

安全访问错误故障排除"；VPN连接由远程控制台已断开连接的远程桌面用户启动"；

目录

[简介](#)

[问题](#)

[解决方案](#)

[相关信息](#)

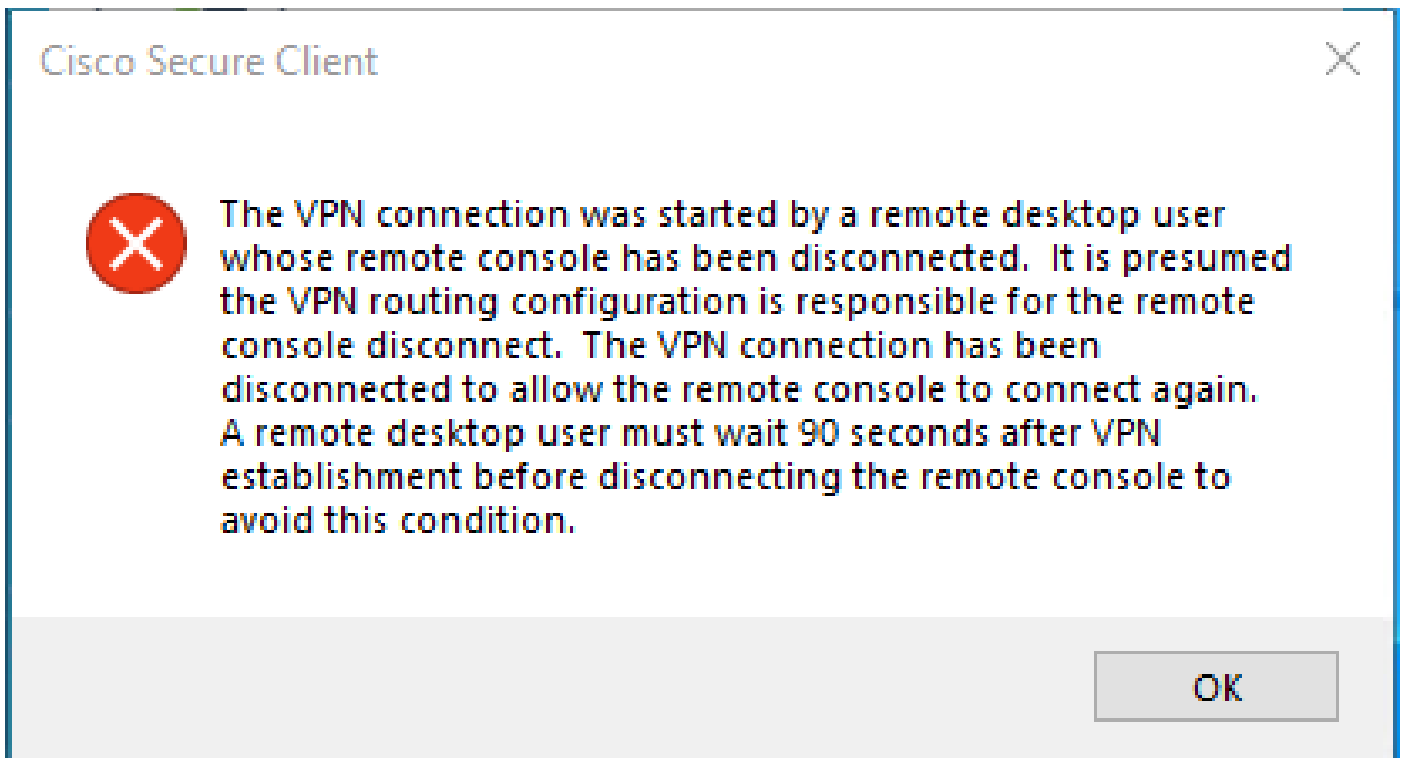
简介

本文档介绍如何修复以下错误：“VPN连接由远程控制台已断开连接的远程桌面用户启动”。

问题

当用户尝试使用RA-VPN（远程接入VPN）连接到安全接入头端时，错误会显示在Cisco Secure Client通知弹出窗口中：

- 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.



当用户通过RDP连接到Windows PC，尝试从给定PC连接到RA-VPN，并且VPN配置文件中的Tunnel Mode设置为 **Connect to Secure Access (default option)** 并且RDP连接的源IP未添加到“例外”时，生成上述错误。

对于 **Traffic Steering (Split Tunnel)**，您可以将VPN配置文件配置为维护与安全访问的全隧道连接，或者仅在必要时将配置文件配置为使用分割隧道连接以通过VPN定向流量。

- 对于**Tunnel Mode**，请依次选择：
 - **Connect to Secure Access** 通过隧道定向所有流量；或者，
 - **Bypass Secure Access** 将所有流量定向到隧道外部。
- 根据您的选择，您可以**Add Exceptions** 控制隧道内部或外部的流量。可以输入逗号分隔的IP、域和网络空间。

解决方案

导航到Cisco Secure Access Dashboard：

- 点击 **Connect > End User Connectivity**
- 点击 **Virtual Private Network**

- 选择要修改的配置文件并点击 **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 | Download XML |

...
Edit
Duplicate
Delete

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

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-81...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.duosecuri | - | - |

Cancel Back Next

- 添加用于建立RDP连接的IP地址

Add Destinations

Comma separated IPs, domains, and network spaces

Cancel

Save

- 点击Save In窗 Add Destinations 口

```
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
```



注：可以从cmd命令 `netstat -an`的输出中找到IP地址。请注意IP地址，其中已建立到远程桌面的本地IP地址到端口3389的连接。

-
- 添加例外后，点击 **Next** ：

- 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
- 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

- 在VPN配置文件中点击 **Save** 更改：

- 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
- 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

相关信息

-

[添加VPN配置文件](#)

- [安全访问用户指南](#)

- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。