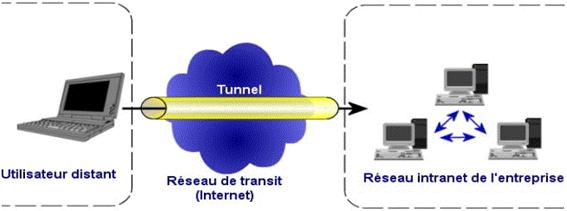
**2 - Principe de fonctionnement**

**2.1 - Principe général**

Un réseau Vpn repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.   
  
Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant Ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.  
  
Les données à transmettre peuvent être prises en charge par un protocole différent d'Ip. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant une en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

**2.2 - Fonctionnalités des Vpn**

  
  
Le Vpn d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion Vpn. Il existe deux cas:

L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le Nas (Network Access Server) du fournisseur d'accès et c'est le Nas qui établit la connexion cryptée.

L'utilisateur possède son propre logiciel client pour le Vpn auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un Nas compatible avec la solution Vpn choisie par l'entreprise. De plus, la demande de connexion par le Nas n'est pas cryptée Ce qui peut poser des problèmes de sécurité.

Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Nous verrons que pour pallier Ce problème certaines entreprises mettent en place des Vpn à base de Ssl, technologie implémentée dans la majorité des navigateurs Internet du marché.

Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le Vpn d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe", par un algorithme dit "Tokens sécurisés" (utilisation de mots de passe aléatoires) ou par certificats numériques.

**VPN : installation et configuration d'un VPN routé avec OpenVPN**

# Introduction[▲](http://mathieu-androz.developpez.com/articles/linux/vpn/)

[OpenVPN](http://openvpn.net/) 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.

# I. Qu'est-ce qu'un VPN ?[▲](http://mathieu-androz.developpez.com/articles/linux/vpn/)

Un VPN (Virtual Private Network) ou Réseau Privé Virtuel en français est connexion inter-réseau permettant de relier 2 réseaux locaux différents de façon sécurisé par un protocole de tunnelisation.  
La tunnelisation est un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

Le terme tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc normalement incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. De plus, créer un tunnel signifie aussi encapsuler un protocole dans un protocole de même niveau du modèle OSI (IP dans IPSec par exemple). Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer les données à l'entrée et serveur VPN (ou plus généralement serveur d'accès distant) l'élément déchiffrant les données en sortie. (Wikipedia)

# II. Installation d'OpenVPN[▲](http://mathieu-androz.developpez.com/articles/linux/vpn/" \o "Haut de page)

*Remarque : La méthode d'installation proposée dans cet article repose sur le fonctionnement de la distribution Debian et ses dérivés. Pour les autres distributions, veuillez vous reporter aux commandes de gestions des paquets implantées pour la distribution choisie.*

Installation d'OpenVPN proprement dit :

Installation d'OpenVPN

Sélectionnez

> apt-get install openvpn

Installation d'OpenSSL pour la sécurisation des données :   
*Remarque : Généralement, OpenSSL est installé par défaut sur les machines et ne nécessite donc pas d'être réinstallé.*

Installation d'OpenSSL

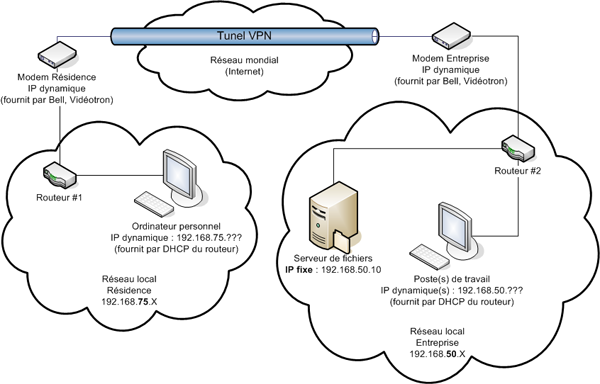
Sélectionnez

> apt-get install openssl

**Avant de débuter**

Pour parvenir à mettre en place la solution proposée, vous devez disposer d'un certain nombre de composantes :

* Des connexions Internet haute vitesse (à la maison et à l'entreprise)
* 2 routeurs identiques offrant le support VPN. De préférence le [Linksys WRV54G](http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US/Layout&cid=1118334818934&pagename=Linksys/Common/VisitorWrapper) (environ 200$/routeur)
* Un abonnement à un service de DNS dynamique. De préférence [DynDns](http://www.dyndns.com/services/dns/dyndns/) (environ 12$/année)

  
*Schéma 1.0 - Solution finale*

**Mettre en place les routeurs**

Vos routeurs actuels n'offrent probablement pas le support VPN. Il faut donc les remplacer par des routeurs spéciaux ayant la capacité d'accepter et de créer des connections VPN. Nous suggérons le modèle [Linksys WRV54G](http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US/Layout&cid=1118334818934&pagename=Linksys/Common/VisitorWrapper). Vous trouverez ce modèle dans la plupart des boutiques informatiques ([MicroBytes](http://www.microbytes.com" \t "_blank), offre généralement de bons prix). La première étape consiste à brancher les routeurs et à les faire fonctionner normalement. Assurez-vous de mettre à jour les routeurs avec [les plus récents firmware](http://www.linksys.com/servlet/Satellite?c=L_Download_C2&childpagename=US%2FLayout&cid=1115417109974&packedargs=sku%3D1115416826120&pagename=Linksys%2FCommon%2FVisitorWrapper).

**Noms de domaine dynamique**

Pour créer un VPN, **le routeur #1 doit connaître en tout temps l'adresse IP du routeur #2 et inversement**. Avec un forfait Internet standard, votre modem reçoit une adresse IP variable. Cet IP change de temps en temps au gré de votre fournisseur Internet. Ceci nous cause un problème majeur puisque si l'adresse IP du routeur #1 change, alors le routeur #2 ne pourra plus le contacter et le VPN s'effondrera. Pour pallier à ce problème, nous utiliserons un nom de domaine dynamique.

**Créer une connexion VPN entre les deux routeurs**

L'étape cruciale : il s'agit d'établir un lien sécurisé entre les deux routeurs. Dans le panneau de contrôle du routeur #1, allez à « **Security-->VPN** » et ajustez les paramètres comme ceci :

Cliquez ensuite sur le bouton « **Advanced VPN Tunnel Setup** » au bas de la page et activez les options comme ceci :

Dans le panneau de contrôle du **routeur #2**, allez à « **Security-->VPN** » et ajustez les paramètres comme ceci :

\***À noter que les configurations sur les deux routeurs doivent être identiques** à l'exception du « Local Secure Group » et du « Remote Secure Group » qui sont inversés et du « Remote Secure Gateway » qui pointe vers le DNS de l'autre routeur.

Cliquez ensuite sur le bouton « **Advanced VPN Tunnel Setup** » au bas de la page et activez les mêmes options que pour le routeur #1. (voir ci-dessus)

À partir de maintenant vous devriez pouvoir cliquer sur le bouton « Connect » ou « Disconnect » au bas la page « **Security-->VPN** ».

**Tester le VPN**

Dans certains cas il y a un délai avant que la connexion VPN se crée. Pour forcer les choses, faites quelques « ping » vers le serveur de fichiers et du serveur vers le poste de travail distant. Si vous obtenez une réponse c'est que tout fonctionne bien.

Si le VPN est connecté correctement, vous devriez pouvoir **accéder aux fichiers du serveur en tapant « \\192.168.50.10\ » dans la barre d'adresse d'Internet Explorer**.

À partir de là, vous pouvez fort bien créer un lecteur réseau dans le poste de travail de Windows en spécifiant l'adresse IP du serveur lors de la création du lecteur.

**Configuration de VPN Server**

Grâce au paquet **VPN Server**, vous pouvez facilement transformer votre Synology NAS en un serveur VPN pour permettre aux utilisateurs d'accéder aux ressources partagées à distance et en toute sécurité dans l'espace du réseau local de votre Synology NAS. En intégrant les protocoles VPN communs - PPTP, OpenVPN et L2TP/IPSec - VPN Server fournit des options pour établir et gérer des services VPN adapté à vos besoins personnels. Pour choisir l'un des types de serveur VPN suivants et pour activer les services VPN sur votre Synology NAS, installez et lancez **VPN Server**.

\*\*\*\*\*\*\*\*\*\*\*\*

**Remarque :**

* L'activation de VPN affecte les performances réseau du système.
* Seuls les **administrateurs** peuvent installer et configurer VPN Server.

**PPTP**

Le protocole PPTP (Point-to-Point Tunneling Protocol) est une solution VPN couramment utilisée prise en charge par la plupart des clients (notamment Windows, Mac, Linux et les appareils mobiles). Pour plus d'informations sur le PPTP, voir [ici](http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol).

**Pour activer VPN server PPTP :**

1. Ouvrez **VPN Server** et ensuite accédez à **Paramètres** > **PPTP** dans le panneau de gauche.
2. Cochez **Activer le serveur VPN PPTP**.

\*\*\*\*\*\*\*\*\*\*\*\*\*

**Remarque :**

* L'activation de VPN affecte les performances réseau du système.
* Seuls les **administrateurs** peuvent installer et configurer VPN Server.

**PPTP**

Le protocole PPTP (Point-to-Point Tunneling Protocol) est une solution VPN couramment utilisée prise en charge par la plupart des clients (notamment Windows, Mac, Linux et les appareils mobiles). Pour plus d'informations sur le PPTP, voir [ici](http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol).

**Pour activer VPN server PPTP :**

1. Ouvrez **VPN Server** et ensuite accédez à **Paramètres** > **PPTP** dans le panneau de gauche.
2. Cochez **Activer le serveur VPN PPTP**.
3. Spécifiez une adresse IP virtuelle de VPN server dans les champs **Adresse IP dynamique**. Consultez [À propos de l'adresse IP dynamique](https://www.synology.com/fr-fr/knowledgebase/DSM/help/VPNCenter/vpn_setup#dynamic) ci-dessous pour plus d'informations.

\*\*\*\*\*\*\*\*\*\*\*

**OpenVPN**

OpenVPN est une solution open source pour la mise en œuvre du service VPN. Il protège la connexion VPN avec le mécanisme de cryptage SSL/TLS. Pour plus d'informations sur le OpenVPN, voir [ici](http://openvpn.net/).

**Pour activer VPN server OpenVPN :**

1. Ouvrez **VPN Server** et ensuite accédez à **Paramètres** > **OpenVPN** sur le panneau de gauche.
2. Cochez **Activer le serveur OpenVPN**.

\*\*\*\*\*\*\*\*\*\*

**L2TP/IPSec**

L2TP (Layer 2 Tunneling Protocol) sur IPSec fournit des réseaux privés virtuels avec une sécurité accrue et est pris en charge par la plupart des clients (tels que Windows, Mac, Linux et les appareils mobiles). Pour plus d'informations sur le L2TP, voir [ici](http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol).

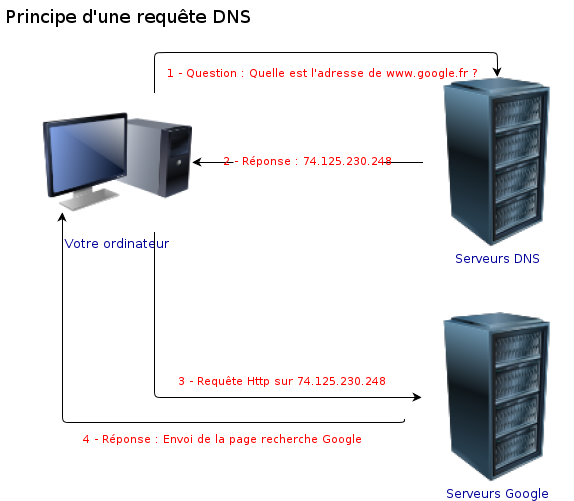
**Remarque :**

* Pour utiliser L2TP/IPSec, assurez-vous que votre Synology NAS est équipé de DSM 4.3 ou version ultérieure.

**Activer le serveur L2TP/IPSec VPN :**

1. Ouvrez **VPN Server** et ensuite accédez à **Paramètres** > **L2TP/IPSec** dans le panneau de gauche.
2. Cochez **Activer le serveur L2TP/IPSec VPN**.

**UTILISATION**

[](http://www.culture-informatique.net/WordPress3/wp-content/uploads/2012/10/Requ%C3%AAte-Dns.png)

|  |
| --- |
| **C'est quoi un proxy ?** |

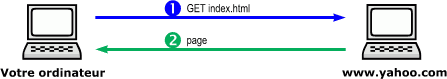
Je prends mon dictionnaire d'anglais : "*proxy : mandataire", "by proxy : par procuration*".

Un proxy, c'est donc un mandataire, un intermédaire.

Sur Internet, il existe différents types de proxy. Les plus courants sont les proxy HTTP. Ils supportent les protocoles HTTP et FTP.

Comment ça marche ?

En tapant une adresse comme **http://www.yahoo.com/index.html**, votre ordinateur va se connecter sur le serveur **www.yahoo.com** et demander la page **index.html**.

  
 **Requête HTTP sans proxy**

Avec un proxy, quand vous tapez **http://www.yahoo.com/index.html**, votre ordinateur va se connecter au proxy et lui demande d'aller chercher la page sur **www.yahoo.com**.

  
 **Requête HTTP avec proxy**

A quoi ça sert ?

Un proxy peut avoir plusieurs utilisations.

* **Le proxy peut vous protéger :** il peut vous autoriser à vous connecter à l'extérieur et interdire les ordinateurs d'Internet de venir se connecter sur le vôtre. Cette fonction de protection du proxy est souvent incluse dans les ***firewalls*** (murs de feu), des ordinateurs programmés pour filtrer les communications entre les réseaux (par exemple entre le réseau d'une entreprise et Internet).
* **Le proxy peut masquer les informations concernant votre ordinateur:** En effet, quand vous surfez, tous les sites Web peuvent savoir de quel site vous venez, quel navigateur vous utilisez, quel est votre système d'exploitation, votre adresse IP... Certains proxy masquent ces informations. Ces proxy sont dits ***proxy anonymes***.
* **Le proxy peut mémoriser les pages les plus demandées**. Ainsi si vous demandez plusieurs fois la page **http://www.yahoo.com/index.html**, le proxy vous la donnera immédiatement sans aller la chercher sur www.yahoo.com. Si vous êtes proche du proxy, cela peut accélérer les choses. Il s'appelle alors ***proxy-cache***.

Les dangers

|  |  |
| --- | --- |
| **Confidentialité:** | Etant donné que vous demandez toutes vos pages au proxy, celui-ci peut savoir tous les sites que vous avez visité. |
| **Mots de passe:** | Certains sites Web nécessitent des mots de passe. Comme vous passez par le proxy, le proxy connaîtra vos mots de passe (sauf si vous utilisez HTTPS/SSL). |
| **Modifications:** | Le proxy vous fournit les pages, mais il est également possible qu'il les modifie à la volée avant de vous les donner (cela reste rare, mais possible !). |
| **Censure:** | Certains proxy peuvent être configurés pour censurer des sites. |

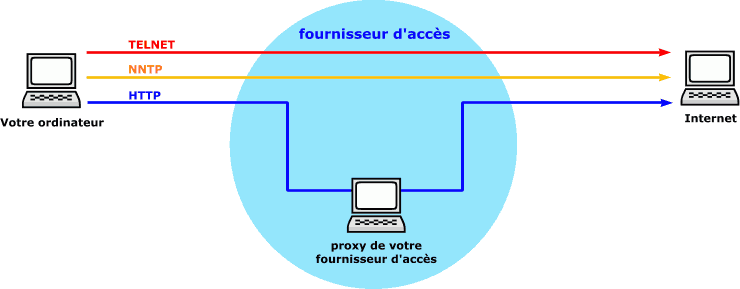
Il faut donc avoir confiance en l'administrateur du proxy. A vous de voir si vous voulez faire confiance au serveur proxy de votre fournisseur d'accès. Pour ceux des entreprises... c'est à voir ! Les spécialistes estiment que 70% des entreprises américaines examinent les accès des employés aux proxy.

Malgré tout, je vous recommande de désactiver - si vous le pouvez - le proxy quand vous devez accéder à des sites nécessitant des mots de passe.

Autre danger : les proxy transparents

En principe, vous indiquez **volontairement** que vous voulez utiliser un proxy.

Certains fournisseurs d'accès (comme *Wanadoo* ou *AOL*, dans certains cas), regardent quels protocoles vous utilisez et **détournent sans vous le dire** les requêtes HTTP vers leurs serveurs proxy.



**Certains fournisseurs détournent les requêtes HTTP  
sur leurs serveurs proxy sans vous le dire.**

**Pourquoi font-ils cela ?**

* Cela permet d'effectuer des statistiques très précises sur les habitudes de navigation des internautes, et ce genre d'information se vend très bien aux sociétés de marketting.
* Cela permet d'économiser de la bande passante pour réduire la quantité de données reçues d'Internet.
* Il est également arrivé chez un fournisseur (AOL) que le proxy-cache recompresse les images avec une qualité moindre pour gagner de la place. Résultat: tous les sites consultés devennaient hideux (images de très mauvaise qualité).

**Comment détecter un proxy transparent ?**

En principe, quand vous vous connectez sur un site Web sans proxy, celui-ci doit voir votre adresse IP (ou celle de votre passerelle).

Il suffit de comparer votre adresse IP avec celle vue par le serveur Web. Désactivez le proxy dans votre navigateur, puis essayez par exemple un des sites suivants:

* <http://cpcug.org/scripts/env.cgi>
* <http://tools.blueyonder.co.uk/cgi-bin/env.cgi>

Si vous ne passez pas par une passerelle, comparez le champ REMOTE\_ADDR avec votre adresse IP. Si elles sont différentes, alors c'est que votre fournisseur d'accès utilise probablement un proxy transparent ! (ou bien que vous passez par une passerelle/firewall).

Je vous recommande de le sermoner votre fournisseur d'accès et d'exiger la suppression du proxy transparent.  
Changez de fournisseur d'accès si ce dernier refuse !

(Pour connaître votre adresse IP, lancez winipcfg.exe sous Windows 95/98/ME, ou ipconfig.exe sous Windows NT/2000/XP)

Où trouver des serveurs proxy ?

Votre fournisseur d'accès possède très certainement des proxy à votre disposition pour accélérer votre navigation sur Internet. Regardez la documentation que vous a fourni votre fournisseur d'accès, ou demandez-leur. Ils se feront un plaisir de vous donner l'adresse.

Comment améliorer l'anonymat ?

Il faut **filtrer le maximum d'information**.

Si vous n'avez pas accès à des proxy anonymes, vous pouvez quand même utiliser des logiciels pour filtrer la plupart des informations (type de navigateur, etc.).

Je vous recommande [Proxomitron](http://www.sebsauvage.net/logiciels/proxomitron.html). Il est gratuit et peut filtrer à la demande ces informations.

Vous avez également la possibilité de passer par des services spécialisés comme <http://www.anonymizer.com> , <http://megaproxy.com> ou <http://surfola.com>. Certains services ne nécessitent pas reconfigurer le proxy, mais s'utilisent en se connectant directement dessus avec votre navigateur.  
Certains services sont payant, d'autres gratuits.