- PDF veröffentlicht am 25.11.2013 — *Jan-Marc Pilawa 2013/11/25 16:23*

VPN einrichten (Cisco Anyconnect 3.0+)

Für alle

1. Windows & MAC OS X
2. Linux
3. Apple IOS und Android
4. VPN-Client "AnyConnect" nutzen
5. Wahl der Profile
6. Wahl zwischen IPSec und SSL-VPN
7. VPN an anderen Einrichtungen nutzen

Einleitung

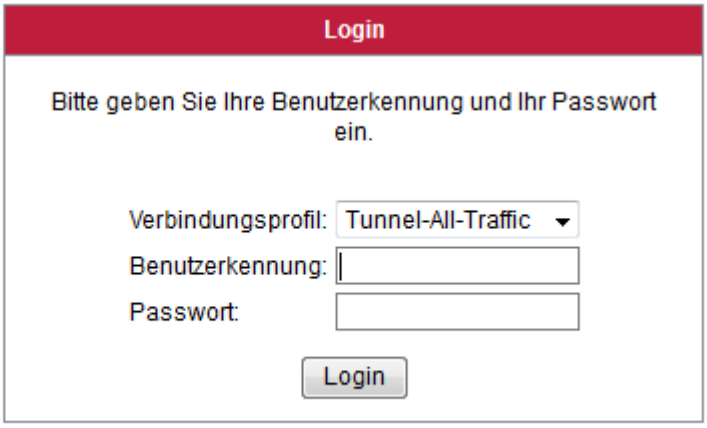
Der zentrale VPN-Dienst der TU Braunschweig ermöglicht es jedem Mitglied der TU Braunschweig, bestimmte Netze und Dienste der TU-Braunschweig auch mobil von unterwegs und von daheim per „Virtual Private Network“ (VPN) zu nutzen. Ziel des VPN-Dienstes ist es, Ihnen den Zugriff auf interne Ressourcen durch Bereitstellung einer IP-Adresse aus dem Netz der TU zu ermöglichen. Das Gauß-IT-Zentrum stellt Ihnen hierzu die notwendige Software zusammen mit der zugehörigen Konfiguration zur Verfügung. Die Software Cisco AnyConnect 3.0+ integriert sich nahtlos in die zentrale VPN-Infrastruktur der TU Braunschweig. Sie steht für mehrere Betriebssysteme in gleicher bzw. sehr ähnlicher Form bereit und integriert neben verschiedenen Zugriffsprofilen gleichzeitig verschiedene VPN-Protokolle. Die großen Vorteile liegen auf der Hand: Die über mehrere Betriebssysteme im wesentlichen gleichartige Software ist für Sie in der Bedienung auf den verschiedenen Betriebsystemen sehr ähnlich. Sie unterscheidet sich im Wesentlichen lediglich durch das Look&Feel des Betriebssystems. Um Ihnen den Einstieg so einfach wie möglich zu machen, haben wir in den folgenden Abschnitten die Installation und Nutzung der Software Cisco AnyConnect 3.0+ in den Abschnitten „Windows & Mac OS X“ sowie im Abschnitt „Linux“ beschrieben. Mit der Integration der Zugriffsprofile und der Möglichkeit mit nur einer Software zwischen den VPN-Protokollen IPSec und SSL-VPN auszuwählen können Sie durch einfache Auswahl in der Software Ihr Anwendungsszenario selbst bestimmen. Hinweise zur Nutzung der verschiedenen Profile finden Sie im Abschnitt „Auswahl der Profile“. Hinweise zur Nutzung und Auswahl der VPN-Protokolle finden Sie im Abschnitt „Wahl zwischen IPSec und SSL-VPN“.

Windows & Mac OS X

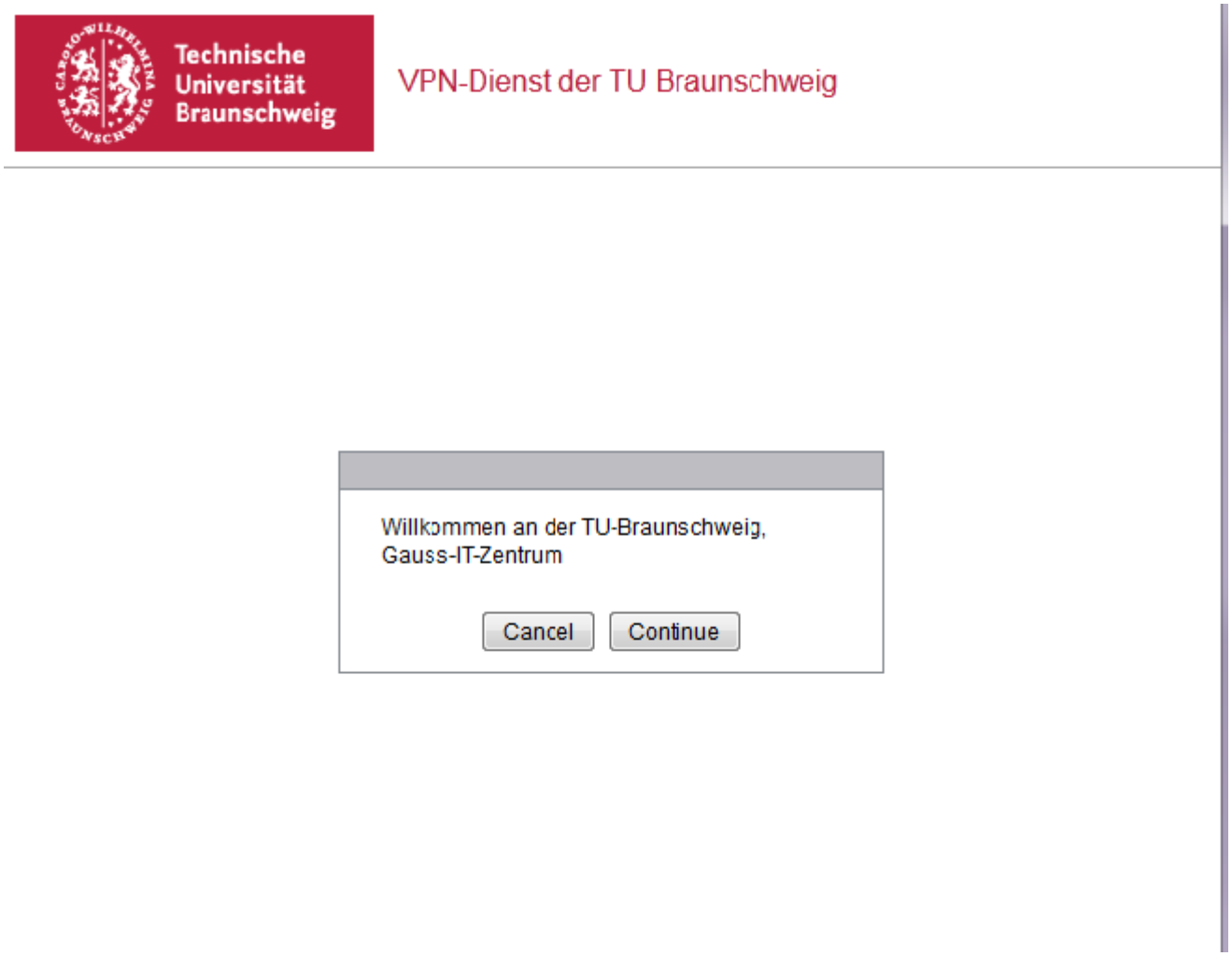
Unter Windows und Mac OS X gibt es zwei Möglichkeiten, den Anyconnect Client zu installieren. Die einfachste und schnellste Variante ist bei bestehender Internet-Verbindung die automatische Installation über den Webbrowser. Diesen Installationsweg sollten Sie einer manuellen Installation vorziehen. Sollten Sie den Client manuell installieren wollen, weil Sie beispielsweise zum Zeitpunkt der Installation keine Verbindung zum Internet haben, können Sie die Installationsdatei zuvor auch von unseren Webseiten herunterladen.

Automatische Installation über den Webbrowser

Öffnen Sie einen Webbrowser (z.B. Firefox) und gehen Sie auf die Seite **https://vpngate.tu-braunschweig.de**. Welches Profil Sie dort wählen, ist für die Installation nicht relevant. Sollten Sie VPN gleich nutzen wollen, wählen Sie das Profil, das Ihren Anforderungen entspricht. Siehe hierzu auch den entsprechenden Abschnitt zur Profilauswahl. Geben Sie Ihre **Benutzerkennung** (z.B. y-Nummer) und Ihr zugehöriges **Passwort** ein.



Im Folgenden Schritt sehen Sie eine Willkommensnachricht, die Sie in einem VPN-Netz begrüßt. (Diese kann auch anders lauten als im Screenshot angegeben). Drücken Sie den Knopf [**Continue**].

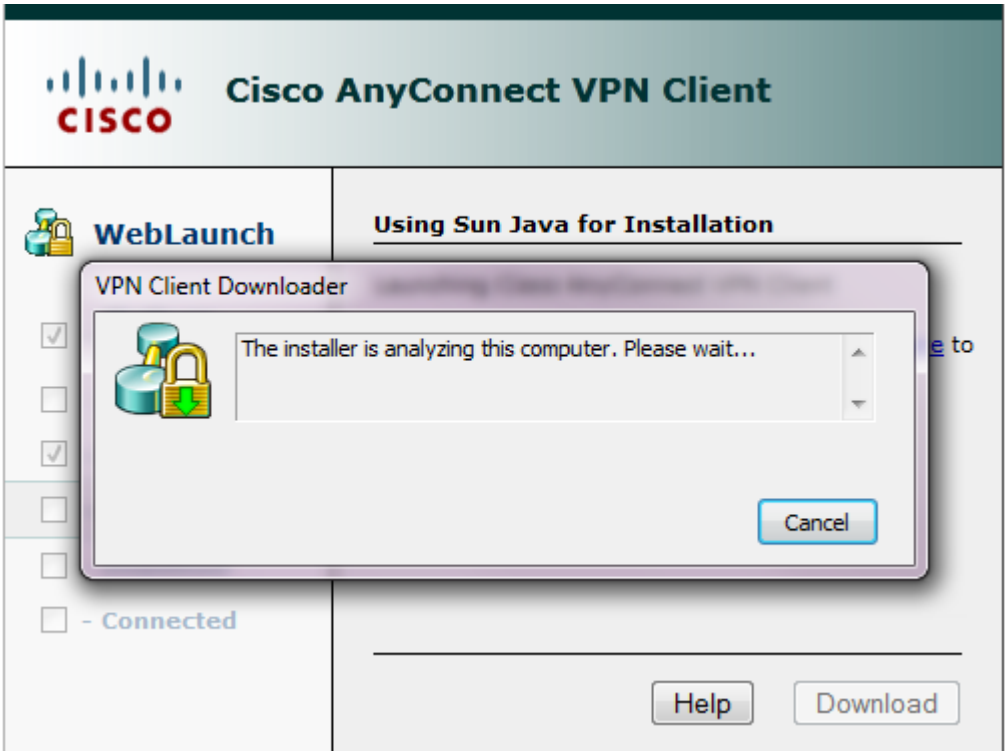


Der Cisco Anyconnect Client wird nun installiert (oder gestartet, falls dieser bereits installiert worden ist).

Im nächsten Schritt wird Ihnen eine Sicherheitsabfrage präsentiert. Hier geht es darum, dass Sie der

Installation der Software zustimmen. Klicken Sie [**Ausführen**]. Das Häkchen bei **Inhalten dieses Urhebers immer vertrauen** muss **nicht** gesetzt sein.

Es kann nun je nach der Güte Ihrer Internetverbindung einige Zeit dauern, bis der Client installiert ist.



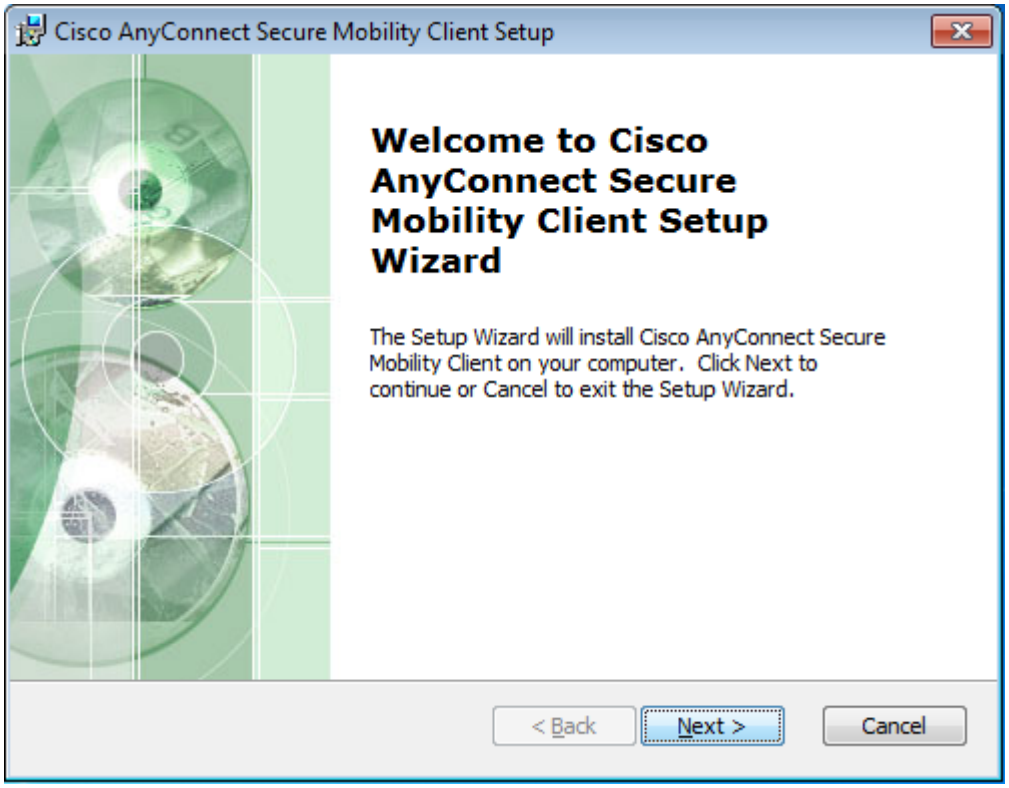
Nach der Installation startet sich der Client, minimiert sich dabei unter Windows aber gleich in die Taskleiste. Unter Mac OS X findet sich das zugehörige Icon oben in der Programmleiste.

Ein Click auf das Icon öffnet das Programmfenster des Clients. Hier können Sie u.a. die VPN-Verbindung trennen und erneut (z.B. mit anderem Profil) aufbauen. Wenn Sie den Client beendet haben, können Sie ihn zukünftig über die im jeweiligen Betriebssystem üblichen Wege zum Starten von Programmen starten. Das Starten bzw. Installieren über den Browser brauchen Sie nun nicht mehr.

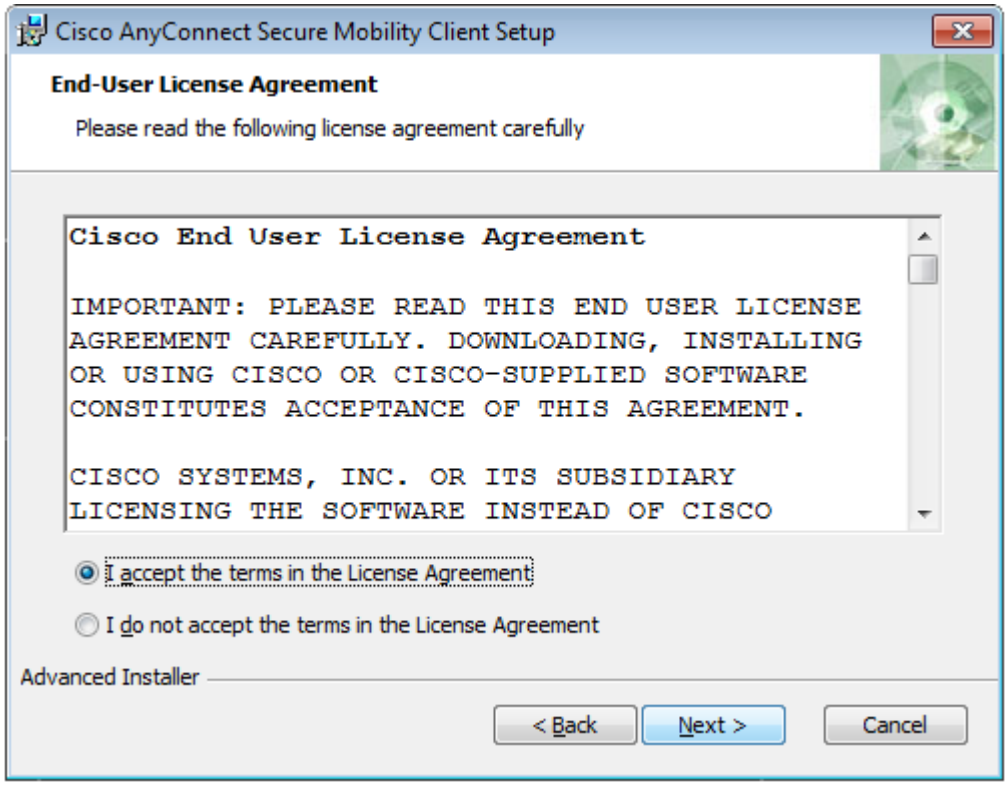
Manuelle Installation aus heruntergeladener Datei unter Windows

Zunächst laden Sie die Installationsdatei „anyconnect-win-<Version etc.>.msi“ für Ihr Betriebssystem unter https://www.tu-braunschweig.de/it/downloads/software bei „V“ für VPN herunter.

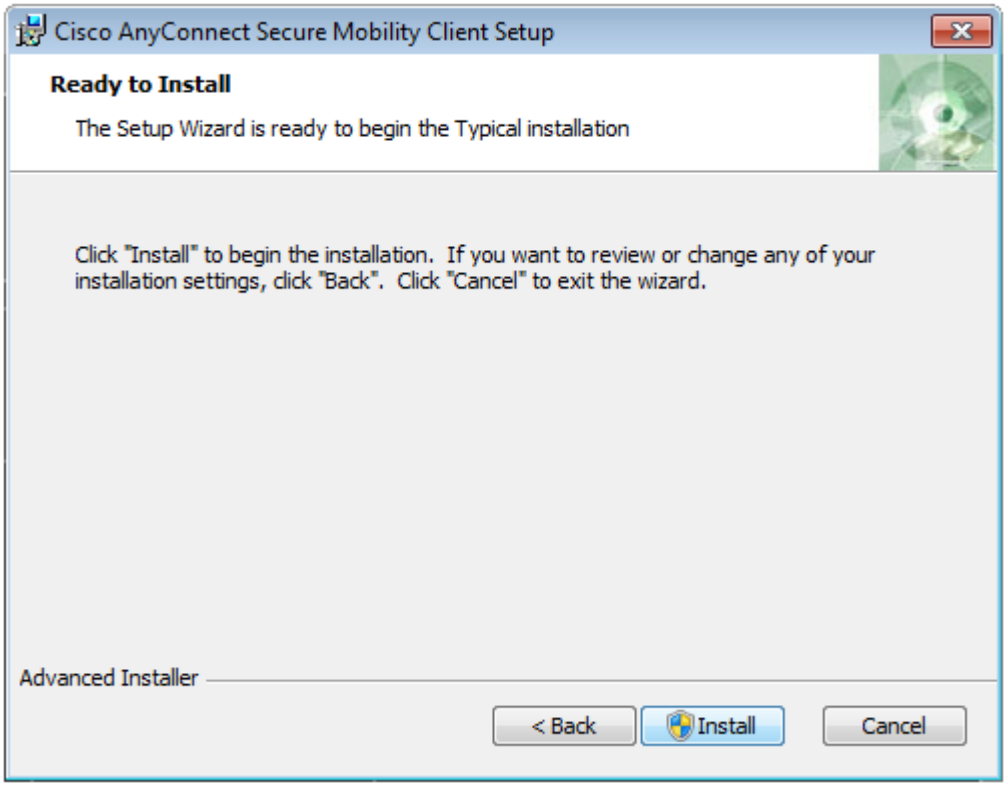
Um die Installation zu starten, klicken sie mit einem Doppelklick auf die Datei. Daraufhin erscheint das erste Installationsfenster. Klicken Sie dann auf die Schaltfläche „Next“, um die Installation fortzusetzen.



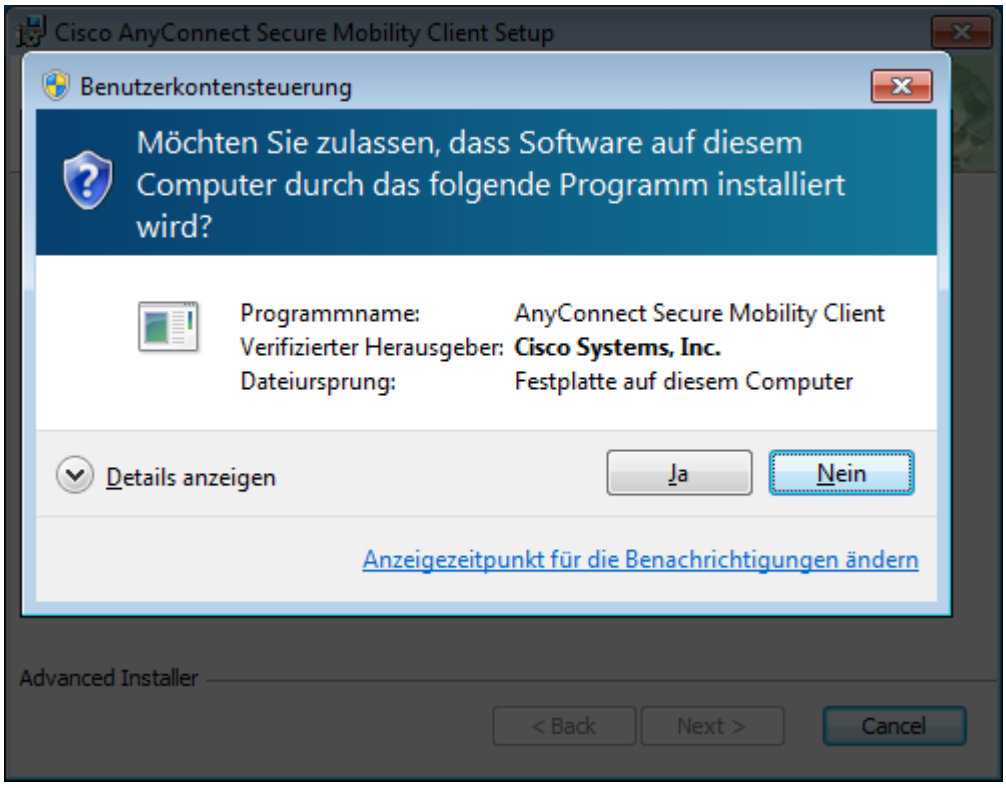
Im Folgenden werden Sie aufgefordert dem „Cisco End User License Agreement“ (der Lizenzvereinbarung) zuzustimmen. Klicken Sie „I accept the terms in the License Agreement“ und dann [**Next**], falls sie fortfahren wollen.



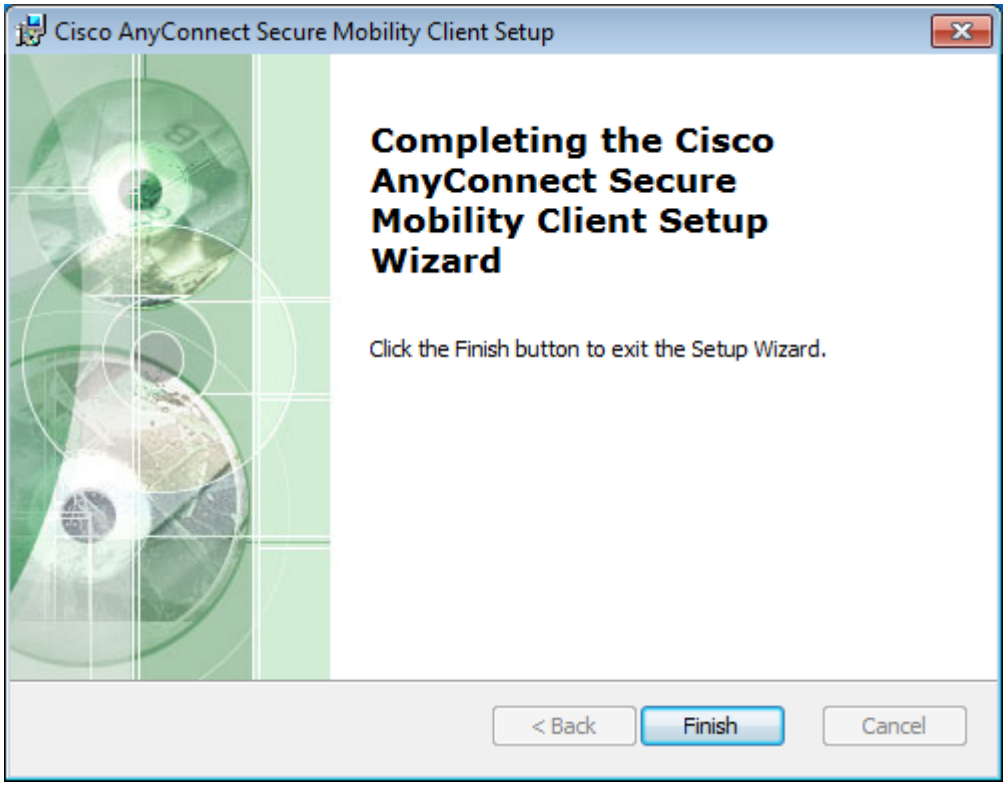
Sie können nun den Installationsvorgang starten, in dem sie auf die [**Install**]-Schaltfläche klicken.



Es kann sein, dass Ihre Sicherheitoptionen so eingestellt sind, dass Sie nun noch einmal aufgefordert werden, die Installation zu bestätigen. Bitte klicken Sie [**Ja**].



Wenn die Installation abgeschlossen ist, wird Ihnen das folgende Fenster gezeigt. Klicken Sie auf [**Finish**].



Die Installation ist nun abgeschlossen. Sie finden den Client fortan im Start-Menü unter **(Alle) Programme → Cisco Anyconnect Secure Mobility Client**.

Manuelle Installation aus heruntergeladener Datei unter Mac OS X

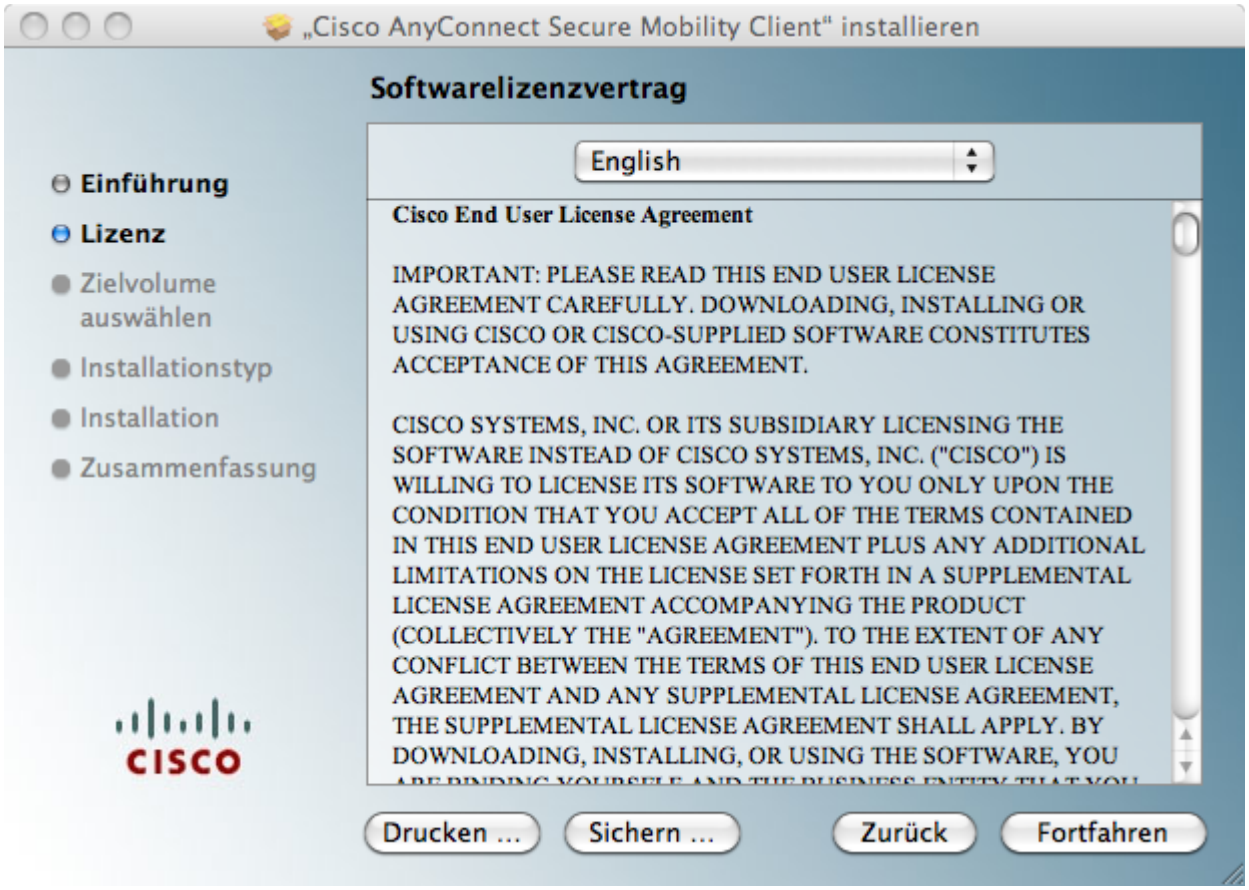
Zunächst laden Sie die Installationsdatei „anyconnect-macosx-i386-<Version>.dmg“ für Ihr Betriebssystem unter https://www.tu-braunschweig.de/it/downloads/software bei „V“ für VPN herunter.

Um, das Setup zu starten, müssen Sie das heruntergeladene Image über einen Doppelklick auf die Datei einbinden. Es öffnet sich folgendes Fenster:

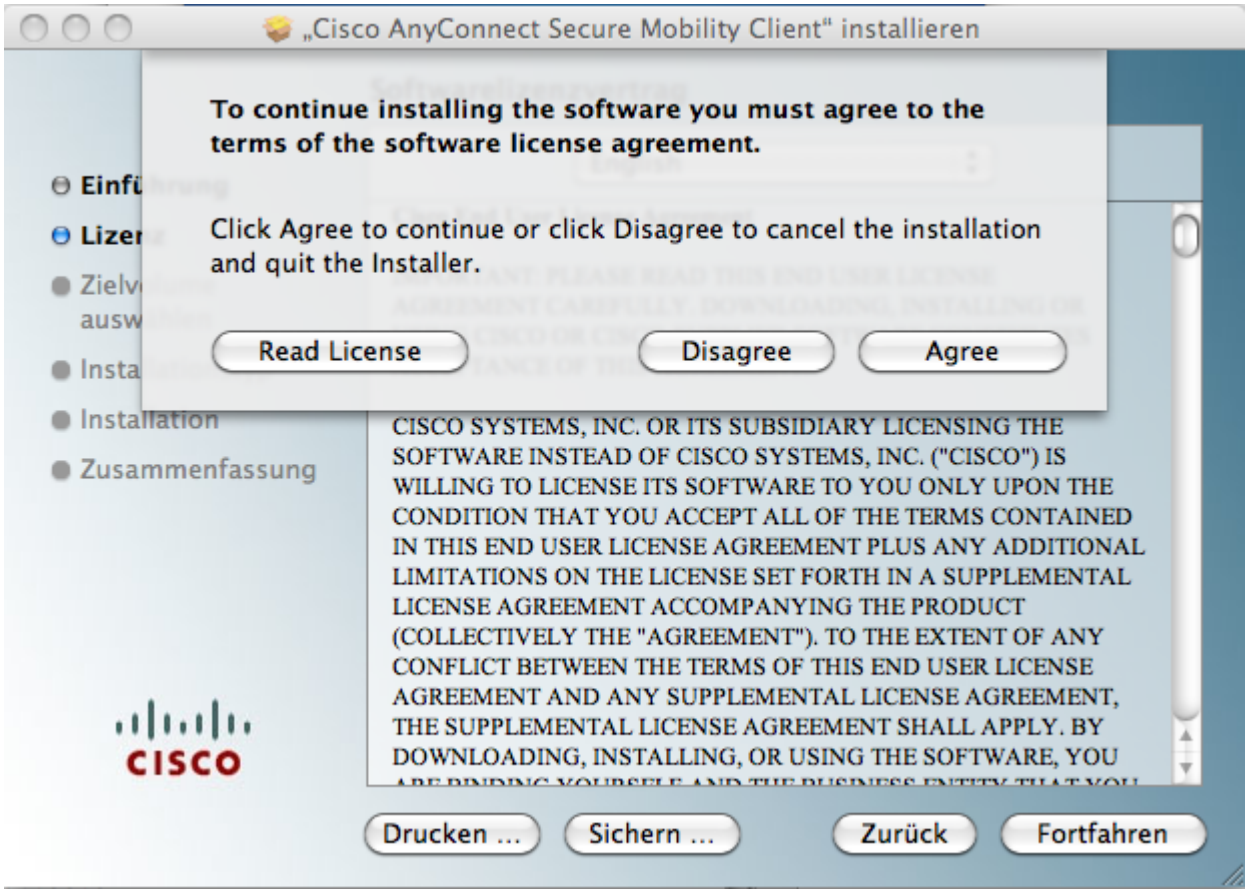
Führen Sie in diesem Fenster einen Doppelcklick auf das Paket-Icon „AnyConnect“ aus. Das Setup wird daraufhin gestartet.

Ein Popup informiert Sie darüber, dass das Setup Ihren Computer zunächst untersuchen wird, um festzustellen, ob eine Installation möglich ist. Bestätigen Sie diese Anfrage, indem Sie [**Fortfahren**] klicken.

Das Setup-Programm ist nun gestartet. Bitte klicken Sie erneut [**Fortfahren**]. Als nächstes müssen Sie der Lizenzvereinbarung zustimmen.



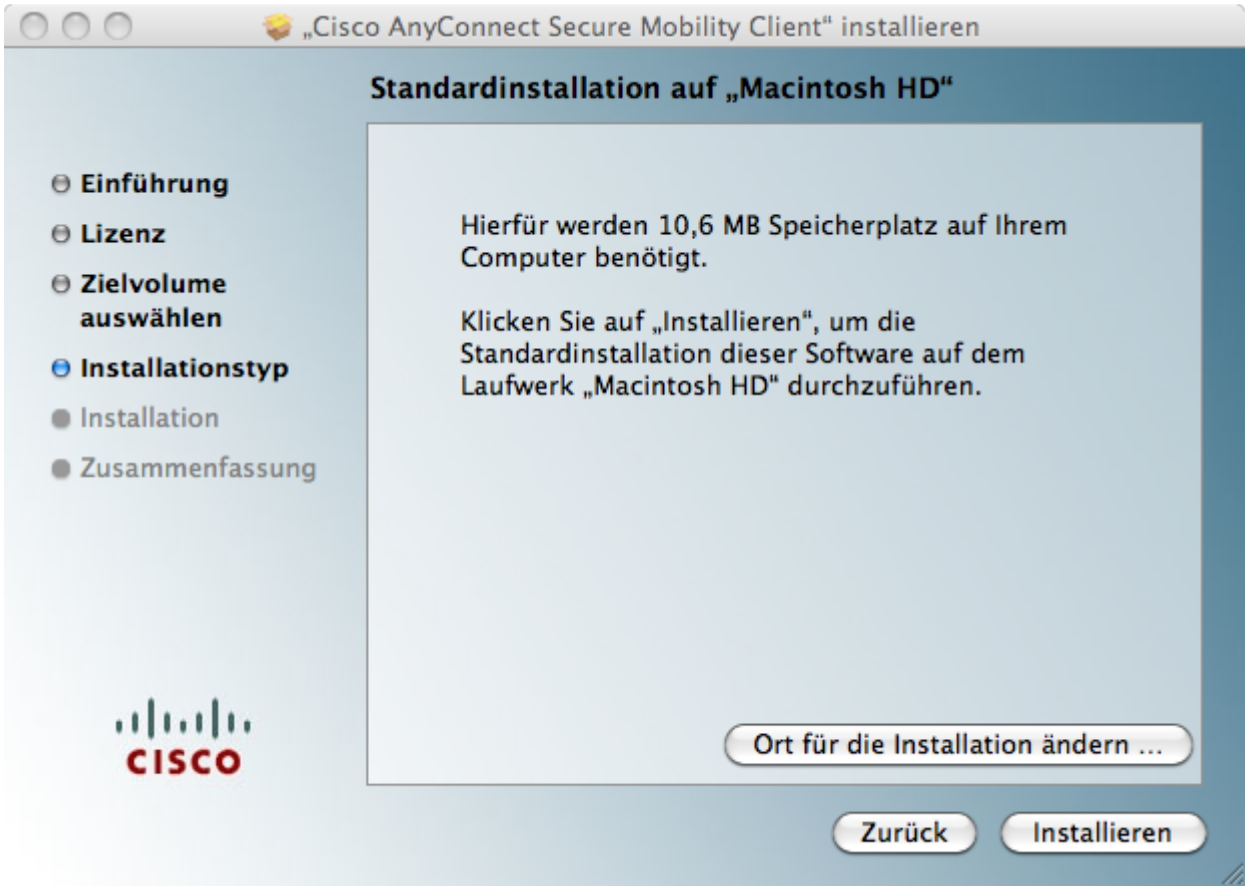
Klicken Sie hier [**Fortfahren**].



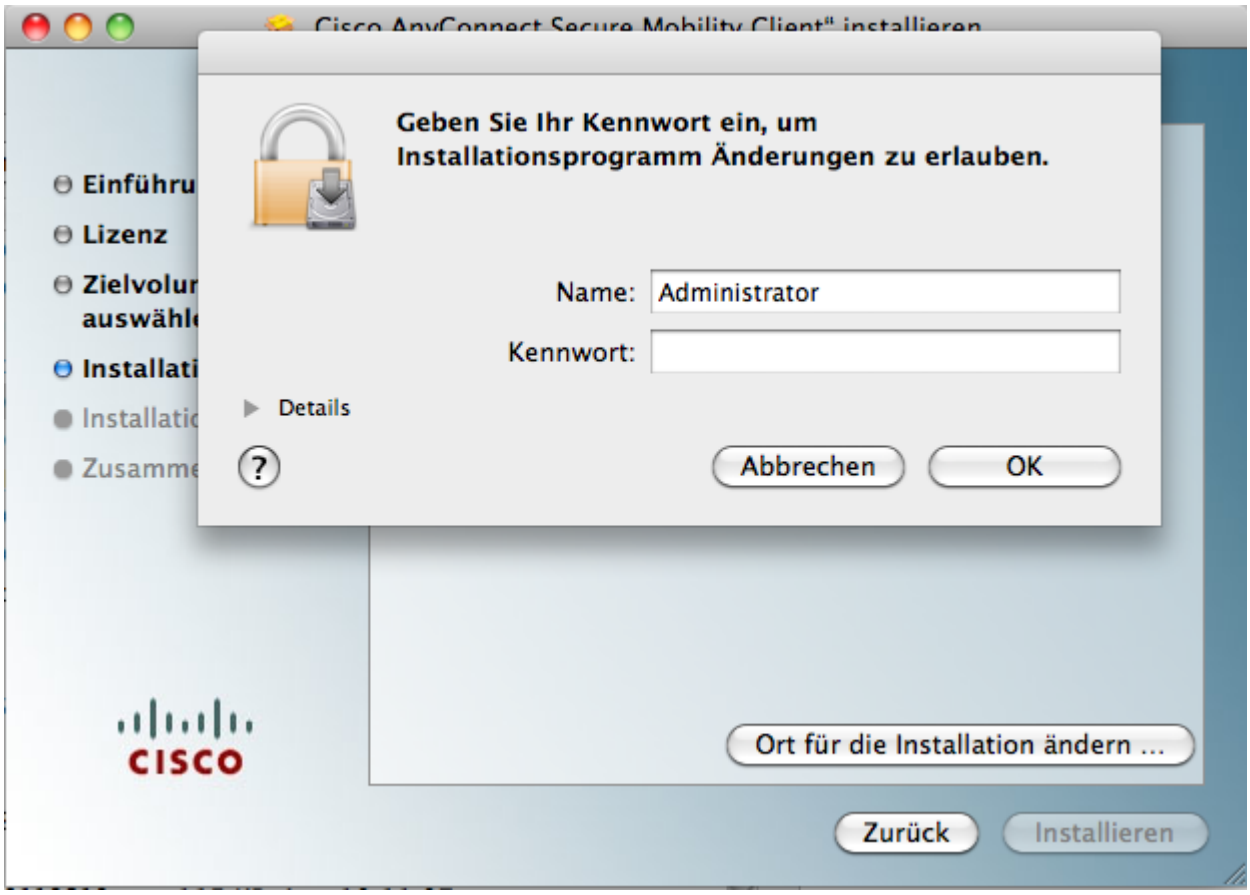
Bestätigen Sie die Lizenzvereinbarung, indem Sie auf [**Agree**] klicken. Im nächsten Schritt wählen Sie, welche Pakete Sie zusätzlich zum Anyconnect Client installieren wollen. Bitte belassen Sie das

Häkchen bei **Diagnostic and Reporting Tool**. Die Haken bei **Web Security** und **Posture** können Sie ggf. entfernen. (Hierzu nötige Dienste werden nicht unterstützt. Es sei an dieser Stelle auf den Virenscanner verwiesen.) Klicken Sie dann auf [**Fortfahren**].

Sie sind nun bereit, die Installation zu starten. Auf der folgenden Schaltfläche steht es Ihnen noch frei, den Ort für die Installation selbst festzulegen, indem Sie auf [**Ort für die Installation festlegen…**] klicken. Wenn Sie gleich auf [**Fortfahren**] klicken, wird der Client im Standardvolume (Festplatte) installiert.



Sie müssen nun das Login und Passwort für einen Administrator-Account Ihres Rechner eingeben, damit die Software installiert werden kann. Durch Klick auf [**Ok**] wird die Installation gestartet.



Die Installation dauert in der Regel weniger als eine Minute. Das Setup können Sie dann durch Klick

auf [**Schließen**] beenden.

Den Client finden Sie nun unter **Programme → Cisco → Cisco AnyConnect Secure Mobility Client**.

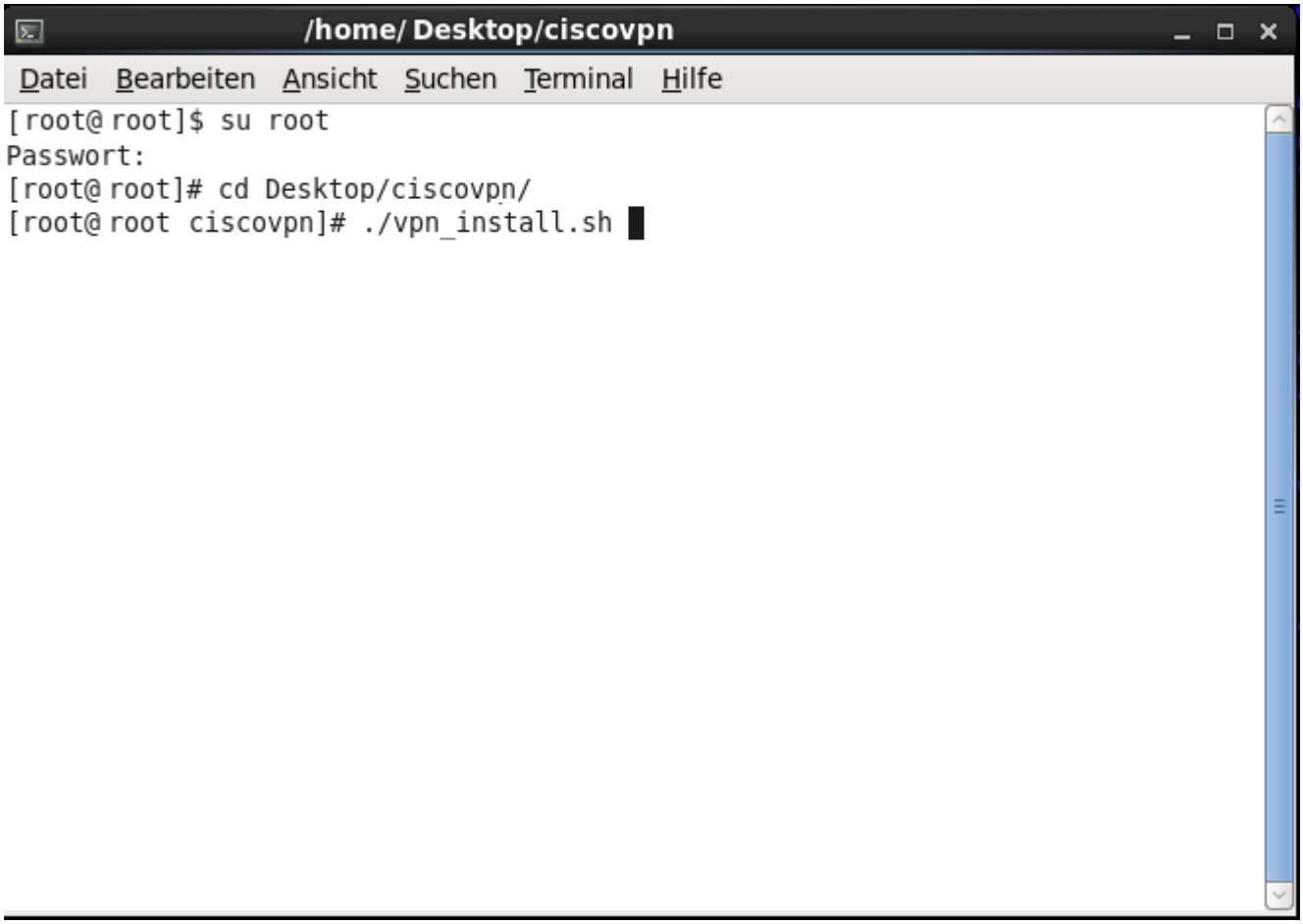
Linux

Unter Linux ist es meistens nicht möglich, den Client automatisch über den Browser zu installieren.

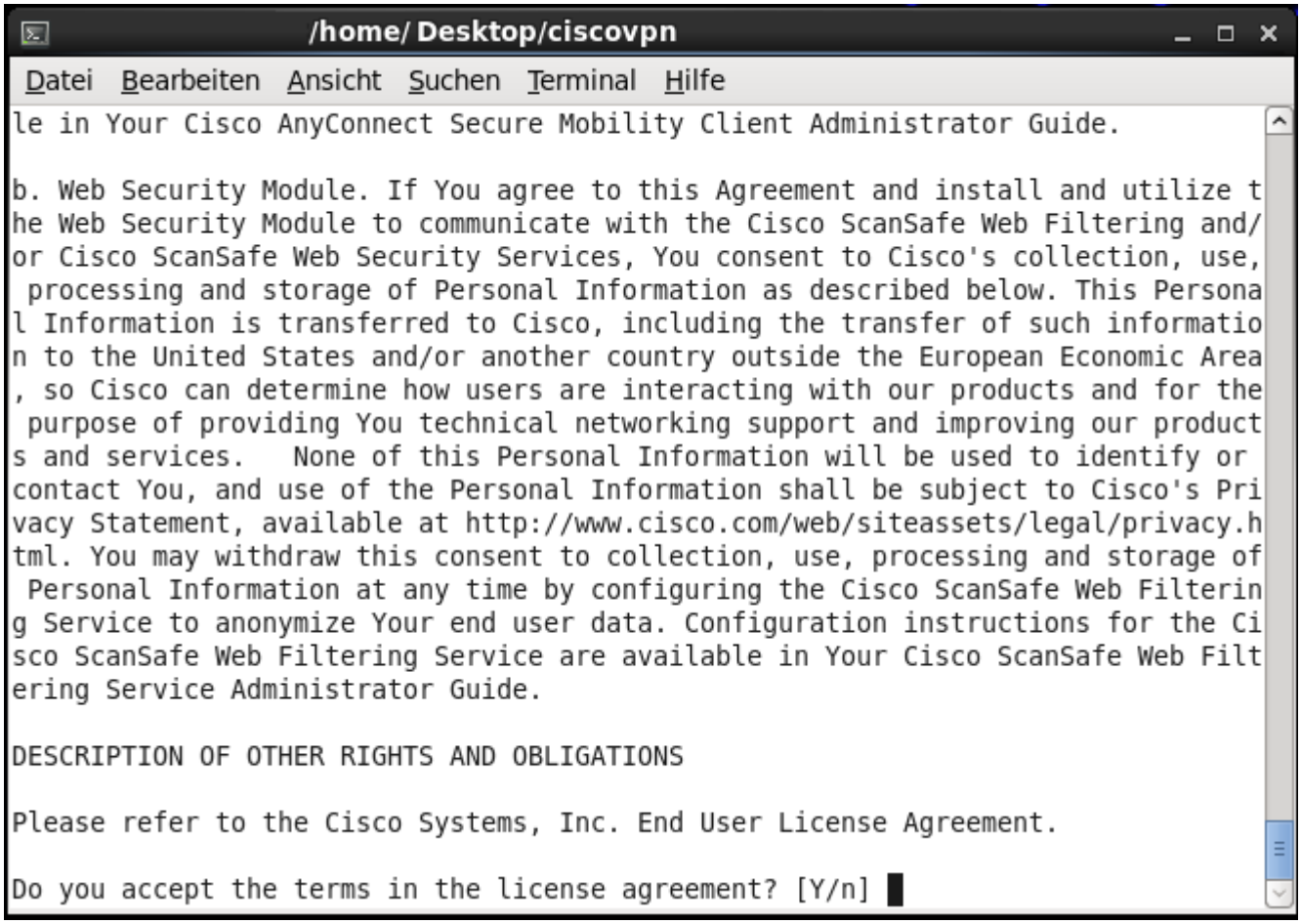
Manuelle Installation aus heruntergeladener Datei

Laden Sie den VPN Client „anyconnect-linux-<Version>.tar.gz“ (32bit) oder „anyconnect-linux-64-<Version>.tar.gz“ (64bit) von der Downloadseite des Gauß-IT-Zentrums (unter Software bei „V“ für VPN) herunter.

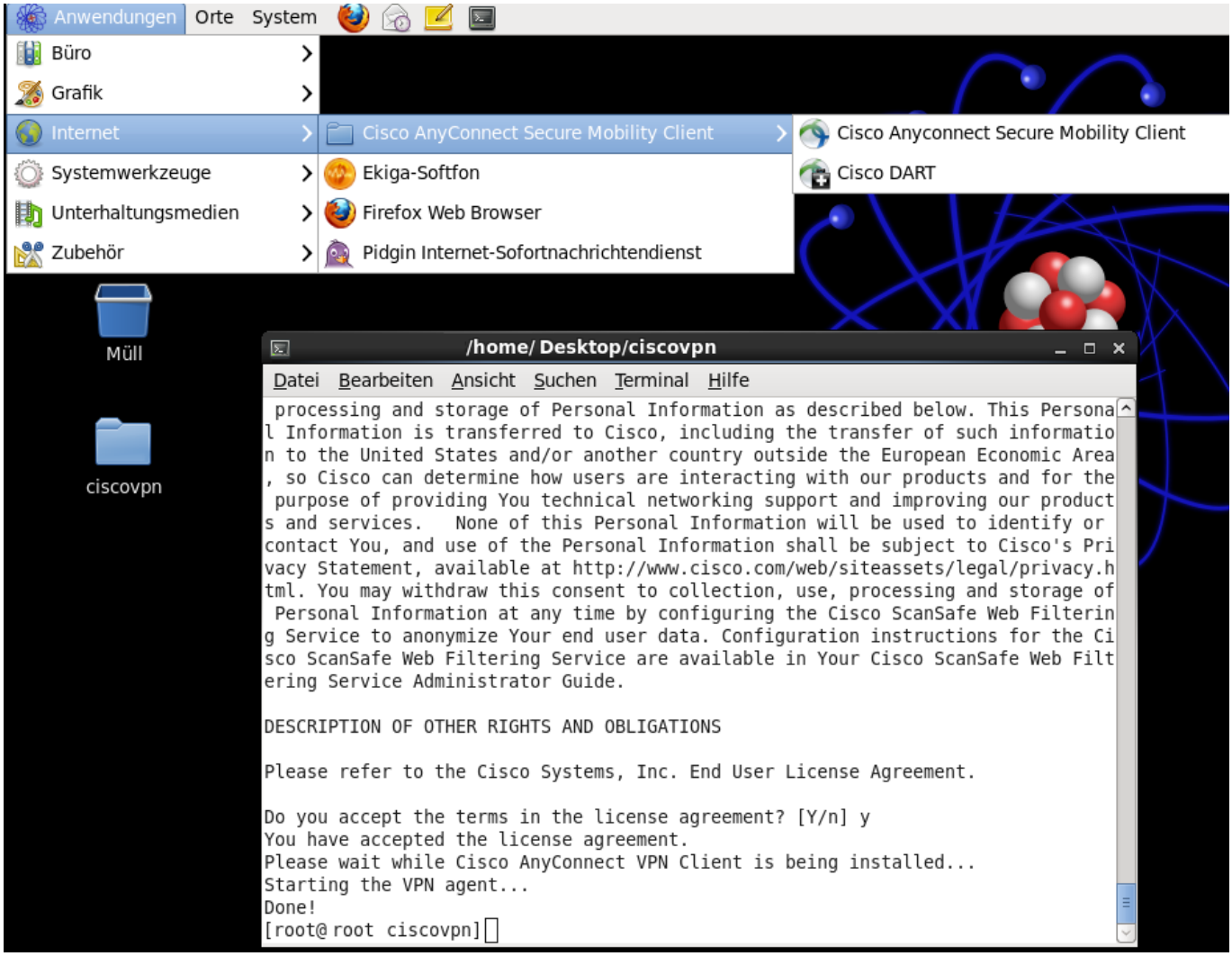
Entpacken Sie die Datei (z.B. im Terminal mit *„tar xvfz <Datei>“*). Falls nicht schon geschehen starten Sie ein Terminal und loggen Sie sich als root ein (z.B. mit dem Befehl *„su root“*). Wechseln Sie dann in das Verzeichnis in dem Sie die Datei entpackt haben **und dort in den Unterordner „vpn“**. Rufen Sie dort das Skript *vpn_install.sh* auf.



Lesen und bestätigen Sie das „End User License Agreement“ (Lizenzvereinbarung). Um die Vereinbarung zu bestätigen, drücken Sie die Taste *y* und bestätigen Sie mit [Enter].



Warten Sie bis sich das Skript mit der Ausgabe „Done!“ beendet. Der Client ist nun installiert. Aus welchem Menü Sie ihn starten können, ist abhängig vom Linux-Desktop, den Sie einsetzen. Unter Gnome2 finden Sie das das Programm z.B. unter „Anwendungen –> Cisco AnyConnect Secure Mobility Client –> Cisco AnyConnect Secure Mobility Client“.



In jedem Fall können Sie das Programm aber über die Kommandozeile öffnen:

```
/opt/cisco/anyconnect/bin/vpnui
```

Apple IOS und Android

Für Smartphones von Apple mit IOS Betriebssystem und Geräten anderer Hersteller mit Googles Android Betriebssystem finden Sie den Cisco AnyConnect Client im jeweiligen Anbieterportal:

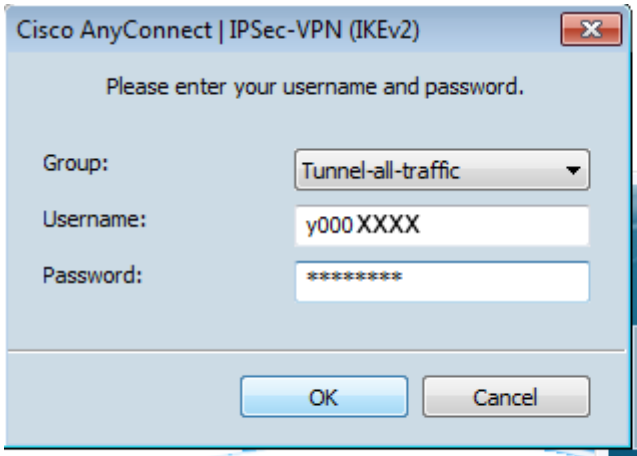
- Cisco AnyConnect im Apple App Store
- Cisco AnyConnect im Google Play Store

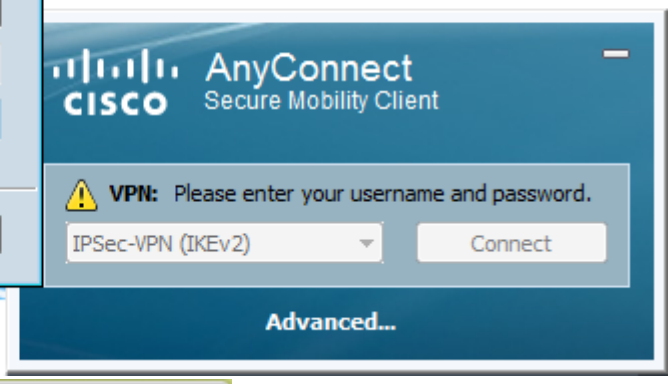
Die Benutzer von Apple-Geräten haben es besonders leicht, da die Monokultur der Hardware es der Softwareentwicklung bei Cisco ermöglicht, genau eine Version anzubieten. Benutzer von Android-Geräten müssen sich die für ihr Gerät passende Version anhand der Beschreibungen heraussuchen. Um eine Verbindung herzustellen, starten Sie bitte den Cisco AnyConnect auf Ihrem Smartphone. Wählen Sie für die erste Verbindung „Neue VPN-Verbindung hinzufügen…“ aus. Es öffnet sich der Verbindungseditor. Tippen Sie auf „Serveradresse“ und geben Sie „vpngate.tu-bs.de“ (oder vpngate.tu-braunschweig.de) in das Feld ein und bestätigen mit OK. In der Liste der verfügbaren Verbindungen erscheint nun „vpngate.tu-bs.de“. Starten Sie die Verbindung, indem Sie einen Eintrag

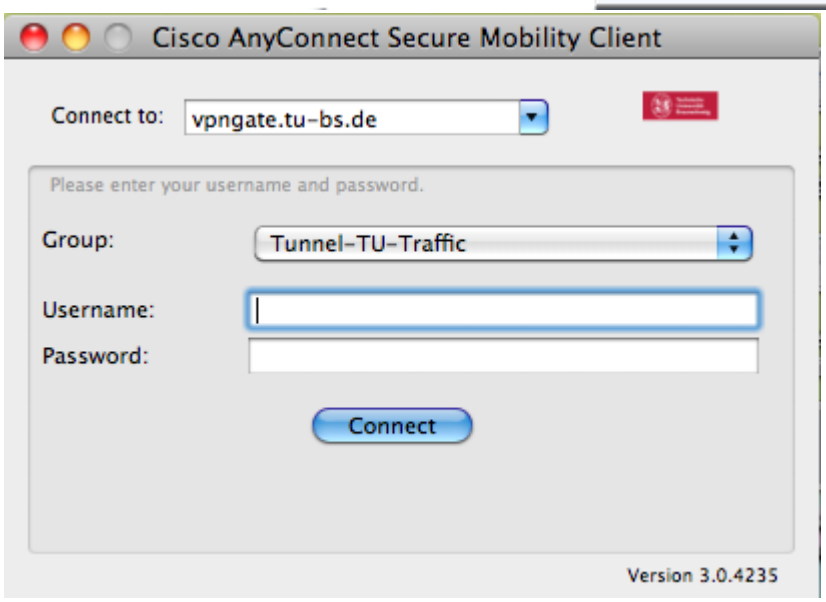
auswählen und ggf. auf den Schalter im Feld „AnyConnect-VPN“ (Apple) tippen. Sie werden nun aufgefordert, Benutzerkennung und Passwort einzugeben, um eine Verbindung herzustellen. Bei der ersten Verbindung werden Konfigurationsprofile heruntergeladen und in der Applikation hinterlegt. Zur Verwendung der Profile und zur Frage, welcher Verkehr über den VPN-Tunnel bedient werden soll, lesen Sie bitte in den entsprechenden Abschnitten VPN-Client "AnyConnect" nutzen, Wahl der Profile und Wahl zwischen IPSec und SSL-VPN dieser Anleitung nach.

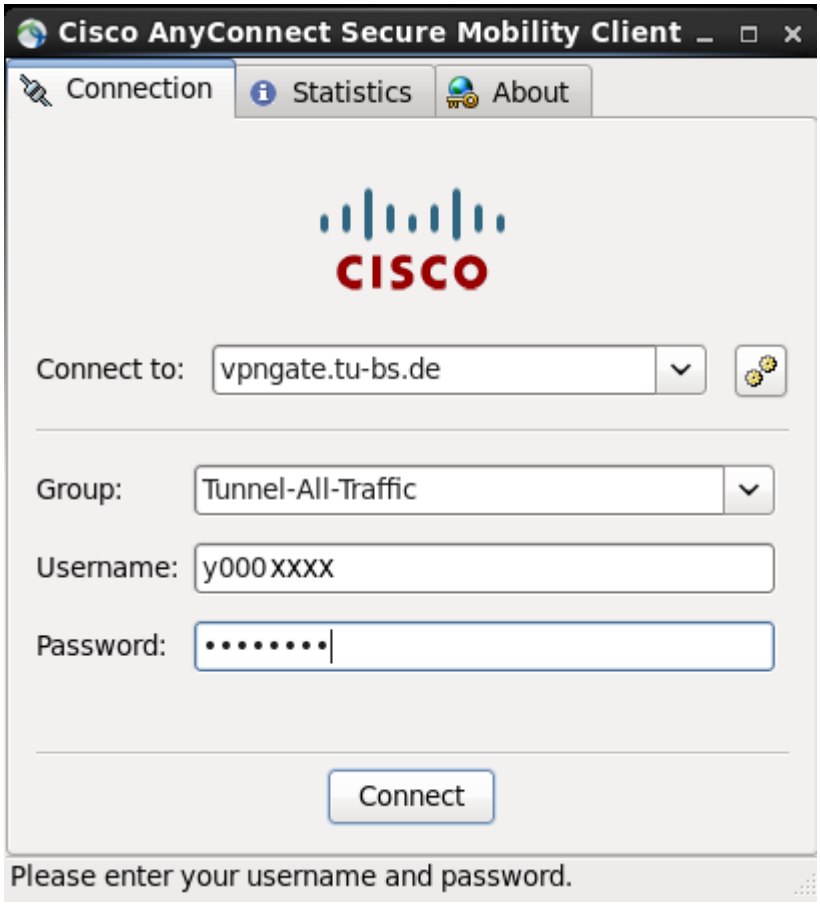
VPN-Client "AnyConnect" nutzen

Die Verwendung des Clients ist unabhängig davon, auf welchem Betriebssystem er installiert ist, oder ob er automatisch über den Browser oder manuell aus der Installationsdatei installiert wurde. Für die Verwendung ist ebenso unerheblich, wie der Client genau aussieht, was unter Mac OS X, Windows und Linux jeweils unterschiedlich ist. Auch die Versionen für Smartphones sehen naturgemäß unterschiedlich aus, als einzige Ausnahme folgen Sie bitte der Beschreibung im vorhergehenden Abschnitt. In dieser Anleitung werden wir daher nicht jeden Schritt mit einem Screenshot aller Versionen belegen, sondern uns an unterschiedlichen Beispielen orientieren. Hier zunächst ein kurzer Überblick über das unterschiedliche Aussehen der Clients unter den verschiedenen Betriebssystemen:

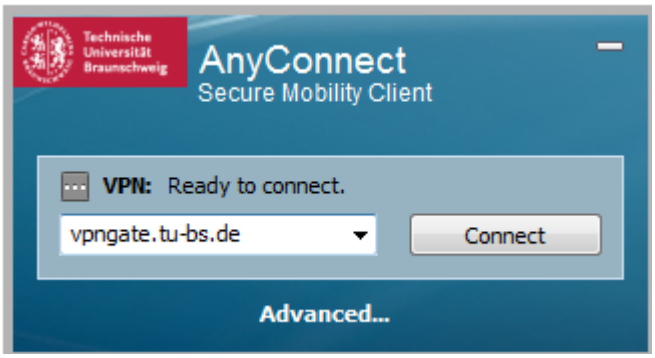

Cisco AnyConnect | IPSec-VPN (IKEv2)
Please enter your username and password.
Group:
Tunnel-all-traffic
Username:
y000 XXXX
Password:
****
OK
Cancel


AnyConnect
Secure Mobility Client
VPN: Please enter your username and password.
IPSec-VPN (IKEv2)
Connect
Advanced...

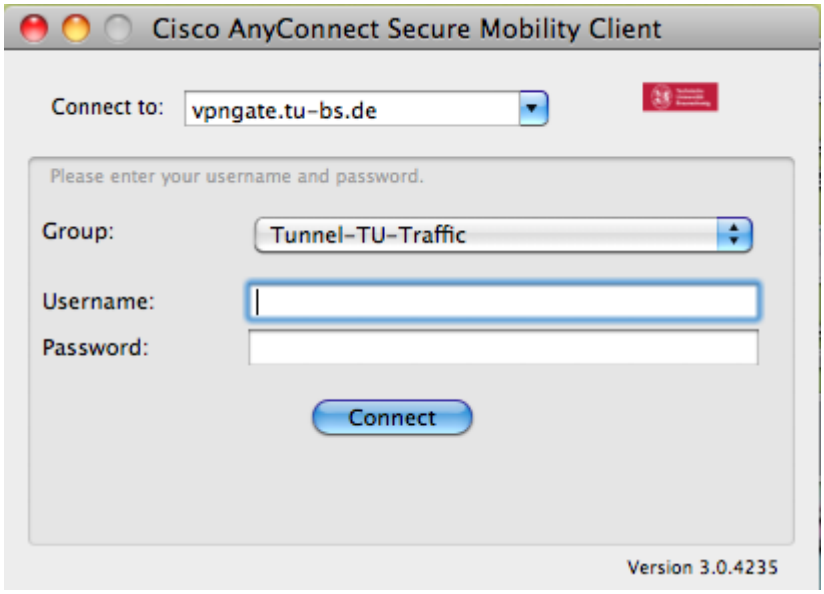

Cisco AnyConnect Secure Mobility Client
Connect to:
vpngate.tu-bs.de
Please enter your username and password.
Group:
Tunnel-TU-Traffic
Username:
Password:
Connect
Version 3.0.4235



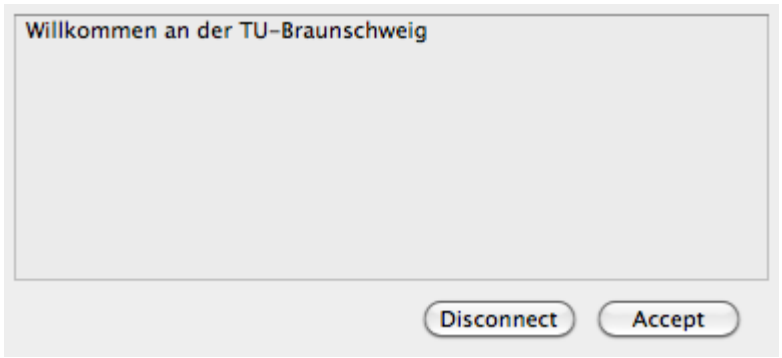
Wenn Sie den Client das erste Mal starten, müssen Sie im Feld **Connect to** den Hostnamen des VPN-Servers *vpngate.tu-bs.de* (oder *vpngate.tu-braunschweig.de*) eingeben.



Wenn die Felder für Benutzername (**Username**) und Passwort (**Password**) noch nicht gleich zu sehen sind, drücken Sie [**Select/Connect**]. Geben Sie dann Ihre Benutzerkennung und Ihr Passwort ein. Im Drop-Down-Menü [**Group**] können Sie zwischen den Profilen [**Tunnel TU Traffic**] und [**Tunnel all Traffic**] wählen. Beim Profil **Tunnel TU Traffic** werden nur solche Verbindungen über den Tunnel übertragen, die Ziele an der TU Braunschweig (IP-Adressbereich 134.169.*.*) betreffen. Wenn Sie wollen, dass sämtlicher Verkehr durch den Tunnel läuft (wie beispielsweise für Bibliotheksrecherchen notwendig), wählen Sie das Profil **Tunnel all Traffic**.



Wenn Sie nach Eingabe Ihrer Benutzerdaten und Auswahl des Profils den [**Connect**]-Knopf betätigen, wird der Tunnel aufgebaut. Als nächstes sehen Sie eine Willkommensnachricht, die sie noch mit [**Accept**] bestätigen müssen.



In der Regel verschwindet nun das AnyConnect-Fenster. Sie finden stattdessen ein Icon in der Task-/Programmleiste Ihres Desktops. Wenn Sie dieses Icon anklicken, öffnet sich das Fenster erneut.

Das Icon wird mit einem Schloss angezeigt, solange eine VPN-Verbindung besteht. Sobald Sie das Fenster öffnen und [**Disconnect**] drücken, verändert sich das Icon. Das Schloss ist nun nicht mehr zu sehen.

Wahl der Profile

An dieser Stelle wird noch einmal näher auf die verschiedenen Wahlmöglichkeiten zu den Profilen eingegangen. Zu verstehen, wie die verschiedenen Profile wirken, ermöglicht es Ihnen die Auswahl des Profils für Ihren Anwendungszweck zu optimieren. Die verschiedenen Profile sorgen für eine unterschiedliche Behandlung des von Ihrem Rechners initiierten Datenverkehrs. Sie benutzen VPN immer dann, wenn Sie z.B. mobil von unterwegs für den Zugriff auf interne Dienste und Ressourcen

eine IP-Adresse aus dem Netz der TU Braunschweig benötigen.

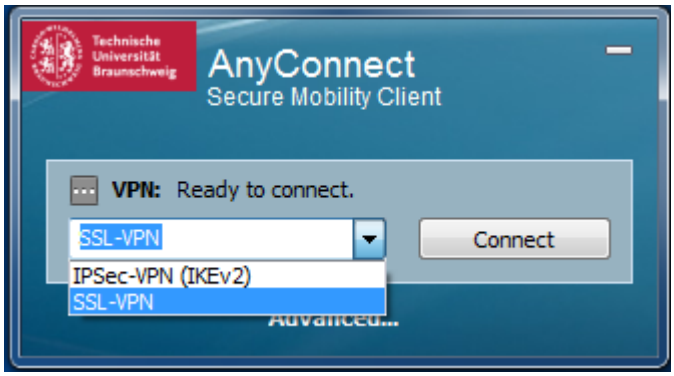
Profil „Tunnel TU Traffic“: Grundsätzlich sollten Sie dem Profil „Tunnel TU Traffic“ den Vorzug geben. Mit diesem Profil wird nämlich nur genau der Datenverkehr zwischen Ihrem Rechner und den TU-internen Diensten und Ressourcen verschlüsselt übertragen. Alle anderen Internetaktivitäten bleiben davon unberührt. Sie greifen weiterhin direkt auf andere Dienste (z.B. „www.google.de“) zu, ohne dass Ihr Datenverkehr einen zusätzlichen Umweg über Systeme der TU Braunschweig nimmt.

Profil „Tunnel all Traffic“: Für manche besonderen Anwendungen ist das Profil „Tunnel all Traffic“ auszuwählen. Beispielsweise kann für die Nutzung von Bibliotheksdiensten die Verwendung notwendig sein, da an Bibliotheken oft auf die Dienste anderer Verlage verweisen und zugegriffen wird. Das Profil „Tunnel all Traffic“ ist also nur dann notwendig, wenn es darauf ankommt, dass nicht nur der Zugriff auf TU-interne Dienste sondern auch der Zugriff auf externe Dienste mit einer IP-Adresse aus dem Netz der TU Braunschweig erfolgt. Diese Anforderung ist eher die Ausnahme.

Wahl zwischen IPSec und SSL-VPN

Mit dem AnyConnect Client in der Version 3 oder neuer haben Sie die Möglichkeit, nicht nur zwischen den Profilen **Tunnel-All-Traffic** und **Tunnel-TU-Traffic** zu wählen, sondern auch, ob der Tunnel über das IPSec-Protokoll hergestellt werden soll (**IPSec-VPN (IKEv2**), oder ob die Verschlüsselung auf Applikationsebene über SSL erfolgen soll (**SSL-VPN**). Während IPSec leichte Sicherheits- und Geschwindigkeitsvorteile hat, bietet SSL-VPN den Vorteil in 99% aller Netze und über alle Übertragungswege zu funktionieren, in denen auch das Ansurfen von SSL-geschützten Webseiten (https) möglich ist.

Die Wahl zwischen IPSec und SSL haben Sie erst, nachdem Sie mindestens einmal wie oben beschrieben einen Tunnel zu vpngate.tu-bs.de aufgebaut hatten. Dieser erste Tunnel wird immer über SSL hergestellt. Dabei wird vom Server eine Konfigurationsdatei heruntergeladen, die Ihnen ab dem nächsten Start des Clients in der Zeile **Connect To** ein Drop-Down-Menü anbietet.

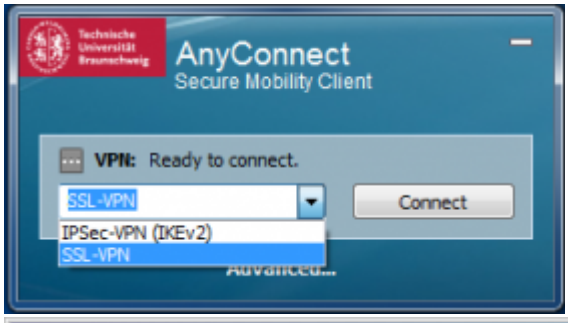


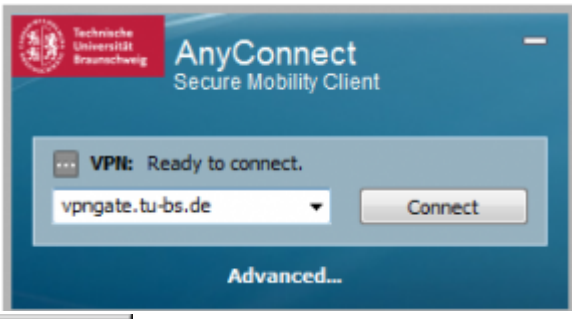
Danach ist die Verwendung des Clients ganz genauso wie oben beschrieben. Sowohl bei SSL als auch bei IPSec können Sie noch zwischen den Profilen Tunnel-All-Traffic und Tunnel-TU-Traffic wählen.

VPN an anderen Einrichtungen nutzen

Wenn Sie an mehr als einer Einrichtung den AnyConnect VPN-Client benutzen müssen oder sollen,

dann können Sie dies ohne erneute Installation des Programms tun. Starten Sie den Client. Klicken Sie in das Feld „Connect to:“ bzw. „VPN: Ready to connect:“ hinein und Tippen Sie den Namen des neuen VPN-Servers in das Feld.





Die vorstehenden Abbildungen von verschiedenen Betriebssystemen sollen eines verdeutlichen: Statt der vorkonfigurierten Werte läßt sich in das Feld jederzeit der Name eines anderen VPN-Servers eintragen zu dem man Verbindung aufbauen möchte und der Verbindungen über den AnyConnect Client zuläßt.