

Cisco VPN Client

VPN Personeel - Hogeschool Gent

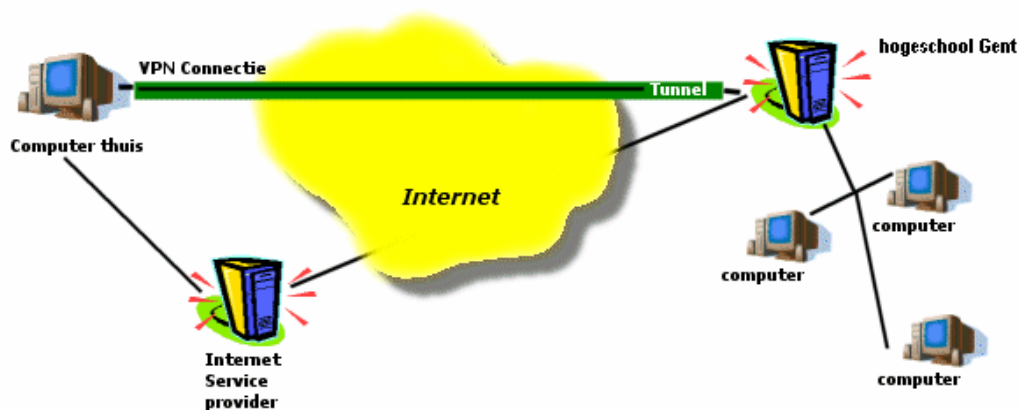
Inleiding

Wat is VPN?

VPN (Virtual Private Networking) is een techniek om een bedrijfsnetwerk te ontsluiten op een veilige manier. Hierdoor kunnen personeelsleden met een internetverbinding thuis toegang krijgen tot de netwerkfaciliteiten (o.a. de bestuursdocumenten op hnet.hogent.be of puntenprogramma tijdens examenperiode...) van de Hogeschool Gent.

Een Virtual Private Network (VPN) verbinding is een veilige manier om een bedrijfsnetwerk uit te breiden door middel van een gedeelde infrastructuur. Op deze manier kan hetzelfde beleid ten aanzien van beveiliging, beheer en netwerkprestaties gelden zodat u kan werken alsof u lokaal op de Hogeschool Gent zit.

Om de vertrouwelijkheid van gegevens en de compatibiliteit van netwerken te waarborgen, zenden VPN's informatie door een versleutelde 'tunnel'. De tunnels die ervoor zorgen dat VPN's veilig zijn, worden opgezet door VPN Client software op een PC of laptop en aan de andere kant van de verbinding door een VPN Gateway. De VPN Client en Gateway zorgen voor versleuteling en ontsleuteling van gegevens zodat buitenstaanders deze niet kunnen bekijken of bewerken. Een VPN is daardoor een goed en voordelig systeem voor wie gebruik wil maken van de netwerk- en informaticafaciliteiten van de Hogeschool Gent thuis.



Cisco VPN Client

De Cisco VPN client is nu de enige ondersteunde VPN Client die kan gebruikt worden met het C² project. Alle andere VPN software is incompatibel met dit project. We raden aan tenminste versie 4.6 te installeren van de Cisco VPN Client. Volg onderstaande instructies om de client te downloaden, installeren en te configureren.

Deze handleiding

Wat kan u erin vinden?

Deze handleiding is geschreven voor het personeel van de Hogeschool Gent en bevat de installatie- en configuratieprocedure van de Cisco VPN software.

Er zijn twee versies van deze handleiding:

- Cisco vpn v4.doc: versie mét logingegevens om het configuratieprofiel te kunnen downloaden; enkel te verkrijgen via e-mail op aanvraag bij de helpdesk (helpdesk@hogent.be). In het document te herkennen aan “MET LOGIN” bovenaan rechts elke pagina.
- Cisco vpn v4_nopw.doc: versie zonder logingegevens om het configuratieprofiel te kunnen downloaden. Te vinden op de website van de helpdesk (<http://helpdesk.hogent.be>) of op public op webs (<http://webs.hogent.be/public/HOGENT/vpn>). Beide websites zijn enkel bereikbaar vanaf het interne netwerk van de Hogeschool Gent, dus niet vanaf het internet! In het document te herkennen aan “ZONDER LOGIN” bovenaan rechts elke pagina.

Controleer vooraleer u wil beginnen welke handleiding u heeft. Indien u dit document thuis zit te lezen, maar het is de versie zonder paswoorden, kan u de installatie en configuratie van de Cisco VPN client niet volledig uitvoeren (u kan de software niet eens downloaden). Stuur een e-mail naar helpdesk@hogent.be met uw officieel hogent.be adres voor de versie met logingegevens.

Deze handleiding omvat uitleg over volgende zaken:

1. De oude niet Cisco VPN software verwijderen;
2. De Cisco VPN Client software versie 3 verwijderen;
3. De nieuwe VPN software en profielbestand downloaden;
4. De nieuwe VPN software installeren;
5. De nieuwe VPN software configureren;
6. De nieuwe VPN software testen.

U dient voor deze handleiding volgende zaken onder de knie te hebben:

- Algemene kennis Windows (of uw geïnstalleerd besturingssysteem);
- Algemene internetkennis (surfen, downloaden);

LET OP: INDIEN U DIT TYPE MEDEDELING ZIET, LEES HEM DAN GRONDIG. HET BEVAT MEESTAL KRITIEKE INFORMATIE.

Besturingssystemen

De Cisco VPN client is beschikbaar voor de drie meest gebruikte besturingssystemen nl. Microsoft Windows, Apple Mac OS X en Linux.

Voor Microsoft Windows leest u gewoon verder, de handleiding gaat er vanuit dat u met dit besturingssysteem werkt. Er kunnen echter wel kleine verschillen optreden tijdens het downloaden, installeren en configureren, zowel in de beschrijving als de screenshots.

Voor Apple Mac OS X dient u enkel voor de (de)installatie van de Cisco VPN Client naar een apart deeltje te gaan iets verder in deze handleiding; downloaden, configureren en testen gebeurt op dezelfde manier als in Windows.

Deze handleiding geeft geen extra uitleg voor de installatie en configuratie onder Linux. Wel dient u de paragraaf over het downloaden van het profielbestand te lezen zodat u de Linux VPN client kan configureren.

LET OP: DE SCREENSHOTS IN DIT DOCUMENT ZIJN AFKOMSTIG VAN DE ORIGINELE VERSIE VAN DE CISCO VPN CLIENT EN KUNNEN IETWAT VERSCHILLEN MET DE VERSIE DIE U GEBRUIKT. VOLG ALTIJD DE GESCHREVEN INSTRUCTIES!

Andere informatiebronnen

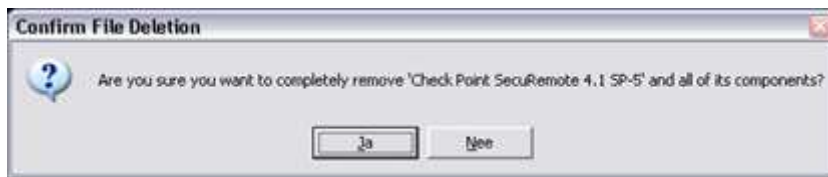
- <http://helpdesk.hogent.be/vpn>: de VPN helpdesk website van de Hogeschool Gent.
- <https://webs.hogent.be/ciscovpn>: website met de VPN software, handleidingen en profielbestand. Deze website is enkel bereikbaar met logingegevens en enkel voor het personeel! De logingegevens kan u vinden in een speciale versie van deze handleiding die u moet aanvragen bij de helpdesk (helpdesk@hogent.be). Deze handleiding wordt enkel naar officiële hogent.be e-mailadressen gestuurd.
- <http://webs.hogent.be/public/HOGENT/vpn>: website met de VPN software en de open handleidingen. Enkel bereikbaar binnen het Hogeschool Gent netwerk of met VPN.
- helpdesk@hogent.be: Indien u problemen heeft of de versie handleiding met paswoorden wil, dient u hier naartoe te mailen met uw Hogeschool Gent e-mailadres!

Procedures

Deïnstallatie oude 'niet' Cisco VPN software

Indien u nog de oude VPN software gebruikt hebt en deze dus geïnstalleerd staat op uw computer, moet u deze eerst verwijderen. Dit doet u door volgende stappen te volgen:

1. Ga naar het Configuratiescherm (START > Configuratiescherm).
2. Dubbelklik op Software.
3. In de lijst van geïnstalleerde software zoekt u: "CheckPoint SecuRemote".
4. Klik op "wijzigen/verwijderen" om de software te verwijderen.
5. Klik op "Ja" om CheckPoint SecuRemote te verwijderen. Indien er een dialoog venster komt met als titel "Confirm Shared File?", dan klikt u op "Yes to All" en vervolgens weer op "Yes".



6. De computer deïnstalleert nu de software en vraagt eventueel om te herstarten.
7. Herstart de computer om er zeker van te zijn dat de software volledig verwijderd is!

Deïnstallatie oude Cisco VPN software

Voor u de laatste versie van de Cisco VPN Client mag installeren, dient u eerst de oude versie te deïnstalleren.

Volg volgende stappen zo nauwkeurig mogelijk:

8. Ga naar START > Configuratiescherm > Software.
9. Selecteer Cisco VPN Client (of Dialer).
10. Druk op "wijzigen/verwijderen".
11. Volg de Wizard die verschijnt door steeds op "Next" te drukken.
12. Op het einde van het deïnstallatieproces drukt u op "Finish" en start u de pc opnieuw op indien dit wordt gevraagd.

Na het heropstarten van de pc kan u beginnen met het downloaden, installeren en configureren van de laatste versie (> 4).

Downloaden van de laatste Cisco VPN software

De laatste versie van de Cisco VPN Client die door ons is getest zit altijd onder onderstaande links. Maak een internetverbinding en klik op de link die bij uw besturingssysteem past.

- <https://webs.hogent.be/ciscovpn/software/vpnclient-LATEST-windows.exe>: Windows 95/98/ME/2000/XP/2003, Windows XP 64-bit is NIET gesupporteerd.
- https://webs.hogent.be/ciscovpn/software/vpnclient-LATEST-darwin_2-3.dmg: Darwin OS X versie 10.2-10.3.x.
- <https://webs.hogent.be/ciscovpn/software/vpnclient-LATEST-darwin.dmg>: Darwin OS X versie 10.4 voor PPC en x86 (Intel) platformen.
- <https://webs.hogent.be/ciscovpn/software/vpnclient-LATEST-linux.tar.gz>: Linux vanaf kernel 2.4, GLIBC_2.2 & libstdc++.so.5 moeten geïnstalleerd zijn (geen helpdesk ondersteuning!)

Indien er wordt gevraagd om login en wachtwoord geeft u volgende waarden op:

- Loginnaam: ***** (indien dit '*' tekens zijn, heeft u een handleiding ZONDER LOGIN, gelieve de helpdesk helpdesk@hogent.be te contacteren voor een handleiding MET LOGIN!)
- Wachtwoord: *****

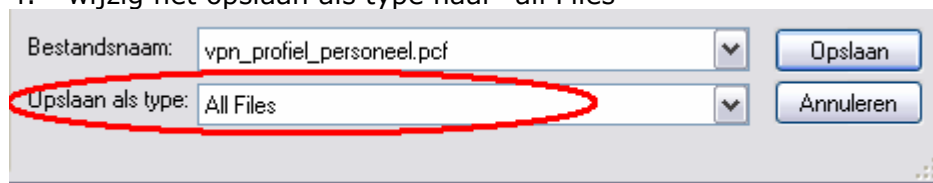
LET OP: DEZE GEGEVENS ZIJN ENKEL GELDIG VOOR DE SOFTWARE TE DOWNLOADEN. ZE HEBBEN GEEN NUT VOOR HET PROGRAMMA ZELF!

Sla het bestand op op uw harde schijf, liefst in een tijdelijke map.

Downloaden van het profielbestand

Na het downloaden van het installatiebestand dient u nu nog het profielbestand te downloaden. Dit is het bestand dat uw VPN software zal configureren. Volg onderstaande stappen:

1. Surf naar volgende link: <https://webs.hogent.be/ciscovpn/profielen/>
2. Klik met de rechter muisknop op de link **vpn_profiel_personeel.pcf**
3. Kies bestand opslaan als
4. wijzig het opslaan als type naar "all Files"



5. Sla dit bestand op op dezelfde locatie als het installatiebestand van de VPN client zodat u het later snel kan weervinden.

Na het downloaden van dit bestand, kan u verder gaan met de installatie van de Cisco VPN Client.

Installatie van de VPN software

Voor u kan beginnen aan de installatie dient u eerst volgende zaken in acht te nemen:

- De installatieprocedure kan verschillen tussen verschillende versies van Microsoft Windows besturingssystemen vertonen. Daarom kunnen screenshots in deze handleiding en ook bepaalde stappen van de installatie op uw pc licht afwijken van wat er in deze handleiding neergeschreven staat.
- De computer waarop u de VPN Software op installeert mag niet voorzien zijn van een Microsoft Firewall ("IPSEC-services"). Indien het installatieprogramma vraagt of u deze wilt uitschakelen, dient u op "ja" te klikken! Zie achteraan dit document bij "problemen en oplossingen" voor meer uitleg.
- De Cisco VPN software is niet compatibel met Internet Connection Sharing op Windows 98SE en Windows ME. Zie "Problemen en Oplossingen, achteraan deze handleiding voor meer informatie!
- Indien er zich foutmeldingen voordoen tijdens de installatie, configuratie of het uitvoeren van het programma, kan u best eens naar "Problemen en Oplossingen" gaan, achteraan deze handleiding. Daar staan de meest gekende problemen omtrent deze software.

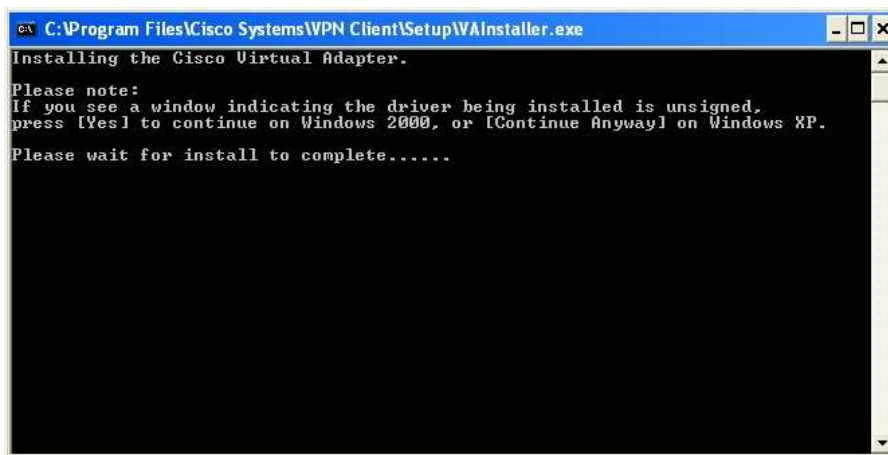
Volg onderstaand stappenplan nauwkeurig om de Cisco VPN v4 client te installeren.

1. Open Windows Verkenner en ga naar de locatie waar u het installatiebestand heeft gedownload. Dubbelklik op het bestand.
2. Er komt een dialoogvenster (zie figuur rechts) te voorschijn dat u vraagt een locatie op te geven waar u de bestanden naar wil uitpakken. Kies bvb. c:\temp en klik "uitpakken".



In de map die u gekozen heeft, worden nu enkele bestanden gezet.

3. Normaalgezien vraagt het programma nu of het "setup.exe" mag opstarten. Druk op "Ja" om de installatie te starten. Indien er niets gebeurt, dient u zelf naar de desbetreffende map te gaan en te dubbelklikken op het bestand "setup.exe".
4. Indien u met Windows 2000 of Windows XP werkt, is er de mogelijkheid dat het installatieprogramma een fout zal geven, waarbij u gevraagd wordt of u de IPSec-Services wilt afzetten. Klik op "Ja" indien u deze foutmelding ziet!
5. Klik op "Next". Nu krijgt u de "Software Licence Agreement" te zien. Klik op "yes".
6. Nu kunt u de installatiemap en de startgroep instellen. Druk tweemaal op "Next" om de standaardwaarden te aanvaarden.
7. Nu wordt het programma effectief geïnstalleerd.
8. Indien u werkt met Windows 2000/XP kan er een zwart DOS venster (zie figuur onder) verschijnen met een waarschuwing dat ongeveer hetzelfde betekent als dit: u zal een bericht zien waar u wordt verteld dat de te installeren hardware niet aan de "Windows Logo test" voldoet en of u nog verder wil gaan: u klikt op "toch doorgaan". Dit dialoogvenster kan meerdere keren verschijnen. Klik steeds op "toch doorgaan" om de installatie te voltooien.



9. Na de installatie wordt gevraagd om de computer opnieuw op te starten. Klik op "Finish" om de computer opnieuw op te starten. Uw nieuwe VPN Client is nu geïnstalleerd. De volgende stap is hem configureren door het importeren van het het VPN profiel.

Configuratie van de Cisco VPN Software

Het laatste deel van de installatie van de nieuwe VPN software is het configureren van de software. Hier hangt alles af van hoe u verbinding maakt met het internet.

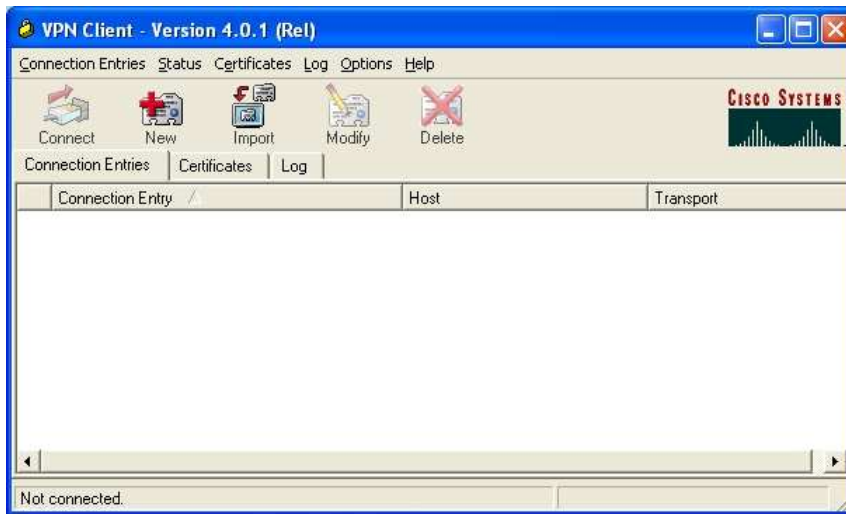
Voor de meeste types verbindingen is er een gewone configuratie. Bij sommige types zijn er enkele aanpassingen nodig. Loop onderstaande lijst af en kijk welke configuratie het beste voor u is:

- Telenet (kabelverbinding) zonder router → gewone configuratie + aanpassingen proxy's indien nodig. Zie "Telenet" achteraan bij "Problemen en Oplossingen" voor meer info.
- Dial-in, ISDN of ADSL zonder router → gewone configuratie.
- Installatie met (wireless) router → gewone configuratie + lees het puntje "routers" bij "problemen en oplossingen" achteraan dit document.

De configuratie van de versie 4 van de Cisco VPN is nog simpeler geworden door het gebruiken van een profielbestand. Dit profielbestand bevat alle informatie dat de software nodig heeft om hem juist te configureren.

Volg de volgende stappen om het profiel te importeren:

1. Start de "VPN Client" onder de startgroep "Cisco Systems VPN Client". U krijgt een dialoogscherm met het logo van Cisco Systems waar nog geen "Connection Entry" in staat (figuur onder) .



2. Klik op het "Import" icoon om een VPN profielbestand te importeren.
3. Een bestandsdialoogvenster verschijnt nu; ga naar de locatie op uw harde schijf waar u het profielbestand hebt opgeslagen. Selecteer het en druk "Openen".
4. Indien het profielbestand succesvol is geïmporteerd, krijgt u een positief klinkend dialoogvenster te zien. Druk op OK om te confirmeren. Bij een negatief bericht download u het profielbestand best eens opnieuw en herhaalt u de import procedure.
5. U ziet nu in het programma één "Connection Entry" staan".

Normaalgezien is de VPN connectie nu degelijk geconfigureerd en kunnen we deze beginnen testen. Dit maakt deel uit van de volgende stap...

Uw Cisco VPN installatie testen

Om uw VPN installatie te testen, dient u eerst ervoor te zorgen dat u een internetverbinding heeft. Maak – indien u geen constante internetverbinding heeft – eerst een verbinding met het internet.

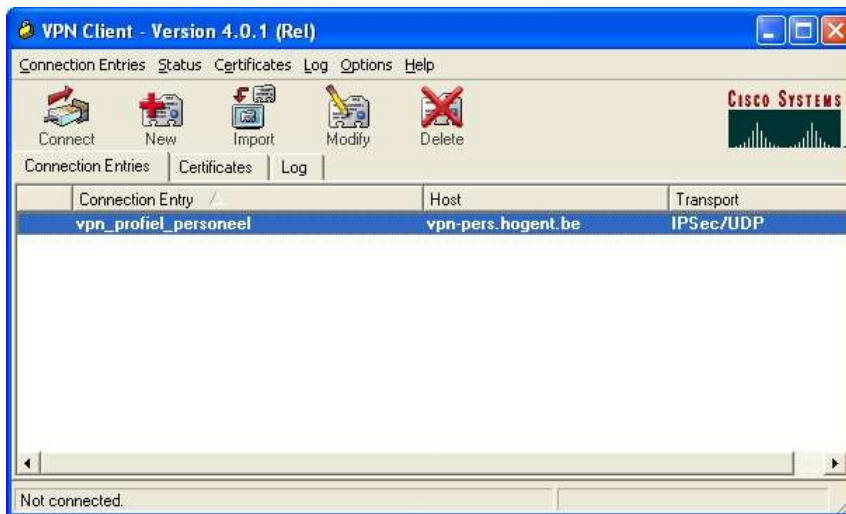
Zorg er ook voor dat alle firewall software zoals ZoneAlarm, Panda Antivirus Titanium e.d. ingesteld staan dat de Cisco VPN client zowel uitgaande als binnenkomende verbinen mag maken.

Indien u werkt met een router, dient ook daar de firewall af te staan en NAT aan te staan. Ga naar "Problemen en Oplossingen" achteraan dit document voor meer informatie i.v.m. het werken met een router en firewalls

Nu kan u volgende stappen ondernemen:

1. Zorg dat uw computer een internet verbinding heeft en dat u online bent (u bent dit als u kan surfen!).
2. Start het VPN Client programma in de startgroep "Cisco Systems VPN Client".

3. Standaard staat de laatst ingestelde configuratie geselecteerd. Klik op "Connect" om te verbinden.



4. U krijgt nu een dialoogvenster (zie figuur rechts) dat u vraagt uw gegevens (User-ID en paswoord) in te typen. Indien u dit niet krijgt, kunnen er meerdere oorzaken zijn. Ga naar "Problemen en Oplossingen" voor mogelijke oplossingen. Vul hier uw user-ID en paswoord in dat u ook gebruikt voor het opvragen van uw e-mail en klik "OK" om te verbinden.



5. Bij het lukken van de VPN verbinding verdwijnt de VPN Client in de taakbalk. Dit kan u zien aan een geel slotje dat nu gesloten is. Als u dubbelklikt op dit slotje krijgt u de VPN Client weer te zien en is de "Connect" knop veranderd in "Disconnect" om uw VPN verbinding te kunnen afsluiten.

6. Als test start u nu een internet browser op en surft u naar <http://webs.hogent.be/public>. Indien deze webpagina zich opent zonder foutmeldingen, is uw VPN installatie gelukt en werkt ze goed! Indien er toch een foutmelding verschijnt dat u niet gerechtigd bent om deze pagina te zien, kan u eerst eens op vernieuwen klikken (het icoontje met 2 groene pijltjes) om de pagina opnieuw te proberen laden. Indien het nu nog niet lukt, is er iets mis met de verbinding.

LET OP: TELENET GEBRUIKERS DIE VOOR HET SURFEN GEBRUIK MAKEN VAN DE PROXYSERVERS VAN TELENET DIENEN DE CONFIGURATIE VAN INTERNET BROWSER AAN TE PASSEN. GA NAAR "PROBLEMEN EN OPLOSSINGEN" BIJ 'TELENET' VOOR DEZE AANPASSING TE KUNNEN MAKEN.

Apple Mac OS X

De verschillen tussen Windows en Apple

Er zijn in principe niet zoveel verschillen tussen Windows en Apple qua werking. Maar het installeren en verwijderen van de software is volledig anders. Daarom dat deze zaken hieronder besproken staan.

Voor het downloaden, configureren en testen van de software lopen de zaken gelijk, daarvoor verwijs ik naar boven bij "Procedures".

Deïnstallatie oude Cisco VPN Client software

Verwijder alle oude installaties met volgend stappenplan:

1. Open een "Terminal" bij "Programma's" > "Hulpprogramma's".
2. Voer volgend commando in: `sudo /usr/local/bin/vpn_uninstall`
3. Er zal een programma opstarten en u tweemaal een vraag stellen; vul tweemaal "yes" in om alle versies van de Cisco VPN Client die op uw Mac staan geïnstalleerd te verwijderen.

Na het verwijderen, kan u de nieuwe versie downloaden. Ga naar het "Downloaden van de Cisco VPN software" bovenaan in deze handleiding.

Installatie VPN Client

De Cisco VPN client werkt enkel op verie OS X van de het besturingssysteem van Apple en dit pas vanaf versie 10.1.5.

We veronderstellen dat het installatie- en profielbestand reeds is gedownload naar een locatie op uw harde schijf. Mac zal automatisch het dmg bestand uitpakken naar een Virtueel Volume waar u op kan dubbelklikken. Volgende stappen dient u hierna te volgen voor de VPN client te installeren:

1. Dubbelklik op het bestand "Cisco VPN Client.mpkg". De installatie wordt opgestart.
2. Mac OS X zal vragen om u te authenticeren voor u kan verder gaan met installatie. Doe dit en druk op "OK".
3. Ga akkoord met de licentie van de software door twee maal op "Akkoord" te drukken.
4. Selecteer uw doelvolume voor de installatie.
5. Druk op "Installeren" om de installatie te laten beginnen.
6. Na de installatie kan u de "VPN Client" terugvinden onder "Programma's".
7. Open een Finder venster en ga naar "Programma's". U vindt de VPN Software weer onder de naam "VPN Client". U kan nu verder gaan met het configureren en testen (zie "Procedures" hoger in die document).

Problemen en Oplossingen

Indien u problemen ondervindt met de nieuwe VPN software en u bent er zeker van dat u alles tot in de details juist hebt gedaan, kunt u hier even kijken of er al een oplossing voor handen is.

Telenet

LET OP: SINDS EEN JAAR LAAT TELENET ZIJN GEBRUIKERS OOK TOE TE SURFEN ZONDER PROXY'S. OOK AL RADEN ZIJDIT TEN STELLIGSTE AF AANGEZIEN DIT EEN SERIEUS SNELHEIDSVOORDEEL HEEFT. INDIEN UW PROXY-INSTELLINGEN NIET INGESTELD STAAN, ZOU VPN MOETEN WERKEN ZONDER ONDERSTAANDE AANPASSINGEN!

De aanpassingen die u moet maken zijn niet echt moeilijk en verlopen in alle internet browsers analoog. U zal echter zelf moeten zoeken waar de instellingen daarin moeten aangepast worden. Wij baseren ons voorbeeld op Internet Explorer 6.

Microsoft Windows 95/98/ME/2000/XP

1. Start Internet Explorer of de browser die u gebruikt;
2. Ga naar "Extra" → "Internet-opties" en kies het tabblad "Verbindingen".
3. In het tabblad "Verbindingen" klikt u op "LAN-instellingen".
4. Alle opties op dit tabblad moeten uitgeschakeld worden indien de VPN client goed moet werken.
5. Druk OK op alle geopende dialoogvensters en herstart uw Internet Explorer.
6. Surf nu naar <http://webs.hogent.be/public>. Indien deze webpagina zich opent, is uw VPN installatie geslaagd! Indien er een foutmelding verschijnt dat u niet gerechtigd bent om deze pagina te zien, kan u eerst een op vernieuwen klikken (het icoontje met 2 groene pijltjes) om de pagina opnieuw te proberen laden. Indien het nu nog niet lukt, is er iets mis met de VPN configuratie.

MAC OS X.x

In MAC OS X.x kan u bepaalde netwerkinstellingen – zoals het gebruiken van proxy's – centraal instellen. Meestal zullen deze dus al degelijk ingesteld zijn. Doch dienen er enkele aanpassingen gedaan te worden om de Cisco VPN Client goed te laten functioneren:

1. Ga naar "Systeemvoorkeuren" → "Netwerk" (zie figuur onderaan pagina).
2. Selecteer het tabblad "Proxy's".
3. Alle opties op dit tabblad moeten uitgeschakeld worden indien de VPN client goed moet werken
4. Klik op "Pas nu toe" om de nieuwe proxy-instellingen te activeren.
5. Start nu Internet Explorer en surf naar <http://webs.hogent.be/public>. Indien deze webpagina zich opent, is uw VPN installatie geslaagd! Indien er een foutmelding verschijnt dat u niet gerechtigd bent om deze pagina te zien, kan u eerst een op vernieuwen klikken (het icoontje met 2 groene pijltjes) om de pagina opnieuw te proberen laden. Indien het nu nog niet lukt, is er iets mis met de VPN configuratie.

Routers

NAT/PAT functionaliteit

De meeste routers zijn vandaag standaard uitgerust met NAT/PAT ondersteuning en deze staat dan ook meestal standaard ingeschakeld.

Indien u problemen zou hebben met uw VPN verbinding en u werkt met een router, kan het zijn dat deze functies zijn uitgeschakeld. Raadpleeg eerst de handleiding van uw router voor het inschakelen van de NAT/PAT functionaliteit. De helpdesk zal u maar heel beperkt kunnen helpen, aangezien het grote aanbod van routers op de markt tegenwoordig.

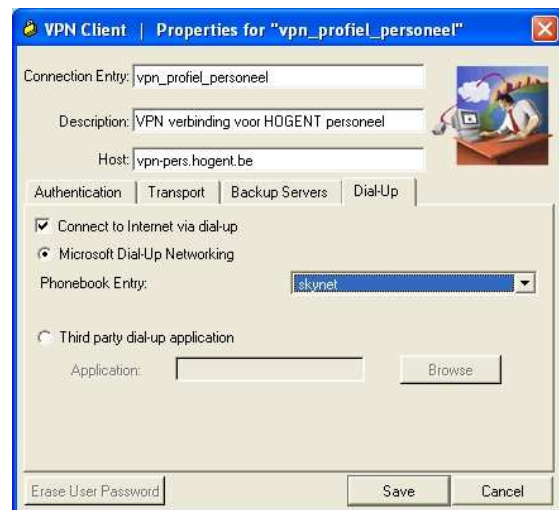
Firewall

Kijk verder dit deeltje om problemen op te lossen die aan de firewall van uw router kunnen liggen...

Problemen met analoge modemverbindingen en USB ADSL modems

Wanneer u een internet verbinding maakt met een interne of externe analoge of ADSL (op bvb. usb) modem, kan het zijn dat u nog altijd niet op de interne servers geraakt. Indien u dit gedrag herkent, kan u dit mogelijk oplossen door volgende onderstaande stappen te volgen:

1. Start de VPN Client programma in de startgroep "Cisco Systems VPN Client".
2. Selecteer het VPN profiel en klik op de knop "Modify".
3. Ga naar het tabblad "Dial-Up" (zie figuur rechts).
4. Vink "Connect to internet..." aan en kies welke verbinding uw internetverbinding vertegenwoordigt.
5. Sluit het venster door op "Save" te drukken.
6. Maak opnieuw een verbinding en probeer opnieuw om op de interne servers te geraken.



VPN problemen bij draadloos surfen

Er zijn ondertussen al vele meldingen binnen gekomen dat de VPN verbinding niet werkt bij draadloze netwerken. Het gedrag is meestal hetzelfde: u zal wel kunnen verbinden maar er zal geen VPN functionaliteit zijn! Ook is er ondervonden dat de gewone internet functionaliteit (e-mail ophalen, surfen e.d.) er onder leidt!

We zijn ervan overtuigd dat met de introductie van de Cisco VPN Client versie 4 deze problemen opgelost zouden moeten zijn. Doch vragen wij u bij het blijven van uw probleem dit te melden aan de helpdesk.

Linux

Indien u de VPN Client op Linux installeert, lees dan goed de README bestanden. Wij bieden voor dit platform geen enkele ondersteuning. Installatie van de Cisco VPN Software voor Linux gebeurt dus op eigen verantwoordelijkheid!

IPSEC-services

Deze service is alleen te vinden op Microsoft Windows 2000/XP installatie. Het is een ingebouwde firewall en deze is niet compatibel met de nieuwe VPN software. Daarom zal deze software – tijdens de installatie – vragen om de IPSEC-services uit te schakelen. Ga akkoord om latere problemen te vermijden!

Windows 98SE/ME Internet Connection Sharing

De Cisco VPN Software is niet compatibel met de Internet Connection Sharing tool dat o.a. standaard geïnstalleerd staat op Windows ME. U dient deze software te deïnstalleren om uw Cisco VPN software te laten werken. Hoe u dit moet doen staat beschreven op <http://support.microsoft.com/default.aspx?scid=kb;en-us;230112> (deze site is in het Engels).

Foutmeldingen VPN Client Software

Volgende foutmeldingen kunnen zich voordoen tijdens de installatie, configuratie of het uitvoeren van de VPN Client Software.

1. "The Necessary VPN sub-system is not available. You can not connect to the remote VPN server."

→ **Oorzaak:** Deze fout verschijnt wanneer bepaalde processen niet lopen die nodig zijn om de VPN Client Software goed te laten functioneren.

→ **Oplossing:** Probeer eerst uw pc opnieuw op te starten. Indien u dezelfde foutmelding krijgt, dient u naargelang uw besturingssysteem bepaalde zaken te doen:

Windows 98/ME: Klik op START → "zoeken". In het zoekveld typt u "cvpnd.exe" (zonder aanhalingstekens) en "OK". Indien dit bestand verschijnt in de lijst met gevonden items, dient u erop te dubbelklikken. Er zal precies niets gebeuren, maar op de achtergrond draait nu het cvpnd proces dat nodig is voor de Cisco VPN client om goed te functioneren.

Windows 2000/XP: Klik op START → (instellingen) → Configuratiescherm → Systeembeheer → Services. Zoek in het opkomende venster de lijn "Cisco Systems, Inc. VPN Service" en vergewis u ervan dat er de service "gestart" is en het opstarttype "automatisch" is. Indien één van deze zaken niet zo is, dient u dit aan te passen door met de rechtermuisknop op deze lijn te klikken, voor "eigenschappen" te kiezen en dan het opstarttype op "automatisch" te zetten. Klik daarna eerst eens op "toepassen" om vervolgens op "starten" te klikken. Nadat de service gestart is, probeert u opnieuw een VPN verbinding te maken. ALLE voorgaande zaken kunnen enkel uitgevoerd worden als beheerder van de pc.

2. "System Error: Unable to retrieve Dial-Up Networking Phonebook Entries."

→ **Oorzaak:** U hebt op het tabblad "Connections" geklikt bij de opties van een VPN verbinding terwijl u geen dial-up verbindingen hebt (bvb. een modem).

→ **Oplossing:** Niet meer op dit tabblad klikken en altijd handmatig een connectie maken met het internet is de beste manier van werken.

Voor andere foutmeldingen wendt u zich best tot de handleiding van Cisco zelf, te vinden op <http://webs.hogent.be/public> (vpn of verbinding van binnenin de Hogeschool Gent vereist) of <http://webs.hogent.be/ciscovpn> (inloggen vereist).

Firewall problemen

Indien u een firewall programma heeft draaien op uw computer waar u de VPN software op heeft geïnstalleerd, dient u deze zo in te stellen dat de Cisco VPN Client zowel uitgaande als binnenkomende verbindingen mag hebben.

Uit onze ervaring hebben we geleerd dat de Windows XP firewall die standaard bij service pack 2 wordt geïnstalleerd normaal geen problemen geeft met de VPN client.

Andere firewalls die geleverd worden bij bepaalde anti virus programma's of op zich staande firewall software zoals ZoneAlarm, dienen soms echter aangepast/geconfigureerd te worden om goed te kunnen samenwerken met de VPN client.

Bij grotere problemen echter en als laatste oplossing kan u de ingebouwde firewall van de VPN client uitschakelen. Dit is een procedure die enkel als laatste redmiddel kan toegepast worden. Zie onder bij "Cisco VPN firewall uitschakelen" hoe u dit doet!

Firewall hardware router

Indien u thuis een hardware router heeft staan omwille van de wireless functionaliteit of dergelijke, dient u – indien uw VPN Client er niet in slaagt een verbinding te maken – deze in te stellen zodat VPN verbindingen worden toegelaten.

Dit gebeurt door ervoor te zorgen dat de firewall op uw router een bepaalde poort expliciet forward naar uw pc waar de VPN software opstaat. Deze poort moet u dan ook instellen in uw VPN Client. Zorg er alleszins ook voor dat de firewall op uw pc dan uit staat of ingesteld is dat deze poort gegevens van het internet mag ontvangen:

1. Start het VPN Client programma in de startgroep "Cisco Systems VPN Client".
2. Selecteer het VPN profiel en klik op de knop "Modify".
3. Ga naar het tabblad "Transport".
4. Nu klikt u de optie "Use IPsec over TCP" aan.
5. In het tekstvak "TCP port" vult u het getal 15000 in.
6. Klik op "Save" om de aanpassingen op te slaan.
7. Nu dient u de firewall op uw router (zie de handleiding van uw router) zodanig te configureren dat deze al het verkeer op TCP poort 15000 doorlaat naar uw PC.

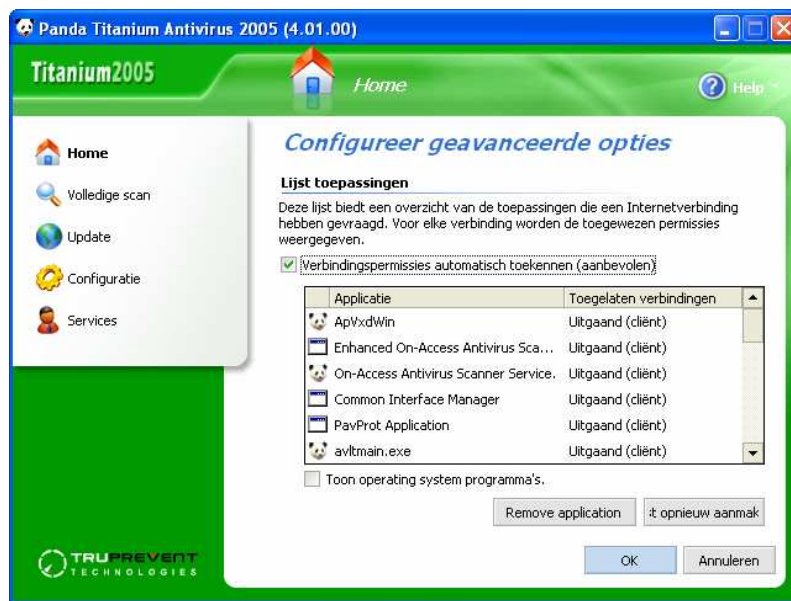
Indien u er niet in slaagt de firewall te configureren dat hij het verkeer op deze poort 15000 doorlaat naar uw pc, dient u deze tijdelijk uit te schakelen.

Panda Antivirus Titanium 2005 – thuisversie!

U kan Panda Titanium zo instellen zodat hij probleem met de Cisco VPN client kan samenwerken. Volg de volgende stappen na het installeren van beide programma's.

1. Start Panda Antivirus op
2. In het Home tabblad klikt u onderaan op "Configuratie automatische bescherming".
3. In het volgende tabblad klikt u op "Firewallbeveiliging".
4. In het volgende tabblad klikt u op "Configuratie van de connectie".

5. U ziet u onderstaand venster verschijnen:



6. In dit venster schakelt u het vinkje met de tekst: "Verbindingspermissies automatisch toekennen (aanbevolen)" uit.
7. Dan zoekt u in de lijst van programma's (dat onder het vinkje staat) naar 'Cisco Systems VPN Client'.
8. In de kolom naast 'Cisco Systems VPN Client' klikt u nu de keuzelijst aan en kiest u voor "Inkomend en uitgaand" (in de kolom "toegelaten verbindingen" dus).
9. Schakel nu het vinkje met de tekst: "Verbindingspermissies automatisch toekennen (aanbevolen)" weer in.
10. Klik nu tweemaal OK en sluit dan Panda Antivirus af.
11. Probeer uw VPN verbinding opnieuw...

Het is gekend dat de Panda Titanium Antivirus Firewall de PC kan doen crashen/heropstarten bij het initialiseren van de VPN software of verbinding. Indien met bovenstaande oplossing dit niet stopt, kan u proberen de Cisco VPN firewall uit te schakelen (zie onder).

Andere zoals ZoneAlarm, Norton Internet Security...

Schakel deze uit door de in de handleiding van deze programma's aangegeven methode te volgen of stel ze zodanig in dat de Cisco VPN Client vrij met het internet mag verbinden en dat de Cisco VPN vrij informatie van het internet mag ontvangen!

De helpdesk geeft geen ondersteuning op software firewalls buiten deze van MS Windows en Panda Antivirus 200x!

Cisco VPN firewall uitschakelen

Deze procedure volgt u best als uw internetverkeer half of niet meer werkt en bovenstaande oplossingen geen soelaas hebben geboden. Na deze procedure dient u ONMIDDELIJK te herstarten, dus sluit alle openstaande toepassingen af voor u hiermee begint.

1. Ga naar START > Configuratiescherm > Systeem.
2. Ga naar het tabblad "Hardware", druk op de knop "apparaatbeheer".
3. In dit dialoogvenster kiest u het menu "Beeld" en klikt u op "Verborgen apparaten weergeven" aan.
4. Klik op het plusteken van het item "Stuurprogramma's die niet plug en play compatibel zijn". De onderliggende lijst wordt uitgevouwd.

5. Zoek het item met de naam "vsdantant" in de uitgevouwde lijst.
6. Klik met de rechter muisknop op deze item en kies "uitschakelen".
7. De computer vraagt nu om te herstarten, doe dit onmiddellijk!

U kan nu weer proberen de Windows XP firewall of andere firewall bescherming weer aan te zetten om uw computer weer te beveiligen.

Andere problemen = helpdesk

Indien u nog problemen ondervindt die hier niet beschreven zijn, dan kan u altijd terecht bij uw lokale informaticaverantwoordelijke of bij de helpdesk.

De helpdesk is elke dag bereikbaar van 8u.30 tot 12u.30 en van 13u. tot 20u. (17u. tijdens schoolvakanties):

- E-mail: helpdesk@hogent.be: zie ook "Hoe uw probleem rapporteren".
- Telefoon: 09/267.11.22

Kijk ook voor nog meer informatie eens op volgende plaatsen:

- Helpdesk website: <http://helpdesk.hogent.be>
- VPN helpdesk website: <http://helpdesk.hogent.be/vpn/>
- Download website VPN: <http://webs.hogent.be/ciscovpn> (inloggegevens nodig!)

Hoe uw probleem rapporteren?

Voer eerst volgende procedure uit om de werkinglogs van de Cisco VPN Client (versie 4!) te verkrijgen:

1. Maak een internetverbinding (controleer dit eens te surfen naar uw favoriete website of door uw mail op te halen).
2. Start de "VPN Client" vanuit het "Cisco Systems VPN Client" startmenu. Druk echter nog niet op "Connect". Indien er tijdens het opstarten van de VPN Dialer foutmeldingen verschijnen, gelieve deze ook te noteren of er een screenshot van te nemen (dialoogvenster van de foutmelding activeren en ALT+'Print Screen' drukken, dan in Word document plakken).
3. In het menu "Log" kiest u voor "Enable". Het programma kan nu even blijven hangen...
4. In het menu "Log" opent u het dialoogvenster "Log Settings" en zet u alles op "High".
5. In het menu "Log" opent u het dialoogvenster "Log Window". Selecteer nu het hoofdvenster van de Cisco VPN Client en probeer te verbinden. Laat ten allen tijde het "Log Window" open staan. Probeer minstens 2 keer in te loggen indien dit niet lukt! U zal zien dat in het "Log Window" veel tekst wordt gegenereerd!
6. In het "Log Window" klikt u nu op "Save" en slaat u het logbestand onder de naam "vpn.log" op.
7. Stuur dit bestand als bijlage in een mailbericht naar helpdesk@hogent.be samen met de extra info die onderaan dit puntje wordt gevraagd.

Extra info ook op te geven bij rapportage probleem:

- Type internetverbinding: analoog, ADSL, ISDN, Kabel (merk en type ook meegeven aub: bvb. Telenet Kabel Mono).
- Bij ADSL: merk en type modem + type aansluiting (via netwerkkabel, USB...).
- Type aansluiting: bvb. rechstreeks op de kabel, via router met firewall, wireless...
- Indien router tussen pc en internet: merk, type, modelnummer...

- Softwarematige firewalls: geef alle software op die uw internetverkeer zouden kunnen blokkeren: bvb. Norton Internet Security.
- Duidelijk omschrijving van het probleem en wanneer het zich voor doet.

Voor de meeste zaken omtrent VPN wordt er ondersteuning gegeven, buiten voor de Linux versie van de Cisco VPN software.