

# Solução de problemas de erro de acesso seguro "A conexão VPN foi iniciada por um usuário de área de trabalho remota cujo console remoto foi desconectado"

## Contents

---

[Introdução](#)

[Problema](#)

[Solução](#)

[Informações Relacionadas](#)

---

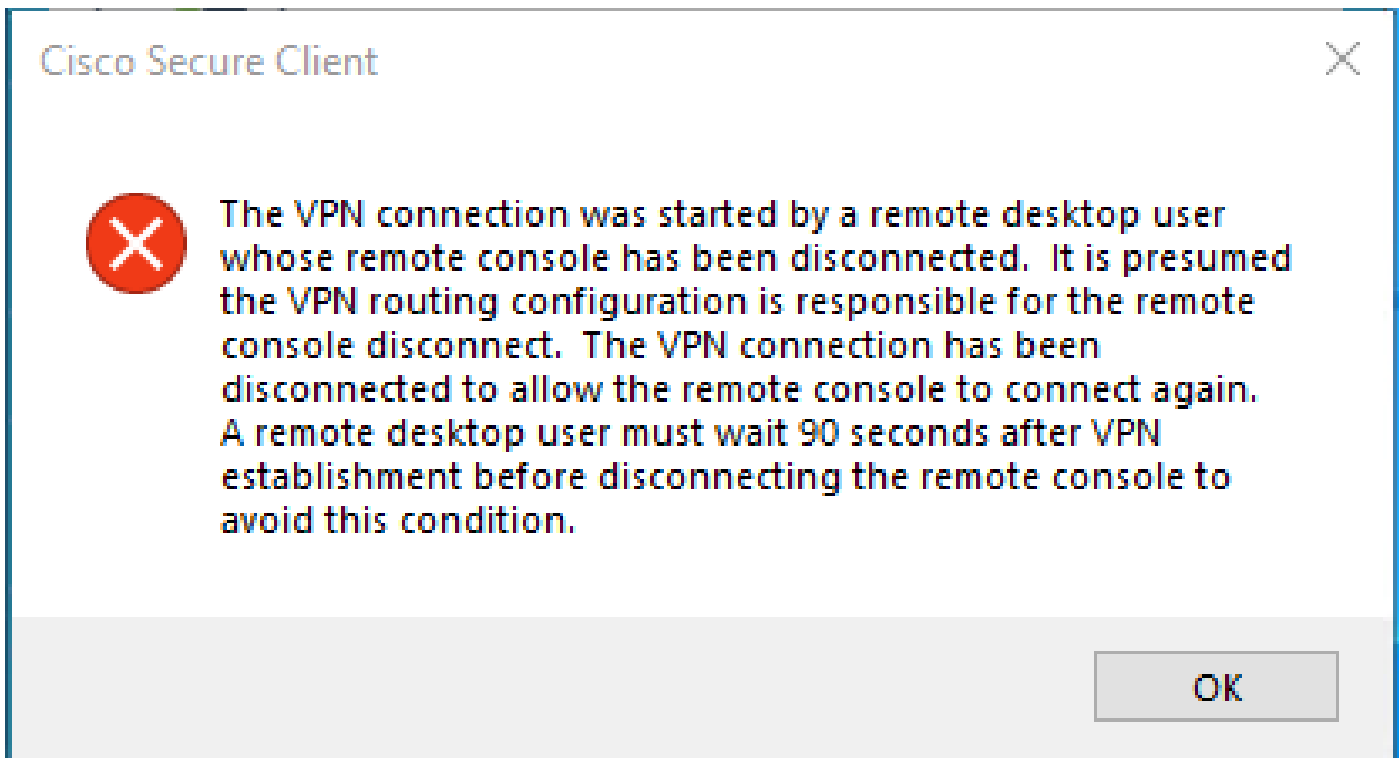
## Introdução

Este documento descreve como corrigir o erro: "A conexão VPN foi iniciada por um usuário de desktop remoto cujo console remoto foi desconectado".

## Problema

Quando um usuário tenta se conectar com RA-VPN (Remote Access VPN) ao headend do Secure Access, o erro é impresso no pop-up de notificação do Cisco Secure Client:

- 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.



O erro mencionado é gerado quando o usuário está conectado via RDP ao PC com Windows, tenta se conectar ao RA-VPN do PC especificado e, Tunnel Mode em Perfil VPN, é definido como **Connect to Secure Access (default option)** e o IP de origem da conexão RDP não é adicionado a Exceções.

Por **Traffic Steering (Split Tunnel)** exemplo, você pode configurar um perfil de VPN para manter uma conexão de túnel completa com o Secure Access ou configurar o perfil para usar uma conexão de túnel dividido para direcionar o tráfego através da VPN somente se necessário.

- Por **Tunnel Mode**, escolha:
  - **Connect to Secure Access** dirigir todo o tráfego através do túnel, ou
  - **Bypass Secure Access** direcionar todo o tráfego para fora do túnel.
- Dependendo da sua seleção, você pode **Add Exceptions** direcionar o tráfego dentro ou fora do túnel. Você pode digitar IPs, domínios e espaços de rede separados por vírgulas.

## Solução

Navegue até o Painel do Cisco Secure Access:

- Clique em **Connect > End User Connectivity**
- Clique em Virtual Private Network

- Escolha o perfil que deseja modificar e clique em **Edit**

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

Q Search + Add

name	General	Authentication	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
██████████iVPNprofile	sspt:██████████ft.com TLS, IKEv2	SAML	Connect to Secure Access 2 Exception(s)	13 Settings	6f1-██████████iVPNprofile	

**Edit**  
Duplicate  
Delete

- Clique em **Traffic Steering (Split Tunnel) > Add Exceptions > + Add**

**General settings**  
Default Domain: sspt:██████████ft.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**  
Destinations specified here will be steered OUTSIDE the tunnel.

**+ Add**

Destinations	Exclude Destinations	Actions
proxy-8██████████3.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.duosecure	-	-

Cancel Back Next

- Adicione seu endereço IP a partir do qual você estabeleceu a conexão RDP

# Add Destinations

Comma separated IPs, domains, and network spaces

Cancel

Save

- Clique **Save** na **Add Destinations** janela

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



**Observação:** o endereço IP pode ser encontrado na saída do comando `cmd netstat -an.`; Observe o endereço IP do qual existe uma conexão estabelecida com o endereço IP local do desktop remoto para a porta 3389.

- 
- Clique em **Next** depois de adicionar a exceção:

- ✓ 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

- Clique em **Save** changes no perfil VPN:

- ✓ 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

- 

[Adicionar perfis de VPN](#)

- [Guia do usuário do Secure Access](#)
- [Suporte técnico e downloads da Cisco](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.