

The Set Port windows Firewall if the access cannot through IP Address.

The case for others to follow URL cannot use them for use the set Port Windows Firewall Outbound Rule by creating Inbound Rule.

Steps to Set Port Windows Firewall.

1. The user clicks a button, "Start"> "Control Panel".



2. The user selects "Windows Firewall".





3. Select the user "Advanced settings".



4. Select the user clicks the button "Inbound Rules"> "New Rule ...".





5. The system displays the New Inbound Rule Wizard window appears, click the "Port" > "Next".

Prev Inbound Rule Wizard	×
Rule Type Select the type of firewall rule to c	preate.
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. P Pot Rule that controls connections for a TCP or UDP port. Predefined: BranchCache - Content Retrieval (Uses HTTP) Rule that controls connections for a Windows experience. C storm Custom rule. Leam more about rule types < Back Cancel

6. The user clicks the button, select "TCP" and "Specific local ports :" after finish filling click "Next "

💣 New Inbound Rule Wiz	ard X
Protocol and Ports	
Specify the protocols and ports	s to which this rule applies.
Steps:	
Rule Type	Does this rule apply to TCP or UDP?
Protocol and Ports	● TCP
Action	⊖ UDP
Profile	
Name	Does this rule apply to all local ports or specific local ports?
	○ All local ports
	Specific local ports: 3344
	Example: 80, 443, 5000-5010
	< Back Next > Cancel



7. Users to click a button to choose "Allow the Connection"> "Next>".

Action	
Specify the action to be taken	when a connection matches the conditions specified in the rule.
Steps:	
Rule Type	What action should be taken when a connection matches the specified conditions?
Protocol and Ports	Allow the connection
Action	This includes connections that are protected with IPsec as well as those are not.
Profile	Allow the connection if it is secure
I IVerine	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
	Learn more about actions

8. The user clicks the button, select "Domain" "Private" and "Public"> "Next>".

Profile Specify the profiles for which the	is rule applies.
Steps:	
Rule Type	When does this rule apply?
Protocol and Ports	
Action	Applies when a computer is connected to its corporate domain.
 Name 	 Private Applies when a computer is connected to a private network location. Public Applies when a computer is connected to a public network location.
	Learn more about profiles < Back Next > Cancel



9. Users to enter their name in the "Name:" this will fill in the name of Port set for easy searching. When done, click the button named "Finish".

💣 New Inbound Rule Wizar	d	>
Name		
Specify the name and description	n of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name	3344	
	Description (optional):	
	< Back Fini	sh Cancel

10. Then the user settings menu "Outbound Rules"> "New Rule..." The next step is the same as the "Inbound Rule".

Action View Help				
Vindows Firewall with Advance	Outbound Rules			Actions
Inbound Rules	Name	Group	-	Outbound Rules
Connection Security Rules	BranchCache Content Retrieval (HTTP-O	BranchCache - Content Retr	_	New Rule
Monitoring	 BranchCache Hosted Cache Client (HTT BranchCache Hosted Cache Server(HTTP BranchCache Peer Discovery (WSD-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev 	BranchCache - Hosted Cach BranchCache - Hosted Cach BranchCache - Peer Discove Connect to a Network Proje Connect to a Network Proje Connect to a Network Proje Connect to a Network Proje Connect to a Network Proje		 Filter by Profile Filter by State Filter by Group View Refresh Export List Help
	Core Networking - DNS (UDP-Out)	Core Networking		BranchCache Cont.
	Core Networking - Dynamic Host Config Core Networking - Dynamic Host Config Core Networking - Group Policy (LSASS Core Networking - Group Policy (NP-Out) Core Networking - Group Policy (NP-Out)	Core Networking Core Networking Core Networking Core Networking		Cut
	Core Networking - Group Policy (TCP-O Core Networking - Internet Group Mana Core Networking - IPHTTPS (TCP-Out)	Core Networking Core Networking Core Networking	-	Properties Help