VPN-clientQ

Inhoud

Inleiding

Dit document beantwoordt vaak gestelde vragen over de Cisco VPN-client.

Opmerking: Hier zijn de naamgevingsconventies voor de verschillende VPN-clients:

- Cisco Secure VPN-clientversies 1.0 tot en met 1.1a
- Cisco VPN 3000 clientversies 2.x alleen
- Cisco VPN-client 3.x en alleen later

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

VPN-clientsoftware downloaden

Q. Waar kan ik de Cisco VPN-clientsoftware downloaden?

A. U moet inloggen en een geldig servicecontract hebben om toegang te krijgen tot de Cisco VPN-clientsoftware. Cisco VPN-clientsoftware kan worden gedownload van de Cisco Download Software (alleen geregistreerde klanten) pagina. **Als u geen geldig servicecontract hebt afgesloten dat aan uw Cisco.com-profiel is gekoppeld, kunt u de VPN-clientsoftware niet inloggen en downloaden.**

U kunt een geldig servicecontract verkrijgen:

- Neem contact op met uw Cisco-accountteam als u een directe koopovereenkomst hebt.
- Neem contact op met een Cisco-partner of Reseller om een servicecontract te kopen.
- Gebruik de Profile Manager (alleen geregistreerde klanten) om uw Cisco.com-profiel te

uploaden en om associatie naar een servicecontract te vragen.

Q. Het downloadgebied van Cisco VPN-client lijkt leeg. Waarom?

A. Wanneer u het VPN-clientgebied van het Software Center bereikt (alleen geregistreerde klanten), zorg er dan voor dat u in het midden van de pagina het downloadgebied voor uw gewenste besturingssysteem selecteert.

Q. Hoe kan ik de functie Stateful Firewall uitschakelen tijdens de installatie van de Cisco VPN-client?

A. Voor VPN-clientversies voorafgaand aan 5.0:

Raadpleeg het gedeelte Documentatie Wijzigingen van de VPN-client Rel 4.7 Releaseopmerkingen om meer te weten te komen over de twee onderwerpen "Gebruik MSI om de Windows VPN-client zonder stateful Firewall te installeren" en "InstalleerShield om de Windows VPN-client zonder stateful Firewall te installeren".

Voor VPN-clientversies na 5.0:

Om te beginnen met Cisco VPN-clientrelease 5.0.3.05.60 is een MSI-installatievlag toegevoegd om te voorkomen dat de fout in firewallbestanden wordt geïnstalleerd:

```
msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1
```

Raadpleeg de installatie van firewallbestanden bij omzeilen wanneer stateful Firewall niet is vereist voor meer informatie hierover.

Q. Hoe kan ik de Cisco VPN-client verwijderen of upgraden?

A. Raadpleeg de versie Een VPN-client verwijderen die met het MSI-installatieprogramma is geïnstalleerd voor informatie over het handmatig verwijderen (InstallShield) en het vervolgens upgraden van de Cisco VPN-clientversie 3.5 en hoger voor Windows 2000 en Windows XP.

De Cisco VPN-client voor Windows 2000 en Windows XP-software kunnen updates en nieuwe versies automatisch downloaden via een tunnel van een VPN 3000 Concentrator of een andere VPN-server die meldingen kan leveren. De minimumvoorwaarde voor dit is dat externe gebruikers de VPN-client voor Windows 4.6 of hoger op hun pc's moeten hebben geïnstalleerd om de automatische update-functie te kunnen gebruiken.

Met deze functie, autoupdate genaamd, hoeven gebruikers geen oude versie van de software te verwijderen, opnieuw te starten, de nieuwe versie te installeren en vervolgens opnieuw te beginnen. In plaats daarvan stelt een beheerder updates en profielen beschikbaar op een webserver en wanneer een externe gebruiker de VPN-client start, detecteert de software dat een download beschikbaar is en automatisch krijgt deze. Raadpleeg voor meer informatie de datums beheren en hoe automatisch bijwerken werkt.

Raadpleeg voor informatie over het configureren van client-update op een Cisco ASA Series 5500 adaptieve security applicatie met ASDM, Clientsoftware bijwerken met ASDM.

Q. Ik wil de VPN-clients voor Vista aanpassen. Ik realiseer me dat er, met de

nieuwe VPN client versie voor Vista, geen bestand is zoals oem.mst. Hoe kunnen we de nieuwe VPN-clientversies (5.x) aanpassen of waar ik dit bestand vind?

A. Het MST-bestand wordt niet langer bij de VPN-client geleverd, maar u kunt het downloaden van de Download Software (alleen geregistreerde klanten) pagina:

Bestandsnaam: Lezen en MST voor installatie in de internationale versie van Windows.

Besturingssysteem

V. verstrekt Cisco een VPN-client voor Windows Vista?

A. De nieuwe release van Cisco VPN-client 5.0.07 ondersteunt Windows Vista op zowel x86 (32-bits) als x64. Raadpleeg de Releaseopmerkingen van 5.0.07.0240 voor meer informatie.

Opmerking: Cisco VPN-client wordt alleen ondersteund tijdens installatie van Windows Vista, wat betekent dat een upgrade van een Windows-besturingssysteem naar Windows Vista niet wordt ondersteund met de VPN-clientsoftware. U dient eerst Windows Vista te installeren en vervolgens de Vista VPN-clientsoftware te installeren.

Opmerking: Als u geen geldig servicecontract hebt afgesloten dat aan uw Cisco.com-profiel is gekoppeld, kunt u de VPN-clientsoftware niet inloggen en downloaden. Zie VPN-clientsoftware downloaden voor meer informatie.

Tip: De Cisco AnyConnect VPN-client is nu beschikbaar voor Windows-besturingssystemen, met onder meer Vista 32- en 64-bits. De AnyConnect-client ondersteunt SSL en DTLS. IPsec wordt momenteel niet ondersteund. Bovendien is AnyConnect alleen beschikbaar voor gebruik met een Cisco adaptieve security applicatie die versie 8.0(2) of hoger uitvoeren. De client kan ook worden gebruikt in weblanceringsmodus met IOS-apparaten die versie 12.4(15)T gebruiken. VPN 3000 wordt niet ondersteund.

De Cisco AnyConnect VPN-client en ASA 8.0 kunnen bij het Software Center worden verkregen (alleen geregistreerde klanten). Raadpleeg de opmerkingen van Cisco AnyConnect VPN-clientrelease voor meer informatie over de AnyConnect-client. Raadpleeg de Cisco ASA 5500 Series adaptieve security applicaties release Notes voor meer informatie over ASA 8.0.

Opmerking: Als u geen geldig servicecontract hebt afgesloten dat aan uw Cisco.com-profiel is gekoppeld, kunt u niet inloggen en de AnyConnect VPN-client of ASA-software downloaden. Zie VPN-clientsoftware downloaden voor meer informatie.

Vraag. Hoe kan ik een PPTP-verbinding van een Microsoft Windows PC opzetten?

A. De installatie is afhankelijk van de versie van Microsoft Windows die u uitvoert. U dient voor specifieke informatie contact op te nemen met Microsoft. Hier zijn setup-instructies voor een aantal gebruikelijke versies van Windows:

Windows 95

1. Installeer het hulpprogramma Msdun13.exe.
2. Kies **Programma's > Accessoires > Netwerken uitbellen**.

3. Maak een nieuwe verbinding met de naam "PPTP."
4. Selecteer de **VPN-adapter** als het apparaat voor de verbinding.
5. Voer het IP-adres in van de openbare interface van de switch en klik op **Voltooien**.
6. Ga terug naar de verbinding die u zojuist hebt gemaakt, klik met de rechtermuisknop en kies **Eigenschappen**.
7. Onder Toegestaan netwerkprotocollen, minstens, niet **controleren** op **netwerk**.
8. Configuratie van de instelling **Geavanceerde opties**: Laat standaardinstellingen om de switch en de client in staat te stellen om automatisch te onderhandelen over de verificatiemethode.Laat **Versleuteld Wachtwoord** toe om de Challenge Handshake Authentication Protocol (CHAP) te forceren.Laat **het versleutelde wachtwoord** toe en **Vereist gegevensencryptie** om MS-CHAP-verificatie te forceren.

Windows 98

1. Voltooi deze stappen om de PPTP-functie te installeren: Kies **Start > Instellingen > Configuratiescherm > Nieuwe hardware toevoegen** en klik op **Volgende**.Klik op **Selecteer in de lijst** en kies **Netwerkadapter** en klik op **Volgende**.Kies **Microsoft** in het linkerpaneel en **Microsoft VPN-adapter** in het rechterpaneel.
2. Voltooi deze stappen om de PPTP-functie te configureren: Kies **Start > Programma's > Accessoires > Communicatie > Netwerkmodule inbelen**.Klik op **Maak een nieuwe verbinding** en kies **Microsoft VPN-adapter** voor Selecteer een apparaat. Het IP-adres van de VPN-server is 3000 tunneleindpunt.
3. Voltooi deze stappen om de pc te wijzigen zodat ook een Wachtwoord-verificatieprotocol (PAP) mogelijk is: **Opmerking:** De standaard Windows 98-verificatie moet wachtwoordencryptie (CHAP of MS-CHAP) gebruiken.Kies **Eigenschappen > servertypen**.Schakel **de** controle **uit. Vereist een versleuteld wachtwoord**. U kunt gegevensencryptie (Microsoft Point-to-Point Encryption [MPPE] of geen MPPE) op dit gebied configureren.

Windows 2000

1. Kies **Start > Programma's > Accessoires > Communicatie > Netwerkverbindingen en inbelverbindingen**.
2. Klik op **Nieuwe verbinding maken** en vervolgens op **Volgende**.
3. Kies **Connect met een privaat netwerk via het internet en kies een verbinding vóór** (selecteer deze niet als u een LAN hebt), en klik op **Volgende**.
4. Voer de naam van de host of IP-adres van het tunneleindpunt in (3000).
5. Als u het wachtwoordtype moet wijzigen, kiest u **Eigenschappen > Beveiliging voor de verbinding > Geavanceerd**. De standaardinstelling is MS-CHAP en MS-CHAP v2 (niet CHAP of PAP). U kunt op dit gebied gegevensencryptie (MPPE of geen MPPE) configureren.

Windows NT

Raadpleeg Installeren, configureren en gebruiken van PPTP met Microsoft Clients en servers .

Q. Welke besturingssysteemversies ondersteunen de Cisco VPN-client?

A. Ondersteuning voor extra besturingssystemen wordt constant toegevoegd voor de VPN-client. Raadpleeg de systeemvereisten in de releaseopmerkingen voor VPN-client 5.0.07 om dit te bepalen, of raadpleeg Cisco hardware- en VPN-clients voor ondersteuning van IPsec/PPTP/L2TP.

Opmerkingen:

- De VPN-client biedt ondersteuning voor dual-processor en dual-core werkstations voor Windows XP en Windows Vista.
- De Windows VPN-clientrelease 4.8.0.40 was de definitieve versie die het Windows 98-besturingssysteem officieel ondersteunde.
- De Windows VPN-clientrelease 4.6.04.0043 was de definitieve versie die het Windows NT-besturingssysteem officieel ondersteunde.
- Cisco VPN-client voor versie 5.0.07 ondersteunt Windows Vista en Windows 7 in zowel de x86 (32-bits) als x64 (64-bits) versies.
- Cisco VPN-client ondersteunt alleen Windows XP 32-bit, maar Windows XP 64-bit wordt niet ondersteund.**Opmerking:** ondersteuning van Windows Vista 32 bit was beschikbaar in alle 5.x-releases. Cisco VPN-clientversie 5.0.07 heeft de 64-bits ondersteuning toegevoegd.

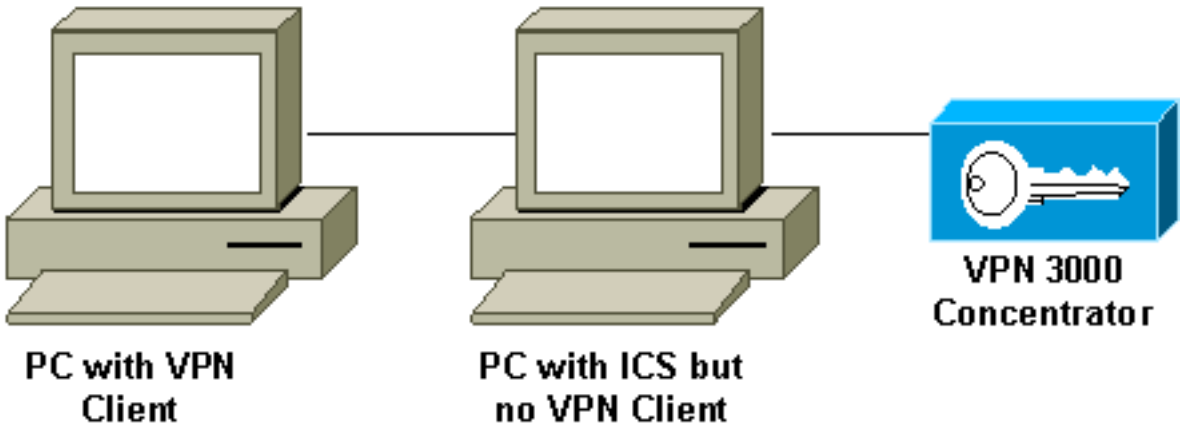
Q. Moet ik een beheerder op Windows NT/2000-machines zijn om de VPN-client te laden?

A. Ja, u moet beheerdersrechten hebben om de VPN-client te installeren op Windows NT en Windows 2000 omdat deze besturingssystemen beheerdersrechten vereisen om aan de bestaande netwerkstuurprogramma's te binden of om nieuwe netwerkstuurprogramma's te installeren. De VPN client software is netwerksoftware. U moet beheerderrechten hebben om het te installeren.

Q. Kan de Cisco VPN-client werken met Microsoft Internet Connection Sharing (ICS) geïnstalleerd op dezelfde machine?

A. De client van Cisco VPN 3000 is niet compatibel met Microsoft ICS op dezelfde machine. U moet ICS verwijderen voordat u de VPN-client kunt installeren. Raadpleeg ICS uitschakelen bij het voorbereiden op installatie of upgrade op Cisco VPN-client 3.5.x onder Microsoft Windows XP voor meer informatie.

Hoewel het hebben van de VPN client en ICS op dezelfde PC niet werkt, werkt deze overeenkomst wel.



Q. Mijn VPN-client lijkt alleen verbinding te maken met bepaalde adressen. Ik voer Windows XP uit. Wat moet ik doen?

A. Controleer dat de ingebouwde firewall in Windows XP is uitgeschakeld.

Q. Is de Cisco VPN-client compatibel met de Windows XP stateful firewall?

A. Deze kwestie is opgelost. Bekijk Cisco Bug ID CSCdx15865 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie.

Q. Wanneer ik de VPN-client op Windows XP en Windows 2000 installeer, is de interface voor meerdere gebruikers uitgeschakeld?

A. De installatie schakelt het welkomstscherm en de snelle gebruikersswitching in. Bekijk Cisco Bug ID CSCdu24073 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie.

Q. Hoe kan ik de VPN-client voor Linux naar de achtergrond verplaatsen na de uitvoering? Als ik een verbinding start zoals vpnclient-verbinding voor, dan kom ik binnen, maar de shell wordt teruggegeven.

A. Typ na het aansluiten:

- **^Z**
- **bg**

Q. Wanneer ik de Cisco VPN-client installeer in Windows XP Home Edition, is de taakbalk niet zichtbaar. Hoe maak ik dit ongedaan?

A. Kies **Configuratiescherm > Netwerkverbindingen > Netwerkbrug verwijderen** om deze instelling aan te passen.

Q. Wanneer ik probeer Linux VPN-client te installeren op RedHat 8.0, krijg ik een fout die aangeeft dat de module niet kan worden geladen omdat de module is gecompileerd met GCC 2 en de kern is gecompileerd met GCC 3.2. Wat moet ik doen?

A. Dit komt doordat de nieuwe release van RedHat een nieuwere versie van de GCC-compiler (3.2+) heeft, die ervoor zorgt dat de huidige Cisco VPN-client mislukt. Dit probleem is opgelost en is beschikbaar in Cisco VPN 3.6.2a. Bekijk Cisco Bug ID CSCdy49082 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie of download de software van het VPN Software Center (alleen geregistreerde klanten).

Q. Waarom schakelt de software Fast User Switching uit wanneer ik VPN-client 3.1 op Windows XP installeer?

A. Microsoft schakelt Fast User Switching in Windows XP automatisch uit wanneer een GINA.dll in het register wordt gespecificeerd. De client van Cisco VPN installeert CSgina.dll om de optie "Begin voor aanmelding" te implementeren. Als u snelle switching nodig hebt, schakelt u de optie "Start voor aanmelding" uit. Geregistreerde gebruikers kunnen meer informatie in Cisco Bug ID CSCdu24073 (alleen geregistreerde klanten) in Bug Toolkit verkrijgen.

Q. ondersteunt de IPsec VPN-client de Start Before Logon (SBL) optie op Windows 7?

A. De SBL-functie wordt niet ondersteund op IPsec VPN-clients in Windows7. Deze worden ondersteund door de AnyConnect VPN-client.

Foutmeldingen

Q. Wanneer ik Cisco VPN-client 4.x installeer, ontvangt ik deze foutmelding: **Waarschuwing 201: Het gewenste VPN-subsysteem is niet beschikbaar. U kunt geen verbinding maken met de externe VPN-server**

A. Dit probleem kan worden veroorzaakt door firewallpakketten die op uw VPN-clientcomputer zijn geïnstalleerd. Om deze foutmelding te voorkomen, moet u ervoor zorgen dat er geen firewall- of antivirusprogramma's op uw pc worden geïnstalleerd of uitgevoerd tijdens de installatie.

Q. Ik heb een upgrade uitgevoerd naar Mac OS X 10.3 (bekend als "Panther"), maar nu geeft mijn Cisco VPN-client 4.x deze foutmeldingen weer: **Secure VPN-verbinding lokaal afgesloten door clientreden: Kan geen contact opnemen met de beveiligingsgateway**

A. U moet UseLegacyIKEPort=0 aan het profiel (.pcf-bestand) toevoegen dat in het /etc/CiscoSystemsVPN/Profiles/folder voor Cisco VPN-client 4.x wordt gevonden om met Mac OS X 10.3 ("Panther") te werken.

Q. Wanneer ik probeer de VPN-client te verwijderen, ontvangt ik deze foutmelding: **Fout in msg: heeft het desinstallatiebestand niet gevonden...** Wat betekent deze foutmelding en hoe kan ik de uninstallatie met succes voltooien?

A. Controleer het netwerkbedieningspaneel om te verzekeren dat de deterministische NDIS extender (DNE) niet geïnstalleerd was. Kies ook **Microsoft > Huidige versie > Verwijderen** om te controleren of het bestand is verwijderd. Verwijder het **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\ {5624C000-B109-11D4-9DB4-00E0290FCAC5]** bestand en probeer het uit de installatie halen.

Q. Ik kan de VPN-client niet installeren op Windows 2000 Professional. Ik krijg deze fout: **Een ondersteuningsbestand voor de installatie kan niet worden geïnstalleerd.** catastrofaal falen. Wat moet ik doen?

A. Verwijder de **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall**-toets. Herstart de computer en installeer de VPN-client opnieuw.

N.B.: Ga naar HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\ en klik op **VPN-client** om de juiste toets voor Cisco VPN-software te vinden *onder het pad HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall*. Bekijk in het rechter venster het pad verwijderen (onder de kolom Naam). De corresponderende kolom van Gegevens toont de waarde van de VPN client-toets. Let op deze toets, ga naar HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\, selecteer de ingestelde toets en verwijder deze.

Raadpleeg Initialisatiefout-probleemoplossing en verwijs naar Cisco bug-ID CSCdv15391 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie.

Q. Wanneer ik probeer Linux VPN-client te installeren op RedHat 8.0, ontvang ik een fout die aangeeft dat de module niet kan worden geladen omdat de module is gecompileerd met GCC 2 en de kern is gecompileerd met GCC 3.2. Wat moet ik doen?

A. Dit probleem doet zich voor omdat de nieuwe release van RedHat een nieuwere versie van de GCC-compiler (3.2+) heeft, waardoor de huidige Cisco VPN-client failliet gaat. Dit probleem is opgelost en is beschikbaar in Cisco VPN 3.6.2a. Bekijk Cisco bug ID CSCdy49082 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie of download de software van het VPN Software Center (alleen geregistreerde klanten).

Q. Ik krijg een 'peer niet meer reagerend' foutbericht wanneer mijn Linux-client 3.5 probeert een IPsec-verbinding naar een PIX of naar een VPN 3000 Concentrator op te zetten. Wat moet ik doen?

A. Het symptoom van dit probleem is dat de Linux-client lijkt te proberen verbinding te maken, maar het krijgt nooit een reactie van het gateway-apparaat.

De Linux-OS hebben een ingebouwde firewall (ingangen) die UDP-poorten 500, UDP-poort 1000 en ESP-pakketten (Security Payload) blokkeert. Aangezien de firewall standaard is ingeschakeld, moet u de firewall uitschakelen of de poorten openen voor IPsec-communicatie voor zowel inkomende als uitgaande verbindingen om het probleem op te lossen.

Q. Ik ontvang een kernel extensie fout wanneer ik probeer om Cisco VPN 5000 5.2.2 client op Mac OS X 10.3 uit te voeren. Wat moet ik doen?

A. Zoals vermeld in de opmerkingen over de productrelease, wordt de Cisco VPN 5000-client ondersteund tot versie 10.1.x en wordt de client daarom niet ondersteund op versie 10.3. Het is mogelijk om de VPN-client te laten werken wanneer u de toegangsrechten in twee van de geïnstalleerde bestanden herstelt nadat u het installatiescript hebt uitgevoerd. Hierna volgt een voorbeeld:

Opmerking: Deze configuratie wordt *niet* ondersteund door Cisco.

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. Ik kan de nieuwe versie van de Cisco VPN-client niet installeren. Tijdens de installatie ontvang ik een van deze foutmeldingen: "**Fout DNE tegen uitvoeringsfout bij installatie van DNE, retourcode -214650093**" of "**InstallDNE-fout: DNE tegen uitvoeringsfout bij installatie van DNE, herhaal code -2147024891.**" Dit probleem doet zich voor wanneer ik de Verbeterer in het netwerk voor kennelijke netwerkanalyse heb geïnstalleerd.

A. Installeer de nieuwste DNE-upgrade van deterministische netwerken .

Q. Ik krijg deze logs voor de Cisco VPN-client als ik een verbinding maak:

```
208    15:09:08.619  01/17/08  Sev=Debug/7CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209    15:09:08.619  01/17/08  Sev=Warning/2CVPND/0xE3400003
```

```
Function RegOpenKey failed with an error code of 0x00000002(WindowsVirtualAdapter:558)

210    15:09:08.619  01/17/08  Sev=Warning/3CVPND/0xE340000C
The Client was unable to enable the Virtual Adapter because it could not open the device.
```

A. Het is een vrij algemeen foutbericht, waarvoor meestal handmatige uninstallatie van de client vereist is. Volg de instructies in deze link. Een VPN-clientversie verwijderen die met het MSI-installatieprogramma is geïnstalleerd.

Controleer na het verwijderen of u de computer opnieuw hebt opgestart. Installeer de client opnieuw. Zorg ervoor dat u bent aangemeld als een gebruiker met beheerrechten op de lokale machine.

Q. Wanneer ik probeer de Cisco VPN-client aan te sluiten op een Mac OS, ontvangt ik deze foutmelding: `Fout 51 - kan niet met het VPN-subsysteem communiceren.` Hoe kan ik deze kwestie oplossen?

A. Het probleem kan worden opgelost als u de service opnieuw start nadat u de VPN-client op deze manier hebt gesloten:

Stop:

```
sudo kextunload -b com.cisco.nke.ipsec
```

Zo start u:

```
sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN
```

Controleer ook het volgende op dezelfde machine waar de VPN-client is geïnstalleerd en blokkeer hetzelfde.

- Alle virtuele software (zoals VMWare Fusion, Parallels, kruisingen).
- Alle antivirale/firewallsoftware.
- Verenigbaarheid van de VPN-client met het 64-bits besturingssysteem; raadpleeg de Cisco VPN Client release Notes.

Ik snap 'Reason 442'. Kan de fout van de virtuele adapter niet inschakelen. Hoe kan ik deze fout oplossen?

A. De `reden 442:` Er verschijnt `geen virtuele` adapterfout nadat Vista meldt dat een dubbel IP-adres is gedetecteerd. Latere verbindingen hebben niet hetzelfde bericht, maar Vista meldt niet dat een dubbel IP-adres wordt gedetecteerd. Raadpleeg Fout 442 van IP-adreszoekers op Windows Vista voor meer informatie over het oplossen van dit probleem.

Q. Wanneer ik de Cisco VPN-client installeer, wordt de `vastberaden netwerkversterker Add Plugin mislukte` fout ontvangen. Hoe is deze fout opgelost?

A. Het installeren van de DNE-adapter kan het probleem oplossen. Het is beter om de installatieschermversie te gebruiken voor installatie in plaats van MSI.

Q. Ik heb deze fout ontvangen: `Reden 442: virtuele adapter is niet ingeschakeld.` Hoe kan ik deze kwestie oplossen?

A. Deze fout verschijnt nadat Windows 7 en Windows Vista een dubbel IP-adres herkend hebben. De volgende verbindingen falen met hetzelfde bericht, maar OS rapporteert niet dat het dubbele IP adres wordt gedetecteerd. Raadpleeg Duplicate IP Address Triggers Error 442 op Windows 7 en Vista voor meer informatie over hoe u dit probleem kunt oplossen.

Q. Wanneer ik probeer om VPN-client 4.9 te starten voor MAC OS 10.6, ontvang ik deze fout: `Fout 51: Kan niet communiceren met het VPN-subsysteem.` Hoe moet dit probleem worden opgelost?

A. Deze kwestie komt voor omdat 64-bits ondersteuning niet beschikbaar is met Cisco VPN-client voor MAC OS release 4.9. Als tijdelijke oplossing kunt u starten in 32-bits kernelmodus. Raadpleeg voor meer informatie Cisco Bug ID CSCth1092 (alleen geregistreerde klanten) en Cisco VPN-client voor MAC OSX release notes.

Compatibiliteit met derden

V. Is de Nortel-client compatibel met Cisco VPN 3000-connectors?

A. Nee. De Nortel-client kan geen verbinding maken met Cisco VPN 3000 Concentrator.

Q. Kan ik VPN-clients van andere verkopers, zoals de client voor Nortel Contivity VPN, tegelijkertijd geïnstalleerd hebben met de Cisco VPN-client?

A. Nee. Er zijn bekende problemen wanneer meerdere VPN-clients op dezelfde pc zijn geïnstalleerd.

Q. worden Cisco VPN-clients ondersteund met VPN-concentrators van derden?

A. Cisco VPN-clients worden niet ondersteund door VPN-concentrators van derden.

Verificatie

Q. Hoe slaan Cisco VPN-clients versies 1.1 en 3.x intern digitale certificaten op (X.509v3)?

A. Cisco VPN-client 1.1 heeft een eigen certificaatwinkel. Cisco VPN Client 3.x kan certificaten in de Microsoft-winkel opslaan met Common-Application Programming Interface (CAPI) of deze in Cisco's eigen winkel opslaan (RSA Data Security).

Kan ik dezelfde groepsnaam en gebruikersnaam hebben op de VPN-concentrator?

A. De groepsnaam en de gebruikersnaam mogen niet hetzelfde zijn. Dit is een bekend probleem, dat is aangetroffen in softwareversies 2.5.2 en 3.0 en dat is geïntegreerd in 3.1.2. Bekijk Cisco bug ID CSCdw29034 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie.

Q. worden de kaarten van het volledige uitdagingen zoals de Defender gesteund op de client van Cisco VPN aan PIX?

A. Nee, kaarten van dit type worden niet ondersteund.

VPN-clientsoftwareversie

Q. Wat is er gebeurd met de optie "MTU-hulpprogramma instellen" die in de Cisco VPN-clientversies 2.5.2 en eerder aanwezig was?

A. De Cisco VPN-client past nu de maximale grootte van de transmissieeenheid (MTU) aan. De optie MTU-hulpprogramma instellen is niet langer een vereiste installatiestap. De optie MTU instellen wordt voornamelijk gebruikt voor problemen met de connectiviteit. Het pad om de optie SetMTU voor een Windows-machine te selecteren is **Start > Programma's > Cisco Systems VPN-client > SetMTU**. Raadpleeg voor meer informatie over de optie SetMTU en deze optie in andere besturingssystemen door MTU te wijzigen met behulp van de optie SetMTU.

Q. Wat zijn de talen die later dan 4.0 op de Cisco VPN-clientGUI-versies worden ondersteund?

A. De talen die later dan 4.0 op de Cisco VPN-clientGUI-versies worden ondersteund, zijn Canadees, Frans en Japans.

Q. Welke persoonlijke firewalls worden ondersteund met de Cisco VPN-client?

A. Om een hoger niveau van beveiliging te bieden, kan de VPN-client de werking van een ondersteunde firewall afdwingen of een geduwd down stateful firewall-beleid voor internetgebonden verkeer ontvangen.

Op dit moment ondersteunt VPN-client 5.0 de volgende persoonlijke firewalls:

- BlackIce Defender
- Cisco Security Agent
- Sygate Mobile Firewall
- Sygate Mobile Firewall Pro
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

Om te beginnen in versie 3.1 wordt een nieuwe functie toegevoegd aan de VPN 3000 Concentrator die detecteert welke persoonlijke firewallsoftware externe gebruikers hebben geïnstalleerd en verhindert dat de gebruikers een verbinding kunnen maken zonder de juiste software. Kies **Configuratie > Gebruikersbeheer > Groepen > Clientsoftware** en klik op het tabblad voor de groep om deze functie te configureren

Raadpleeg voor meer informatie over het afdwingen van firewallbeleid op een Cisco VPN-clientmachine de firewallconfiguratiescenario's.

V. Zijn er aansluitingsproblemen bij het gebruik van Cisco VPN-client 3.x met AOL

7.0?

A. De Cisco VPN-client werkt niet met AOL 7.0 zonder gesplitste tunneling. Bekijk Cisco bug ID CSCdx04842 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie.

VPN-clientsoftwareconfiguratie

Q. Waarom koppelt de Cisco VPN-client na 30 minuten los? Mag ik deze periode verlengen?

A. Als er tijdens deze periode van 30 minuten geen communicatieactiviteit op een gebruikersverbinding is, wordt de verbinding beëindigd. De standaardinstelling van de inactiviteitstimer is 30 minuten, met een minimum toegestane waarde van 1 minuut en een maximum toegestane waarde van 2.147.483.647 minuten (meer dan 4.000 jaar).

Kies **Configuratie > Gebruikersbeheer > Groepen**, en kies de juiste groepsnaam om de instelling voor ongebruikte tijden aan te passen. Klik op **Wijzigen**, klik op het tabblad **HW-client** en type de gewenste waarde in het veld Time-out bij inactiviteitstimer van gebruiker. Type **0** om tijd uit te schakelen en een onbeperkte onbeperkte periode toe te staan.

Q. Kan de Cisco VPN-client worden uitgevoerd met alle parameters die vooraf zijn ingesteld?

A. Als het bestand vpnclient.ini bij de installatie is gebundeld met de VPN-clientsoftware wanneer het eerst wordt geïnstalleerd, wordt de VPN-client automatisch ingesteld. U kunt de profielbestanden (één .pcf-bestand voor elke verbindingsingang) ook distribueren als vooraf ingesteld verbindingsprofielen voor automatische configuratie. Voltooi de volgende stappen om vooraf ingestelde exemplaren van de VPN-clientsoftware aan gebruikers te distribueren:

1. Kopieer de VPN-clientsoftwarebestanden van de distributie-CD-ROM naar elke directory waarin u een VPN-client.ini-bestand (globaal) en afzonderlijke verbindingsprofielen hebt gemaakt voor een aantal gebruikers.**Opmerking:** Voor het Mac OS X-platform worden vooraf ingestelde bestanden in de profielen en bronnen-mappen geplaatst voordat de VPN-client is geïnstalleerd. Het vpnclient.ini-bestand wordt in de installatiemap geplaatst. U moet aangepaste vpnclient.ini-bestanden in de map VPN-clientinstallatieprogramma op hetzelfde niveau plaatsen als de mappen profielen en bronnen. Zie Hoofdstuk 2 van de VPN-clientgebruikershandleiding voor Mac OS X voor meer informatie
2. Bereid en distribueer de gebundelde software. Distributie van cd-rom of netwerk. Verzeker u ervan dat het bestand vpnclient.ini en de profielbestanden in dezelfde map staan als alle afbeeldingsbestanden van CD-ROM. U kunt gebruikers uit deze map laten installeren via een netwerkverbinding. of u kunt alle bestanden naar een nieuwe CD-ROM kopiëren voor distributie; of u kunt een ZIP-bestand maken dat zelf wordt geëxtraheerd en dat alle bestanden uit deze map bevat, terwijl gebruikers het kunnen downloaden en de software installeren.
3. Geef gebruikers alle andere benodigde configuratieinformatie en instructies. Zie Hoofdstuk 2 van de VPN-clientgebruikershandleiding voor uw platform.

Q. Het lijkt erop dat de Cisco VPN-client een conflict heeft met mijn NIC-kaart. Hoe

moet ik dit oplossen?

A. Zorg ervoor dat u de laatste stuurprogramma's op de NIC-kaart gebruikt. Dit wordt altijd aanbevolen. Indien mogelijk, test om te zien of het probleem specifiek is voor het besturingssysteem, PC hardware en andere NIC kaarten.

Q. Hoe automatisering ik de Cisco VPN-clientverbinding van inbelnetwerken?

A. Kies **Opties > Eigenschappen > Aansluitingen** en laat de Cisco VPN-client een inbel voor inbelnetwerk omlaag halen om de inbel-up naar de VPN-verbinding te automatiseren.

Q. Hoe vorm ik de Cisco VPN 3000 Concentrator om externe gebruikers op de hoogte te stellen voor VPN client update?

A. U kunt VPN-clientgebruikers op de hoogte stellen als het tijd is de VPN-clientsoftware op hun externe systemen bij te werken. Raadpleeg Afstandsgebruikers van een clientupdate voor een stapsgewijze benadering. Zorg ervoor dat u de releaseinformatie als "(Rel)" typt, zoals in stap 7 van het proces is opgemerkt.

Q. Wat kan een vertraging veroorzaken voordat de Cisco VPN-client wordt weergegeven, in het bijzonder wanneer de optie "Begin voor aanmelding" is ingeschakeld?

A. De Cisco VPN-client is in *de* terugvalmodus. Dit draagt bij aan de vertraging. In de back-upmodus presteert de VPN-client anders als start voordat de aanmelding is geactiveerd. Bij het werken in de back-upmodus controleert de VPN-client niet of de benodigde Windows-services zijn gestart. Als resultaat hiervan zou de VPN-verbinding kunnen mislukken als deze te snel werd geïnitieerd.Installeer de Cisco VPN-client en verwijder de offending applicaties om opstarten mogelijk te maken zonder in "fall back"-modus te zitten. Installeer vervolgens de Cisco VPN-client opnieuw. Raadpleeg voor meer informatie over de terugvalmodus Start voor de aanmelding.

Bekijk Cisco bug-ID's CSCdt8922 (alleen geregistreerde klanten) en CSCdt5739 (alleen geregistreerde klanten) in Bug Toolkit voor meer informatie.

Ik moet het verschil tussen ipsecdialer.exe en vpngui.exe begrijpen. Waarom is vpngui.exe in STARTUP in mijn Windows XP geïnstalleerd, maar ik moet nog handmatig beginnen in een dialoogvenster om mijn bedrijfsmiddelen te bereiken? En (afgezien van de omvang) lijken deze programma's hetzelfde te veroorzaken: een VPN-aanmelding bij mijn bedrijfsnetwerk.

A. Het ipsecdialer.exe was het oorspronkelijke lanceermechanisme voor de Cisco VPN-clientversie 3.x. Toen de GUI in de 4.x-versies werd gewijzigd, werd er een nieuw uitvoerbaar hulpprogramma met de naam vpngui.exe gemaakt. Het bestand ipsecdialer.exe werd alleen in naam uitgevoerd voor compatibiliteit op de achtergrond en startte gewoon het vpngui.exe. Dit is de reden waarom u het verschil in de bestandsgrootte kunt zien.

Wanneer u dus van versie 4.x naar versie 3.x van de Cisco VPN-client bent gedegradeerd, hebt u het bestand ipsecdialer.exe nodig om dit te starten.

Q. Kan ik het opstartVPN-pictogram veilig verwijderen? Waarom is die nodig?

A. De Cisco VPN-client in de opstartmap ondersteunt de optie "Begin voor aanmelding". Als u de functie niet gebruikt, hebt u deze niet nodig in de opstartmap.

Q. Waarom wordt "user_aanmelding" toegevoegd en niet in de sneltoets ipsecdialer.exe? Wat is het doel van "gebruikersaanmelding"?

A. Voor de optie "Begin voor aanmelding" is de "user_aanmelding" vereist, maar dit is niet nodig bij een normale start van de Cisco VPN-client.

Problemen met NAT/PAT

Q. Ik ervaart problemen met slechts één VPN-client (voor releases 3.3 en eerder) die verbinding kan maken via een PAT-apparaat (Port Address Translation). Wat kan ik doen om dit probleem te verzachten?

A. Er is een bug in verschillende NAT-implementaties (Network Address Translation)/PAT waardoor poorten van minder dan 1024 niet worden vertaald. Op Cisco VPN-client 3.1 gebruikt de ISAKMP-sessie (Internet Security Association en Key Management Protocol), zelfs met enabled NAT-transparantie, UDP 512. De eerste VPN-client gaat via het PAT-apparaat en houdt bronpoort 512 aan de buitenkant bij. Wanneer de tweede VPN-client zich aansluit, is poort 512 al in gebruik. De poging mislukt.

Er zijn drie mogelijke werkronden.

- Bevestig het PAT-apparaat.
- Upgradeer de VPN-clients naar 3.4 en gebruik TCP-insluiting.
- Installeer een VPN 3002 dat alle VPN-clients vervangt.

Q. Kan twee laptops vanuit dezelfde locatie worden aangesloten op de Cisco VPN-client?

A. Twee cliënten kunnen aan het zelfde head eind van de zelfde plaats verbinden zolang de cliënten niet beiden achter een apparaat zijn dat PAT zoals een router/firewall SOHO uitvoert. Veel PAT-apparaten kunnen de ONE VPN-verbinding naar een client achter de client in kaart brengen, maar niet twee. Om twee VPN cliënten toe te staan om van de zelfde plaats achter een apparaat te verbinden, geef een of ander soort insluiting zoals NAT-T, IPSec over UDP, of IPsec over TCP aan het hoofd toe. Over het algemeen, NAT-T of een andere insluiting zou moeten worden geactiveerd als EEN NAT-apparaat tussen de client en het head-end is.

Diversen

V. Als ik op kantoor verbinding maakt met het netwerk met mijn laptop en de laptop naar huis neemt, heb ik problemen met mijn verbinding met de VPN 3000 Concentrator van thuis. Wat is het probleem?

A. Mogelijk behoudt de laptop de routinginformatie van de LAN-verbinding. Raadpleeg VPN-

clients met Microsoft Routing Problemen voor informatie over de oplossing van dit probleem.

Vraag. Hoe kan ik weten of een VPN-client is verbonden met de VPN-concentrator?

A. Controleer de registratiesleutel genaamd HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. Als een tunnel actief is, is de waarde 1. Als er geen tunnel is, is de waarde 0.

Q. Ik heb problemen met de NetMeeting verbinding van een PC achter een VPN Concentrator aan een VPN client, maar de verbinding werkt wanneer ik van de PC naar een VPN client achter een VPN Concentrator loop. Hoe kan ik dit oplossen?

A. Volg de hier genoemde stappen om de verbindingsinstellingen te controleren:

- Kies op het hoofdstation van de pc **programmabestanden > Cisco Systems > VPN-client > profielen**. Klik met de rechtermuisknop op het profiel dat u gebruikt en kies **Met openen** om het profiel in een teksteditor (zoals Kladblok) te openen. (Wanneer u het te gebruiken programma kiest, dient u het vakje uit te schakelen dat luidt: **Gebruik dit programma altijd om deze bestanden te openen**.) Pak de profielparameter voor ForcekeepAlife vast en verander de waarde van 0 naar **1**, en bewaar het profiel.of
- Voor de VPN-client kiest u **Opties > Eigenschappen > Algemeen** en voert u een waarde in voor de "Peer response timeout", zoals in dit voorbeeldvenster wordt getoond. U kunt een tijdelijke gevoeligheid van 30 seconden tot 480 seconden specificeren.of
- Kies voor de VPN-concentrator **Configuratie > Gebruikersbeheer > Groepen > *groep wijzigen***. Kies in het tabblad IPsec de optie voor IKE-keepalives, zoals in dit voorbeeldvenster wordt weergegeven.

Het DPD-interval (Dead Peer Detection) varieert afhankelijk van de gevoeligheidsinstelling. Zodra een antwoord niet ontvangen is beweegt het zich in een agressievere modus en stuurt het elke vijf seconden een pakketten naar de peer response threshold (bij ontvangst van deze aanvallen). Op dat moment is de verbinding verbroken. U kunt de keepalives uitschakelen, maar als uw verbinding daadwerkelijk daalt, moet u op de tijdelijke versie wachten. Cisco raadt u aan om de gevoeligheidswaarde aanvankelijk zeer laag in te stellen.

Q. ondersteunt de Cisco VPN-client dubbele verificatie?

A. Nee. Dubbele verificatie wordt niet ondersteund op de Cisco VPN-client.

Vraag. Hoe kan ik de Cisco VPN-client configureren om verbinding te maken in de hoofdmodus, in plaats van in de agressieve modus?

A. U moet digitale handtekeningen (certificaten) gebruiken om Cisco VPN-client in de hoofdmodus te laten aansluiten. Daarvoor zijn twee methoden:

1. Verkrijg CA certificaten van de derde certificaathouder (bijvoorbeeld Verticaal of Vertrouw) op de router en alle Cisco VPN Clients. Installeer de identiteitscertificaten van dezelfde CA-server en gebruik digitale handtekeningen als authenticatie tussen de Cisco VPN-client en de router. Raadpleeg voor meer informatie over deze configuratie het configureren van IPSec tussen Cisco IOS routers en Cisco VPN-client die vertrouwenscertificaten gebruikt.

2. De tweede optie is om de router als de CA server samen met het hoofd te vormen aan de afstandsbediening VPN. Het installeren van de certificaten (en al het andere) zal blijven zoals beschreven in de vorige link behalve dat de router zich zal gedragen als een CA-server. Raadpleeg voor meer informatie Dynamic LAN-to-LAN VPN tussen Cisco IOS-routers die IOS CA gebruiken in het voorbeeld van de Hub Configuration.

Q. Hoe maak ik de vereiste parameters in het VPN client access bestand alleen lezen?

A. Voeg een uitroepteken (!) toe aan de voorkant van elke parameter in het .pcf-bestand voor elke gebruiker om de parameter alleen lezen te maken.

De waarden voor parameters die met een uitroepteken (!) beginnen kunnen niet door de gebruiker in de VPN-client worden gewijzigd. De velden voor deze waarden in de GUI zullen worden weergegeven (alleen lezen).

Hier is een voorbeeldconfiguratie:

Origineel .pcf-bestand

```
[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1

GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C85
              1ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice
```

Gewijzigd .pcf-bestand

```
[main]

!Description=connection to TechPubs server

!Host=10.10.99.30

AuthType=1

!GroupName=docusers
```

```
GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C
          851ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

!Username=alice
```

In dit voorbeeld kan de gebruiker de waarden *Description*, *Host*, *GroupName* en *Gebruikersnaam* niet wijzigen.

Q. Is het mogelijk de toegang voor VPN-klanten te beperken of te beperken op basis van MAC-adressen?

A. Nee. Het is niet mogelijk de toegang voor VPN-clients te beperken of te beperken op basis van MAC-adressen.

Gerelateerde informatie

- Cisco VPN 3000 clientondersteuningspagina
- Cisco VPN-clientondersteuningspagina
- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- Technische ondersteuning en documentatie – Cisco Systems