Dépannage de l'erreur d'accès sécurisé " ; La connexion VPN a été démarrée par un utilisateur du Bureau à distance dont la console a été déconnectée" ;

Table des matières

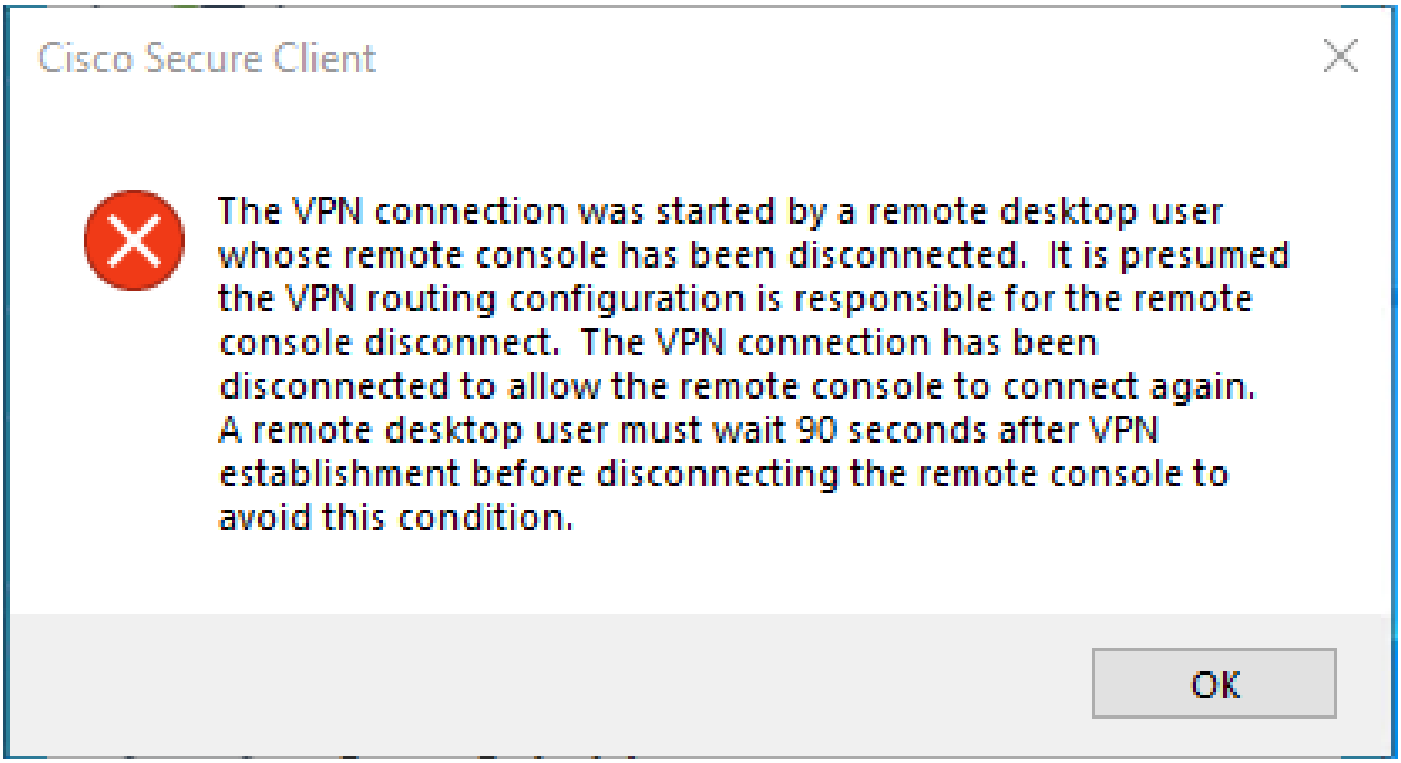
Introduction

Ce document décrit comment corriger l'erreur : "La connexion VPN a été démarrée par un utilisateur de bureau à distance dont la console à distance a été déconnectée".

Problème

Lorsqu'un utilisateur tente de se connecter avec RA-VPN (Remote Access VPN) à la tête de réseau d'accès sécurisé, l'erreur s'affiche dans la fenêtre contextuelle de notification du client sécurisé 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.



L'erreur mentionnée est générée lorsque l'utilisateur est connecté via le protocole RDP au PC Windows, tente de se connecter à RA-VPN à partir du PC donné, et Tunnel Mode dans le profil VPN est défini sur **Connect to Secure Access (default option)** et l'IP source de la connexion RDP n'est pas ajoutée aux exceptions.

Pour **Traffic Steering (Split Tunnel)**, vous pouvez configurer un profil VPN pour maintenir une connexion de tunnel complète à l'accès sécurisé ou configurer le profil pour utiliser une connexion de tunnel partagée pour diriger le trafic via le VPN uniquement si nécessaire.

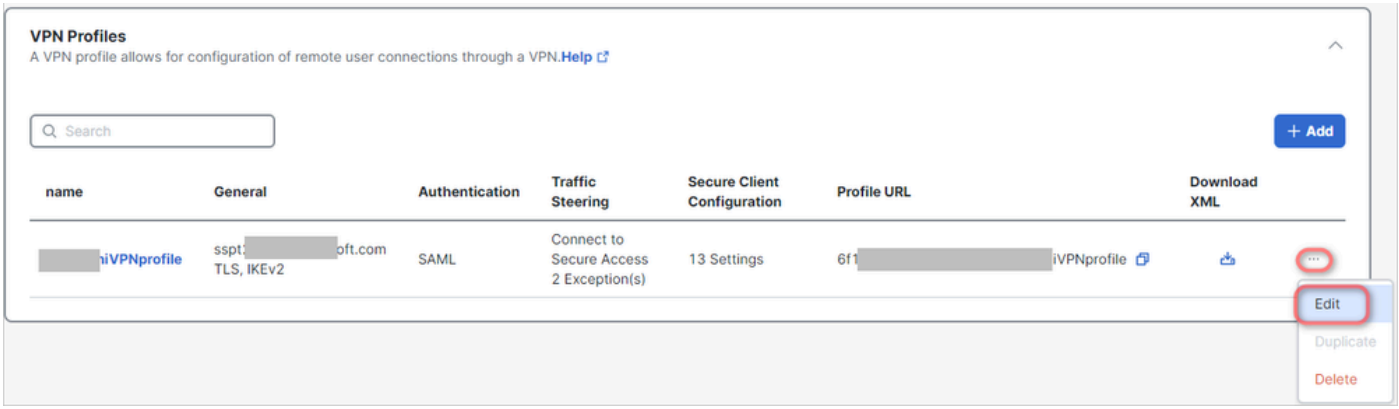
- Pour **Tunnel Mode**, choisissez :
  - **Connect to Secure Access** diriger tout le trafic à travers le tunnel ; ou
    - **Bypass Secure Access** pour diriger tout le trafic en dehors du tunnel.
- En fonction de votre sélection, vous pouvez **Add Exceptions** diriger le trafic à l'intérieur ou à l'extérieur du tunnel. Vous pouvez saisir des adresses IP, des domaines et des espaces réseau séparés par des virgules.

Solution

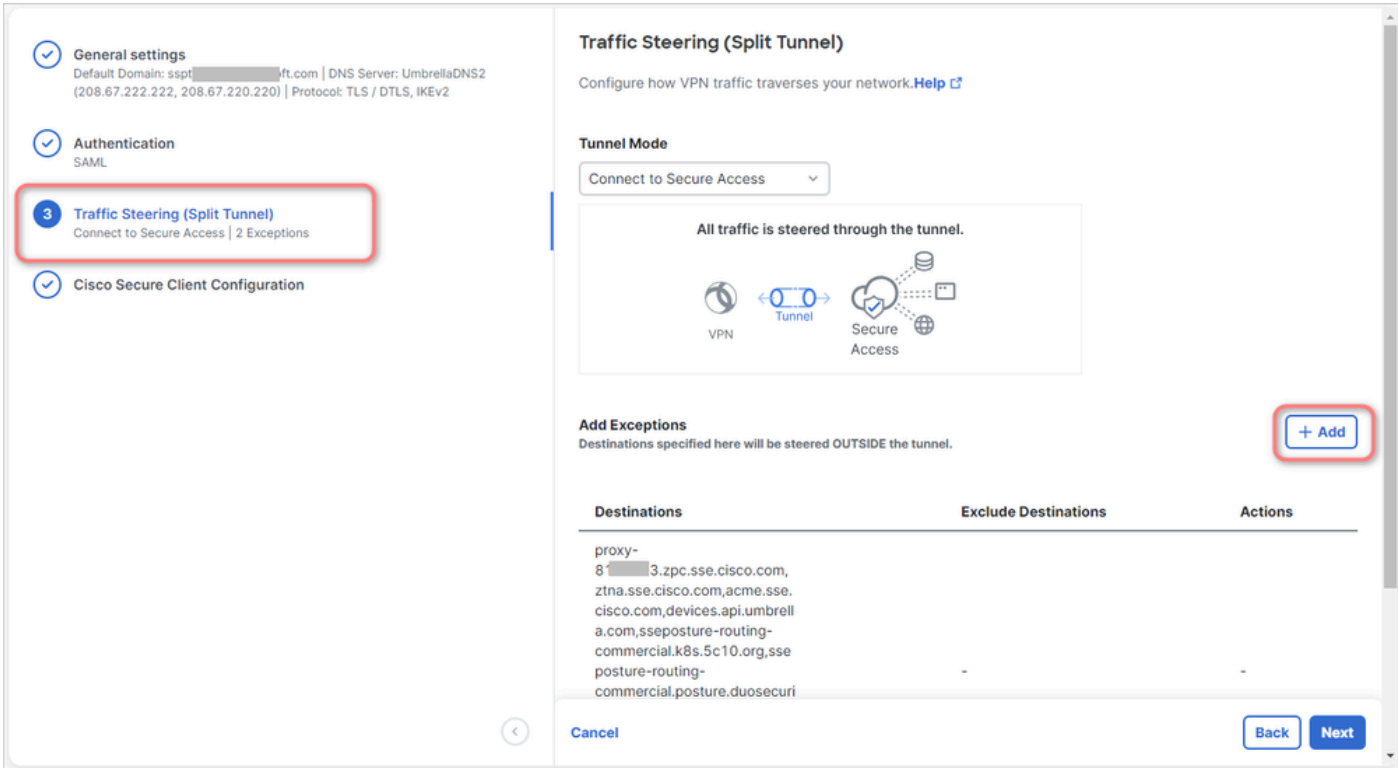
Accédez au tableau de bord Cisco Secure Access :

- Cliquez sur **Connect > End User Connectivity**
- Cliquez sur Virtual Private Network

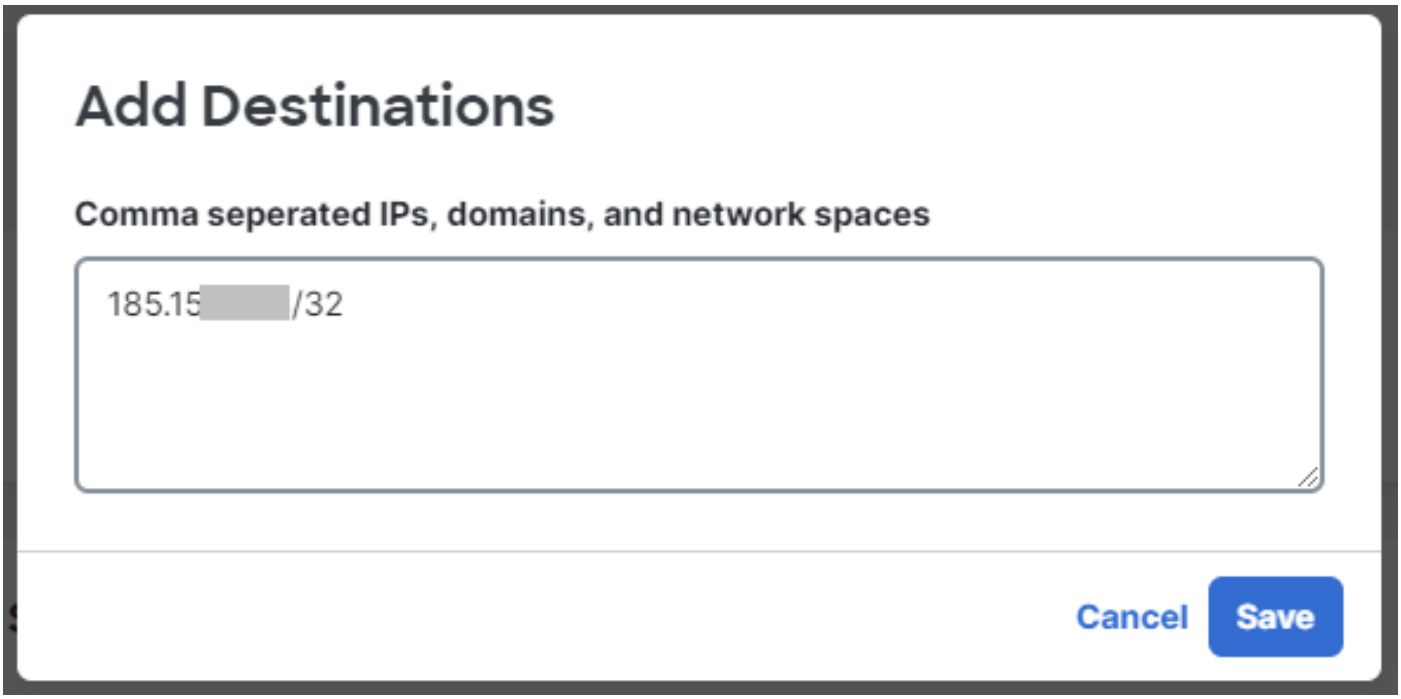
- Choisissez le profil que vous souhaitez modifier et cliquez sur **Edit**



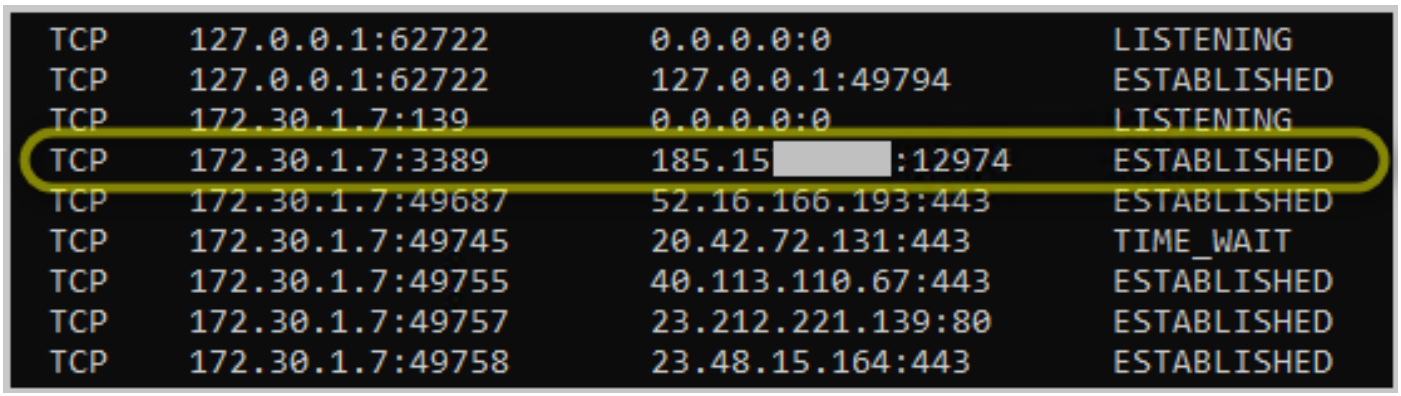
- Cliquez sur **Traffic Steering (Split Tunnel)** > **Add Exceptions** > **+ Add**

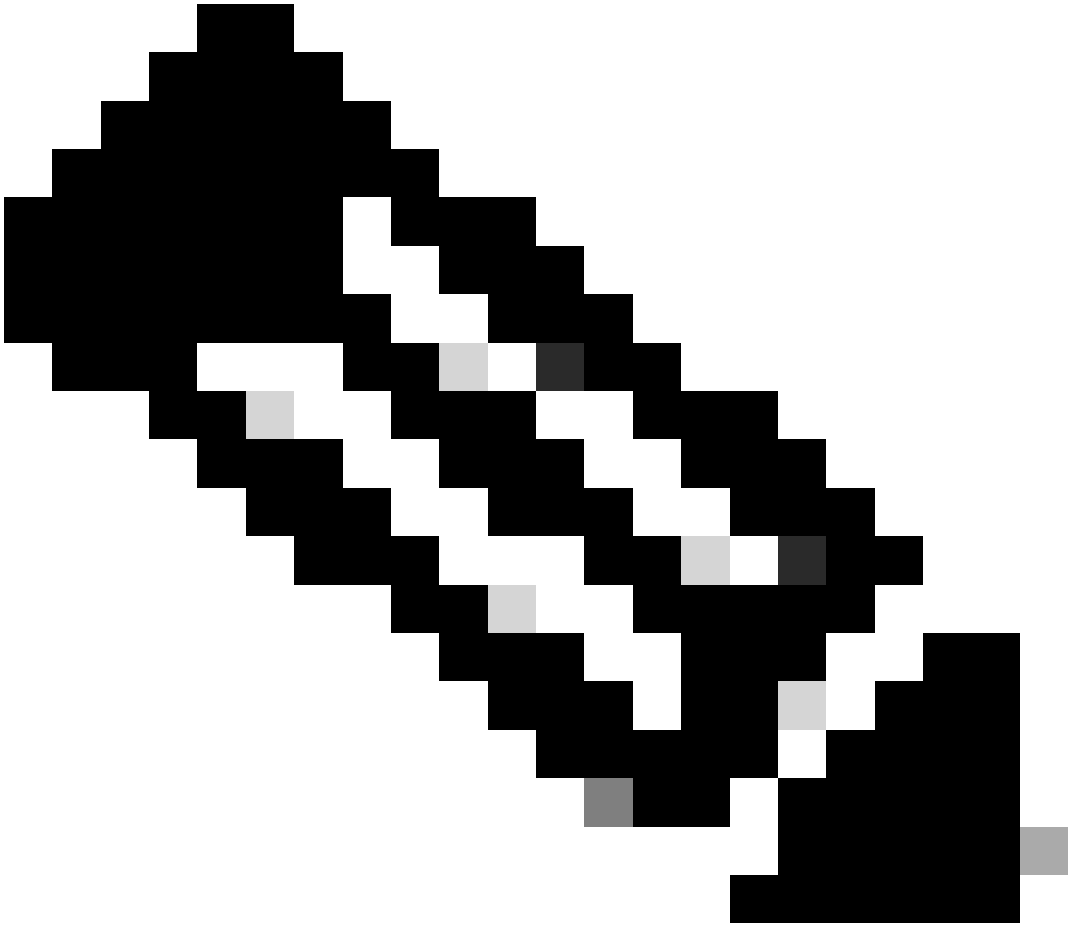


- Ajoutez votre adresse IP à partir de laquelle vous avez établi la connexion RDP



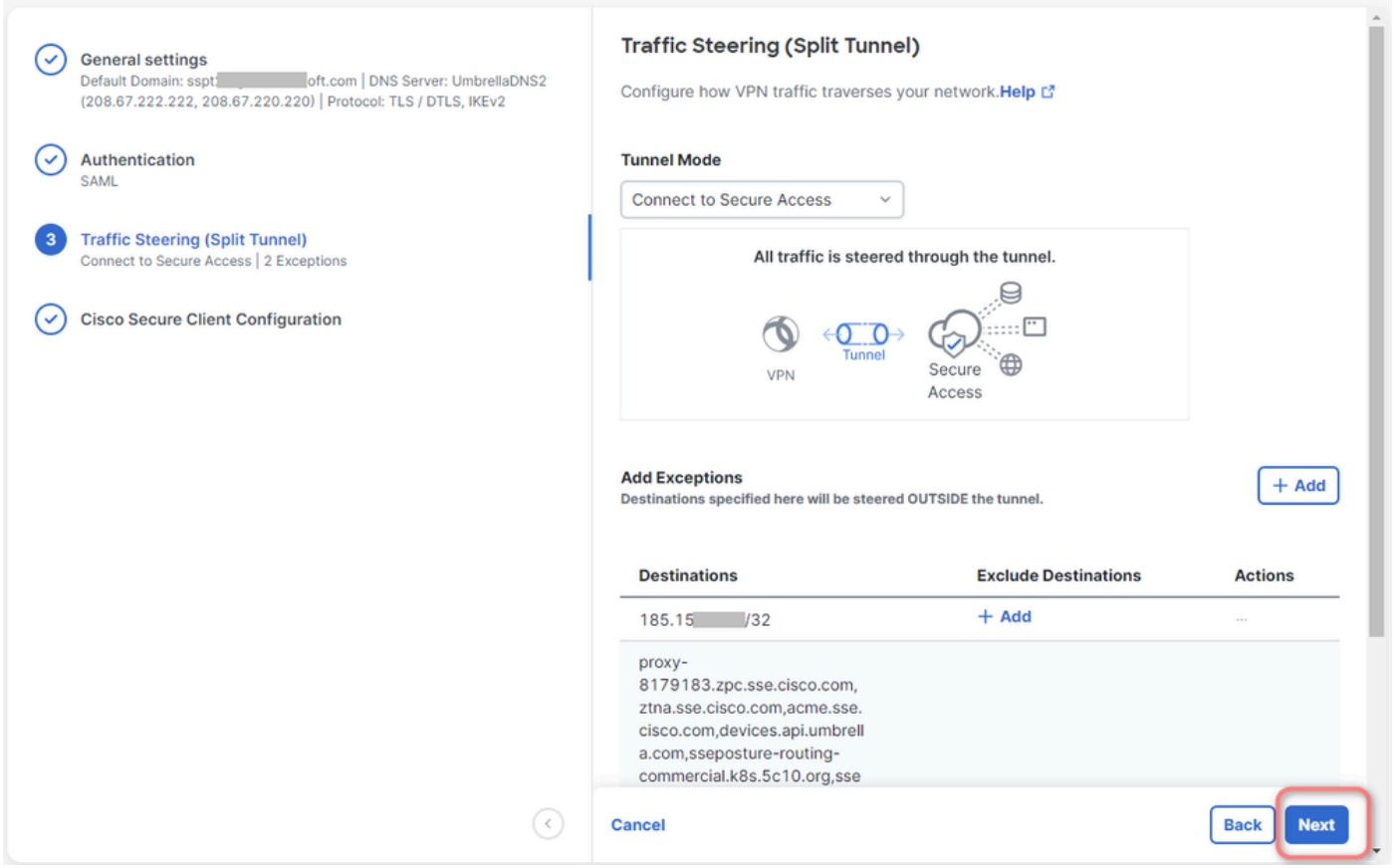
- Cliquez sur **Save** In **Add Destinations** window



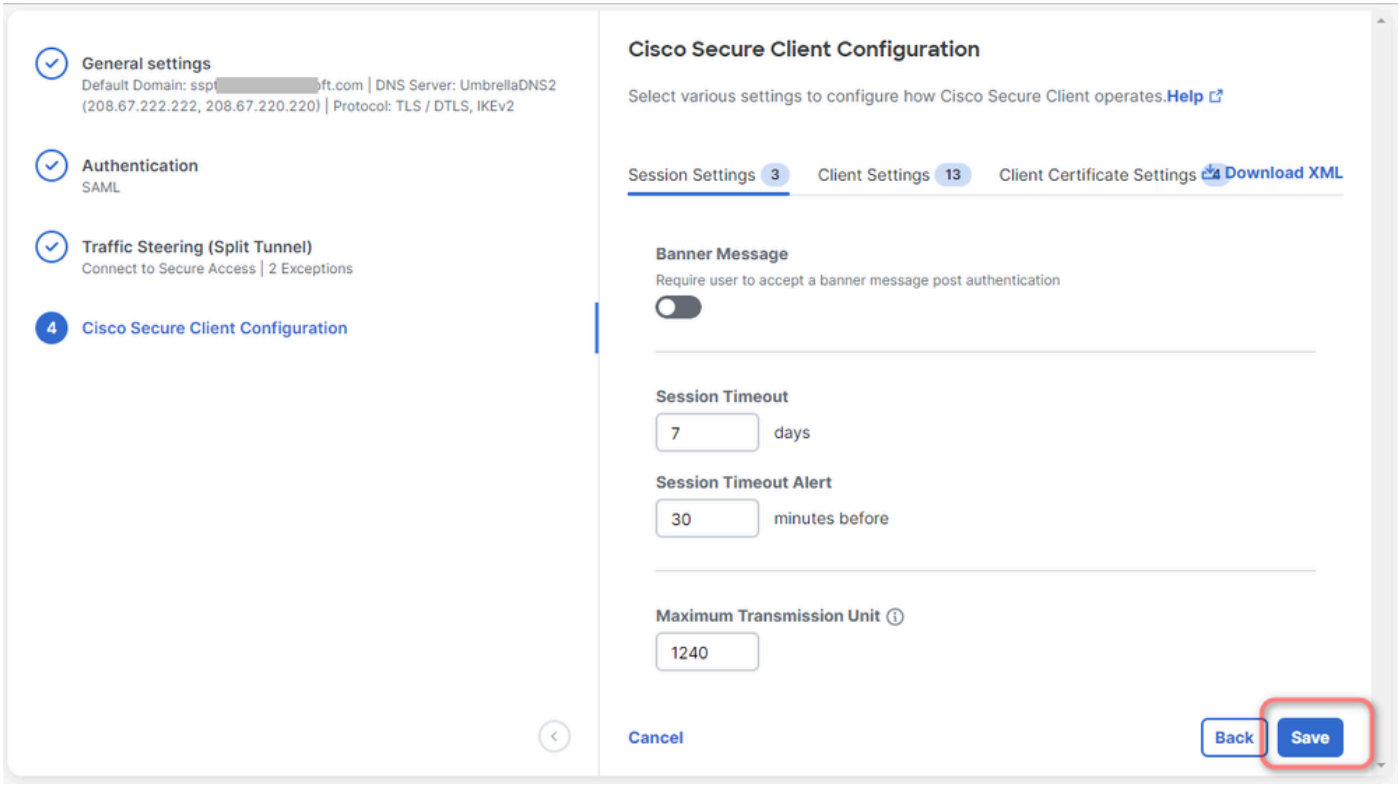


Remarque : l'adresse IP peut être trouvée à partir du résultat de la commande cmd **netstat -an**. ; Notez l'adresse IP à partir de laquelle il y a une connexion établie à l'adresse IP locale du bureau distant vers le port 3389.

- Cliquez **Next** après avoir ajouté l'exception :



- Cliquez sur **Save** changes dans le profil VPN :



Informations connexes

-

Ajouter des profils VPN

- Guide de l'utilisateur Secure Access
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.