Risoluzione dei problemi relativi a errore accesso sicuro "La connessione VPN è stata avviata da un utente di Desktop remoto la cui console remota è stata disconnessa"

Sommario

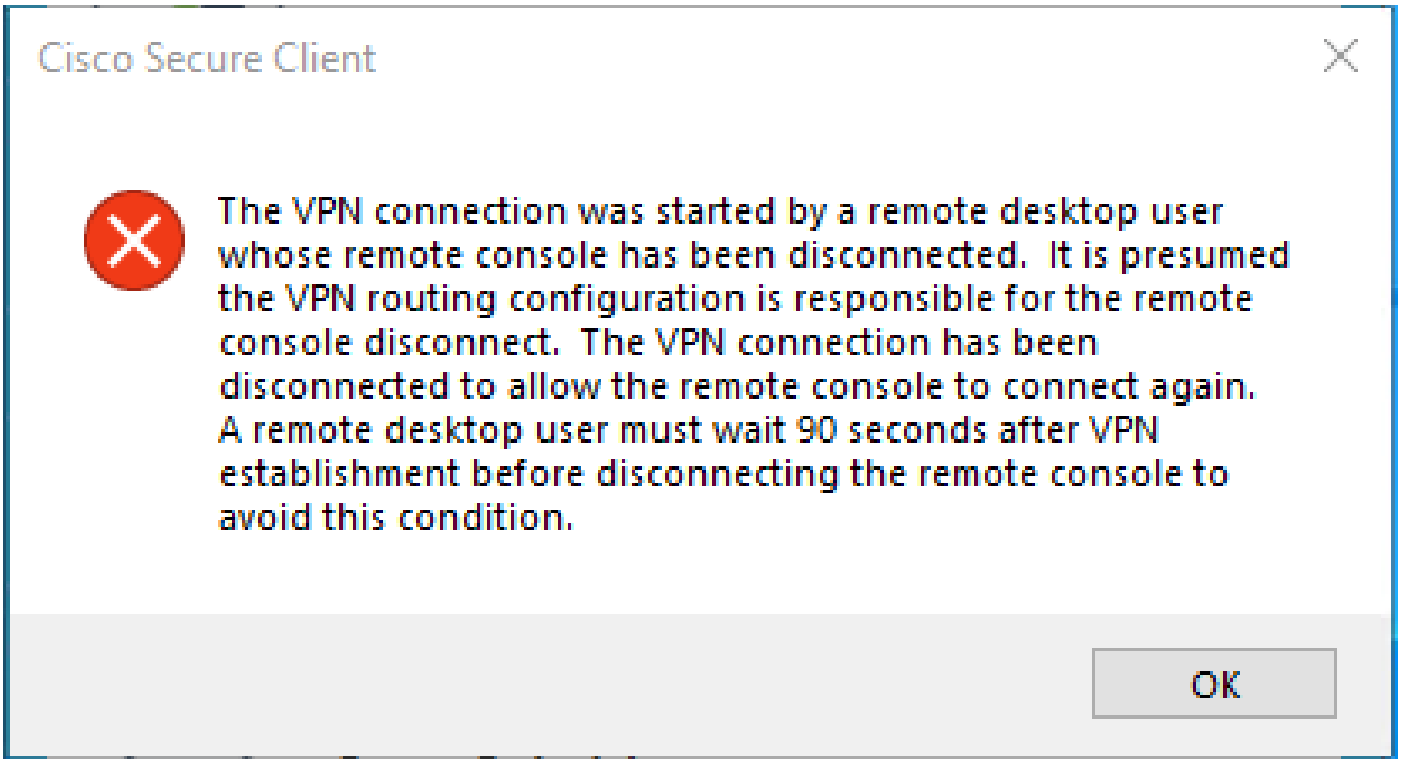
Introduzione

In questo documento viene descritto come correggere l'errore: "La connessione VPN è stata avviata da un utente desktop remoto la cui console remota è stata disconnessa".

Problema

Quando un utente tenta di connettersi all'headend di Secure Access tramite una VPN ad accesso remoto (RA-VPN), l'errore viene stampato nel popup di notifica di 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.



L'errore indicato viene generato quando l'utente è connesso tramite RDP al PC Windows, tenta di connettersi a RA-VPN dal PC specificato e Tunnel Mode in Profilo VPN è impostato su **Connect to Secure Access (default option)** e l'indirizzo IP di origine della connessione RDP non viene aggiunto a Eccezioni.

Ad esempio, **Traffic Steering (Split Tunnel)**è possibile configurare un profilo VPN per mantenere una connessione tunnel completa ad Accesso sicuro oppure configurare il profilo in modo che utilizzi una connessione tunnel divisa per indirizzare il traffico attraverso la VPN solo se necessario.

- Per **Tunnel Mode**, scegliere:
  - **Connect to Secure Access** dirigere tutto il traffico attraverso la galleria; oppure
    - **Bypass Secure Access** per indirizzare tutto il traffico all'esterno del tunnel.

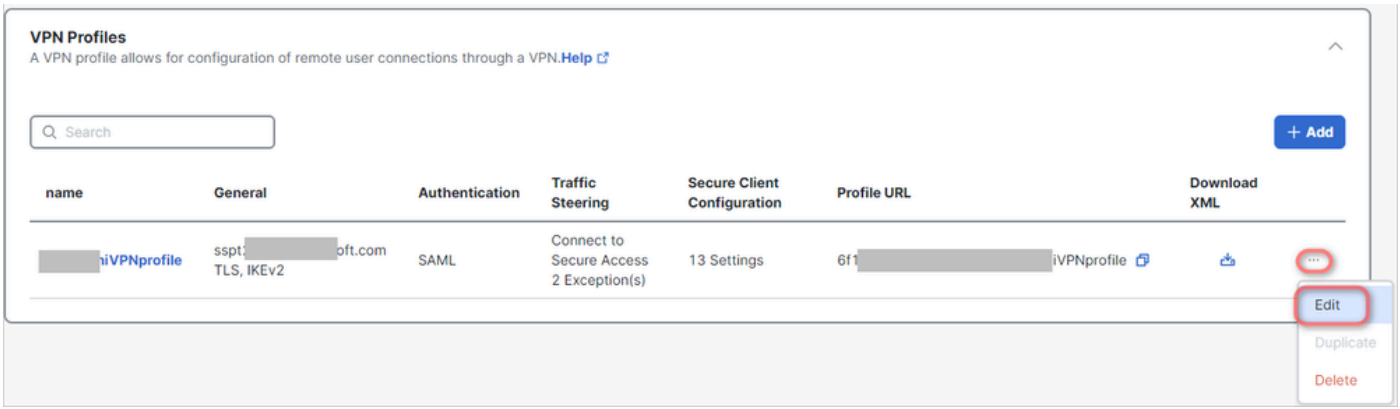
- A seconda della selezione effettuata, è possibile indirizzare **Add Exceptions** il traffico all'interno o all'esterno del tunnel. È possibile immettere indirizzi IP, domini e spazi di rete separati da virgole.

Soluzione

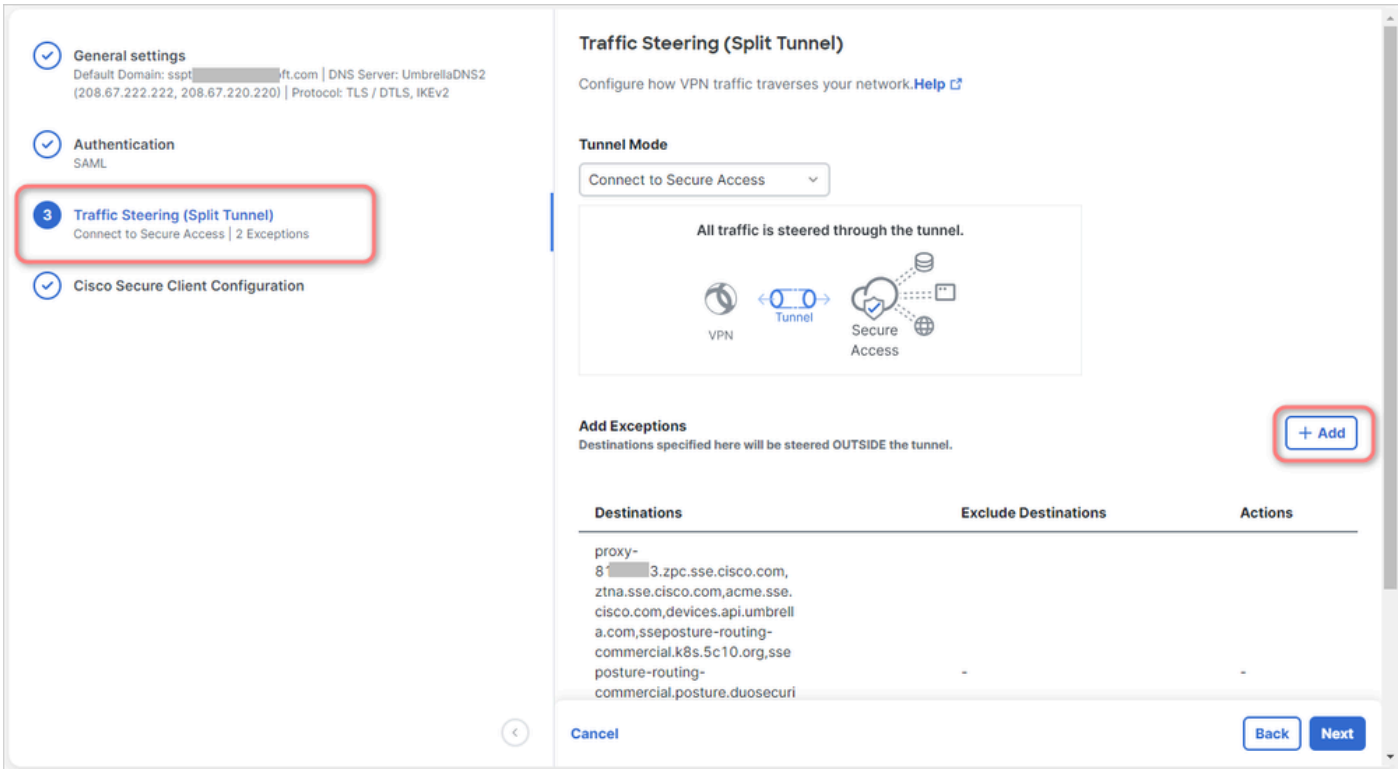
Passare al Cisco Secure Access Dashboard:

- Fare clic su **Connect > End User Connectivity**

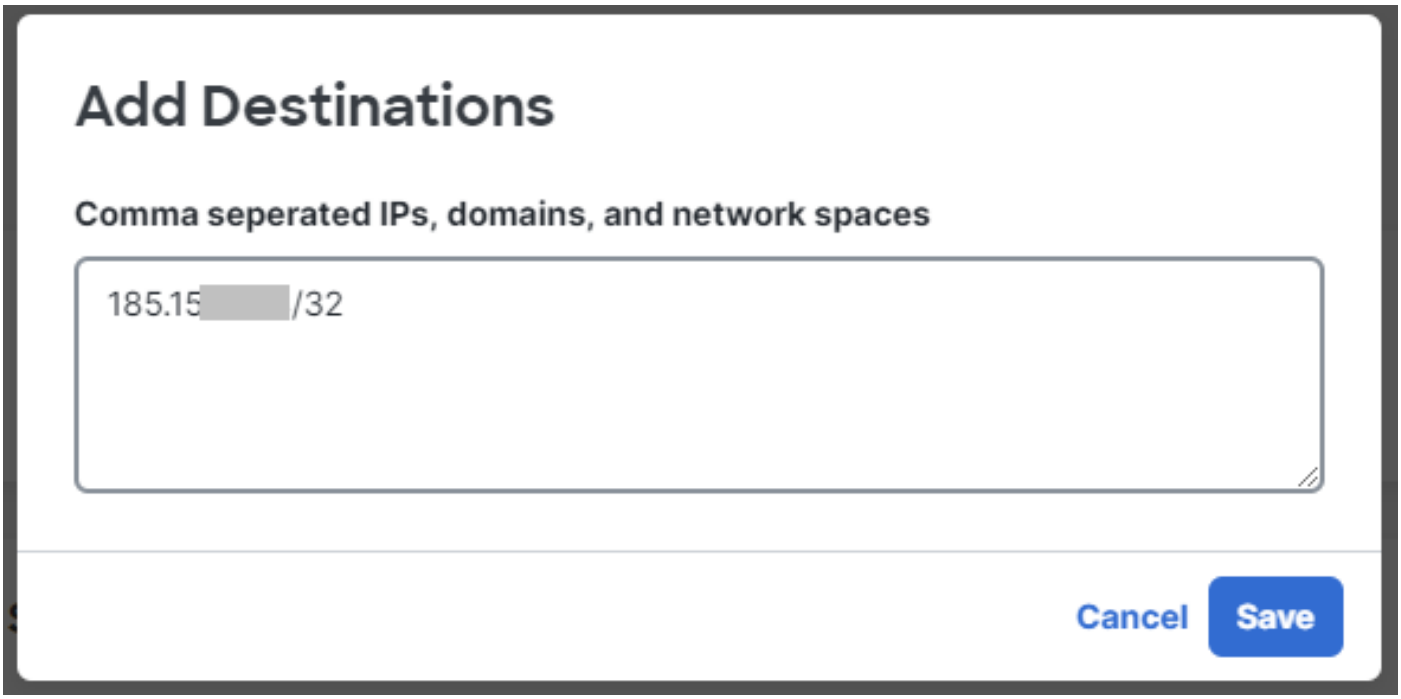
- Fare clic su Virtual Private Network
- Scegliere il profilo da modificare e fare clic su **Edit**



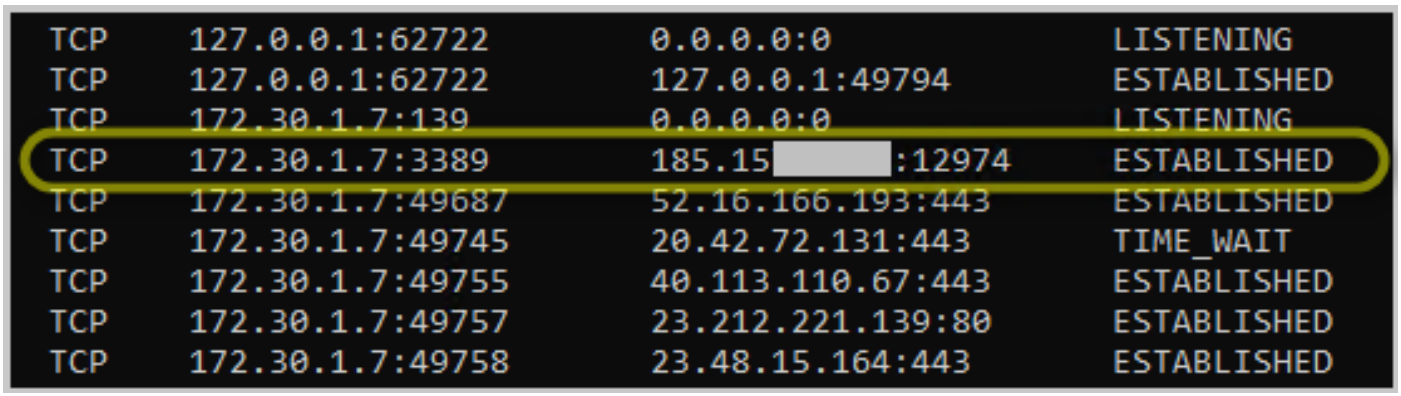
- Fare clic su **Traffic Steering (Split Tunnel) > Add Exceptions > + Add**

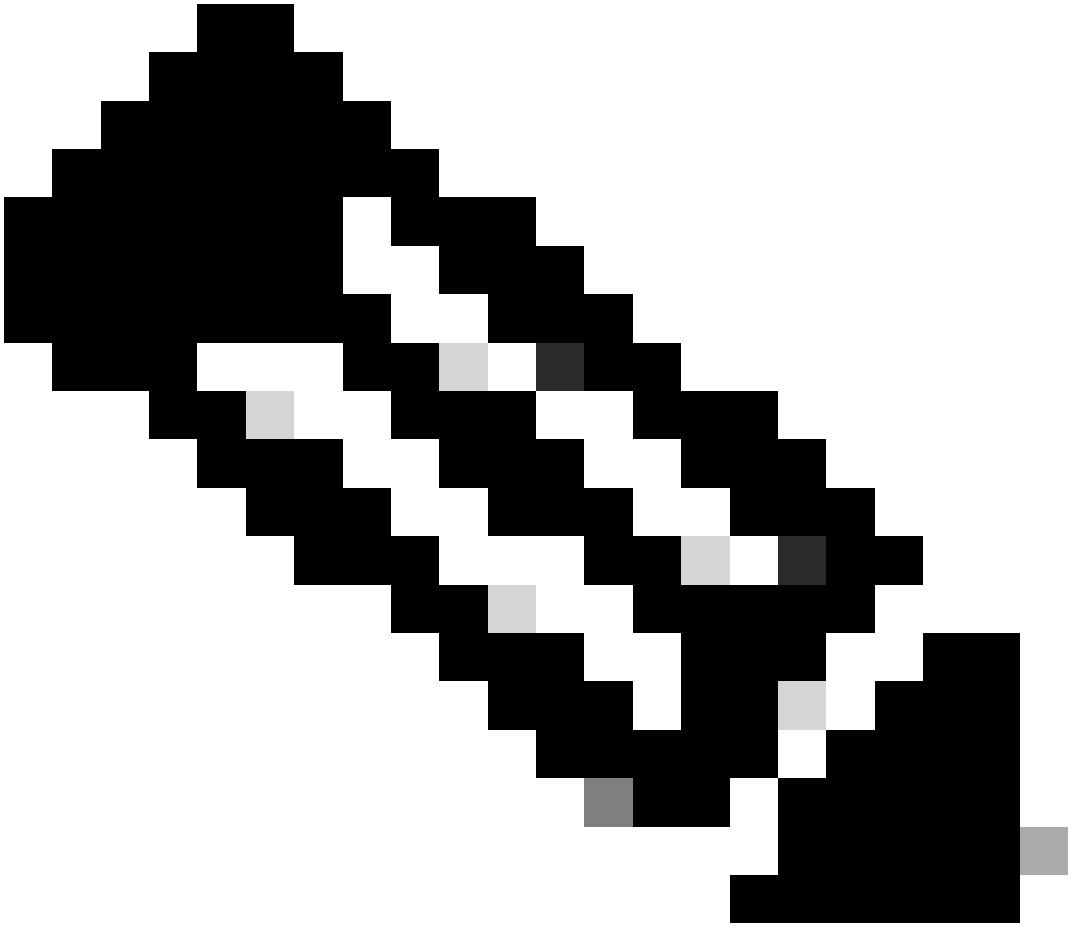


- Aggiungere l'indirizzo IP da cui è stata stabilita la connessione RDP



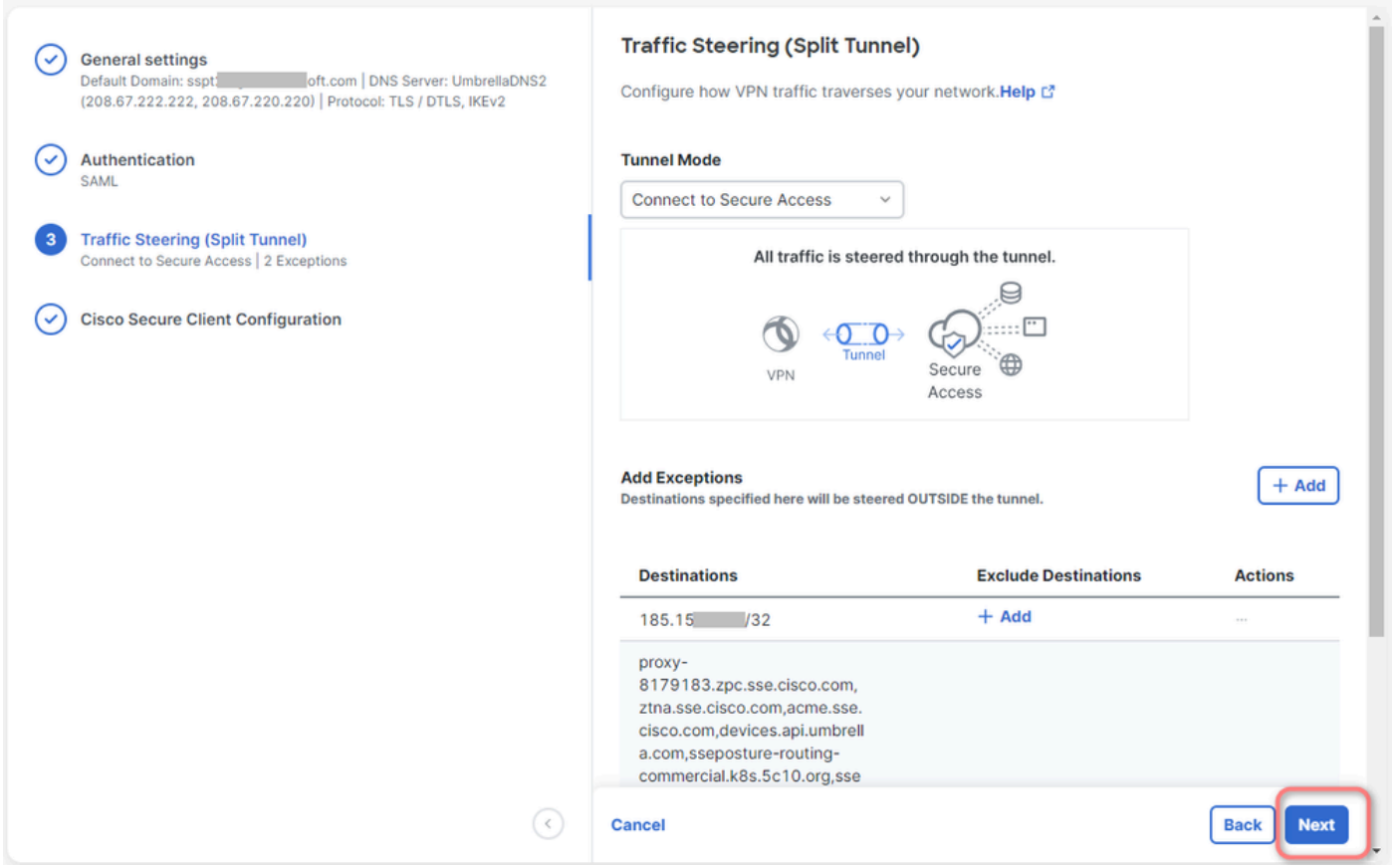
- Fare clic su **Save** In **Add Destinations** window



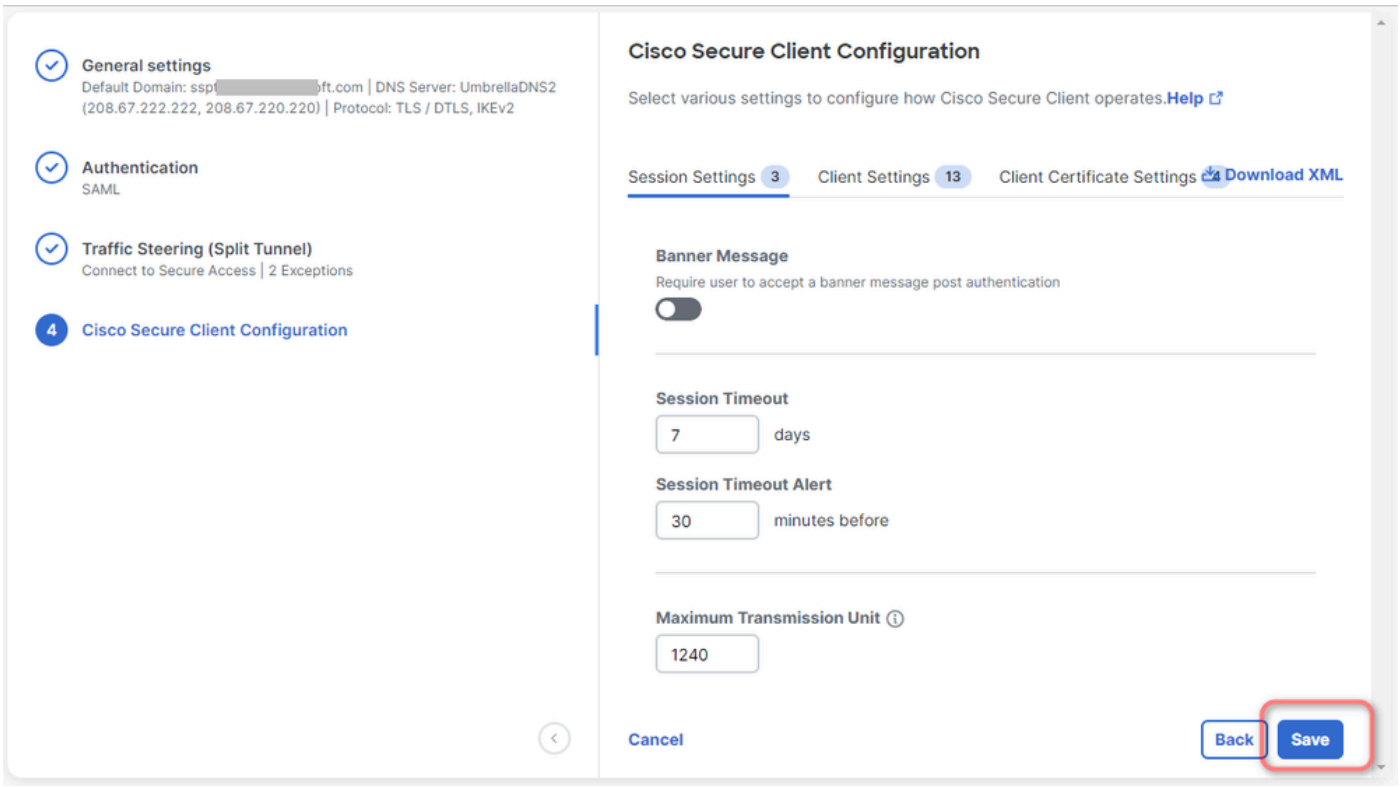


Nota: l'indirizzo IP può essere trovato dall'output del comando **netstat -an**cmd.; Notare l'indirizzo IP da cui è stata stabilita una connessione all'indirizzo IP locale del desktop remoto alla porta 3389.

- Fare clic su **Next** dopo aver aggiunto l'eccezione:



- Fare clic su **Save** Changes (Modifiche) nel profilo VPN:



Informazioni correlate

-

Aggiungi profili VPN

- Guida per l'utente di Secure Access
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).