSSL était déjà installer.

B) Génération des certificats :

L'installation d'OpenVPN crée un dossier dans **/usr/share/doc/openvpn/easy-rsa/** contenant tous les scripts permettant de générer facilement tous les certificats et clés d'authentification nécessaire au fonctionnement d'OpenVPN.

Ces certificats permettront de procéder a l'échange d'une clé de session et permettront de vérifier l'identité des parties.Ils nécessitent bien sûr d'utiliser une autorité de certification(AC), qui sera créée par nos soins.

La connexion entre le serveur et un client du VPN se passe de la façon suivante : -Chaque entité du VPN (Serveur Inclus) doit disposer d'un certificat valide.

- A la connexion , le client vérifie le certificat du serveur grâce au certificat de l'AC.

-Le client soumet son certificat et si celui-ci est vérifié grace au certificat de l'AC et qu'il ne se trouve pas sur la liste de révocation, la connexion est mise en place.

Le paquet « easy-rsa » installé précédemment va faciliter la création des certificats requis ; il contient en effet un ensemble de scripts permettant de gérer ces certificats.

NGUYEN Frédéric BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

C) Le fichier de variables :

Avant toute chose, créez un dossier easy-rsa dans le répertoire d'OpenVPN et copier les scripts originaux dedans afin de centraliser applications et scripts :

> mkdir /etc/openvpn/easy-rsa/

> cp /usr/share/doc/openvpn/examples/easy-rsa/2.0/*
/etc/openvpn/easy-rsa/

On crée ensuite un dossier keys destiné à contenir les différents certificats et clés générés :

> mkdir /etc/openvpn/easy-rsa/keys/

A partir du dossier **/etc/openvpn/easy-rsa/**, il faut dans un premier temps éditer le fichier « vars » afin d'initialiser différentes variables servant à la génération des certificats :

Comme vous le verrez ci-après , renseigner ces différents champs facilitera la création des clés dans la suite des opérations.

Deux méthodes s'offre à nous pour configurer le fichier « vars »

- Première méthode :

> nano /etc/openvpn/easy-rsa/vars

On entre les informations personnelles comme suit :

Export KEY DIR=\$D/keys

```
Export KEY_COUNTRY=''FR''
Export KEY_PROVINCE=''FR''
Export KEY_CITY=''Dugny''
Export KEY_ORG=''serveurvpn'
Export KEY_EMAIL=''frederic_95140@hotmail.fr''
```

```
Ce qui nous donne :
```

GNU nano 2.2.4

Fichier : vars

Modifié

xport CA_EXPIRE=3650

In how many days should certificates expire? export KEY_EXPIRE=3650 # These are the default values for fields # which will be placed in the certificate. # Don't leave any of these fields blank. export KEY_COUNTRY="FR" export KEY_COUNTRY="FR" export KEY_CITY="Dugny" export KEY_ORG="serveurvpn" export KEY_EMAIL="frederic_95140@hotmail.fr<u>"</u>

- Deuxième méthode :

On télécharge et installe WinSCP.

WinSCP est un client SFTP graphique pour Windows. Il utilise SSH et est open source. Le protocole SCP est également supporté. Le but de ce programme est de permettre la copie sécurisée de fichiers entre un ordinateur local et un ordinateur distant.

On fait ifconfig pour voir notre adresse IP, dans notre cas notre adresse ip est : « 192.168.115.132 »

root@Ser	rveurVPN:~# ifconfig
eth0	Link encap:Ethernet HWaddr 00:0c:29:34:ad:37 inet adr:192.168.115.132 Bcast:192.168.115.255 Masque:255.255.255.0 adr inet6: fe80::20c:29ff:fe34:ad37/64 Scope:Lien UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:6602 errors:0 dropped:0 overruns:0 frame:0 TX packets:3046 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 lg file transmission:1000 RX bytes:8334941 (7.9 MiB) TX bytes:174271 (170.1 KiB)
10	Link encap:Boucle locale inet adr:127.0.0.1 Masque:255.0.0.0 adr inet6: ::1/128 Scope:Hôte UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:165 errors:0 dropped:0 overruns:0 frame:0 TX packets:165 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 lg file transmission:0 RX bytes:26317 (25.7 KiB) TX bytes:26317 (25.7 KiB)

Puis on remplit les différents champs comme dans l'image :

- Protocole de fichier : « SFTP »
- Nom d'hôte : « 192.168.115.132 »
- Nom d'utilisateur : « root »
- Numéro de port : « 22 »
- Mot de passe : « admin »

Nouveau Site	Session	
	Protocole de <u>fi</u> chier	
	SFTP 👻	
	Nom d'hôte	Numéro de port
	192.168.115.132	22 🛓
	Nom d'utilisateur Mo	t de passe
	root	••••
	Sauver 📘	Avancé

Une fenêtre apparaît, on met « Oui »

On transfère depuis la machine, le fichier « vars » qui se situe dans le répertoire « /etc/openvpn/easy-rsa/» vers notre ordinateur avec WinSCP.

素 easy-rsa - root@192.1	68.115.131 - WinSCP						l	– 🗆 X
Local Marquer Fichier	rs Commandes Session	Options	Distant Aide					
🖶 🔁 違 Synchronise	er 🗾 🧬 💽 🍥	😨 🍙 File	 Réglages de transfert D 	éfaut 🔹 🥑 🗸				
aroot@192.168.115.13	1 Nouvelle session							
. C: Disque local	• 🚝 🔽 🥧 • =>	-	A 2 .	🔒 easv-rsa 🔹 🚅	🔽 👍 🗸	• • I 🖻 🖻 🏠 🍠	Rechercher	des fichiers
Envoyer in E	aiter 🗙 📷 Lig Propriet				Editer 💢 📰			
C:\Users\NGUYEN\VPN				/etc/openvpn/easy-rsa				
Nom Ext	Taille Type		Date de modification	Nom Ext	Taille	Date de modification	Droits	Proprié
<u>.</u>	Répertoi	re parent	27/02/2014 19:59:33	- 🄐		27/02/2014 19:30:13	rwxr-xr-x	root
				hevs.	9	27/02/2014 19:36:43	rwxr-xr-x	root
		Télécharge	er	and the second s	R	2014 19:34:02	rwxr-xr-x	root
		Te Te	élécharger fichier 'vars' vers Répert	toire local :		2014 19:34:02	rwxr-xr-x	root
			: Users WGUYEN \VPN *. *		- Explore	2014 19:34:02	rwxr-xr-x	root
		Dádaas	e de fanacture			2014 19:34:02	rwxr-xr-x	root
	8.	Type de	transfer : Binaire			2014 19:34:02	rwxr-xr-x	root
						2014 19:34:02	rwxr-xr-x	root
	\mathbf{X}					2014 19:34:02	rwxr-xr-x	root
		Trans	fert en arrière plan (ajout à la que	ue de transfert)		2014 19:34:02	rwxr-xr-x	root
		Pa	aramètres	OK Annuler	Aide	2014 19:34:02	rwxr-xr-x	root
		TR No. of	a affecture an distance			2014 19:34:02	rwxr-xr-x	root
		Ne più	is afficher ce dialogue			2014 19:34:02	rwxr-xr-x	root
					201 0	27,02/2014 19:34:02	rwxr-xr-x	root
					389 B	27/02/2014 19:34:02	rw-rr	root
				openssi.cnf	8 328 B	27/02/2014 19:34:02	rw-rr	root
				openssi-0.9.0.cnf.gz	2 9/0 B	27/02/2014 19:34:02	rw-rr	root
				D PKILOOI	12 504 B	27/02/2014 19:34:02	rwxr-xr-x	root
					3 /45 B	27/02/2014 19:34:02	rw-rr	root
				revoke-tuli	920 B	27/02/2014 19:34:02	rwxr-xr-x	root
				sign-req	180 B	27/02/2014 19:34:02	rwxr-xr-x	root
				Vars	10/88	27/02/2014 19:34:02	rw-rr	root
				whichopenssicnf	190 B	27/02/2014 19:34:02	rwxr-xr-x	root
0 B de 0 B dans 0 de 0				1 678 B de 34 981 B dans 1 d	de 22		SCD	0.01.26
							SCP	0:01:20

Depuis notre ordinateur, on ouvre bloc note le fichier « vars », on modifie ces champs et on enregistre :

```
Export KEY_DIR=$D/keys
Export KEY_COUNTRY=''FR''
Export KEY_PROVINCE=''FR''
Export KEY_CITY=''Dugny''
Export KEY_ORG=''serveurvpn'
Export KEY_EMAIL=''frederic_95140@hotmail.fr''
```

Ce qui nous donne :

Puis on transfère depuis WinSCP dans « /etc/openvpn/easy-rsa/ » et on met « Oui » pour l'écraser

🚰 📑 Synchronise	r 🗾 💞 💽 🛞 🔢 🗃 File	Keglages de transfert D					
root@192.168.115.13	Nouvelle session						
C: Disgue local	- 🚝 🔽 🗢 - 🔿 - 🛛 🖾 🖾		🔋 easv-rsa 🔹 🥰	🔽 🔶	+ · 🖻 🗖 🏠 🎜	Rechercher	des fichier
			I c Télécharger c D	Editor W			
			(etc/openium/cape.rsa				
	T.00. T	Data Inc. Provide	N C	T . 10	Data la contra di	D. it	D
1 EXT	Talle Type	Date de modification	NOM EXt	Talle	Date de modification	Droits	Proprie.
	Képertoire parent	27/02/2014 20:00:38	See		27/02/2014 19:30:13	rwxr-xr-x	root
irs i	1 00 D Fichier		10		21/02/2014 19:30:43	Z N N N N N N N N N N N N N N N N N N N	root
	Confirmer			_		WXr-Xr-X	root
X III						WAI-AI-A	1000
		11				BOYE-YE-Y	root
	Ecraser le fichier	distant 'vars' ?				WXF-XF-X	root
\backslash	Ecraser le fichier	distant 'vars' ? ation contient déià un fichier no	mmé 'vars'. Choisissez si vous souh	aitez écraser l	e fichier ou annuler ce	•xr-xr-x •xr-xr-x	root
	Ecraser le fichier Le répertoire de destin transfert et conserver l	distant 'vars' ? ation contient déjà un fichier no e fichier existant.	mmé 'vars'. Choisissez si vous souh	aitez écraser l	e fichier ou annuler ce	NXT-XT-X NXT-XT-X NXT-XT-X	root root root root
\backslash	Ecraser le fichier Le répertoire de destin transfert et conserver l	distant 'vars' ? ation contient déjà un fichier no le fichier existant.	mmé 'vars'. Choisissez si vous souh	aitez écraser l	e fichier ou annuler ce	VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X	root root root root
	Ecraser le fichier Le répertoire de destin transfert et conserver l Nouveau : 1 656 octet Existant : 1 678 octet	distant 'vars' ? ation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02	mmé 'vars'. Choisissez si vous souh	aitez écraser l	e fichier ou annuler ce	NXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X NXT-XT-X	root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver l Nouveau : 1 656 octet Existant : 1 678 octe	distant 'vars' ? ation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02	mmé 'vars'. Choisissez si vous souh	aitez écraser l	e fichier ou annuler ce	NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X	root root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver Nouveau : 1656 octe Existant : 1678 octe	distant 'vars' ? ation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02	mmé 'vars'. Choisissez si vous souh	aitez écraser l	e fichier ou annuler ce Aide	NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X NXT-XT-X	root root root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver 1 Nouveau : 1 656 octe Existant : 1 678 octe	distant 'vars' ? Hation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Out	mmé 'vars'. Choisissez si vous souh Non 💌 Ann	aitez écraser l uler	e fichier ou annuler ce Aide	VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X	root root root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver l Nouveau : 1656 octel Existant : 1678 octe Ne plus me demander	distant 'vars' ? ation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Oui	mmé 'vars'. Choisissez si vous souh Non 💌 Ann	aitez écraser l nuler	e fichier ou annuler ce Aide 21702/2014 19:34:02	VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X VXT-XT-X	root root root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver Nouveau : 1656 octe Existant : 1678 octe	distant 'vars' ? tation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Oui	mmé 'vars'. Choisissez si vous souh Non 💌 Ann	uler 389 B	e fichier ou annuler ce Aide 27/02/2014 19:34:02 27/02/2014 19:34:02	VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X TVXT-XF-X TVXT-XF-X	root root root root root root root root
	 Ecraser le fichier. Le répertoire de destin transfert et conserver l Nouveau : 1 656 octet Existant : 1 678 octet Ne plus me demander 	distant 'vars' ? Iation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02	mmé 'vars'. Choisissez si vous souh	uler 389 B 8 328 B 8 328 B	e fichier ou annuler ce Aide 27/02/2014 19:334:02 27/02/2014 19:34:02	VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X VXT-XF-X	root root root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver l Nouveau : 1656 octet Existant : 1678 octe Ne plus me demander	distant 'vars' ? ation contient déjà un fichier no le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Oui	Mon Vars'. Choisissez si vous souh	uler 389 B 8 328 B 2 976 B	e fichier ou annuler ce <u>Aide</u> 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02	007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X 007-X1-X	root root root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver Nouveau : 1656 octe Existant : 1678 octe	distant 'vars' ? tation contient déjà un fichier nc le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Oui	Mon Ann Makefile Openssl.cof. Deprissl.of	aitez écraser l uuler 389 B 8 328 B 2 976 B 12 504 B 2 504 B	e fichier ou annuler ce Aide 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02	007-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X	root root root root root root root root
	 Ecraser le fichier Le répertoire de destin transfert et conserver l Nouveau : 1 656 octet Existant : 1 678 octet Ne plus me demander 	distant 'vars' ? ation contient déjà un fichier nc le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Oui	Mon Ann Non Ann Makefile openssl.onf openssl.onf openssl.onf. penssl.onf. openssl.onf. penssl.onf. openssl.onf. penssl.onf. openssl.onf	aitez écraser l nuler 389 B 8 328 B 2 976 B 12 504 B 3 745 B 3 745 C	e fichier ou annuler ce Aide 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02	007-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 0X7-X1-X 1X7-X	root root root root root root root root
	Craser le fichier Le répertoire de destin transfert et consever l Nouveau : 1656 octel Existant : 1678 octe Ne plus me demander	distant 'vars' ? ation contient déjà un fichier ne le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Out	Mon Vars'. Choisissez si vous souh	aitez écraser l nuler 389 B 8 328 B 2 976 B 12 504 B 3 745 B 920 B 129 0 P	e fichier ou annuler ce <u>Aide</u> 27/02/2014 19:3-9:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02	007-X1-X 007-X1	root root root root root root root root
	Craser le fichier Le répertoire de destin transfert et conserver Nouveau : 1656 octe Existant : 1678 octe	distant 'vars' ? ation contient déjà un fichier ne le fichier existant. ts, 27/02/2014 20:03:27 ts, 27/02/2014 19:34:02 Oui	Non Ann Makefile openssl-of pkitool README.gz www.full	uler 8898 8328 2976 12504 83745 8920 8920 8020 8020 8020 8020 8020 8020	e fichier ou annuler ce Aide 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02 27/02/2014 19:34:02	007-X1-X 007-X1	root root root root root root root root

On exécute enfin le script afin d'initialiser les variables :

> . ./vars

Ceci fait , on met à jour le fichier via la commande :

> source ./vars

Puis on exécute la commande :

> ./clean-all

NGUYEN Frédéric BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

D) L'autorité de certification :

On crée un certificat d'autorité de certification (fichiers « ca.crt » et « ca.key ») avec la commande :

> ./build-ca

il faut faire [Entrée] à toutes les questions.

```
Ce qui nous donne :
root@ServeurVPN:/etc/openvpn/easy–rsa# ./build–ca
Generating a 1024 bit RSA private key
writing new private key to 'ca.key'
____
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [FR]:
State or Province Name (full name) [FR]:
Locality Name (eg, city) [Dugny]:
Organization Name (eg, company) [serveurvpn]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [serveurvpn CA]:
Name []:
Email Address [frederic_95140@hotmail.fr]:
root@ServeurVPN:/etc/openvpn/easy–rsa#
root@ServeurVPN:/etc/openvpn/easy-rsa#
```

Tous les certificats et les clés créés sont stockés automatiquement dans le répertoire keys/. Les fichier .key ne doivent pas être accessibles en lecture/écriture que par leur propriétaire respectif.

E) L'autorité du serveur :

La génération du certificat et de la clé du serveur VPN se fait simplement, par l'exécution du script buildkey-server, toujours à partir du dossier **/etc/openvpn/easy-rsa** :

Différentes informations sont demandées pendant l'exécution de ce script :

« Commun-name » : Entrez le nom du serveur que vous avez pour lancer le script, pour notre cas c'est « ServerVPN »

« Sign the certificate ? » : tapez "yes"

« 1 out of 1 certificate requests certificated, commit » : tapez "yes"

Ce script conduit à la création des fichiers nom_choisi_du_serveur.crt et nom_choisi_du_serveur.key dans le dossier /etc/openvpn/easy-rsa/keys.

> ./build-key-server nom_choisi_du_serveur

Dans notre cas ça sera :

> ./build-key-server serveurvpn

```
Ce qui donne :
Name []:
Email Address [frederic_95140@hotmail.fr]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName
                        :PRINTABLE: 'FR'
                        :PRINTABLE: 'FR'
stateOrProvinceName
                        :PRINTABLE: 'Dugny'
localityName
                        :PRINTABLE: 'serveurvpn'
organizationName
                        :PRINTABLE: 'serveurvpn'
commonName
                        :IA5STRING:'frederic_95140@hotmail.fr'
emailAddress
Certificate is to be certified until Feb 25 20:36:18 2024 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

F) Le certificat du client :

On crée les certificats du(des) client(s) avec :

> ./build-key nom_du_client1

Dans notre cas, le nom du client est « client1 » ce qui donne :

> ./build-key nom_du_client1

Pour le paramètre « Commun-name », saisissez le même nom que nom_du_client1 que vous avez utilisé dans la commande.

Répétez cette opération autant de fois que vous voulez pour générer plusieurs certificats et clés si vous avez plusieurs clients. N'oubliez pas cependant de changer de nom_du_client à chaque fois .

Ce script entraine la création des fichiers nom_du_client1.crt et nom_du_client1.key dans le dossier /etc/opnevpn/easy-rsa/keys.

Ce qui donne :

```
Name []:
Email Address [frederic_95140@hotmail.fr]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
                        :PRINTABLE: 'FR
countryName
                        :PRINTABLE: 'FR'
stateOrProvinceName
                        :PRINTABLE: 'Dugny'
localityName
                        :PRINTABLE: Dugny
:PRINTABLE: 'serveurvpn'
:PRINTABLE: 'client1'
:IA5STRING: 'frederic_95140@hotmail.fr'
organizationName
commonName
emailAddress
Certificate is to be certified until Feb 25 20:45:19 2024 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

III) Configuration du Serveur

Dans cette partie nous allons configurer le serveur.

Dans notre contexte le serveur VPN doit avoir comme adresse : « 192.168.3.254 »

Donc on va changer notre ip en fessant :

> nano /etc/network/interfaces

Et on mettra dans interfaces :

```
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see
interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback
#NetworkManager
auto eth0
iface eth0 inet dhcp
address 192.168.3.251
network 192.168.3.0
netmask 255.255.255.0
broadcast 192.168.0.255
gateway 192.168.0.254
```

Puis on fait un « reboot »

Le script de démarrage d'OpenVPN recherche les fichiers .conf se trouvant dans « /etc/openvpn/ ».

Nous allons donc créer un fichier de configuration dans ce répertoire :

> nano /etc/openvpn/server.conf

Et on mettera dans server.conf :

Elements de base

port 1194 proto udp dev tun comp-lzo persist-key persist-tun keepalive 10 120 server 24.0.0.0 255.25<u>5.255.0</u> Parametres ssl ca easy-rsa/keys/ca.crt cert easy-rsa/keys/servervpn.crt key easy-rsa/keys/servervpn.key dh easy-rsa/keys/dh1024.pem Logs status openvpn-status.log verb 3

port = port d'écoute d'OpenVPN (ici 1194), proto = Protocol utilisé (ici udp), dev tun = Tunnel IP, complzo = active la compression des paquets, persist-key et persist-tun = rendent l'acces au cles et au périphérique tun persistant au redémarrage, keepalive = garder la connexion active meme si rien ne se passe, server = adresse du serveur dans le VPN, push "route"= serveur joignable via la connexion VPN, push "redirect-gateway" = pour que le trafic passe entierement par le VPN, status = enregistre l'état courant du serveur (ici dans openvpn-status.log), verb = niveau de verbosité des logs.

Voila, la configuration du côté serveur est terminée.

Pour démarrer le serveur, la commande est :

> /etc/init.d/openvpn start

IV) Configuration des Clients

Dans cette partie voir comment configurer un client Linux et un client Windows pour ce connecter au VPN.

A) Client Linux :

Le client Linux nécessite la même installation que le serveur :

> apt-get install openvpn

Pour garder une certaine cohérence entre le serveur et les clients, j'utilise la même hiérarchie de dossiers sur les clients que sur le serveur. Ainsi, on crée un dossier « config » et un dossier « /easy-rsa/keys dans /etc/openvpn »

> mkdir /etc/openvpn/config && mkdir /etc/openvpn/easy-rsa && mkdir /etc/openvpn/easy-rsa/keys

Pour fonctionner, les clients ont besoin de 4 fichiers provenant du serveur :

- 1. ca.crt
- 2. nom_du_client1.crt
- 3. nom_du_client1.key
- 4. le fichier de configuration client.conf

Bit Developing Control of the second sec	root@192.168.115.132	Nouvelle	a session		🔒 keys 🔻 🙋	V	 	Rechercher	des fichiers	ę
Nome Life Taille Type Date de modification Toits Proprié. evers.conf 1120 B Fichier 28/02/2014 1213.140 0.0.pem 3724 B 28/02/2014 06.35.61 nover-tre- root interfaces 373 B Fichier 28/02/2014 10.20.04 28/02/2014 10.20.04 28/02/2014 06.35.01 nover-tre- root interfaces 373 B Fichier 28/02/2014 10.20.04 28/02/2014 06.35.01 nover-tre- root interfaces 373 B Fichier 28/02/2014 06.35.01 nover-tre- root interfaces 373 B Fichier 28/02/2014 02.20.04 10.20.04 877 B 28/02/2014 06.35.00 nover-tre- root interfaces 373 B Fichier 28/02/2014 06.35.01 nover-tre- root root 10.49 B 28/02/2014 06.35.01 nover-tre- root interfaces 373 B Fichier 28/02/2014 06.35.01 nover-tre- root 10.49 B 28/02/2014 06.35.41 nover-tre- root interfaces 374 B 28/02/2014 06.35.41 nover-tre- root 10.48 B 10.48 B 20/02/2014 06.36.41 nover-tre- root indext.tatriol 118 B 28/02/2014 06.36.41 nover-tre- </th <th>Liners\NGUYEN\Desktop</th> <th>VPN</th> <th>2 Proprietes </th> <th></th> <th>/etc/openyon/easy-rsa/k</th> <th>Fediter 👗 📰</th> <th>5 L2 Proprietes 🔛 山</th> <th></th> <th></th> <th></th>	Liners\NGUYEN\Desktop	VPN	2 Proprietes		/etc/openyon/easy-rsa/k	Fediter 👗 📰	5 L2 Proprietes 🔛 山			
Aus La La <thla< th=""> La La La<</thla<>	lom Ext	Taille	Type	Date de modification	Nom Ext	Taille	Date de modification	Droits	Proprié	
	yvis Jerver.conf Jinterfaces	1677 8 1120 8 373 8	Répetitive parent Fichier Fichier CONF Fichier	28/02/2014 10:05:36 27/02/2014 21:31:40 28/02/2014 12:10:41 28/02/2014 10:20:04	de	3 9022 B 3 704 B 1 240 B 878 B 3 704 B 676 B 877 B 877 B 877 B 2245 B 2245 B 2245 B 2245 B 2245 B 2245 B 2245 B 224 B 3 8 3 9 2 28 3 8 3 9 2 28 6 8 7 7 B	28.02/2014 06:34:39 28.02/2014 06:35:04 28.02/2014 06:35:00 28.02/2014 06:35:00 28.02/2014 06:35:00 28.02/2014 06:35:00 28.02/2014 06:35:04 28.02/2014 06:37:43 28.02/2014 06:37:43 28.02/2014 06:37:43 28.02/2014 06:37:43 28.02/2014 06:35:13 28.02/2014 06:35:14 28.02/2014 06:35:24 28.02/2014 06:35:24 28.02/2014 06:35:24 28.02/2014 06:35:24 28.02/2014 06:35:24 28.02/2014 06:35:24 28.02/2014 06:35:24		root root root root root root root root	

Voici le contenu du fichier client.conf permettant de se connecter au serveur défini précédemment :

```
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.
# This configuration can be used by multiple
                                             #
# clients, however each client should have
# its own cert and key files.
                                             H
#
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client.
# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun
# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one. On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap
# Are we connecting to a TCP or
# UDP server? Use the same setting as
# on the server.
;proto tcp
proto udp
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.0.31 1194
;remote my-server-2 1194
# Choose a random host from the remote
 list for load-balancing. Otherwise
# try hosts in the order specified.
;remote-random
# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite
# Most clients don't need to bind to
# a specific local port number.
nobind
# Downgrade privileges after initialization (non-Windows only)
;user nobody
group nogroup;
# Try to preserve some state across restarts.
persist-kev
```

NGUYEN Frédéric BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

persist-tun

If you are connecting through an # HTTP proxy to reach the actual OpenVPN # server, put the proxy server/IP and # port number here. See the man page # if your proxy server requires # authentication. ;http-proxy-retry # retry on connection failures ;http-proxy [proxy server] [proxy port #] # Wireless networks often produce a lot # of dynamic product a lot

of duplicate packets. Set this flag
to silence duplicate packet warnings.
;mute-replay-warnings

SSL/TLS parms. # See the server config file for more # description. It's best to use # a separate .crt/.key file pair # for each client. A single ca # file can be used for all clients. ca easy-rsa/keys/ca.crt cert easy-rsa/keys/client1.crt key easy-rsa/keys/client1.key

Verify server certificate by checking # that the certicate has the nsCertType # field set to "server". This is an # important precaution to protect against # a potential attack discussed here: # http://openvpn.net/howto.html#mitm

To use this feature, you will need to generate # your server certificates with the nsCertType # field set to "server". The build-key-server # script in the easy-rsa folder will do this. ns-cert-type server

If a tls-auth key is used on the server # then every client must also have the key. ;tls-auth ta.key 1

Select a cryptographic cipher.
If the cipher option is used on the server
then you must also specify it here.
;cipher x

Enable compression on the VPN link.
Don't enable this unless it is also
enabled in the server config file.
comp-lzo

Set log file verbosity.
verb 3

Silence repeating messages
;mute 20

B) Client Windows :

Pour le client Windows, il est nécessaire d'installer une application spécifique, OpenVPN GUI for Windows, qui se trouve ici :

http://openvpn.se

Une fois téléchargée, lancer l'installation d'OpenVPN. Une fenêtre vous demandera si vous acceptez d'installer une nouvelle interface «TAP-Win32 Adapter V8». Acceptez.

Hardwa	re Installation
1	The software you are installing for this hardware: TAP-Win32 Adapter V8 has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.) Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
	Continue Anyway STOP Installation

L'installation finie, deux petits ordinateurs avec un globe font leur apparition dans la barre des tâches. Cela correspond à l'interface virtuelle nouvellement créée « TAP-Win32 Adapter V8 » permettant la connexion au VPN.

5

← Icône de l'interface TAP Win32 pour OpenVPN dans la barre des tâches de Windows.

Copiez les 4 fichiers suivants dans le dossier « C:\Program Files\OpenVPN\config » :

- 1. ca.crt
- 2. nom_du_client1.crt
- 3. nom_du_client1.key
- 4. client.conf

\rightarrow II faut renommer le fichier client.conf en client.ovpn

La configuration du fichier de configuration client.ovpn est la même que pour un client Linux, excepté pour les chemins de fichiers. Si les certificats et clés sont bien placés dans le dossier config, le contenu du fichier client.ovpn doit être :


```
# Try to preserve some state across restarts.
persist-key
persist-tun
# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here. See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
# Wireless networks often produce a lot
# of duplicate packets. Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings
# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/client1.crt
key easy-rsa/keys/client1.key
# Verify server certificate by checking
#
  that the certicate has the nsCertType
# field set to "server". This is an
# important precaution to protect against
# a potential attack discussed here:
  http://openvpn.net/howto.html#mitm
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server". The build-key-server
# script in the easy-rsa folder will do this.
#
ns-cert-type server
# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1
# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x
# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo
# Set log file verbosity.
verb 3
# Silence repeating messages
;mute 20
```

Ce qui donne :

🕒 💭 🗢 📕 🕨 Ordinateur	 Disque local (C:) Program 	mmes 🕨 OpenVPN 🕨 config			Rechercher dans : config	Q
Organiser 👻 Inclure da	ns la bibliothèque 🔻 🛛 Partag	er avec 🔻 Nouveau dossier			855 -	
🔆 Favoris	Nom	Modifié le	Туре	Taille		
📃 Bureau	🔄 ca	01/03/2014 00:52	Certificat de sécur	2 Ko		
📃 Emplacements récer	🕥 client	01/03/2014 00:52	OpenVPN Config	1 Ko		
\rm Téléchargements	📮 client1	01/03/2014 00:52	Certificat de sécur	4 Ko		
	client1.key	01/03/2014 00:52	Fichier KEY	1 Ko		
詞 Bibliothèques	dh1024.pem	01/03/2014 00:52	Fichier PEM	1 Ko		
Documents	README	27/02/2014 22:53	Document texte	1 Ko		
🔚 Images						
👌 Musique						
🛃 Vidéos						
👰 Ordinateur						
🗣 Réseau						
6 élément(s)					ſ	Afficher le Bure
9 🙆 🥘					FR 🔺 😼 🖺 🌗	00:54 01/03/2014

Pour se connecter au VPN, un clic droit sur l'icône d'interface « TAP-Win32 Adaptater V8 » et « connect »

NGUYEN Frédéric BTS SIO

Installation d'un VPN avec OpenVPN sous Debian Squeeze

Une fenêtre appârait alors :

OpenVPN Connection (client)	
Current State: Connecting	
Fri Mar 21 05:18:07 2014 LZO compression initialized Fri Mar 21 05:18:07 2014 Control Channel MTU parms [L:1542 D:138 EF:38 EB:0 ET Fri Mar 21 05:18:07 2014 Socket Buffers: R=[8192->8192] S=[8192->8192] Fri Mar 21 05:18:07 2014 Data Channel MTU parms [L:1542 D:1450 EF:42 EB:135 E Fri Mar 21 05:18:07 2014 Local Options hash [VER=V4]: '41690919' Fri Mar 21 05:18:07 2014 Expected Remote Options hash [VER=V4]: '530fdded' Fri Mar 21 05:18:07 2014 UDPv4 link local: [undef] Fri Mar 21 05:18:07 2014 UDPv4 link remote: 82:247.234.77:1194, sid=2be724c5 Fri Mar 21 05:18:07 2014 VERIFY OK: depth=1, /C=FR/ST=FR/L=Dugny/O=serveur Fri Mar 21 05:18:07 2014 VERIFY OK: nsCertType=SERVER Fri Mar 21 05:18:07 2014 VERIFY OK: depth=0, /C=FR/ST=FR/L=Dugny/O=serveur Fri Mar 21 05:18:08 2014 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 b Fri Mar 21 05:18:08 2014 Data Channel Encrypt: Using 160 bit message hash 'SHA1' Fri Mar 21 05:18:08 2014 Data Channel Decrypt: Using 160 bit message hash 'SHA1' Fri Mar 21 05:18:08 2014 Data Channel Decrypt: Using 160 bit message hash 'SHA1' Fri Mar 21 05:18:08 2014 Data Channel Decrypt: Using 160 bit message hash 'SHA1' Fri Mar 21 05:18:08 2014 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-A Fri Mar 21 05:18:08 2014 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-A Fri Mar 21 05:18:08 2014 [servervpn] Peer Connection Initiated with 82:247.234.77:	COEL:0] T:0EL:0AF:3/1] 51ddebe7d rvpn/CN=serveurvpn_1 pit key for HMAC authenticati pit key for HMAC authenticati S256-SHA, 1024 bit 194
<	*
Disconnect Reconnect	Hide

Si la connexion au VPN est un succès, les écrans de l'icône de l'interface « TAP-Win32 Adaptater V8 » deviennent verts.

Le tutoriel est maintenant finis.