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

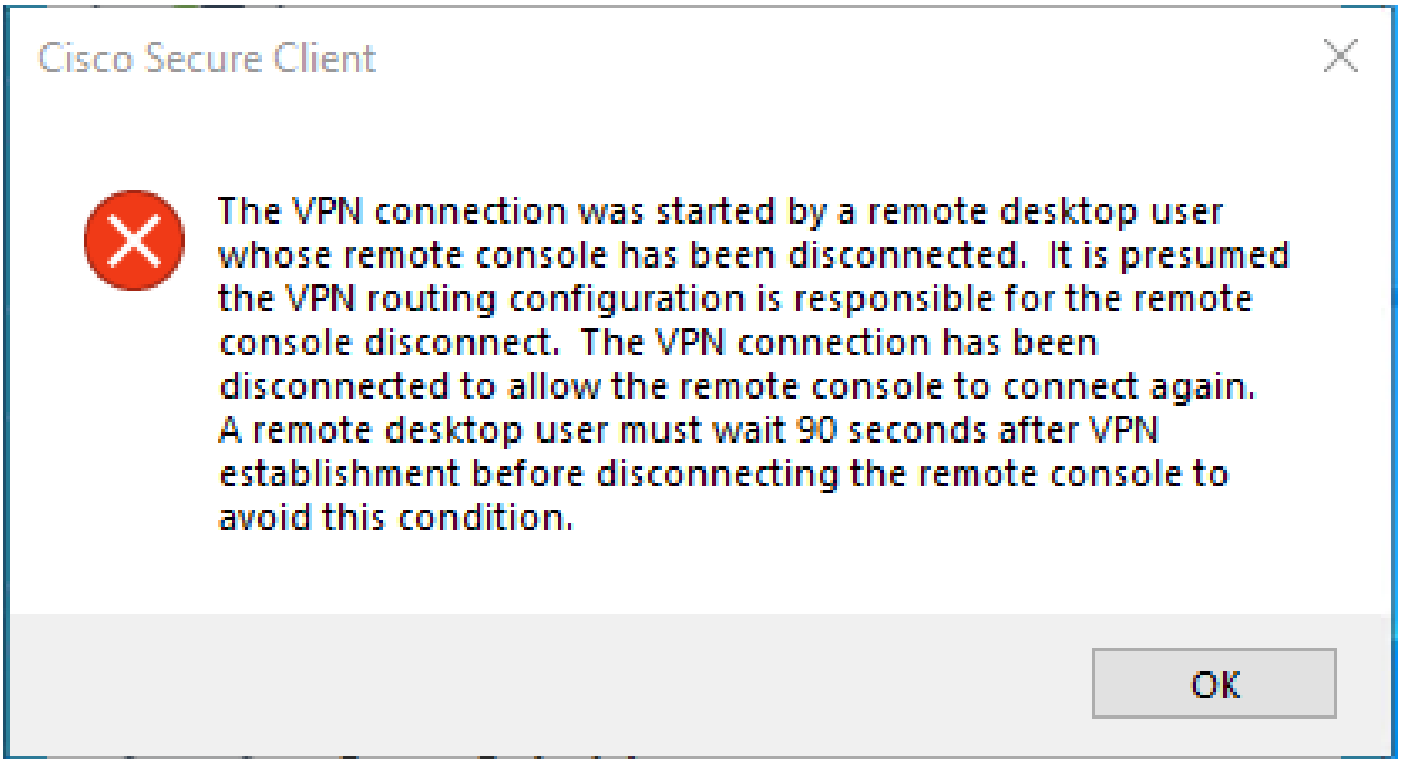
Inleiding

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.

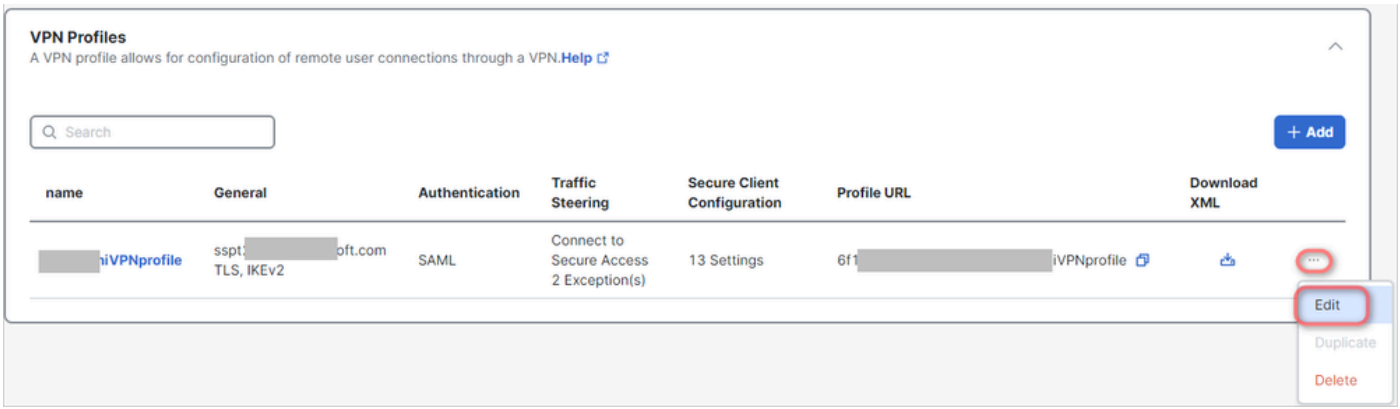
- Kies voor **Tunnel Mode**:
  - **Connect to Secure Access** om al het verkeer door de tunnel te leiden, of
    - **Bypass Secure Access** om al het verkeer buiten de tunnel te leiden.
- Afhankelijk van uw selectie, kunt u verkeer binnen of buiten de tunnel **Add Exceptions** te sturen. U kunt door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

Oplossing

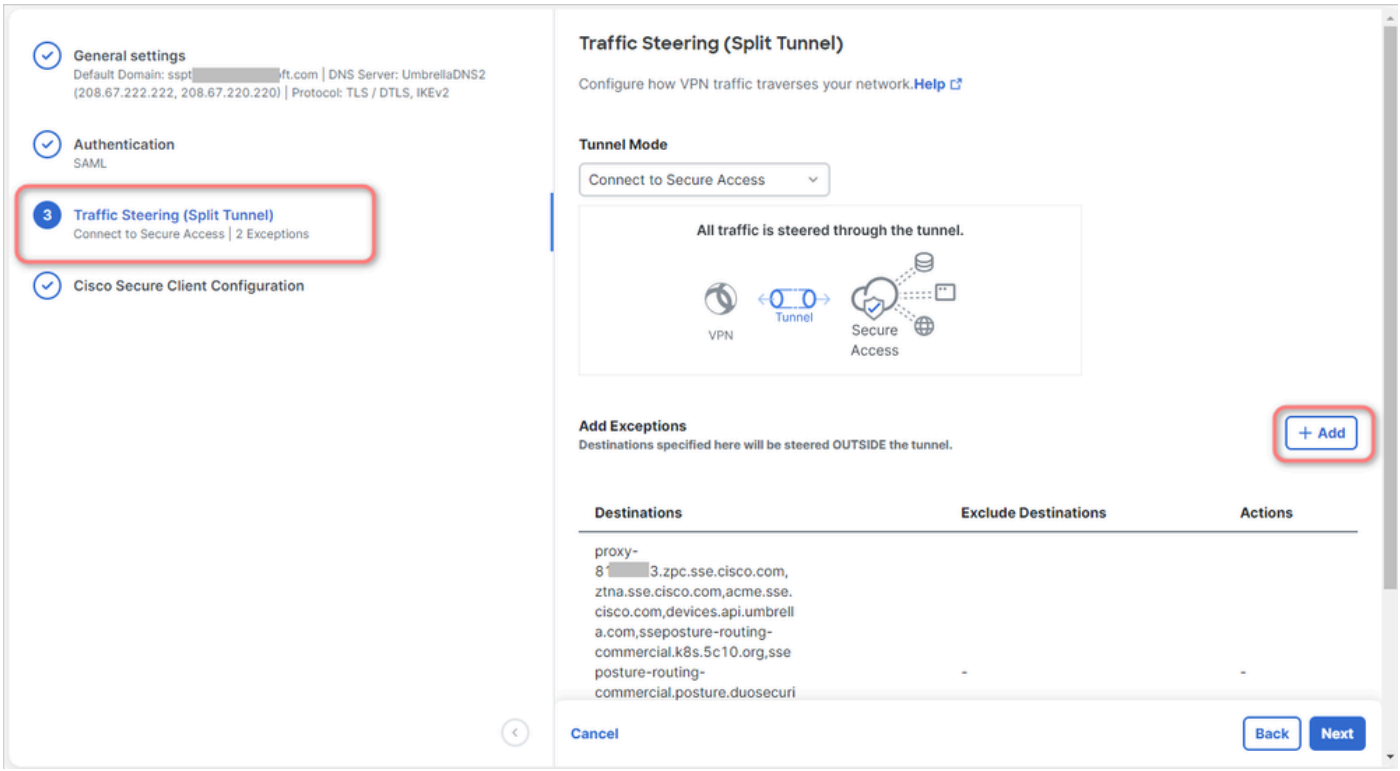
Navigeren naar het Cisco Secure Access Dashboard:

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

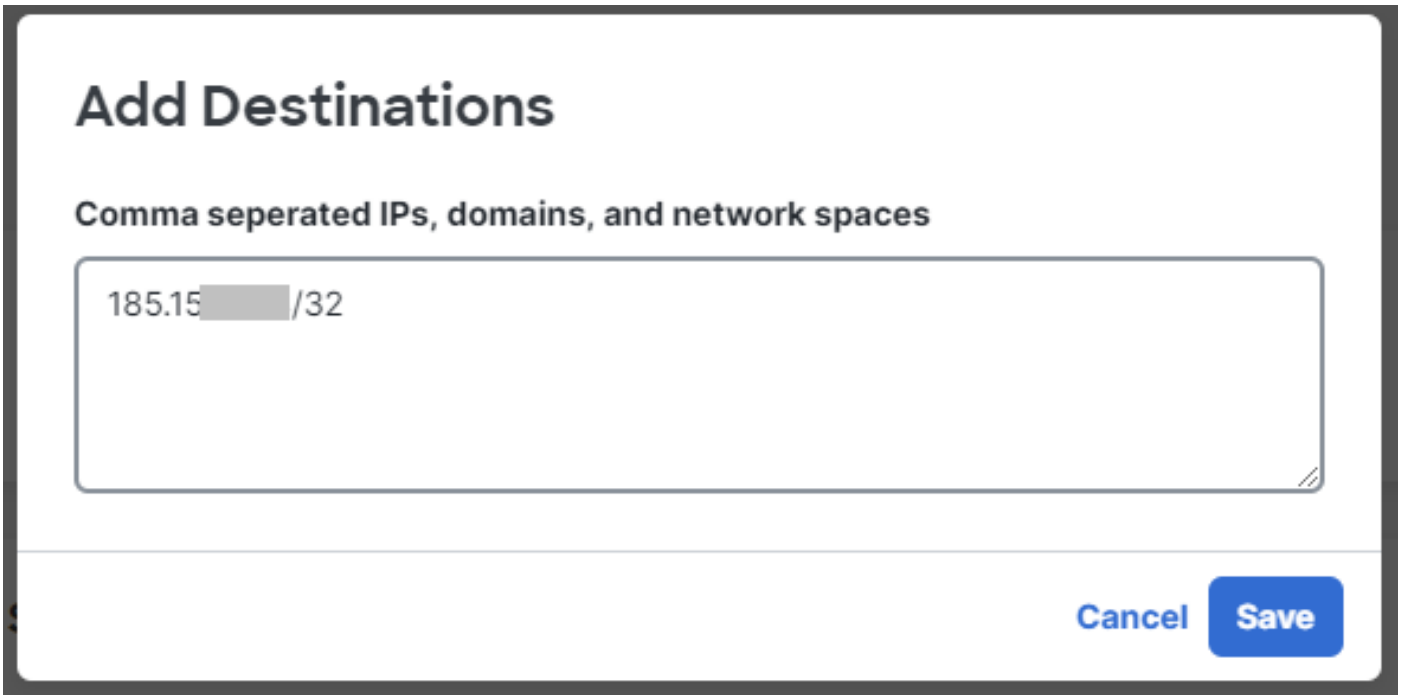
- Klik op Virtual Private Network
- Kies het profiel dat u wilt wijzigen en klik op **Edit**



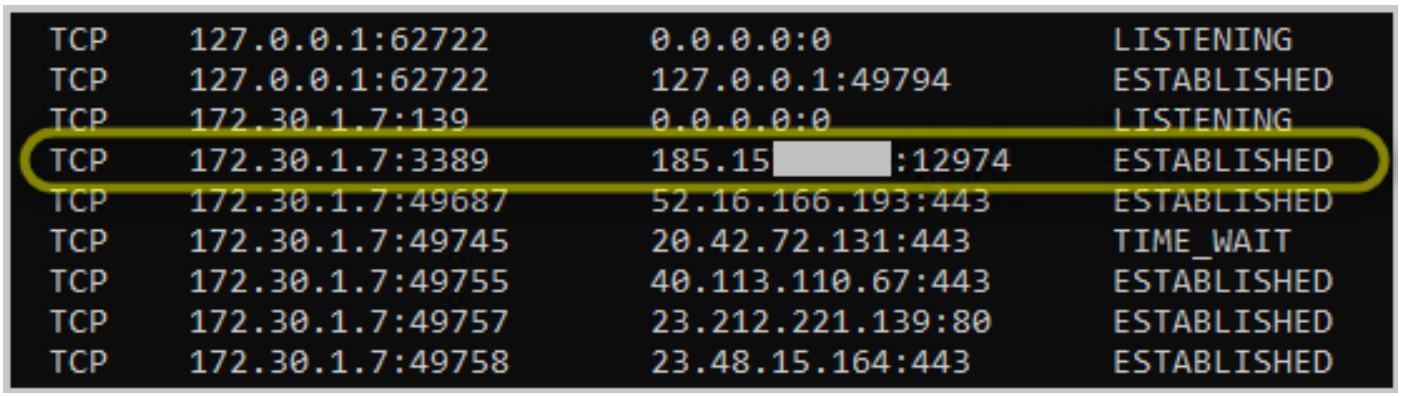
- Klik op **Traffic Steering (Split Tunnel) > Add Exceptions > + Add**

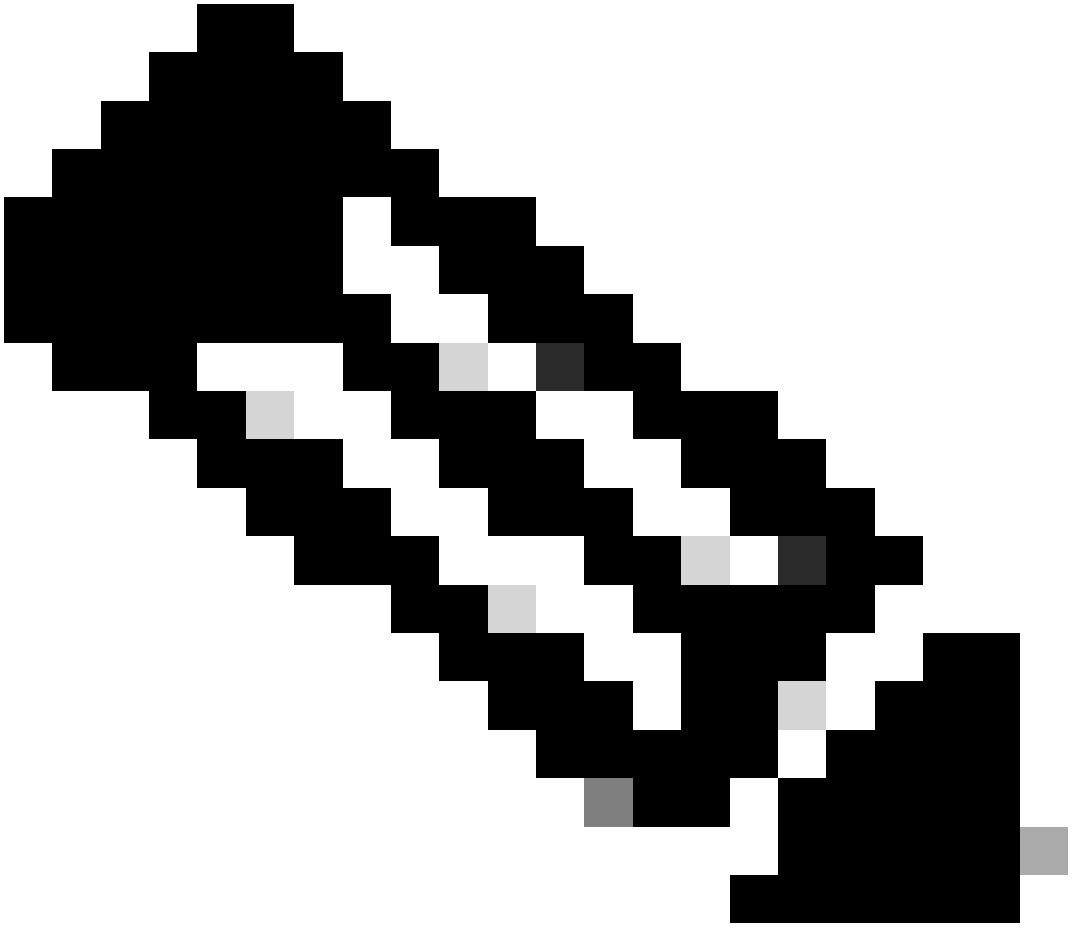


- Voeg uw IP-adres toe van waaruit u de RDP-verbinding hebt gemaakt



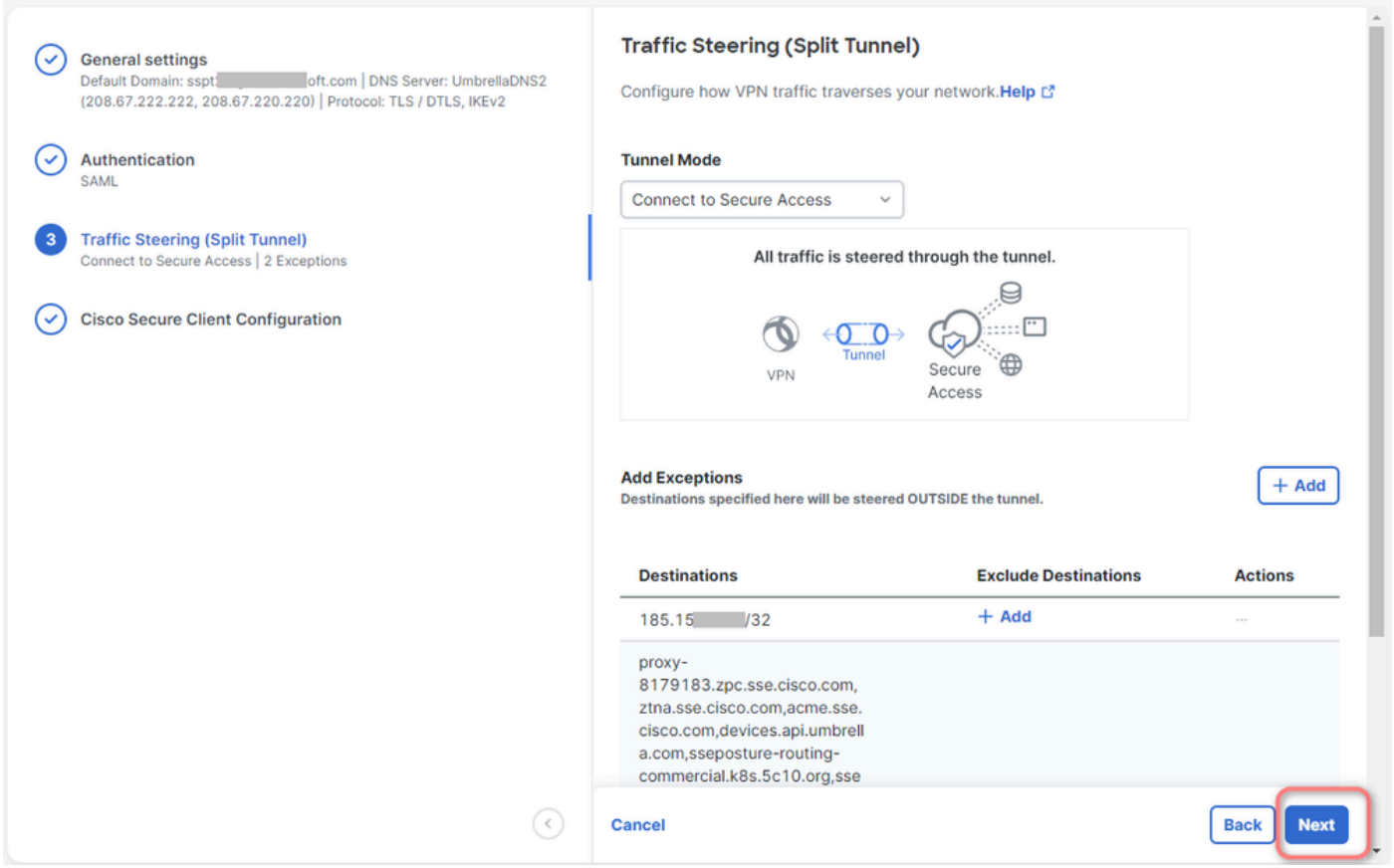
- Klik op **Save** in **Add Destinations** het venster



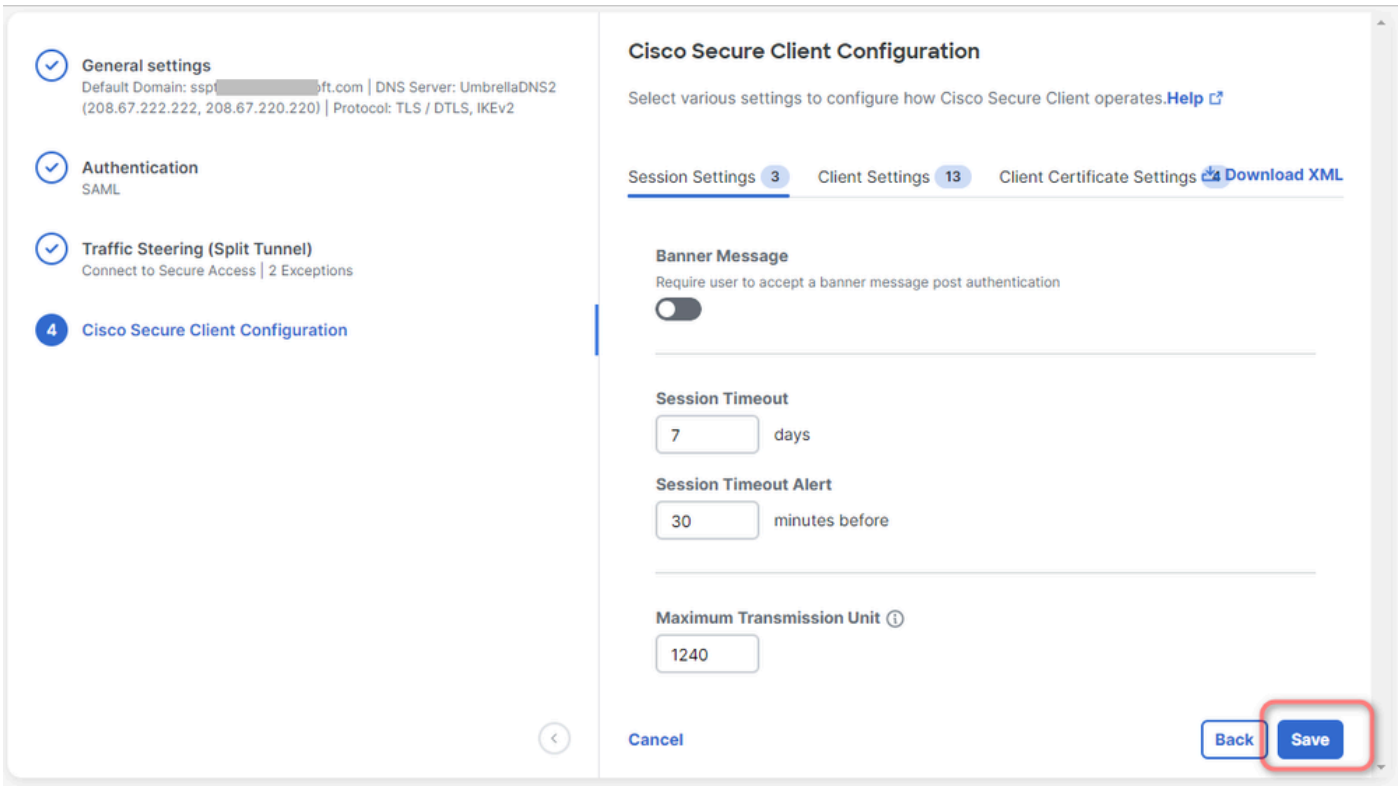


Opmerking: het IP-adres kan worden gevonden via de uitvoer van cmd **netstat -an**.; Let op het IP-adres van waaruit een verbinding met het lokale IP-adres van de externe desktop naar poort 3389 tot stand is gebracht.

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



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



Gerelateerde informatie

-

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.