

# Probleemoplossingsgids AnyConnect VPN-client – veelvoorkomende problemen

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Troubleshooting](#)

[Problemen bij installatie en met virtuele adapter](#)

[Verbroken verbinding of niet mogelijk eerste verbinding tot stand te brengen](#)

[Problemen met passerend verkeer](#)

[Crashproblemen met AnyConnect](#)

[Problemen met fragmentatie/passierend verkeer](#)

[Automatisch verwijderen](#)

[Probleem met invullen van cluster-FQDN](#)

[Configuratie van back-upserverlijst](#)

[AnyConnect: Probleem met beschadigde stuurprogrammadatabase](#)

[Herstellen](#)

[Mislukte herstelpoging](#)

[De database analyseren](#)

[Foutmeldingen](#)

[Fout: Unable to Update the Session Management Database](#)

[Oplossing 1](#)

[Oplossing 2](#)

[Fout: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register"](#)

[Oplossing](#)

[Fout: "An error was received from the secure gateway in response to the VPN negotiation request. Please contact your network administrator"](#)

[Oplossing](#)

[Fout: Session could not be established. Session limit of 2 reached.](#)

[Oplossing 1](#)

[Oplossing 2](#)

[Fout: AnyConnect not enabled on VPN server bij verbinden van AnyConnect met ASA](#)

[Oplossing](#)

[Fout:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 \(threshold 1206\)](#)

[Oplossing](#)

[Fout: The secure gateway has rejected the agent's vpn connect or reconnect request.](#)

[Oplossing](#)

[Fout: "Unable to update the session management database"](#)

[Oplossing](#)

[Fout: "The VPN client driver has encountered an error"](#)

[Oplossing](#)

[Fout: "Unable to process response from xxx.xxx.xxx.xxx"](#)

[Oplossing](#)

[Fout: "Login Denied, unauthorized connection mechanism, contact your administrator"](#)

[Oplossing](#)

[Fout: "AnyConnect package unavailable or corrupted. Contact your system administrator"](#)

[Oplossing](#)

[Fout: "The AnyConnect package on the secure gateway could not be located"](#)

[Oplossing](#)

[Fout: "Secure VPN via remote desktop is not supported"](#)

[Oplossing](#)

[Fout: "The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established"](#)

[Oplossing](#)

[Fout: "Certificate Validation Failure"](#)

[Oplossing](#)

[Fout: "VPN Agent Service has encountered a problem and needs to close. We are sorry for the inconvenience"](#)

[Oplossing](#)

[Fout: "This installation package could not be opened. Verify that the package exists"](#)

[Oplossing](#)

[Fout: "Error applying transforms. Verify that the specified transform paths are valid."](#)

[Oplossing](#)

[Fout: "The VPN client driver has encountered an error"](#)

[Oplossing](#)

[Fout: "A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restored."](#)

[Oplossing](#)

[Fout van AnyConnect bij het aanmelden](#)

[Oplossing](#)

[Fout: IE-proxy-instelling wordt niet hersteld nadat AnyConnect-verbinding is verbroken op Windows 7](#)

[Oplossing](#)

[Fout: AnyConnect Essentials can not be enabled until all these sessions are closed.](#)

[Oplossing](#)

[Fout: Tabblad Verbindingen bij optie Internet van Internet Explorer wordt verborgen nadat verbinding met AnyConnect-client tot stand is gebracht.](#)

[Oplossing](#)

[Fout: Enkele gebruikers krijgen melding Login Failed Error terwijl anderen wel verbinding kunnen maken via AnyConnect VPN](#)

[Oplossing](#)

[Fout: The certificate you are viewing does not match with the name of the site you are trying to view.](#)

[Oplossing](#)

[Kan AnyConnect niet starten vanuit de CSD-vault op een computer met Windows 7](#)

[Oplossing](#)

[AnyConnect-profiel wordt niet gerepliceerd naar de standby na failover](#)

[Oplossing](#)

[AnyConnect-client crasht wanneer Internet Explorer offline gaat](#)

[Oplossing](#)

[Fout: TLSPROTOCOL\\_ERROR\\_INSUFFICIENT\\_BUFFER](#)

[Oplossing](#)

[Fout: "Connection attempt has failed due to invalid host entry"](#)

[Oplossing](#)

[Fout: "Ensure your server certificates can pass strict mode if you configure always-on VPN"](#)

[Oplossing](#)

[Fout: "An internal error occurred in the Microsoft Windows HTTP Services"](#)

[Oplossing](#)

[Fout: "Het SSL-transport heeft een beveiligde kanaalstoring ontvangen. May be a result of a unsupported crypto configuration on the Secure Gateway."](#)

[Oplossing](#)

[Gerelateerde informatie](#)

## Inleiding

In dit document wordt een troubleshooting-scenario beschreven voor toepassingen die niet werken via de Cisco AnyConnect VPN-client.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco ASA (adaptive security applicatie) met versie 8.x.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Troubleshooting

Dit typische troubleshooting-scenario geldt voor toepassingen die niet werken via de Cisco AnyConnect VPN-client en is bedoeld voor eindgebruikers met Microsoft Windows-computers. In de volgende secties worden oplossingen beschreven voor de volgende problemen:

- [Problemen bij installatie en met virtuele adapter](#)
- [Verbroken verbinding of niet mogelijk eerste verbinding tot stand te brengen](#)

- [Problemen met passerend verkeer](#)
- [Crashproblemen met AnyConnect](#)
- [Problemen met fragmentatie/passerend verkeer](#)

## Problemen bij installatie en met virtuele adapter

Voer de volgende stappen uit:

1. Haal het logboek van het apparaat op:

Windows XP/Windows 2000:

```
\Windows\setupapi.log
```

Windows Vista:

**Opmerking:** Verborgen mappen moeten zichtbaar zijn om deze bestanden te kunnen zien.

```
\Windows\Inf\setupapi.app.log  
  \Windows\Inf\setupapi.dev.log
```

Als u fouten in het logbestand van **setupapi** ziet, kunt u breedtegraad instellen op 0x2000FFFF.

2. Haal het logboek van het MSI-installatieprogramma op:

Bij een eerste installatie voor webimplementatie bevindt dit logboek zich in de map temp van de gebruiker.

Windows XP/Windows 2000:

```
\Documents and Settings\  
  \
```

Windows Vista:

`\Users\`

Als er sprake is van een automatische upgrade, bevindt dit logboek zich in de map temp van het systeem:

`\Windows\Temp`

De bestandsnaam heeft de volgende opmaak: **anyconnect-win-x.x.xxxx-k9-install-yyyy.log**. Haal het recentste bestand op voor de versie van de client die u wilt installeren. De waarde x.xxxx verandert op basis van de versie (bijvoorbeeld 2.0.0343); yyyyyyyyyyyyyy staat voor de datum en tijd van de installatie.

3. Haal het bestand met de pc-systeeminformatie op:

Typ het volgende in een opdrachtprompt-/DOS-venster:

Windows XP/Windows 2000:

```
winmsd /nfo c:\msinfo.nfo
```

Windows Vista:

```
msinfo32 /nfo c:\msinfo.nfo
```

**Opmerking:** Wacht even nadat u dit heeft getypt. Het kan twee tot vijf minuten duren voordat het bestand is gegenereerd.

Haal een bestandsdump van systeeminformatie op via een opdrachtprompt:

Windows XP en Windows Vista:

```
systeminfo c:\sysinfo.txt
```

Zie [AnyConnect: Probleem met beschadigde stuurprogrammadatabase voor het opsporen van fouten met het stuurprogramma.](#)

## Verbroken verbinding of niet mogelijk eerste verbinding tot stand te brengen

Heeft verbindingproblemen met de AnyConnect-client, zoals verbroken verbindingen, of als het niet mogelijk is om een eerste verbinding tot stand te brengen? Haal dan de volgende bestanden op:

- Het configuratiebestand van de ASA om te bepalen of iets in de configuratie de verbindingfout veroorzaakt:

Vanuit de console van de ASA, type `schrijf netto x.x.x:ASA-Config.txt` waar `x.x.x` het IP-adres van een TFTP-server op het netwerk is.

OF

Typ in de ASA-console `show running-config`. Wacht tot de configuratie volledig op het scherm wordt getoond, kopieer deze dan naar een tekstverwerker en sla de configuratie op.

- De ASA-gebeurtenislogboeken:

Om ASA-logboekregistratie van autorisatie-, WebVPN-, SSL- (Secure Sockets Layer) en SVC-evenementen (SSL VPN-client) mogelijk te maken, voert u de volgende CLI-opdrachten uit:

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

Start een AnyConnect-sessie en controleer of de fout kan worden gereproduceerd. Kopieer de logboekregistratie van de console naar een tekstverwerker en sla deze op.

Als u logboekregistratie wilt uitschakelen, voert u de opdracht `no logging enable` uit.

- Het logbestand van de Cisco AnyConnect VPN-client in Windows Event Viewer (Logboeken) op de client-pc:

Selecteer **Start > Run** (Start > Uitvoeren).

Voer in:

```
eventvwr.msc /s
```

Klik met de rechtermuisknop op het logboek van de **Cisco AnyConnect VPN-client** en selecteer **Save Log File As (Logbestand opslaan als) AnyConnect.evt**.

**Opmerking:** Sla het bestand altijd op in de bestandsindeling **.evt**.

Als de gebruiker geen verbinding kan maken met de AnyConnect VPN-client, wordt het probleem mogelijk veroorzaakt door een tot stand gebrachte RDP-sessie (Remote Desktop Protocol) of doordat Snelle gebruikerswisseling is ingeschakeld op de client-pc. De gebruiker ziet de foutmelding `AnyConnect profile settings mandate a single local user, but multiple local users are currently logged into your computer. A VPN connection will not be established. (AnyConnect-profielinstellingen machtigen één lokale gebruiker, maar momenteel zijn meerdere gebruikers bij uw computer aangemeld. Er wordt geen VPN-verbinding tot stand gebracht.)` op de client-pc. Om dit probleem op te lossen, moet elke tot stand gebrachte RDP-sessie worden verbroken en de functie Snelle gebruikerswisseling worden uitgeschakeld. Dit gedrag wordt gestuurd door uitvoering van het kenmerk [Windows Logon Enforcement \(Afdwinging van Windows-aanmelding\) in het clientprofiel, maar momenteel is er geen instelling die een gebruiker toestaat een VPN-verbinding tot stand te brengen terwijl meerdere gebruikers tegelijk op dezelfde computer zijn aangemeld](#). Verbeteringsaanvraag [CSCsx15061](#) is gedeponeed om deze optie aan te pakken.

**Opmerking:** Zorg dat poort 443 niet wordt geblokkeerd zodat de AnyConnect-client verbinding kan maken met de ASA.

Wanneer een gebruiker de AnyConnect VPN-client niet kan verbinden met de ASA, wordt het probleem mogelijk veroorzaakt door een incompatibiliteit tussen de versie van de AnyConnect-client en de versie van de software-image van de ASA. In dat geval wordt de volgende foutmelding getoond: `The installer was not able to start the Cisco VPN client, clientless access is not available` (Het installatieprogramma kan de Cisco VPN-client niet starten, clientloze toegang is niet mogelijk).

Om dit probleem op te lossen, voert u een upgrade uit van de versie van de AnyConnect-client zodat deze compatibel is met de versie van de software-image van de ASA.

Wanneer u zich voor de eerste keer aanmeldt bij AnyConnect, wordt het aanmeldingsscript niet uitgevoerd. Als u de verbinding verbreekt en uzelf opnieuw aanmeldt, wordt het aanmeldingsscript wel goed uitgevoerd. Dit is het verwachte gedrag.

Wanneer u de AnyConnect VPN-client verbinding laat maken met de ASA, wordt mogelijk de volgende foutmelding getoond: `User not authorized for AnyConnect Client access, contact your administrator`. (Gebruiker is niet geautoriseerd voor toegang tot AnyConnect-client. Neem contact op met de beheerder.)

Deze foutmelding wordt getoond wanneer de AnyConnect-image ontbreekt in de ASA. Zodra de image in de ASA is geladen, kan AnyConnect zonder problemen verbinding maken met de ASA.

Deze fout kan worden opgelost door Datagram Transport Layer Security (DTLS) uit te schakelen. Ga naar **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect**

**Connection Profiles (Configuratie > VPN voor externe toegang > Netwerktogang (client) > AnyConnect-verbindingprofielen) en verwijder het vinkje uit het selectievakje Enable DTLS (DTLS inschakelen). Hierdoor wordt DTLS uitgeschakeld.**

De dartbundle-bestanden bevatten de volgende foutmelding wanneer de verbinding van de gebruiker wordt verbroken: `TUNNELPROTOCOLDPDMGR_FOUR_NO_DPD_RESPONSE:De beveiligde gateway is niet ingegaan op Dead Peer Detectie-pakketten`. Deze melding geeft aan dat het DTLS-kanaal is verbroken als gevolg van een DPD-fout (Dead Peer Detection). U kunt deze fout oplossen door de DPD-keepalives aan te passen en de volgende opdrachten uit te voeren:

```
webvpn
svc keepalive 30
svc dpd-interval client 80
svc dpd-interval gateway 80
```

In ASA-versie 8.4(1) en hoger worden de opdrachten `svc keepalive` en `svc dpd-interval` vervangen door de respectievelijke opdrachten `anyconnect keepalive` en `anyconnect dpd-interval` zoals hieronder wordt getoond:

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

## Problemen met passerend verkeer

Wanneer problemen worden gedetecteerd met passerend verkeer naar het private netwerk tijdens een AnyConnect-sessie via de ASA, moet u de volgende stappen uitvoeren om data te verzamelen:

1. Haal de output van de ASA-opdracht `show vpn-sessiondb detail svc filter name <username>` op van de console. Als de output `Filter Name: XXXXX`, verzamel dan de uitvoer voor weergave van de toegangslijst in XXXXX. Controleer of access-list XXXXX de beoogde verkeersstroom niet blokkeert.
2. Exporteer de AnyConnect-statistieken via **AnyConnect VPN Client > Statistics > Details > Export (AnyConnect VPN-client > Statistieken > Details > Exporteren)** naar bestand `AnyConnect-ExportedStats.txt`.
3. Controleer het ASA-configuratiebestand op de aanwezigheid van **nat-instructies**. Als Network Address Translation (NAT) is ingeschakeld, moeten die instructies data vrijstellen die als gevolg van NAT naar de client worden geretourneerd. Om bijvoorbeeld de IP-adressen uit de AnyConnect-pool vrij te stellen via NAT (nat 0), voert u het volgende in via de opdrachtregelinterface:

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. Bepaal of de getunnelde standaardgateway moet worden ingeschakeld voor de configuratie.



De traditionele standaardgateway is de gateway die als laatste optie wordt gebruikt voor niet-ontsleuteld verkeer.

Voorbeeld:

```
!--- Route outside 0 0 is an incorrect statement.

route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

Als de VPN-client bijvoorbeeld toegang nodig heeft tot een bron die niet is opgenomen in de routingtabel van de VPN-gateway, wordt het pakket gerouteerd via de standaardgateway. De VPN-gateway heeft hiervoor niet de gehele interne routingtabel nodig. In dat geval kan het trefwoord **tunneled** worden gebruikt.

5. Verifieer of het AnyConnect-verkeer wordt afgewezen door het controlebeleid van de ASA. U kunt de specifieke toepassing die door de AnyConnect-client wordt gebruikt vrijstellen als u het Modular Policy Framework van Cisco ASA implementeert. U kunt bijvoorbeeld het skinny protocol vrijstellen met de volgende opdrachten.

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect skinny
```

## Crashproblemen met AnyConnect

Voer de volgende stappen uit om data te verzamelen:

1. Controleer of het Microsoft-hulpprogramma Dr. Watson is ingeschakeld. Om dit te doen, kiest u **Start > Run** en voert u het programma **Drwtsn32.exe** uit. Configureer en klik op **OK**:

```
Number of Instructions      : 25
Number of Errors To Save  : 25
Crash Dump Type           : Mini
Dump Symbol Table         : Checked
Dump All Thread Contexts  : Checked
Append To Existing Log File : Checked
Visual Notification       : Checked
Create Crash Dump File    : Checked
```

Wanneer de crash optreedt, kopieert u de **.log** en **.dmp** bestanden op uit **C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson**. Als deze bestanden in gebruik zijn, gebruikt u **ntbackup.exe**.

2. Haal het logboek van de Cisco AnyConnect VPN-client op uit Windows Event Viewer (Logboeken) op de client-pc:

Selecteer **Start > Run** (Start > Uitvoeren).

Voer in:

```
eventvwr.msc /s
```

Klik met de rechtermuisknop op het logboek van de **Cisco AnyConnect VPN-client** en selecteer **Save Log File As** (Logbestand opslaan als) **AnyConnect.evt**.

**Opmerking:** Sla het bestand altijd op in de bestandsindeling **.evt**.

## Problemen met fragmentatie/passierend verkeer

Sommige toepassingen, zoals Microsoft Outlook, werken niet. De tunnel kan echter wel ander verkeer laten passeren, zoals kleine pings.

Dit kan inzicht wijzen op een fragmentatieprobleem in het netwerk. Met name niet-zakelijke routers zijn slecht in het fragmenteren en opnieuw samenstellen van pakketten.

Gebruik een reeks pings van toenemende lengte om te bepalen of het misgaat bij een bepaalde grootte. Bijvoorbeeld ping -l 500, ping -l 1000, ping -l 1500, ping -l 2000.

Het wordt aanbevolen een speciale groep te configureren voor gebruikers met fragmentatieproblemen en de Maximum Transition Unit (MTU) van de SVC voor die groep in te stellen op 1200. Op die manier kunt u gebruikers helpen die dit probleem ervaren, maar wordt de bredere gebruikersgroep niet beïnvloed.

### Probleem

TCP-verbindingen blijven hangen nadat verbinding is gemaakt met AnyConnect.

### Oplossing

Om te verifiëren of de gebruiker een fragmentatieprobleem heeft, past u de MTU voor AnyConnect-clients op de ASA aan.

```
ASA(config)#group-policy <name> attributes
webvpn
svc mtu 1200
```

## Automatisch verwijderen

### Probleem

De AnyConnect VPN-client verwijdert zichzelf zodra de verbinding wordt beëindigd. In de logboeken van de client staat dat de optie keep installed is uitgeschakeld.

### Oplossing

AnyConnect verwijderd zichzelf, ondanks dat de optie **keep installed is geselecteerd in Adaptive Security Device Manager (ASDM)**. Om dit probleem op te lossen, configureert u de opdracht **svc keep-installer installed** onder groepsbeleid.

## Probleem met invullen van cluster-FQDN

**Probleem:** AnyConnect-client wordt vooraf gevuld met de hostnaam in plaats van de cluster-FQDN (Fully Qualified Domain Name).

Wanneer u een taakverdelingscluster heeft ingesteld voor SSL VPN en de client verbinding met het cluster probeert te maken, wordt het verzoek omgeleid naar het ASA-knooppunt en kan de client zich aanmelden. Wanneer de client na enige tijd opnieuw verbinding met het cluster probeert te maken, is de cluster-FQDN niet aanwezig bij de vermeldingen **Connect to (Verbinding maken met)**. In plaats daarvan wordt het ASA-knooppunt getoond waarnaar de client was omgeleid.

## Oplossing

Dit probleem wordt veroorzaakt doordat de AnyConnect-client de hostnaam behoudt waarmee voor het laatst verbinding is gemaakt. Dit gedrag is vastgelegd als een bug. Raadpleeg voor volledige informatie over de bug Cisco [CSCsz39019](#) van [het](#) bug-ID. De voorgestelde tijdelijke oplossing is om de Cisco AnyConnect naar versie 2.5 te upgraden.

## Configuratie van back-upserverlijst

Een back-upserverlijst wordt geconfigureerd voor het geval dat de hoofdserver die de gebruiker selecteert niet bereikbaar is. Dit wordt gedefinieerd in het venster **Backup Server (Back-upserver)** in het **AnyConnect-profiel**. Voer de volgende stappen uit:

1. Download [AnyConnect Profile Editor \(alleen voor geregistreerde klanten\)](#). De bestandsnaam is **AnyConnectProfileEditor2\_4\_1.jar**.
2. Maak een XML-bestand via AnyConnect Profile Editor.

Ga naar het tabblad **Server list (Serverlijst)**.

Klik op **Add (Toevoegen)**.

Voer in het veld **Hostname (Hostnaam)** de hoofdserver in.

Voeg de back-upserver toe onder de back-upserverlijst in het veld **Host address (Hostadres)**. Klik vervolgens op **Add (Toevoegen)**.

3. Zodra u het XML-bestand heeft, moet u dit toewijzen aan de verbinding die u op de ASA gebruikt.

Ga in ASDM naar **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** (Configuratie > VPN voor externe toegang > Netwerктоegang (client) > AnyConnect-verbindingprofielen).

Selecteer uw profiel en klik op **Edit** (Bewerken).

Klik op **Manage (Beheren)** in de sectie **Default Group Policy (Standaardgroepsbeleid)**.

Selecteer uw groepsbeleid en klik op **Edit** (Bewerken).

Selecteer **Advanced (Geavanceerd)** en klik vervolgens op **SSL VPN Client (SSL VPN-client)**.

Klik op **New** (Nieuw). Voer een naam in voor het profiel en wijs het XML-bestand toe.

4. Verbind de client met de sessie om het XML-bestand te downloaden.

## AnyConnect: Probleem met beschadigde stuurprogrammadatabase

De volgende vermelding in het bestand SetupAPI.log geeft aan dat het catalogussysteem mogelijk beschadigd is:

```
W239 driver signing class list "C:\WINDOWS\INF\certclas.inf" was missing or invalid. Error
0xfffffde5: Unknown Error. (Handtekeningklassenlijst van stuurprogramma W239
"C:\WINDOWS\INF\certclas.inf" ontbrak of was ongeldig. Fout 0xfffffde5: Onbekende fout.), ervan
uitgaande dat alle apparaatklassen onderhevig zijn aan handtekeningverificatiebeleid.
```

U kunt ook de volgende foutmelding krijgen: **Error(3/17): Unable to start VA, setup shared queue, or VA gave up shared queue** (Fout (3/17): Kan VA niet starten, instellen van gedeelde wachtrij, of VA heeft gedeelde wachtrij beëindigd).

Op de client kunt u de volgende melding krijgen: **"Het VPN-clientstuurprogramma heeft een fout aangetroffen"**.

### Herstellen

Dit probleem is te wijten aan Cisco bug-ID [CSCsm54689](#). Zorg ervoor dat routing en Remote Access Service zijn uitgeschakeld voordat u AnyConnect start. Als dit het probleem niet oplost, voer dan de volgende stappen uit:

1. Open een opdrachtprompt als beheerder op de pc (bij Vista: opdrachtprompt met verhoogde bevoegdheid).
2. Voer de opdracht `net stop cryptSvc` uit.
3. Voer uit:

```
esentutl /p%systemroot%\System32\catroot2\
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. Klik op **OK** wanneer daarom wordt gevraagd om te herstellen.

5. Sluit de opdrachtprompt.
6. Start opnieuw op.

## Mislukte herstelpoging

Als het herstellen mislukt, voer dan de volgende stappen uit:

1. Open een opdrachtprompt als beheerder op de pc (bij Vista: opdrachtprompt met verhoogde bevoegdheid).
2. Voer de opdracht `net stop CryptSvc` uit.
3. Wijzig de naam van de map `%WINDIR%\system32\catroot2` in `catroot2_old`.
4. Sluit de opdrachtprompt.
5. Start opnieuw op.

## De database analyseren

U kunt de database op elk gewenst moment analyseren om te bepalen of deze geldig is.

1. Open een opdrachtprompt als beheerder op de pc.
2. Voer uit:

```
esentut1 /g%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

Raadpleeg het artikel [System Catalog Database Integrity \(Integriteit van database van systeemcatalogus\)](#) voor meer informatie.

## Foutmeldingen

### Fout: Unable to Update the Session Management Database

Terwijl de SSL VPN is verbonden via een webbrower, wordt de foutmelding `Unable to Update the Session Management Database`. (Kan de sessiebeheerdatabase niet bijwerken.) getoond en bevatten de ASA-logboeken de vermelding `%ASA-3-211001: Memory allocation Error. The adaptive security appliance failed to allocate RAM system memory`. (Geheugentoewijzingsfout. De adaptieve security applicatie kan geen RAM-systeemgeheugen toekennen.)

### Oplossing 1

Dit probleem is te wijten aan Cisco bug-ID [CSCsm51093](#). Om dit probleem op te lossen, laadt u

de ASA-software opnieuw op of upgrade van de ASA-software naar de voorlopige release die in het bug wordt genoemd. Raadpleeg Cisco bug-id [CSCsm51093](#) voor meer informatie .

## Oplossing 2

Dit probleem kan ook worden opgelost door dreigingsdetectie op de ASA uit te schakelen (als dreigingsdetectie wordt gebruikt).

### **Fout: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register"**

Wanneer u de AnyConnect-client gebruikt op laptops of pc's kan tijdens de installatie een fout optreden:

```
"Module C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register..."
```

In dat geval kan het installatieprogramma niet verder worden uitgevoerd en wordt de client verwijderd.

## Oplossing

Hierna volgen de mogelijke tijdelijke oplossingen om deze fout op te lossen:

- De nieuwste AnyConnect-client wordt niet meer officieel ondersteund op Microsoft Windows 2000. Het betreft een registerprobleem op de Windows 2000-computer.
- Verwijder de VMware-toepassingen. Zodra AnyConnect is geïnstalleerd kunnen de VMware-toepassingen weer op de pc worden gezet.
- Voeg de ASA toe aan de vertrouwde sites.
- Kopieer de volgende bestanden uit de map **\ProgramFiles\Cisco\CiscoAnyconnect** naar een **nieuwe map** en voer daarna via de opdrachtprompt **regsvr32 vpnapi.dll** uit:

```
vpnapi.dllvpncommon.dllvpncommoncrypt.dll
```

- Maak een nieuwe image van het besturingssysteem op de laptop/pc.

Het logboekbericht gerelateerd aan deze fout op de AnyConnect-client is ongeveer als volgt:

```
DEBUG: Error 2911: Could not remove the folderC:\Program Files\Cisco\Cisco AnyConnect VPN Client\.
```

```
The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 2911. The arguments are:
```

```
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
```

```
DEBUG: Error 2911: Could not remove the folder C:\Program Files\Cisco\Cisco AnyConnect VPN Client\.
```

```
The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 2911. The arguments are:
```

```
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
```

```
Info 1721. There is a problem with this Windows Installer package. A program required for
```

this install to complete could not be run. Contact your support personnel or package vendor. Action: InstallHelper.exe, location: C:\Program Files\Cisco\Cisco AnyConnect VPN Client\InstallHelper.exe, command: -acl "C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\\" -r

## **Fout: "An error was received from the secure gateway in response to the VPN negotiation request. Please contact your network administrator"**

Deze fout wordt getoond wanneer clients verbinding proberen te maken met het VPN via de Cisco AnyConnect VPN-client.

De volgende melding is ontvangen van de beveiligde gateway:

"Illegal address class" (Ongeldige adresklasse), "Host or network is 0" (Host of netwerk is 0) of "Other error" (Andere fout)

### **Oplossing**

Het probleem treedt op als gevolg van het leegraken van de lokale IP-adresgroep van de ASA. Als de VPN-groepsbron leeg is, moet het bereik van de IP-adresgroep worden vergroot.

Voor dit probleem is Cisco bug-ID [CSCsl82188 vastgelegd](#). Deze fout treedt doorgaans op wanneer de lokale groep voor adrestoewijzing leeg is, of als een 32-bits subnetmasker wordt gebruikt voor de adresgroep. De tijdelijke oplossing hiervoor is het uitbreiden van de adresgroep en het gebruik van een 24-bits subnetmasker.

## **Fout: Session could not be established. Session limit of 2 reached.**

Wanneer u meer dan twee clients verbinding wilt laten maken met de AnyConnect VPN-client, wordt de foutmelding `Login Failed` (Aanmelden mislukt) getoond op de client en wordt in de ASA-logboeken het volgende waarschuwingsbericht opgenomen: `Session could not be established. Session limit of 2 reached`. Ik heb een **AnyConnect Essentials-licentie op de ASA, die versie 8.0.4 draait**.

### **Oplossing 1**

Deze fout komt voor omdat de **AnyConnect essentiële** licentie niet wordt ondersteund door ASA versie 8.0.4. U moet de ASA upgrades naar versie 8.2.2 uitvoeren. Dit lost de fout op.

**Opmerking:** Als de sessielimiet is bereikt, krijgt de gebruiker de foutmelding `Login Failed` (Aanmelden mislukt), ongeacht welke licentie er wordt gebruikt.

### **Oplossing 2**

Deze fout kan ook optreden wanneer de opdracht `vpn-sessiondb max-anyconnect-premium-or-essentials-limit session-limit` wordt gebruikt om de limiet in te stellen voor het aantal VPN-sessies dat tot stand kan worden gebracht. Als de sessielimiet wordt ingesteld op twee, kan de gebruiker slechts twee sessies tot stand brengen, ook als de geïnstalleerde licentie meer sessies ondersteunt. Stel de sessielimiet in op het aantal benodigde VPN-sessies om deze foutmelding te voorkomen.

## **Fout: AnyConnect not enabled on VPN server bij verbinden van AnyConnect met**

## ASA

U krijgt de foutmelding `AnyConnect not enabled on VPN server` (AnyConnect niet ingeschakeld op VPN-server) wanneer u AnyConnect wilt verbinden met de ASA.

### Oplossing

U lost deze fout op door AnyConnect in te schakelen op de buiteninterface van de ASA met ASDM. Raadpleeg voor meer informatie over het inschakelen van AnyConnect op de externe interface het [configureren](#) van [Clientloze SSL VPN \(WebVPN\) in de ASA](#).

### Fout:- %ASA-6-722036: Group client-group User xxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

Het bericht `%ASA-6-722036: Group < client-group > User < xxx > IP < x.x.x.x > Transmitting large packet 1220 (threshold 1206) error` (Gebruiker `<xxx>` met IP `<x.x.x.x>` in groep `<clientgroep>` verzendt groot pakket 1220 (drempelwaarde 1206)) wordt vastgelegd in de logboeken van de ASA. Wat betekent dit logboekbericht en hoe kan het probleem worden opgelost?

### Oplossing

Dit logboekbericht geeft aan dat een groot pakket naar de client is verzonden. De bron van het pakket is niet op de hoogte van de MTU van de client. Dit kan ook het gevolg zijn van compressie van data die niet kunnen worden gecomprimeerd. Als tijdelijke oplossing kan SVC-compressie worden uitgeschakeld met de opdracht [svc compression none](#). Hiermee wordt het probleem opgelost.

### Fout: The secure gateway has rejected the agent's vpn connect or reconnect request.

De volgende foutmelding wordt getoond wanneer u verbinding maakt met de AnyConnect-client: `"The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires re-authentication and must be started manually. Please contact your network administrator if this problem persists. The following message was received from the secure gateway: no assigned address"`. (De beveiligde gateway heeft het verzoek van de agent tot (vernieuwde) VPN-verbinding afgewezen. Voor een nieuwe verbinding is herverificatie nodig en deze moet handmatig worden gestart. Neem contact op met de netwerkbeheerder als dit probleem zich blijft voordoen. De volgende melding werd ontvangen van de beveiligde gateway: Geen toegewezen adres).

U krijgt deze foutmelding ook wanneer u verbinding maakt met de AnyConnect-client: `"De beveiligde poort heeft de verbindingsooging verworpen. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication. Het volgende bericht werd ontvangen van de veilige gateway:Host of Network is 0"`.

U krijgt deze foutmelding ook wanneer u verbinding maakt met de AnyConnect-client: `"The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires re-authentication and must be started manually. Please contact the network administrator if the problem persists. The following message was received from the secure gateway: No License"`. (De beveiligde gateway heeft het verzoek van de agent tot (vernieuwde) VPN-verbinding afgewezen. Voor een nieuwe verbinding is herverificatie nodig en deze moet handmatig worden gestart. Neem contact op met de netwerkbeheerder als dit probleem zich blijft voordoen. De volgende melding



werd ontvangen van de beveiligde gateway: Geen licentie.)

## Oplossing

De router had geen groepsconfiguratie na het opnieuw laden. U moet de betreffende configuratie opnieuw toevoegen aan de router.

```
Router#show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254  
svc address-pool SSLPOO
```

De foutmelding "The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires re-authentication and must be started manually. Please contact the network administrator if the problem persists. The following message was received from the secure gateway: No License". (De beveiligde gateway heeft het verzoek van de agent tot (vernieuwde) VPN-verbinding afgewezen. Voor een nieuwe verbinding is herverificatie nodig en deze moet handmatig worden gestart. Neem contact op met de netwerkbeheerder als dit probleem zich blijft voordoen. De volgende melding werd ontvangen van de beveiligde gateway: Geen licentie".) wordt getoond wanneer de AnyConnect Mobility-licentie ontbreekt. Zodra de licentie is geïnstalleerd is het probleem opgelost.

## Fout: "Unable to update the session management database"

Wanneer u in WebPortal wilt verifiëren, krijgt u de volgende foutmelding: "Kan de sessiebeheerdatabse niet bijwerken".

## Oplossing

Dit probleem is gerelateerd aan geheugentoe wijzing op de ASA. Deze kwestie wordt het meest aangetroffen wanneer de ASA Versie 8.2.1 is. Oorspronkelijk vereist dit een 512 MB RAM voor zijn volledige functionaliteit.

Upgrade het geheugen naar 512 MB om dit probleem permanent op te lossen.

Als tijdelijke oplossing kunt u geheugen proberen vrij te maken door de volgende stappen uit te voeren:

1. Schakel dreigingsdetectie uit.
2. Schakel SVC-compressie uit.
3. Laad de ASA opnieuw.

## Fout: "The VPN client driver has encountered an error"

Deze foutmelding wordt getoond op de clientcomputer wanneer u verbinding maakt met AnyConnect.

## Oplossing

Voer de volgende procedure uit om de AnyConnect VPN-agent handmatig op Interactive (Interactief) te zetten en dit probleem op te lossen:

1. Klik met de rechtermuisknop op **My Computer > Manage > Services and Applications > Services (Deze Computer > Beheren > Services en toepassingen > Services)** en selecteer de **Cisco AnyConnect VPN-agent**.
2. Klik met de rechtermuisknop op **Properties (Eigenschappen)**, meld u aan en selecteer **Allow service to interact with the desktop** (Service kan interactief met bureaublad worden uitgevoerd).

Hierdoor wordt de DWORD-waarde van `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent` in het Windows-register ingesteld op 110 (de standaardwaarde is 010).

**Opmerking:** Het heeft hierbij de voorkeur om het transformatiebestand met extensie **.MST te gebruiken**. Als u dit namelijk handmatig via deze methoden instelt, moet dit na elke installatie/upgrade worden gedaan. Daarom is het van belang de toepassing te identificeren die het probleem veroorzaakt.

Wanneer Routing and Remote Access Service (RRAS) wordt ingeschakeld op de Windows-computer, werkt AnyConnect niet en wordt de foutmelding `The VPN client driver has encountered an error`. (Het stuurprogramma van de VPN-client heeft een fout aangetroffen.) getoond. Om dit probleem op te lossen, moet de Routing and Remote Access Service (RRAS) worden uitgeschakeld voordat u AnyConnect start. Raadpleeg Cisco bug-ID [CSCsm54689 voor meer informatie](#).

## Fout: "Unable to process response from xxx.xxx.xxx.xxx"

AnyConnect-clients kunnen geen verbinding maken met een Cisco ASA. In het AnyConnect-venster wordt de foutmelding `"Unable to process response from xxx.xxx.xxx.xxx"` (Kan respons van xxx.xxx.xxx.xxx niet verwerken) getoond.

## Oplossing

Probeer deze tijdelijke oplossingen om dit probleem op te lossen:

- Verwijder WebVPN van de ASA en installeer dit daarna opnieuw.
- Wijzig het poortnummer van het bestaande 443 naar 444 en zet dit weer op 443.

Raadpleeg deze [oplossing](#) voor meer informatie over het inschakelen van WebVPN en het wijzigen van de poort voor WebVPN.

## Fout: "Login Denied, unauthorized connection mechanism, contact your administrator"

AnyConnect-clients kunnen geen verbinding maken met een Cisco ASA. In het AnyConnect-venster wordt de foutmelding `"Login Denied, unauthorized connection mechanism, contact your administrator"` getoond.

`administrator`" (Aanmelden niet toegestaan, ongeautoriseerd verbindingmechanisme, neem contact op met de beheerder) getoond.

## Oplossing

Deze foutmelding is meestal het gevolg van configuratieproblemen (onjuiste of onvolledige configuratie). Controleer de configuratie en zorg dat deze aan de eisen voldoet om het probleem op te lossen.

<

## Fout: "AnyConnect package unavailable or corrupted. Contact your system administrator"

Deze fout treedt op wanneer u de AnyConnect-software start op een Macintosh-client om verbinding te maken met een ASA.

## Oplossing

Voer de volgende stappen uit om dit probleem op te lossen:

1. Upload het AnyConnect-pakket voor Macintosh naar het flash-geheugen van de ASA.
2. Pas de WebVPN-configuratie aan om het AnyConnect-pakket aan te geven dat wordt gebruikt.

```
webvpn
svc image disk0:/anyconnect-macosx-i386-2.3.2016-k9.pkg 2
svc image disk0:/anyconnect-macosx-powerpc-2.3.2016-k9.pkg 3
```

In ASA-versie 8.4(1) en hoger wordt de opdracht `svc image` vervangen door de opdracht `anyconnect image` zoals hieronder wordt getoond:

```
hostname(config)#webvpn

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-win-3.0.0527-k9.pkg 1

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

## Fout: "The AnyConnect package on the secure gateway could not be located"

Deze fout wordt veroorzaakt op de Linux-computer van de gebruiker wanneer wordt getracht verbinding te maken met de ASA door AnyConnect te starten. De volledige foutmelding is als volgt:

"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."

## Oplossing

Controleer of het besturingssysteem (OS) op de clientcomputer wordt ondersteund door de AnyConnect-client.

Als het besturingssysteem wordt ondersteund, moet u controleren of het AnyConnect-pakket is opgegeven in de WebVPN-configuratie. Zie [AnyConnect package unavailable or corrupted in dit document voor meer informatie](#).

## Fout: "Secure VPN via remote desktop is not supported"

Gebruikers krijgen geen toegang tot een externe desktop. De foutmelding `Secure VPN via remote desktop is not supported` (Beveiligd VPN via externe desktop wordt niet ondersteund) wordt getoond.

## Oplossing

Dit probleem wordt veroorzaakt door de volgende Cisco bug-ID's: [CSCsu22088](#) en [CSCso42825](#). Als u de AnyConnect VPN-client verbetert, kan dit probleem worden opgelost. Raadpleeg de genoemde bugs voor meer informatie.

## Fout: "The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established"

Wanneer u verbinding via VPN wilt maken met ASA 5505 wordt de foutmelding `The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established`. (Het ontvangen servercertificaat of de certificatenketen voldoet niet aan FIPS. Er wordt geen VPN-verbinding tot stand gebracht.) getoond.

## Oplossing

U moet FIPS (Federal Information Processing Standards) uitschakelen in het bestand `AnyConnectLocalPolicy`. Dit bestand bevindt zich doorgaans in `c:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml`. Als dit bestand niet in dit pad voorkomt, moet u het bestand in een andere map plaatsen op een pad zoals `c:\Documents and Settings\All Users\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml`. Wanneer u het XML-bestand heeft gevonden, voert u daarin de volgende wijzigingen door:

Wijzig de waarde:

```
<FipsMode>true</FipsMode>
```

in:

```
<FipsMode>>false</FipsMode>
```

Start vervolgens de computer opnieuw op. Gebruikers moeten beheerdersrechten hebben om dit bestand te kunnen wijzigen.

## Fout: "Certificate Validation Failure"

Gebruikers kunnen AnyConnect niet starten en krijgen de foutmelding `certificate Validation Failure (Certificaatvalideringsfout)`.

### Oplossing

Certificaatverificatie met de AnyConnect-client werkt anders dan met de IPsec-client. Voor goede certificaatverificatie moet u het clientcertificaat importeren naar uw browser en het verbindingsprofiel wijzigen. U moet ook de volgende opdracht inschakelen op de ASA om het gebruik van SSL-clientcertificaten toe te staan op de buiteninterface:

```
ssl certificate-authentication interface outside port 443
```

## Fout: "VPN Agent Service has encountered a problem and needs to close. We are sorry for the inconvenience"

Wanneer AnyConnect-versie 2.4.0202 wordt geïnstalleerd op een computer met Windows XP, wordt er gestopt bij het bijwerken van lokalisatiebestanden en wordt de foutmelding getoond dat `vpnagent.exe` niet werkt.

### Oplossing

Dit gedrag is vastgelegd in Cisco bug-ID [CSCsq49102](#). De voorgestelde workround is bedoeld om de Citrix-client uit te schakelen.

## Fout: "This installation package could not be opened. Verify that the package exists"

Wanneer AnyConnect wordt gedownload, wordt de volgende foutmelding getoond:

```
"Contact your system administrator. The installer failed with the following error: This installation package could not be opened. Verify that the package exists and that you can access it, or contact the application vendor to verify that this is a valid Windows Installer package." (Neem contact op met de systeembeheerder. De installatie is mislukt met de volgende foutmelding: Kan dit installatiepakket niet openen. Controleer of het pakket bestaat en toegankelijk is, of neem contact op met de leverancier van de toepassing om te controleren of dit een geldig Windows Installer-pakket is.)
```

### Oplossing

Voer de volgende stappen uit om dit probleem op te lossen:

1. Verwijder eventuele antivirussoftware.
2. Schakel de Windows-firewall uit.
3. Als stap 1 noch stap 2 het probleem oplost, moet u de computer formatteren en vervolgens het pakket installeren.
4. Open een [TAC-case](#) als het probleem aanhoudt.

## Fout: "Error applying transforms. Verify that the specified transform paths are valid."

De volgende foutmelding wordt getoond tijdens het automatisch downloaden van AnyConnect van de ASA:

```
"Contact your system administrator. The installer failed with the following error:  
Error applying transforms. Verify that the specified transform paths are valid."
```

De volgende foutmelding wordt getoond wanneer verbinding wordt gemaakt met AnyConnect voor macOS:

```
"The AnyConnect package on the secure gateway could not be located. You may be  
experiencing network connectivity issues. Please try connecting again."
```

## Oplossing

Probeer een van de volgende tijdelijke oplossingen om dit probleem op te lossen:

1. De hoofdoorzaak van deze fout kan een (bijvoorbeeld geïmporteerde) beschadigde MST-vertaaltabel zijn. Voer de volgende stappen uit om dit probleem op te lossen:

Verwijder de MST-vertaaltabel.

Configureer de AnyConnect-image voor macOS op de ASA.

2. Selecteer in **ASDM Network (Client) Access > AnyConnect Custom > Installs (Netwerktoegang (client) > AnyConnect - aangepast > Installaties)** en verwijder het AnyConnect-pakketbestand. Zorg dat het bestand aanwezig blijft in **Network (Client) Access > Advanced > SSL VPN > Client Setting (Netwerktoegang (client) > Geavanceerd > SSL VPN > Clientinstelling)**.

Neem contact op met [Cisco Technical Support](#) als geen van deze tijdelijke oplossingen het probleem oplost.

## Fout: "The VPN client driver has encountered an error"

De volgende foutmelding wordt getoond:

```
The VPN client driver has encountered an error when connecting through Cisco  
AnyConnect Client.
```

## Oplossing

Dit probleem kan worden opgelost door de AnyConnect-client te verwijderen en vervolgens de antivirussoftware te verwijderen. Installeer daarna de AnyConnect-client opnieuw. Als deze oplossing niet werkt, moet u de computer opnieuw formatteren.

**Fout: "A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restored."**

De volgende foutmelding wordt getoond wanneer u AnyConnect start:

**"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."**

## Oplossing

Los deze fout als volgt op:

```
group-policy <Name> attributes
webvpn
svc mtu 1200
```

In ASA-versie 8.4(1) en hoger wordt de opdracht **svc mtu** vervangen door de opdracht **anyconnect mtu** zoals hieronder wordt getoond:

```
hostname(config)#group-policy
```

```
hostname(config-group-policy)#webvpn
```

```
hostname(config-group-webvpn)#anyconnect mtu 500
```

## Fout van AnyConnect bij het aanmelden

### Probleem

De volgende foutmelding wordt getoond wanneer AnyConnect verbinding maakt met de client:

The VPN connection is not allowed via a local proxy. This can be changed through AnyConnect profile settings.

## Oplossing

Het probleem kan worden opgelost door wijzigingen door te voeren in het AnyConnect-profiel.

Voeg de volgende regel toe aan het AnyConnect-profiel:

```
<ProxySettings>IgnoreProxy</ProxySettings><
AllowLocalProxyConnections>
false</AllowLocalProxyConnections>
```

## Fout: IE-proxy-instelling wordt niet hersteld nadat AnyConnect-verbinding is verbroken op Windows 7

### Probleem

Als in Windows 7 de instelling voor IE-proxy is ingesteld op **Instellingen automatisch detecteren** en AnyConnect een nieuwe proxy-instelling oplegt, wordt de instelling voor IE-proxy niet teruggezet

naar Instellingen automatisch detecteren nadat de gebruiker de AnyConnect-sessie heeft beëindigd. Dit leidt tot LAN-problemen bij gebruikers die de optie Instellingen automatisch detecteren nodig hebben.

## Oplossing

Dit gedrag is vastgelegd in Cisco bug-ID [CSCtj51376](#). De voorgestelde werkruimte is een upgrade naar [AnyConnect 3.0](#).

## Fout: AnyConnect Essentials can not be enabled until all these sessions are closed.

Deze foutmelding wordt getoond op Cisco ASDM wanneer u de AnyConnect Essentials-licentie wilt inschakelen:

```
There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.
```

## Oplossing

Dit is het normale gedrag van de ASA. AnyConnect Essentials is een afzonderlijk gelicentieerde SSL VPN-client. Deze wordt volledig op de ASA geconfigureerd en biedt alle AnyConnect-mogelijkheden met de volgende uitzonderingen:

- Geen Cisco Secure Desktop (CSD) (inclusief HostScan/Vault/Cache Cleaner)
- Geen clientloze SSL VPN
- Optionele Windows Mobile-ondersteuning

Deze licentie kan niet gelijktijdig met de gedeelde SSL VPN Premium-licentie worden gebruikt. Wanneer u een van deze licenties wilt gebruiken, moet u de andere uitschakelen.

## Fout: Tabblad Verbindingen bij optie Internet van Internet Explorer wordt verborgen nadat verbinding met AnyConnect-client tot stand is gebracht.

In Internet Explorer is het tabblad **Connections (Verbindingen)** bij **Internet Options (Internetopties)** verborgen nadat u verbinding heeft gemaakt met de AnyConnect-client.

## Oplossing

Dit probleem wordt veroorzaakt door de functie msie-proxy lockdown. Als u deze functie inschakelt, wordt het tabblad Verbindingen in Microsoft Internet Explorer gedurende de duur van de AnyConnect VPN-sessie verborgen. Als u deze functie uitschakelt, wordt het tabblad Verbindingen wel weergegeven.

## Fout: Enkele gebruikers krijgen melding Login Failed Error terwijl anderen wel verbinding kunnen maken via AnyConnect VPN

Enkele gebruikers krijgen de foutmelding Login Failed (Aanmelden mislukt) terwijl anderen wel



verbinding kunnen maken via AnyConnect VPN.

## Oplossing

Dit probleem kan worden opgelost door ervoor te zorgen dat het selectievakje **do not require pre-authentication (verificatie vooraf niet vereisen)** is ingeschakeld voor de gebruikers.

**Fout: The certificate you are viewing does not match with the name of the site you are trying to view.**

Tijdens het bijwerken van het AnyConnect-profiel wordt aangegeven dat het certificaat ongeldig is. Dit gebeurt alleen onder Windows en in de fase dat het profiel wordt bijgewerkt. De getoonde foutmelding is als volgt:

```
The certificate you are viewing does not match with the name of the site
you are trying to view.
```

## Oplossing

Pas de serverlijst van het AnyConnect-profiel aan om de FQDN van het certificaat te gebruiken.

Hieronder volgt een voorbeeld van het XML-profiel:

```
<ServerList>
<HostEntry>
<HostName>vpn1.ccsd.net</HostName>
</HostEntry>
</ServerList>
```

**Opmerking:** Als er een bestaande vermelding is voor het openbare IP-adres van de server, zoals `<HostAddress>`, verwijdert u deze en behoudt u alleen de FQDN van de server (bijvoorbeeld `<HostName>` maar niet `<Host Address>`).

## Kan AnyConnect niet starten vanuit de CSD-vault op een computer met Windows 7

Wanneer AnyConnect wordt gestart via de CSD-vault, werkt AnyConnect niet. Dit is van toepassing op computers met Windows 7.

## Oplossing

Momenteel is er geen oplossing omdat deze gebruikstoepassing niet wordt ondersteund.

## AnyConnect-profiel wordt niet gerepliceerd naar de standby na failover

De VPN-client van AnyConnect 3.0 met ASA-softwareversie 8.4.1 werkt prima. Na failover vindt er echter geen replicatie plaats van de aan het AnyConnect-profiel gerelateerde configuratie.

## Oplossing

Dit probleem is waargenomen en geregistreerd onder Cisco bug-ID [CSCtn71662](#). De tijdelijke bewerking is om de bestanden handmatig naar de stand-by unit te kopiëren.

## AnyConnect-client crasht wanneer Internet Explorer offline gaat

Wanneer dit probleem optreedt, bevat de gebeurtenislogboek van AnyConnect een vermelding vergelijkbaar met de volgende:

```
Description : Function:
CAdapterNetworkStateIfc::SetConnectedStateToConnected
File: .\AdapterNetworkStateIfc.cpp
Line: 147
Invoked Function: InternetSetOption
Return Code: 12010 (0x00002EEA)
Description: The length is incorrect for the option type
```

```
Description : Function: CTransportWinHttp::InitTransport
File: .\CTransportWinHttp.cpp
Line: 252
Invoked Function: CConnectedStateIfc::SetConnectedStateToConnected
Return Code: -25362420 (0xFE7D000C)
Description: CADAPTERNETWORKSTATEIFC_ERROR_SET_OPTION
```

## Oplossing

Dit gedrag wordt waargenomen en geregistreerd onder Cisco bug-ID [CSCtx28970](#). Stop de AnyConnect-toepassing en herstart om dit op te lossen. De verbindingvermeldingen worden daarna weer getoond.

## Fout: TLSPROTOCOL\_ERROR\_INSUFFICIENT\_BUFFER

De AnyConnect-client kan geen verbinding maken en de foutmelding **Unable to establish a connection (Kan geen verbinding maken)** wordt getoond. In het gebeurtenislogboek van AnyConnect wordt de fout **TLSPROTOCOL\_ERROR\_INSUFFICIENT\_BUFFER** vastgelegd.

## Oplossing

Dit probleem treedt op wanneer de head-end is geconfigureerd voor split-tunneling met een zeer grote split-tunnellijst (circa 180 tot 200 vermeldingen) en een of meer andere clientkenmerken zijn geconfigureerd in het groepsbeleid, zoals dns-server.

Voer de volgende stappen uit om dit probleem op te lossen:

1. Verminder het aantal vermeldingen in de split-tunnellijst.
2. Gebruik de volgende configuratie om DTLS uit te schakelen:

```
group-policy groupName attributes
webvpn
svc dtls none
```

Raadpleeg Cisco bug-ID [CSCtc41770](#) voor meer informatie.

## Fout: "Connection attempt has failed due to invalid host entry"

De foutmelding `Connection attempt has failed due to invalid host entry` (Verbindingspoging is mislukt als gevolg van ongeldige hostvermelding) wordt getoond terwijl AnyConnect wordt geverifieerd via een certificaat.

## Oplossing

Probeer een van de volgende oplossingen om dit probleem op te lossen:

- Voer een upgrade van AnyConnect uit naar versie 3.0.
- Schakel Cisco Secure Desktop uit op uw computer.

Raadpleeg Cisco bug-ID [CSCti73316](#) voor meer informatie.

## Fout: "Ensure your server certificates can pass strict mode if you configure always-on VPN"

Wanneer u de functie Always-On uitschakelt in AnyConnect, wordt de foutmelding `Ensure your server certificates can pass strict mode if you configure always-on VPN` (Zorg dat uw servercertificaten aan de strikte modus voldoen als u always-on VPN configureert) getoond.

## Oplossing

Deze foutmelding geeft aan dat een geldig, op de head-end geconfigureerd servercertificaat nodig is om de functie Always-On te kunnen gebruiken. Deze functie werkt niet zonder een geldig servercertificaat. U kunt de optie Strict Cert Mode instellen in het lokale AnyConnect-beleidsbestand om ervoor te zorgen dat de verbindingen een geldig certificaat gebruiken. Als u deze optie inschakelt in het beleidsbestand en verbinding maakt met een ongeldig certificaat, wordt er geen verbinding tot stand gebracht.

## Fout: "An internal error occurred in the Microsoft Windows HTTP Services"

De Diagnostic AnyConnect Reporting Tool (DART) toont één mislukte poging:

```
*****
```

```
Date : 03/25/2014  
Time : 09:52:21  
Type : Error  
Source : acvpnui
```

```
Description : Function: CTransportWinHttp::SendRequest  
File: .\CTransportWinHttp.cpp  
Line: 1170
```

```
Invoked Function: HttpSendRequest
```

```
Return Code: 12004 (0x00002EE4)
```

```
Description: An internal error occurred in the Microsoft  
Windows HTTP Services
```

```
*****
```

```
Date : 03/25/2014  
Time : 09:52:21  
Type : Error
```

Source : acvpnui

Description : Function: ConnectIfc::connect

File: .\ConnectIfc.cpp

Line: 472

Invoked Function: ConnectIfc::sendRequest

Return Code: -30015443 (0xFE36002D)

Description: CTRANSPORT\_ERROR\_CONN\_UNKNOWN

\*\*\*\*\*

Date : 03/25/2014

Time : 09:52:21

Type : Error

Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode

File: .\ConnectIfc.cpp

Line: 2999

Invoked Function: ConnectIfc::TranslateStatusCode

Return Code: -30015443 (0xFE36002D)

Description: CTRANSPORT\_ERROR\_CONN\_UNKNOWN

**Connection attempt failed. Please try again.**

\*\*\*\*\*

Raadpleeg tevens de logboeken op de Windows-computer.

## Oplossing

Dit probleem kan worden veroorzaakt door een beschadigde Winsock-verbinding. Stel de verbinding via de opdrachtprompt met de volgende opdracht opnieuw in en start de Windows-computer opnieuw op:

### netsh winsock reset

Raadpleeg het Knowledge Base-artikel [Vaststellen en herstellen van Winsock2-beschadiging in Windows Server 2003, Windows XP en Windows Vista voor meer informatie.](#)

**Fout: "Het SSL-transport heeft een beveiligde kanaalstoring ontvangen. May be a result of a unsupported crypto configuration on the Secure Gateway."**

De Diagnostic AnyConnect Reporting Tool (DART) toont één mislukte poging:

\*\*\*\*\*

Date : 10/27/2014

Time : 16:29:09

Type : Error

Source : acvpnui

Description : Function: CTransportWinHttp::handleRequestError

File: .\CTransportWinHttp.cpp

Line: 854

The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway.

\*\*\*\*\*

Date : 10/27/2014

Time : 16:29:09

Type : Error

Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest  
File: .\CTransportWinHttp.cpp  
Line: 1199  
Invoked Function: CTransportWinHttp::handleRequestError  
Return Code: -30015418 (0xFE360046)  
Description: CTRANSPORT\_ERROR\_SECURE\_CHANNEL\_FAILURE

\*\*\*\*\*  
Date : 10/27/2014  
Time : 16:29:09  
Type : Error  
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode  
File: .\ConnectIfc.cpp  
Line: 3026  
Invoked Function: ConnectIfc::TranslateStatusCode  
Return Code: -30015418 (0xFE360046)  
Description: CTRANSPORT\_ERROR\_SECURE\_CHANNEL\_FAILURE  
Connection attempt failed. Please try again.  
\*\*\*\*\*

## Oplossing

Volgens de volgende KB-update ondersteunt Windows 8.1 RC4 niet:

<http://support2.microsoft.com/kb/2868725>

Configureer DES/3DES-encryptie voor SSL VPN op de ASA met de opdracht "ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1" OF bewerk het Windows-register op de clientcomputer zoals hieronder aangegeven:

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

## Gerelateerde informatie

- [Adaptieve security applicaties van Cisco ASA 5500 Series](#)
- [Veelgestelde vragen over AnyConnect VPN-client](#)
- [Veelgestelde vragen over Cisco Secure Desktop \(CSD\)](#)
- [Cisco AnyConnect VPN-client](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)