

# Probleemoplossing voor beveiligde toegangsfout "de VPN-verbinding is gestart door een externe desktopgebruiker van wie de externe console is losgekoppeld"

## Inhoud

---

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

---

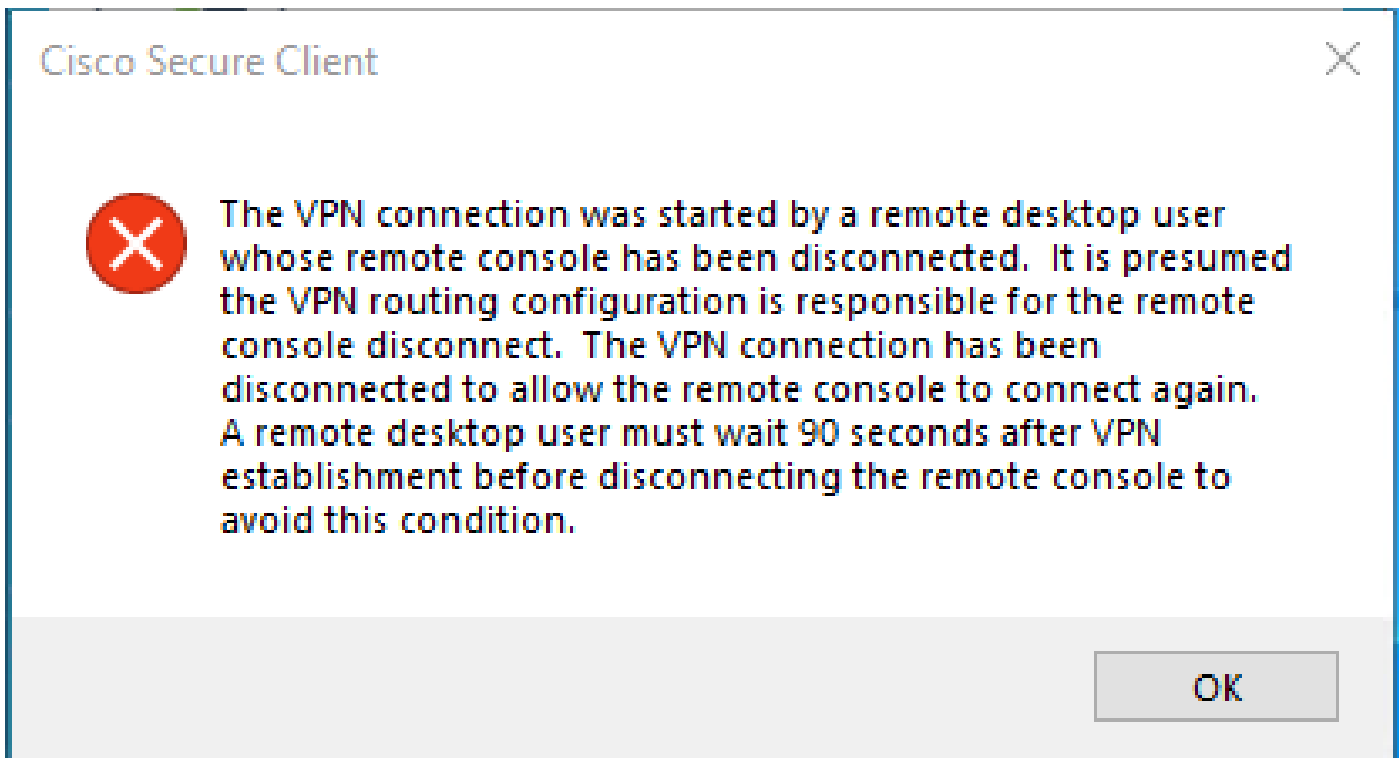
## Inleiding

Dit document beschrijft hoe de fout moet worden opgelost: "De VPN-verbinding is gestart door een externe desktopgebruiker wiens externe console is losgekoppeld".

## Probleem

Wanneer een gebruiker probeert verbinding te maken met RA-VPN (Remote Access VPN) met de Secure Access-head-end, wordt de fout afgedrukt in het venster voor beveiligde clientmelding van Cisco:

- The VPN connection was started by a remote desktop user whose remote console has been disconnected. It is presumed the VPN routing configuration is responsible for the remote console disconnect. The VPN connection has been disconnected to allow the remote console to connect again. A remote desktop user must wait 90 seconds after VPN establishment before disconnecting the remote console to avoid this condition.



De genoemde fout wordt gegenereerd wanneer de gebruiker via de RDP is verbonden met de Windows-pc, probeert verbinding te maken met RA-VPN vanaf de gegeven pc, en Tunnel Mode in VPN Profile is ingesteld op **Connect to Secure Access (default option)** en source IP van de RDP-verbinding is niet toegevoegd aan Exceptions.

U **Traffic Steering (Split Tunnel)** kunt bijvoorbeeld een VPN-profiel configureren om een volledige tunnelverbinding te onderhouden voor beveiligde toegang of het profiel configureren om een gesplitste tunnelverbinding te gebruiken om alleen verkeer door VPN te leiden als dat nodig is.

- Kies voor **Tunnel Mode**:
  - **Connect to Secure Access** om al het verkeer door de tunnel te leiden, of
  - **Bypass Secure Access** om al het verkeer buiten de tunnel te leiden.
- Afhankelijk van uw selectie, kunt u verkeer binnen of buiten de tunnel **Add Exceptions** te sturen. U kunt door komma's gescheiden IP's, domeinen en netwerkruidtes invoeren.

## Oplossing

Navigeren naar het Cisco Secure Access Dashboard:

- Klik op **Connect > End User Connectivity**

- Klik op Virtual Private Network
- Kies het profiel dat u wilt wijzigen en klik op **Edit**

**VPN Profiles**  
A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

Search

[+ Add](#)

name	General	Authentication	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
niVPNprofile	sspt: pft.com TLS, IKEv2	SAML	Connect to Secure Access 2 Exception(s)	13 Settings	6f1 iVPNprofile	<a href="#">Download XML</a>

[Edit](#)  
[Duplicate](#)  
[Delete](#)

- Klik op **Traffic Steering (Split Tunnel) > Add Exceptions > + Add**

**General settings**  
Default Domain: sspt: pft.com | DNS Server: UmbrellaDNS2 (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS, IKEv2

**Authentication**  
SAML

**3 Traffic Steering (Split Tunnel)**  
Connect to Secure Access | 2 Exceptions

**Cisco Secure Client Configuration**

**Traffic Steering (Split Tunnel)**  
Configure how VPN traffic traverses your network. [Help](#)

**Tunnel Mode**  
Connect to Secure Access

All traffic is steered through the tunnel.

VPN Tunnel Secure Access

**Add Exceptions**  
Destinations specified here will be steered OUTSIDE the tunnel. [+ Add](#)

Destinations	Exclude Destinations	Actions
proxy-8 zpc.sse.cisco.com, ztna.sse.cisco.com, acme.sse.cisco.com, devices.api.umbrella.com, sseposture-routing-commercial.k8s.5c10.org, sseposture-routing-commercial.posture.duosec	-	-

[Cancel](#) [Back](#) [Next](#)

- Voeg uw IP-adres toe van waaruit u de RDP-verbinding hebt gemaakt

# Add Destinations

Comma seperated IPs, domains, and network spaces

Cancel

Save

- Klik op **Save** in **Add Destinations** het venster

TCP	127.0.0.1:62722	0.0.0.0:0	LISTENING
TCP	127.0.0.1:62722	127.0.0.1:49794	ESTABLISHED
TCP	172.30.1.7:139	0.0.0.0:0	LISTENING
TCP	172.30.1.7:3389	185.15[REDACTED]:12974	ESTABLISHED
TCP	172.30.1.7:49687	52.16.166.193:443	ESTABLISHED
TCP	172.30.1.7:49745	20.42.72.131:443	TIME_WAIT
TCP	172.30.1.7:49755	40.113.110.67:443	ESTABLISHED
TCP	172.30.1.7:49757	23.212.221.139:80	ESTABLISHED
TCP	172.30.1.7:49758	23.48.15.164:443	ESTABLISHED



**Opmerking:** het IP-adres kan worden gevonden via de uitvoer van cmd **netstat -an.**; Let op het IP-adres van waaruit een verbinding met het lokale IP-adres van de externe desktop naar poort 3389 tot stand is gebracht.

- 
- Klik **Next** na het toevoegen van de uitzondering:

- General settings  
Default Domain: ssp[redacted]oft.com | DNS Server: UmbrellaDNS2 (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS, IKEv2
- Authentication  
SAML
- 3** Traffic Steering (Split Tunnel)  
Connect to Secure Access | 2 Exceptions
- Cisco Secure Client Configuration

### Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network. [Help](#)

**Tunnel Mode**

Connect to Secure Access

All traffic is steered through the tunnel.

**Add Exceptions** + Add

Destinations specified here will be steered OUTSIDE the tunnel.

Destinations	Exclude Destinations	Actions
185.15[redacted]/32	+ Add	...
proxy-8179183.zpc.sse.cisco.com, ztna.sse.cisco.com, acme.sse.cisco.com, devices.api.umbrella.com, sseposture-routing-commercial.k8s.5c10.org, sse		

Cancel Back Next

- Klik op **Save** wijzigingen in het VPN-profiel:

- General settings  
Default Domain: ssp[redacted]oft.com | DNS Server: UmbrellaDNS2 (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS, IKEv2
- Authentication  
SAML
- Traffic Steering (Split Tunnel)  
Connect to Secure Access | 2 Exceptions
- 4** Cisco Secure Client Configuration

### Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **4** [Download XML](#)

**Banner Message**  
Require user to accept a banner message post authentication

**Session Timeout**  
 days

**Session Timeout Alert**  
 minutes before

**Maximum Transmission Unit** ⓘ

Cancel Back Save

- 

[VPN-profielen toevoegen](#)

- [Gebruikershandleiding voor beveiligde toegang](#)
- [Cisco Technical Support en downloads](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.