Basic instructions for configuring PPP MSSQL Express Firewall Settings for Server 2008 and Windows 7 Operating Systems

Prerequisites and Assumptions: PPP, MSSQL Express and Pervasive 32-bit and/or 64-bit database server is correctly installed and operational on Windows 7 or Server 2008/2008R2.

Firewalls block unauthorized access to computer resources. If a firewall is not configured correctly communications from the client to the SQL Server may not work.

By default, in Server 2008 and Windows 7 the firewall is on and is blocking remote connections. IT support and administrators need to be careful when adjusting the firewall settings as it will affect programs that access computer resources.

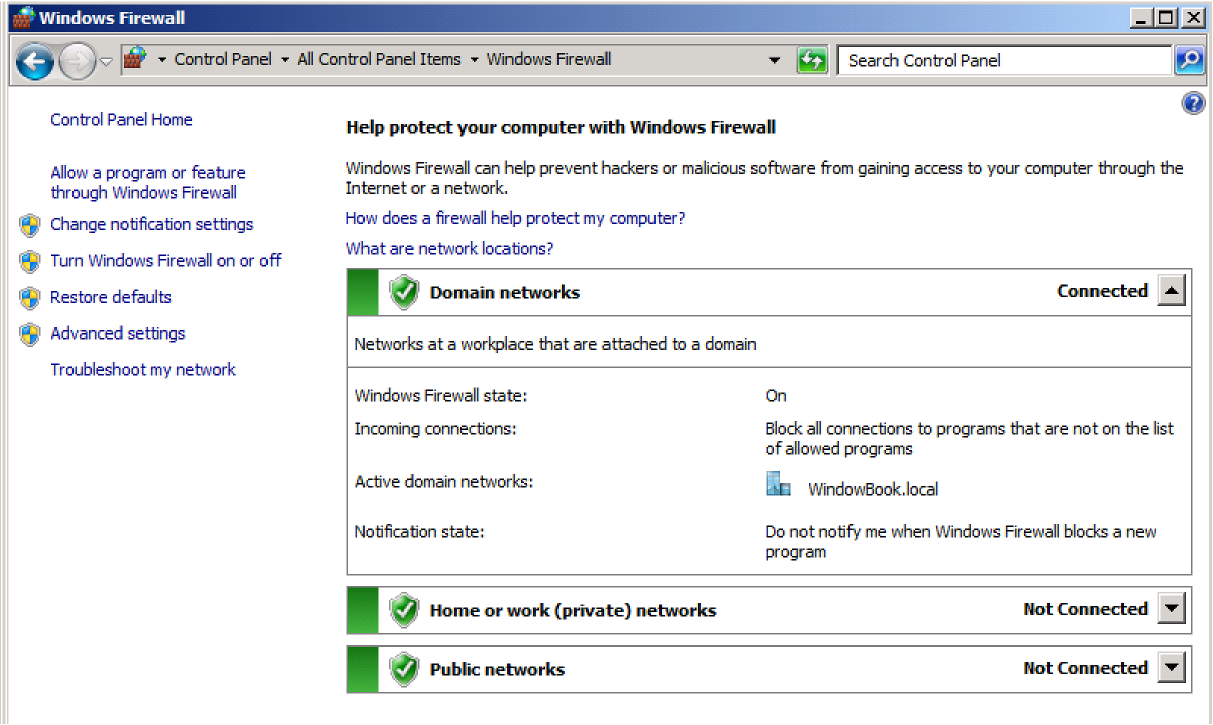
The following is a basic list of commonly used SQL Server ports related to PPP:

- TCP port 1433 – SQL Server default instance running over TCP. Note - If there is more than one named instance of the Database Engine installed you may be need to change the default port 1433 to something else to avoid port conflicts. These instructions assume you only have the default instance and we will use port 1433.
- UDP port 1434 – SQL Server Browser service
- TCP port 135 – Transact SQL debugger. Since SQL Express will be used and Management Studio is on the host server, the service ssms.exe must be added to the "allow programs to communicate through the Windows Firewall" exceptions list and TCP port 1433 opened (see screenshot)

Using Windows Firewall item in Control Panel to verify the proper firewall settings for SQL Server:

Click **Start**, click **Run** and then enter **firewall.cpl**

You will see a screen similar to below



Windows Firewall
Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
How does a firewall help protect my computer?
What are network locations?

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

Domain networks — **Connected**

Networks at a workplace that are attached to a domain

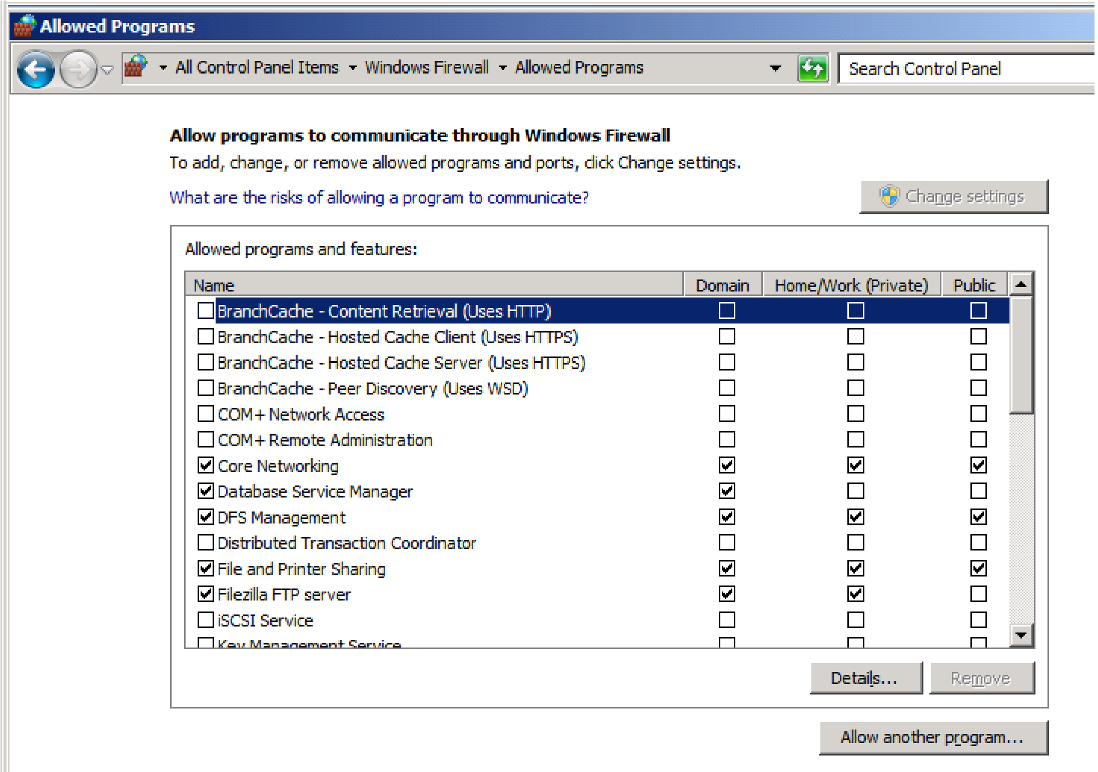
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active domain networks:	WindowBook.local
Notification state:	Do not notify me when Windows Firewall blocks a new program

Home or work (private) networks — **Not Connected**

Public networks — **Not Connected**

Click Allow a program or feature through Windows Firewall and verify the following programs are in the list.

- Database Service manager – this is PSQL
- Pervasive PSQl 32-bit Database Engine (Server) – required for PSQL
- Pervasive PSQl 64-bit Database Engine (Server) – required for PSQL
- SQL Server Domain-Access Only
- SSMS – configure for TCP on Port 1433. This allows SQL server access


Allowed Programs
All Control Panel Items ▸ Windows Firewall ▸ Allowed Programs
Search Control Panel

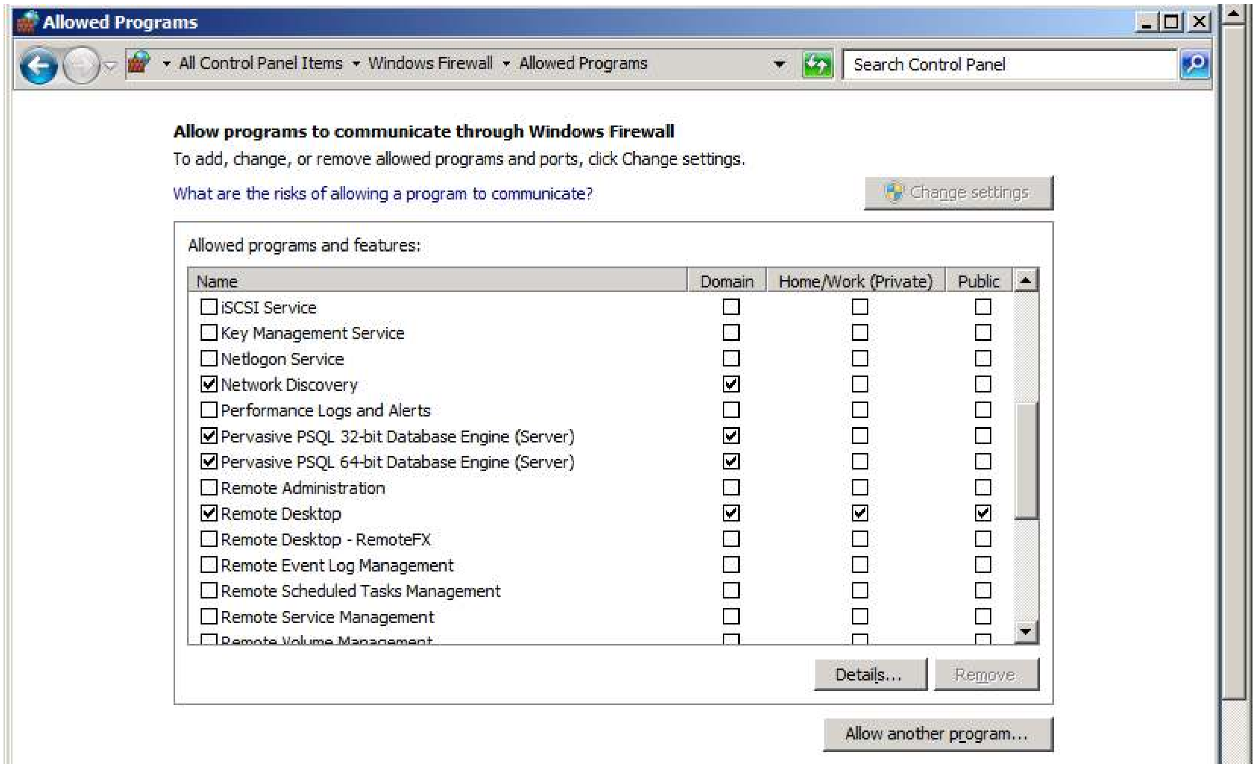
Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
□ BranchCache - Content Retrieval (Uses HTTP)	□	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□	□
□ COM+ Network Access	□	□	□
□ COM+ Remote Administration	□	□	□
☑ Core Networking	☑	☑	☑
☑ Database Service Manager	☑	□	□
☑ DFS Management	☑	☑	☑
□ Distributed Transaction Coordinator	□	□	□
☑ File and Printer Sharing	☑	☑	☑
☑ Filezilla FTP server	☑	☑	□
□ iSCSI Service	□	□	□
□ Key Management Service	□	□	□


Allowed Programs
All Control Panel Items ▸ Windows Firewall ▸ Allowed Programs
Search Control Panel

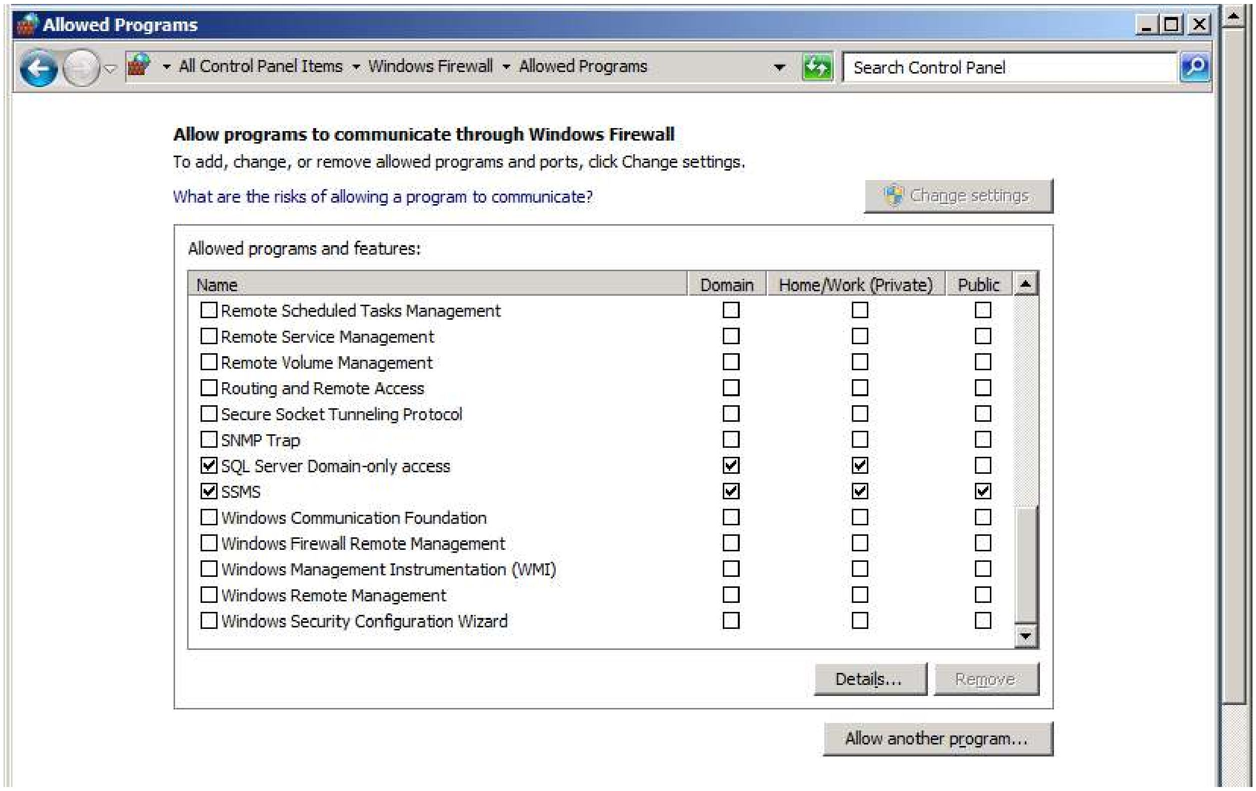
Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
□ iSCSI Service	□	□	□
□ Key Management Service	□	□	□
□ Netlogon Service	□	□	□
☑ Network Discovery	☑	□	□
□ Performance Logs and Alerts	□	□	□
☑ Pervasive PSQL 32-bit Database Engine (Server)	☑	□	□
☑ Pervasive PSQL 64-bit Database Engine (Server)	☑	□	□
□ Remote Administration	□	□	□
☑ Remote Desktop	☑	☑	☑
□ Remote Desktop - RemoteFX	□	□	□
□ Remote Event Log Management	□	□	□
□ Remote Scheduled Tasks Management	□	□	□
□ Remote Service Management	□	□	□
□ Remote Volume Management	□	□	□



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

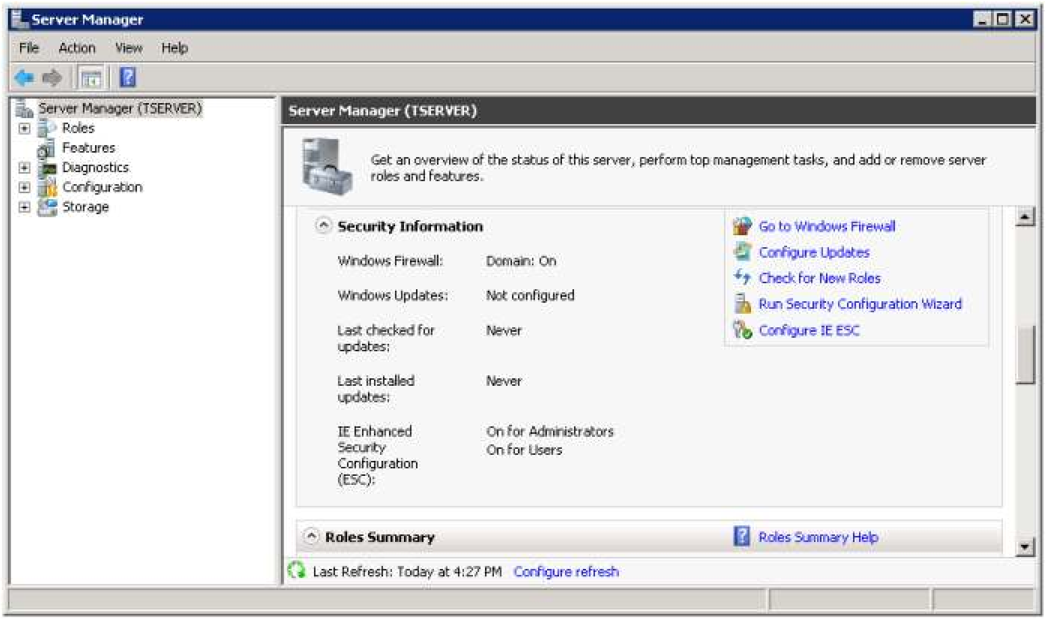
Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
☐ Remote Scheduled Tasks Management	☐	☐	☐
☐ Remote Service Management	☐	☐	☐
☐ Remote Volume Management	☐	☐	☐
☐ Routing and Remote Access	☐	☐	☐
☐ Secure Socket Tunneling Protocol	☐	☐	☐
☐ SNMP Trap	☐	☐	☐
☑ SQL Server Domain-only access	☑	☑	☐
☑ SSMS	☑	☑	☑
☐ Windows Communication Foundation	☐	☐	☐
☐ Windows Firewall Remote Management	☐	☐	☐
☐ Windows Management Instrumentation (WMI)	☐	☐	☐
☐ Windows Remote Management	☐	☐	☐
☐ Windows Security Configuration Wizard	☐	☐	☐

If SQL Server and/or SSMS is not listed in the "allowed programs" you must add them.

How to configure Windows firewall to allow SQL Server access to users (Source for screenshots & information: http://www.mssqltips.com)

1. Click Start | All Programs | Administrative Tools | Server Manager. This will open up Server Manager as shown in the below snippet.



Server Manager (TSERVER)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Windows Firewall: Domain: On

Windows Updates: Not configured

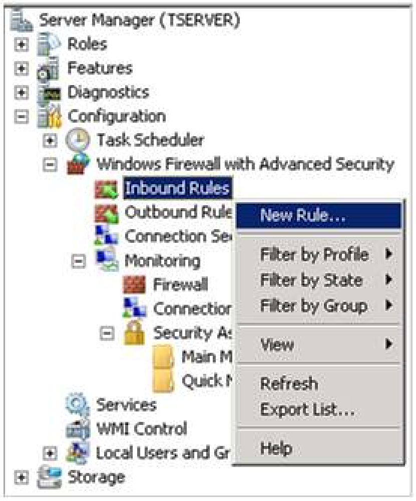
Last checked for updates: Never

Last installed updates: Never

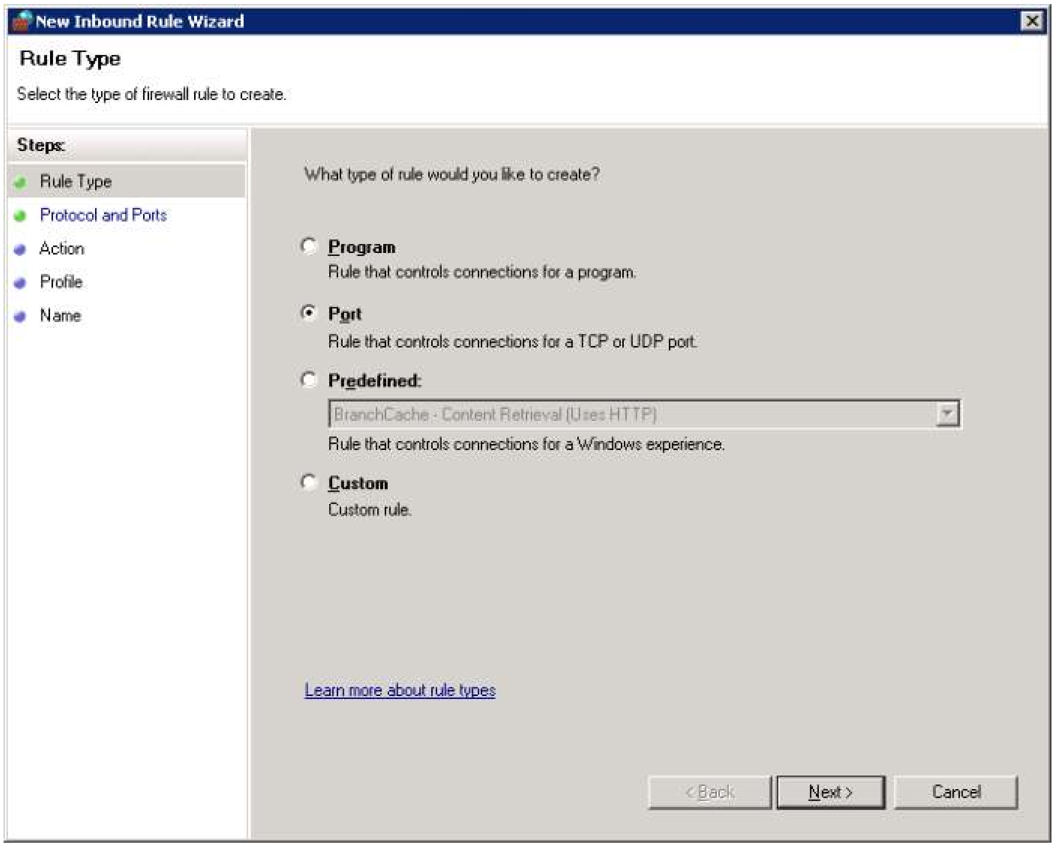
IE Enhanced Security Configuration (ESC): On for Administrators
On for Users

Last Refresh: Today at 4:27 PM

2. In **Server Manager**, expand **Configurations** tab and then expand **Windows Firewall with Advanced Security**. Right click **Inbound Rules** and click on **New Rule...** as shown in the below snippet to open up **New Inbound Rule Wizard**.



3. In New Inbound Rule Wizard's **Rule Type** Page, you need to select **Port** option as shown in the below snippet to control connections for a TCP or UDP Port. Click Next to continue with the wizard.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

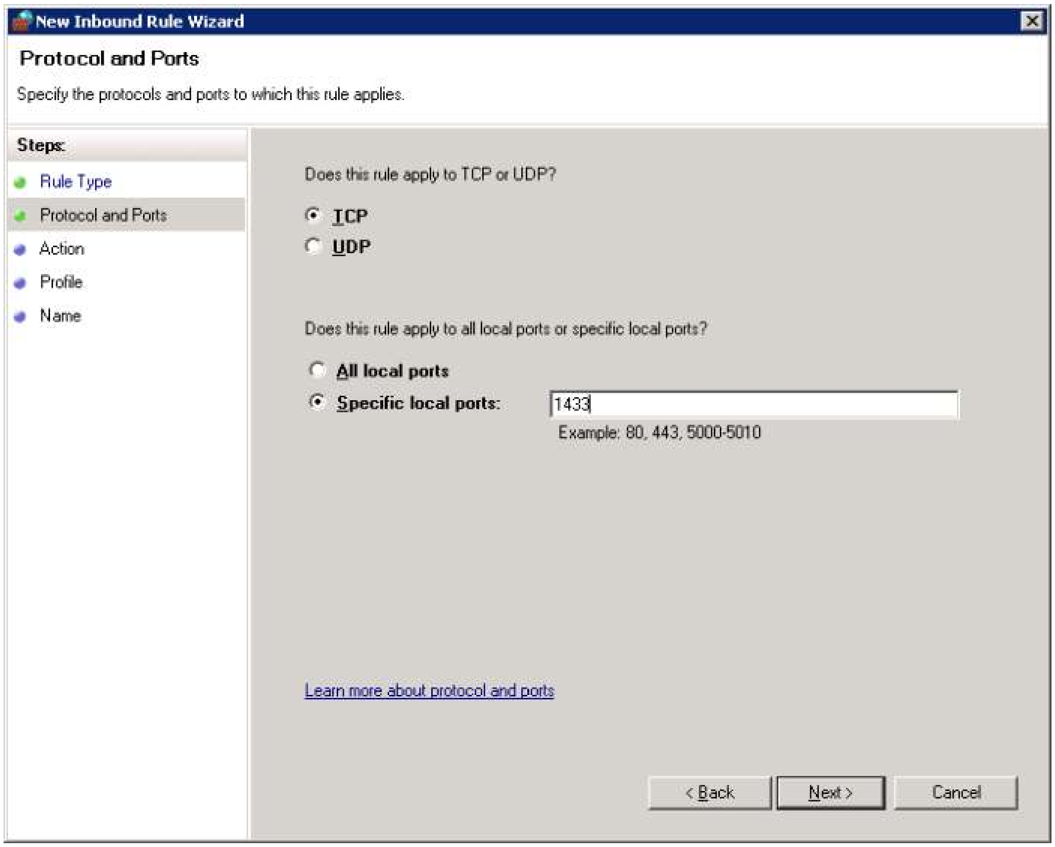
○ Program
Rule that controls connections for a program.

● Port
Rule that controls connections for a TCP or UDP port.

○ Predefined:
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.

4. In **Protocol and Ports**, specify the protocols and ports to which this rule applies. As we know that SQL Server when installed as a default instance will use 1433 as the default port, hence you need to choose TCP option and then specify the port number as 1433 as shown in the below snippet. Click Next to continue with the wizard.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP
○ UDP

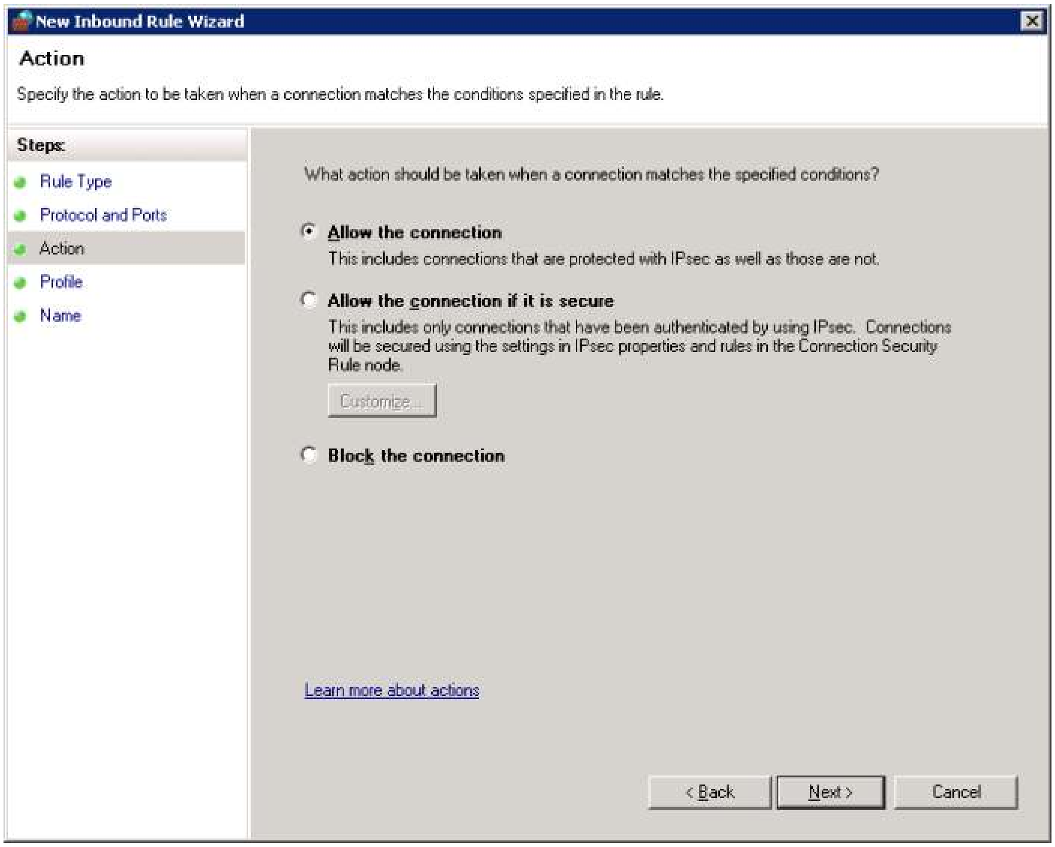
Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 1433
Example: 80, 443, 5000-5010

5. In **Action** page, specify the action to be taken when a connection matches the conditions specified in this rule. There are basically three options available to choose from which are self explanatory.

```
a) Allow the connection
b) Allow the connection if it is secure
c) Block the connection
```

Here, you need to choose the first option which is **Allow the connection** and click Next, to continue with the wizard.



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

● Allow the connection

This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure

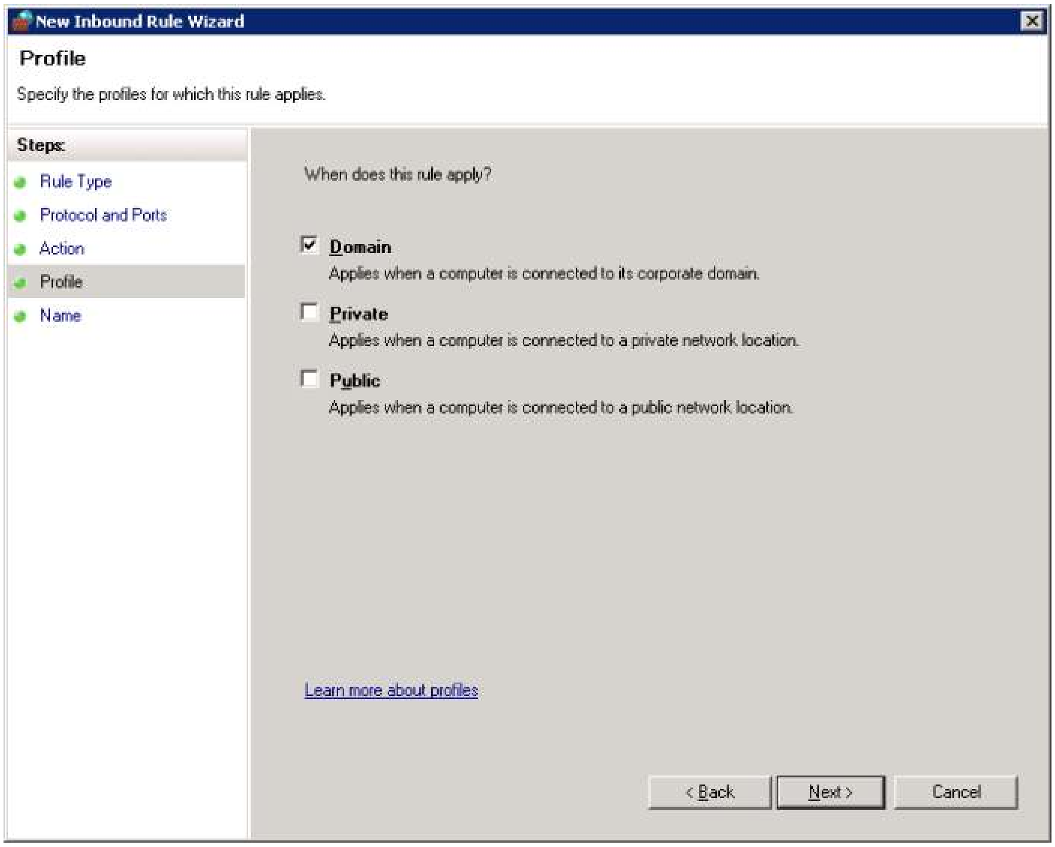
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

6. In **Profile** page, specify the profiles for which this rule should apply. There are three options available to choose from which are self explanatory.

```
a) Domain - Applies when a computer is connected to its corporate domain
b) Private - Applies when a computer is connected to a private network location
c) Public - Applies when a computer is connected to a public network location
```

Here, you need to choose the first option which is **Domain** as you want everyone who is connected to its corporate domain to get connected to the SQL Server Instance as long as they have permissions to connect to the SQL Server 2008 Instance. Click Next, to continue with the wizard.



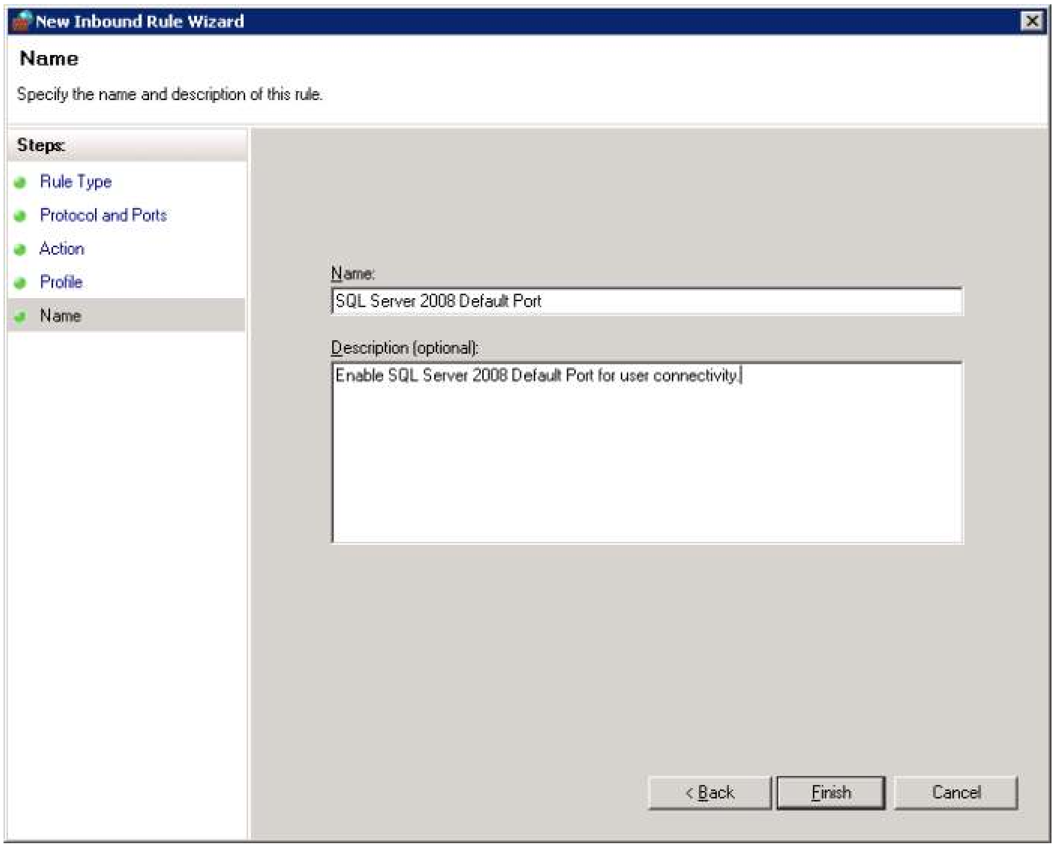
When does this rule apply?

☑ Domain
Applies when a computer is connected to its corporate domain.

☐ Private
Applies when a computer is connected to a private network location.

☐ Public
Applies when a computer is connected to a public network location.

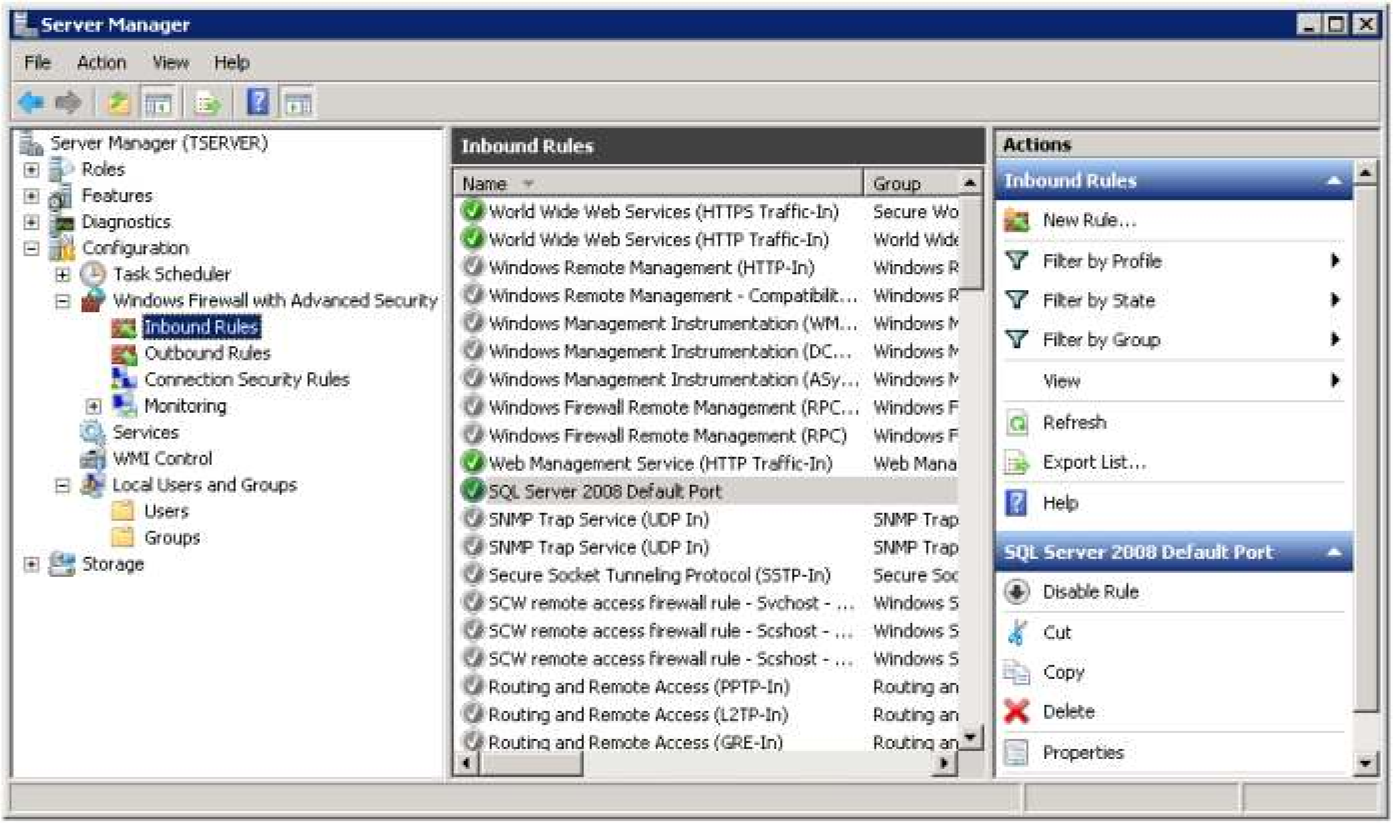
7. In **Name** Page, you need to provide a meaningful name and also provide a meaningful description as shown in the below snippet and click Finish to complete the wizard.



Name:
SQL Server 2008 Default Port

Description (optional):
Enable SQL Server 2008 Default Port for user connectivity.

Once the wizard configuration is complete, you will be able to see the new rule available under Inbound Rules as shown in the below snippet.



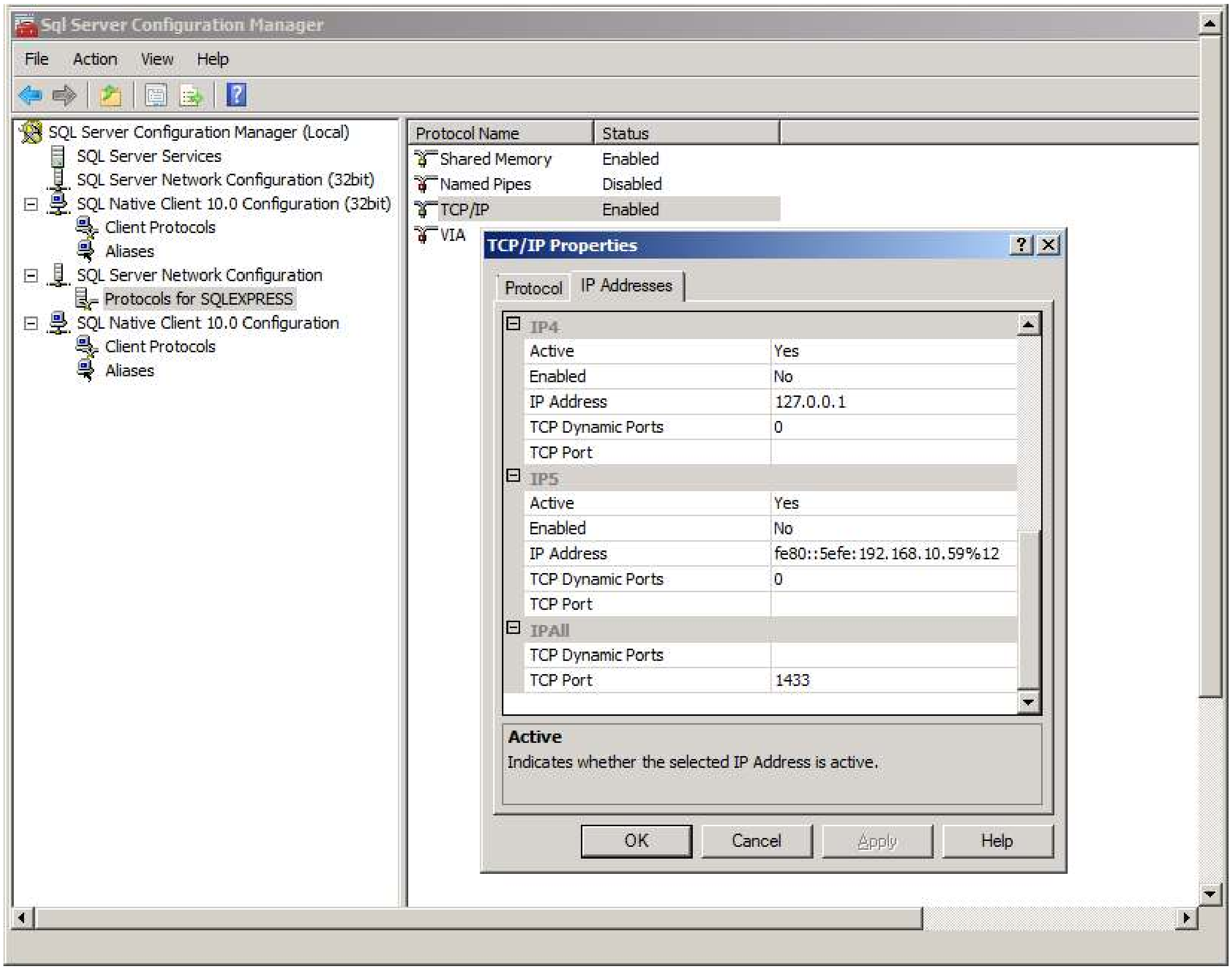
Name	Group
World Wide Web Services (HTTPS Traffic-In)	Secure Wo
World Wide Web Services (HTTP Traffic-In)	World Wide
Windows Remote Management (HTTP-In)	Windows R
Windows Remote Management - Compatibilit...	Windows R
Windows Management Instrumentation (WM...	Windows M
Windows Management Instrumentation (DC...	Windows M
Windows Management Instrumentation (ASy...	Windows M
Windows Firewall Remote Management (RPC...	Windows F
Windows Firewall Remote Management (RPC)	Windows F
Web Management Service (HTTP Traffic-In)	Web Mana
SQL Server 2008 Default Port	
SNMP Trap Service (UDP In)	SNMP Trap
SNMP Trap Service (UDP In)	SNMP Trap
Secure Socket Tunneling Protocol (SSTP-In)	Secure Soc
SCW remote access firewall rule - Svchost - ...	Windows S
SCW remote access firewall rule - Scshost - ...	Windows S
SCW remote access firewall rule - Scshost - ...	Windows S
Routing and Remote Access (PPTP-In)	Routing an
Routing and Remote Access (L2TP-In)	Routing an
Routing and Remote Access (GRE-In)	Routing an

On the computer running MSSQL Express, add ssms.exe to exceptions list in Windows Firewall

•Add TCP port 135 to the exceptions list.

•Add program ssms.exe (SQL Server Management Studio) to the exceptions list. By default, ssms.exe is installed in C:\Program Files\Microsoft SQL Server\100\Tools\Binn\VSShell\Common7\IDE.

On the computer running MSSQL Express verify in SQL Server Configuration Manager -> SQL Server Network Configuration -> Protocols for SQLEXPRESS -> TCP/IP properties -> that TCP Port 1433 is configured as below


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
Client Protocols
Aliases
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration
Client Protocols
Aliases
TCP/IP Properties
Protocol
IP Addresses
OK
Cancel
Apply
Help

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled
VIA	

IP4	
Active	Yes
Enabled	No
IP Address	127.0.0.1
TCP Dynamic Ports	0
TCP Port	
IP5	
Active	Yes
Enabled	No
IP Address	fe80::5efe:192.168.10.59%12
TCP Dynamic Ports	0
TCP Port	
IPAll	
TCP Dynamic Ports	
TCP Port	1433

Active
Indicates whether the selected IP Address is active.