Cisco QuickVPN Installation Tips for Windows Operating Systems

For a video showing installation tips on Quick VPN, visit http://youtu.be/hHu2z6A78N8

Objective

Cisco QuickVPN is a free software designed for remote access to a network. It is easy to install on a PC and simple to manage. QuickVPN is compatible with Windows operating system (both the 32-bit and 64 bit editions). In order for QuickVPN to work properly, a set of requirements must be checked off to ensure the VPN connectivity with the network.

This article explains the requirements and tips to properly run QuickVPN, as well as an explanation of how QuickVPN gains access to your network.

Applicable Devices

- RV215W
- RV110W
- RV180 / RV180W
- RV120W
- RV220W
- RV016
- RV042 / RV042G
- RV082
- RVS4000
- SA520 / SA520W
- SA540
- WRV200
- WRV210
- WRVS4400N
- Windows XP, Windows Vista, Windows 7

QuickVPN Process

The following is an explanation of how QuickVPN acts in your computer and why it is important to meet the requirements before attempting to run QuickVPN.

1. The client connects to the router using SSL (Secure Socket Layer). The connection uses port number 443 or 60443 (depending on your VPN configuration on the router) and looks for a certificate. For more information refer to the section *Router Requirements*.

Note: If you use a certificate, make sure it is saved in your computer. Otherwise, click **No** to not use a certificate when the certificate warning message appears.

2. The client username and password is authenticated by the router. Once the user is authenticated, the IPSec tunnel is then established.

Note: If you are unable to log in to the VPN, you will receive an error message.

3. The client sends an ICMP Echo Request packet to the internal IP address of the router. The router replies back with an ICMP Echo Reply packet. The purpose is to establish connectivity between both ends. This is why you need to make sure (depending on your Operating System) to set the proper requirements for ICMP. For more information refer to the section, *Windows Vista / Windows 7 Operating System Requirements*.

Note: If connection fails, you will get a Remote Gateway Not Responding error message.

Router Requirements

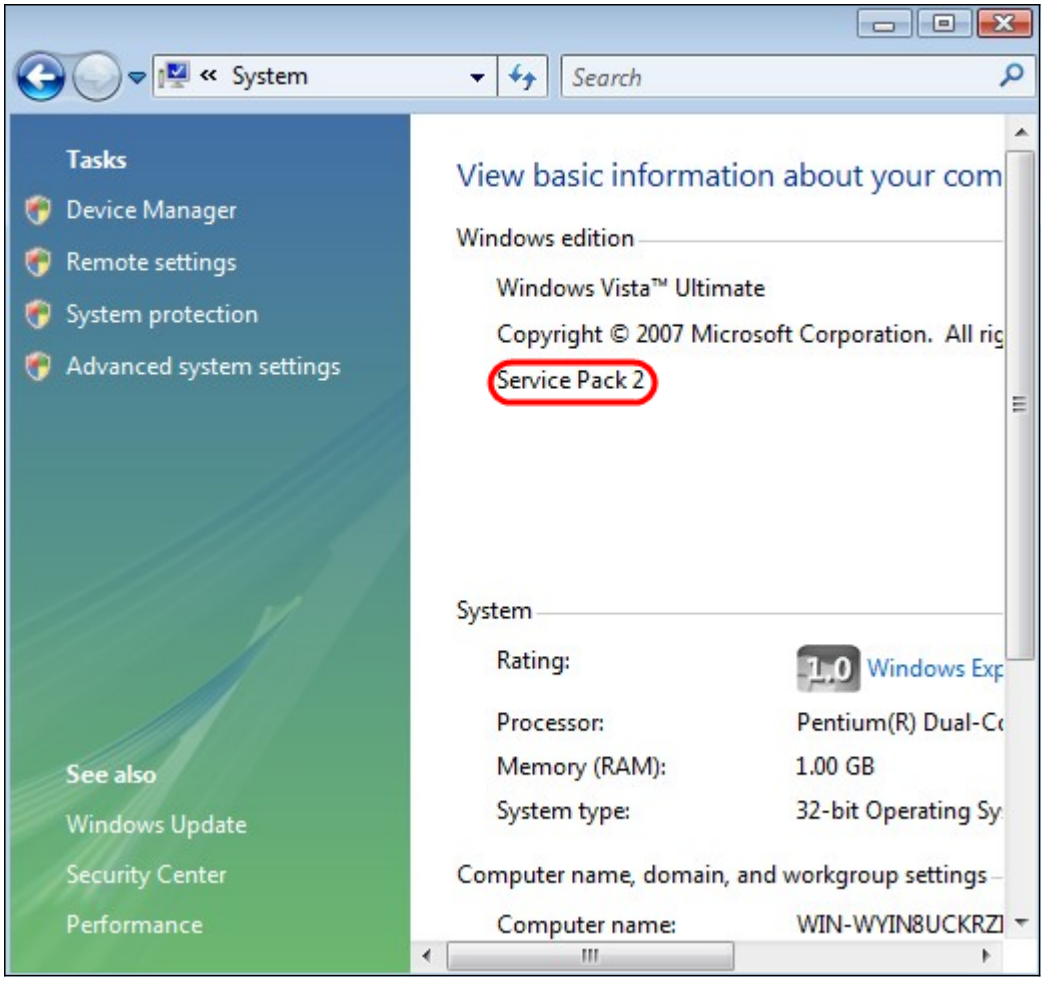
Below is a list of requirements your small business router must meet.

- Remote Management must be enabled for ports 443 and 60443.
- Users must create and enable the VPN tunnel.
- Username and password are both case sensitive and must match in both ends of the connection.
- Only one connection per user account is permitted.
- Local network subnet must be different from the remote network subnet.
- If you are using a certificate, the certificate file needs to be saved in your computer in the QuickVPN Client folder.

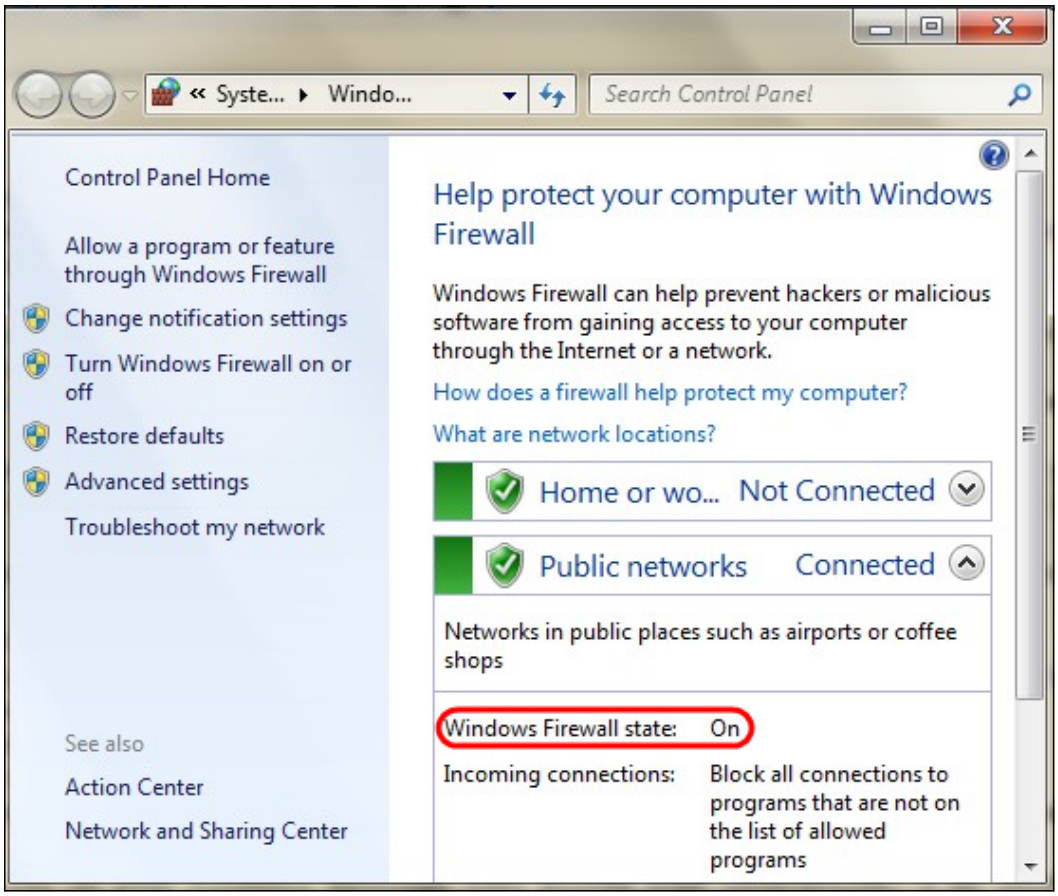
Windows Vista / Windows 7 Operating System Requirements

Step 1. If your computer has Windows Vista, then you must have Service pack 2 or Vista Service Pack 2 compatibility for Windows 7 installed. To check this, choose **Start > Computer System Properties**. If your computer has Windows 7, then skip this step.

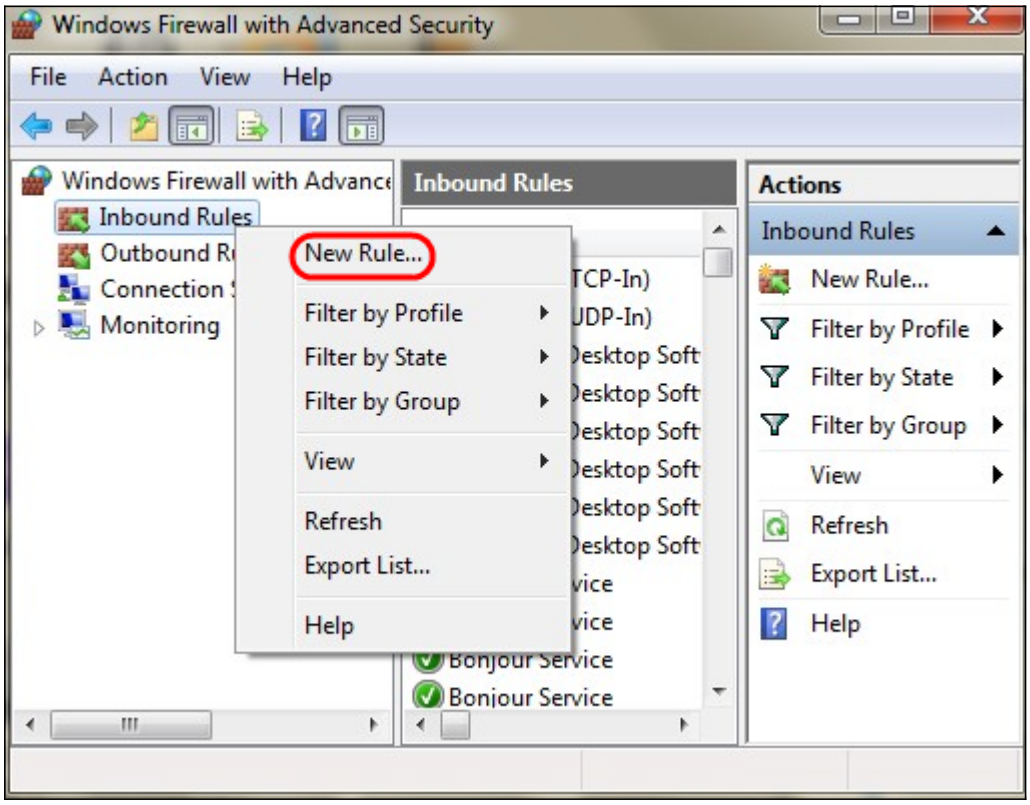
Note: For Windows Vista, if you do not have the Service Pack installed, choose **Start > All Programs > Windows Update** to update your system.



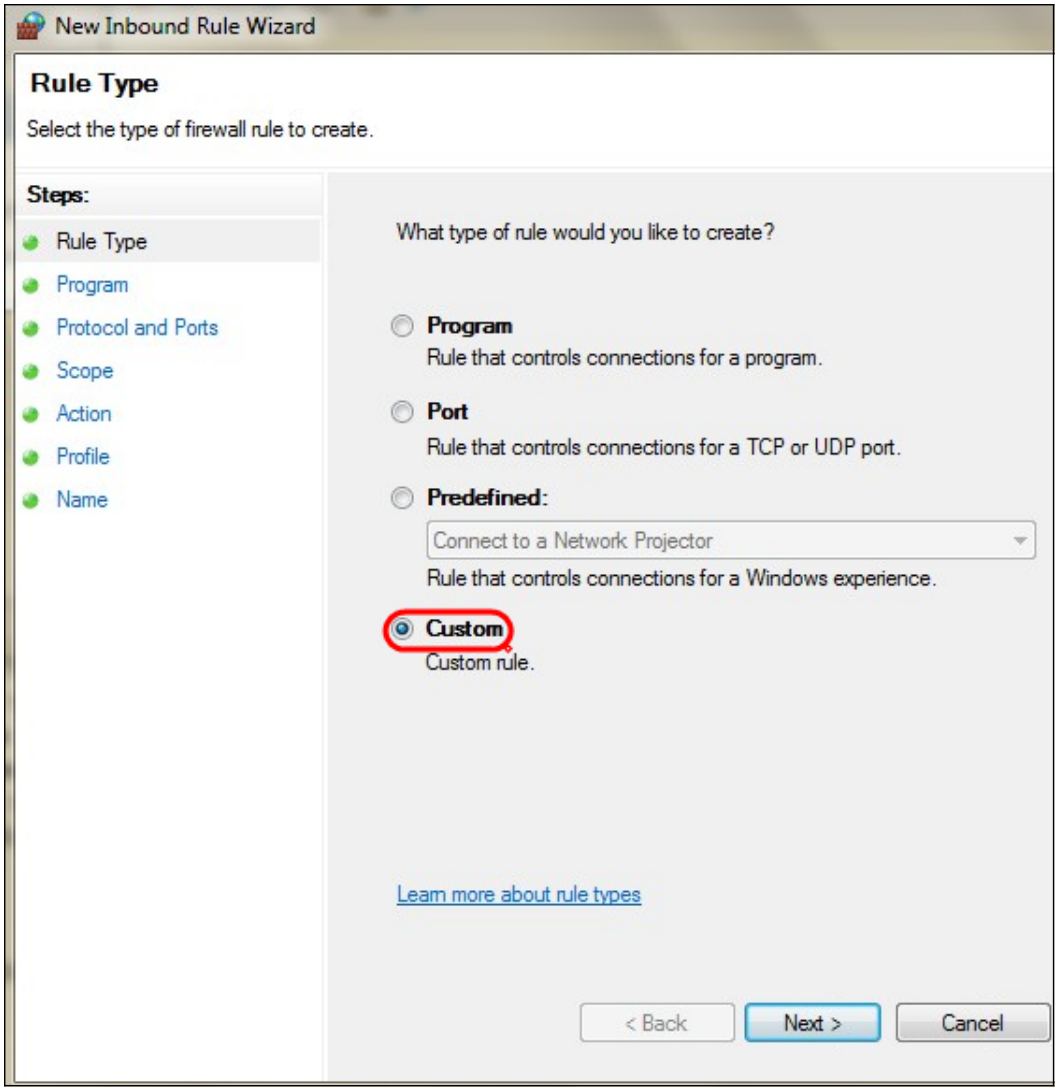
Step 2. Your Windows Firewall must be turned on. To check this, choose **Start > Control Panel > System and Security > Windows Firewall**.



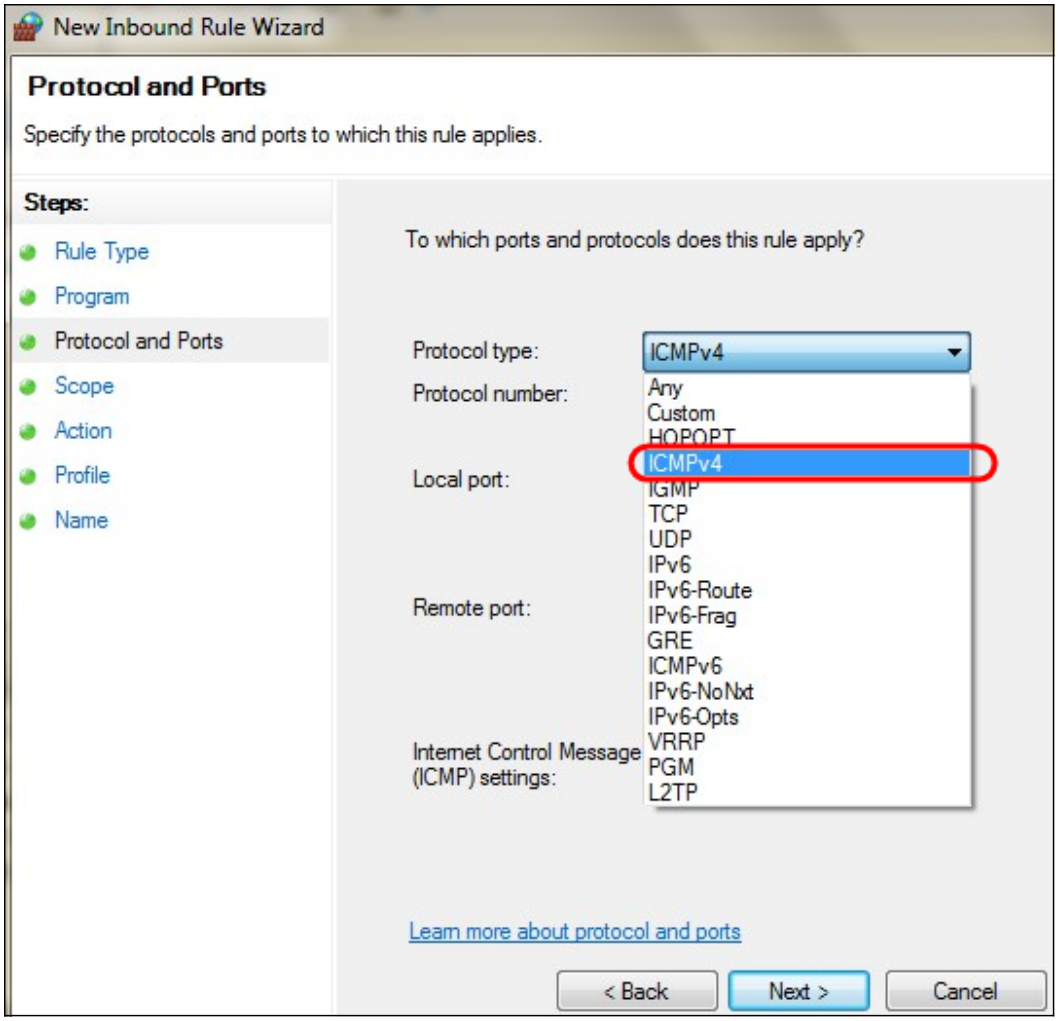
Step 3. A rule must be created to allow ICMP (Internet Control Message Protocol) packets transmissions. To do this, choose **Start > Control Panel > System and Security > Windows Firewall > Advanced Settings**. The *Windows Firewall with Advanced Security* window opens:



Step 4. Right-click on **Inbound Rules** and choose **New Rule**. The *New Inbound Rule Wizard* page opens:

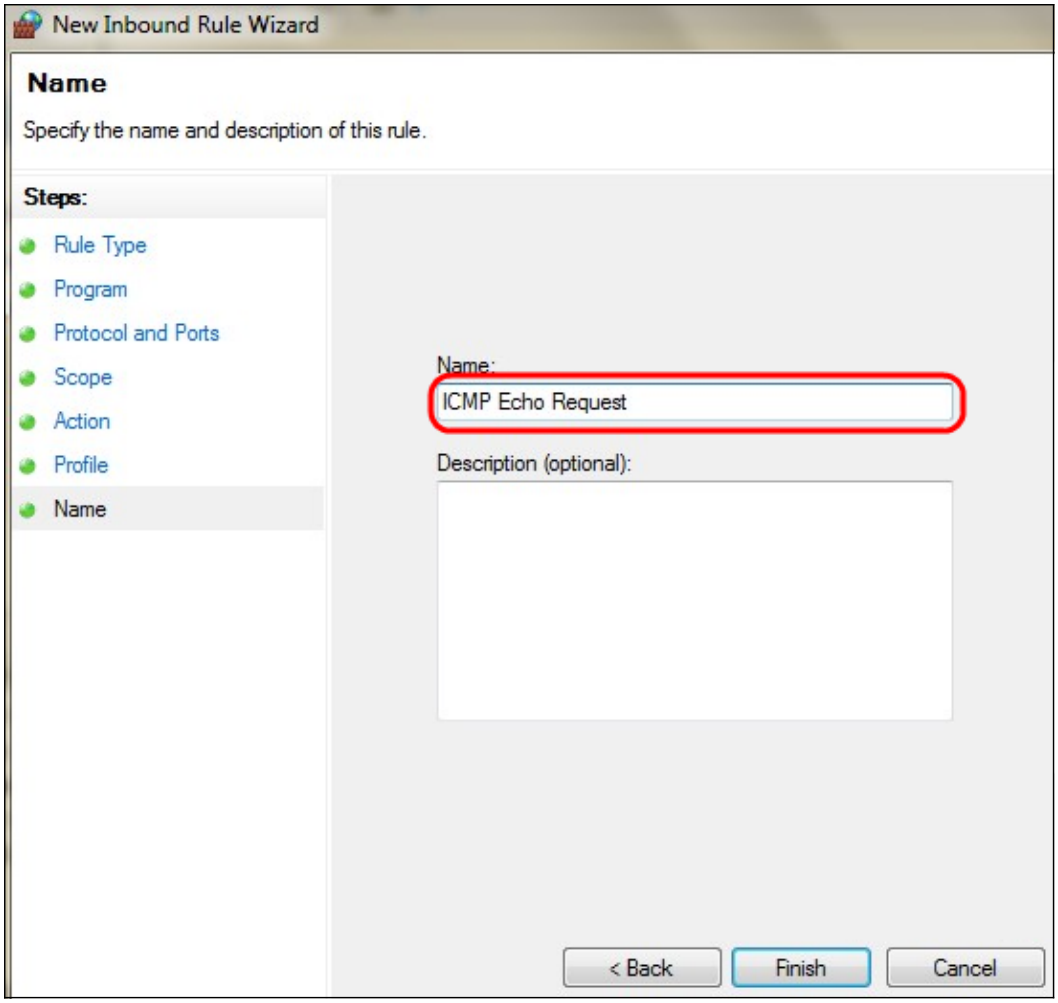


Step 5. Click **Custom** to create a custom rule.



Step 6. In the Protocol Type drop-down list, choose **ICMPv4**.

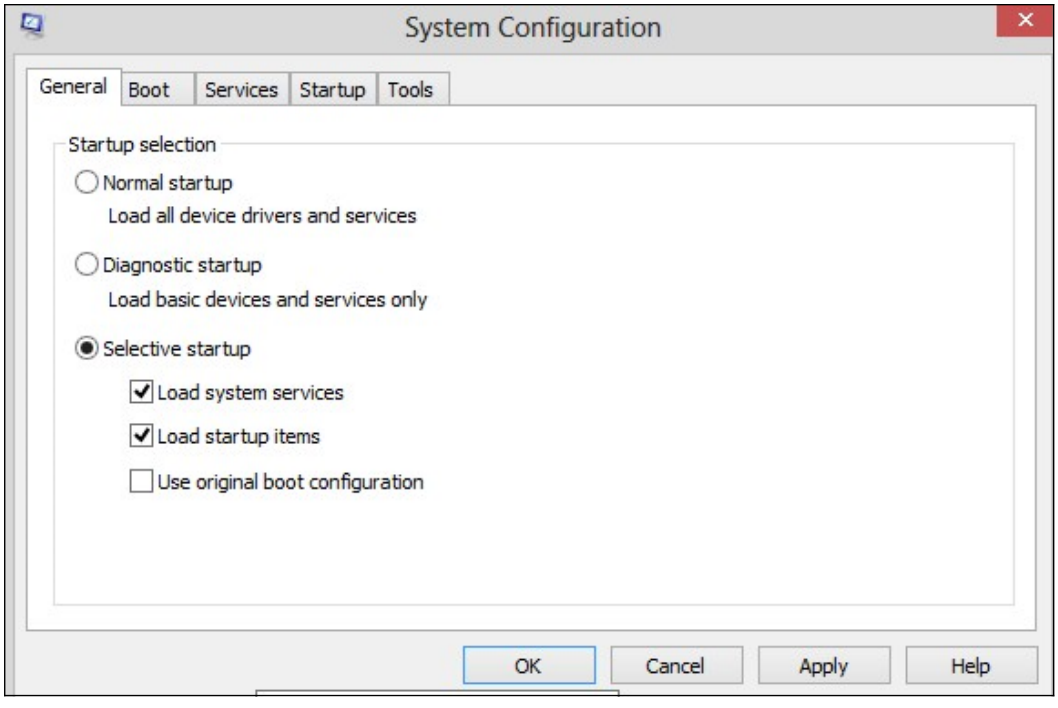
Note: The other fields can remain as default configuration.



Step 7. In the Name field, enter a name that describes this rule.

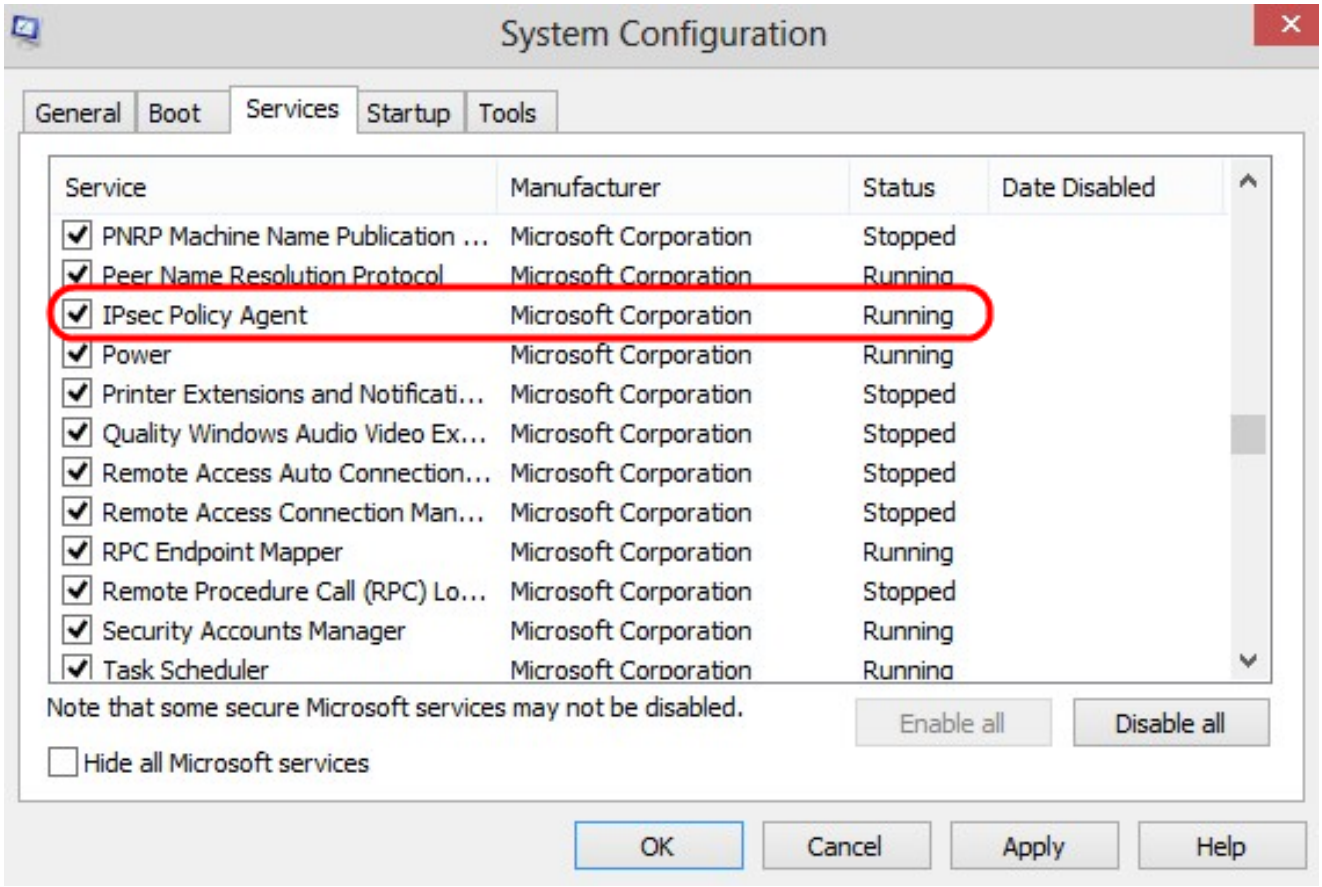
Step 8. Click **Finish**.

Step 9. You must have IPSec service running. To check this, click **Start** and in the Search Programs and Files field, enter **msconfig**. The *System Configuration* window opens:



Step 10. Click **Services** tab to ensure the IPSec Policy Agent is enabled. If it is not enabled,

check the **IPSec Policy Agent** check box to allow IPSec service.



Step 11. Click **Apply** to save the settings.