

보안 액세스 오류 트러블슈팅(&Quot);원격 콘솔의 연결이 끊어진 원격 데스크톱 사용자가 VPN 연결을 시작했습니다(&Quot;).

목차

[소개](#)

[문제](#)

[솔루션](#)

[관련 정보](#)

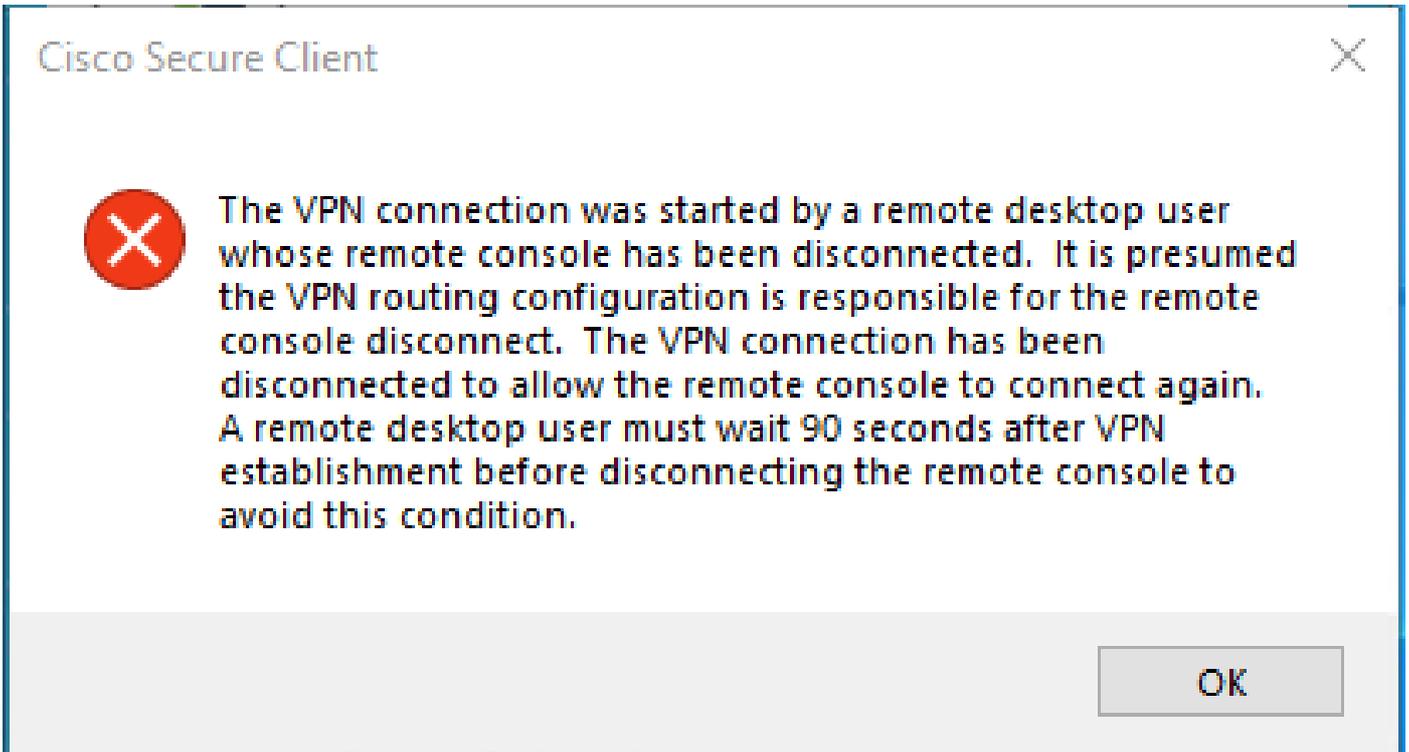
소개

이 문서에서는 오류를 수정하는 방법에 대해 설명합니다. "원격 콘솔의 연결이 끊어진 원격 데스크톱 사용자가 VPN 연결을 시작했습니다."

문제

사용자가 RA-VPN(Remote Access VPN)을 사용하여 Secure Access 헤드엔드에 연결하려고 하면 Cisco Secure Client 알림 팝업에 오류가 출력됩니다.

- 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.



언급된 오류는 사용자가 RDP를 통해 Windows PC에 연결되고 지정된 PC에서 RA-VPN에 연결하려고 할 때 Tunnel Mode VPN 프로파일로 설정되어 **Connect to Secure Access (default option)** 있고 RDP 연결의 소스 IP가 예외에 추가되지 않을 때 발생합니다.

예를 **Traffic Steering (Split Tunnel)** 들어, Secure Access에 대한 전체 터널 연결을 유지 관리하도록 VPN 프로파일을 구성하거나, 필요한 경우에만 분할 터널 연결을 사용하여 VPN을 통해 트래픽을 전달하도록 프로파일을 구성할 수 있습니다.

- 의 경우 **Tunnel Mode** 다음 중 하나를 선택합니다.
 - **Connect to Secure Access** 모든 트래픽을 터널을 통해 전달하거나
 - **Bypass Secure Access** 모든 트래픽을 터널 외부로 전달합니다.
- 선택에 따라 터널 내부 또는 외부 **Add Exceptions** 로 트래픽을 조종할 수 있습니다. 심표로 구분된 IP, 도메인 및 네트워크 공간을 입력할 수 있습니다.

솔루션

Cisco Secure Access Dashboard(Cisco Secure Access 대시보드)로 이동합니다.

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

- 수정할 프로필을 선택하고 **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
hVPNprofile	sspt: [redacted] pft.com TLS, IKEv2	SAML	Connect to Secure Access 2 Exception(s)	13 Settings	6f1 [redacted] iVPNprofile	

Edit
 Duplicate
 Delete

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

General settings
Default Domain: sspt: [redacted] 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.

Add Exceptions
Destinations specified here will be steered OUTSIDE the tunnel. + Add

Destinations	Exclude Destinations	Actions
proxy-8 [redacted] 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

- RDP 연결을 설정한 IP 주소를 추가합니다

Add Destinations

Comma seperated IPs, domains, and network spaces

Cancel

Save

- In 창Save 을 Add Destinations 클릭합니다

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



참고: cmd 명령의 출력에서 IP 주소를 찾을 수 있습니다. `netstat -an`; 포트 3389에 대한 원격 데스크톱의 로컬 IP 주소에 설정된 연결이 있는 IP 주소를 확인하십시오.

-
- 예외를 `Next` 추가한 후 클릭합니다.

- ✓ 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

- VPN Save 프로필에서 변경 사항을 클릭합니다.

- ✓ 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 프로파일 추가](#)

- [보안 액세스 사용 설명서](#)

- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.