Configuring Firewall Settings For Configuration Manager 2012 R2

Prajwal Desai

In this post we will look at the steps for configuring firewall settings for configuration manager 2012 R2. System Center 2012 R2 Configuration Manager is a distributed client/server system. The distributed nature of Configuration Manager means that connections can be established between site servers, site systems, and clients. Some connections use ports that are not configurable, and some support custom ports you specify. You must verify that the required ports are available if you use any port filtering technology such as firewalls, routers, proxy servers, and IPsec. To know more about ports used by configuration manager 2012 R2 click here.

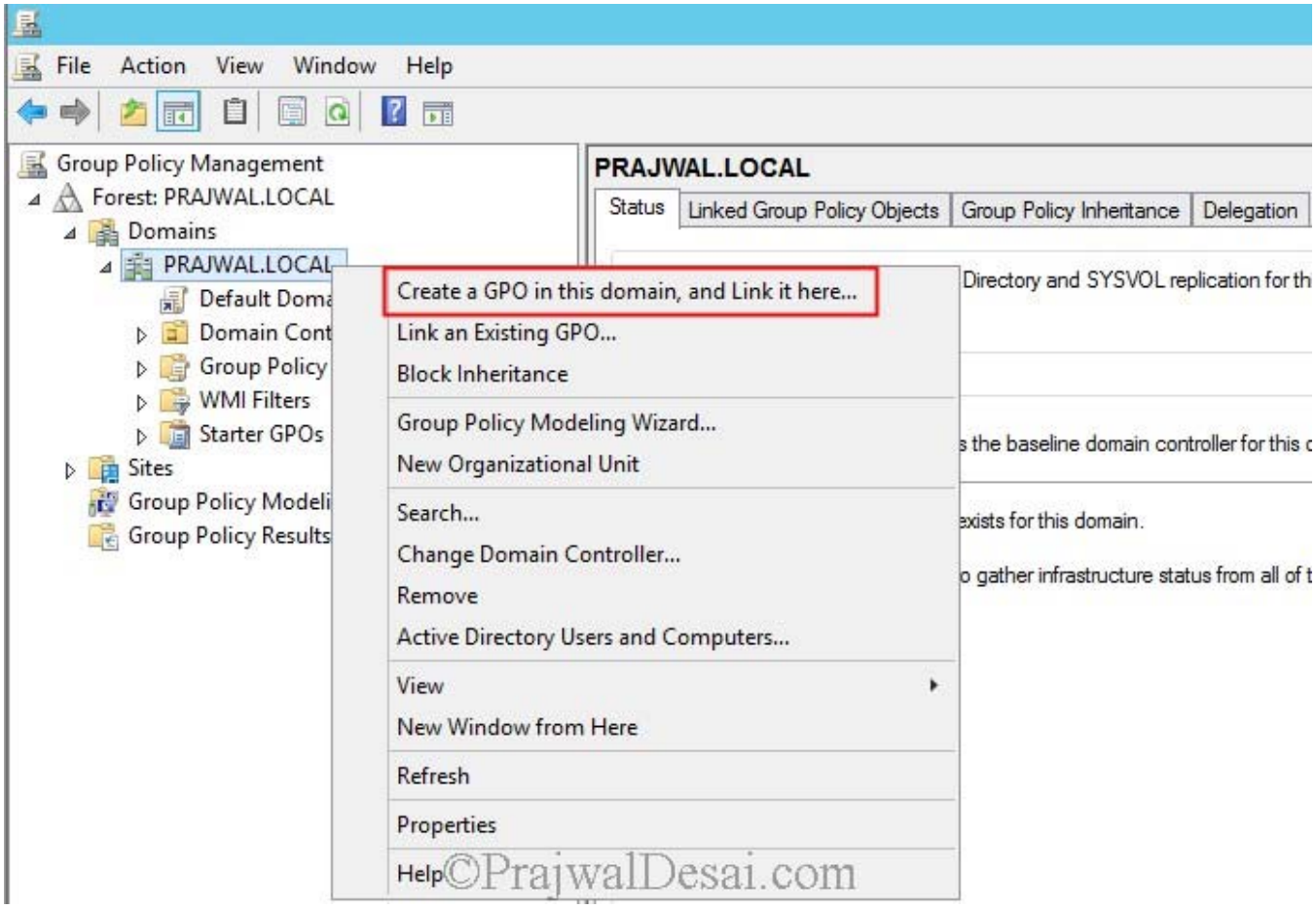
Note

In order to successfully use client push to install the Configuration Manager 2012 R2 client, you must add the following as exceptions to the Windows Firewall. If there is a firewall between the site system servers and the client computer, confirm whether the firewall permits traffic for the ports that are required for the client installation.

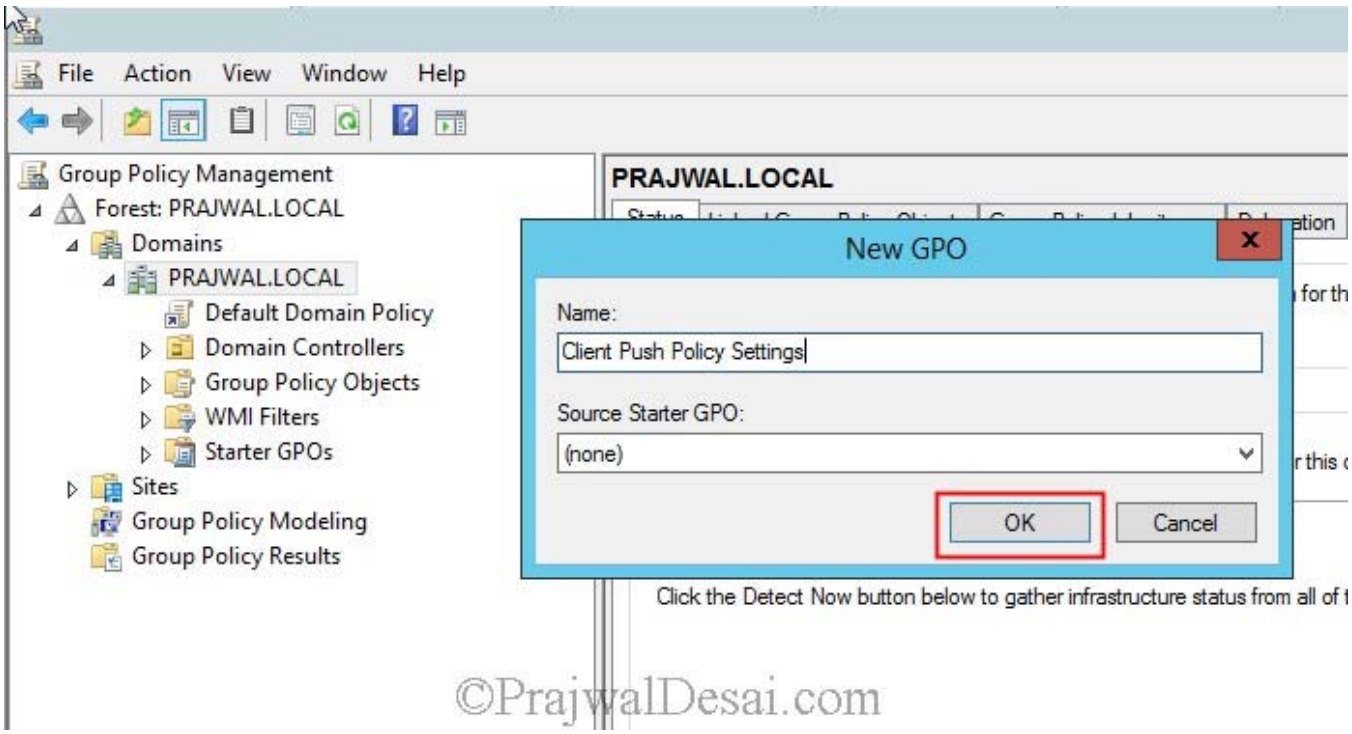
1) **File and Printer Sharing**

2) **Windows Management Instrumentation (WMI)**

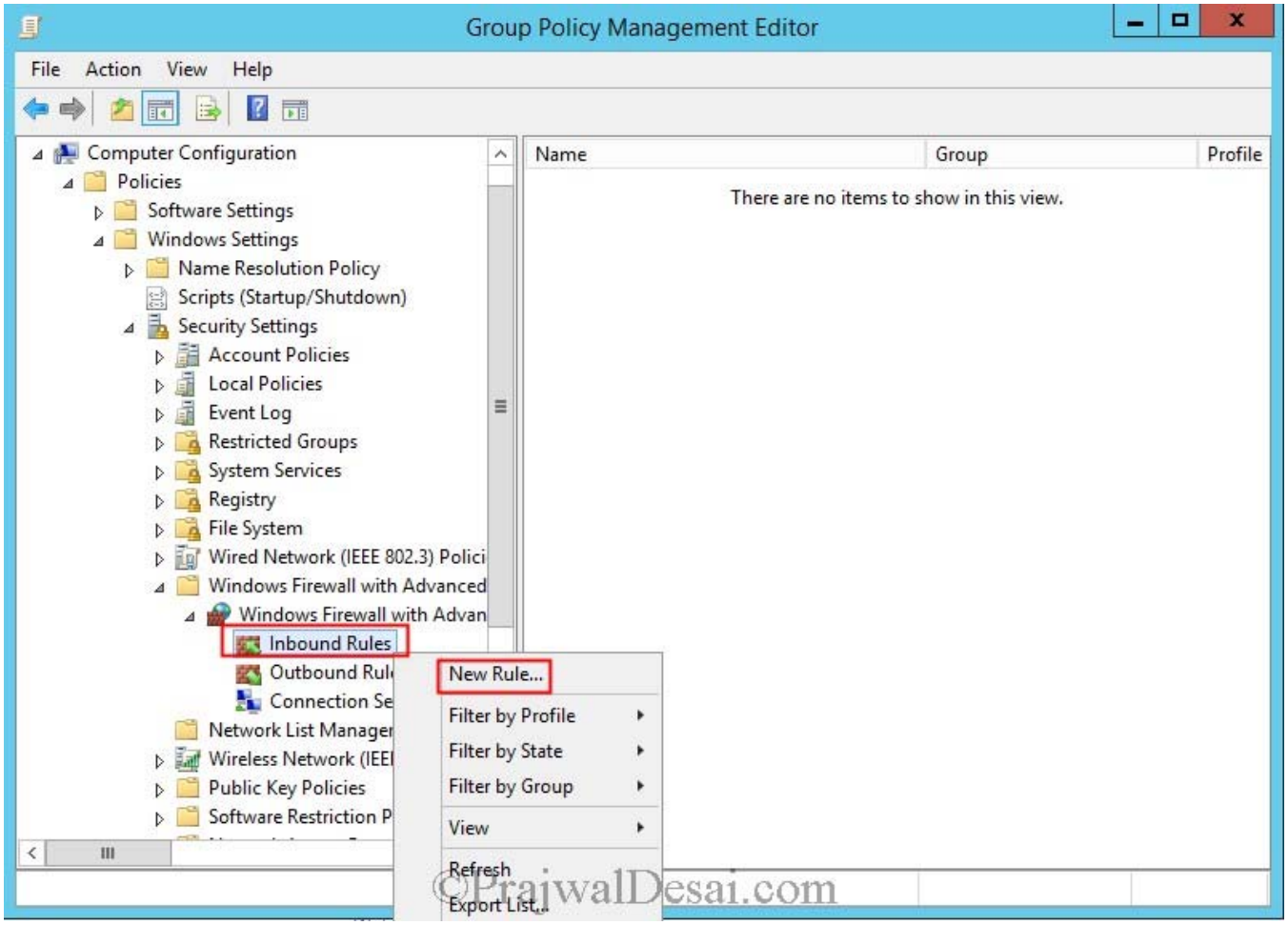
We will create an **inbound** and **outbound** rule, add **File and Printer sharing service** as exception to firewall and an **Inbound rule** to allow WMI. We will perform this activity on the Domain Controller. Click on **Server Manager**, click on **Tools**, open **Group policy management console**. Right Click on the domain and Create a **GPO**.



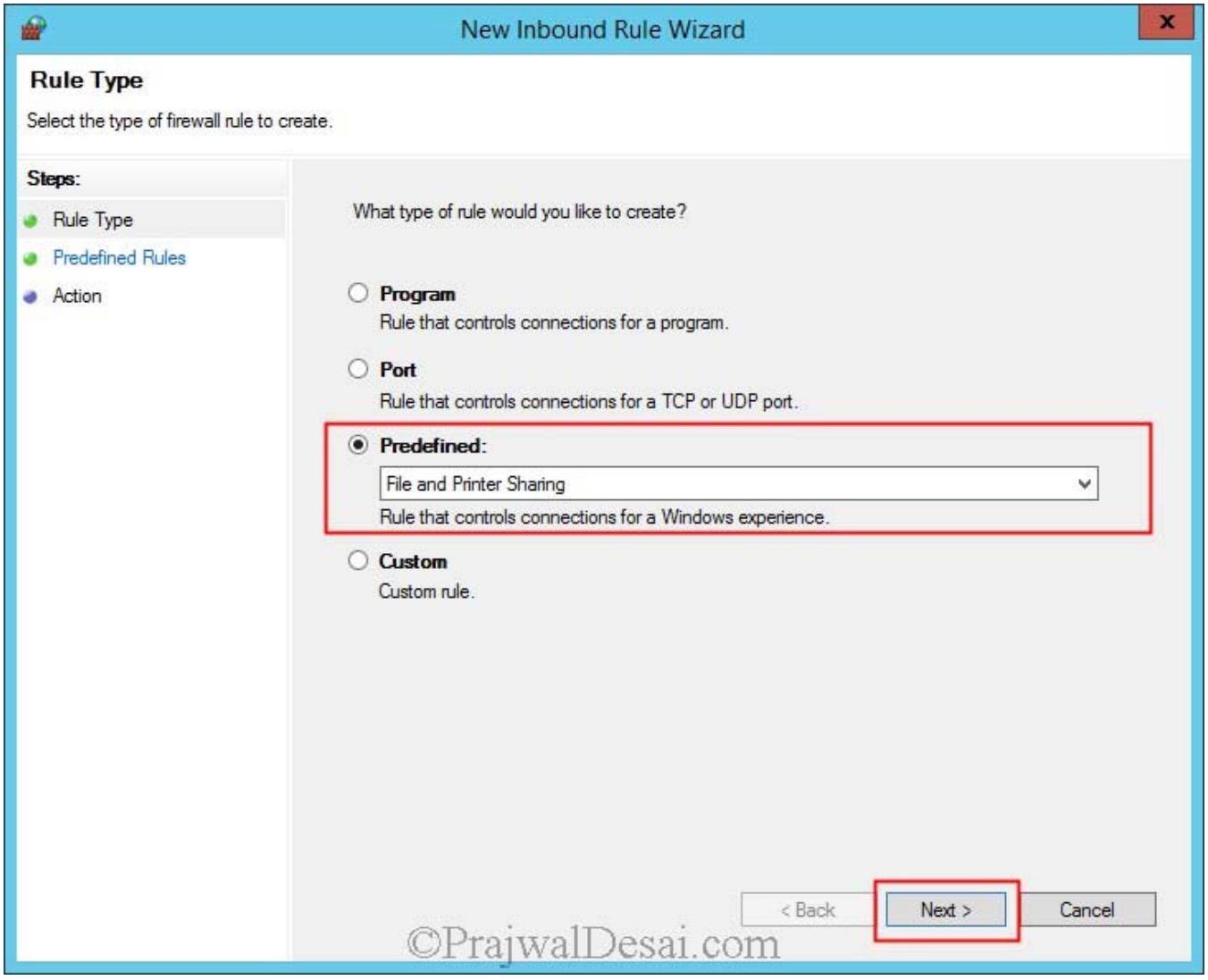
Provide a name to the GPO and click on **OK**.



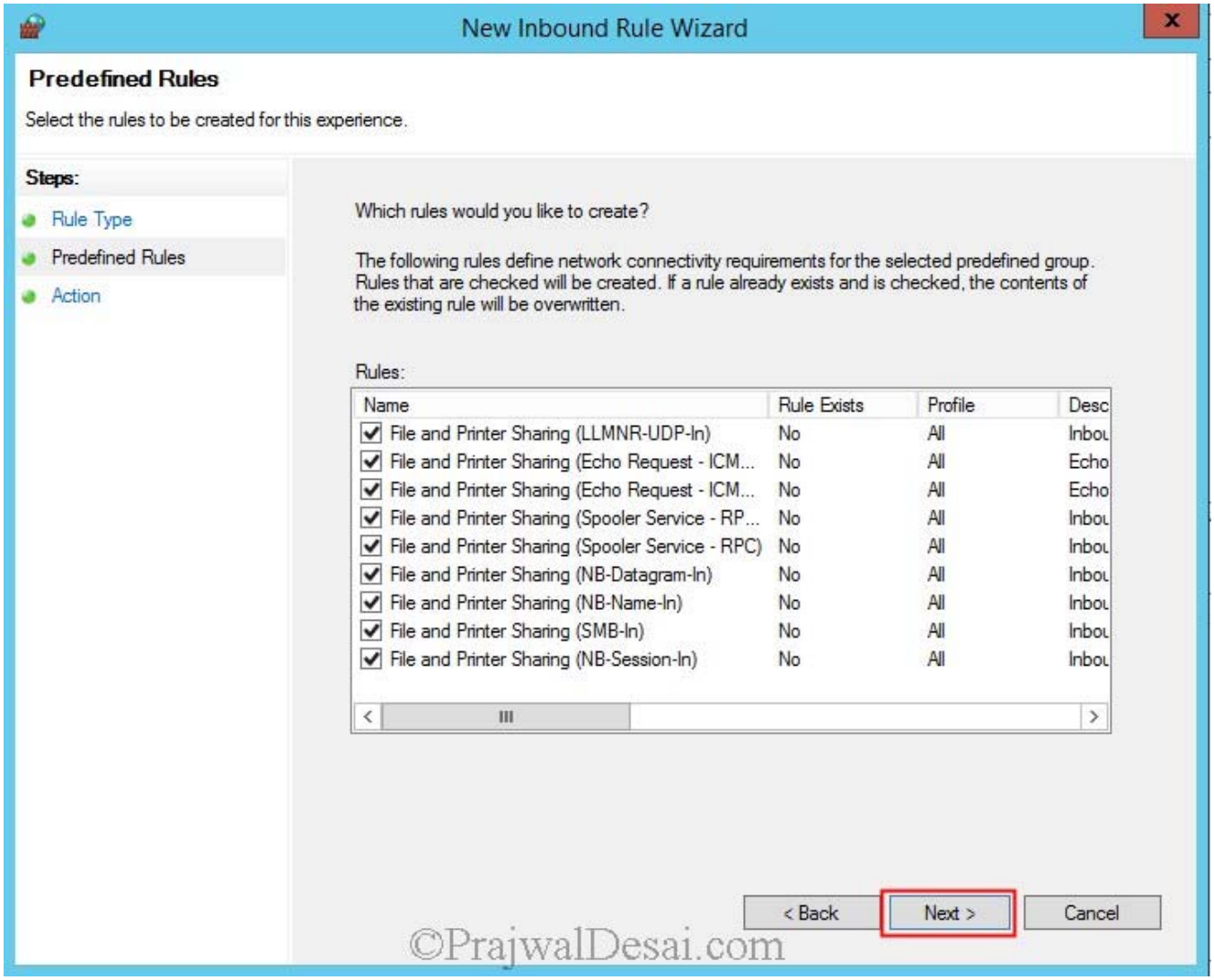
Right click on the policy that you created and click on **Edit. Expand computer configuration, Windows settings, Security settings, Windows Firewall with advanced security.** Right click **on Inbound rules and click on New Rule…**



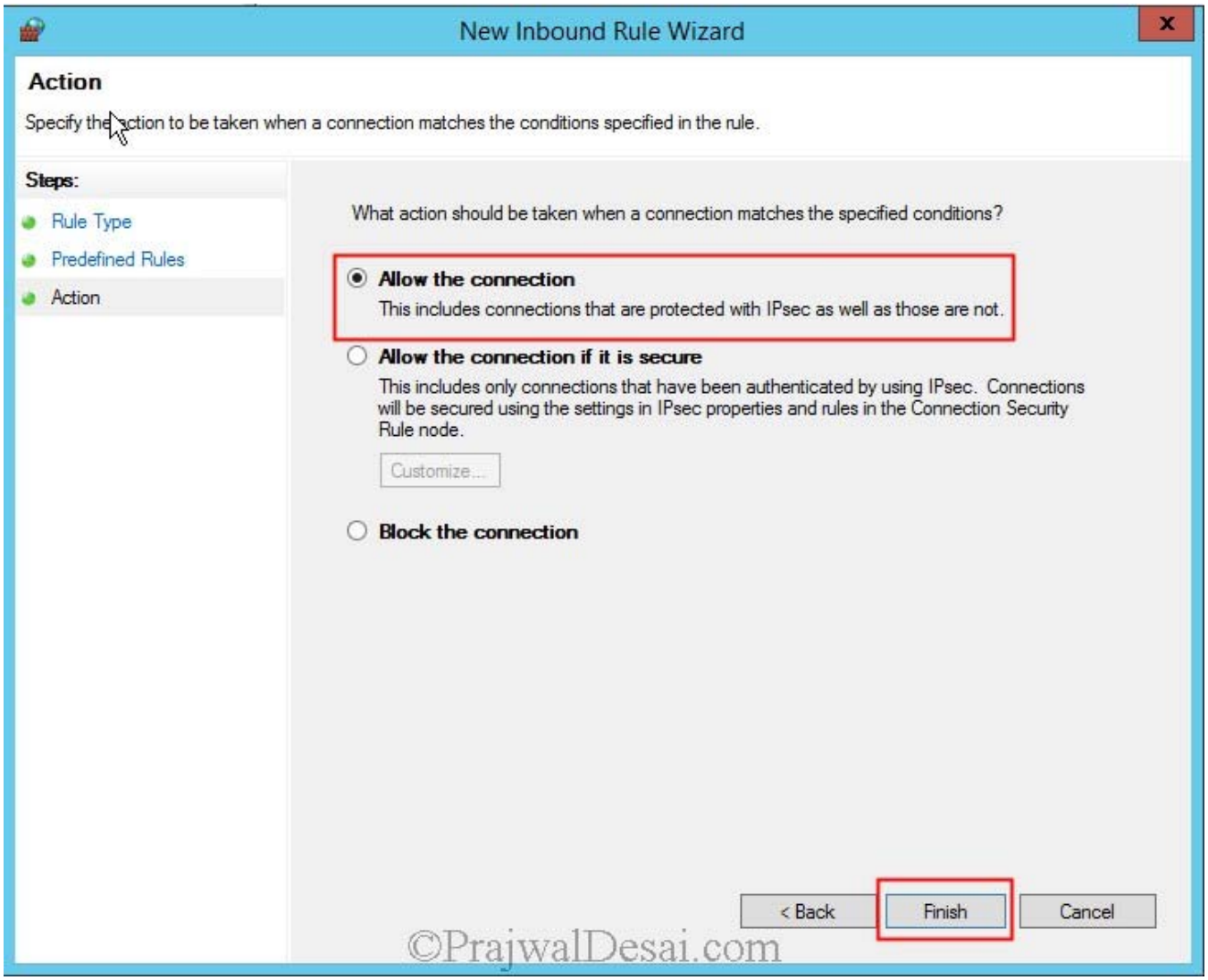
Click on **Predefined** and select **File and Printer Sharing.** Click on **Next**.



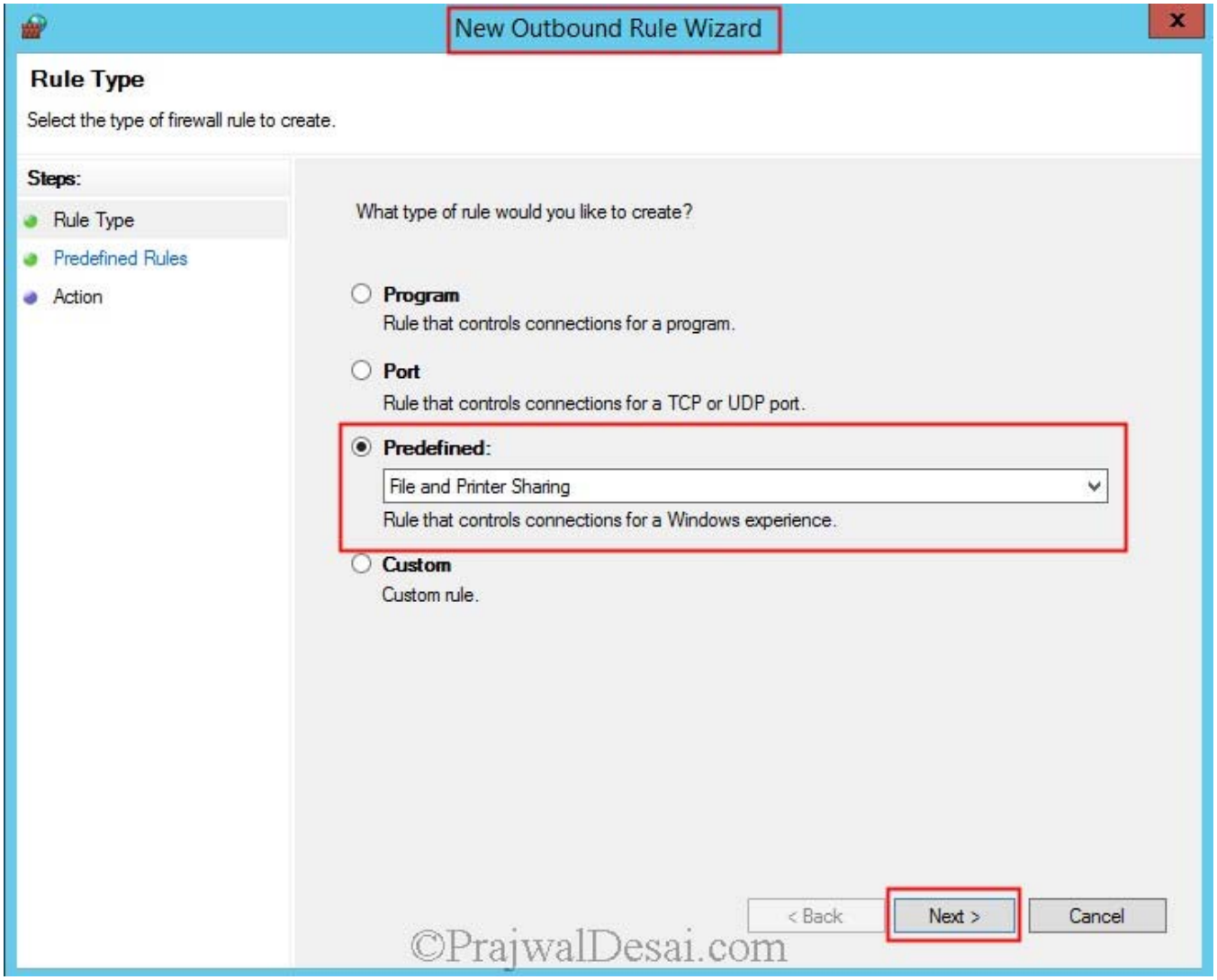
Don’t change anything here, click on **Next**.



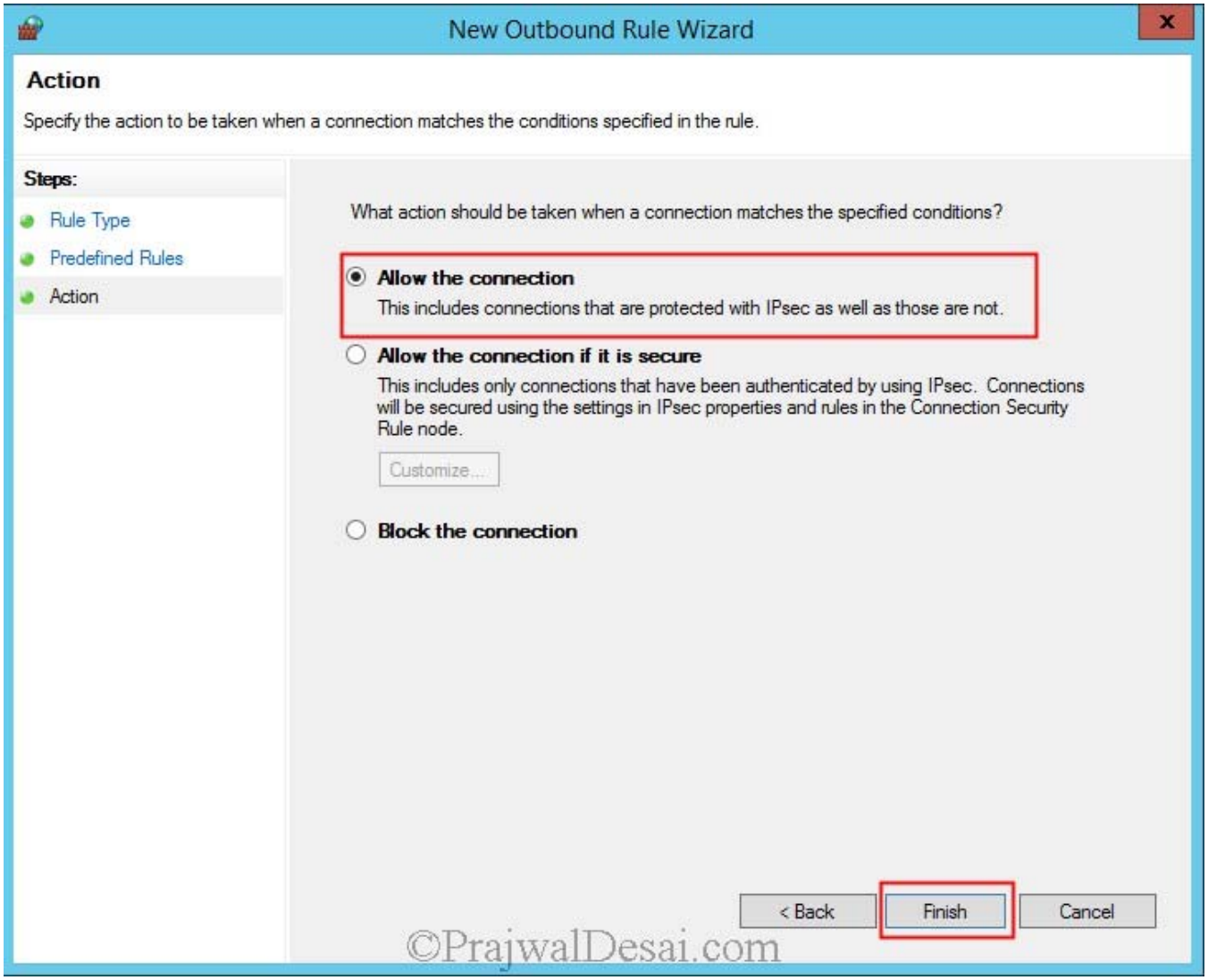
Click on **Allow the connection**. Click **Finish**.



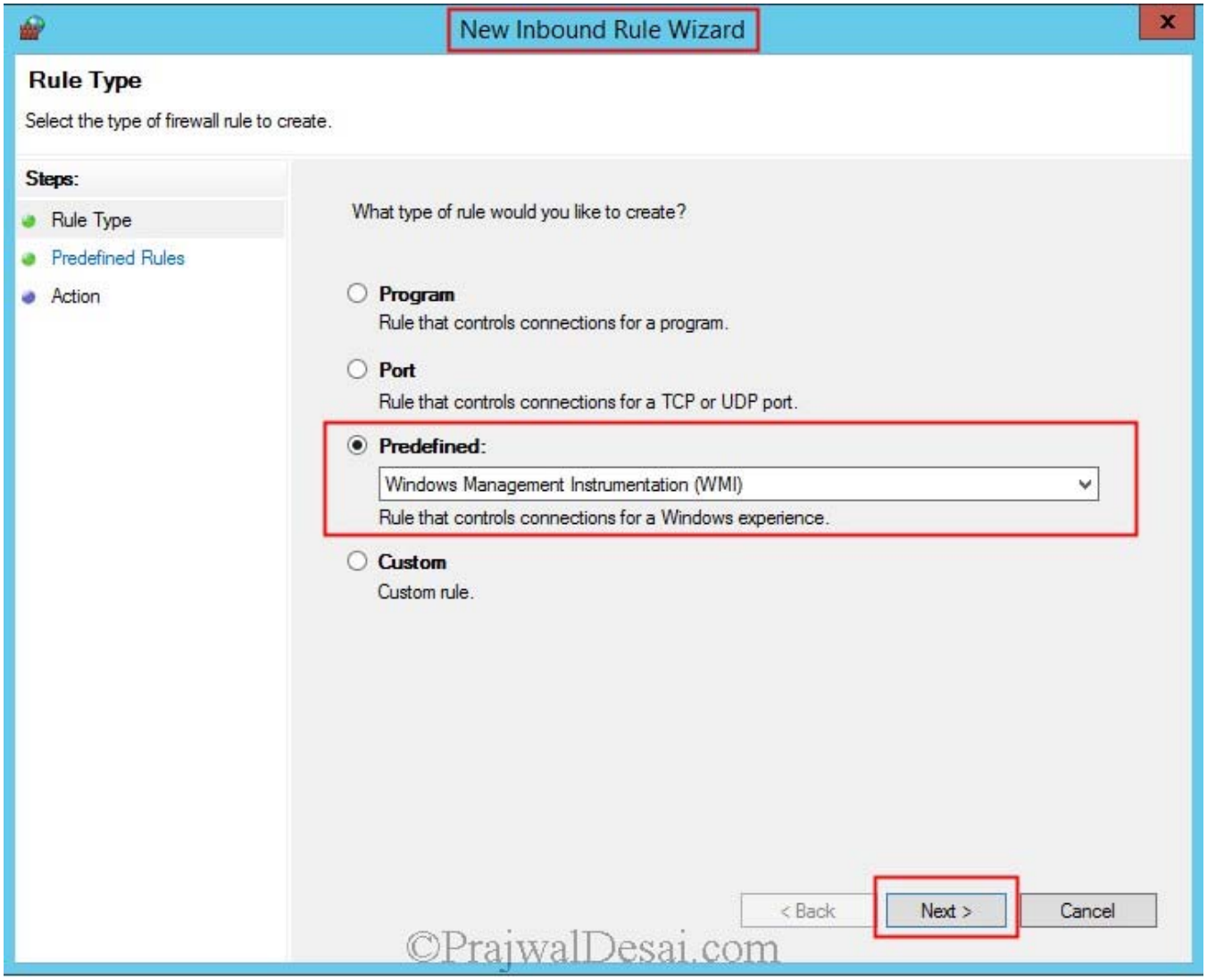
Now we will create an outbound rule to allow **File and Printer sharing**. Right click on the **Outbound Rule** and click on **New Rule**. Choose **Predefined** and select **File and Printer Sharing**. Click on **Next**.



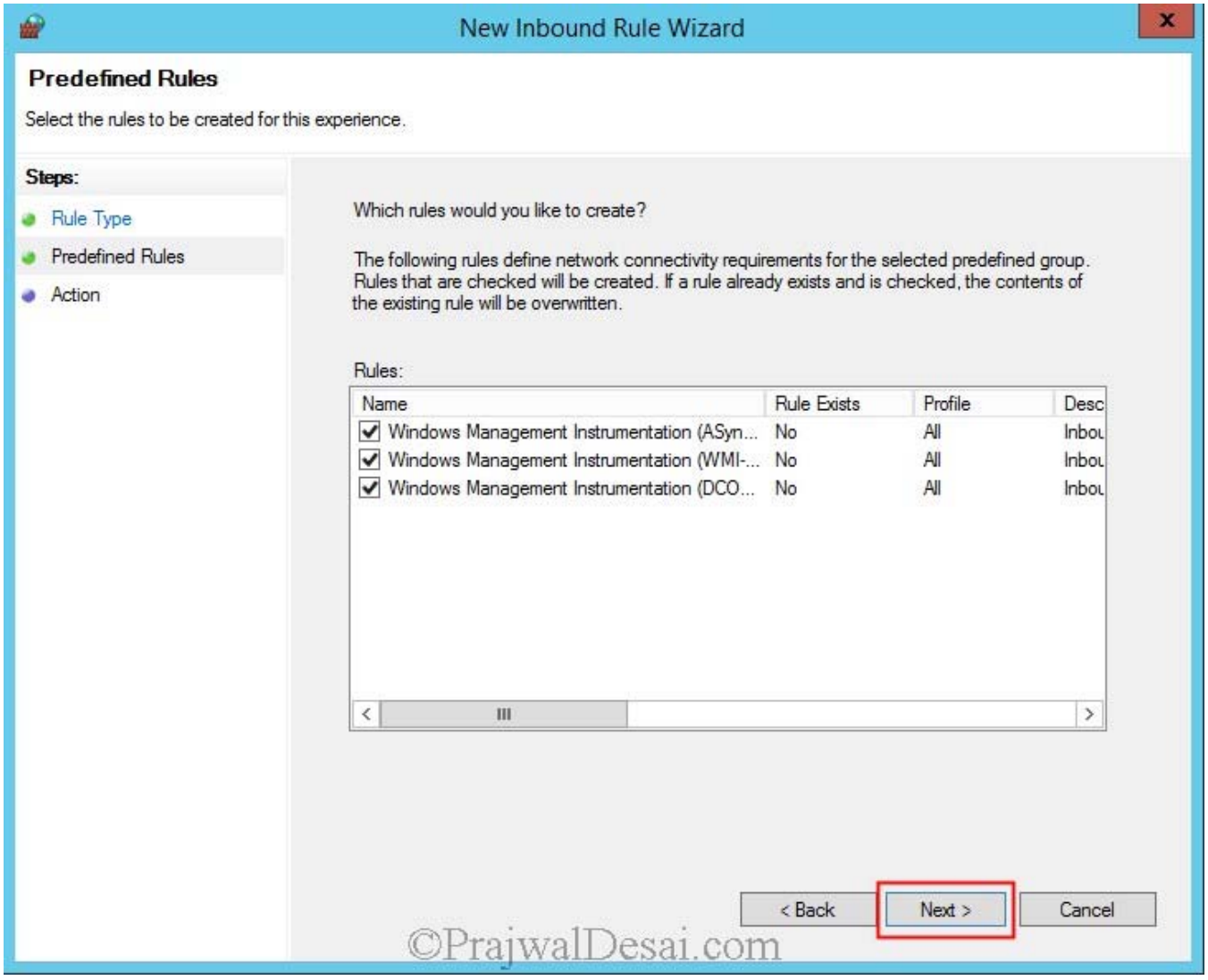
Click on **Allow the connection**. Click **Finish**.



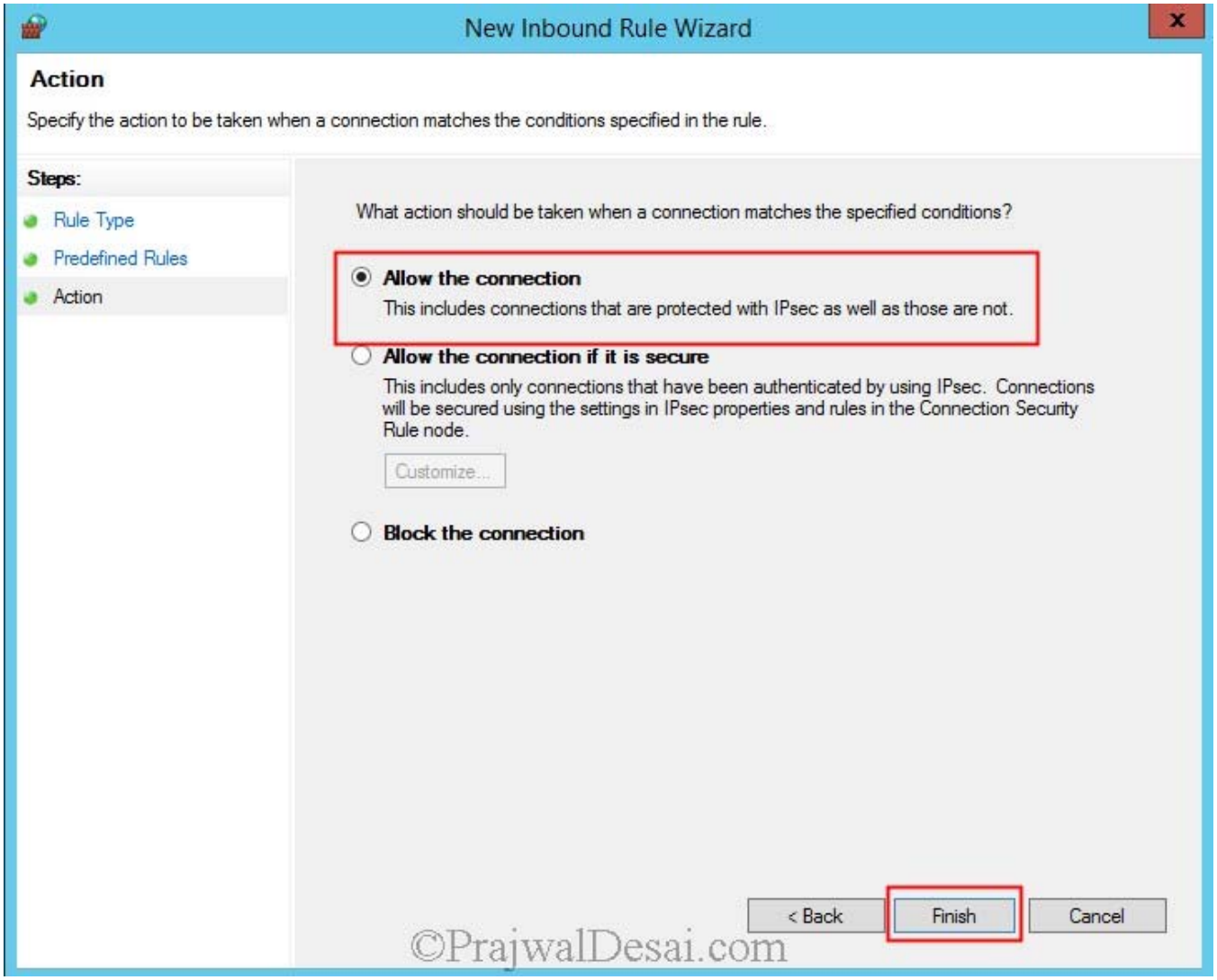
Now we will create an **Inbound Rule** to allow the **WMI** service on our Firewall. So right click on **Inbound Rule** and click on **New Rule**. Click on **Predefined** and select **Windows Management Instrumentation (WMI).** Click on **Next**.


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Predefined Rules
Action
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Windows Management Instrumentation (WMI)
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel
©PrajwalDesai.com

Click **Next**.



Choose **Allow the connection** and click **Finish**.



Opening Ports for SQL Replication

We will now see the steps to open the ports for SQL Replication. Please note that Configuration Manager does not support dynamic ports. Because SQL Server named instances by default use dynamic ports for connections to the database engine, when you use a named instance, you must manually configure the static port that you want to use for intrasite communication. This point has been discussed while installing SQL server for configuration manager 2012 R2.

Why should the ports 1433 and 4022 opened on Firewall ??

Port 1433 – SQL Server listens for incoming connections on a particular port. The default port for SQL Server is 1433. It applies to routine connections to the default installation of the Database Engine, or a named instance that is the only instance running on the computer.

Port 4022 – This is SQL Service Broker, though there is no default port for SQL Server Service Broker, but this is the port that we allow inbound on our firewall.

Site System roles that communicate directly with the SQL Server database

Application Catalog web service point

Certificate registration point role

Enrollment point role

Management point

Site server

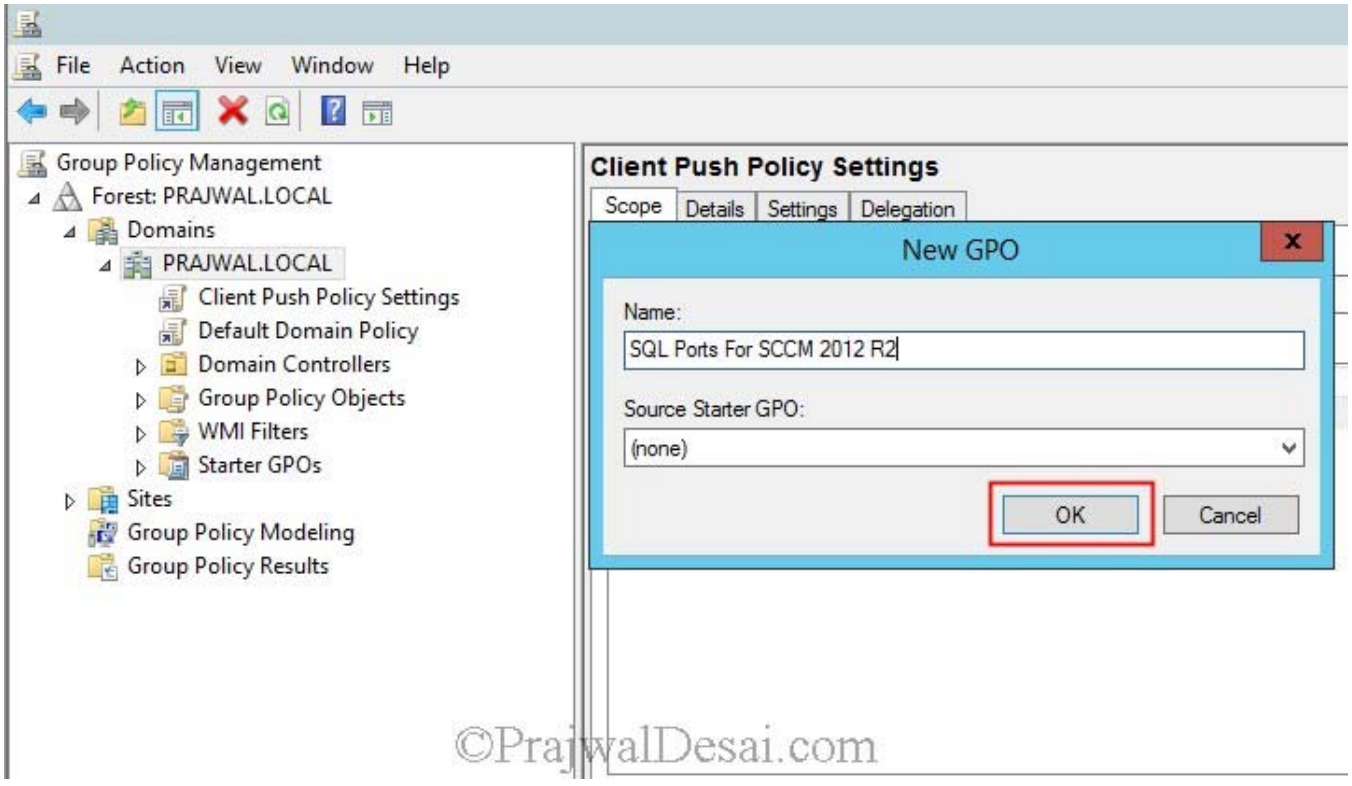
Reporting services point

SMS Provider

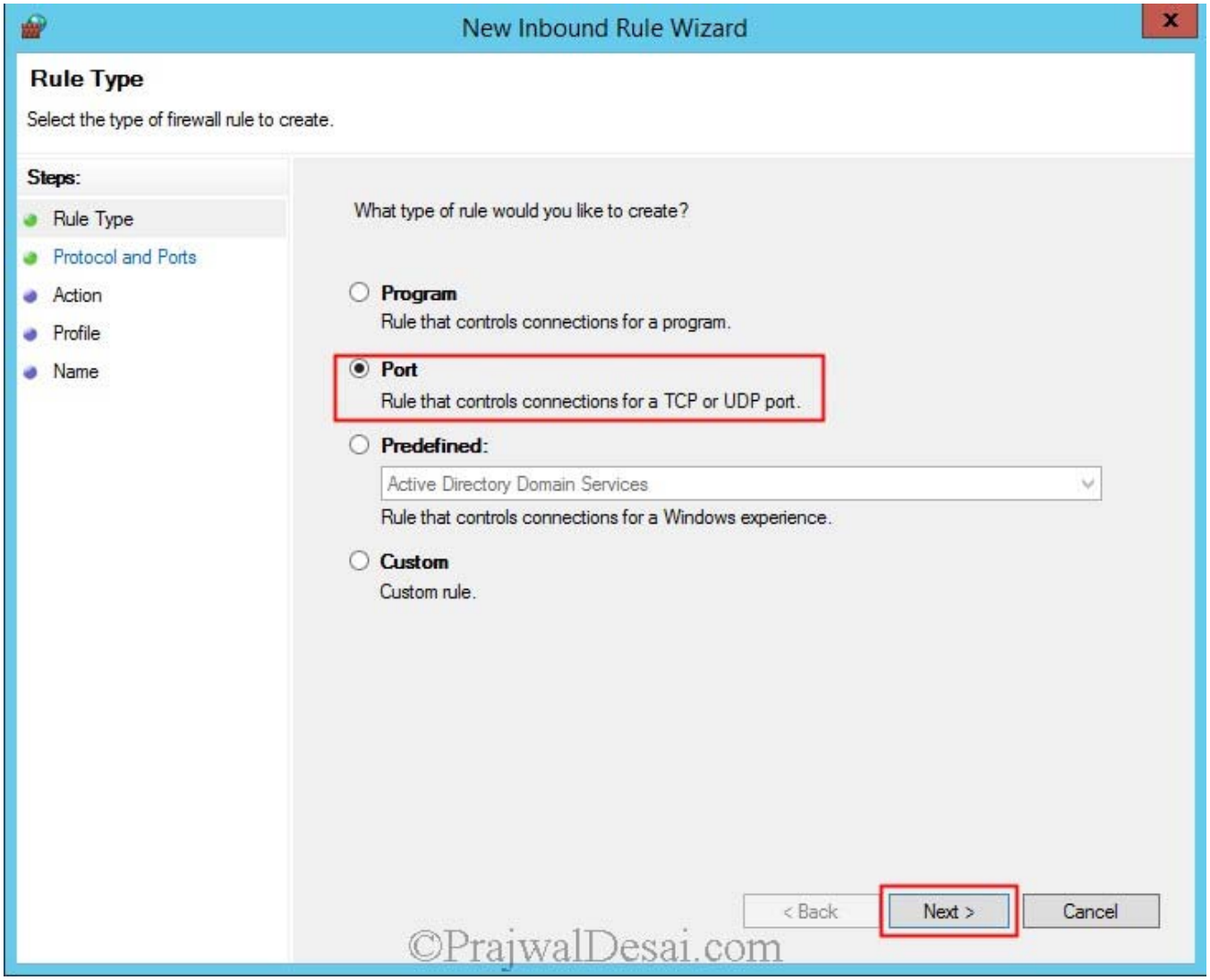
SQL Server to SQL Server

By default, Microsoft Windows enables the Windows Firewall, which closes port 1433 to prevent Internet computers from connecting to a default instance of SQL Server on your computer. Connections to the default instance using TCP/IP are not possible unless you reopen port 1433. We will now create a group policy to open TCP ports **1433** and **4022**.

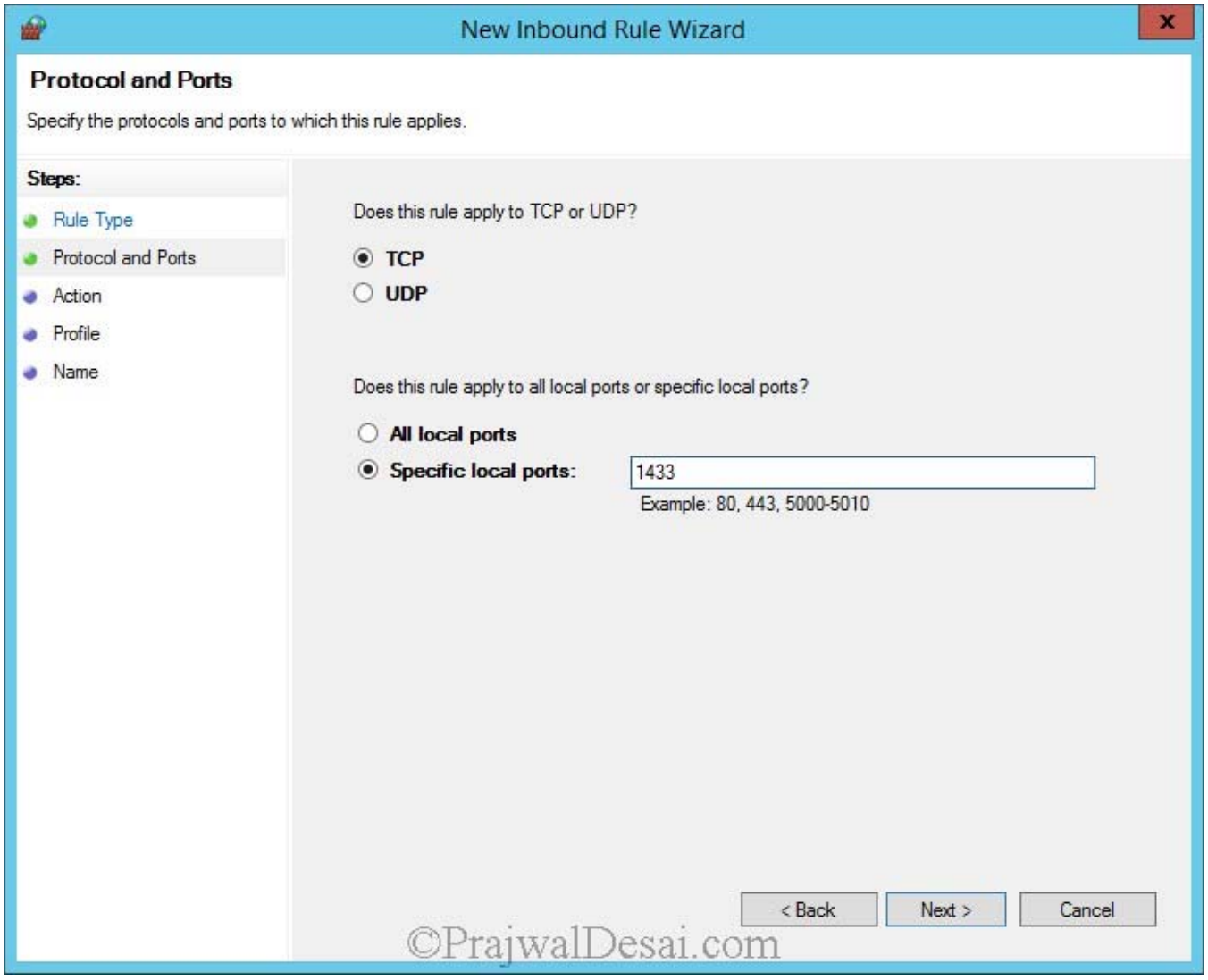
Open the **Group Policy Management console**. Create a new policy and provide a name for the policy. Right Click the policy and edit it.



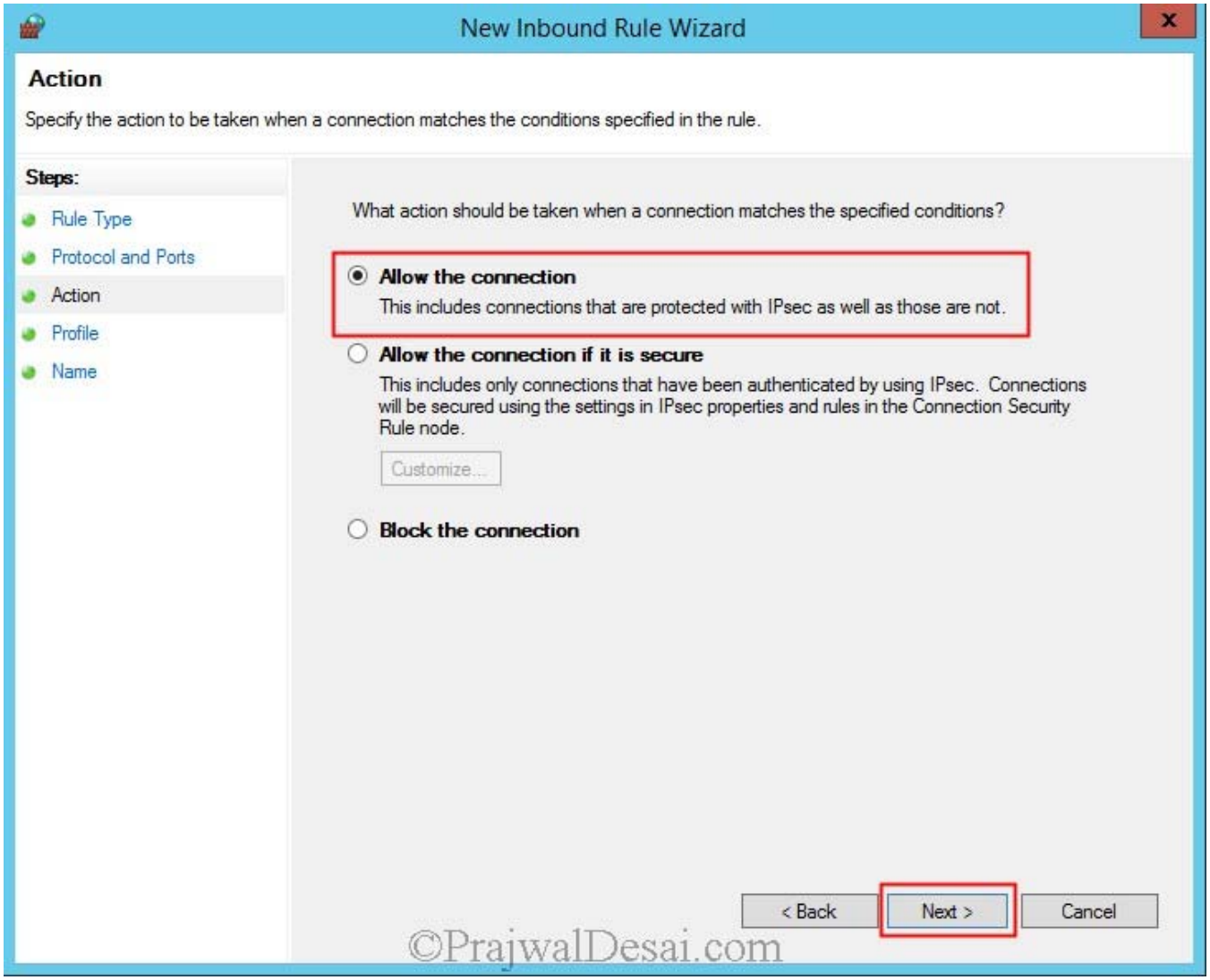
In the Windows GP management console, expand **computer configuration**, **Windows settings**, **Security settings**, **Windows firewall with advanced security**. Right click on **Inbound Rule** and create an **Inbound Rule** and select **Port**. Click on **Next**.



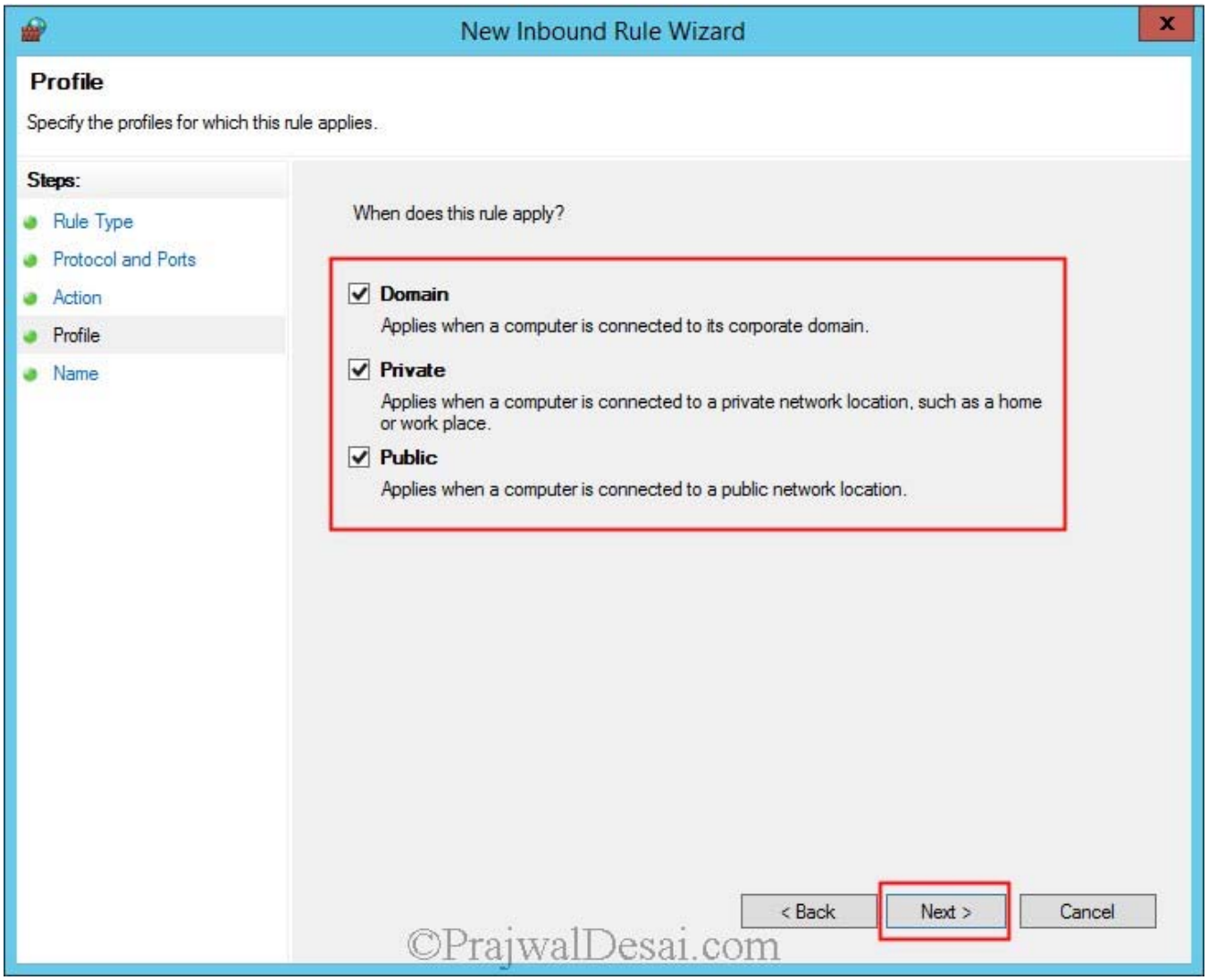
Select **TCP**, and specify port **1433** in **specific local ports**. Click **Next**.



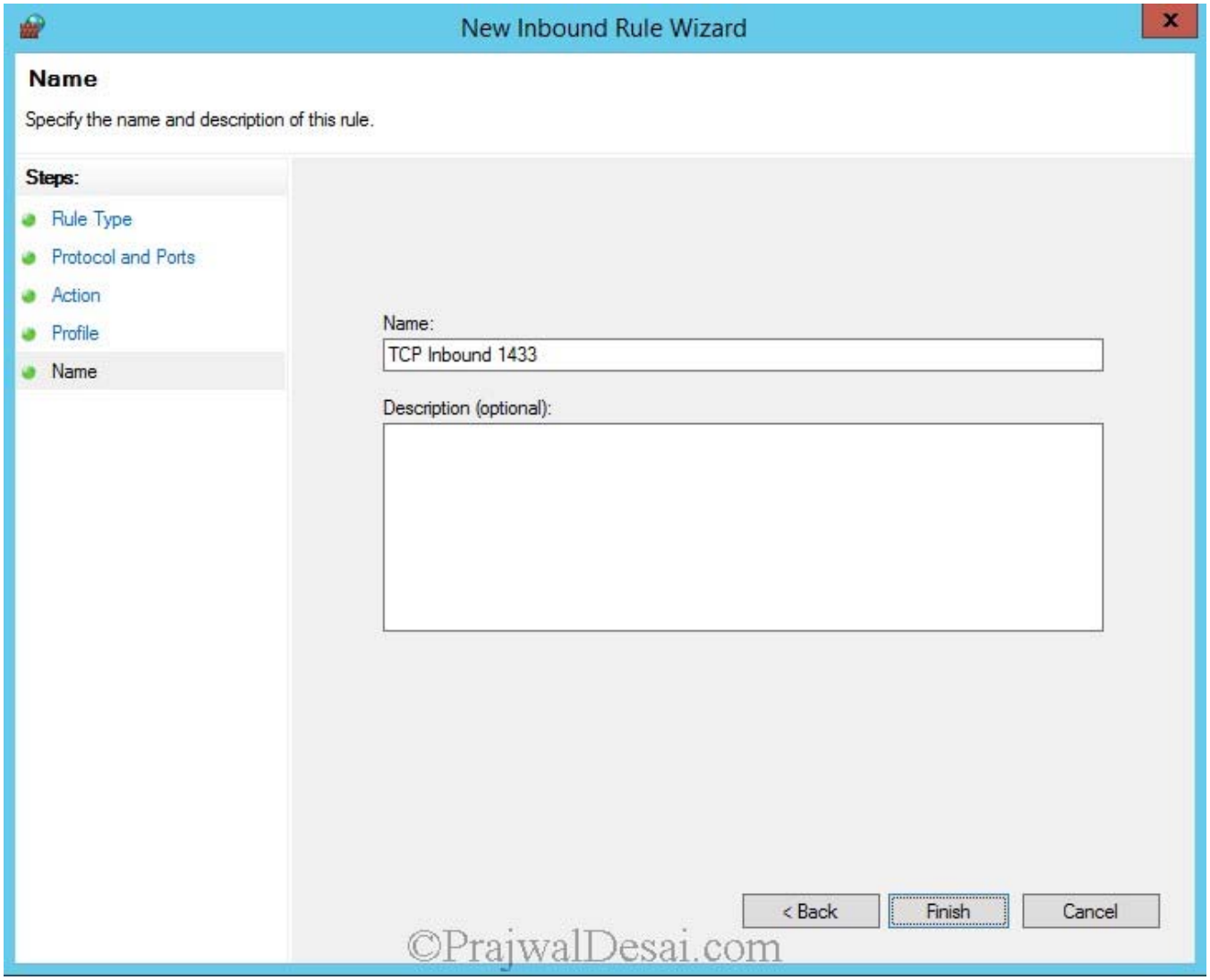
Click on **Allow connection** and click on **Next**.



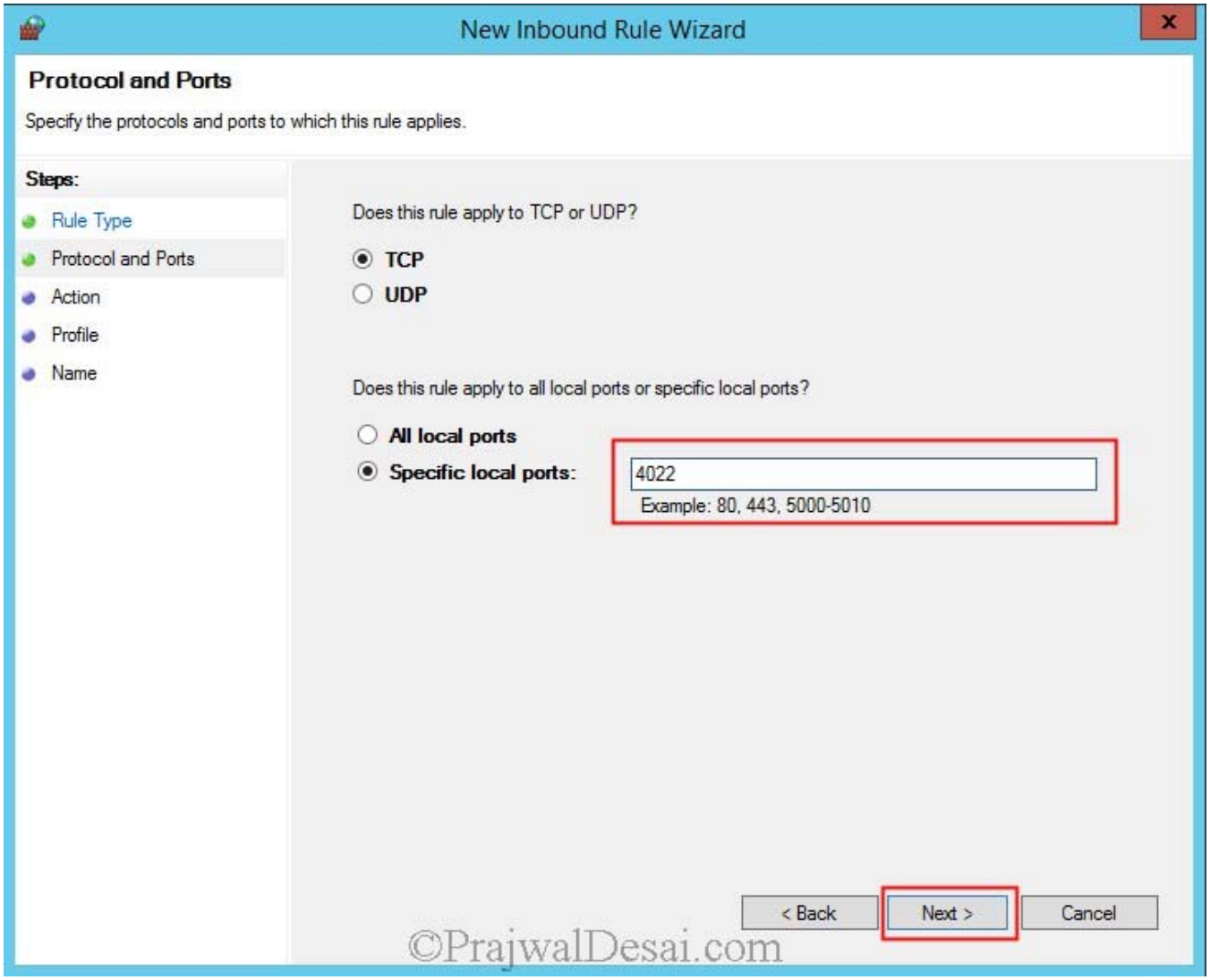
The firewall rule will be applied for all the 3 profiles. Click on **Next**.



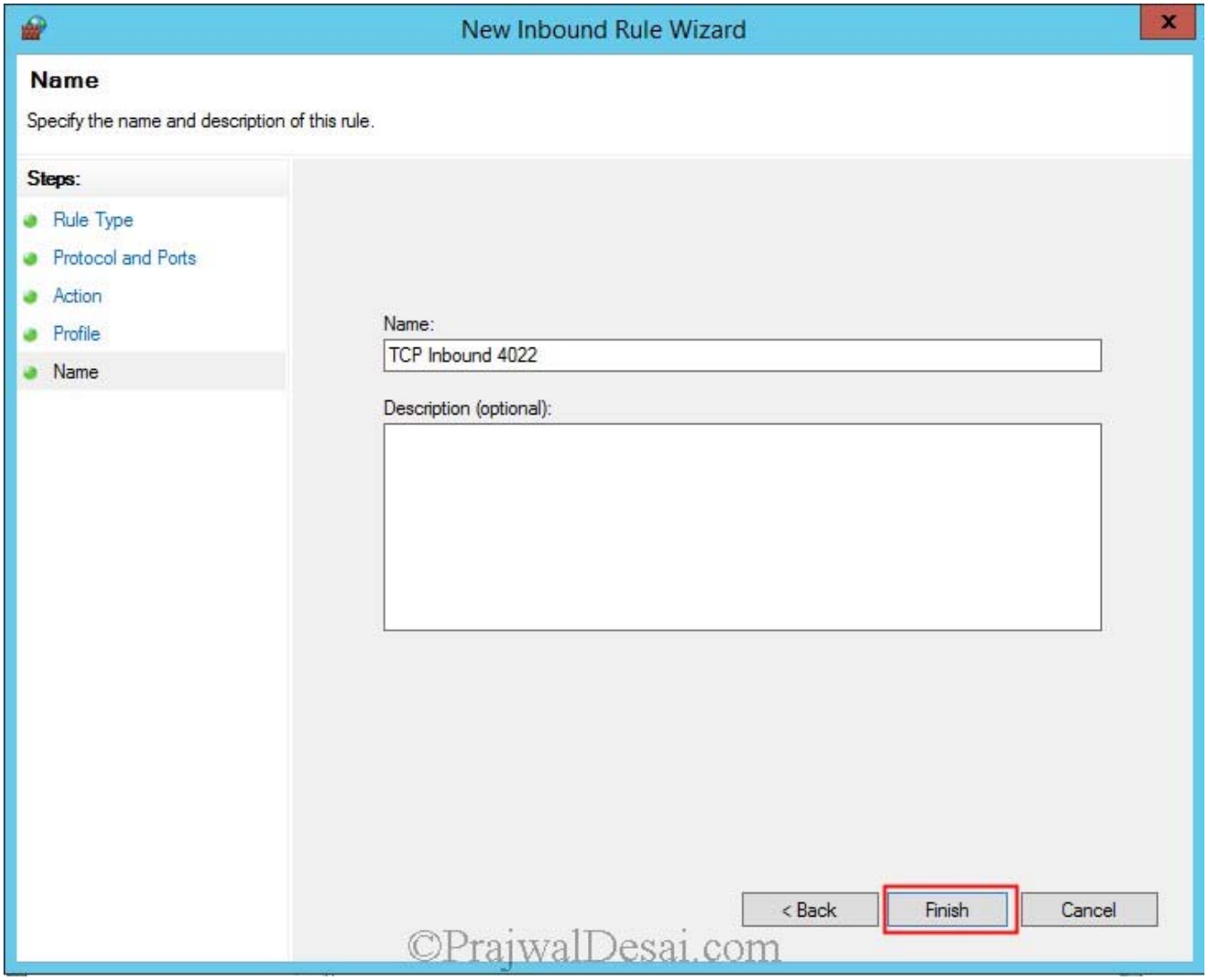
Name the rule as **TCP Inbound 1433**. Click on **Finish**.



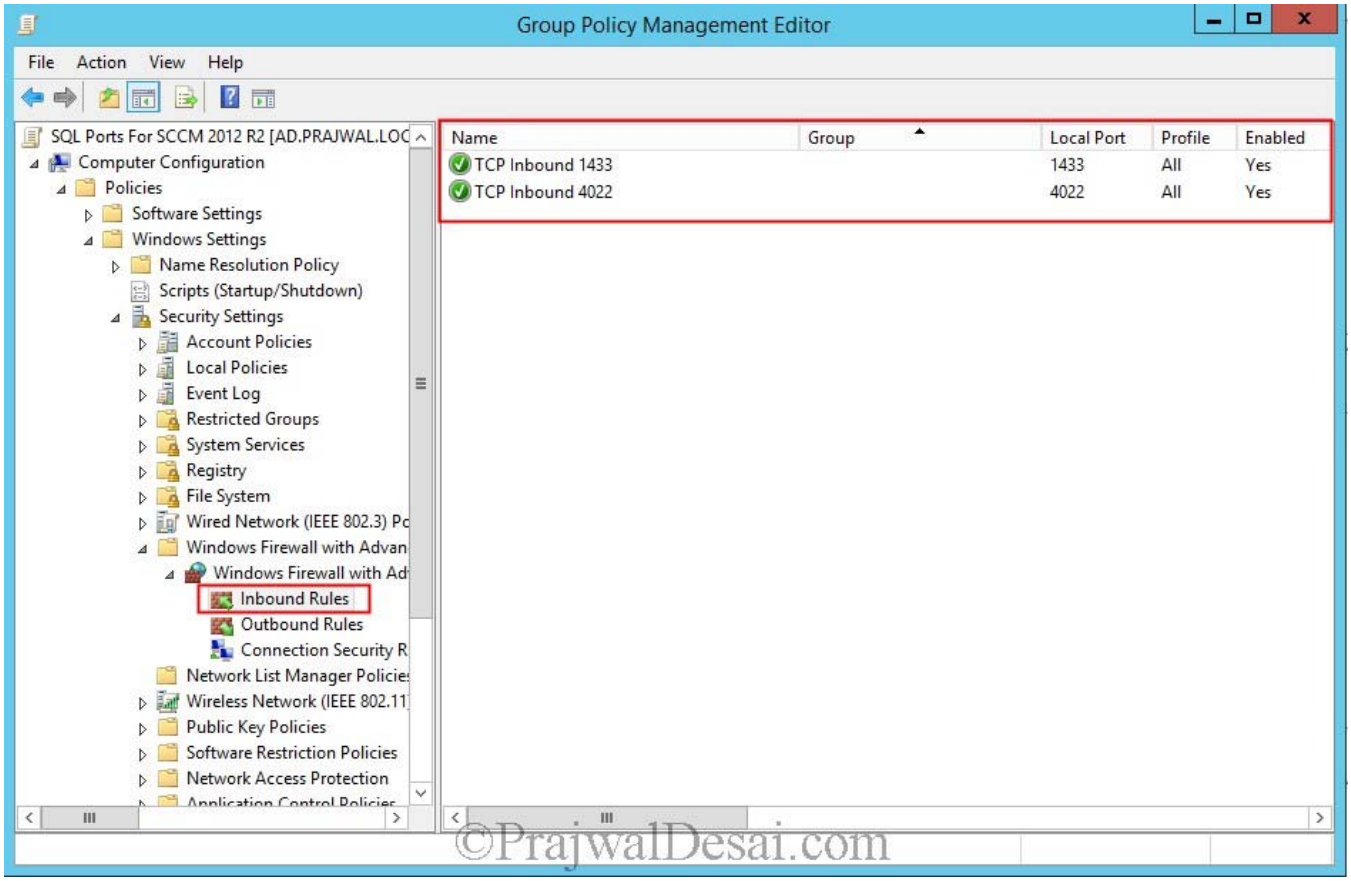
Similarly create an **Inbound Rule** to allow port **4022**. choose **TCP** and specify the port number as **4022**. Click on **Next.**



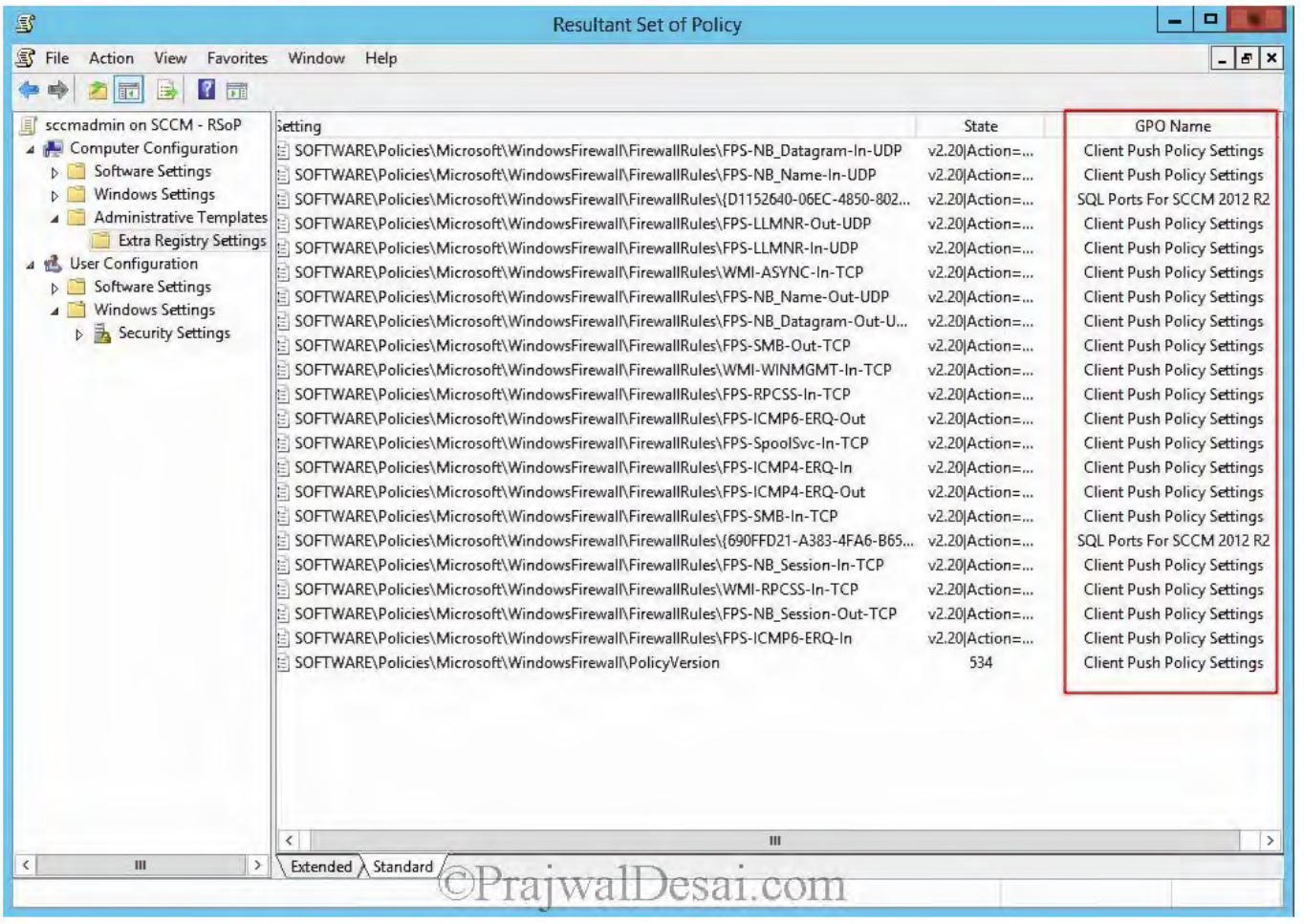
Click on **Allow the connection**. Click on **Next**. Select **Domain**, **Private** and **Public** and click on **Next**. Provide the name as **TCP Inbound 4022** to identify the rule. Click on **Finish**.



We have allowed TCP inbound ports 1433 and 4022 on our firewall.



Run the gpupdate /force command on the domain controller and on any of the client machine, launch the command prompt and type the command **gpupdate /force** and hit enter. In the same command prompt, type the command **rsop.msc**. This will show the resultant set of policies, group policies that are applied to this client. Expand **Administrative Templates** and click on **Extra Registry Settings**. On the right side pane you will find that the policies that we created are applied on the machine.


Resultant Set of Policy
File Action View Favorites Window Help
sccmadmin on SCCM - RSoP
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Extra Registry Settings
User Configuration
Software Settings
Windows Settings
Security Settings
Setting
State
GPO Name
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-NB_Datagram-In-UDP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-NB_Name-In-UDP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\{D1152640-06EC-4850-802... v2.20|Action=... SQL Ports For SCCM 2012 R2
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-LLMNR-Out-UDP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-LLMNR-In-UDP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\WMI-ASYNC-In-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-NB_Name-Out-UDP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-NB_Datagram-Out-U... v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-SMB-Out-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\WMI-WINMGMT-In-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-RPCSS-In-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-ICMP6-ERQ-Out v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-SpoolSvc-In-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-ICMP4-ERQ-In v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-ICMP4-ERQ-Out v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-SMB-In-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\{690FFD21-A383-4FA6-B65... v2.20|Action=... SQL Ports For SCCM 2012 R2
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-NB_Session-In-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\WMI-RPCSS-In-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-NB_Session-Out-TCP v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS-ICMP6-ERQ-In v2.20|Action=... Client Push Policy Settings
SOFTWARE\Policies\Microsoft\WindowsFirewall\PolicyVersion 534 Client Push Policy Settings
Extended
Standard
©PrajwalDesai.com