

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:

22

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

Actions

Inbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

Allow SSH

Disable Rule

Cut

Copy

Delete

Properties

Help

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



## 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