用户代理的实时状态显示为未知

目录

简介

部署Sourcefire用户代理后，您可能会注意到在执行所有配置步骤后，实时状态仍为未知。本文档提供有关如何将状态从**未知**更改为**可用**的说明。

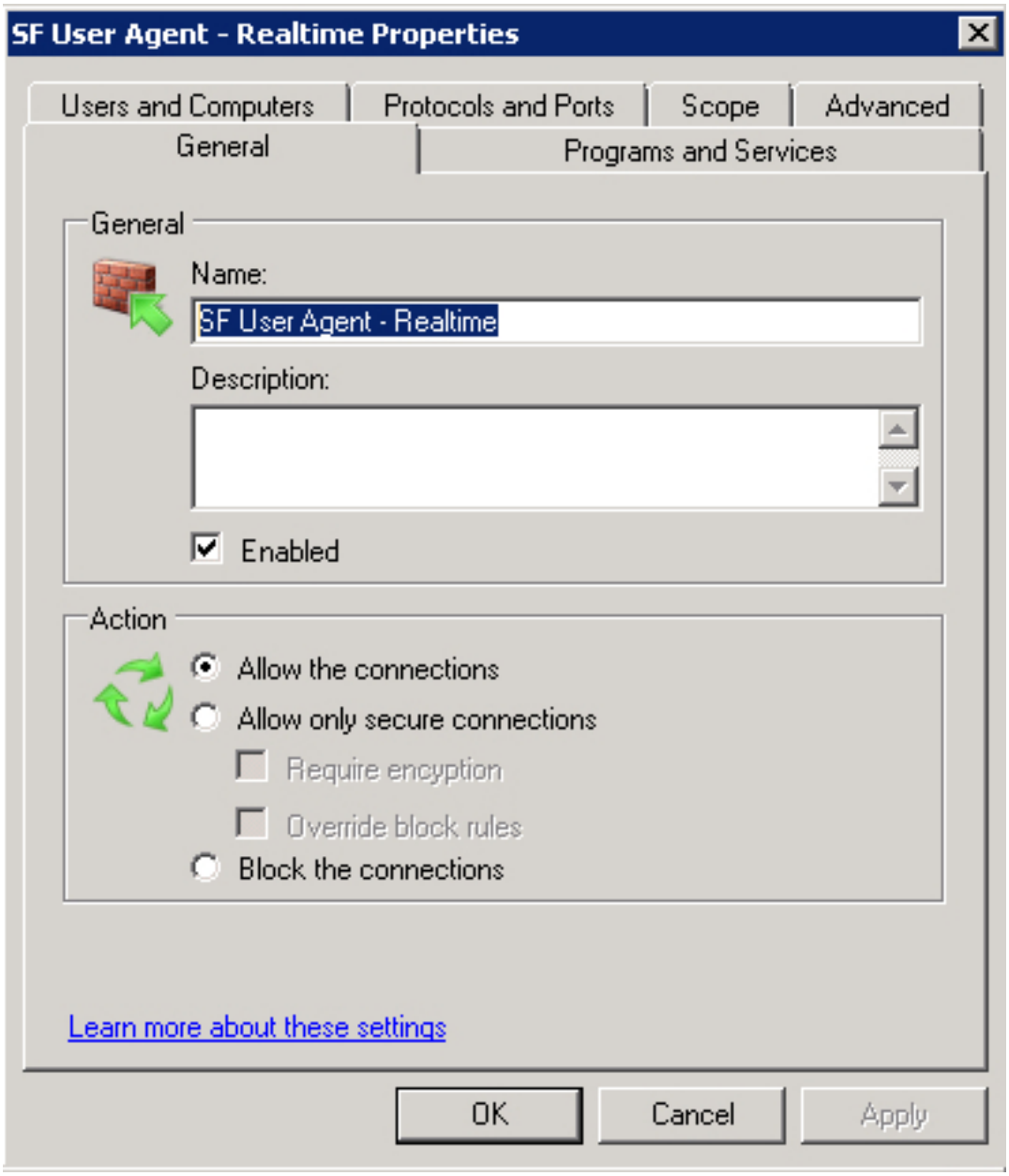
症状

域控制器的防火墙设置阻止建立所需的RPC连接。 用户代理使用RPC动态端口连接连接到域控制器并建立实时监控。

解决方案

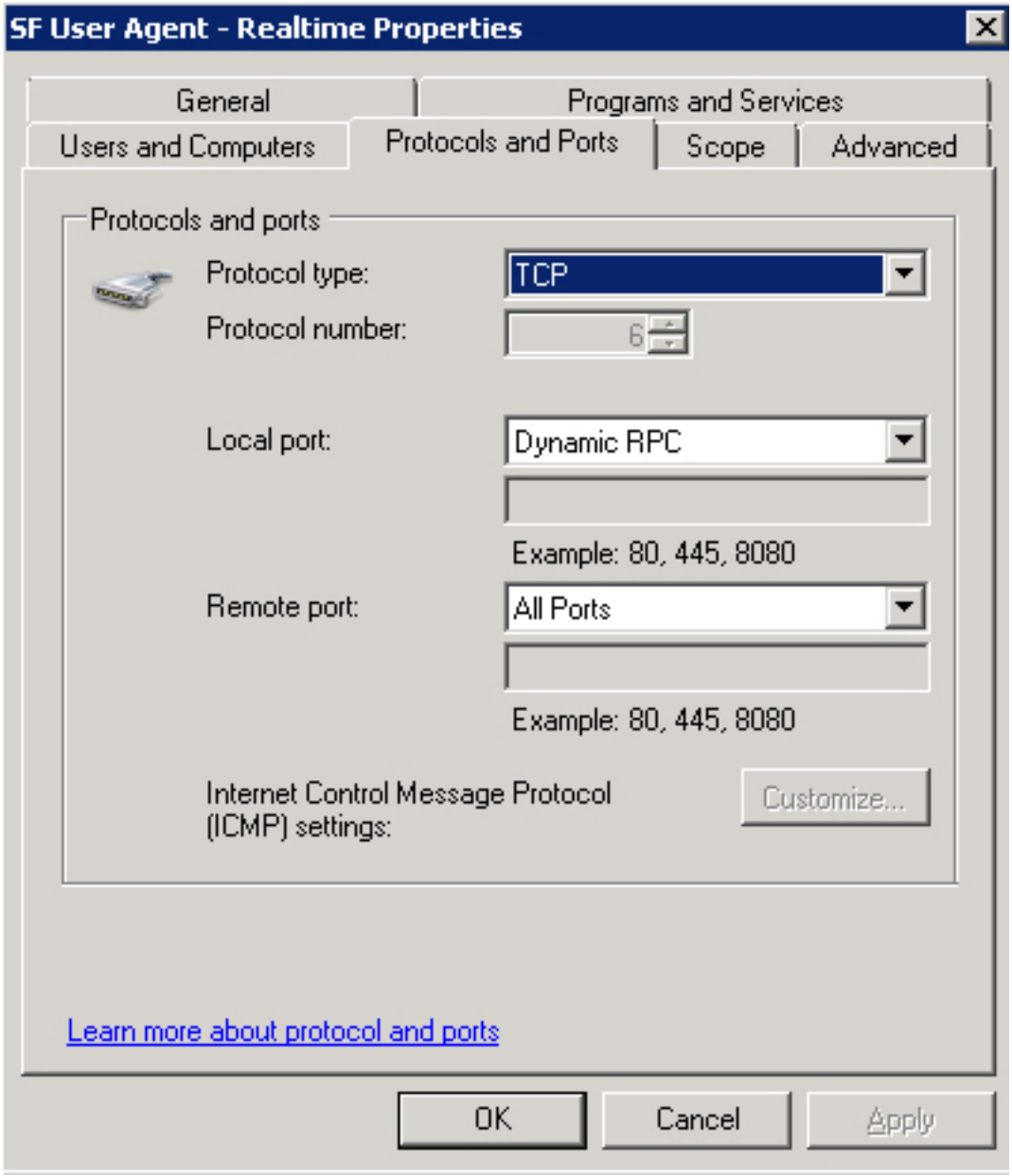
使用**Windows Firewall with Advanced Security**控制台在目标域控制器上创建入站防火墙规则，从而允许从用户代理进行必要的连接。设置和步骤示例如下所示：

1. 在**General**选项卡上，命名规则并选择**Allow the Connections**。

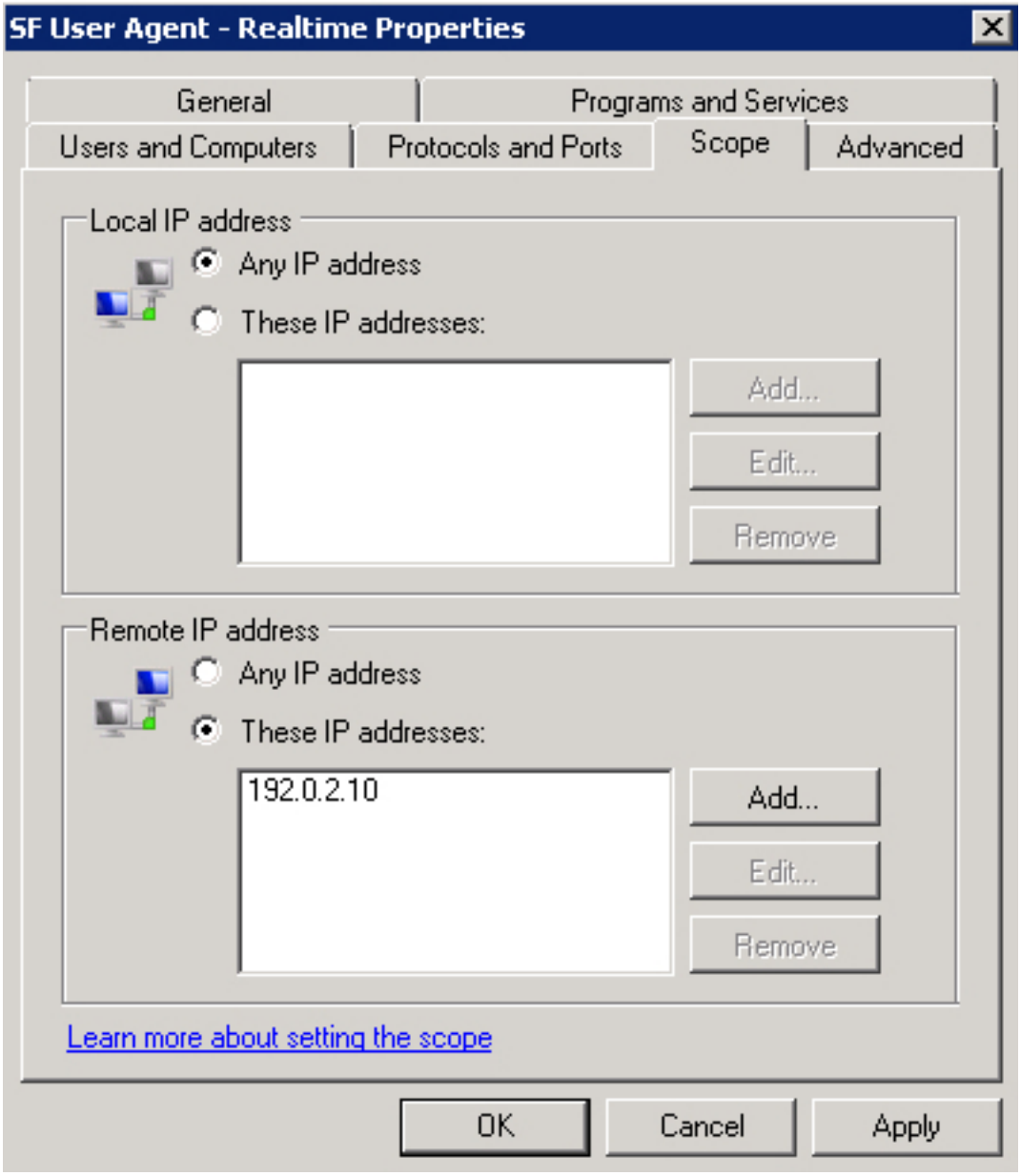


2. 在**Protocols and Ports**选项卡上，选择以下项目：

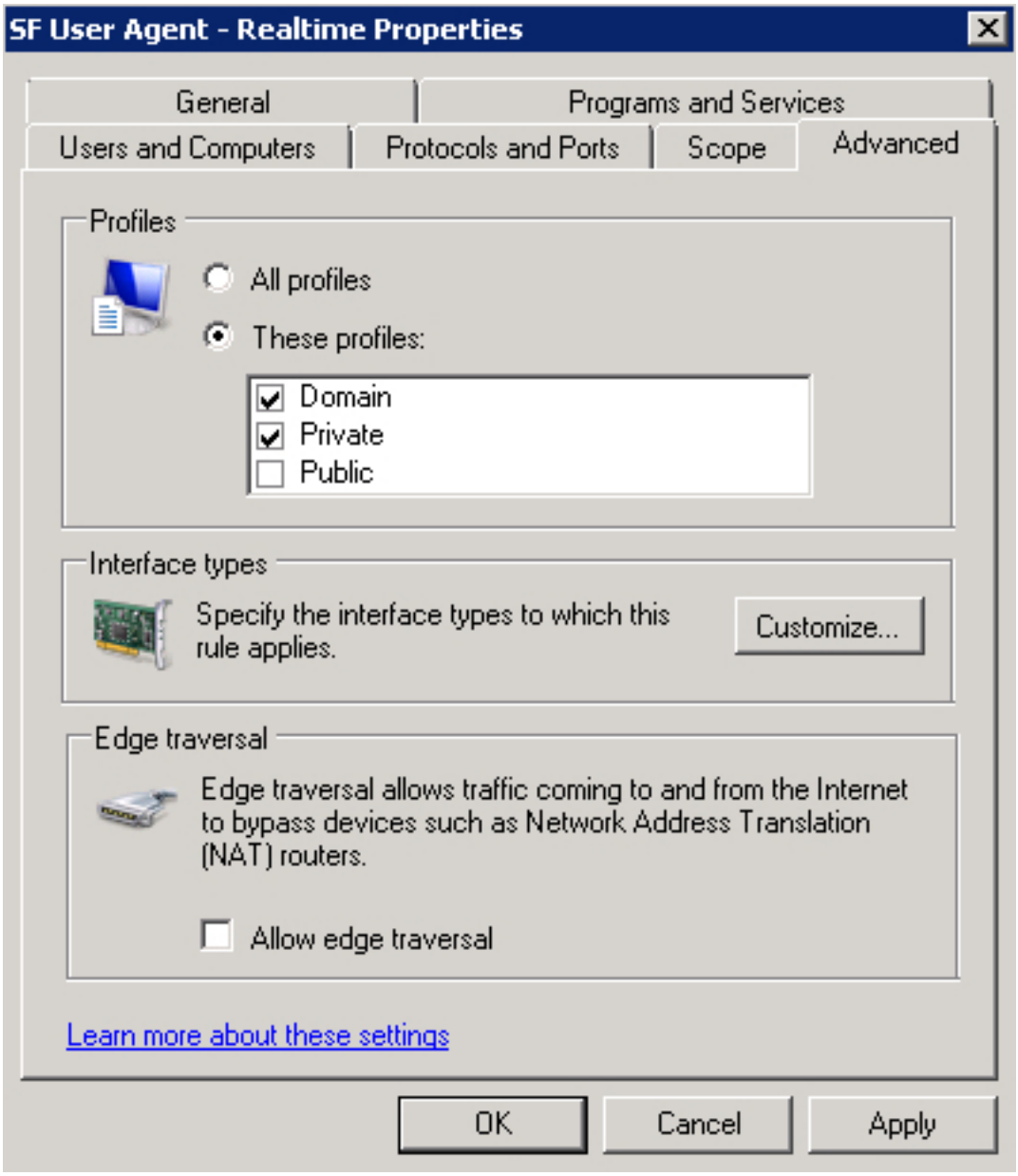
- **协议类型:**TCP
- **本地端口:**动态RPC
- **远程端口:**所有端口



3. 在**范围**选项卡上，添加**远程IP地址**。单击**Add**以输入用户代理主机的IP地址。



4. 在**Advanced**选项卡上，选择适当的**Profiles**。



保存防火墙规则，将其启用并重新启动Sourcefire用户代理服务。 您的实时连接状态现在应从**未知**更改为**可用**。