O estado do tempo real do agente de usuário é mostrado como o desconhecido

Índice

Introdução

Após ter distribuído um agente de usuário de Sourcefire, você pode observar que o estado do tempo real permanece desconhecido após ter seguido todas as etapas de configuração. Este documento fornece a instrução em como mudar o estado de **desconhecido a disponível**.

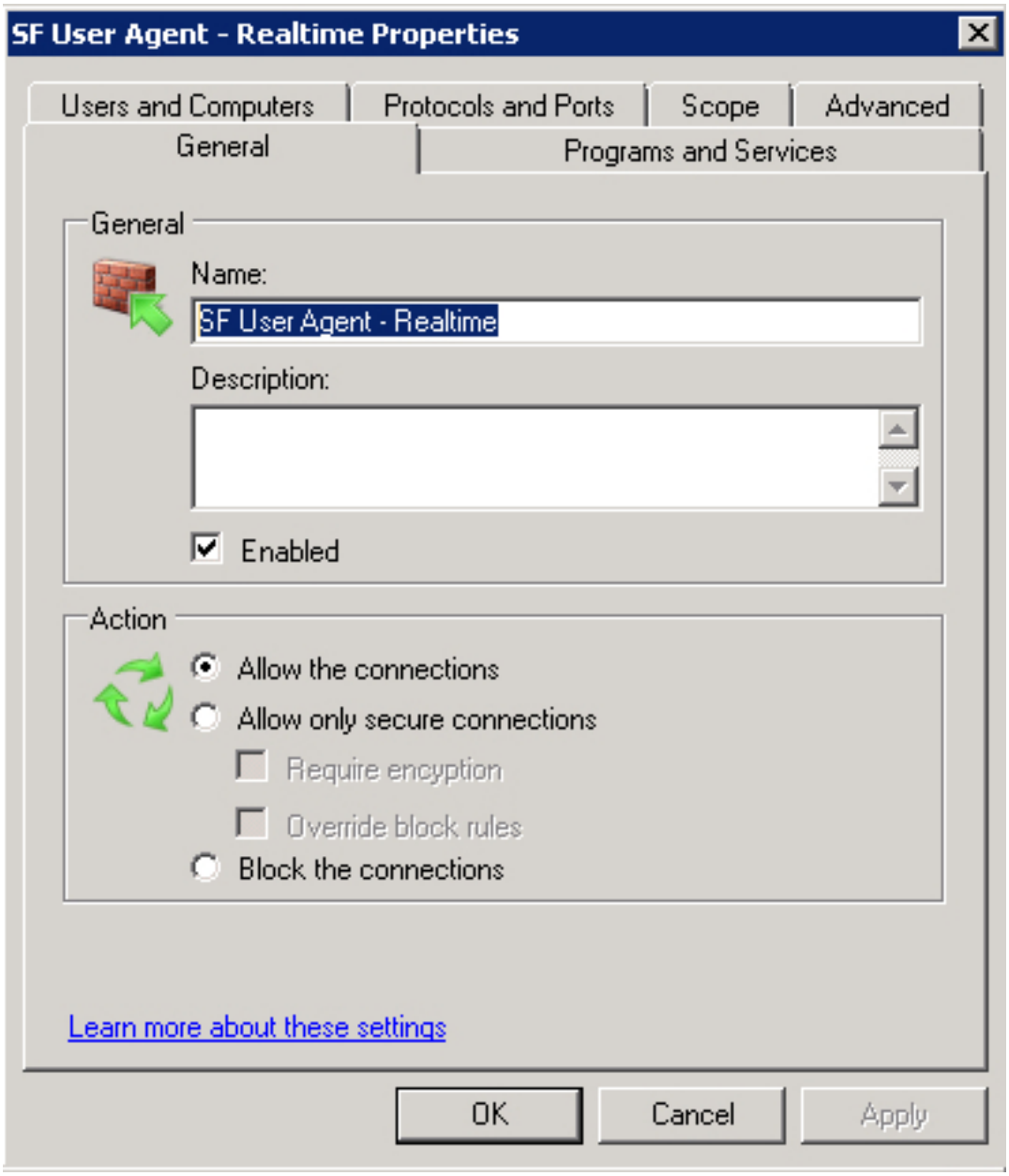
Sintoma

As configurações de firewall do controlador de domínio impedem que as conexões RPC exigidas estejam estabelecidas. O agente de usuário usa conexões da porta dinâmica RPC para anexar ao controlador de domínio e para estabelecer o monitoramento em tempo real.

Solução

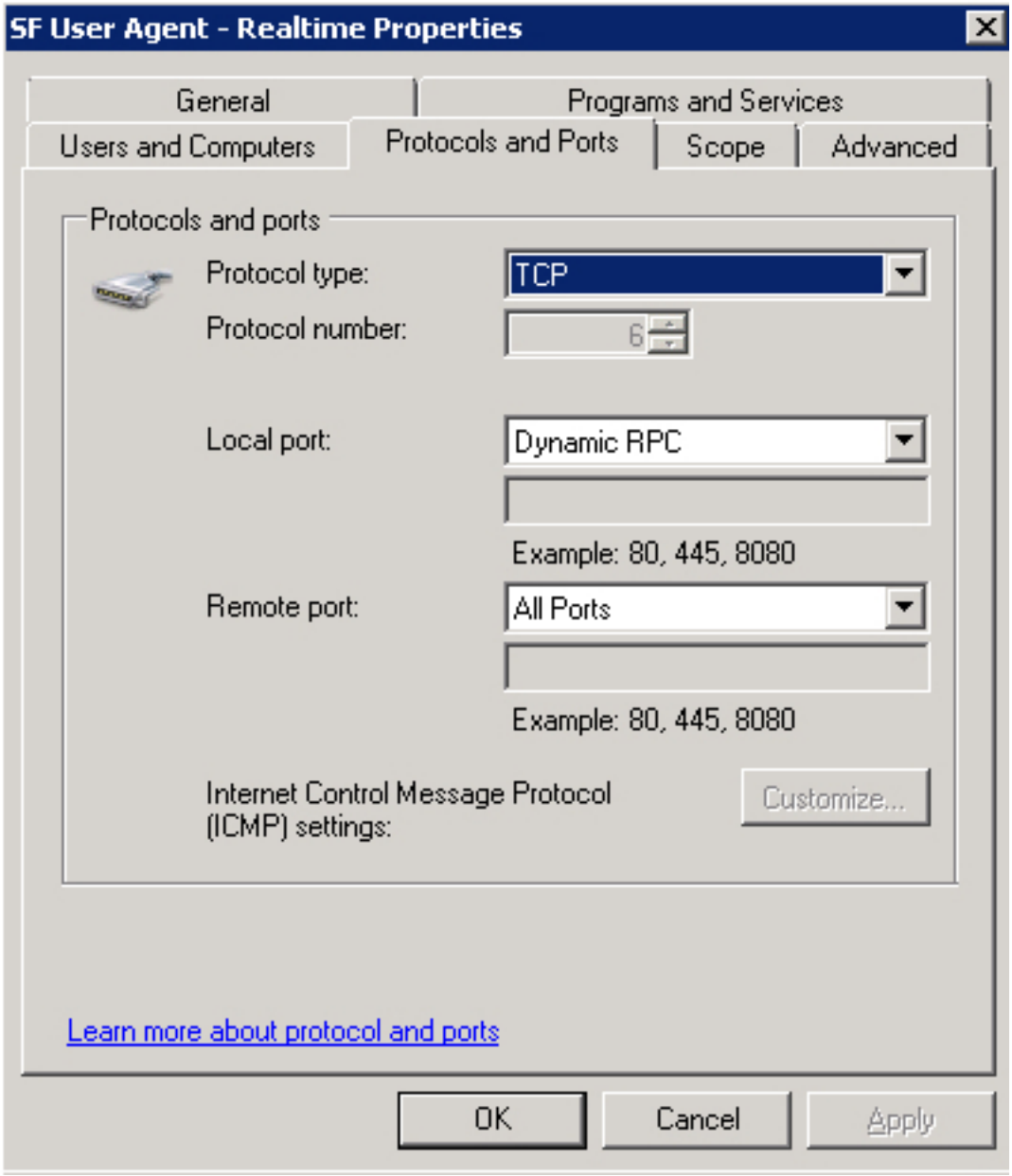
Crie uma regra de entrada do Firewall no controlador de domínio visado usando o **Windows Firewall com o** console da **segurança avançada**, permitindo que a conexão necessária do agente de usuário ocorra. Um exemplo dos ajustes e as etapas são mostrados abaixo:

1. **No tab geral**, nomeie a regra e seleto **permita as conexões**.

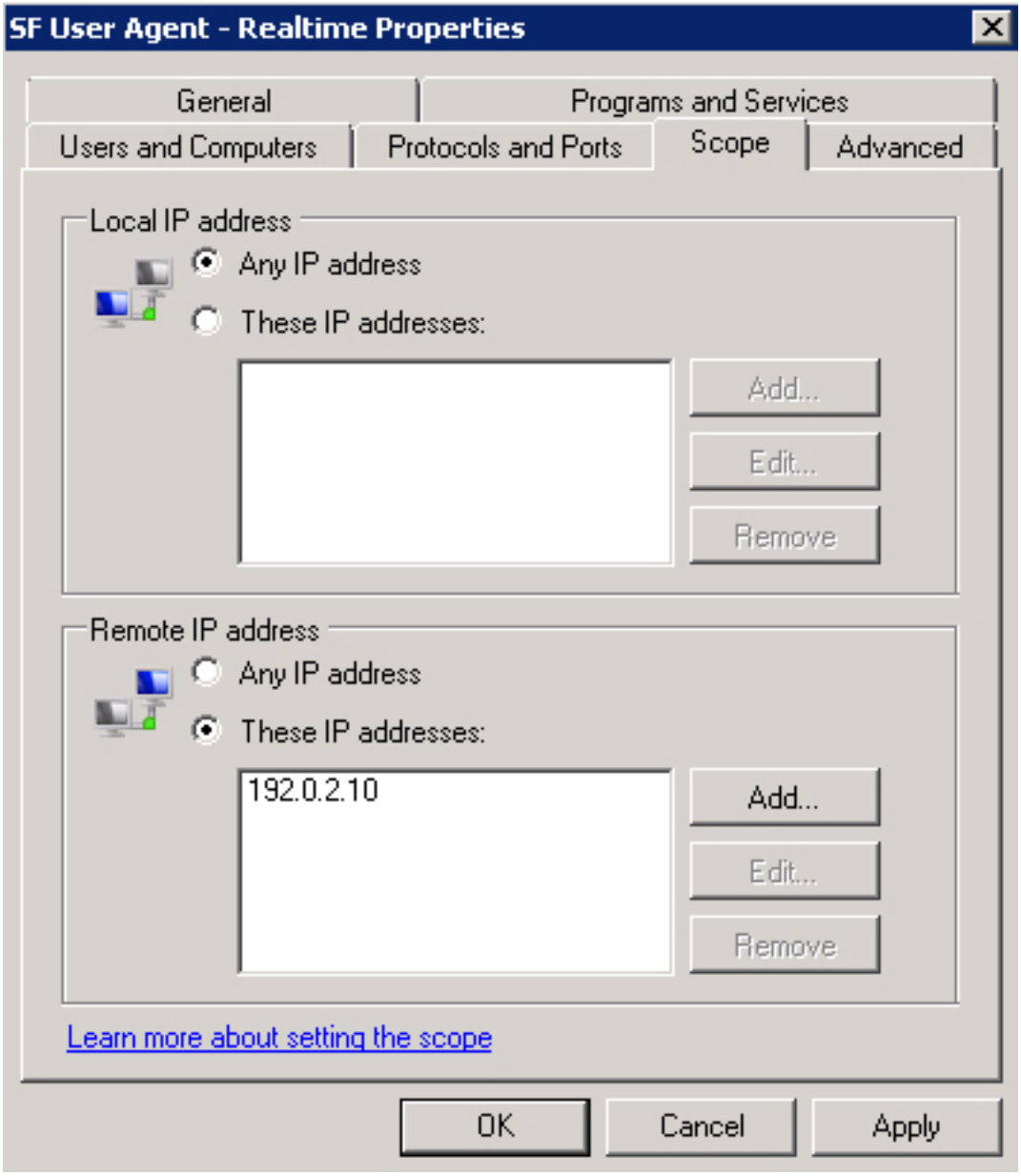


2. **Nos protocolos e nas portas** catalogue, selecione os itens seguintes:

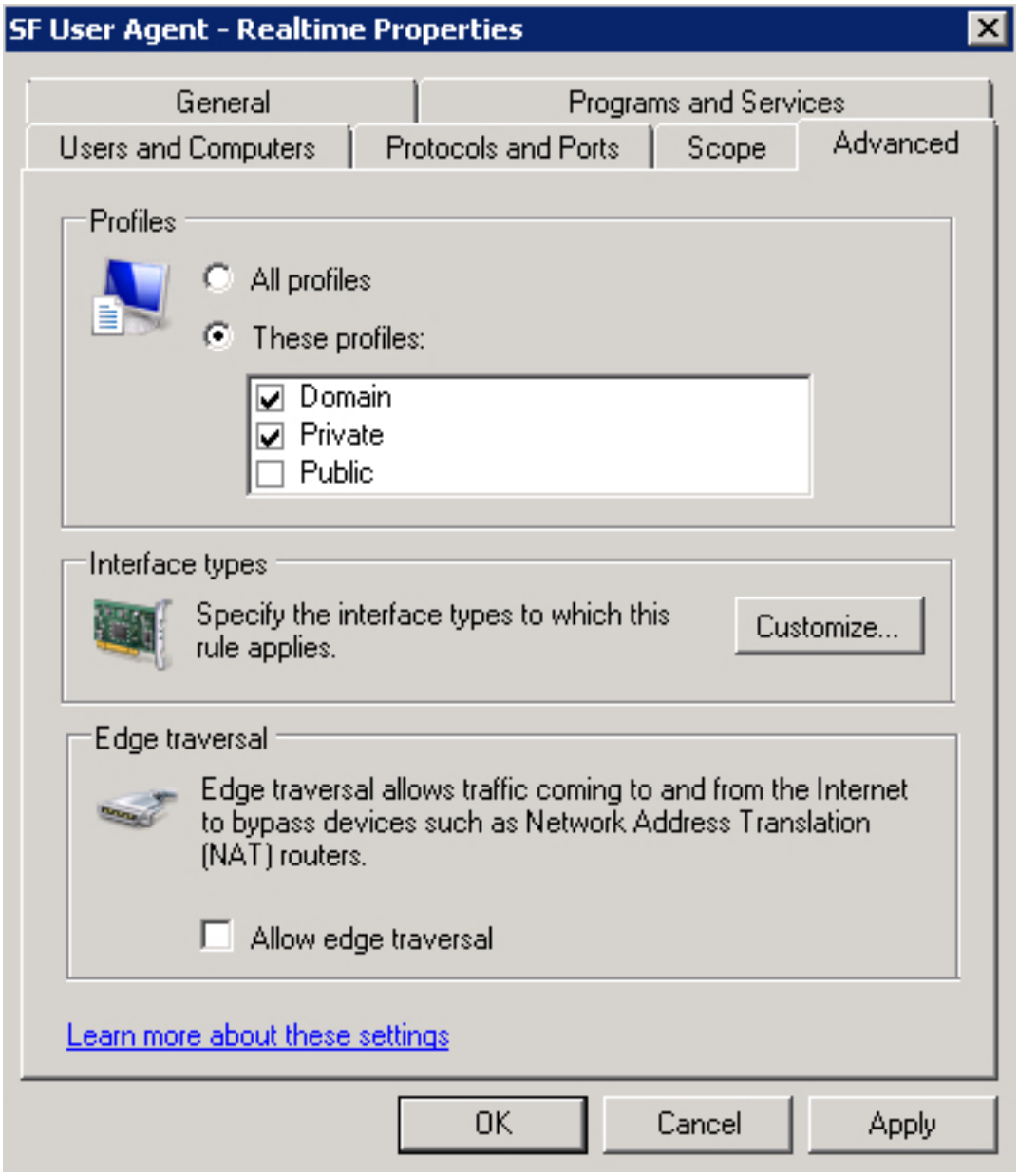
- **Tipo de protocolo**: TCP
- **Porta local**: RPC dinâmico
- **Porta remota**: Todas as portas



3. Na aba do **espaço**, adicionar o **endereço IP remoto**. O clique **adiciona** para incorporar o endereço IP de Um ou Mais Servidores Cisco ICM NT do host do agente de usuário.



4. **No guia avançada**, selecione **perfis** apropriados.



Salvar a regra do Firewall, permita-a e reinicie-o o serviço do agente de usuário de Sourcefire. Seu estado da conexão em tempo real deve agora mudar de **desconhecido a disponível**.