用户代理实时状况显示作为未知

目录

简介

在部署Sourcefire用户代理以后，您可以注意实时状态依然是未知在跟随所有以后配置步骤。本文提供说明关于怎样更改状态从**未知**到**联机**。

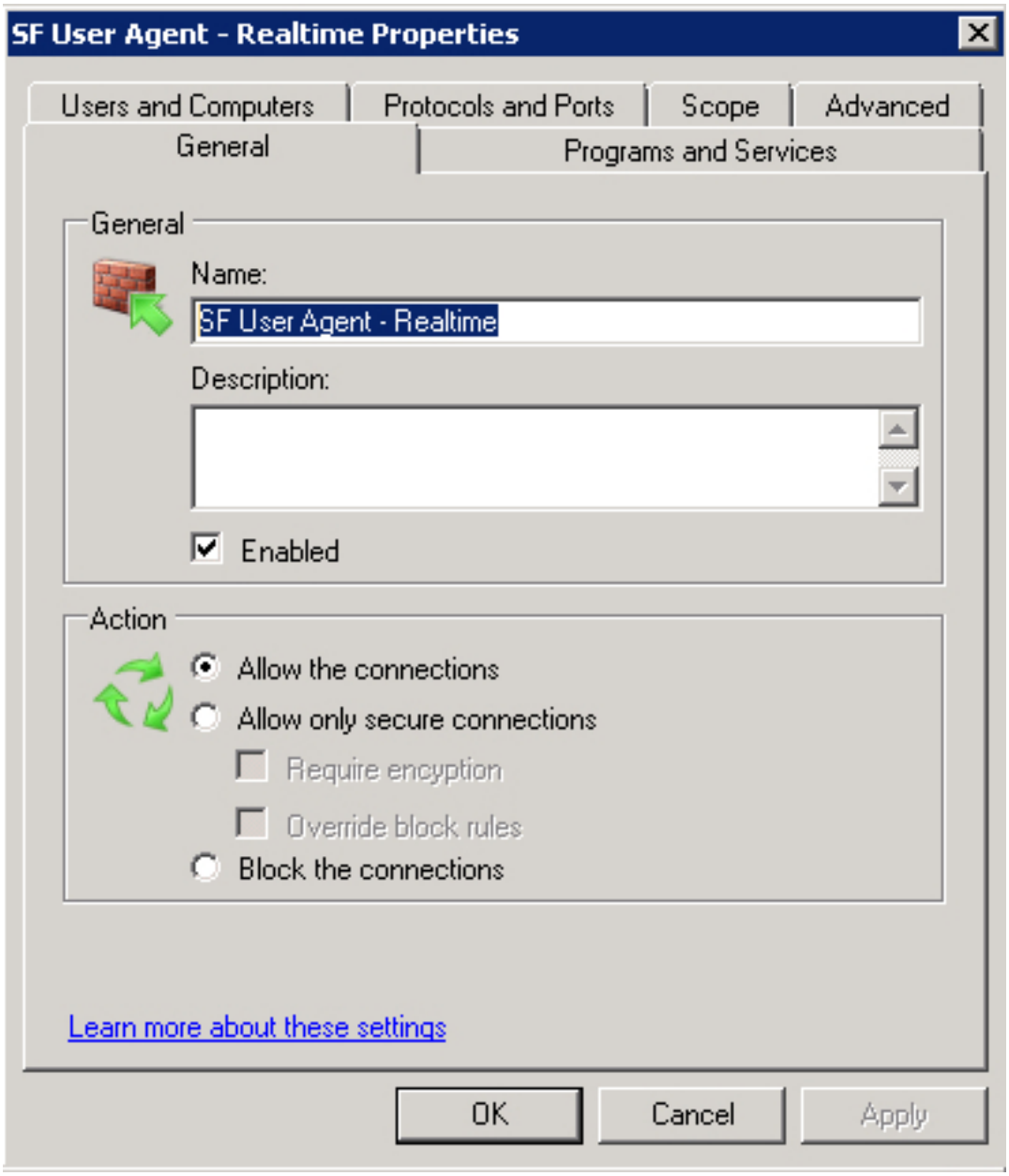
症状

域控制器的防火墙设置防止需要的RPC连接设立。 用户代理使用RPC动态端口连接附加到域控制器和设立实时监控。

解决方案

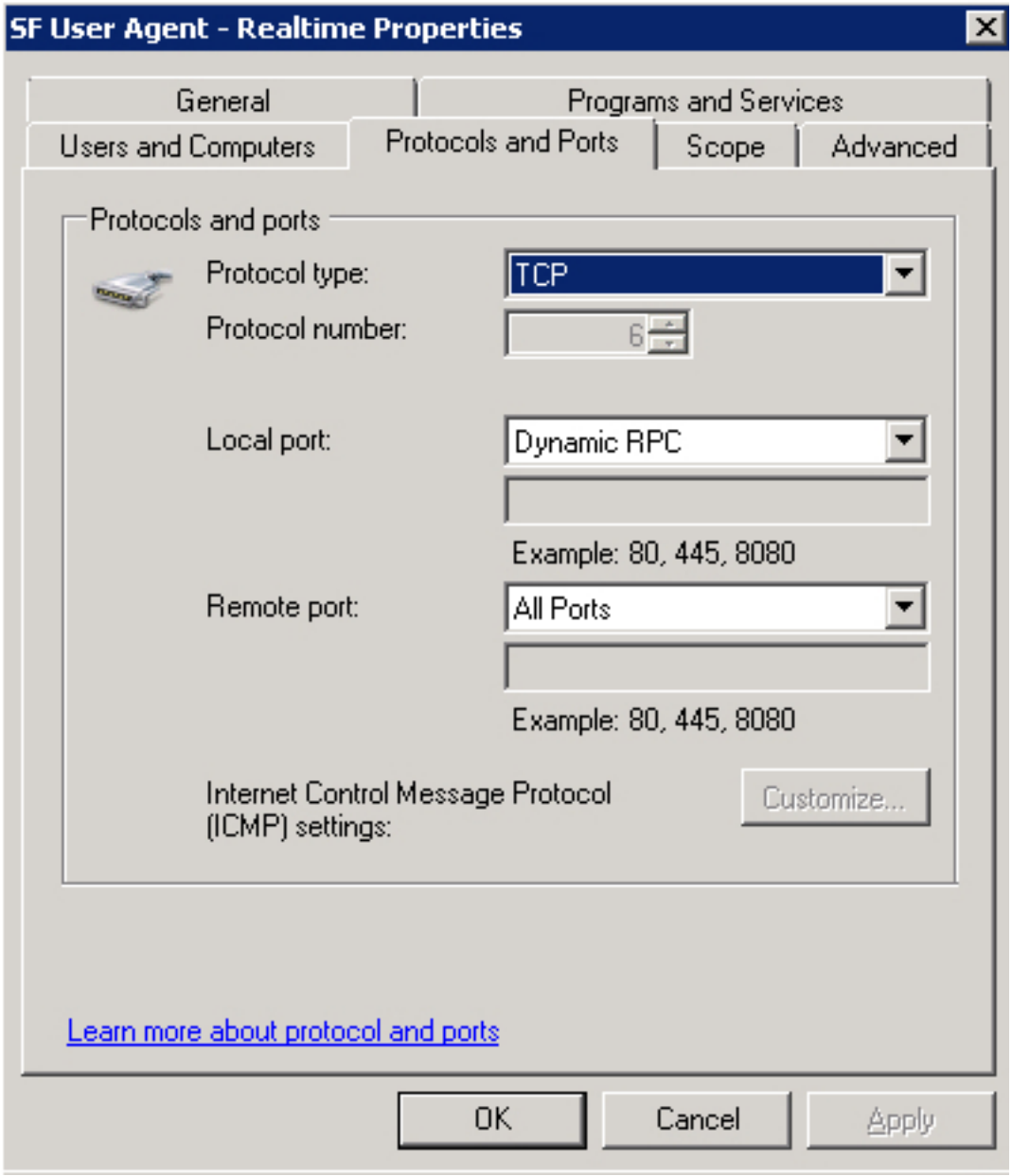
创建在使用**Windows防火墙的**被瞄准的域控制器的一个入站防火墙规则**以高级安全**控制台，允许必要的连接从用户代理发生。设置示例和步骤如下显示：

1. 在**常规选项卡**，请命名规则并且选择**允许连接**。

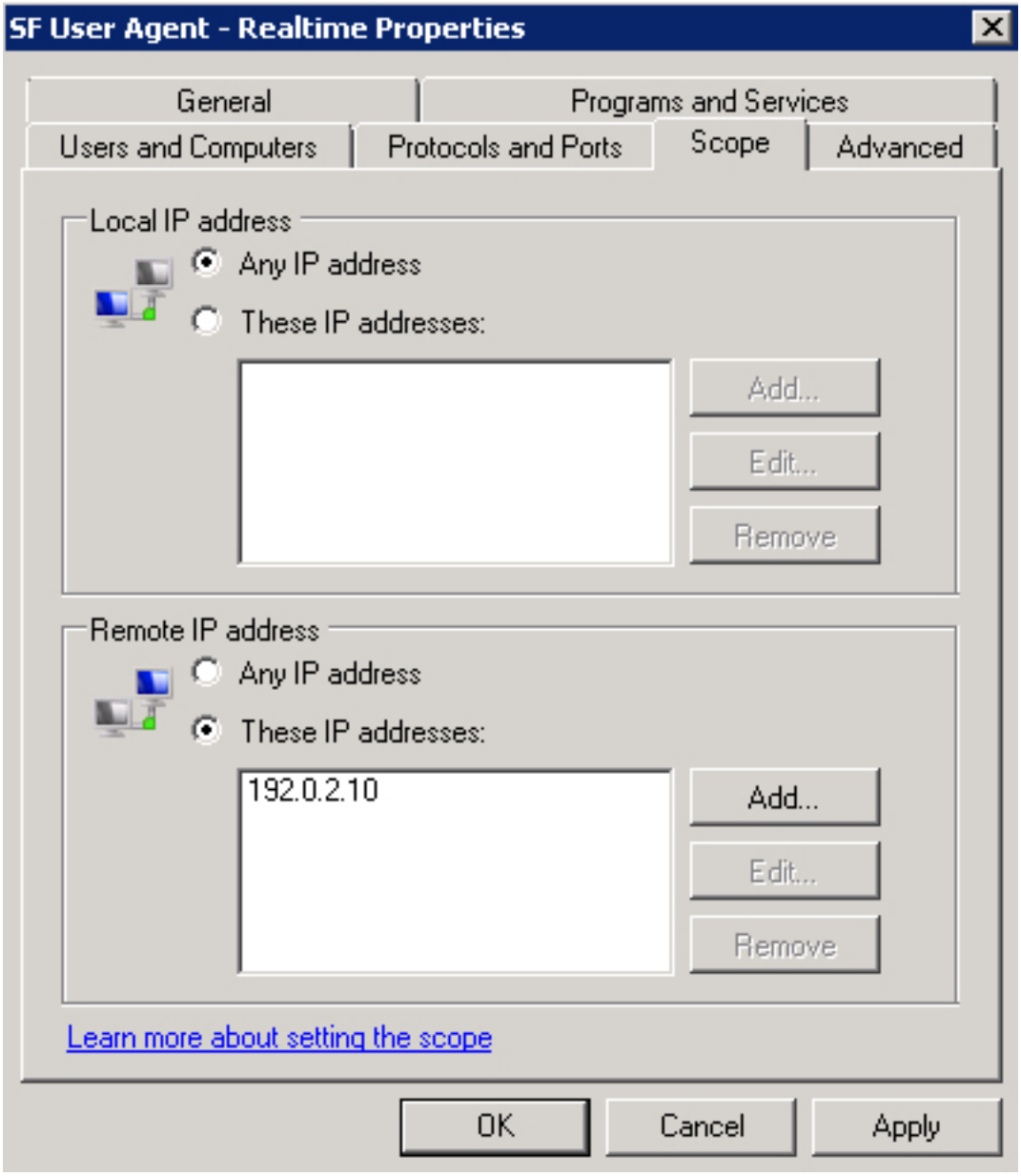


2. 在**协议和端口上请**选中，选择以下项目：

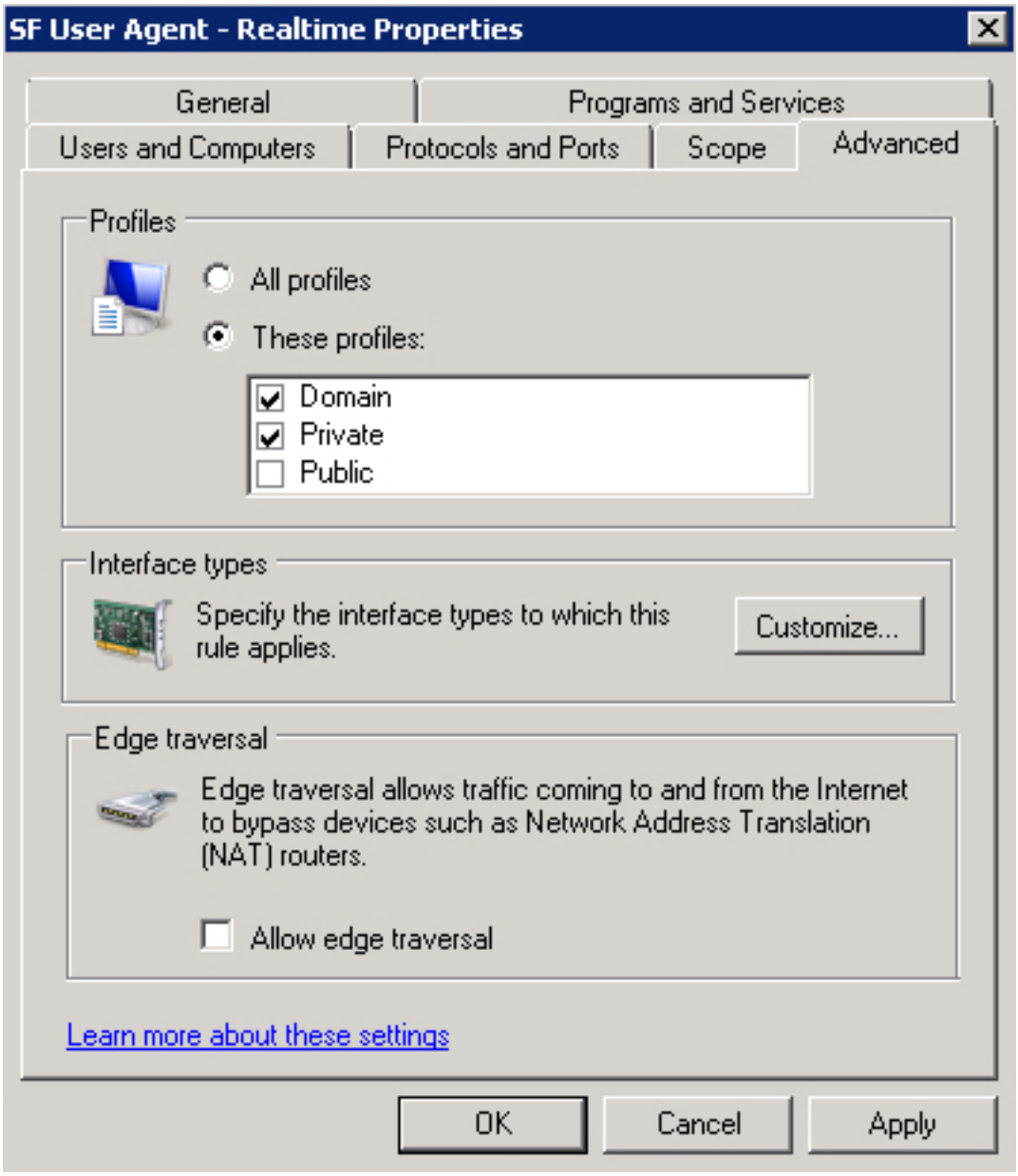
- **协议类型**：TCP
- **本地端口**：动态RPC
- **远程端口**：所有端口



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



4. 在**高级选项卡。**，挑选适当的**配置文件。**



保存防火墙规则，启用它并且重新启动Sourcefire用户代理服务。 您的实时连接状态应该从**未知**当前变成**联机**。