

L'état en temps réel de l'agent utilisateur est affiché comme Inconnu

Contenu

[Introduction](#)

[Symptôme](#)

[Solution](#)

Introduction

Après le déploiement d'un agent utilisateur Sourcefire, vous remarquerez peut-être que l'état en temps réel reste inconnu après avoir suivi toutes les étapes de configuration. Ce document fournit des instructions sur la façon de changer l'état de **Inconnu** à **Disponible**.

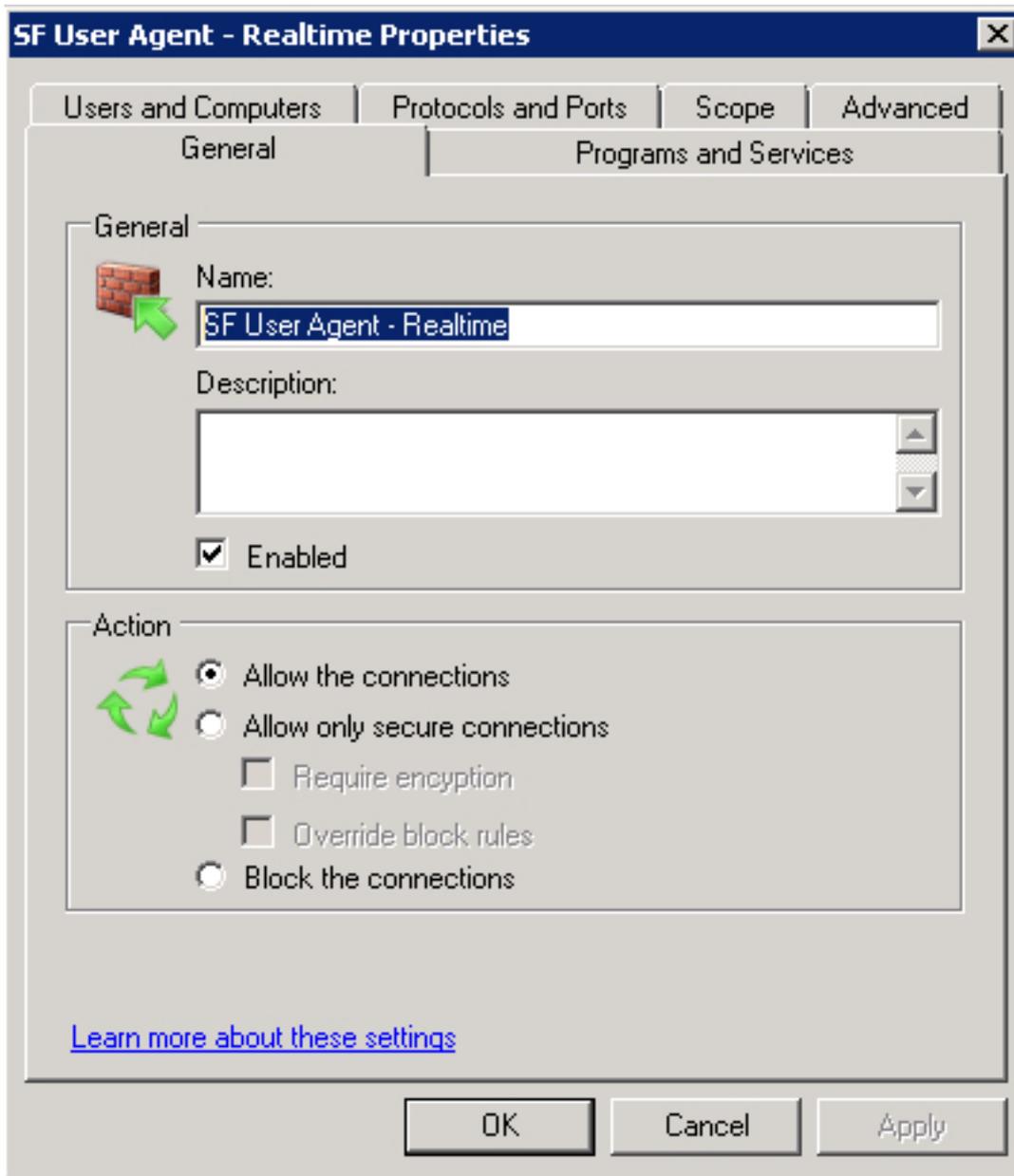
Symptôme

Les paramètres de pare-feu du contrôleur de domaine empêchent l'établissement des connexions RPC requises. L'agent utilisateur utilise les connexions de port dynamique RPC pour se connecter au contrôleur de domaine et établir une surveillance en temps réel.

Solution

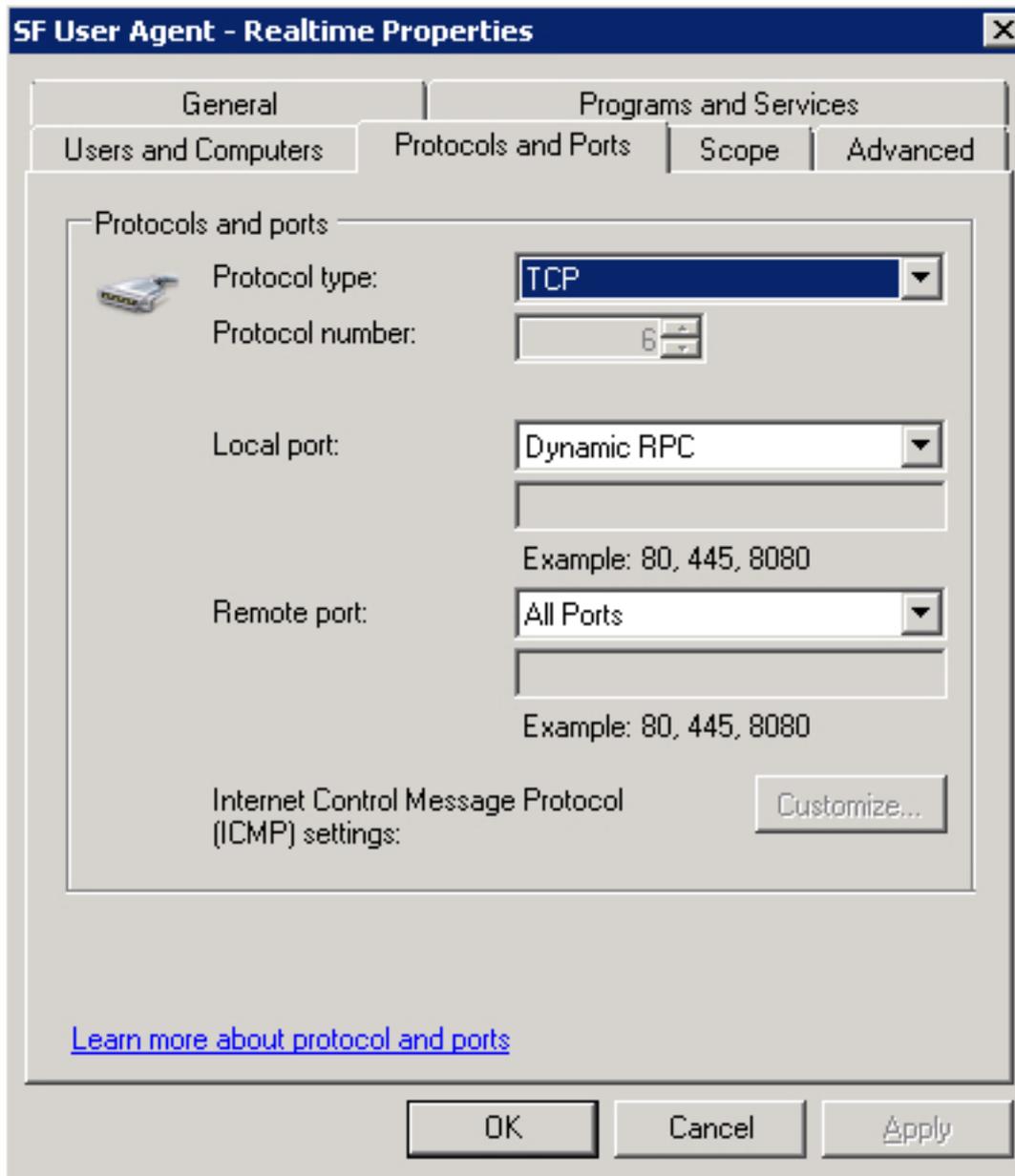
Créez une règle de pare-feu entrante sur le contrôleur de domaine ciblé à l'aide de la console **Pare-feu Windows avec sécurité avancée**, permettant la connexion nécessaire à partir de l'agent utilisateur. Voici un exemple de paramètres et d'étapes :

1. Dans l'onglet **General**, nommez la règle et sélectionnez **Allow the Connections**.

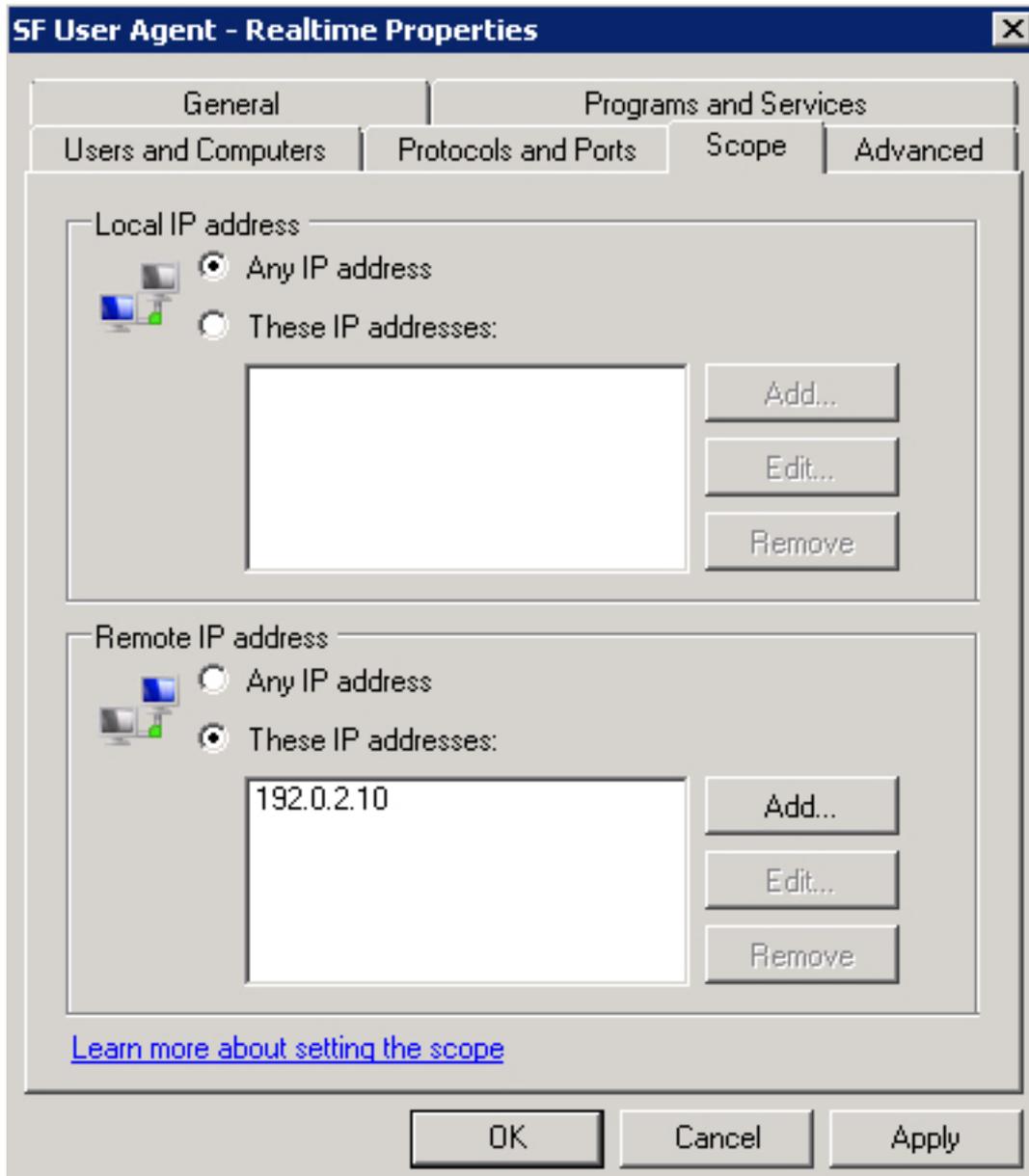


2. Dans l'onglet **Protocoles et ports**, sélectionnez les éléments suivants :

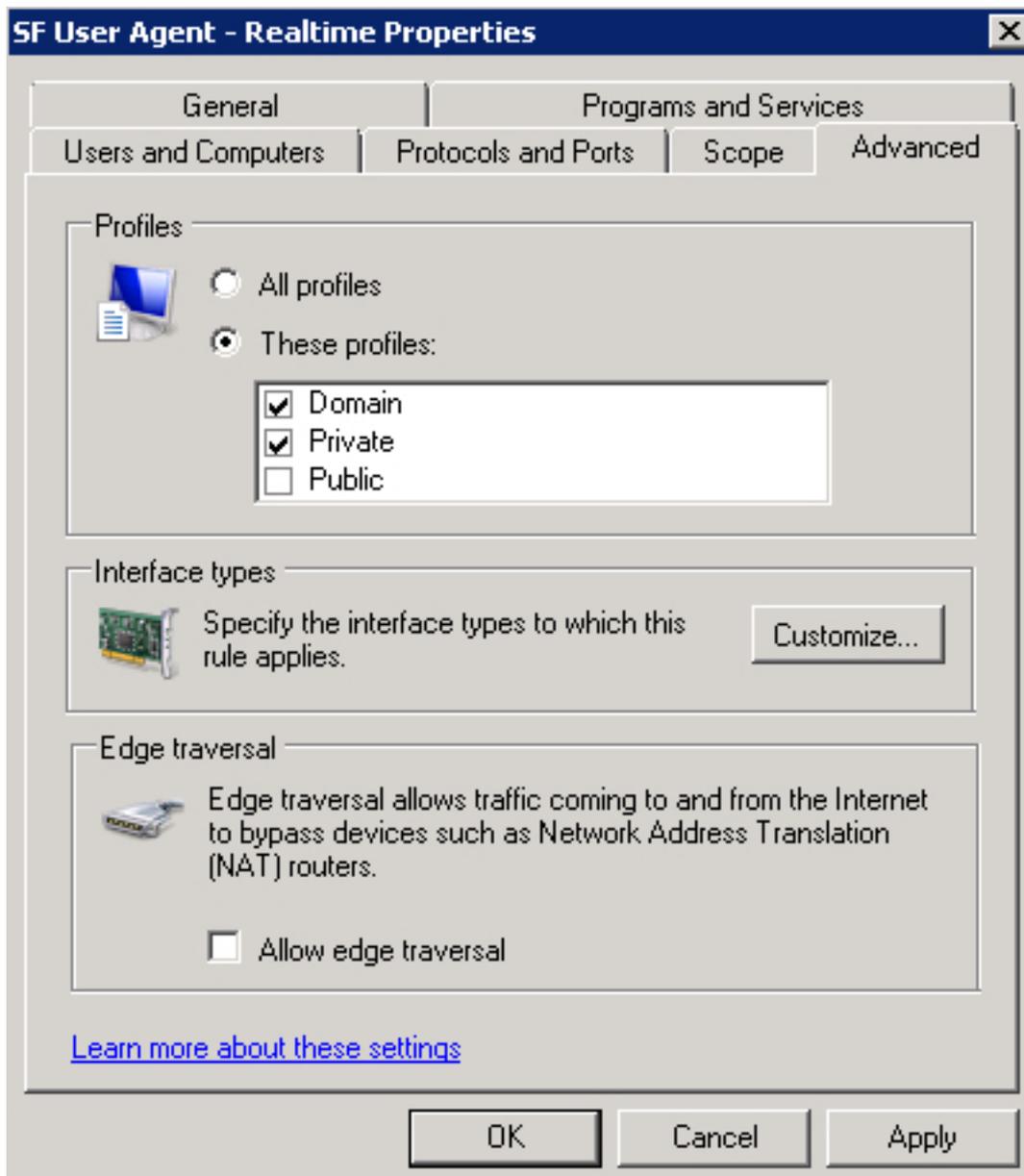
- **Type de protocole:** TCP
- **Port local :** RPC dynamique
- **Port distant :** Tous les ports



3. Dans l'onglet **Scope**, ajoutez l'adresse IP distante. Cliquez sur **Add** pour entrer l'adresse IP de l'hôte User Agent.



4. Dans l'onglet **Avancé**, sélectionnez les **profils** appropriés.



Enregistrez la règle de pare-feu, activez-la et redémarrez le service Sourcefire User Agent. L'état de votre connexion en temps réel doit maintenant passer de **Inconnu** à **Disponible**.