Local Deployment in Windows Machines

There are two types of deployment

1. Local Deployment
2. Global Deployment

1. Local System Deployment

Will run the application on a machine / Will run the application on a group of machines which is connected to local network

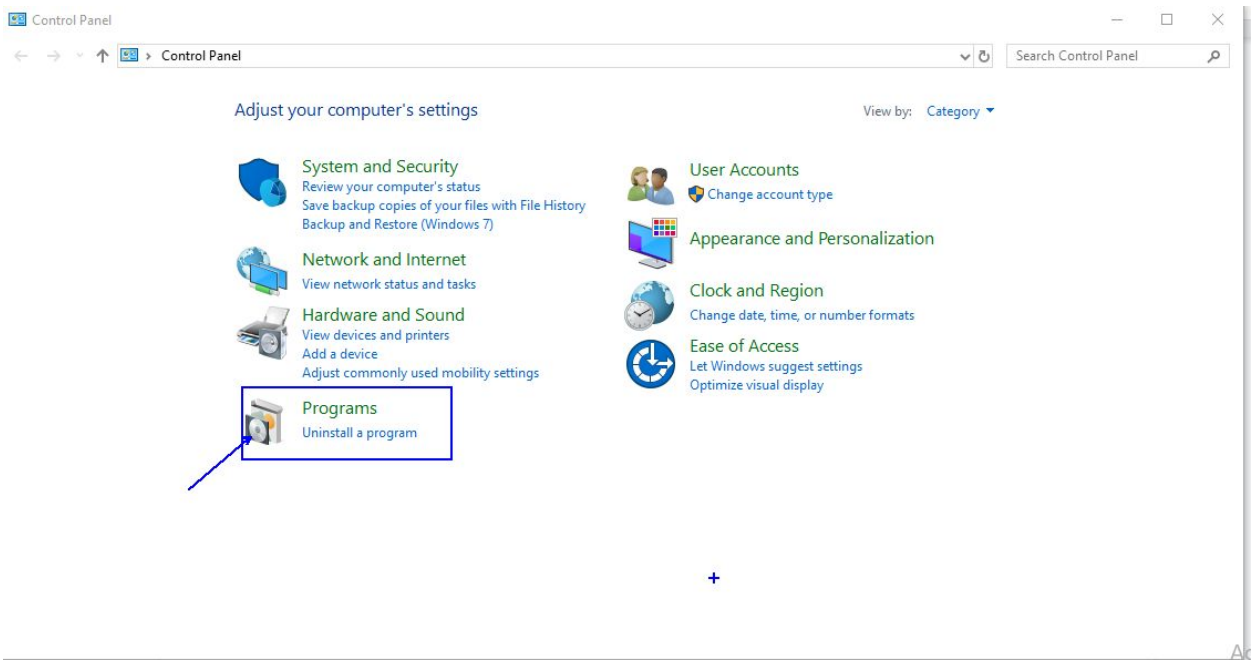
2. Global Deployment

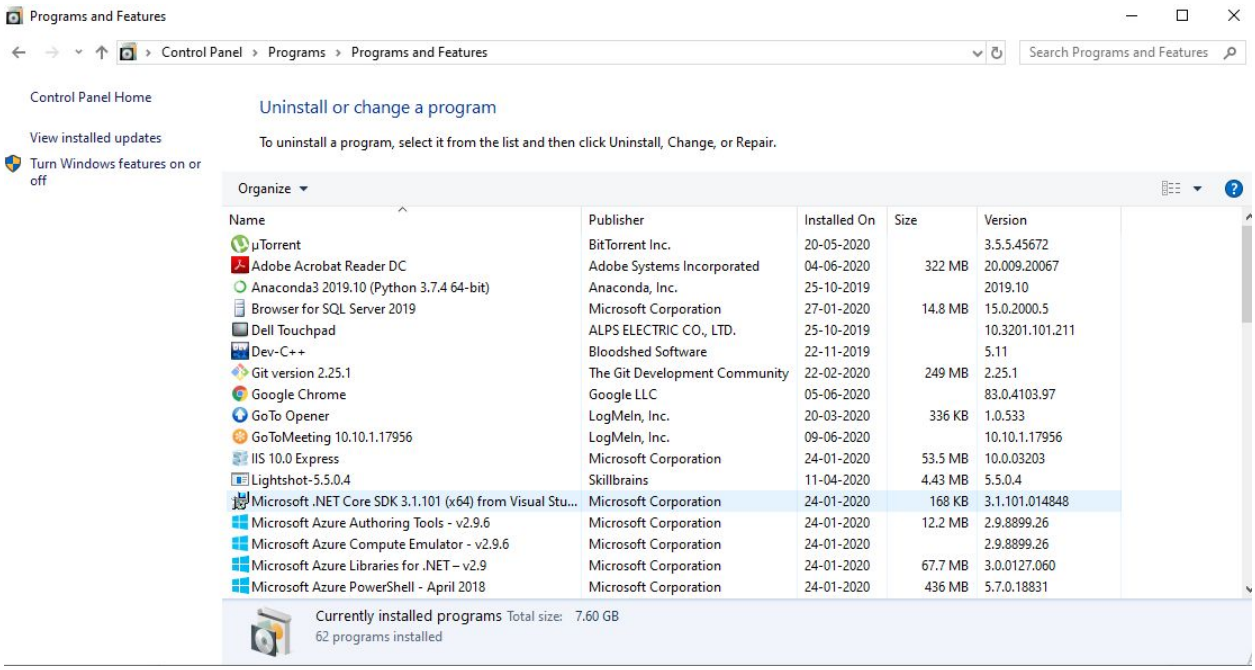
Will run the application any part of the globe with having internet connection

Example: goDaddy, HostIndia.....

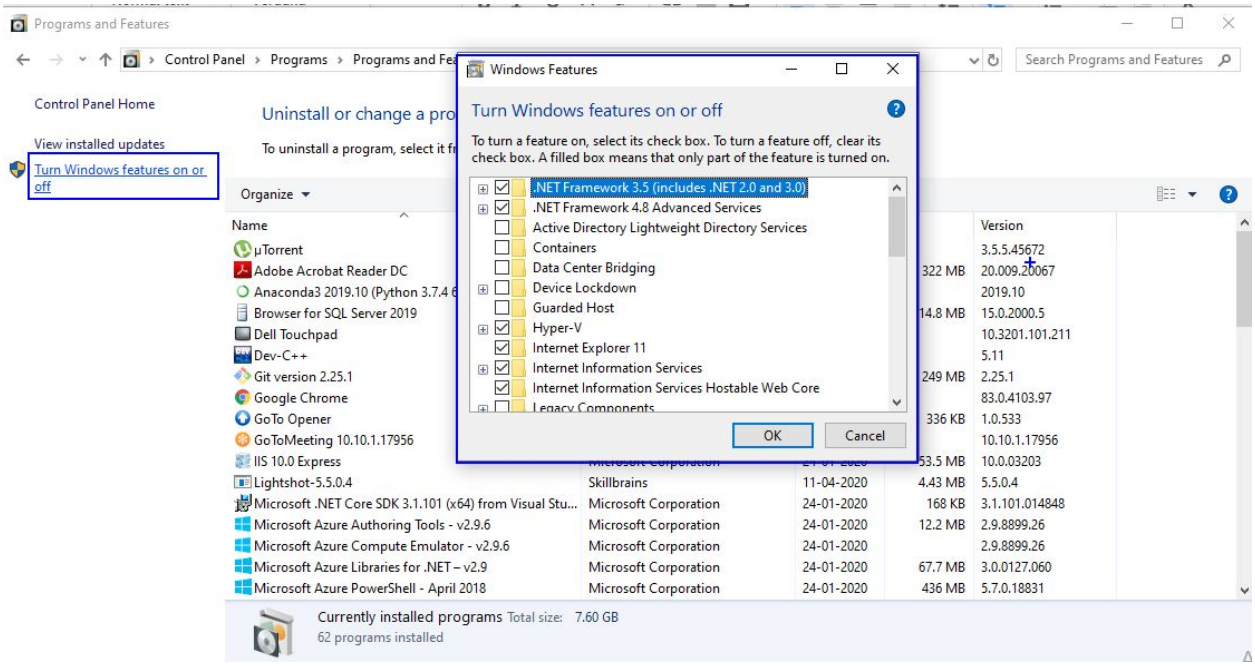
Let's make the setup for the Deployment

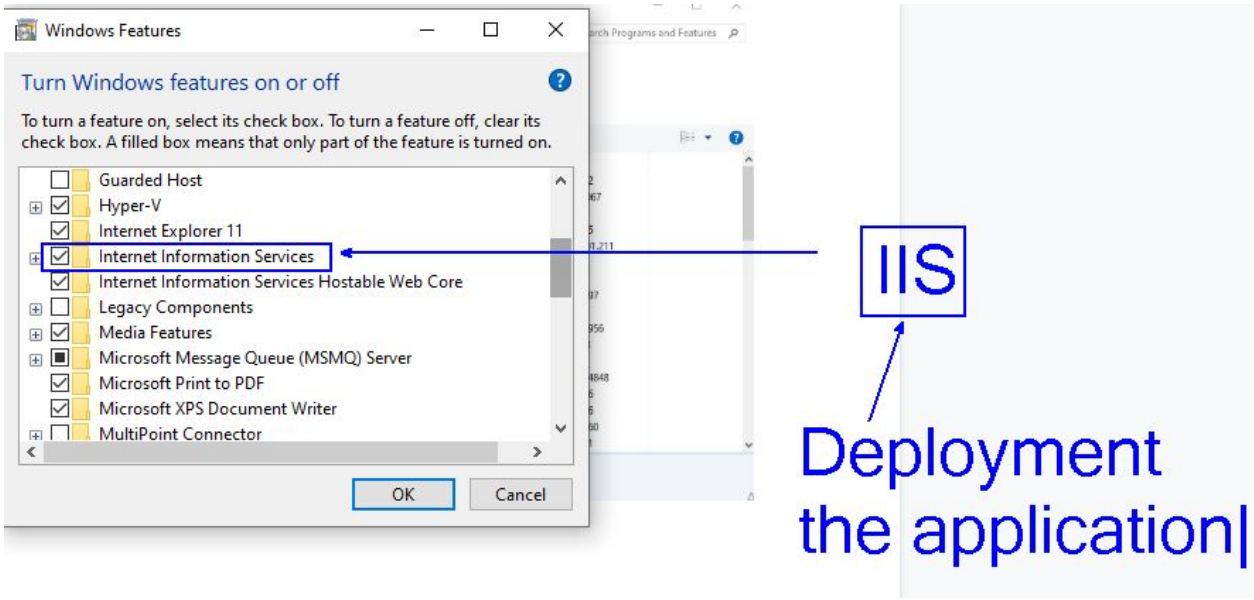
1. Everyone go to control panel and click on Programs option

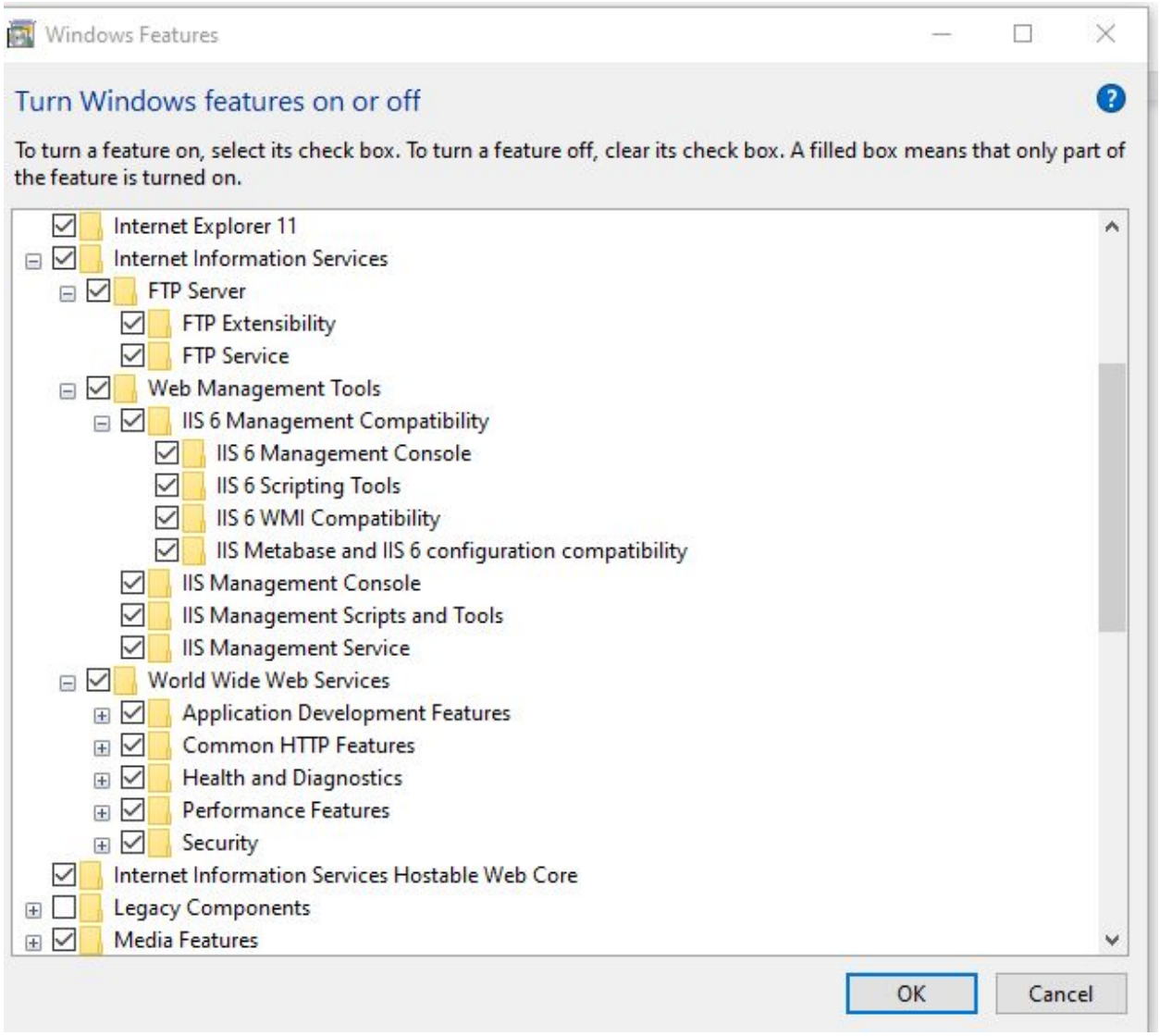


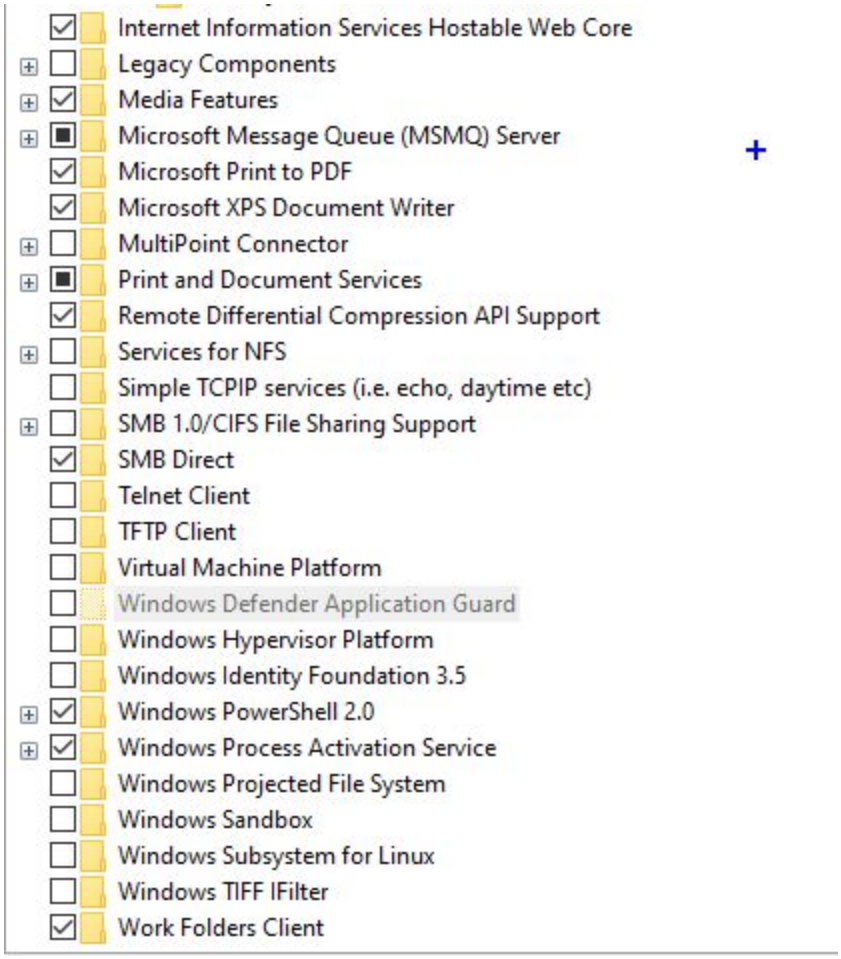


2. Click on Turn windows features on or off which is available on the left side panel




Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Guarded Host
Hyper-V
Internet Explorer 11
Internet Information Services
Internet Information Services Hostable Web Core
Legacy Components
Media Features
Microsoft Message Queue (MSMQ) Server
Microsoft Print to PDF
Microsoft XPS Document Writer
MultiPoint Connector
OK
Cancel
IIS
Deployment
the application

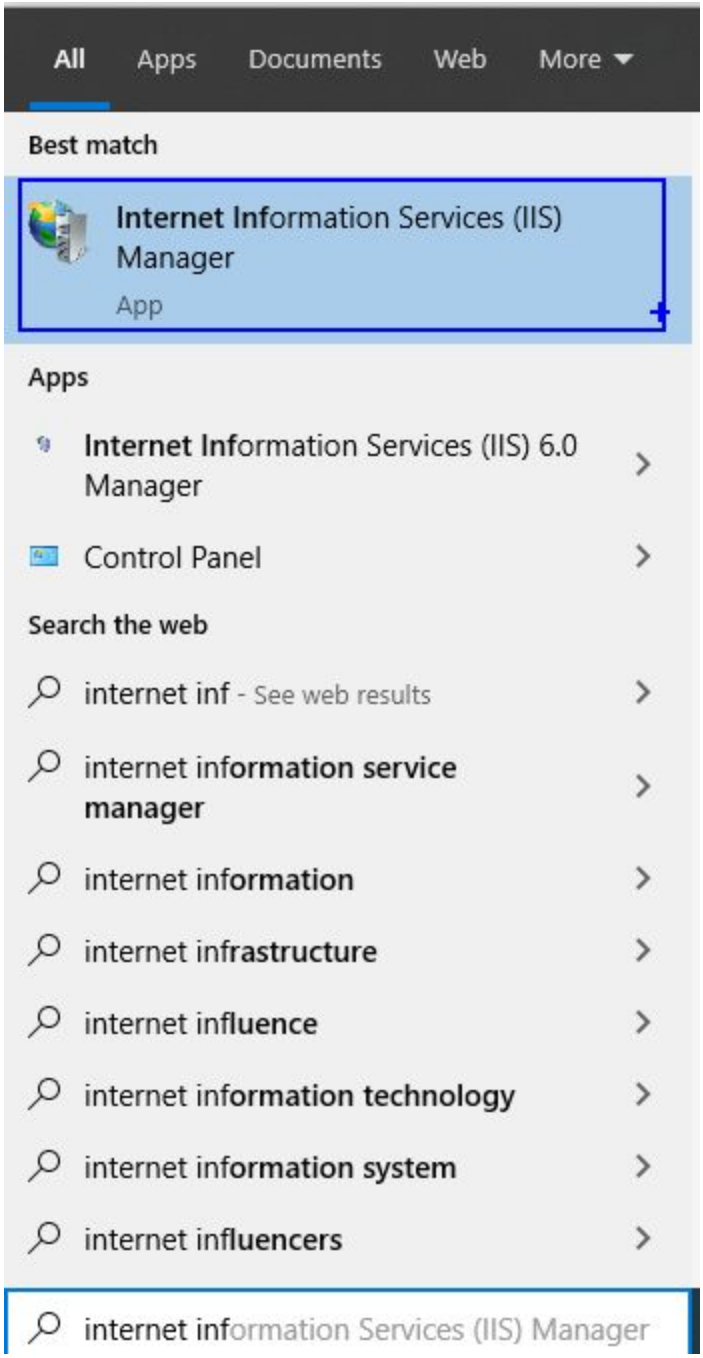

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Internet Explorer 11
Internet Information Services
FTP Server
FTP Extensibility
FTP Service
Web Management Tools
IIS 6 Management Compatibility
IIS 6 Management Console
IIS 6 Scripting Tools
IIS 6 WMI Compatibility
IIS Metabase and IIS 6 configuration compatibility
IIS Management Console
IIS Management Scripts and Tools
IIS Management Service
World Wide Web Services
Application Development Features
Common HTTP Features
Health and Diagnostics
Performance Features
Security
Internet Information Services Hostable Web Core
Legacy Components
Media Features
OK
Cancel

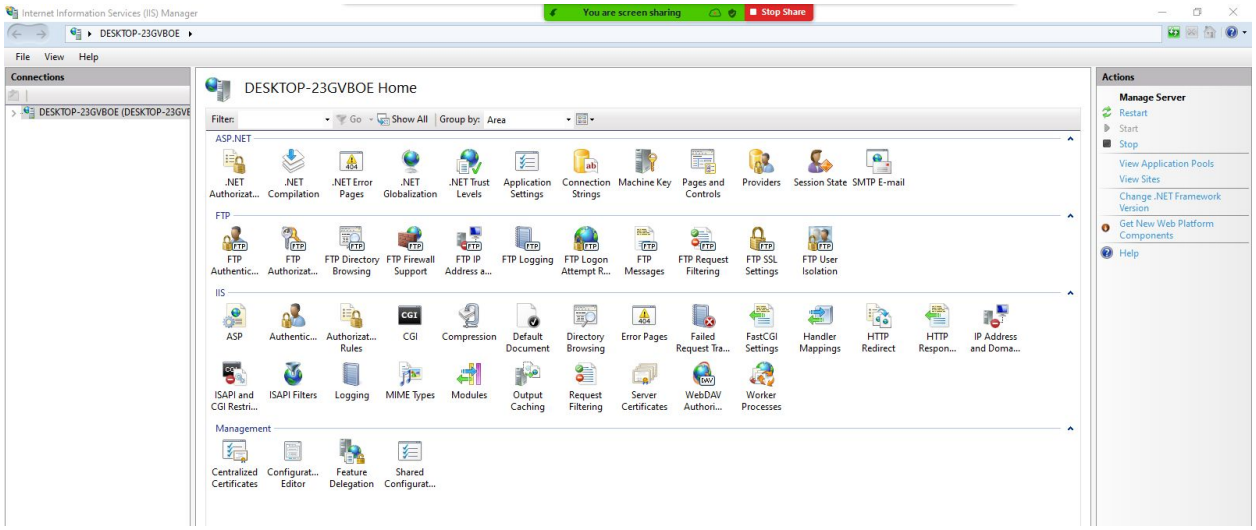


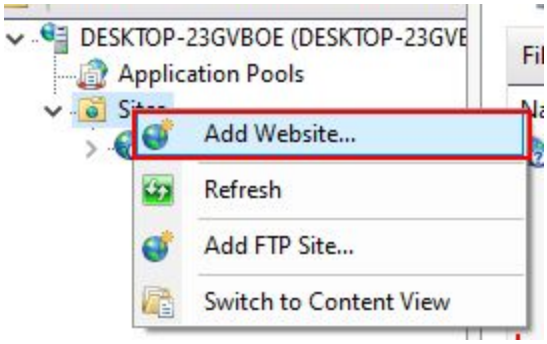
Deployment using IIS

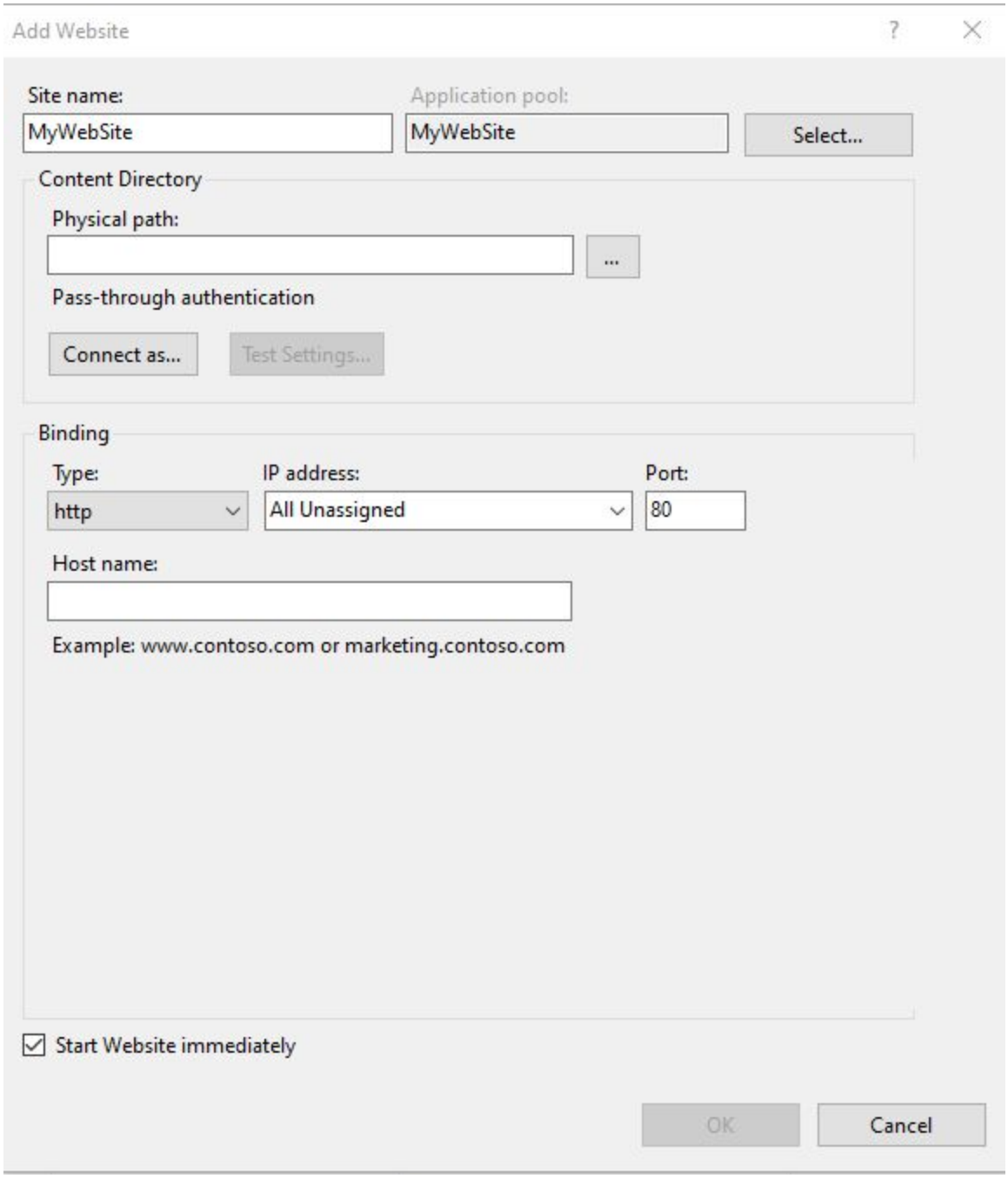
IIS: Internet Information Services which is available in all windows operating system to deploy the application

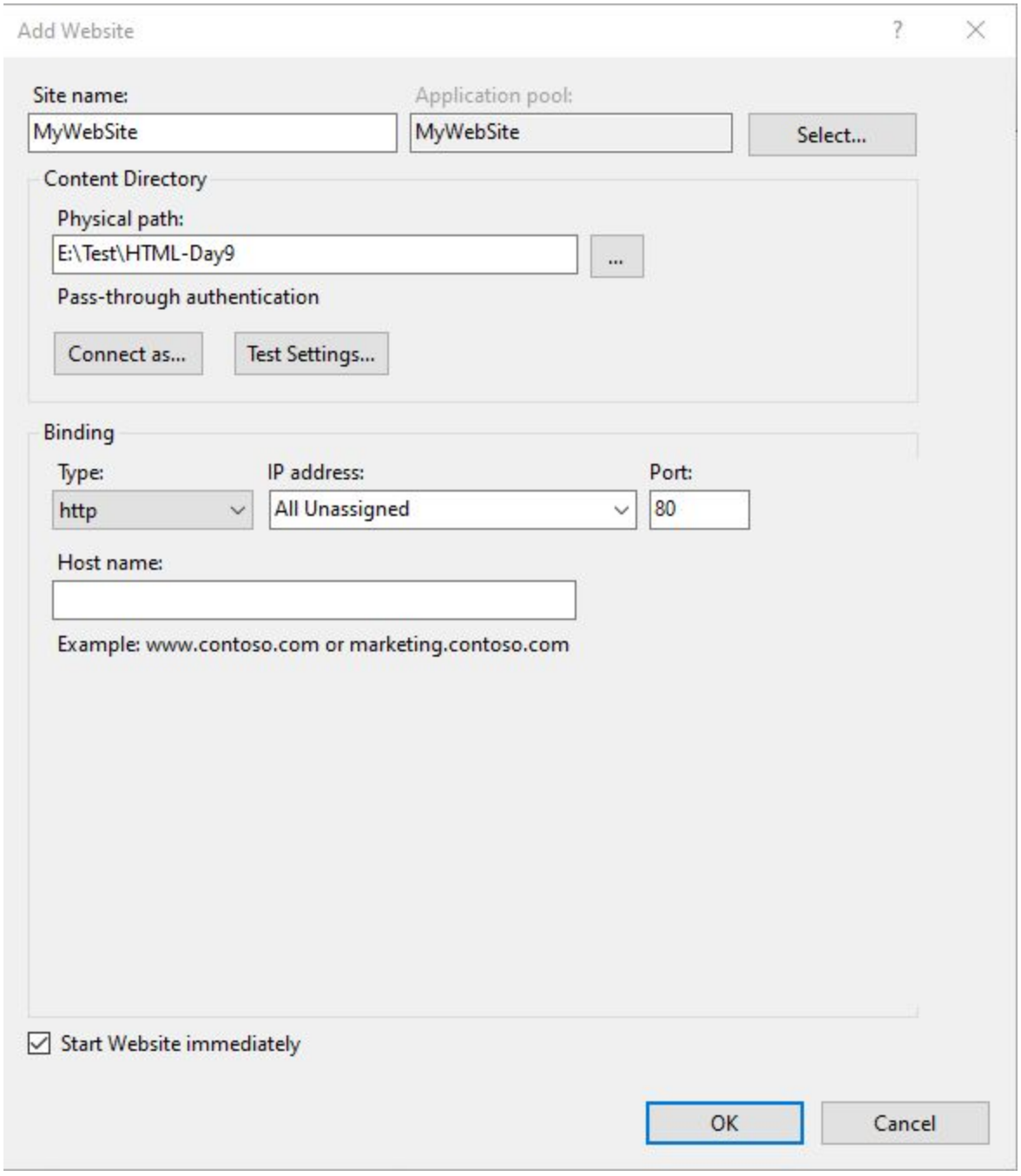
Open IIS

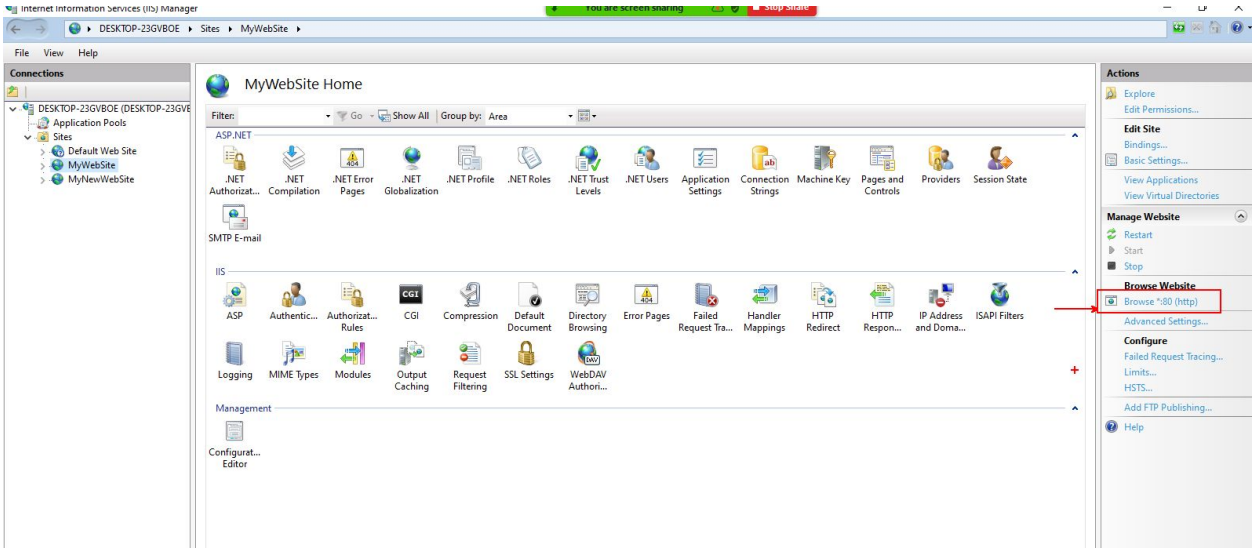

All
Apps
Documents
Web
More
Best match
Internet Information Services (IIS) Manager
App
Apps
Internet Information Services (IIS) 6.0 Manager
Control Panel
Search the web
internet inf - See web results
internet information service manager
internet information
internet infrastructure
internet influence
internet information technology
internet information system
internet influencers
internet information Services (IIS) Manager


Internet Information Services (IIS) Manager
You are screen sharing
Stop Share
DESKTOP-23GVBOE
File View Help
Connections
DESKTOP-23GVBOE (DESKTOP-23GVE
DESKTOP-23GVBOE Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Trust Levels
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
FTP
FTP Authentic...
FTP Authorizat...
FTP Directory Browsing
FTP Firewall Support
FTP IP Address a...
FTP Logging
FTP Logon Attempt R...
FTP Messages
FTP Request Filtering
FTP SSL Settings
FTP User Isolation
IIS
ASP
Authentic...
Authorizat... Rules
CGI
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
FastCGI Settings
Handler Mappings
HTTP Redirect
HTTP Respon...
IP Address and Doma...
ISAPI and CGI Restri...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
WebDAV Authori...
Worker Processes
Management
Centralized Certificates
Configurat... Editor
Feature Delegation
Shared Configurat...
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Change .NET Framework Version
Get New Web Platform Components
Help


DESKTOP-23GVBOE (DESKTOP-23GVE
Application Pools
Add Website...
Refresh
Add FTP Site...
Switch to Content View

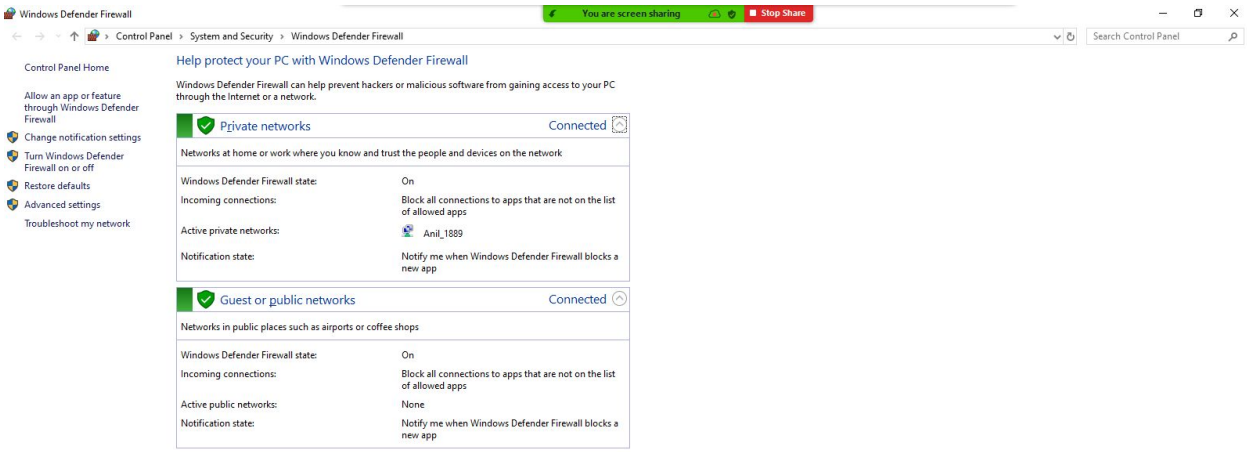

Add Website
Site name:
MyWebSite
Application pool:
MyWebSite
Select...
Content Directory
Physical path:
...
Pass-through authentication
Connect as...
Test Settings...
Binding
Type:
http
IP address:
All Unassigned
Port:
80
Host name:
Example: www.contoso.com or marketing.contoso.com
Start Website immediately
OK
Cancel

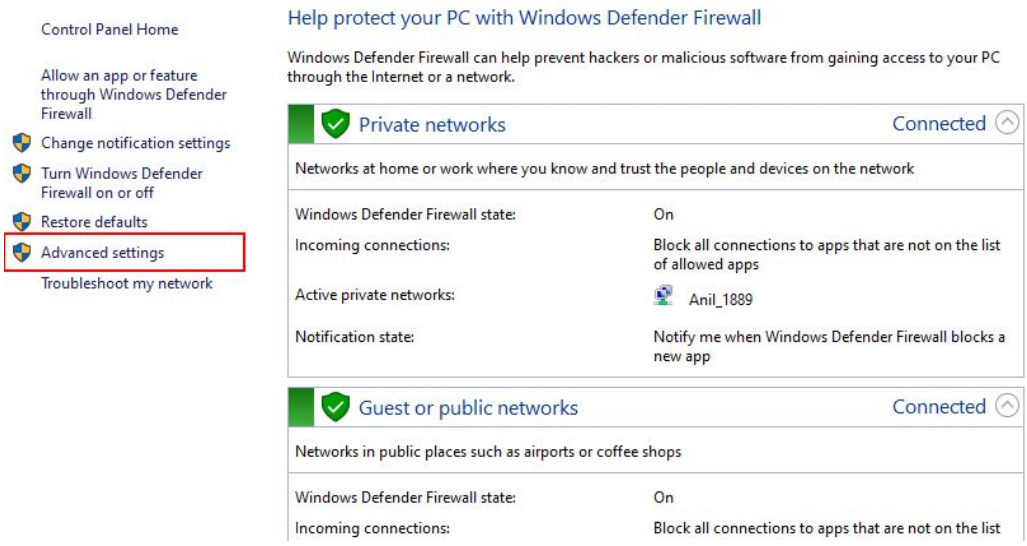

Add Website
Site name:
MyWebSite
Application pool:
MyWebSite
Select...
Content Directory
Physical path:
E:\Test\HTML-Day9
...
Pass-through authentication
Connect as...
Test Settings...
Binding
Type:
http
IP address:
All Unassigned
Port:
80
Host name:
Example: www.contoso.com or marketing.contoso.com
Start Website immediately
OK
Cancel

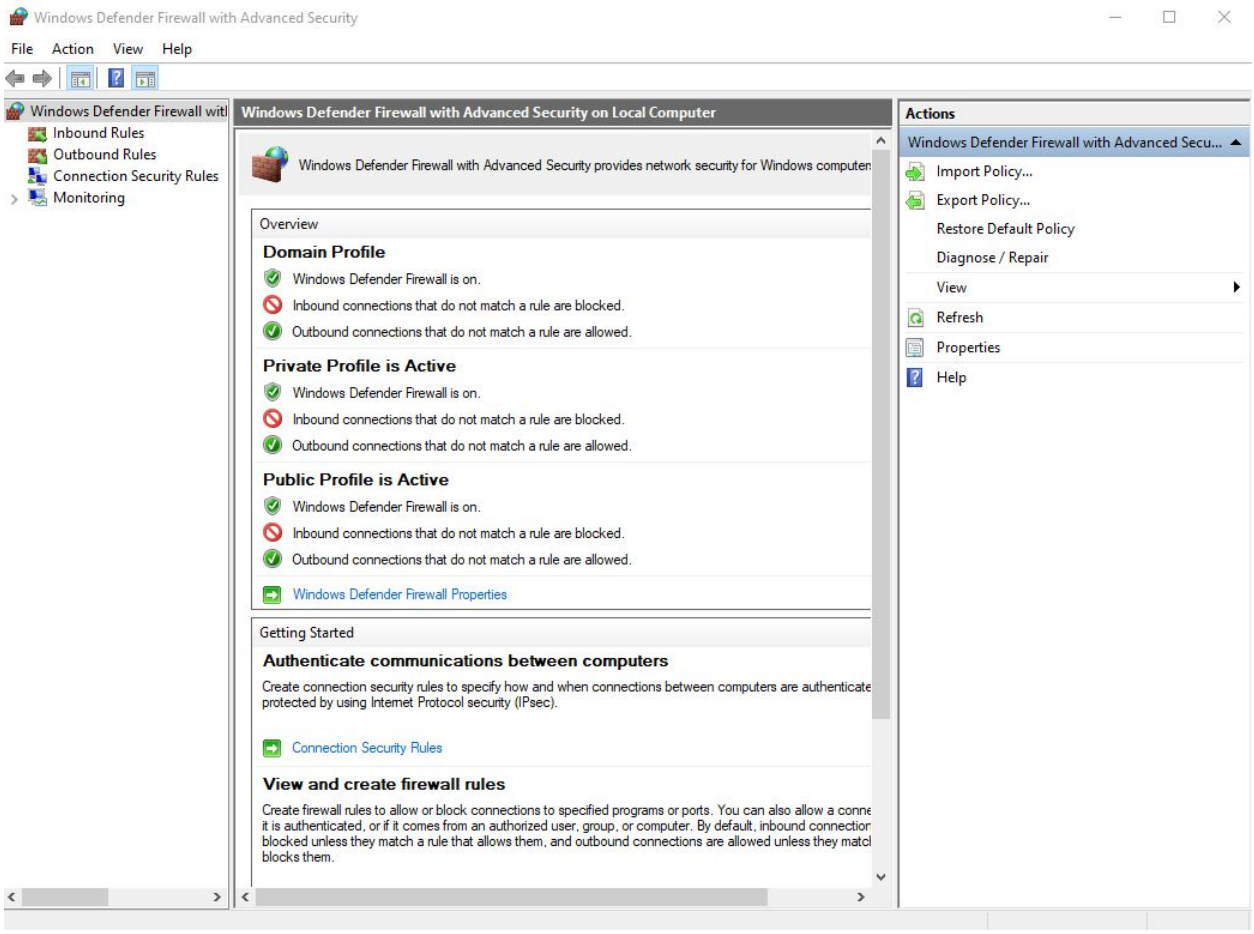


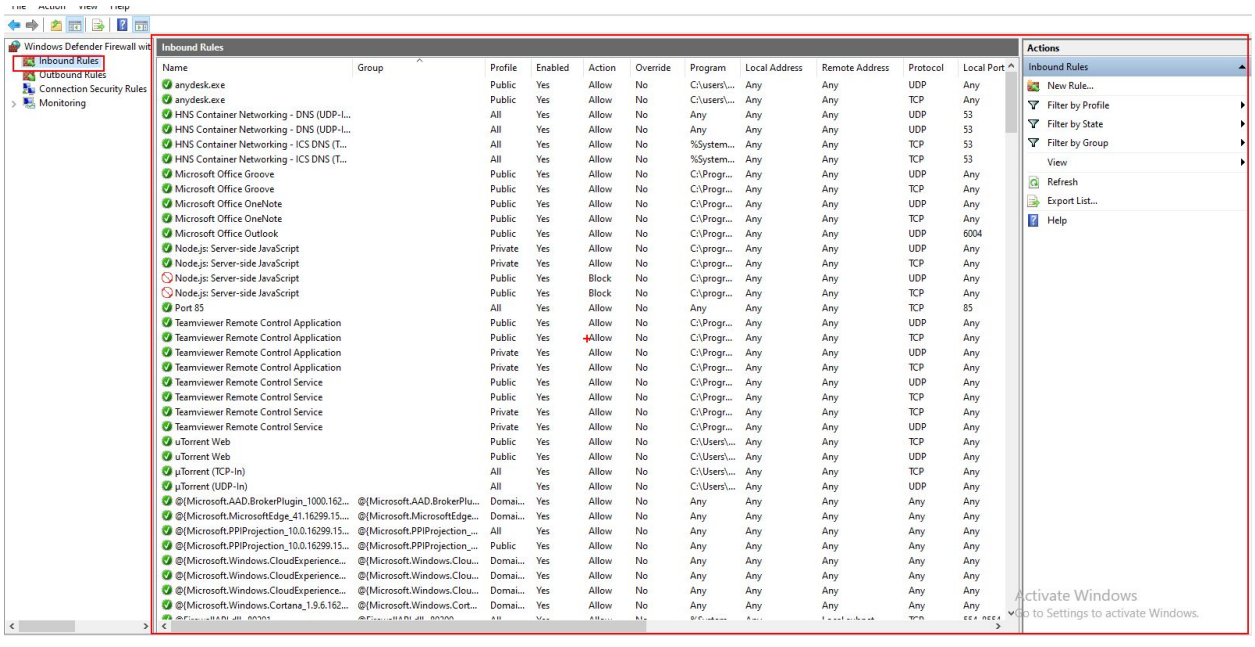
To make the input and output rules for port no 82

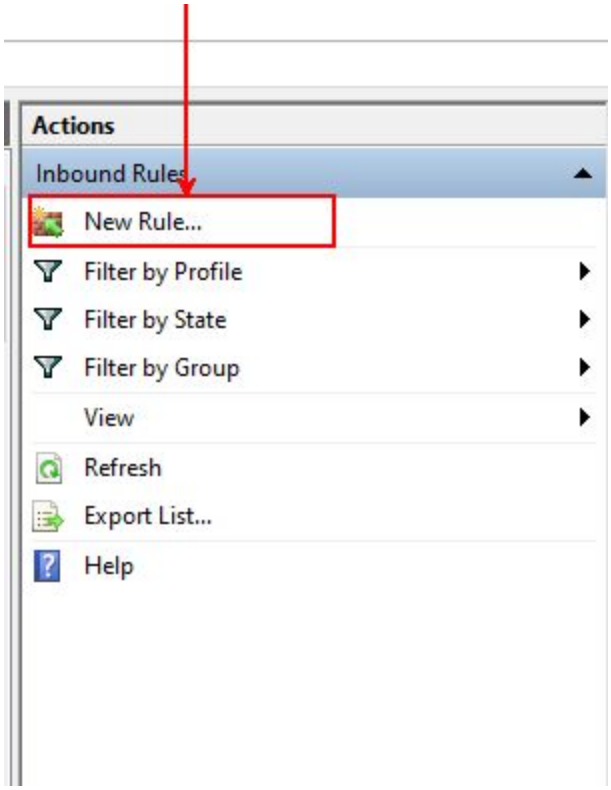
All
Apps
Documents
Web
More
Best match
Windows Defender Firewall
Control panel
Apps
Windows Defender Firewall with Advanced Security
Settings
Firewall & network protection
Allow an app through Windows Firewall
Windows Security
Find and fix problems with Windows Firewall
Search the web
windows fire - See web results
windows firewall
windows firefox
windows firestick
windows fire

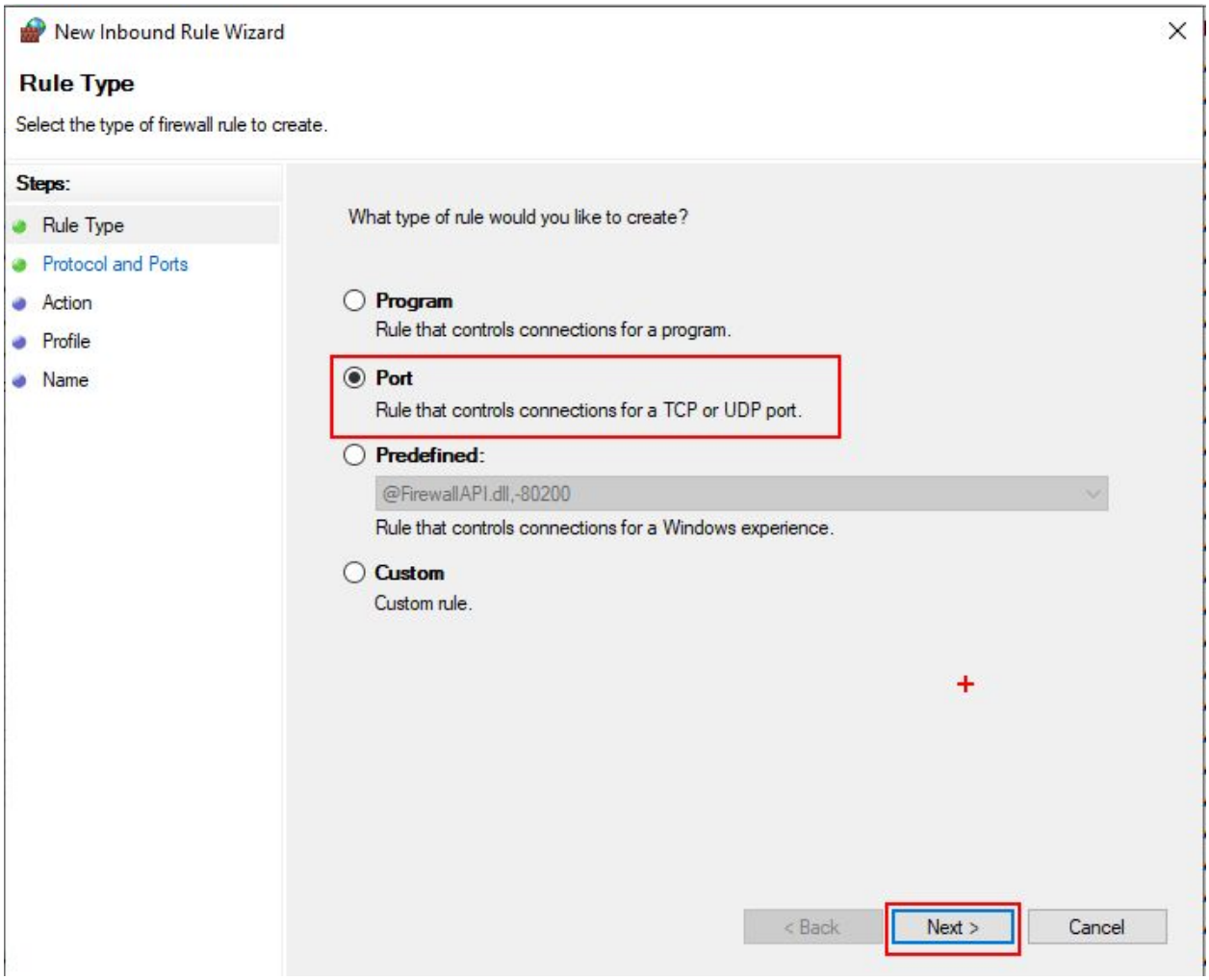

Windows Defender Firewall
You are screen sharing
Stop Share
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Connected
Networks at home or work where you know and trust the people and devices on the network
Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active private networks: Anil_1889
Notification state: Notify me when Windows Defender Firewall blocks a new app
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active public networks: None
Notification state: Notify me when Windows Defender Firewall blocks a new app

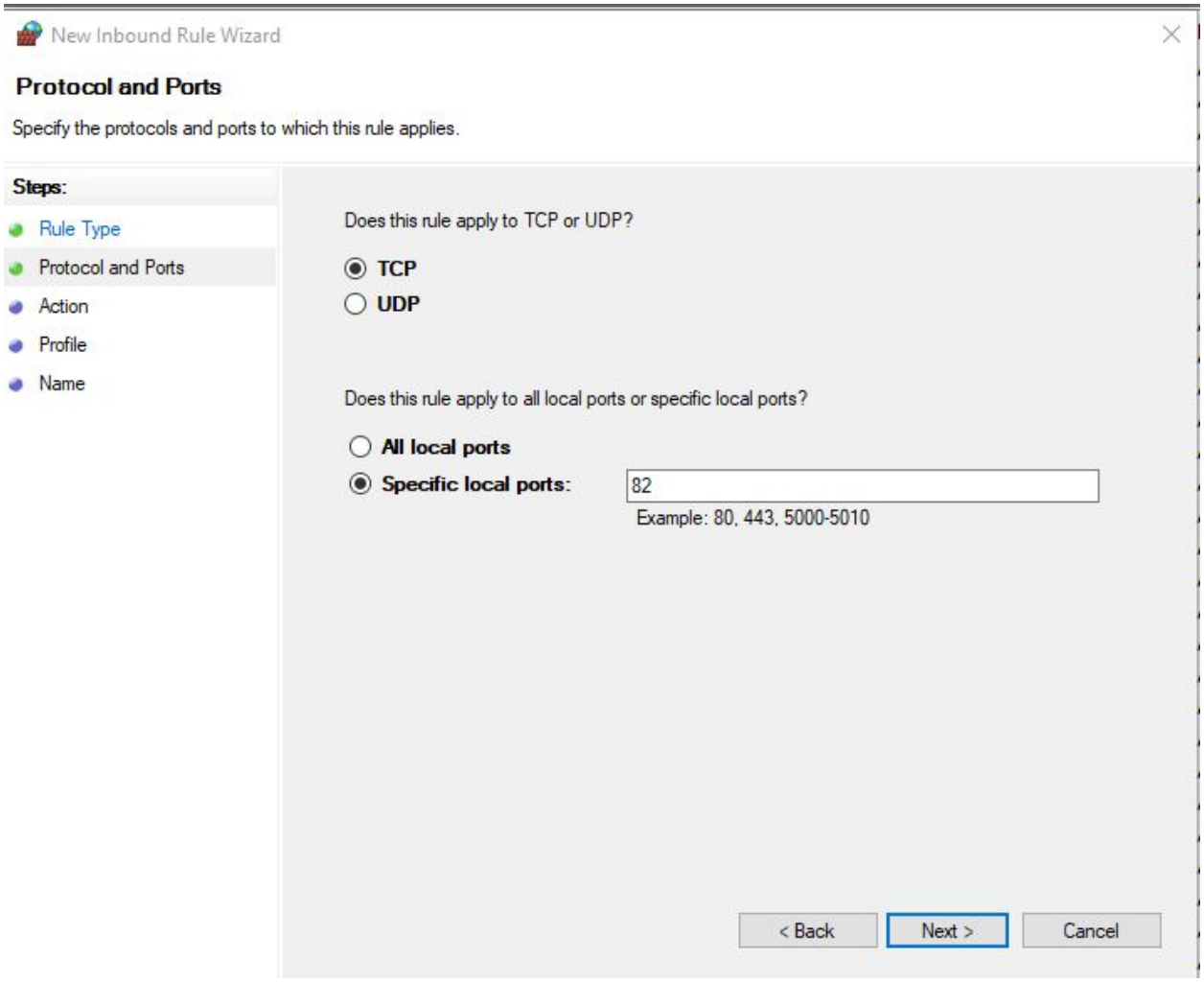

Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Connected
Networks at home or work where you know and trust the people and devices on the network
Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active private networks: Anil_1889
Notification state: Notify me when Windows Defender Firewall blocks a new app
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list

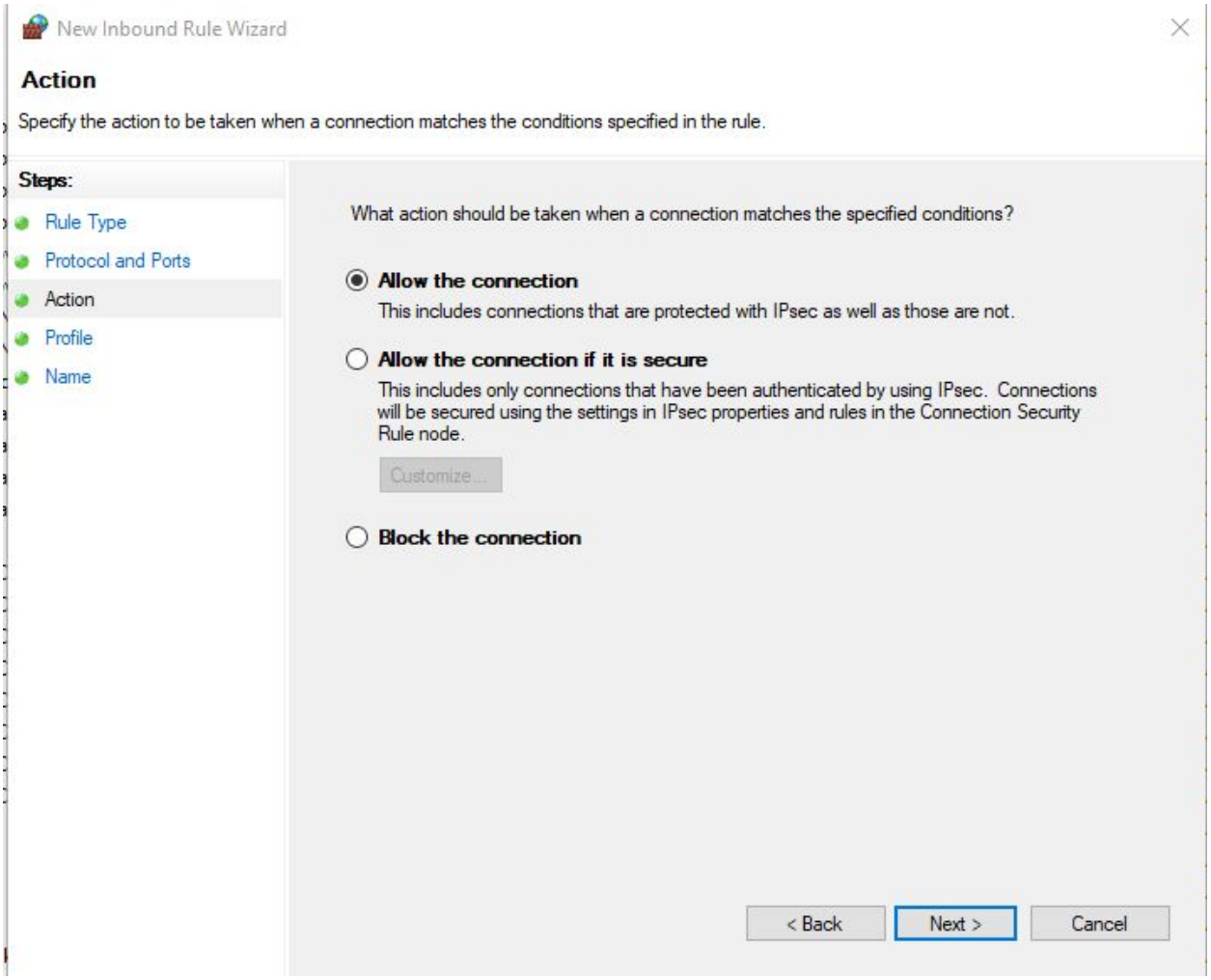

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for Windows computer
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticate
protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a conne
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connectior
blocked unless they match a rule that allows them, and outbound connections are allowed unless they matcl
blocks them.
Actions
Windows Defender Firewall with Advanced Secu...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

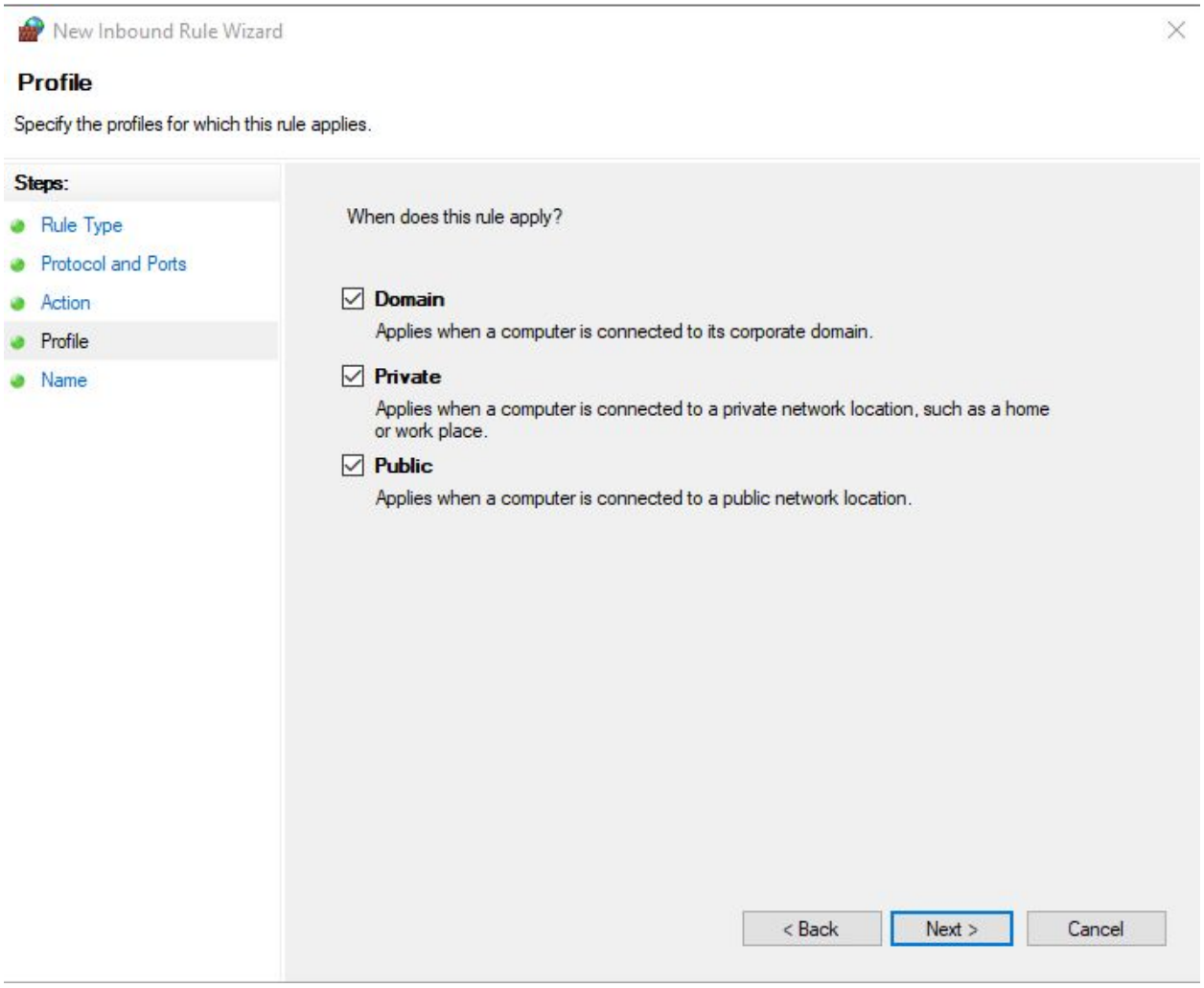

Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
New Rule...
Filter by Profile
Filter by State
Filter by Group
Refresh
Export List...
Help
Activate Windows

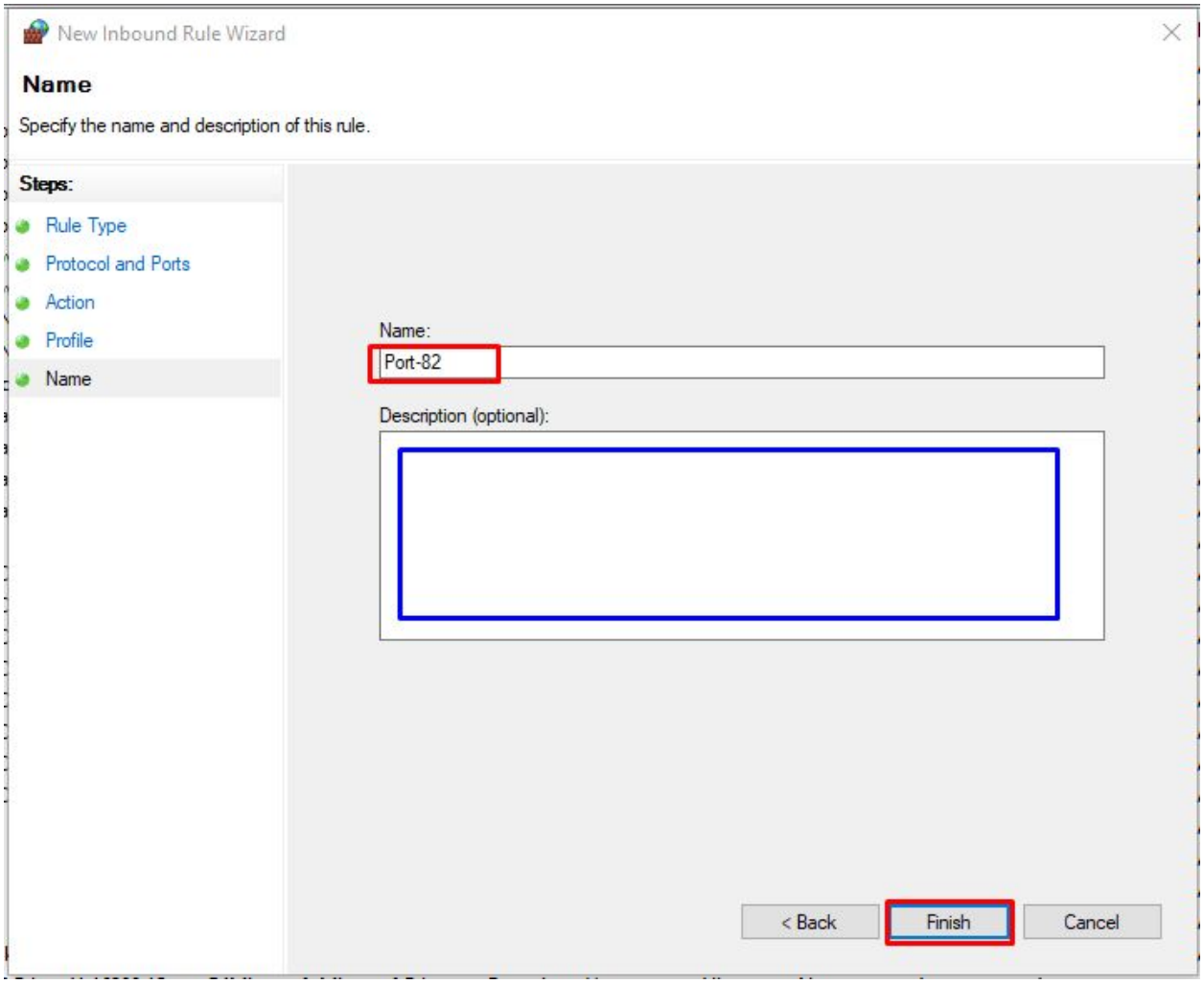

Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
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:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

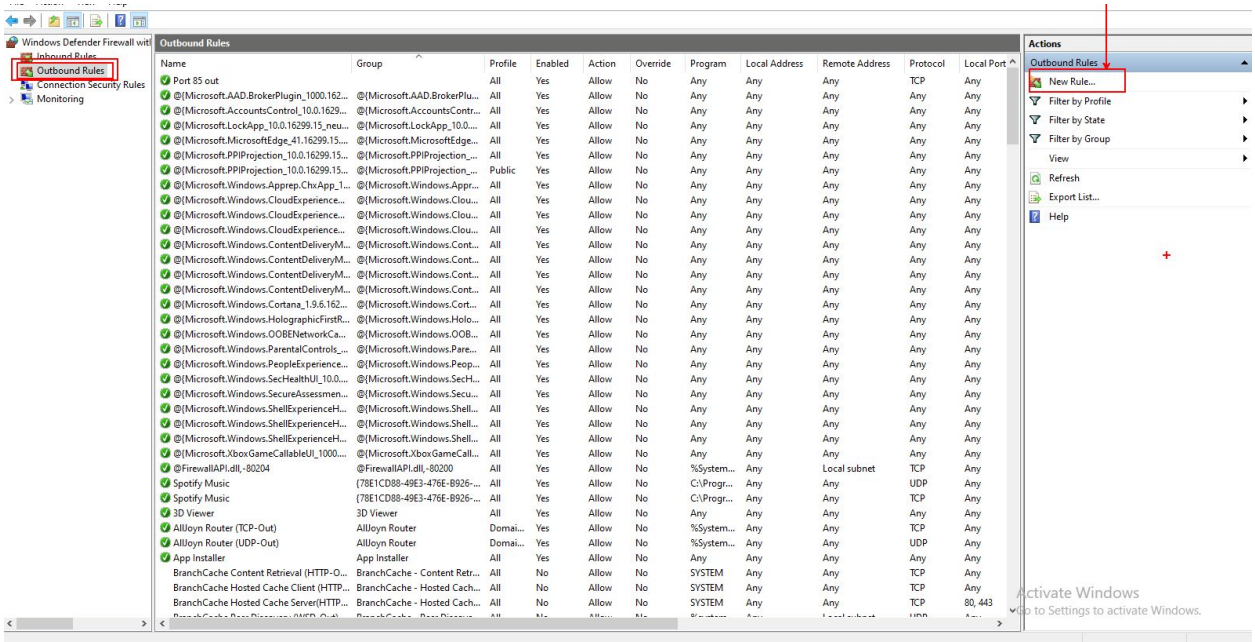

New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
82
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
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.
Customize...
Block the connection
< Back
Next >
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
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, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel



Need to create the Outbound rule as well



You need to same steps as like inbound rules and give any meaningful name at the last step

Task : Create a new Application or website in IIS with the port as 83, Create the inbound and outbound for the port no 83