

Lesson 19: Configuring Windows Firewall

MOAC 70-410: Installing and Configuring
Windows Server 2012

Overview

- Exam Objective 6.4: Configure Windows Firewall
- Building a Firewall
- Using the Windows Firewall Control Panel
- Using the Windows Firewall with Advanced Security Console

Building a Firewall

Lesson 19: Configuring Windows Firewall

Building a Firewall

- A **firewall** is a software program that protects a computer or a network by allowing certain types of network traffic in and out of the system while blocking others.
- A firewall is essentially a series of filters that examine the contents of packets and the traffic patterns to and from the network to determine which packets they should allow to pass through the filter.

Firewalls Protect Against:

- Network scanner applications that probe systems for unguarded ports, which are essentially unlocked doors that attackers can use to gain access to the system.
- Trojan horse applications that open a connection to a computer on the Internet, enabling an attacker on the outside to run programs or store data on the system.
- Attackers that obtain passwords by illicit means, such as social engineering, and then use remote access technologies to log on to a computer from another location and compromise its data and programming.
- Denial of service attacks that use authorized access points to bombard a system with traffic, preventing legitimate traffic from reaching the computer.

Firewall Settings

The three most important criteria that firewalls can use in their rules are:

- **IP addresses:** Identify specific hosts on the network. You can use IP addresses to configure a firewall to allow only traffic from specific computers or networks in and out.
- **Protocol numbers:** Specify whether the packet contains TCP or UDP (User Datagram Protocol) traffic. You can filter protocol numbers to block packets containing certain types of traffic.
- **Port numbers:** Identify specific applications running on the computer. The most common firewall rules use port numbers to specify the types of application traffic the computer is allowed to send and receive.

Firewall Settings

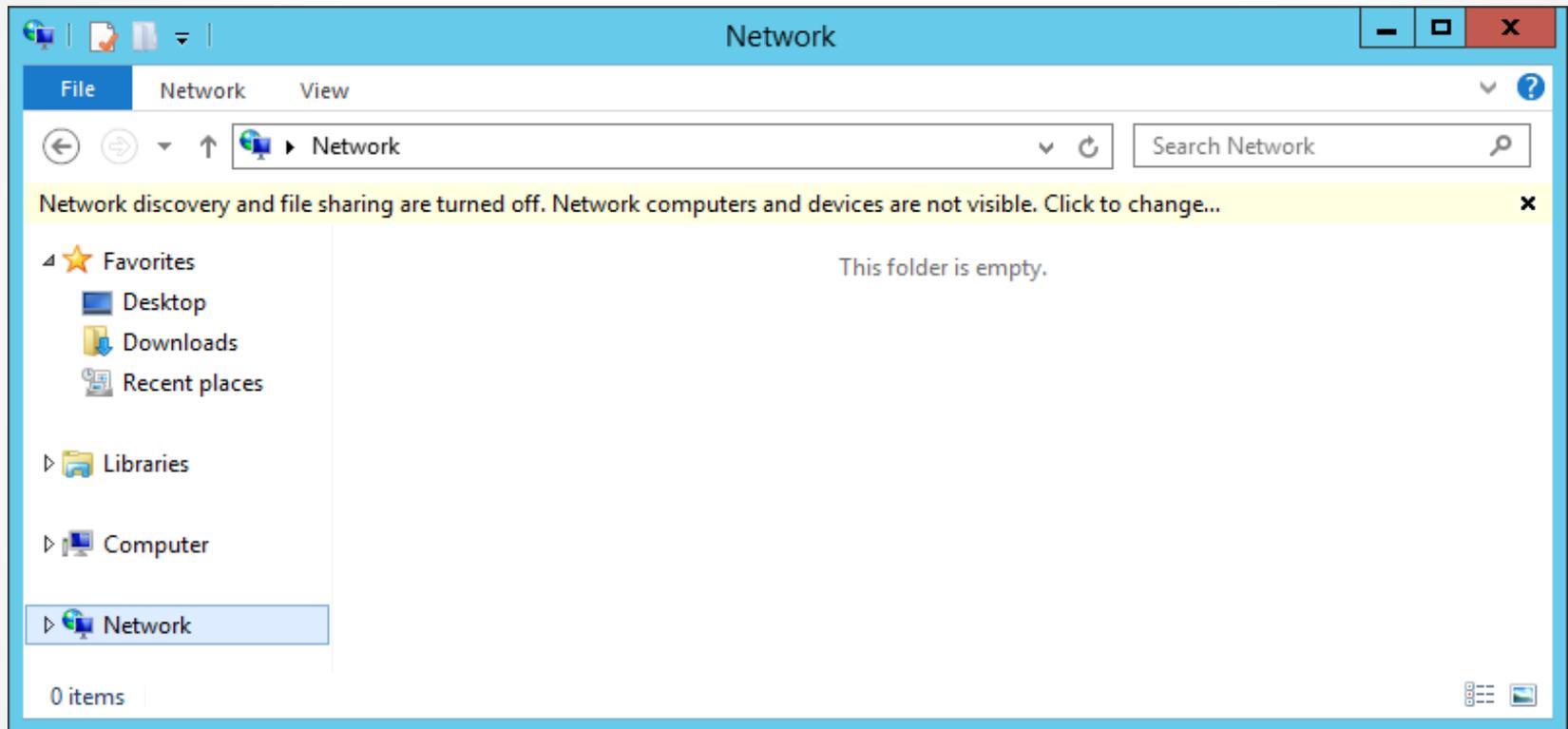
Firewall rules can function in two ways:

- **Admit all traffic**, except that which conforms to the applied rules
- **Block all traffic**, except that which conforms to the applied rules

Working with Windows Firewall

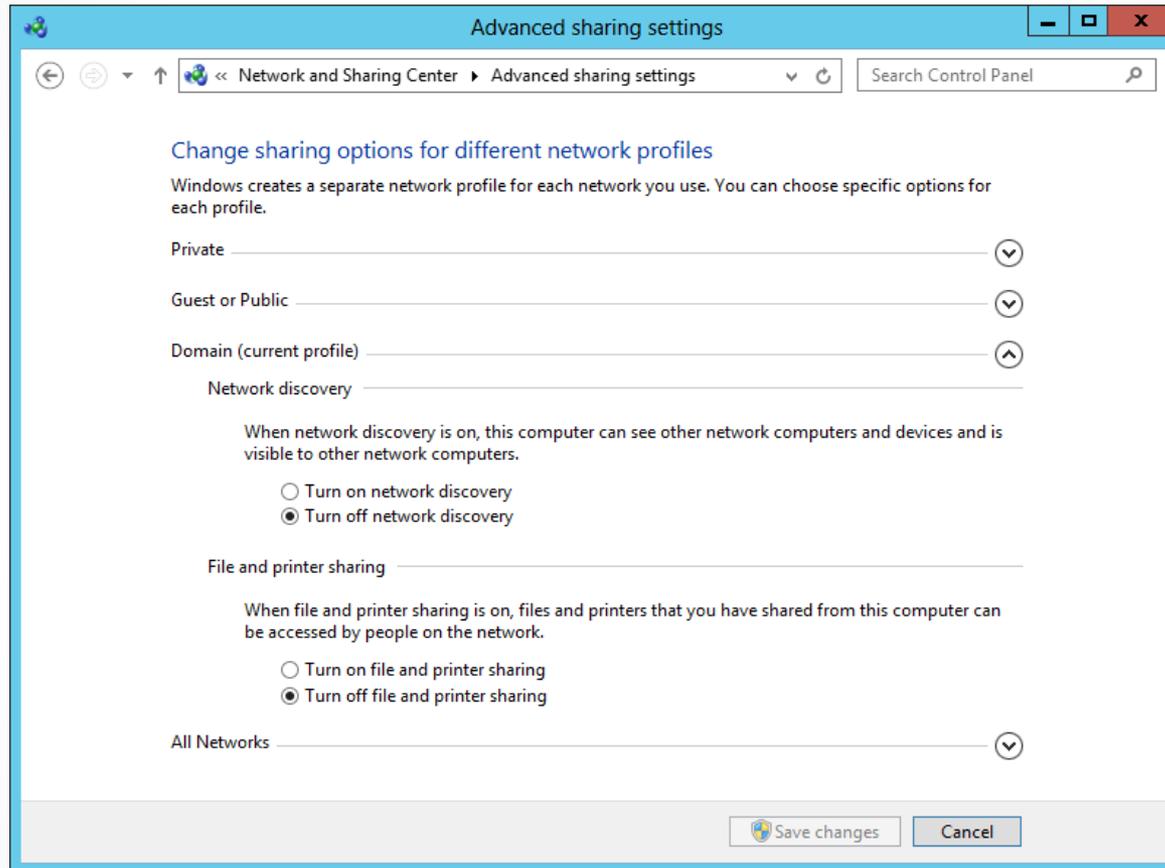
- The **Windows Firewall control panel** provides a simplified interface that enables you to avoid the details of rules and port numbers.
- For full access to firewall rules and more sophisticated functions, you must use the **Windows Firewall with Advanced Security console**.
- Many of the roles and features included in Windows Server 2012 automatically open the appropriate firewall ports when you install them.
- The system warns you of firewall issues.

Working with Windows Firewall



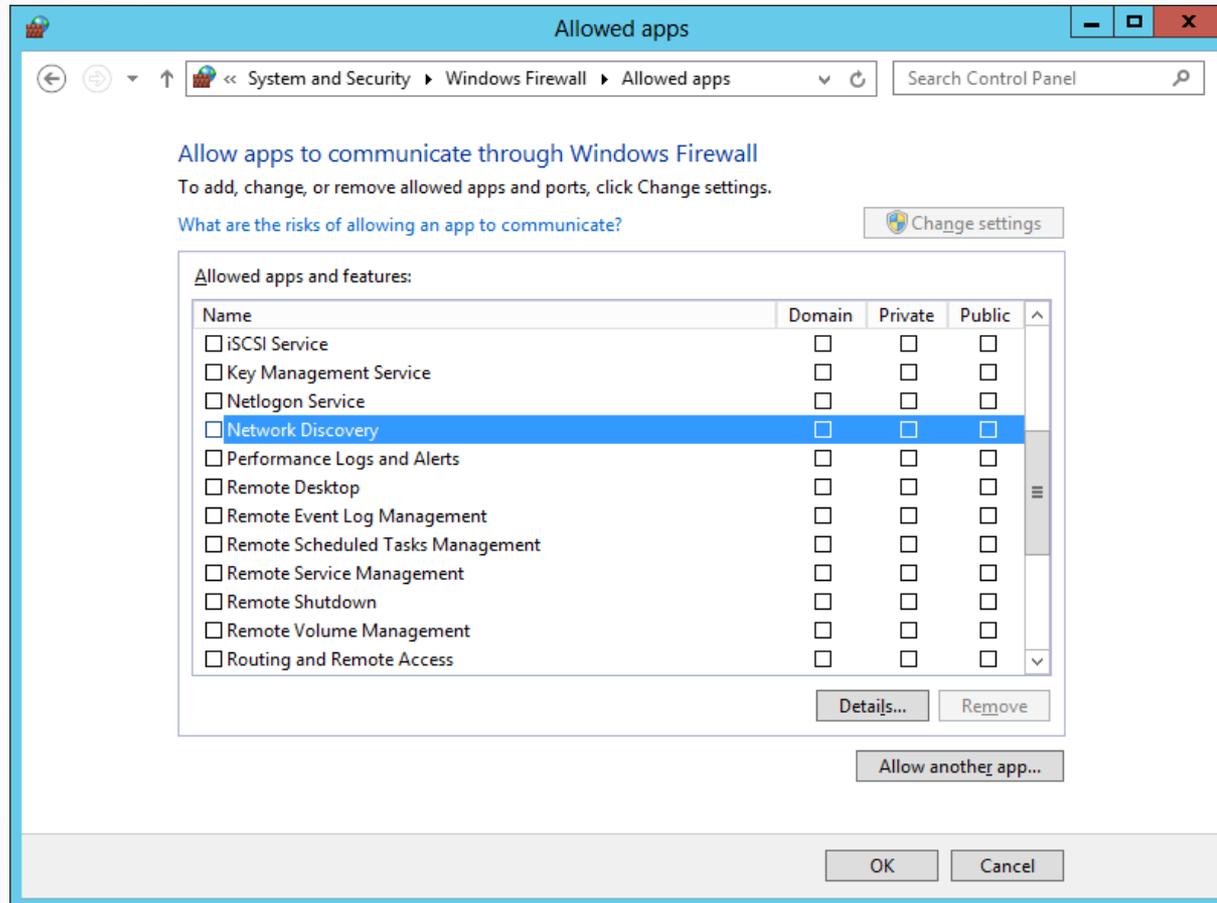
Windows Explorer with Network Discovery and File Sharing turned off

Working with Windows Firewall



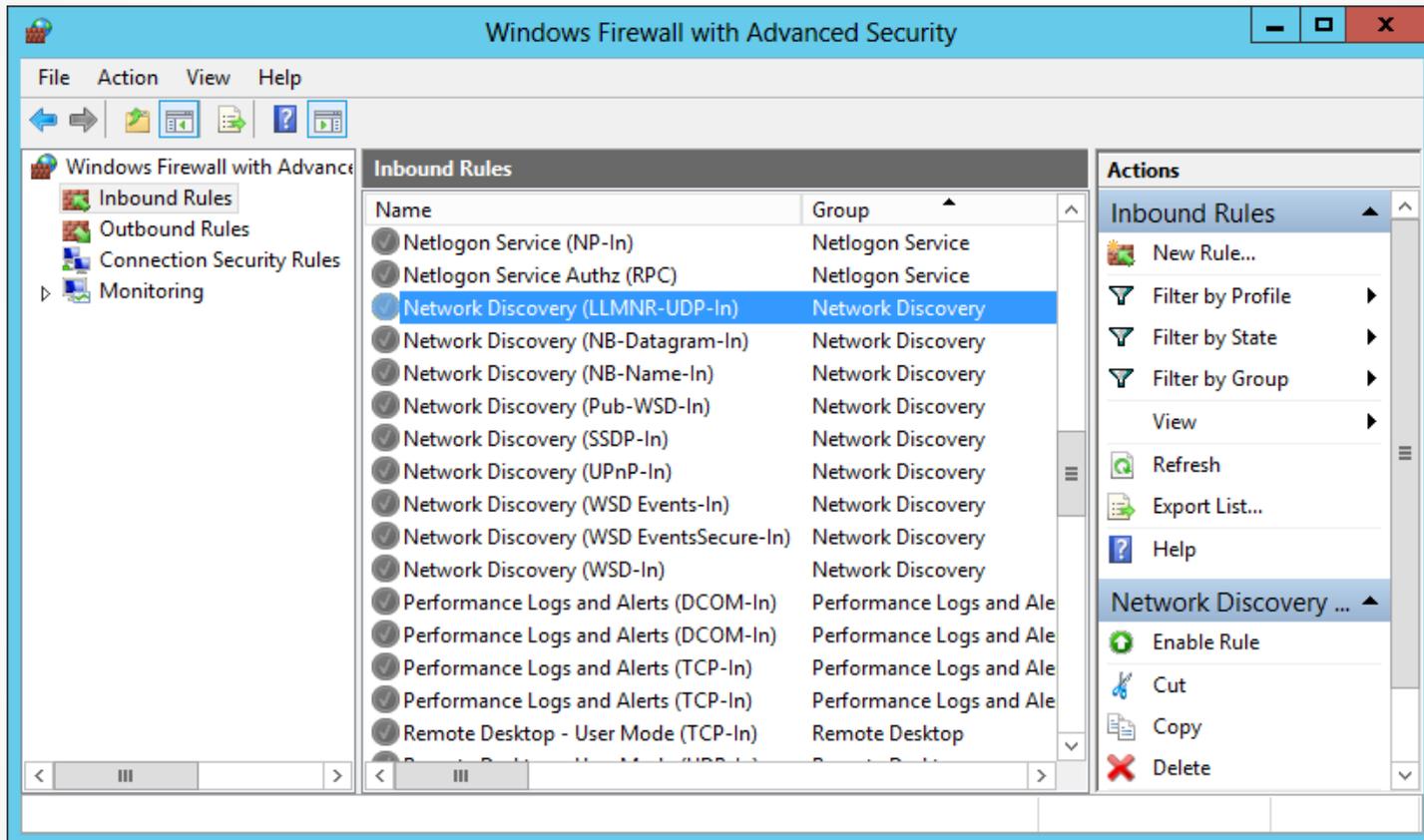
The Advanced Sharing Settings page of the Network and Sharing Center control panel

Working with Windows Firewall



The Network Discovery application in the Allowed apps dialog box

Working with Windows Firewall

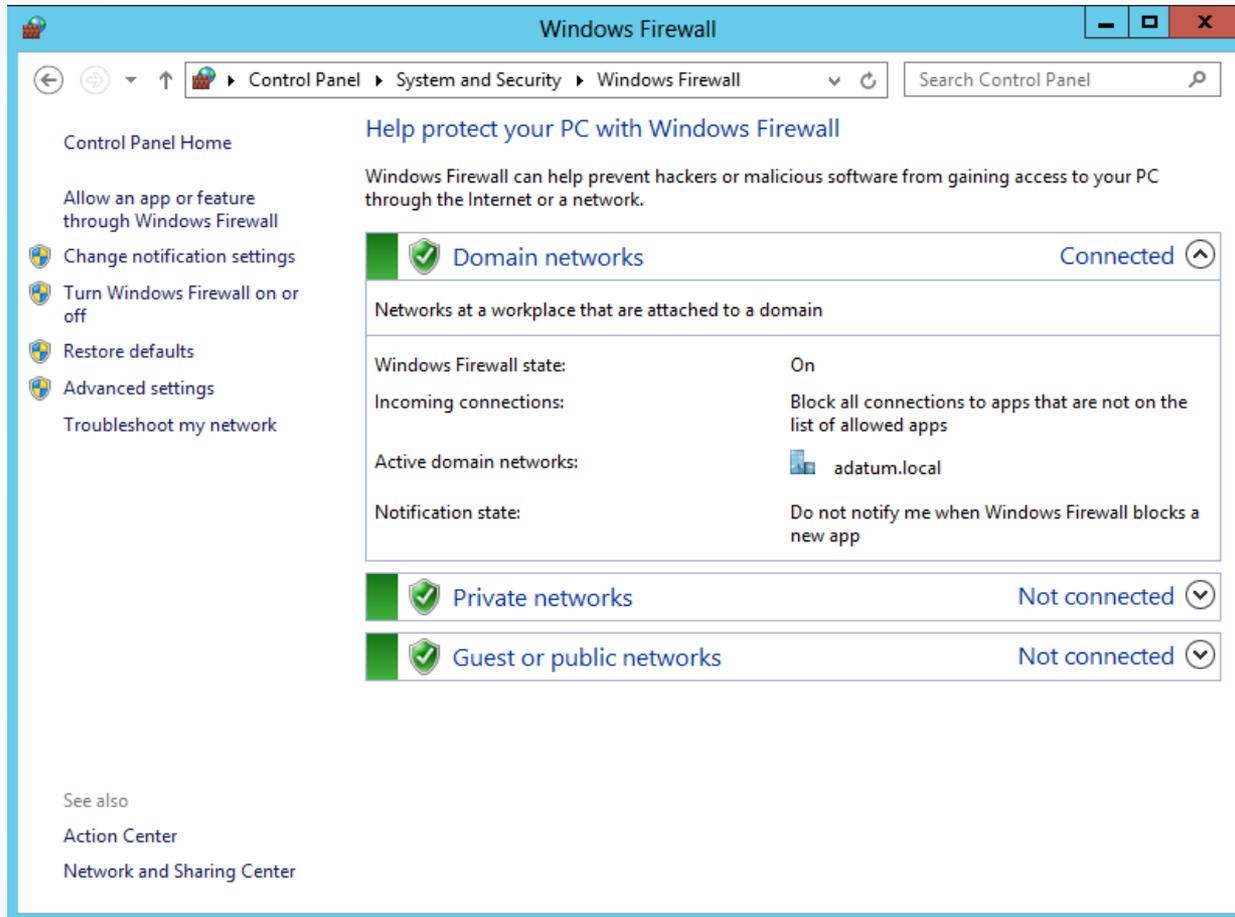


Network Discovery rules in the Windows Firewall with Advanced Security console

Using the Windows Firewall Control Panel

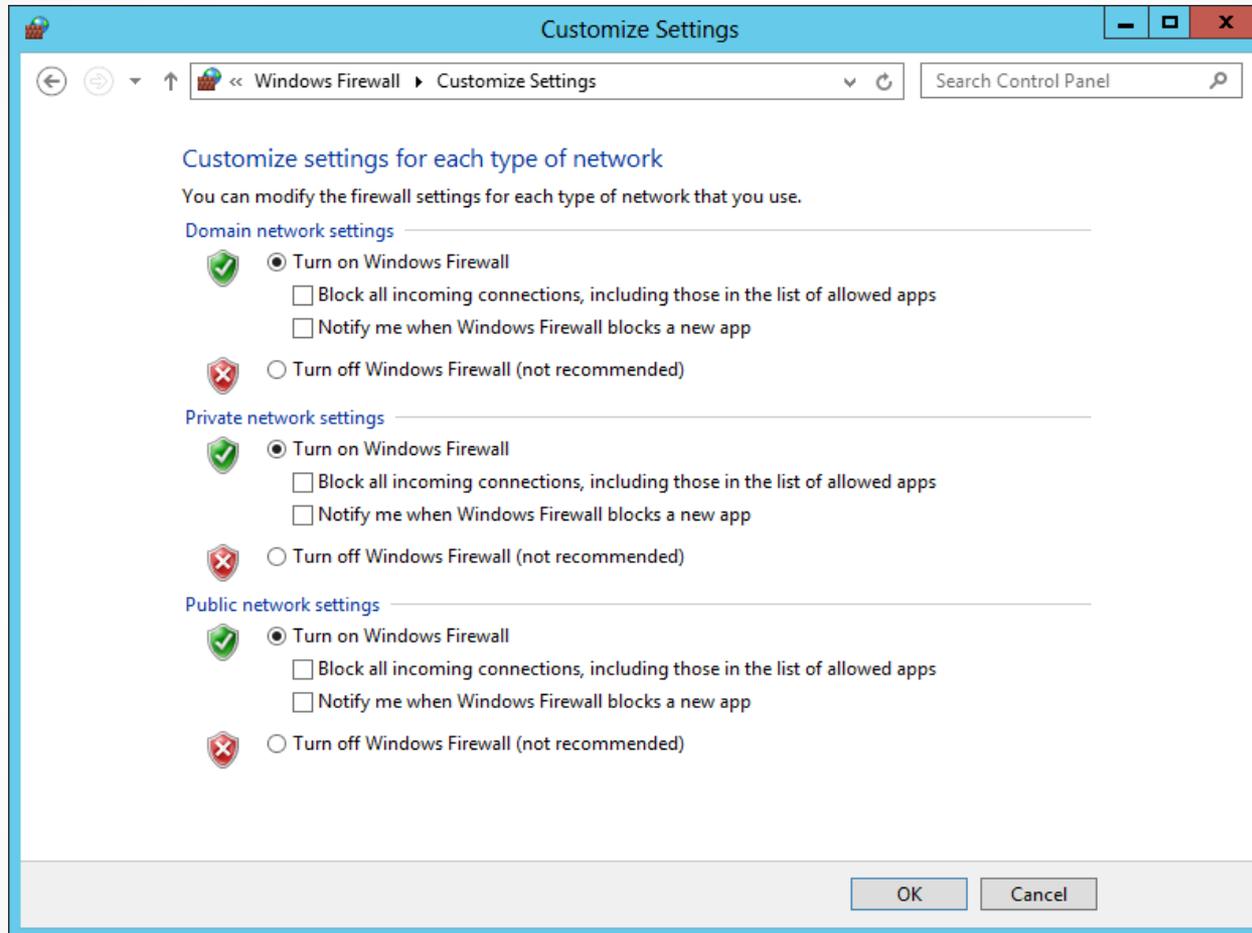
Lesson 19: Configuring Windows Firewall

Using the Windows Firewall Control Panel



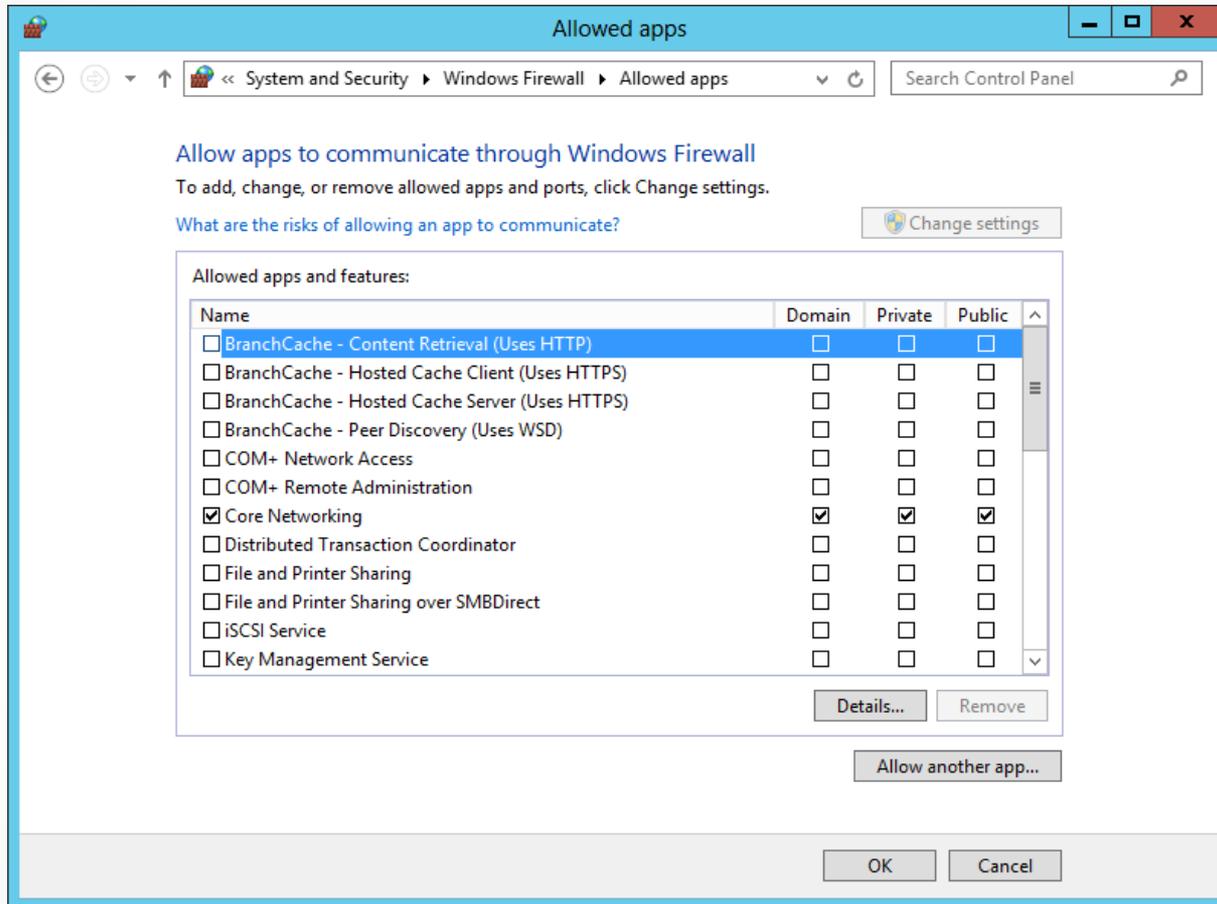
The Windows Firewall control panel window

Using the Windows Firewall Control Panel



The Customize Settings dialog box for Windows Firewall

Allowing Applications

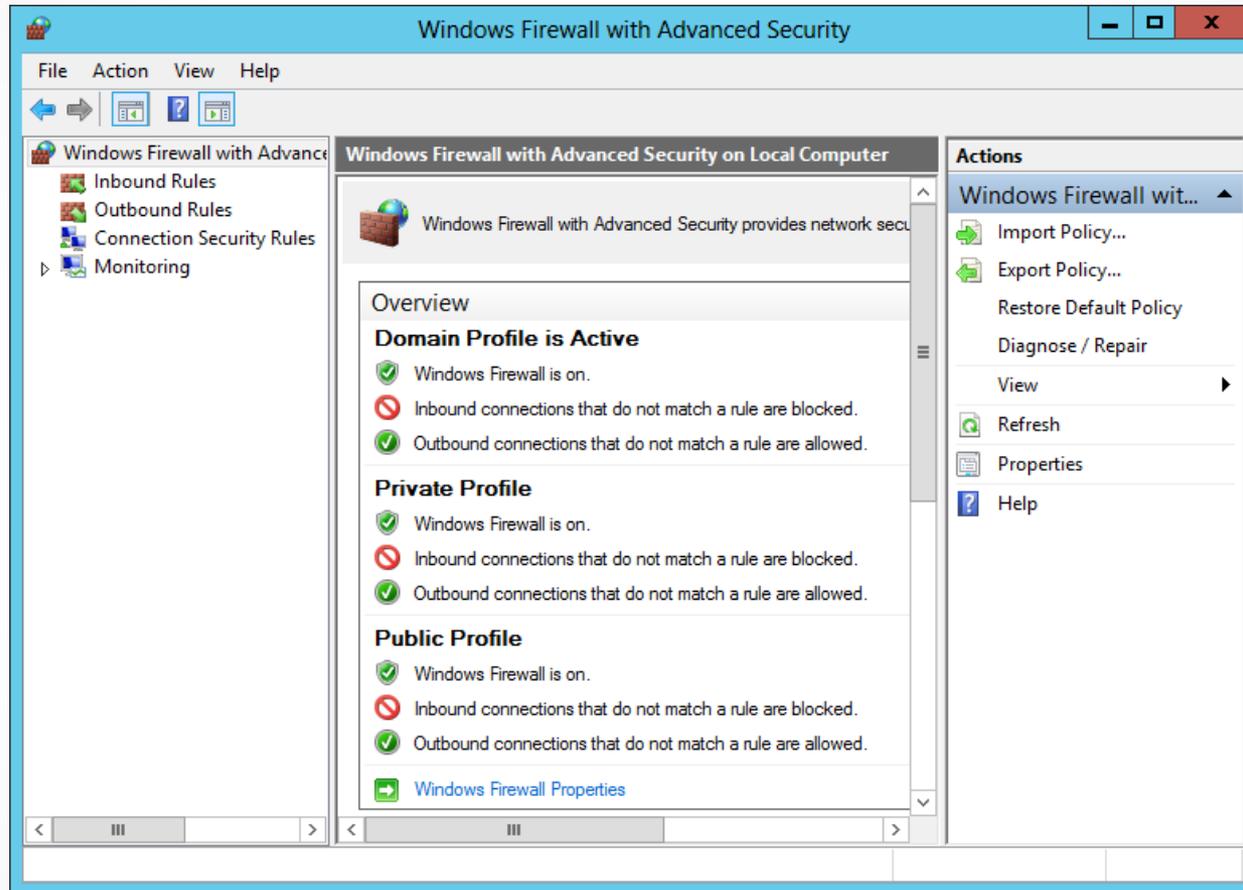


The Allowed Apps dialog box for Windows Firewall

Using the Windows Firewall with Advanced Security Console

Lesson 19: Configuring Windows Firewall

Using the Windows Firewall with Advanced Security Console

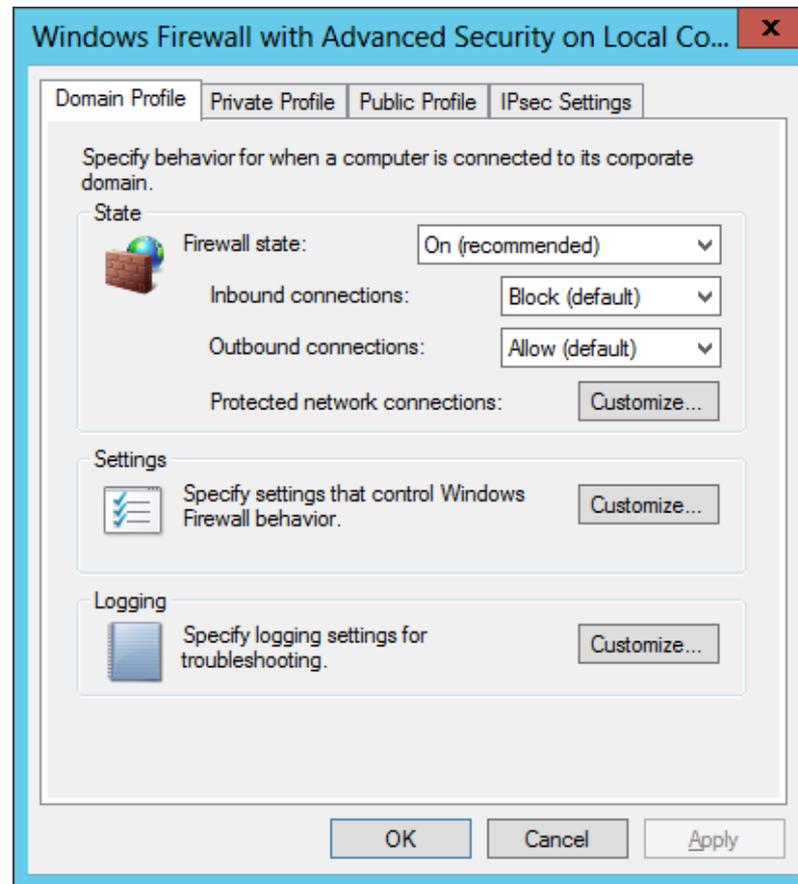


The Windows Firewall with Advanced Security console

Configuring Profile Settings

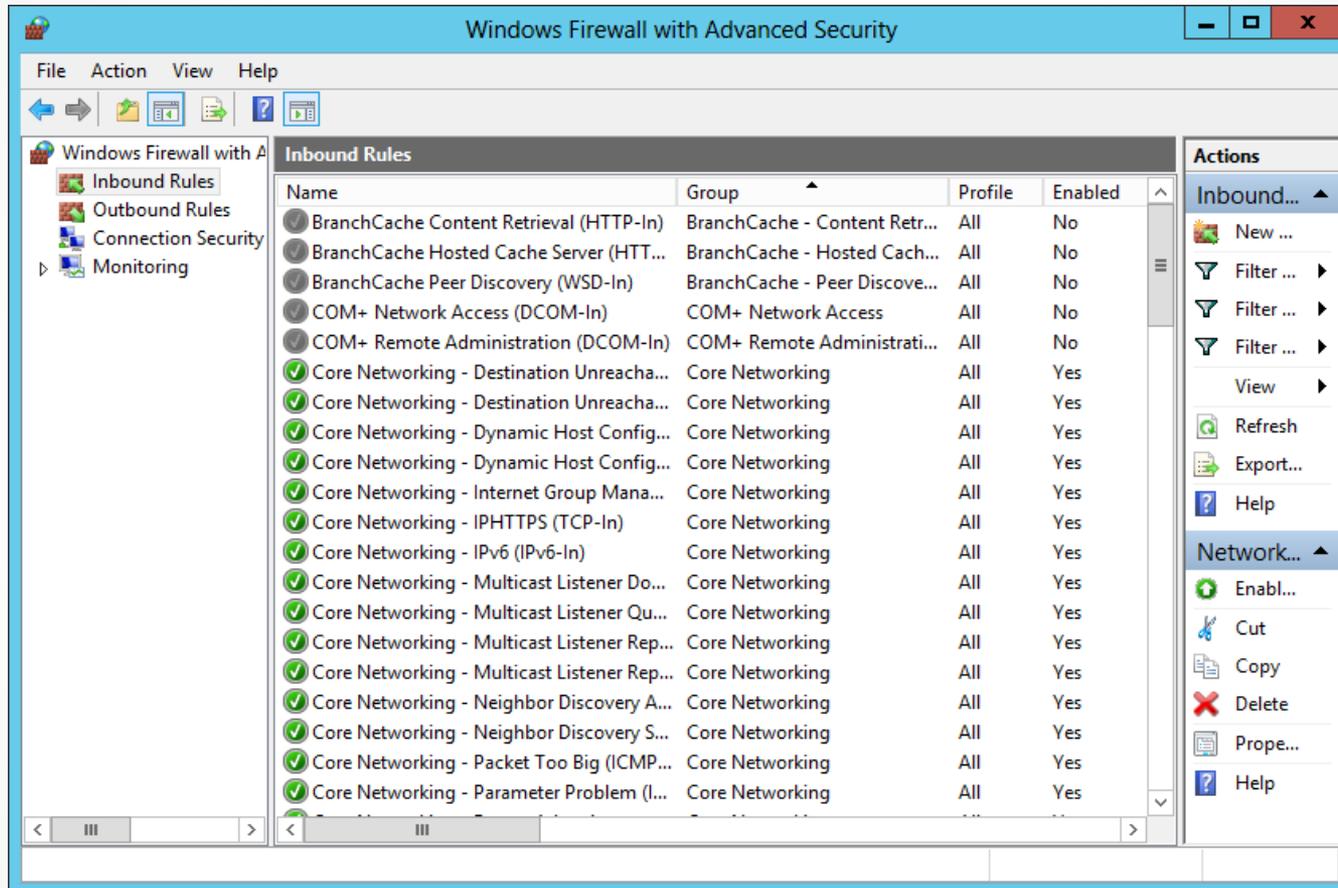
- The default Windows Firewall configuration calls for the same basic settings for all three profiles:
 - The firewall is turned on.
 - Incoming traffic is blocked unless it matches a rule.
 - Outgoing traffic is allowed unless it matches a rule.

Configuring Profile Settings



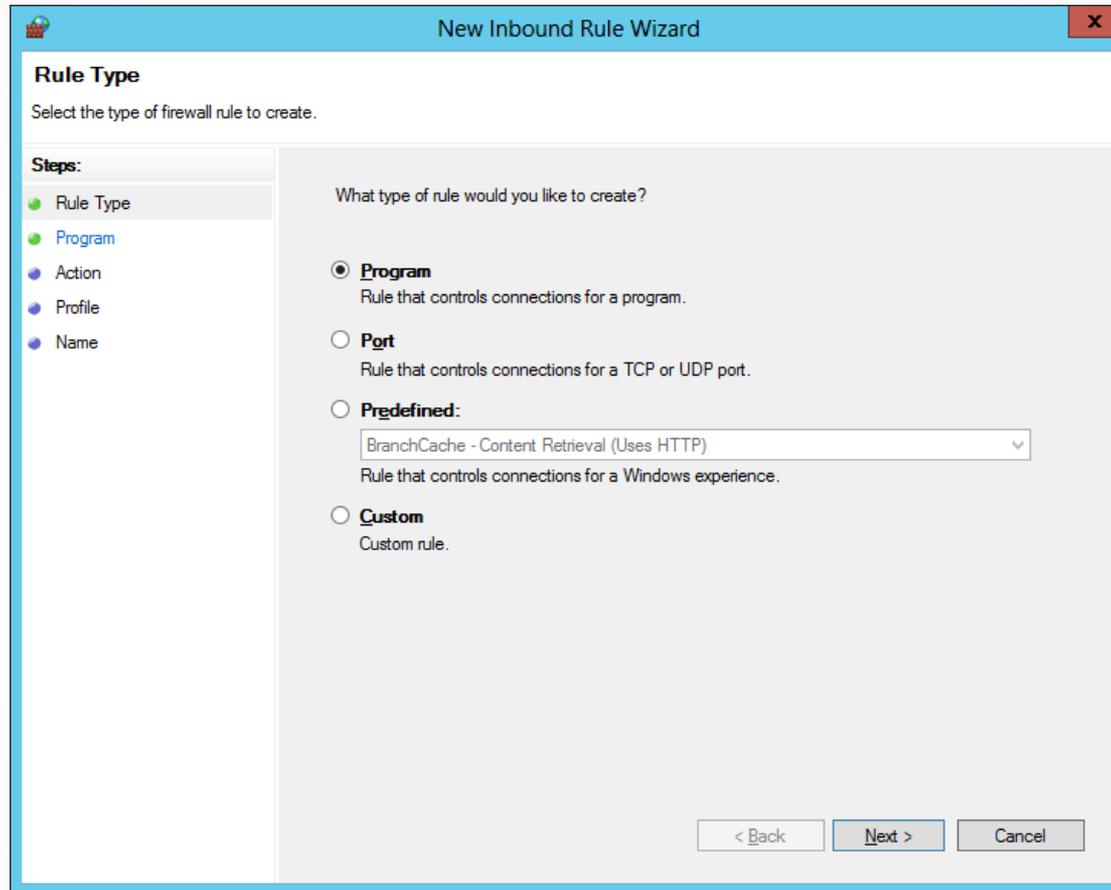
The Windows Firewall with Advanced Security on Local Computer dialog box

Creating Rules



The Inbound Rules list in the Windows Firewall with Advanced Security console

Creating Rules



The Rule Type page in the New Inbound Rule Wizard

Creating Rules

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Program' step. The title bar reads 'New Inbound Rule Wizard' with a close button (X) on the right. The main heading is 'Program', followed by the instruction: 'Specify the full program path and executable name of the program that this rule matches.'

On the left, a 'Steps:' pane lists the wizard's stages: 'Rule Type' (selected with a green dot), 'Program' (selected with a green dot), 'Action' (blue dot), 'Profile' (blue dot), and 'Name' (blue dot).

The main area contains the question: 'Does this rule apply to all programs or a specific program?'. There are two radio button options:

- All programs**
Rule applies to all connections on the computer that match other rule properties.
- This program path:**
A text input field is provided, followed by a 'Browse...' button. Below the field, an example is shown: 'Example: c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'.

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

The Program page in the New Inbound Rule Wizard

Creating Rules

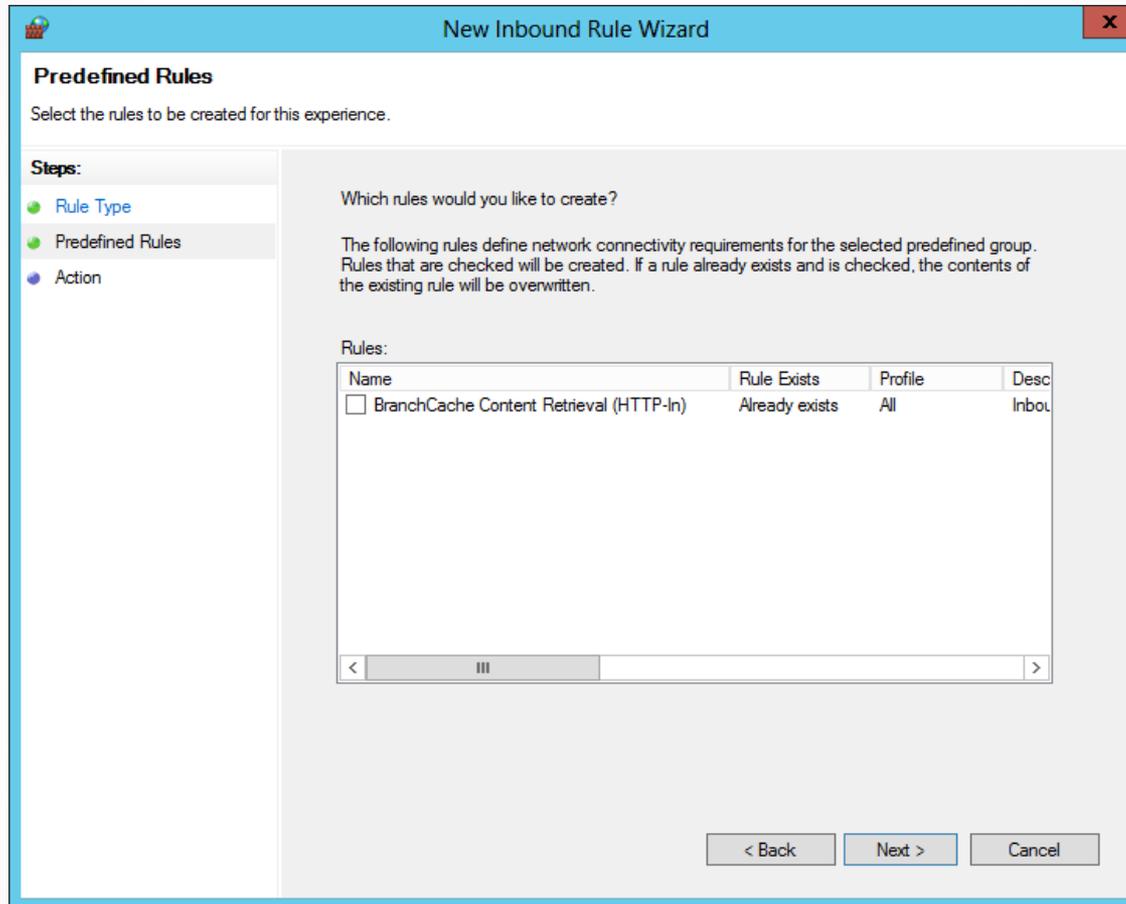
The screenshot shows a window titled "New Inbound Rule Wizard" with a close button (X) in the top right corner. The main heading is "Protocol and Ports" with the instruction "Specify the protocols and ports to which this rule applies." On the left, a "Steps:" sidebar lists: Rule Type, Program, Protocol and Ports (highlighted), Scope, Action, Profile, and Name. The main area is titled "To which ports and protocols does this rule apply?" and contains the following fields:

- Protocol type: A dropdown menu with "Any" selected.
- Protocol number: A spinner box with "0" and up/down arrows.
- Local port: A dropdown menu with "All Ports" selected, followed by a text input field and the example text "Example: 80, 443, 5000-5010".
- Remote port: A dropdown menu with "All Ports" selected, followed by a text input field and the example text "Example: 80, 443, 5000-5010".
- Internet Control Message Protocol (ICMP) settings: A label with a "Customize..." button.

At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

The Protocols and Ports page in the New Inbound Rule Wizard

Creating Rules



The Predefined Rules page in the New Inbound Rule Wizard

Creating Rules

Scope
Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- **Scope**
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

Any IP address

These IP addresses:

Add...
Edit...
Remove

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

Any IP address

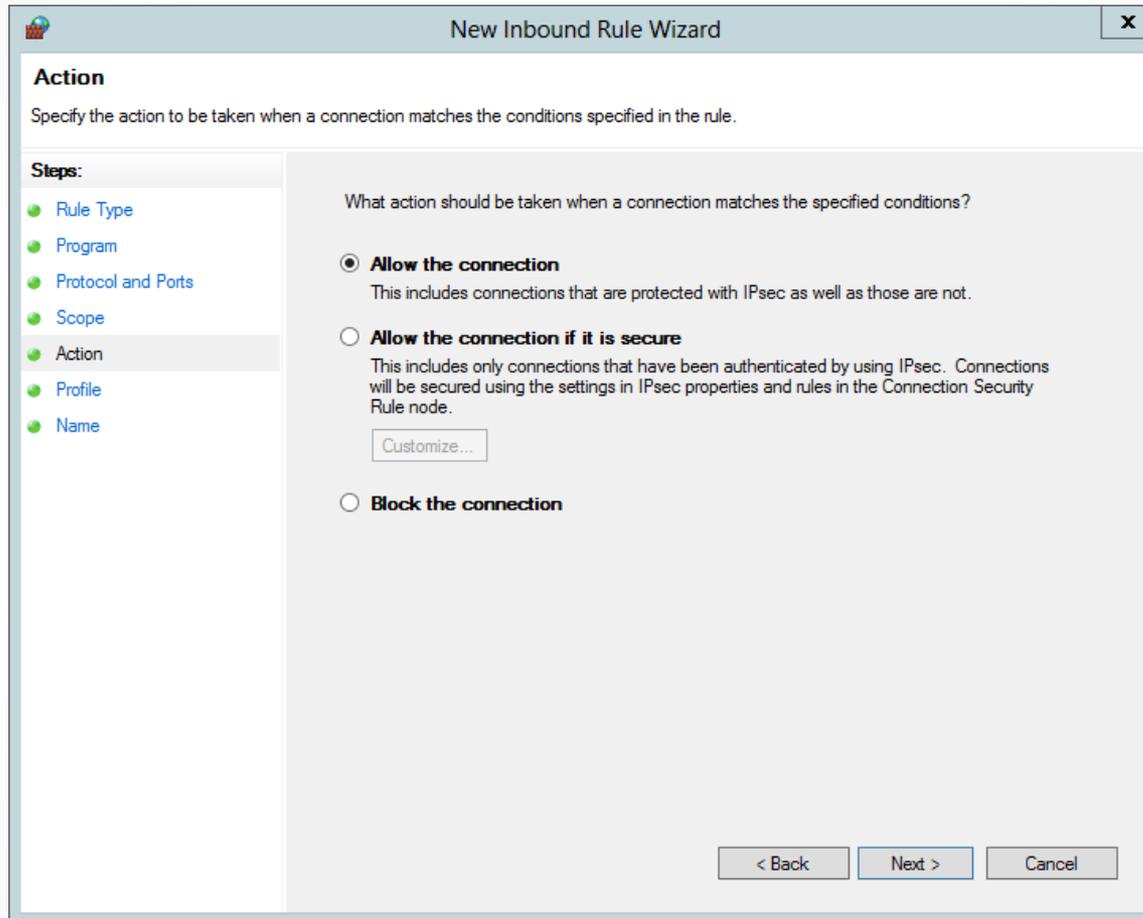
These IP addresses:

Add...
Edit...
Remove

< Back Next > Cancel

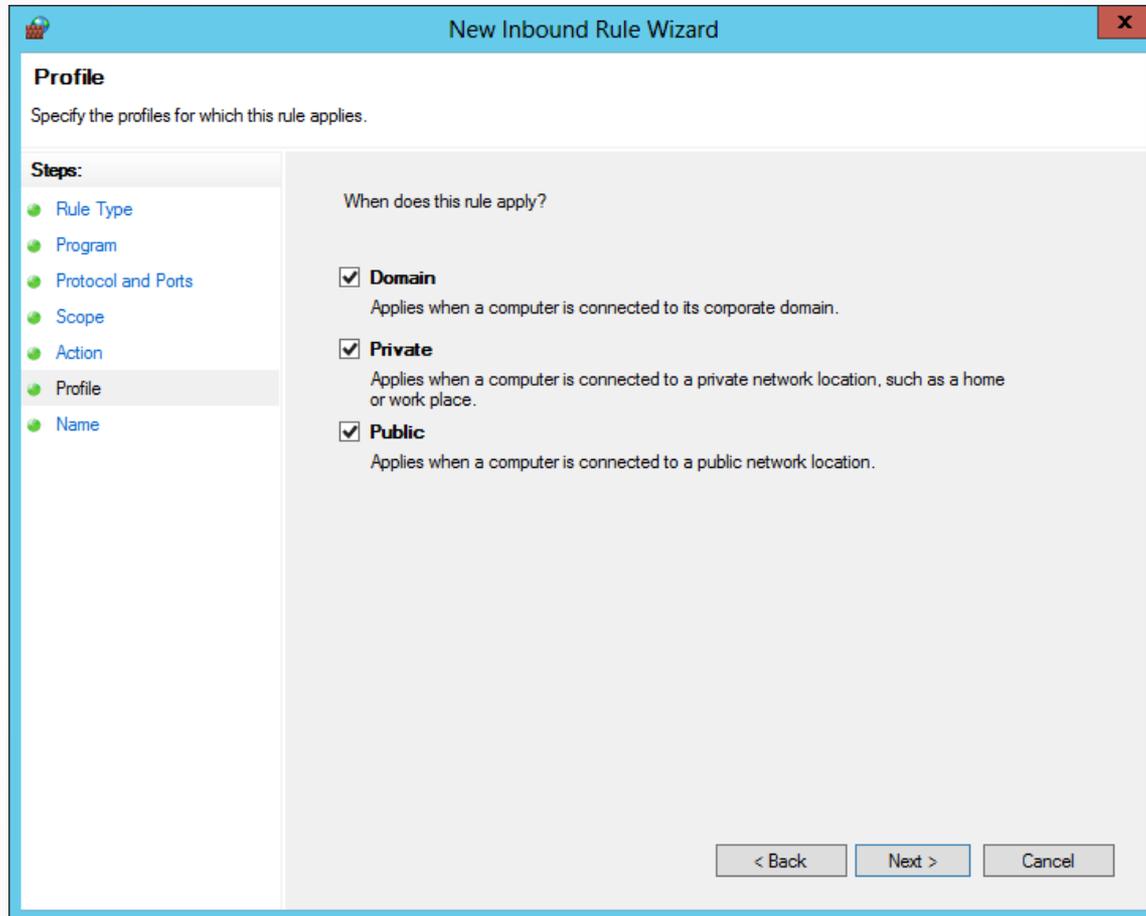
The Scope page of the New Inbound Rule Wizard

Creating Rules



The Action page of the New Inbound Rule Wizard

Creating Rules



The Profile page of the New Inbound Rule Wizard

Creating Rules

The screenshot shows a window titled "New Inbound Rule Wizard" with a close button (X) in the top right corner. The main area is titled "Name" and contains the instruction "Specify the name and description of this rule." On the left, a "Steps:" list includes "Rule Type", "Program", "Protocol and Ports", "Scope", "Action", "Profile", and "Name", with "Name" selected. The main area has a "Name:" label above a text input field and a "Description (optional):" label above a larger text area. At the bottom right, there are three buttons: "< Back", "Finish", and "Cancel".

The Name page of the New Inbound Rule Wizard

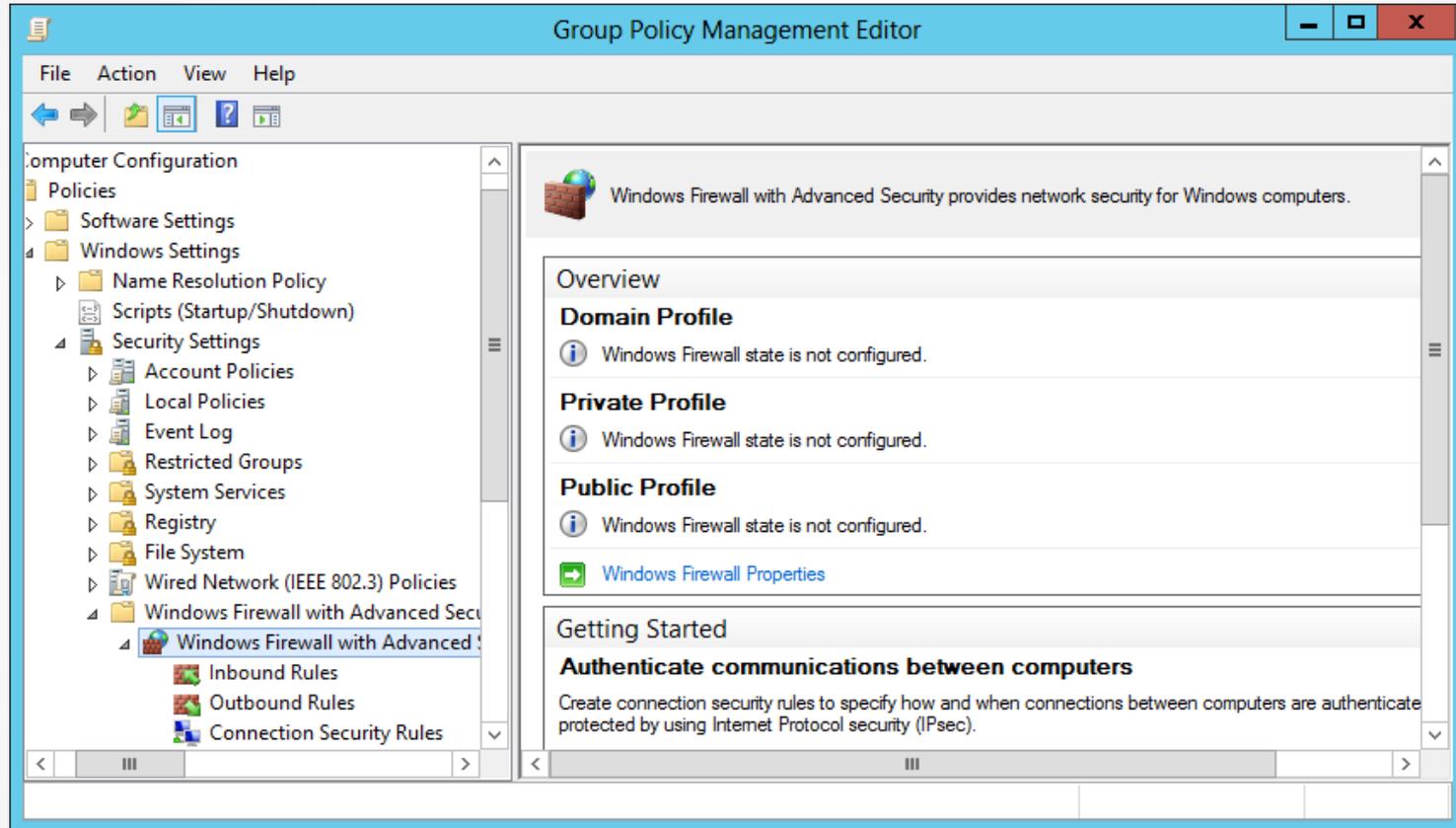
Importing and Exporting Rules

- The process of creating and modifying rules in the Windows Firewall with Advanced Security console can be time consuming.
- The console makes it possible for you to save the rules and settings you create by exporting them to a policy file.
- A policy file is a file with a .wfw extension that contains all the property settings in a Windows Firewall installation, as well as all of its rules, including the preconfigured rules and the ones you created or modified.

Creating Rules Using Group Policy

- Windows Firewall is an application designed to protect a single computer from intrusion
- Administrators can distribute firewall settings to computers throughout the network by using Group Policy.

Creating Rules Using Group Policy



The Windows Firewall with Advanced Security node in a Group Policy object

Using Filters

- The **filter** feature enables you to display inbound or outbound rules according to:
 - The profile they apply to
 - Their current state
 - The group to which they belong

Creating Connection Security Rules

- The IP Security (IPsec) standards are a collection of documents that define a method for securing data while it is in transit over a TCP/IP network.
- IPsec includes a connection establishment routine, during which computers authenticate each other before transmitting data, and a technique called **tunneling**, in which data packets are encapsulated within other packets, for their protection.
- Windows Server 2012 also includes a feature that incorporates IPsec data protection into the Windows Firewall.

Creating Connection Security Rules

The screenshot shows a window titled "New Connection Security Rule Wizard" with a close button in the top right corner. The main area is titled "Rule Type" and contains the instruction "Select the type of connection security rule to create." On the left, a "Steps:" list shows five items: "Rule Type" (selected with a green dot), "Requirements", "Authentication Method", "Profile", and "Name". The main content area asks "What type of connection security rule would you like to create?" and lists five options, each with a radio button:

- Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.
- Authentication exemption**
Do not authenticate connections from the specified computers.
- Server-to-server**
Authenticate connection between the specified computers.
- Tunnel**
Authenticate connections between two computers.
- Custom**
Custom rule.

At the bottom, there is a note: "Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule." Below the note are three buttons: "< Back", "Next >", and "Cancel".

The Rule Type page in the New Connection Security Rule Wizard

Creating Connection Security Rules

Endpoints
Specify the computers between which secured connections will be established using IPsec.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

Create a secured connection between computers in Endpoint 1 and Endpoint 2.

Which computers are in Endpoint 1?

Any IP address

These IP addresses:

Add...
Edit...
Remove

Customize the interface types to which this rule applies:

Which computers are in Endpoint 2?

Any IP address

These IP addresses:

Add...
Edit...
Remove

< Back Next > Cancel

The Endpoints page in the New Connection Security Rule Wizard

Creating Connection Security Rules

The screenshot shows a window titled "New Connection Security Rule Wizard" with a close button (X) in the top right corner. The main area is titled "Requirements" and contains the instruction: "Specify the authentication requirements for connections that match this rule." On the left, a "Steps:" sidebar lists: Rule Type, Endpoints, Requirements (highlighted), Authentication Method, Profile, and Name. The main content area asks "When do you want authentication to occur?" and lists three radio button options:

- Request authentication for inbound and outbound connections**
Authenticate whenever possible but authentication is not required.
- Require authentication for inbound connections and request authentication for outbound connections**
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.
- Require authentication for inbound and outbound connections**
Both inbound and outbound connections must be authenticated to be allowed.

At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

The Requirements page in the New Connection Security Rule Wizard

Creating Connection Security Rules

New Connection Security Rule Wizard

Authentication Method
Specify how authentication is performed for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method**
- Profile
- Name

What authentication method would you like to use?

Computer certificate
Restrict communications to connections from computers that have a certificate from this certification authority (CA).

Signing Algorithm: RSA (default) ▼

Certificate store type: Root CA (default) ▼

CA name:

Accept only health certificates
These certificates are issued by Network Access Protection health certificate servers.

Advanced
Specify custom first and second authentication settings.

The Authentication Method page in the New Connection Security Rule Wizard

Lesson Summary

- A firewall is a software program that protects a computer by allowing certain types of network traffic in and out of the system while blocking others.
- A firewall is essentially a series of filters that examine the contents of packets and the traffic patterns to and from the network to determine which packets they should allow to pass through the filter.
- The default rules preconfigured into the firewall are designed to admit the traffic used by standard Windows networking functions, such as file and printer sharing. For outgoing network traffic, Windows Firewall allows all traffic to pass the firewall except that which conforms to a rule.
- The Windows Firewall control panel is designed to enable administrators to perform basic firewall configuration tasks as needed.
- For full access to the Windows Firewall configuration settings, you must use the Windows Firewall with Advanced Security snap-in for the Microsoft Management console.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.