

MANUEL UTILISATEUR



Titre	MANUEL UTILISATEUR DU SERVICE ACCÈS NOMADE SOUS GNU/LINUX
Référence	CRIUN/MU SEC 002
Version	1.3 du 10/01/2012
Dernière page	14
Classification	Diffusion Libre
Mots clés	Accès distant, Réseau Privé Virtuel, WebVPN, Cisco AnyConnect

Résumé

Ce document décrit l'installation pas à pas et la prise en main du service accès nomade depuis les environnements GNU/Linux.

AUTEUR DSI	DÉPARTEMENT DSI Université de Nantes		
Destinataire(s) * étudiants	Département -	Destinataire(s) DSI	Département IRTS

Table des matières

1 Principe général.....	3
1.1 Modalités d'accès.....	3
1.2 Restrictions d'usage.....	4
2 Pré-requis.....	5
3 Établissement d'un accès WebVPN.....	6
4 Établissement d'un accès AnyConnect.....	9
4.1 Pré-requis logiciels et matériels.....	9
4.2 Installation en ligne.....	9
4.3 Installation hors ligne.....	10
4.4 Démarrage de l'accès AnyConnect.....	11
4.5 Utilisation courante.....	15

Glossaire

AnyConnect	Nom du logiciel établissant un RPV avec l'Université de Nantes
RPV	Réseau Privé Virtuel ou Virtual Private Network (VPN) en anglais
SSL	Secure Socket Layer
TLS	Transport Layer Security
WebVPN	Mode d'accès distant web à l'intranet de l'Université

 UNIVERSITÉ DE NANTES	DSI de l'Université de Nantes	Service Accès Nomade Guide pour GNU/Linux	Référence CRIUN/MU SEC 002	Date 24/12/2008
			Version 1.2	Page 2

1 Principe général

Le **service accès nomade** est un moyen d'accès distant à l'intranet de l'Université de Nantes proposé à l'ensemble de ses étudiants. Il est accessible à partir de n'importe quelle prise banalisée à internet (ADSL, Hot Spot WiFi...), dont les zones WiFi de l'Université de Nantes ou encore les chambres étudiantes du CROUS. S'agissant d'un service multiplate-forme, vous pouvez aussi bien l'utiliser sous les environnements GNU/Linux, Mac OS X ou Microsoft Windows.

Tous vos **services internet** habituels comme la messagerie SMTP, la messagerie instantanée Jabber avec ses connecteurs MSN, Yahoo! Messenger (...), l'ensemble des Web Services de l'Université restent disponibles en plus de **services intranet**, jusque là inaccessibles à distance. La navigation sur internet au travers de l'infrastructure de l'Université est également proposée à tous les étudiants connectés.

Les services intranet mis à votre disposition sont susceptibles de varier d'une filière d'études à l'autre. Le plus courant est incontestablement le partage de fichiers. En vous connectant sur le serveur CIFS/SMB de votre filière, vous gérez votre espace de stockage personnel comme si vous étiez physiquement présent à l'Université. **Pour connaître la liste exhaustive des serveurs de fichiers accessibles, toutes filières confondues, vous devez vous rendre sur la page du WebVPN. La procédure est intégralement décrite plus bas.**

Nota : selon les services intranet contactés, une nouvelle phase d'authentification pourra être demandée. Les paramètres d'authentification peuvent différer de ceux du service accès nomade (ex. dans le cas d'un accès à un partage de fichiers).

1.1 Modalités d'accès

Tous les étudiants inscrits à l'Université de Nantes bénéficient du service accès nomade. Pour d'évidentes raisons de sécurité, la connexion à ce service est soumise à une phase d'authentification préalable. Vous devez alors vous munir de vos paramètres personnels de connexion :

- le nom d'utilisateur correspond à votre numéro étudiant précédé de la lettre E (ex. E99001),
- le mot de passe correspondant vous a été attribué lors de votre inscription à l'Université.

Selon vos besoins, deux modes d'accès sont proposés. Le premier d'entre-eux, dénommé **accès WebVPN**, offre des fonctionnalités réduites mais n'exige, en retour, qu'un simple navigateur web pour fonctionner.

Les principales ressources joignables au travers de l'accès WebVPN sont :

- l'intégralité des Web Services de l'Université de Nantes,
- l'espace de stockage personnel, selon votre filière d'affectation,
- la navigation sur Internet.

Le second mode, dénommé **accès AnyConnect**, procure des fonctionnalités complètes au détriment d'un impact plus grand sur votre poste de travail. Ce mode requiert en effet l'installation de l'application AnyConnect servant à établir un Réseau Privé Virtuel avec l'Université de Nantes. Vous retrouvez naturellement les fonctionnalités du mode WebVPN sans certaines contraintes d'usage liées à l'usage systématique d'un navigateur web, et bien d'autres... Vous utilisez les services dont vous avez besoin exactement comme si vous étiez physiquement connecté à l'intranet de l'Université.

	DSI de l'Université de Nantes	Service Accès Nomade Guide pour GNU/Linux	Référence CRIUN/MU SEC 002	Date 24/12/2008
			Version 1.2	Page 3

L'accès AnyConnect est transparent à l'usage puisque vos applications courantes comme Mozilla Thunderbird, Mozilla Firefox, Microsoft Outlook, Microsoft Internet Explorer, Gajim, Univ'tchat, l'explorateur Windows (...) sont pleinement fonctionnelles sans reconfiguration. Si vous désirez, par exemple, vous connecter à votre espace de stockage personnel depuis Microsoft Windows, il suffit simplement de créer un partage réseau vers la ressource désirée !

1.2 Restrictions d'usage

Plusieurs mesures sécuritaires sont mises en œuvre à l'établissement d'un accès AnyConnect :

- déconnexion automatique de l'intranet de l'Université après un délai d'inactivité de 10 minutes,
- interdiction des connexions multiples simultanées en WebVPN ou AnyConnect,
- routage par défaut dans le Réseau Privé Virtuel de l'Université de tout le trafic sortant du poste utilisateur. En d'autres termes, votre poste de travail s'isole du reste de votre réseau local ou plus généralement d'internet dès la connexion AnyConnect. **Vous devez donc obligatoirement passer par le serveur mandataire de l'Université pour continuer à surfer sur internet.**

Le service accès nomade n'est pas une porte ouverte sur l'ensemble de l'intranet de l'Université de Nantes. Il fait l'objet de contrôles actifs, de filtrages multi-niveaux et d'une journalisation complète du trafic. Il se peut qu'une ressource que vous utilisez régulièrement au sein de votre filière d'études ne soit pas (ou pas encore) accessible par le WebVPN ou AnyConnect. Dans cette situation, remontez le besoin à l'un de vos enseignants ou encore l'un des correspondants informatiques de votre filière.

	DSI de l'Université de Nantes	Service Accès Nomade Guide pour GNU/Linux	Référence CRIUN/MU SEC 002	Date 24/12/2008
			Version 1.2	Page 4

2 Pré-requis

Nous spécifions ci-après tous les pré-requis logiciels et matériels nécessaires à l'installation du client AnyConnect ou à l'usage des modes d'accès WebVPN ou AnyConnect. En termes de connectivité réseau, vous devez impérativement disposer d'un accès à Internet non filtré sur le port sécurisé https (443/TCP) vers le serveur nomade.etu.univ-nantes.fr (193.52.107.14).

Mode d'accès	Environnement	Pré-requis
AnyConnect - Installation hors ligne	GNU/Linux	<p>AnyConnect est officiellement supporté sous Red Hat Enterprise Linux et Ubuntu. Il est probable qu'il puisse fonctionner sur la plupart des autres distributions GNU/Linux.</p> <p>L'installation du client AnyConnect exige les droits du super-utilisateur root</p>
AnyConnect - Installation en ligne	GNU/Linux	<ul style="list-style-type: none"> • L'ensemble des pré-requis d'installation hors ligne d'AnyConnect • Mozilla Firefox • Oracle Java 1.5 ou version ultérieure <p>Les systèmes bi-architecture (cohabitation de bibliothèques 32 et 64 bits) ne supportent pas l'installation en ligne d'AnyConnect</p> <p>L'installation du client AnyConnect exige les droits du super-utilisateur root</p>
WebVPN	-	<ul style="list-style-type: none"> • N'importe quel navigateur web récent avec JavaScript

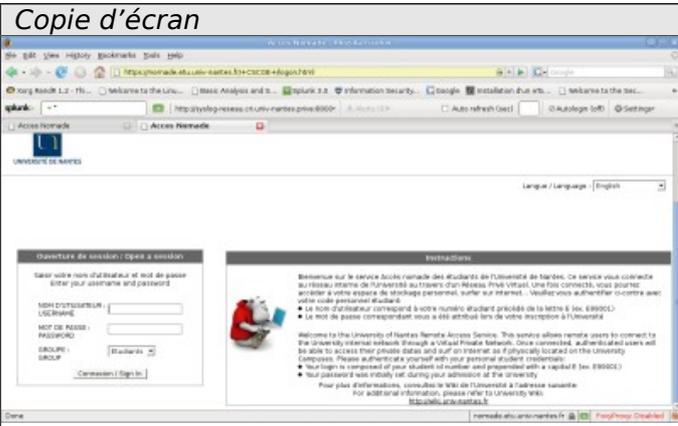
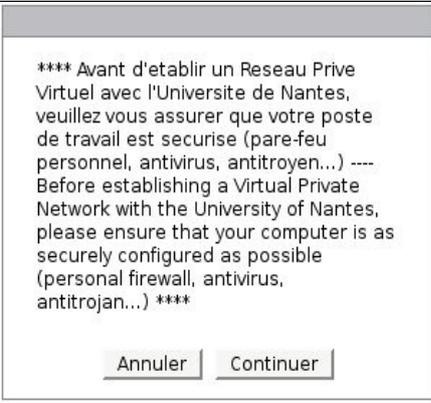
Seule la phase d'installation du client AnyConnect demande des droits privilégiés sur votre environnement de travail. Par la suite, ce logiciel peut être exécuté à partir de n'importe quel compte système non privilégié.

	DSI de l'Université de Nantes	Service Accès Nomade Guide pour GNU/Linux	Référence CRIUN/MU SEC 002	Date 24/12/2008
			Version 1.2	Page 5

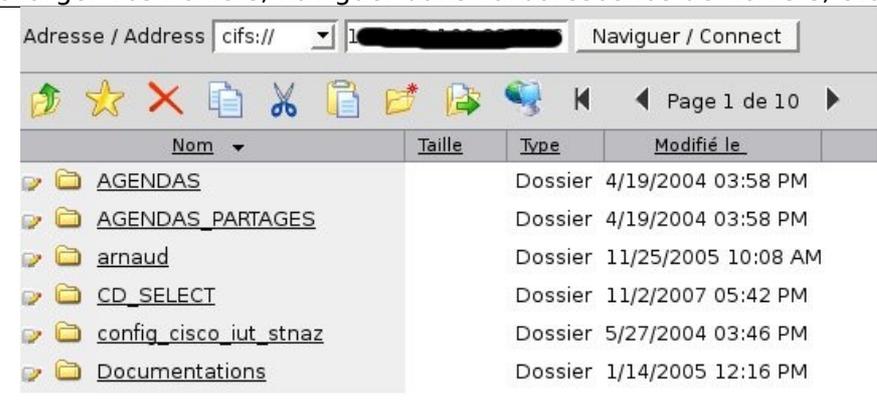
3 Établissement d'un accès WebVPN

Le mode d'accès WebVPN est aucunement intrusif sur les postes de travail puisqu'il n'exige pas la moindre installation logicielle. Un simple navigateur web supportant le JavaScript suffit. On s'assurera, tout de même, que les pré-requis exposés au §2 sont satisfaits avant d'aller plus loin.

Lancez votre navigateur et saisissez l'url suivante: <https://nomade.etu.univ-nantes.fr>

N°	Copie d'écran	Explications
1		<p>La page ci-contre s'affiche. Changez la langue proposée par défaut si celle-ci ne vous convient pas puis saisissez alors votre identifiant de connexion et le mot de passe associé. Enfin, cliquez sur le bouton Connexion / Sign In.</p> <p>En cas de succès de la phase d'authentification, vous êtes automatiquement redirigé vers la page ci-dessous.</p>
2		<p>Avant d'aller plus loin, contrôlez le niveau de sécurité de votre poste de travail. Un anti-virus à jour est notamment demandé aux étudiants sous les environnements Microsoft Windows. Dans tous les cas, un pare-feu personnel est requis pour minimiser les risques de piratage de votre poste par internet. Si vous satisfaites à ces pré-requis, cliquez sur le bouton Continuer. Le cas échéant, cliquez sur Annuler. La connexion au WebVPN est alors rompue.</p>

N°	Copie d'écran	Explications
3		<p>La fenêtre ci-contre apparaît ; plusieurs rubriques sont proposées dans la partie gauche de la fenêtre.</p> <p>Sélectionnez la rubrique Accueil / Home.</p>
4		<p>La page d'accueil se compose de messages d'information, fils RSS de l'Université, liens vers différentes ressources intranet comme les serveurs de partage de fichiers...</p>
5	<p>La navigation sur internet ne nécessite aucun paramétrage spécifique de votre poste de travail. Sélectionnez simplement le protocole désiré dans la barre de navigation (http:// ou https://) puis saisissez à côté l'url du site et enfin cliquez sur le bouton Naviguer / Connect. Le site en question s'ouvre dans la fenêtre courante.</p> <p>Nota : la navigation sur internet au travers du WebVPN empreinte l'infrastructure des serveurs mandataires de l'Université de Nantes.</p>	
6	<p>Vous trouverez sur la page d'accueil du WebVPN ou encore dans la rubrique Partage de fichiers / Share files des liens hypertextes vers tous les serveurs de fichiers de l'Université autorisés à ce jour. Cette liste est en constante évolution. Vous pouvez aussi ouvrir un partage de fichiers à partir de la barre générale de navigation. Sélectionnez alors le protocole cifs (cifs://), l'url complète de la ressource (sous la forme nom_du_serveur/chemin_complet) puis cliquez sur le bouton Naviguer / Connect.</p>	
7	<p>Il vous est ensuite demandé de vous authentifier auprès du serveur de fichiers contacté. Attention, selon votre filière, les paramètres d'authentification peuvent différer de ceux du WebVPN.</p>	

N°	Copie d'écran	Explications
8		<p>Une fois authentifié, l'interface de gestion de votre partage de fichiers s'ouvre dans le navigateur. Vous pouvez effectuer des opérations simples comme : supprimer, copier, coller, télécharger vos fichiers, naviguer dans l'arborescence de fichiers, etc.</p>

4 Établissement d'un accès AnyConnect

L'accès AnyConnect est conditionné à l'installation préalable d'un logiciel client éponyme. Celui-ci s'installe, à votre choix, en ligne à l'aide du WebVPN ou bien encore à partir d'un paquetage binaire. **La première méthode d'installation est fortement conseillée** puisqu'elle minimise le nombre d'opérations manuelles. Elle est fonctionnelle sur les principales plates-formes logicielles, à savoir, GNU/Linux, Mac OS X ou encore Microsoft Windows.

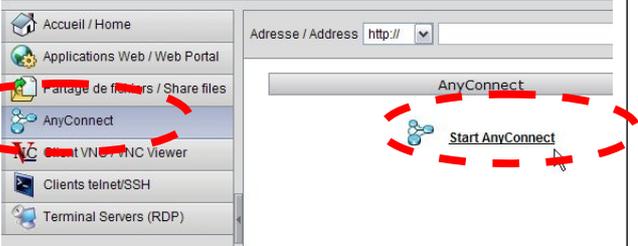
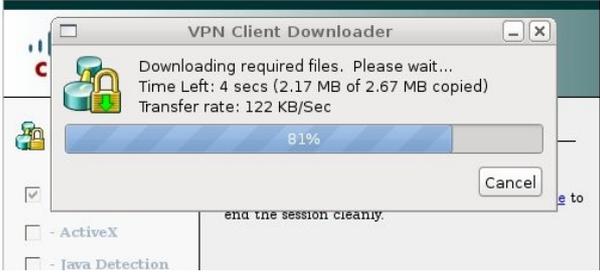
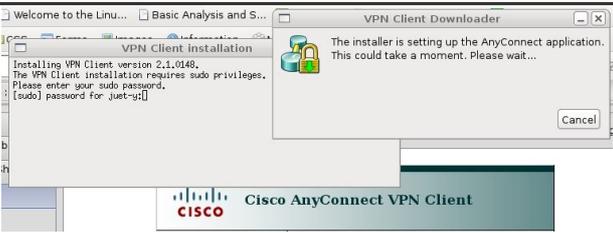
En cas d'échec de l'installation en ligne du client AnyConnect, vous devrez procéder à une installation hors ligne manuelle.

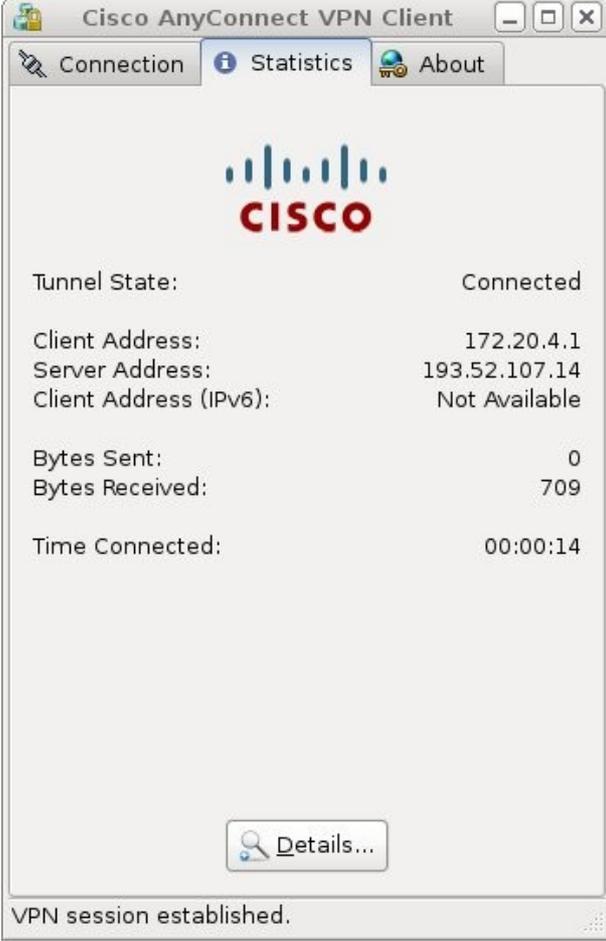
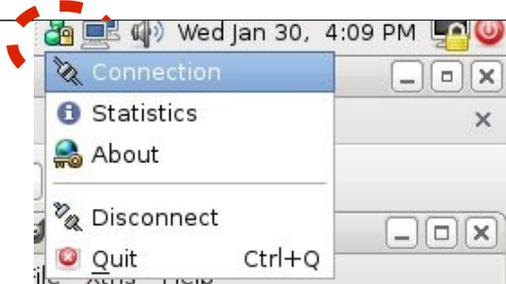
4.1 Pré-requis logiciels et matériels

Il est rappelé que l'installation en ligne ou hors ligne du client AnyConnect nécessite les droits administrateur sur le poste de travail.

4.2 Installation en ligne

L'installation en ligne du client AnyConnect s'effectue entièrement depuis le WebVPN.

N°	Commande et résultat de commande	Explications
1		<p>Sous la rubrique AnyConnect, cliquez sur l'hyperlien Start AnyConnect</p>
2		<p>La barre de progression de téléchargement de l'archive d'installation du client AnyConnect apparaît. Patientez quelques instants.</p>
3		<p>Saisissez le mot de passe de votre compte utilisateur système local (sudo).</p>

4		<p>En cas de succès de l'installation en ligne, AnyConnect est automatiquement lancé. Le Réseau Privé Virtuel est monté avec l'Université de Nantes.</p> <p>Vous devez par la suite configurer le serveur proxy de l'université dans votre navigateur, comme indiqué au §4.5.</p>
5		<p>L'application AnyConnect apparaît également en barre des tâches. Cette icône est caractéristique de l'état "RPV connecté".</p>

4.3 Installation hors ligne

Les fichiers d'installation hors ligne du client AnyConnect sont librement téléchargeables sur le Wiki de l'Université wiki.univ-nantes.fr. Choisissez, évidemment, le fichier correspondant à votre architecture matérielle et logicielle :

<http://wiki.univ-nantes.fr/doku.php?id=etudiants>

N°	Commande et résultat de commande	Explications
1	<code>\$ cd <répertoire_téléchargement></code>	Placez-vous dans le répertoire de téléchargement de l'archive d'installation du client AnyConnect
2	<code>\$ tar -zxf anyconnect-linux-2.1.0148-k9.tar.gz</code>	Décompressez et extrayez les fichiers de l'archive
3	<code>\$ cd ciscovpn</code>	Placez-vous dans le sous-répertoire créé

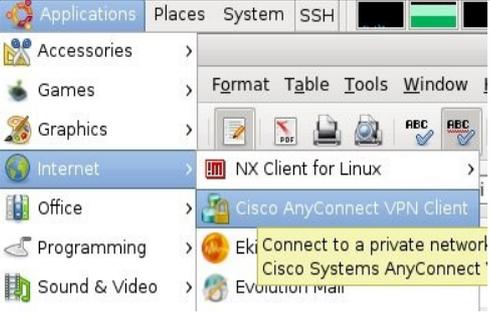
		lors de l'extraction des fichiers
4	<code>\$ sudo ./vpn_install.sh</code>	Lancez le script d'installation ; attention, l'opération requiert les droits du super-utilisateur root.
5	<pre>Installing Cisco AnyConnect VPN Client ... Client Software License Agreement of Cisco Systems ... Starting the VPN agent... Done!</pre>	L'installation du client AnyConnect débute. En cas de succès de l'opération, le message Done! est affiché.
6	<p>Le client AnyConnect est installé sous le répertoire <code>/opt/cisco</code>. Le processus <code>vpnagentd</code> est automatiquement démarré.</p> <pre>\$ ls -R /opt/cisco/ /opt/cisco/: vpn /opt/cisco/vpn: anyconnect-linux-2.1.0148-k9-15011927012008.log bin lib pixmaps profile update.txt VPNManifest.dat /opt/cisco/vpn/bin: vpn vpnagentd vpndownloader.sh vpnoi vpn_uninstall.sh /opt/cisco/vpn/lib: libcrypto.so.0.9.8 libssl.so.0.9.8 /opt/cisco/vpn/pixmaps: company-logo.png cvc-connect.png cvc-info.png systray_disconnecting.png vpnoi48.png cvc-about.png cvc-disconnect.png systray_connected.png systray_notconnected.png \$ ps -ef grep cisco grep -v grep root 15659 1 0 15:01 ? 00:00:00 /opt/cisco/vpn/bin/vpnagentd</pre>	

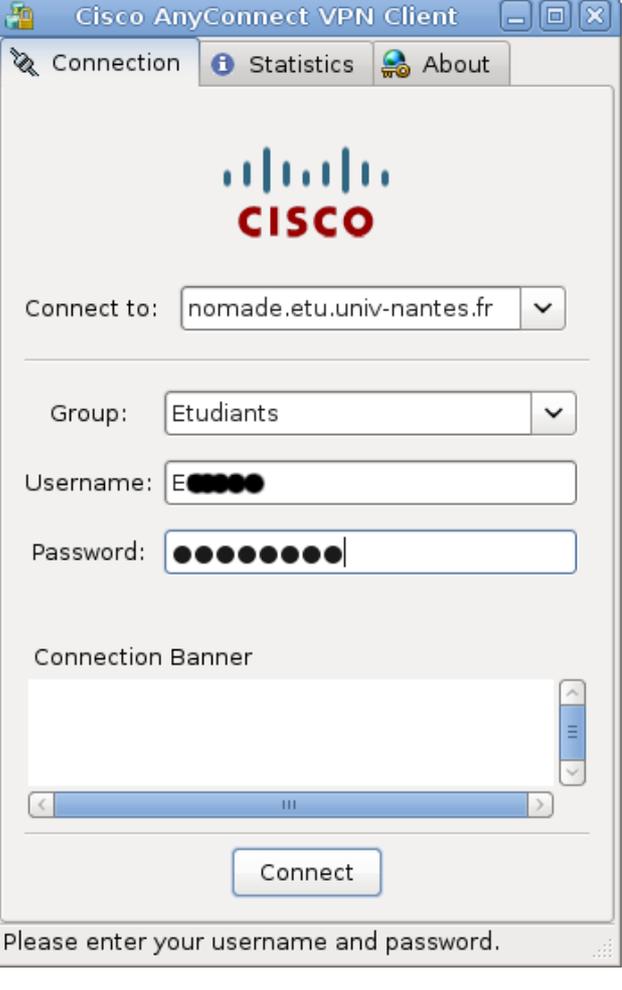
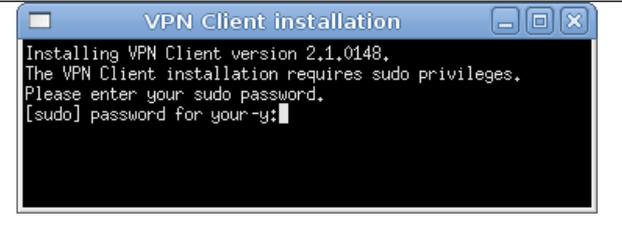
4.4 Démarrage de l'accès AnyConnect

Pré-requis : le client AnyConnect a été installé avec succès sur le poste de travail par la méthode en ligne ou hors ligne.

Il existe deux méthodes distinctes pour démarrer un accès AnyConnect. La première d'entre elles s'appuie sur le WebVPN. Une fois authentifié sur la page d'accueil, vous arrivez dans la rubrique AnyConnect où il vous reste à cliquer sur le lien `Start AnyConnect`. Le client AnyConnect se lance automatiquement puis établit le RPV avec l'Université de Nantes. Vous n'avez pas à vous réauthentifier puisque vos paramètres personnels d'authentification sont transportés par le WebVPN.

La seconde méthode de démarrage de l'accès AnyConnect est traditionnelle et décrite en détail ci-après. Elle doit être mise en œuvre en cas d'échec du démarrage en ligne du client AnyConnect depuis le WebVPN.

N°	Copie d'écran, commande	Explications
1		<p>Démarrez le client AnyConnect en sélectionnant le raccourci Applications -> Internet -> Cisco AnyConnect VPN Client</p> <p>ou en exécutant la commande suivante depuis une fenêtre terminal :</p> <p>/opt/cisco/vpn/bin/vpnui</p>
2		<p>Au premier lancement, la barre de connexion est vide et aucun profil utilisateur n'est chargé. Saisissez le nom DNS <code>nomade.etu.univ-nantes.fr</code> dans la barre puis cliquez sur le bouton Connect.</p> <p>Aux lancements suivants, l'identité de la passerelle sera automatiquement inscrite. Il suffira juste de cliquer sur le bouton Connect pour établir le Réseau Privé Virtuel avec l'Université de Nantes.</p>

N°	Copie d'écran, commande	Explications
3		<p>A présent, saisissez votre nom d'utilisateur (I.e. numéro d'étudiant précédé de la lettre E) et le mot de passe associé puis cliquez sur le bouton Connect.</p>
4		<p>Nous retrouvons à cette étape la bannière d'avertissement du WebVPN. Avant d'aller plus loin, contrôlez le niveau de sécurité de votre poste de travail. Un anti-virus à jour est notamment demandé aux étudiants sous les environnements Microsoft Windows. Dans tous les cas, un pare-feu personnel est requis pour minimiser les risques de piratage de votre poste par internet. Si vous satisfaites à ces pré-requis, cliquer sur le bouton Accept. Le cas échéant, cliquez sur Disconnect. La connexion AnyConnect est alors rompue.</p>
5		<p>Rentrez le mot de passe de votre compte utilisateur système.</p>

N°	Copie d'écran, commande	Explications
6	 <p>The screenshot shows the Cisco AnyConnect VPN Client window. The title bar reads "Cisco AnyConnect VPN Client". There are three tabs: "Connection", "Statistics", and "About". The "Statistics" tab is active, displaying the Cisco logo and the following information:</p> <pre> Tunnel State: Connected Client Address: 172.20.4.1 Server Address: 193.52.107.14 Client Address (IPv6): Not Available Bytes Sent: 0 Bytes Received: 1235 Time Connected: 00:00:24 </pre> <p>At the bottom of the window, there is a "Details..." button and a status bar that says "VPN session established."</p>	<p>Le Réseau Privé Virtuel est établi lorsque l'état du tunnel (Tunnel State) vaut "Connected".</p> <p>Le fenêtre ci-contre AnyConnect peut désormais librement être fermée. Elle sera alors iconifiée dans la barre des tâches.</p>

	DSI de l'Université de Nantes	Service Accès Nomade Guide pour GNU/Linux	Référence CRIUN/MU SEC 002	Date 24/12/2008
			Version 1.2	Page 14

4.5 Utilisation courante

Navigation sur Internet

La navigation sur internet et sur l'intranet de l'Université de Nantes se fait au moyen du serveur mandataire `cache.etu.univ-nantes.fr` joignable sur le port TCP 3128. Les utilisateurs de Mozilla Firefox ou d'un autre navigateur web doivent obligatoirement renseigner les nouveaux paramètres proxy. La procédure est décrite ci-dessous pour Firefox :

1. Sélectionnez le menu Outils --> Options
2. Sélectionnez l'onglet Avancé --> Réseau et cliquez sur le bouton Paramètres
3. Sélectionnez Configuration manuelle du proxy puis renseignez les champs comme suit:
 - Proxy HTTP: `cache.etu.univ-nantes.fr`
 - Port: 3128
 - Cocher la case Utiliser ce serveur proxy pour tous les protocoles

Vous devrez supprimer manuellement la configuration proxy une fois AnyConnect arrêté.

Partages de fichiers

A l'aide de l'explorateur Nautilus, il vous suffit de « Connecter un lecteur réseau » en renseignant à la fois le nom du serveur de fichiers de votre composante et le répertoire recherché.