بسمه تعالی

با توجه به مشکل به وجود آمده برای سرویس TeamViewer تا اطلاع ثانوی از سرویس ریموت ویندوز جهت ارتباط و پشتیبانی استفاده خواهد شد.

شرح مشکل:

عدم دریافت مشخصه کاربری و رمز عبور جهت ارتباط با نقاط مختلف.

راهکار جایگزین:

استفاده از سرویس Remote Desktop.

مراحل راه اندازی:

ابتدا در تنظیمات مودم باید بخشPort Forward یا DMZ را فعال نمایید.مشخصات لازم جهت پر کردن اطلاعات این مورد بدین شرح است:

تنظیمات روی مودم:

Income Port: 3389

Income Port start: 3389

Income Port End: 3389

Remote Port: 3389

Remote Port Start: 3389

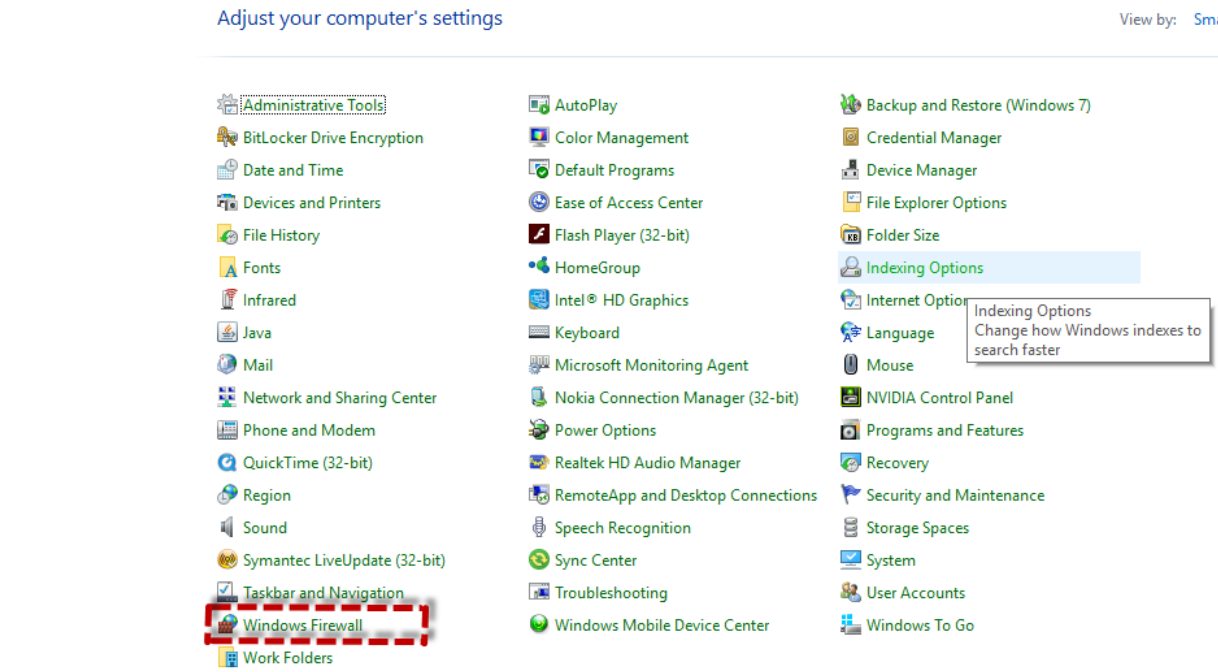
Remote Port End: 3389

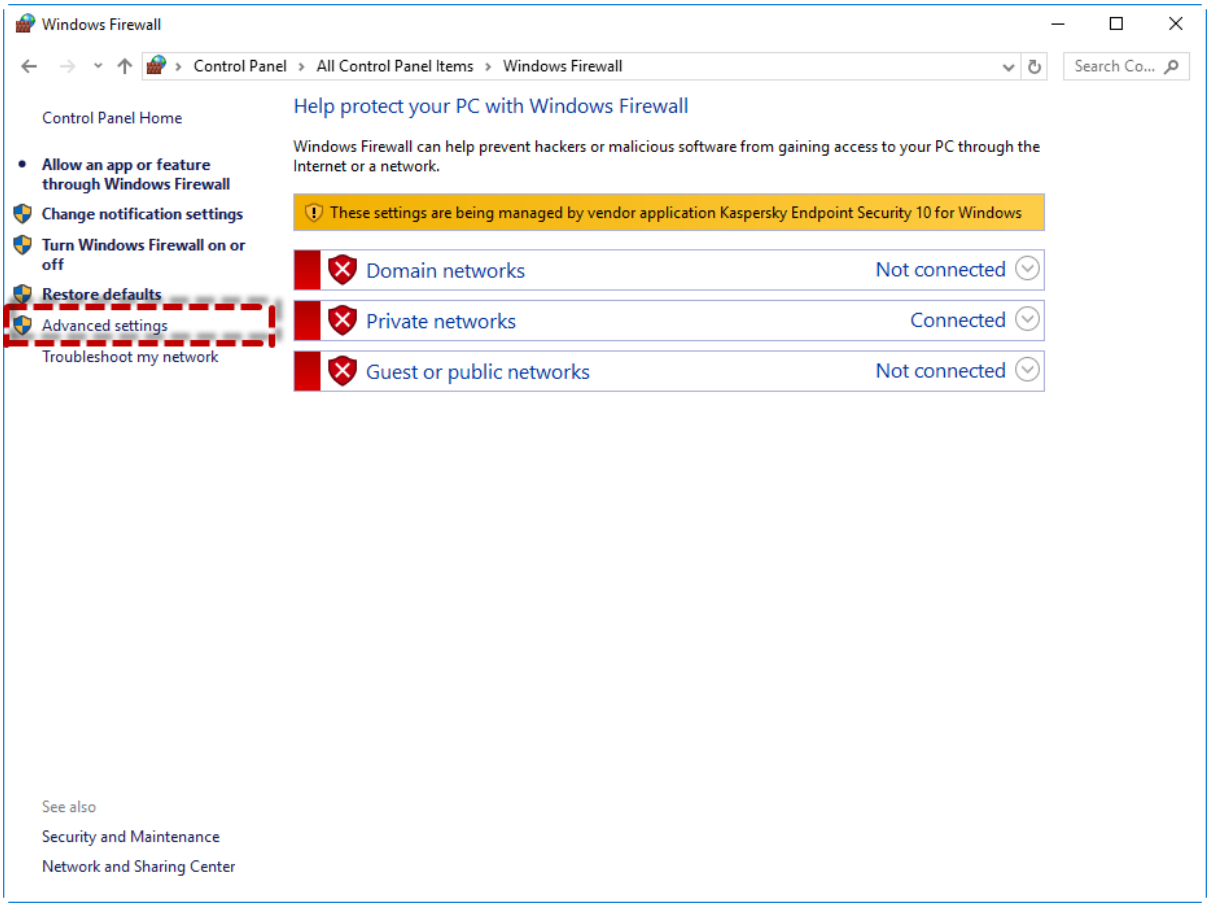
Remote IP: 192.168.1.100(ادرس سروری که میخواهید بتوان رو آن ریموت شد را وارد نمایید)

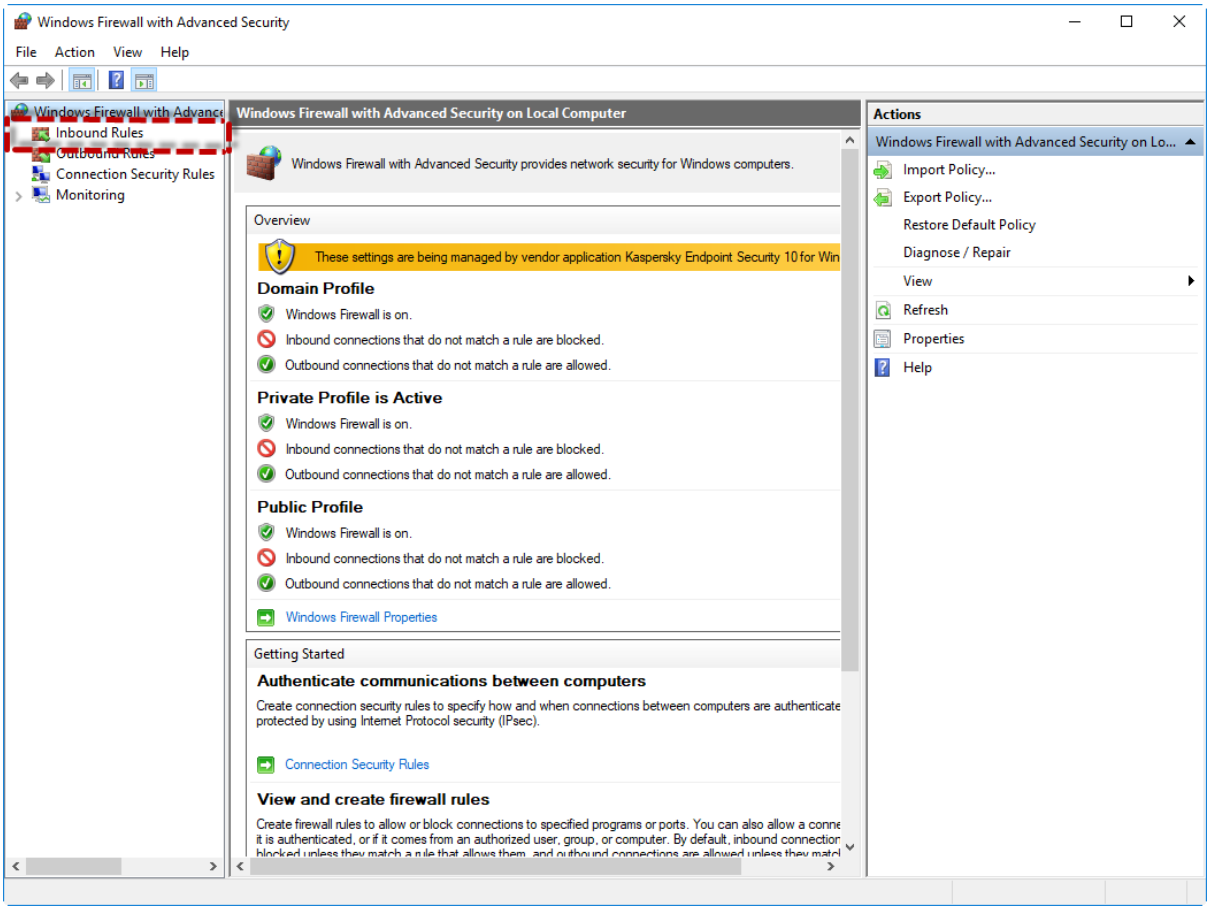
Protocol: TCP/UDP

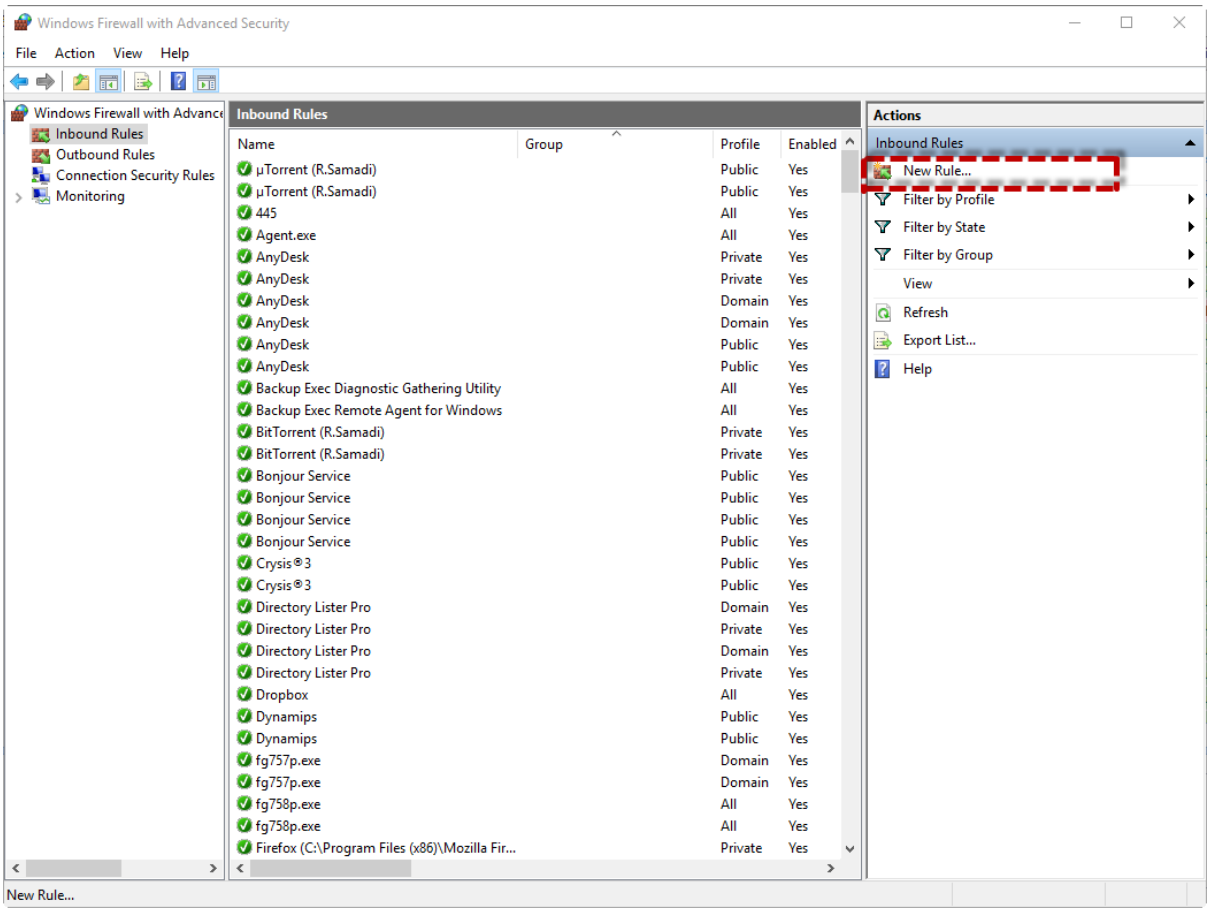
تنظیمات روی سرور:

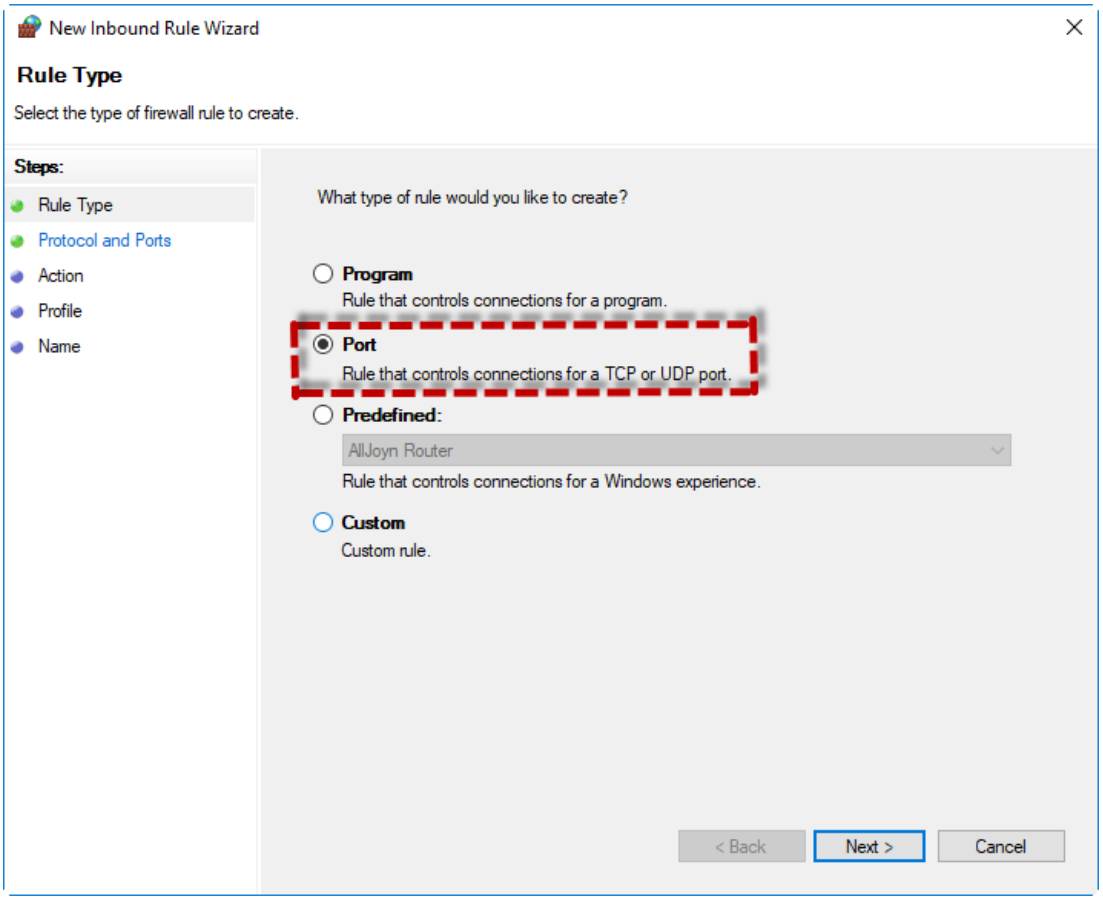
ایتدا فایروال را تنظیم نمایید به نحوی که بتوان به آن سرور ریموت شد. برای اینکار طبق عکسهای زیر عمل کنید:

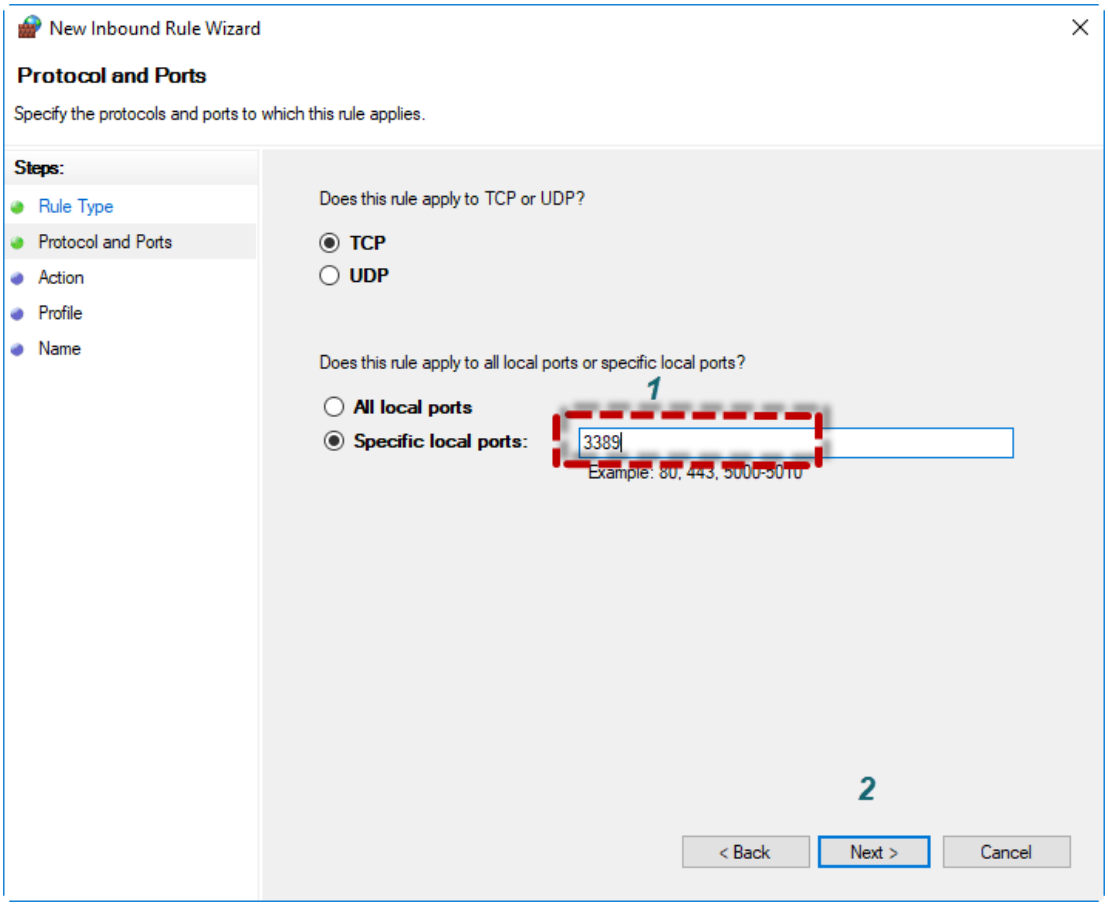

Adjust your computer's settings
View by: Small icons
Administrative Tools
BitLocker Drive Encryption
Date and Time
Devices and Printers
File History
Fonts
Infrared
Java
Mail
Network and Sharing Center
Phone and Modem
QuickTime (32-bit)
Region
Sound
Symantec LiveUpdate (32-bit)
Taskbar and Navigation
Windows Firewall
Work Folders
AutoPlay
Color Management
Default Programs
Ease of Access Center
Flash Player (32-bit)
HomeGroup
Intel® HD Graphics
Keyboard
Microsoft Monitoring Agent
Nokia Connection Manager (32-bit)
Power Options
Realtek HD Audio Manager
RemoteApp and Desktop Connections
Speech Recognition
Sync Center
Troubleshooting
Windows Mobile Device Center
Backup and Restore (Windows 7)
Credential Manager
Device Manager
File Explorer Options
Folder Size
Indexing Options
Internet Options
Language
Mouse
NVIDIA Control Panel
Programs and Features
Recovery
Security and Maintenance
Storage Spaces
System
User Accounts
Windows To Go
Indexing Options
Change how Windows indexes to search faster

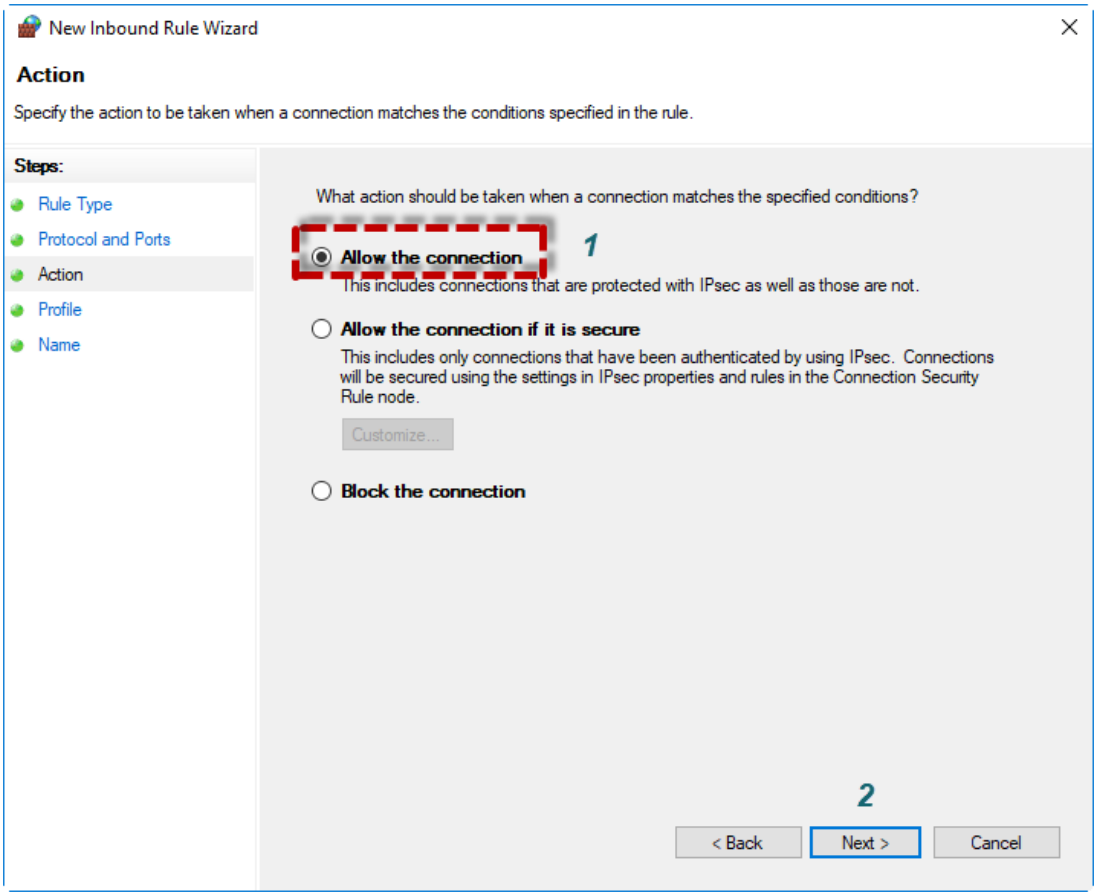

Windows Firewall
Control Panel › All Control Panel Items › Windows Firewall
Search Co...
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
These settings are being managed by vendor application Kaspersky Endpoint Security 10 for Windows
Domain networks
Not connected
Private networks
Connected
Guest or public networks
Not connected
See also
Security and Maintenance
Network and Sharing Center

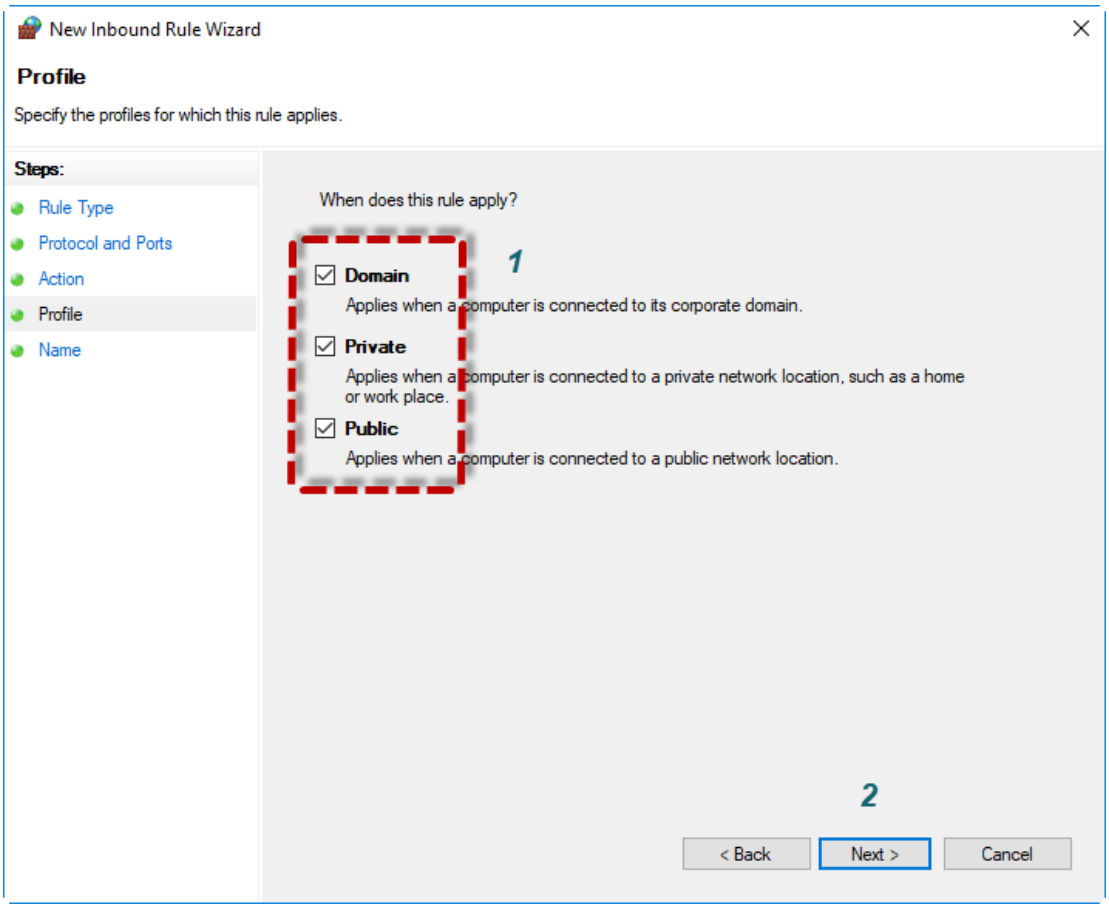

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
These settings are being managed by vendor application Kaspersky Endpoint Security 10 for Win
Domain Profile
Windows 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 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
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows 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
Actions
Windows Firewall with Advanced Security on Lo...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

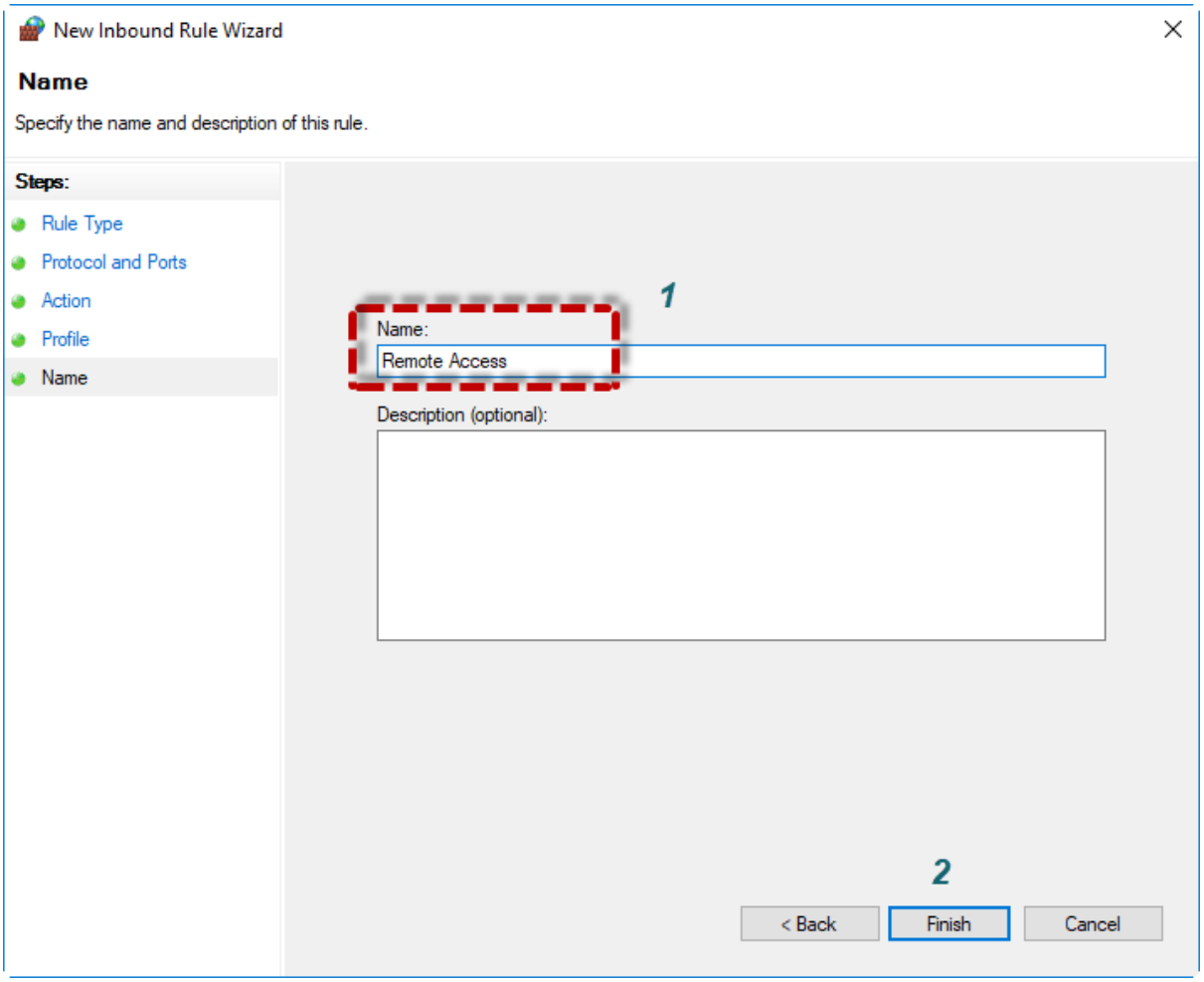

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled
µTorrent (R.Samadi) Public Yes
µTorrent (R.Samadi) Public Yes
445 All Yes
Agent.exe All Yes
AnyDesk Private Yes
AnyDesk Private Yes
AnyDesk Domain Yes
AnyDesk Domain Yes
AnyDesk Public Yes
AnyDesk Public Yes
Backup Exec Diagnostic Gathering Utility All Yes
Backup Exec Remote Agent for Windows All Yes
BitTorrent (R.Samadi) Private Yes
BitTorrent (R.Samadi) Private Yes
Bonjour Service Public Yes
Bonjour Service Public Yes
Bonjour Service Public Yes
Bonjour Service Public Yes
Crysis® 3 Public Yes
Crysis® 3 Public Yes
Directory Lister Pro Domain Yes
Directory Lister Pro Private Yes
Directory Lister Pro Domain Yes
Directory Lister Pro Private Yes
Dropbox All Yes
Dynamips Public Yes
Dynamips Public Yes
fg757p.exe Domain Yes
fg757p.exe Domain Yes
fg758p.exe All Yes
fg758p.exe All Yes
Firefox (C:\Program Files (x86)\Mozilla Fir... Private Yes
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Rule...


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:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

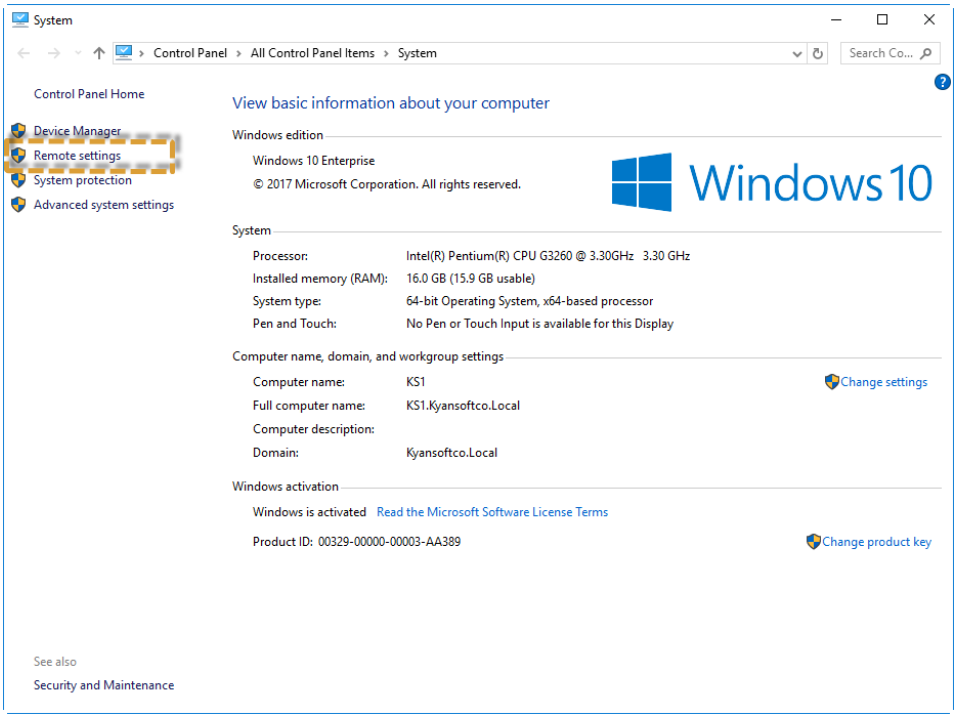

New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
1
All local ports
Specific local ports:
3389
Example: 80, 443, 5000-5010
2
< Back
Next >
Cancel

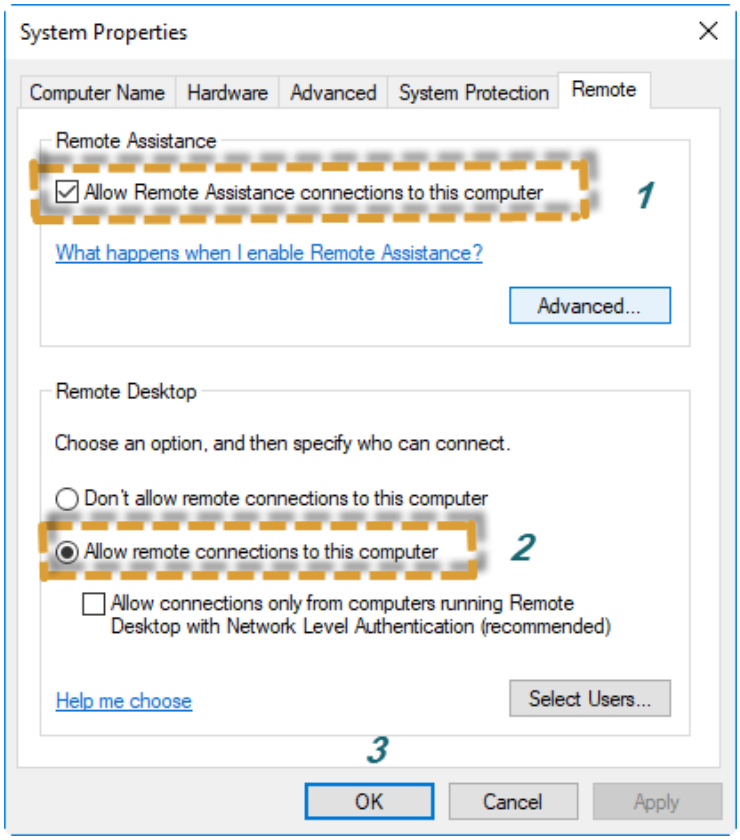

New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
1
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
2
< 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.
1
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.
2
< Back
Next >
Cancel



با انجام این مراحل فایروال مانع عبور درخواست ریموت نخواهد شد. حال با کلیک راست رو کامپیوتر و انتخاب گزینه Properties مراحل زیر را پیگیری نمایید:





حال با ارائه یوزر و پسورد ویندوز، همکاران ما میتوانند به صورت ریموتی مشکل را رفع نمایند.