L'état en temps réel de l'agent d'utilisateur est affiché en tant qu'inconnu

Contenu

[Introduction](#)
[Symptôme](#)
[Solution](#)

Introduction

Après avoir déployé un agent d'utilisateur de Sourcefire, vous pouvez noter que l'état en temps réel demeure inconnu après avoir suivi toutes les étapes de configuration. Ce document fournit l'instruction sur la façon dont changer l'état d'**inconnu à disponible**.

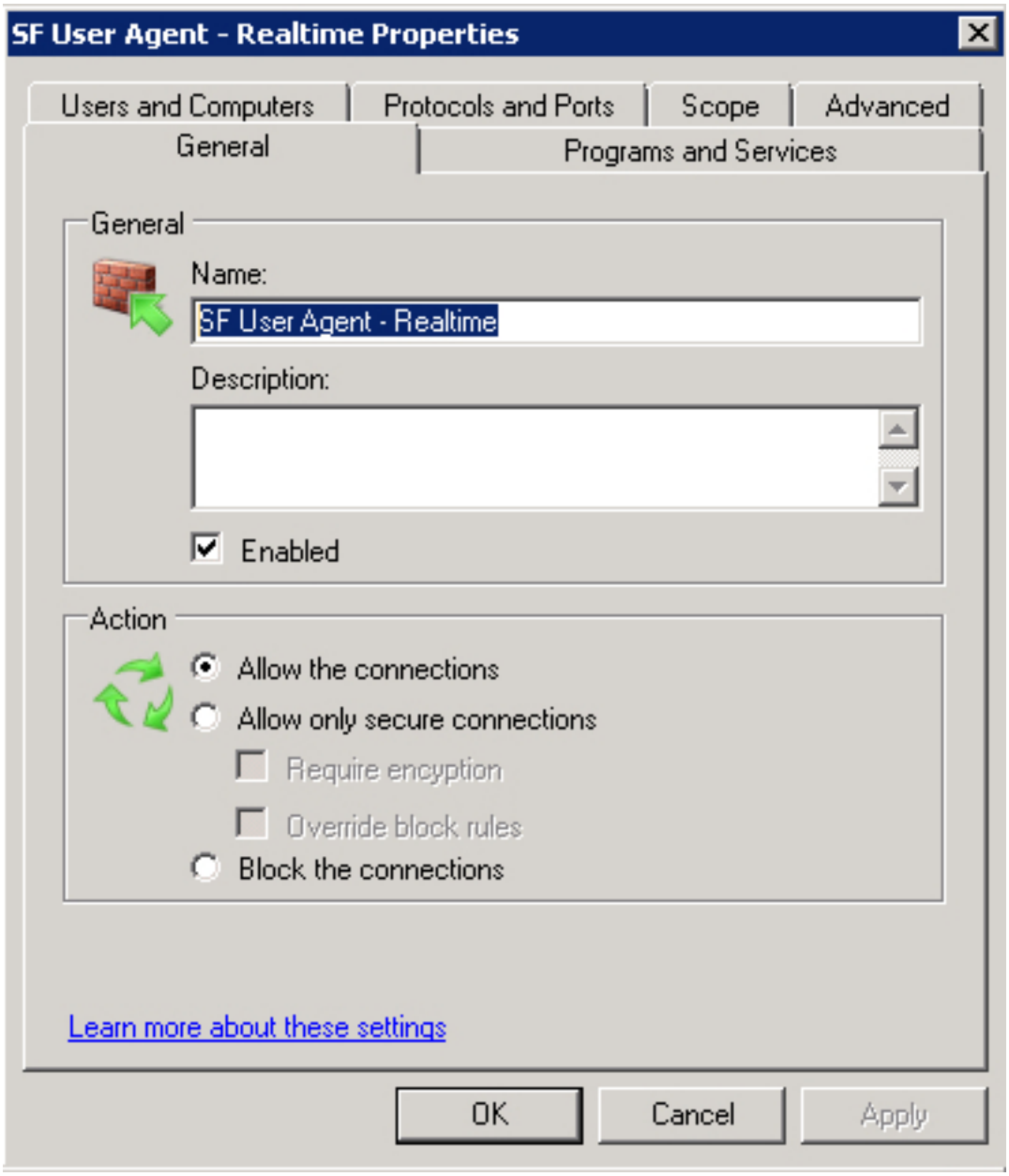
Symptôme

Les paramètres du pare-feu du contrôleur de domaine empêchent les connexions exigées RPC d'être établi. L'agent d'utilisateur emploie les connexions de port dynamiques RPC pour se relier au contrôleur de domaine et pour établir le suivi en temps réel.

Solution

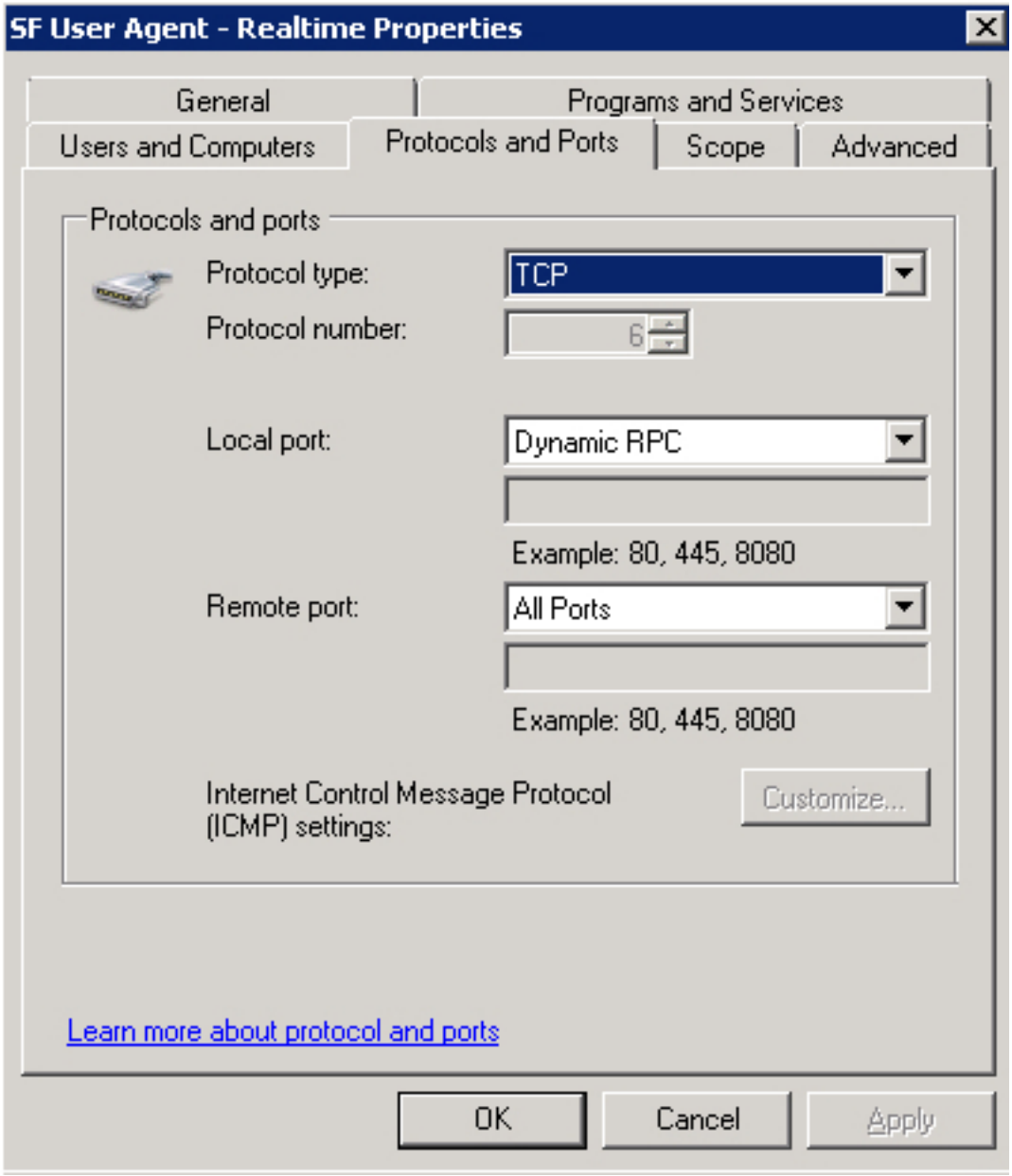
Créez une règle d'arrivée de Pare-feu sur le contrôleur de domaine visé utilisant le **pare-feu Windows avec la** console de **sécurité avancée**, permettant à la connexion nécessaire de l'agent d'utilisateur pour avoir lieu. Un exemple des configurations et des étapes sont affichés ci-dessous :

1. Sur l'**onglet Général**, nommez la règle et choisi **permettez les connexions**.

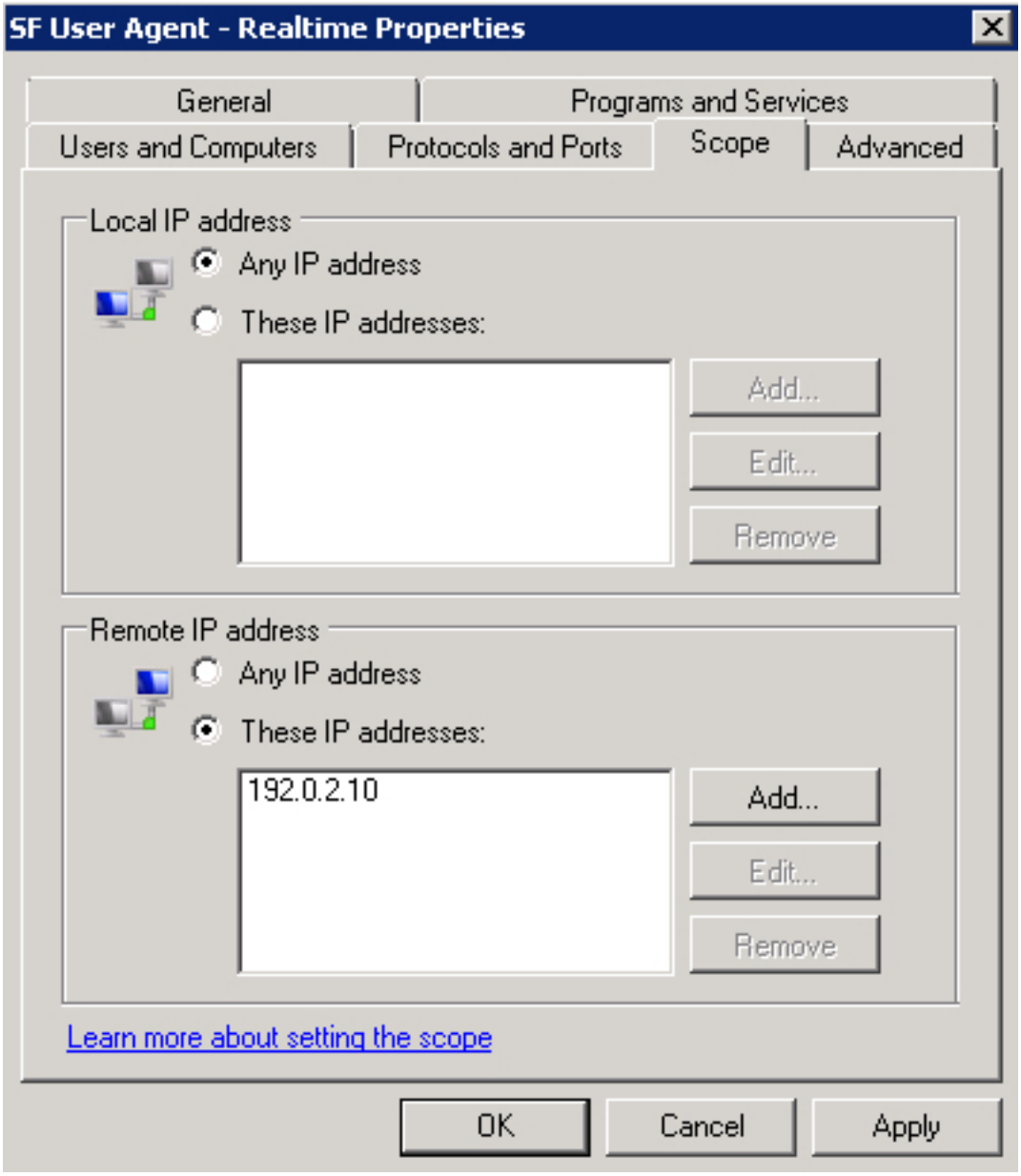


2. Sur les **protocoles et les ports** tabulez, sélectionnez les articles suivants :

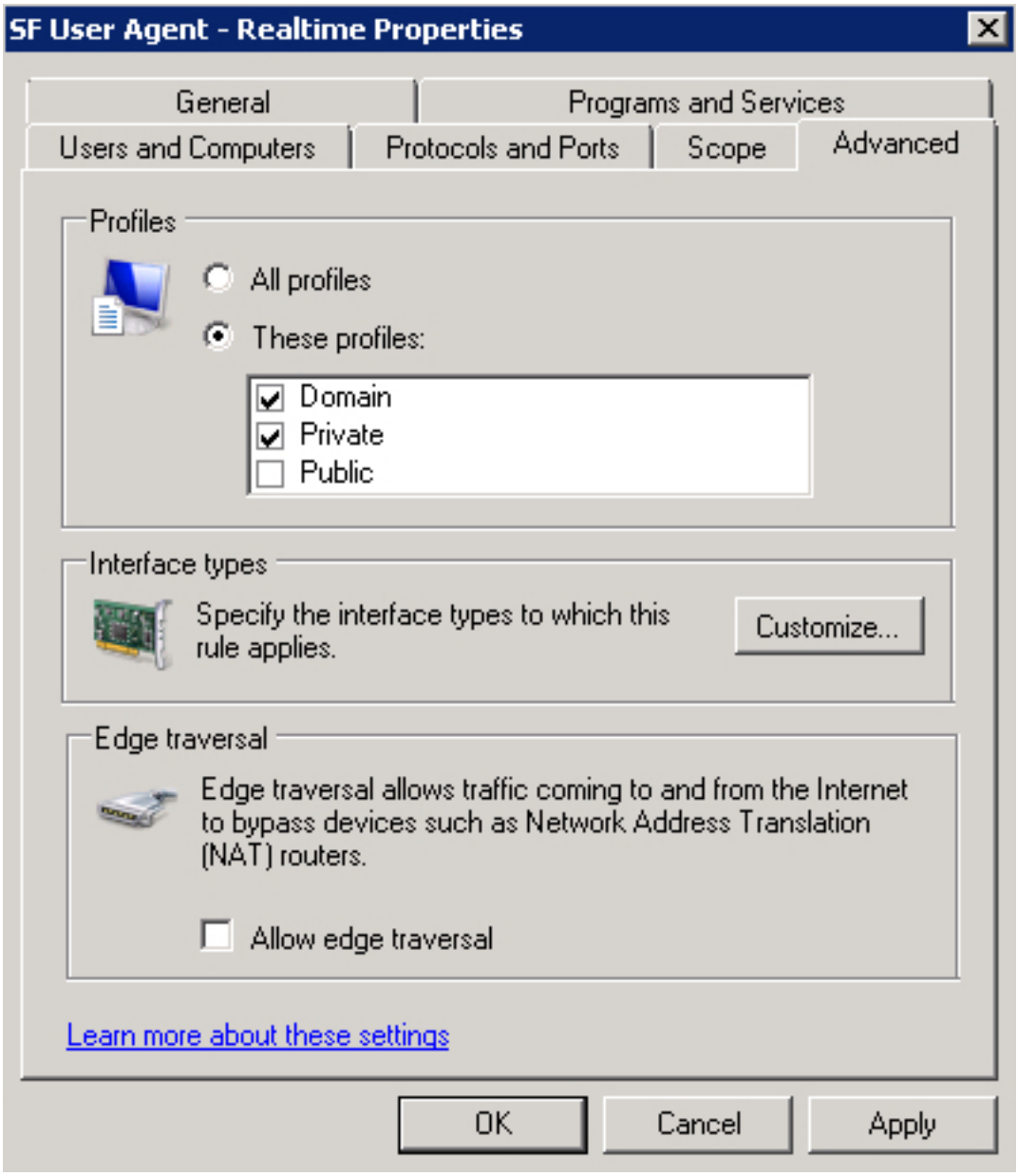
- **Type de Protocol** : TCP
- **Port local** : RPC dynamique
- **Port distant** : Tous les ports



3. Sur l'onglet de **portée**, ajoutez l'**adresse IP distante**. Cliquez sur Add pour écrire l'adresse IP de l'hôte d'agent d'utilisateur.



4. Sur l'**onglet Avancé**, **profils** appropriés choisis.



Sauvegardez la règle de Pare-feu, activez-la et redémarrez le service d'agent d'utilisateur de Sourcefire. Votre état de la connexion en temps réel devrait maintenant changer d'**inconnu à disponible**.