Lesson 19: Configuring Windows Firewall

MOAC 70-410: Installing and Configuring Windows Server 2012

Microsoft Official Academic Course

WILEY

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

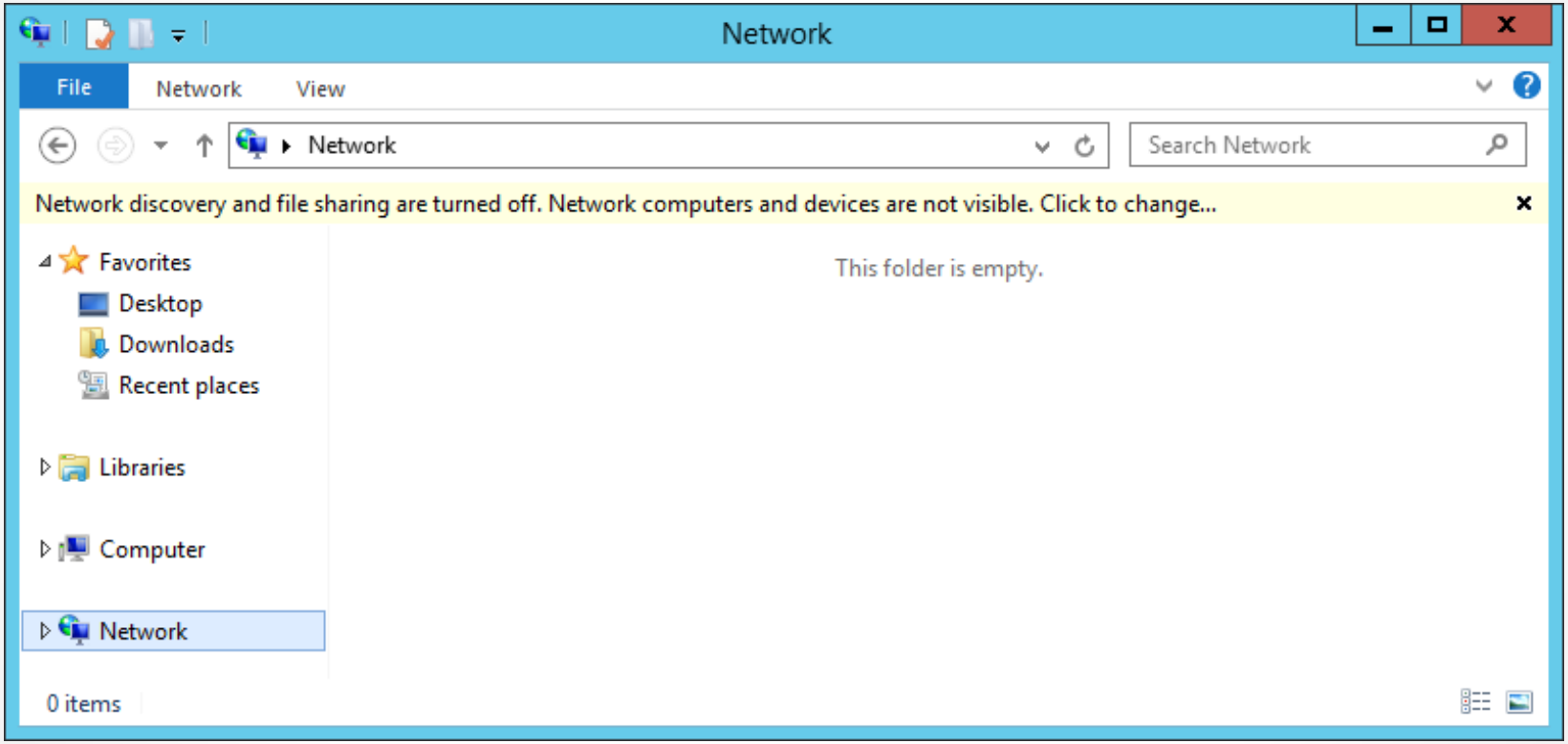
Firewall rules can function in two ways:

- **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

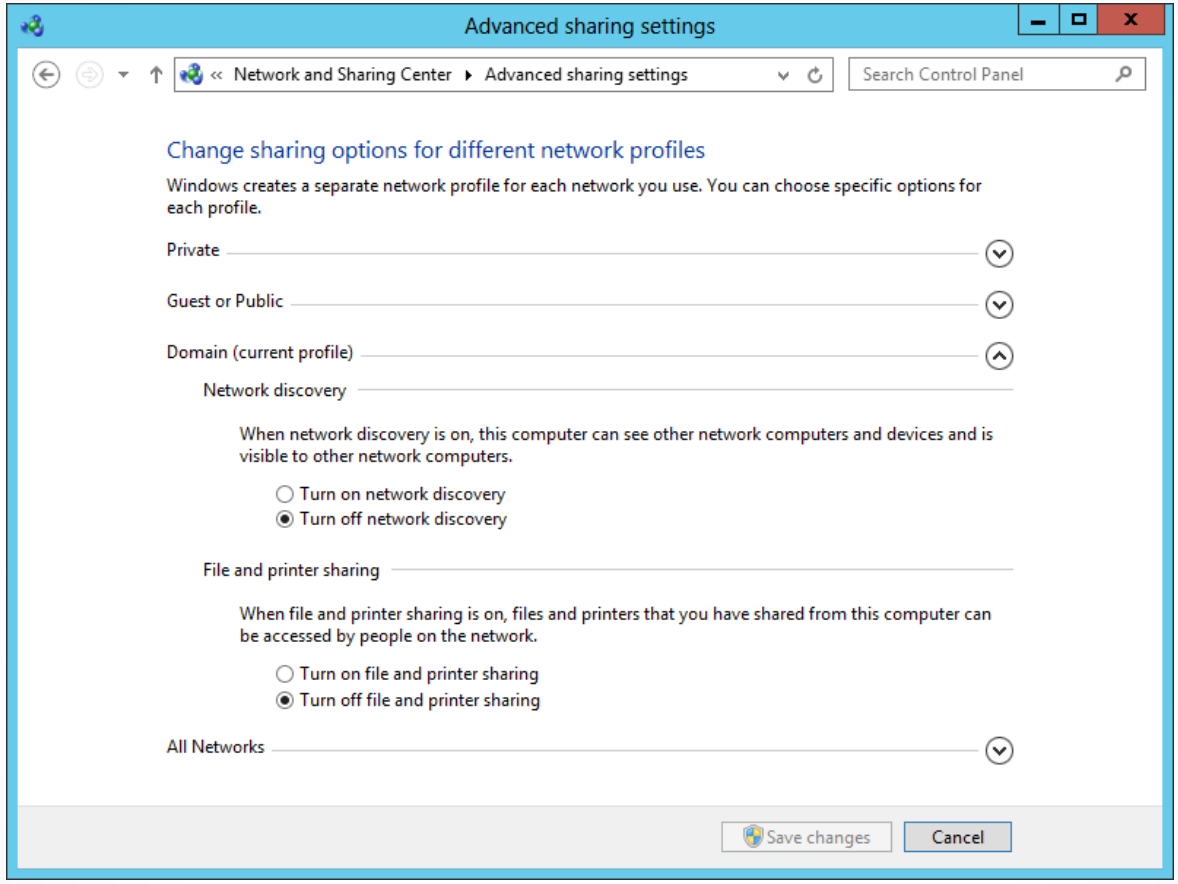
- The **Windows Firewall control panel** provides a simplified interface that enables you to avoid the details of rules and port numbers.
- For full access to firewall rules and more sophisticated functions, you must use the **Windows Firewall with Advanced Security console**.
- Many of the roles and 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



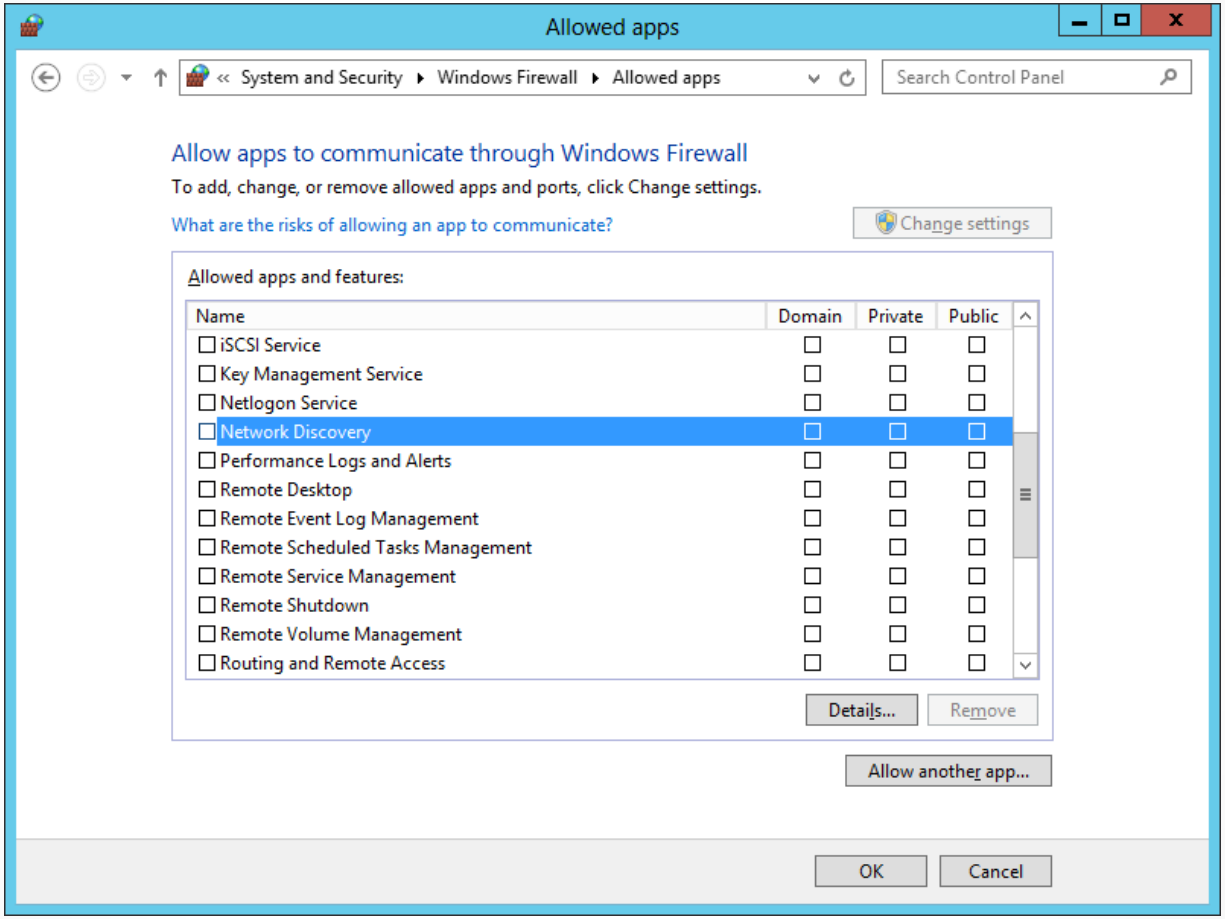
Windows Explorer with Network Discovery and File Sharing turned off

Working with Windows Firewall



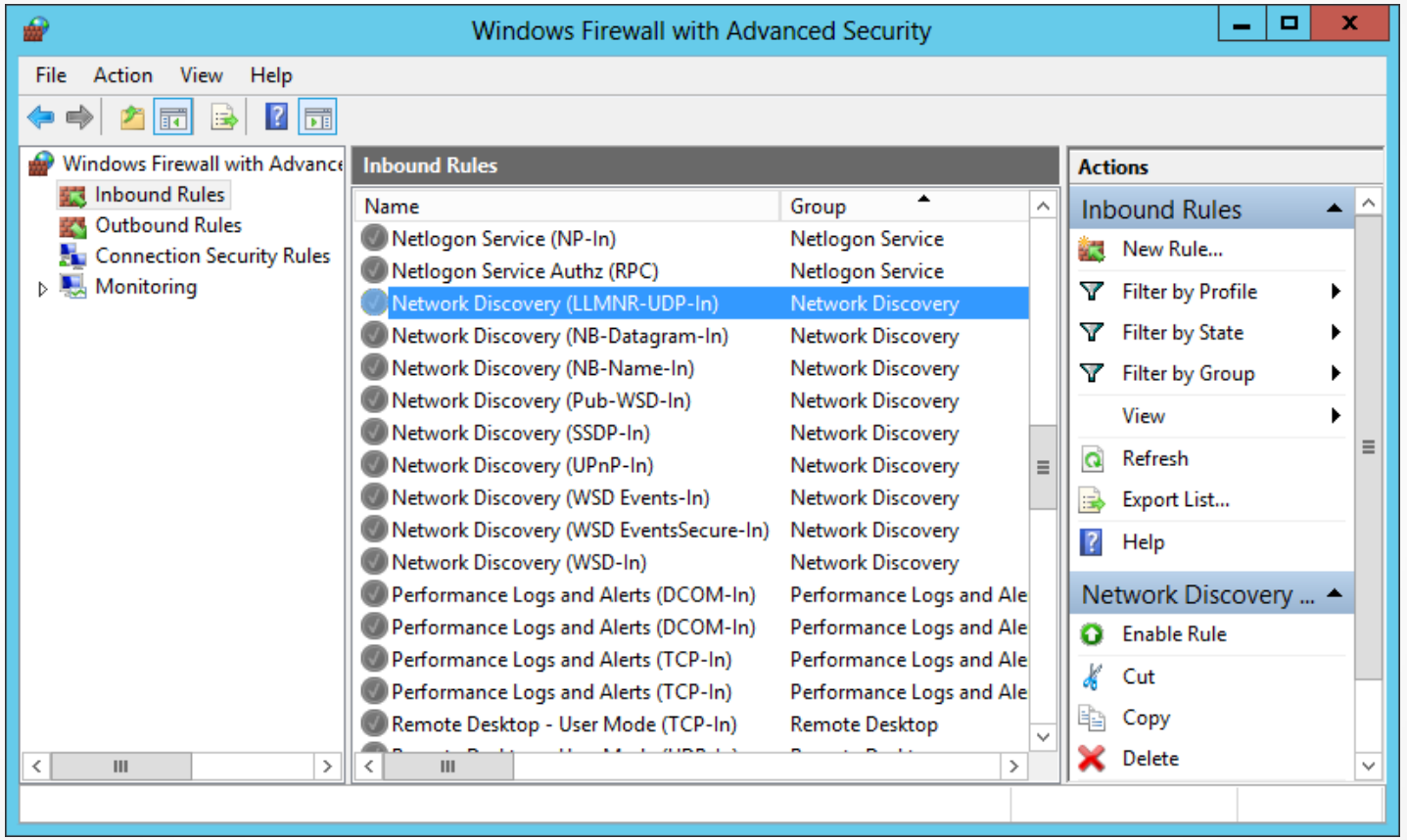
The Advanced Sharing Settings page of the Network and Sharing Center control panel

Working with Windows Firewall



The Network Discovery application in the Allowed apps dialog box

Working with Windows Firewall

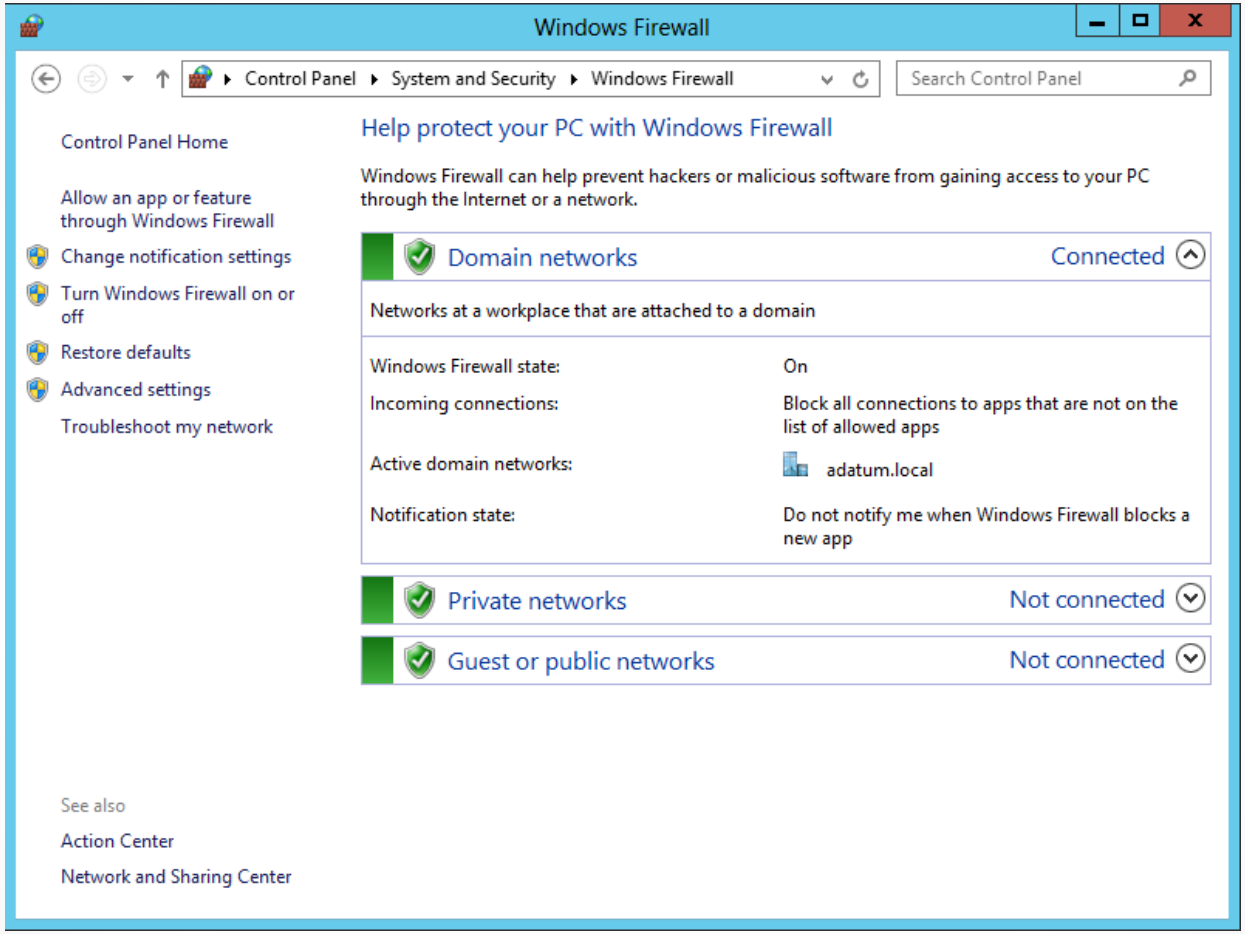


Network Discovery rules in the Windows Firewall with Advanced Security console

Using the Windows Firewall Control Panel

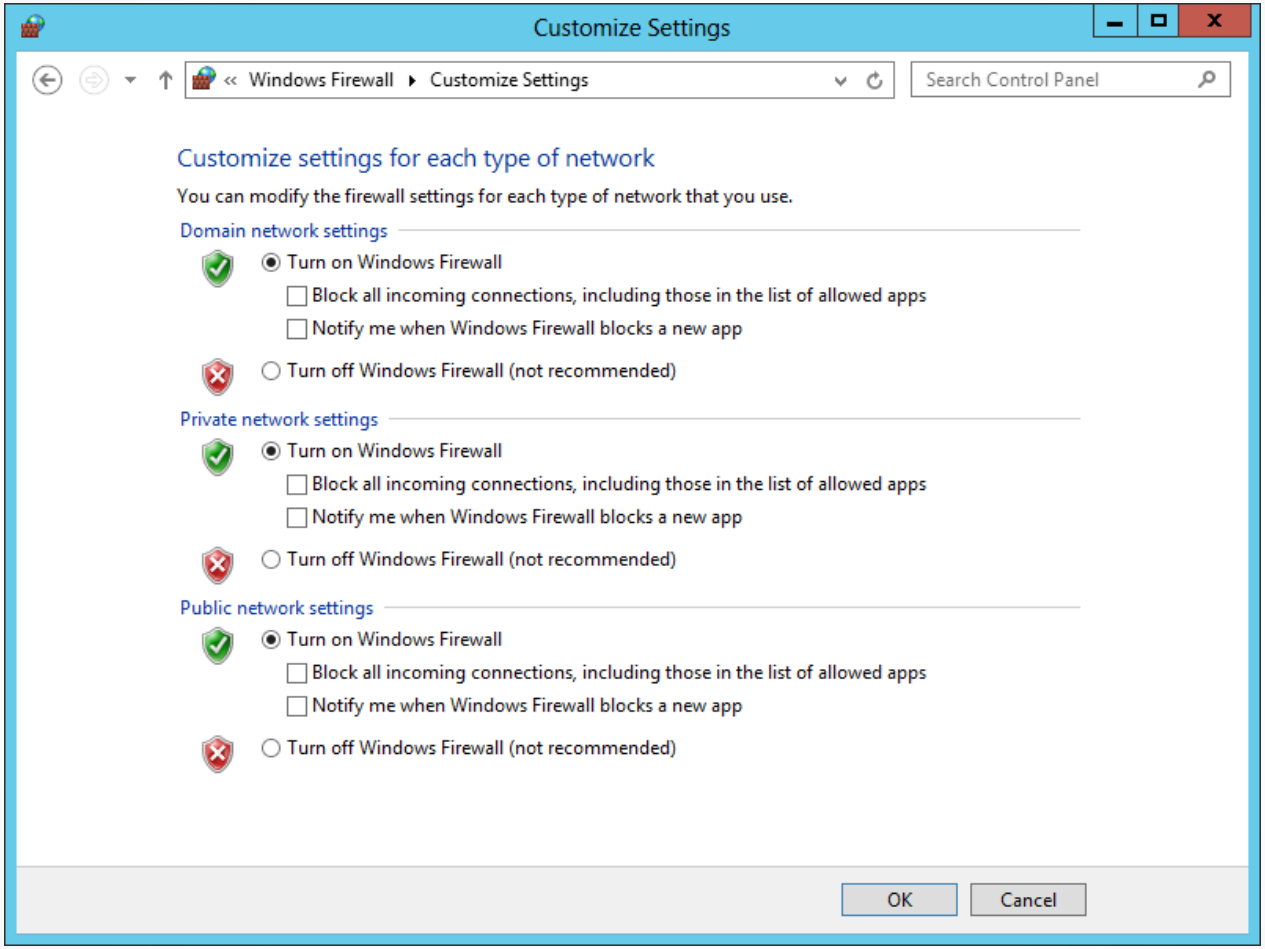
Lesson 19: Configuring Windows Firewall

Using the Windows Firewall Control Panel



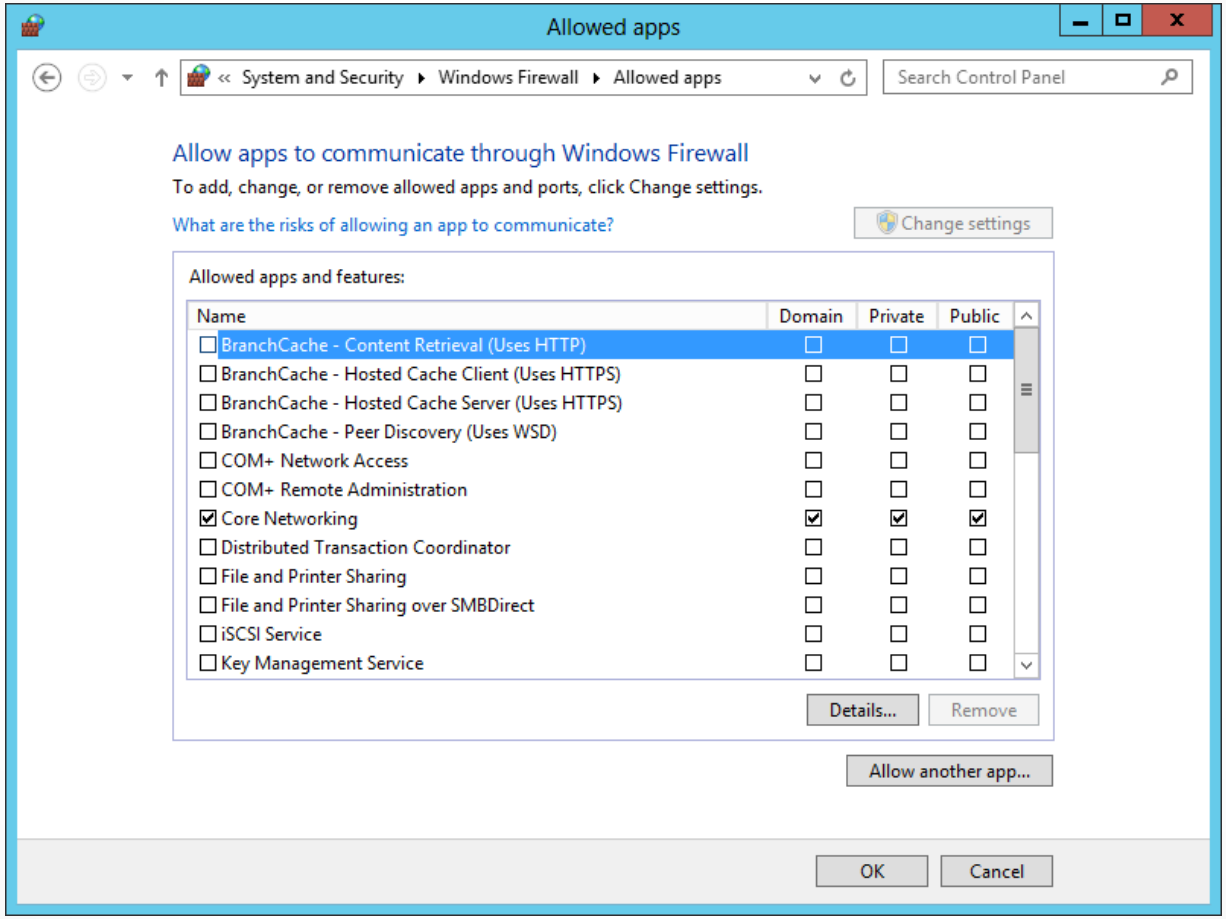
The Windows Firewall control panel window

Using the Windows Firewall Control Panel



The Customize Settings dialog box for Windows Firewall

Allowing Applications

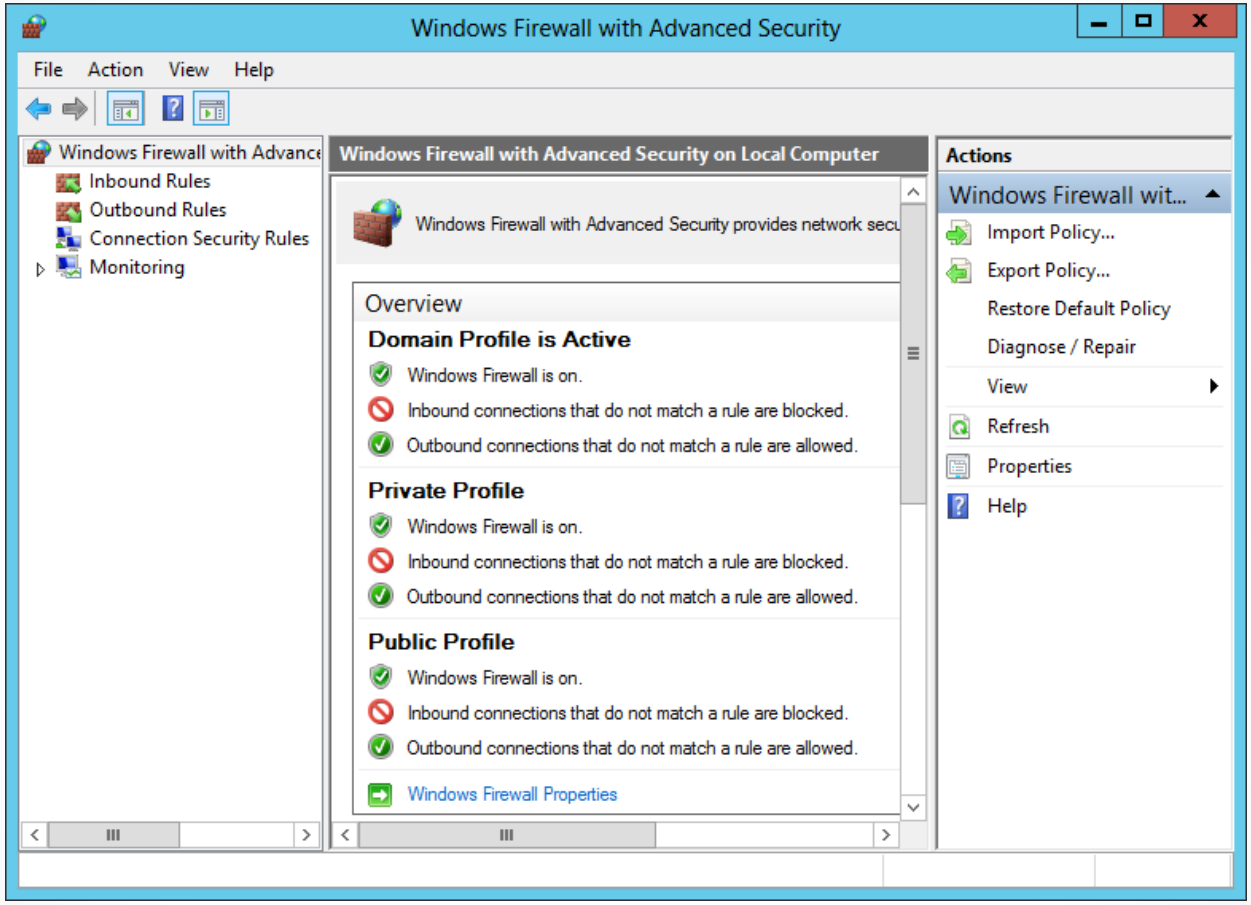


The Allowed Apps dialog box for Windows Firewall

Using the Windows Firewall with Advanced Security Console

Lesson 19: Configuring Windows Firewall

Using the Windows Firewall with Advanced Security Console

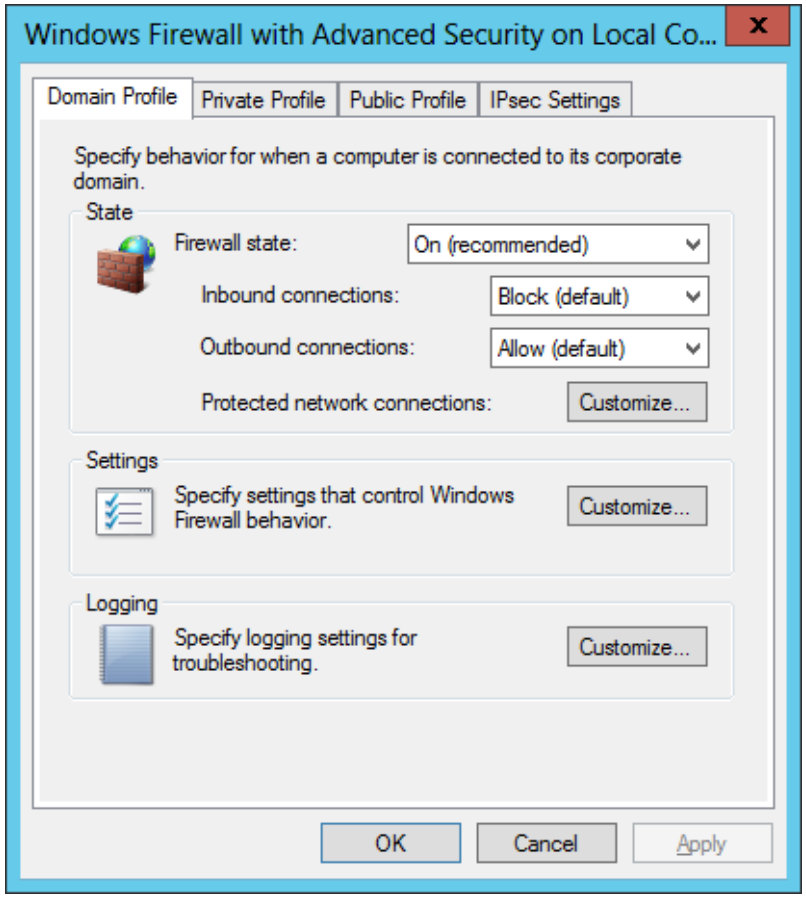


The Windows Firewall with Advanced Security console

Configuring Profile Settings

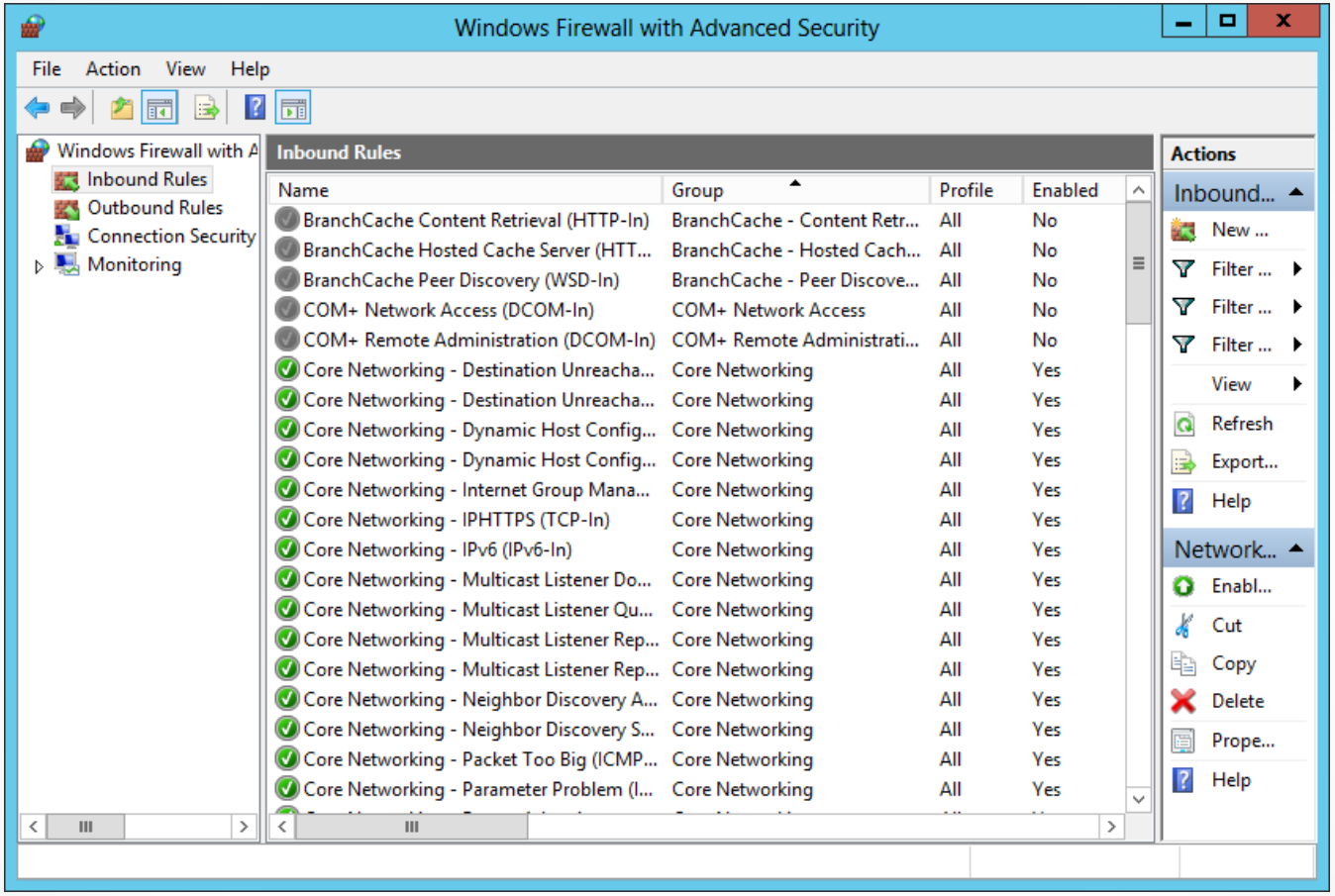
- The default Windows Firewall configuration calls for the same basic settings for all three profiles:
  - The firewall is turned on.
  - Incoming traffic is blocked unless it matches a rule.
  - Outgoing traffic is allowed unless it matches a rule.

Configuring Profile Settings



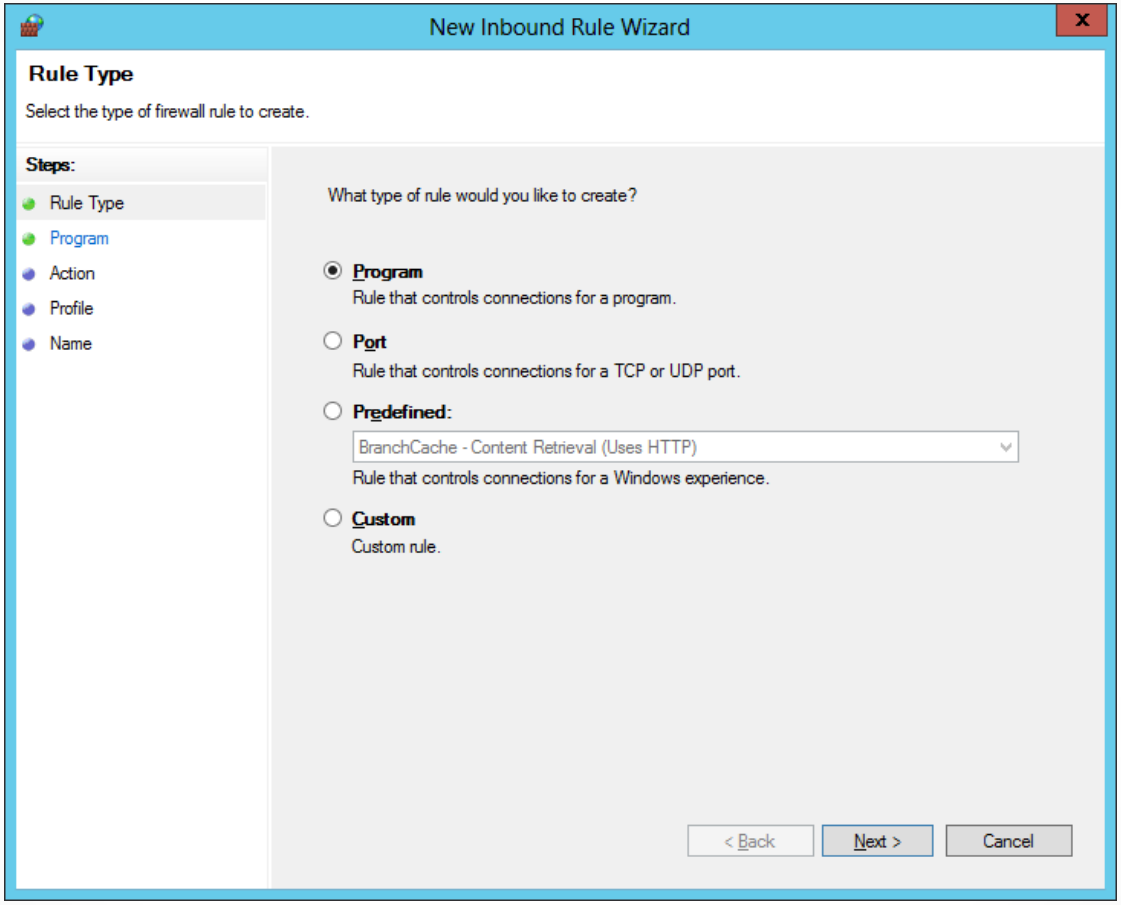
The Windows Firewall with Advanced Security on Local Computer dialog box

Creating Rules



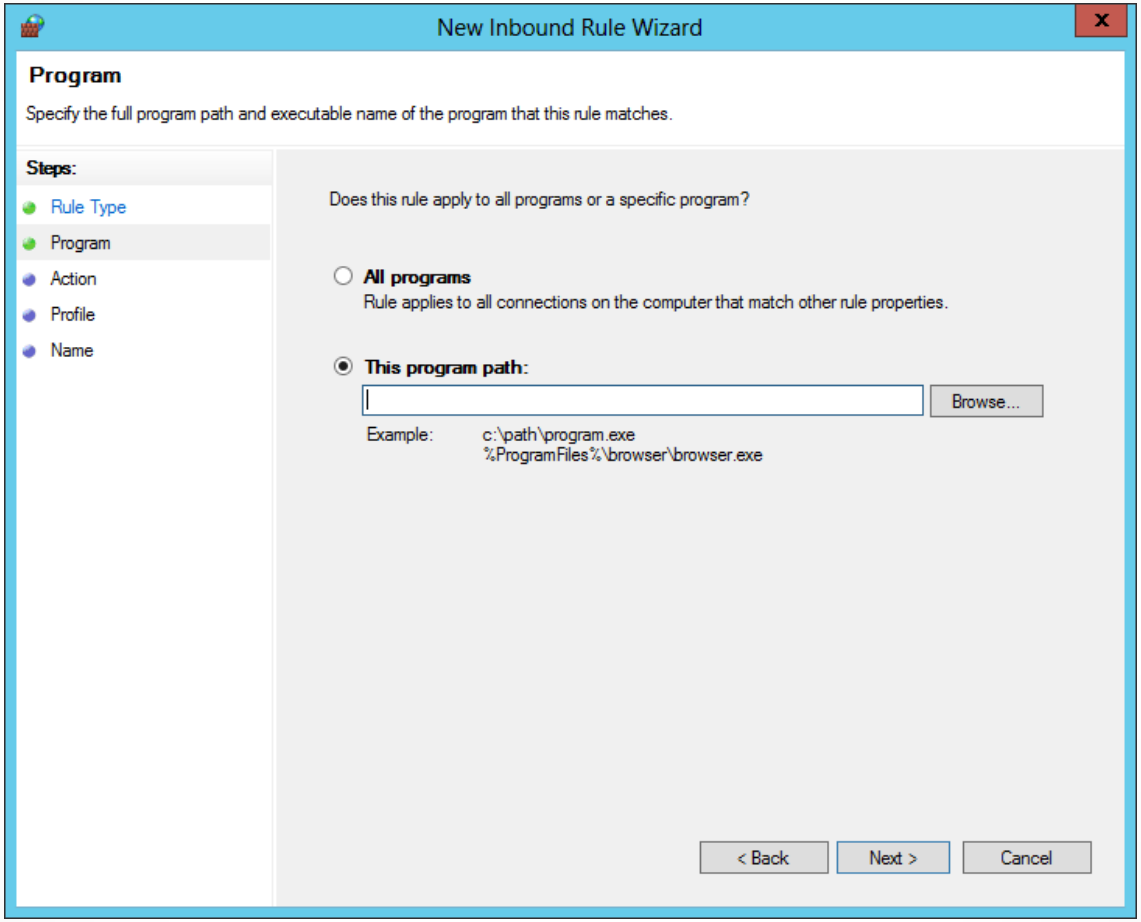
The Inbound Rules list in the Windows Firewall with Advanced Security console

Creating Rules



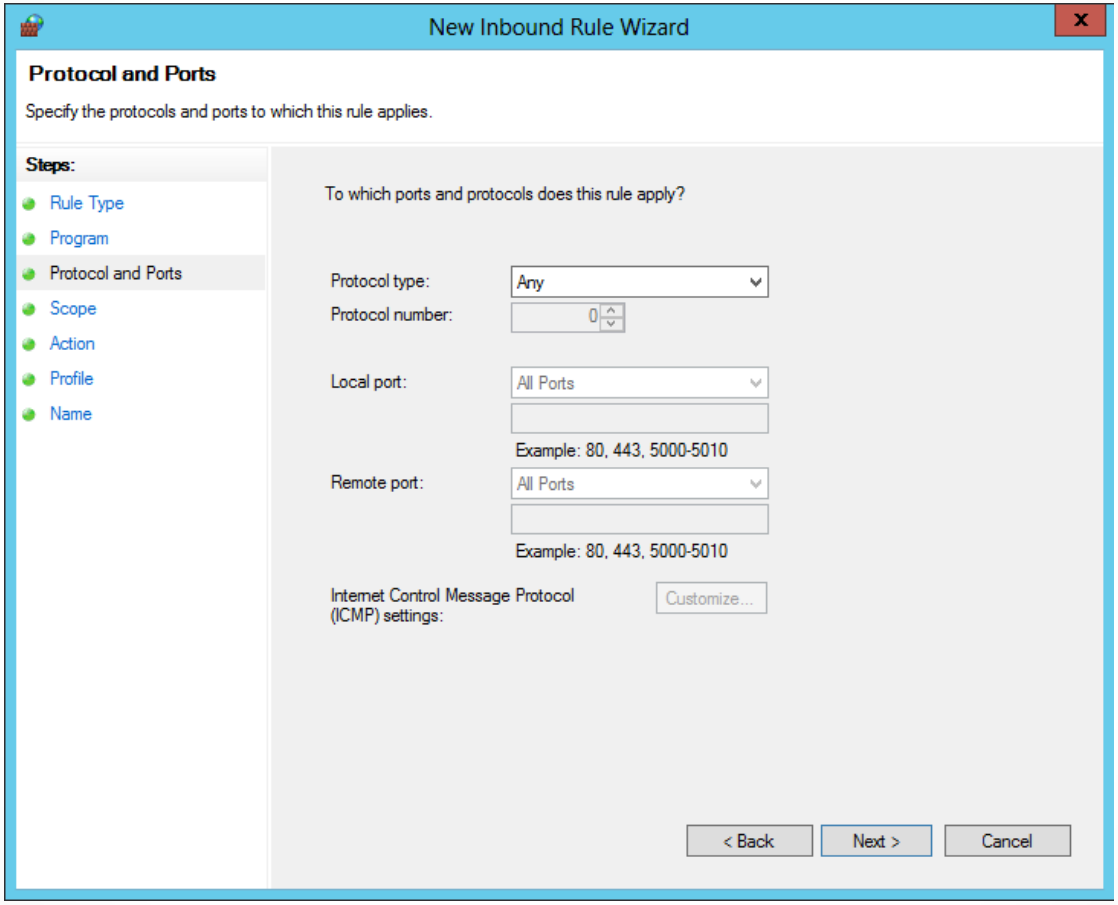
The Rule Type page in the New Inbound Rule Wizard

Creating Rules



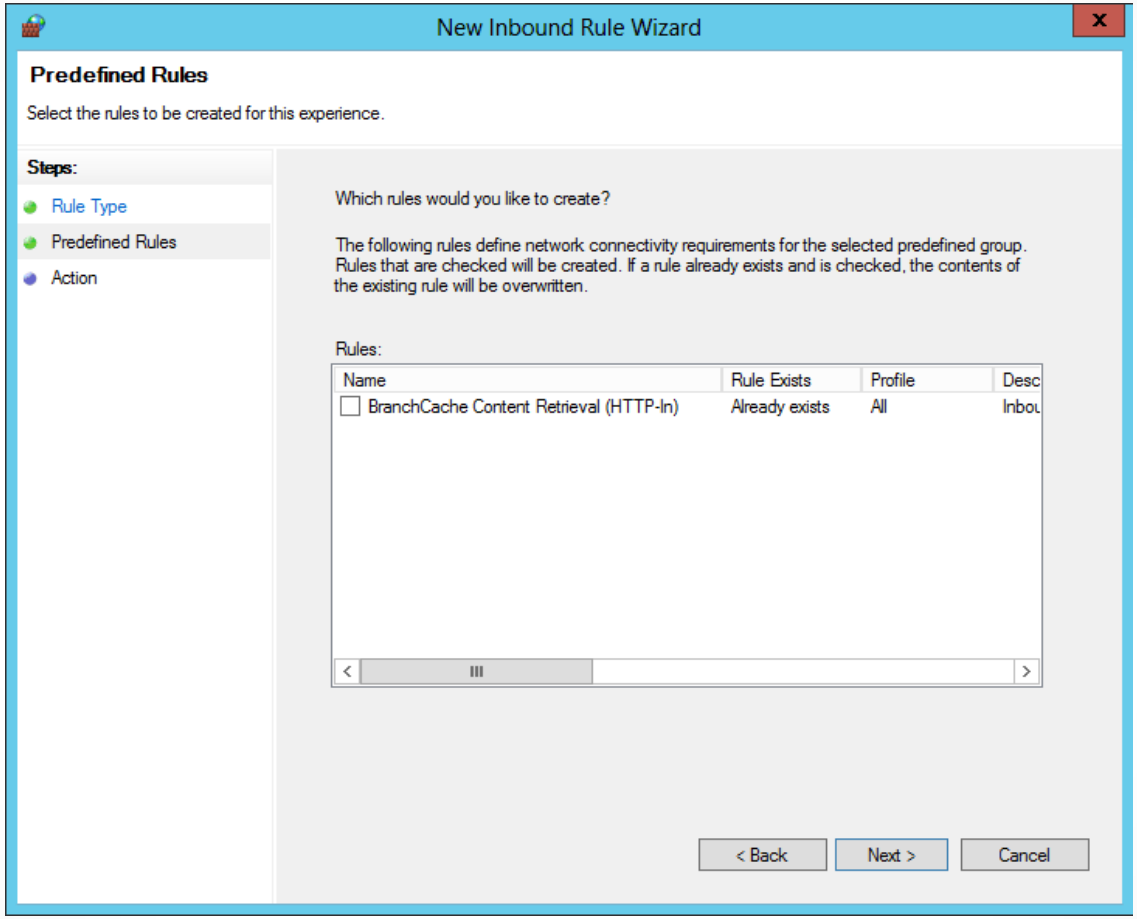
The Program page in the New Inbound Rule Wizard

Creating Rules



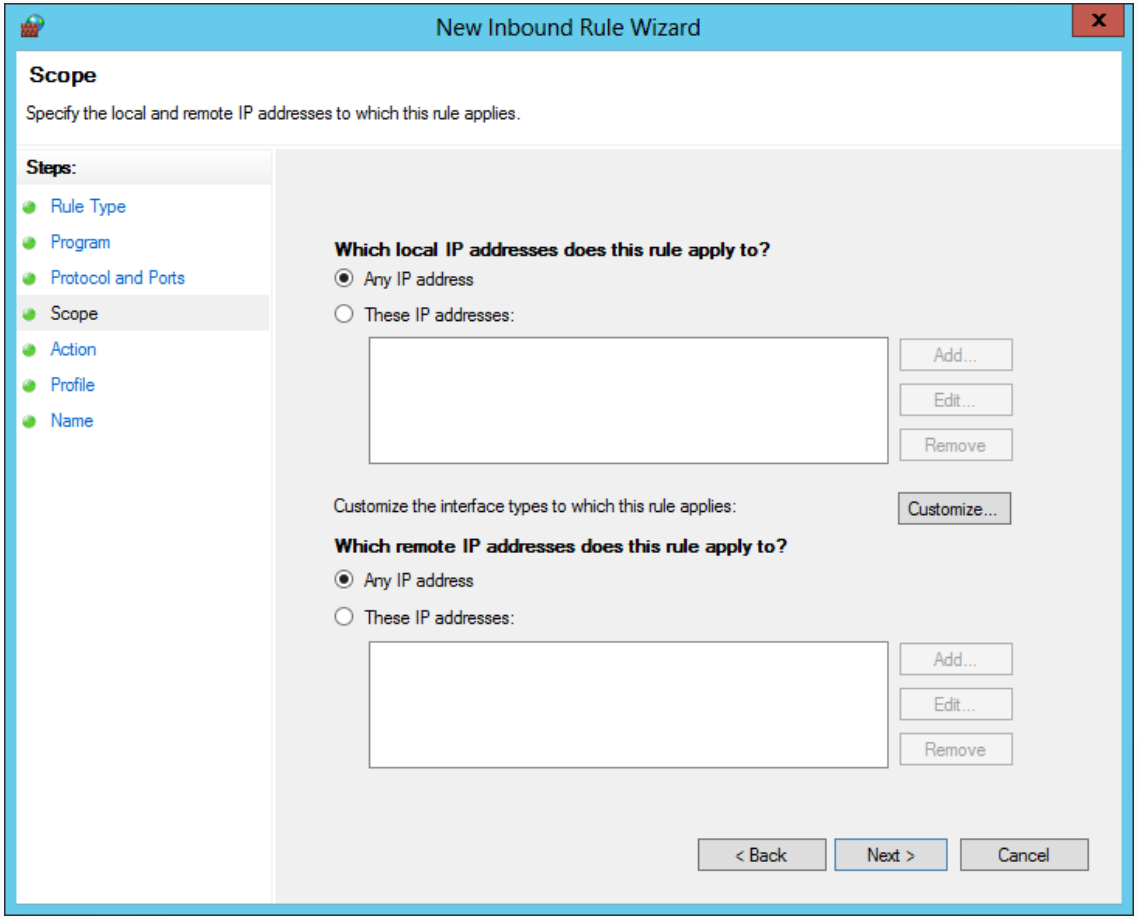
The Protocols and Ports page in the New Inbound Rule Wizard

Creating Rules



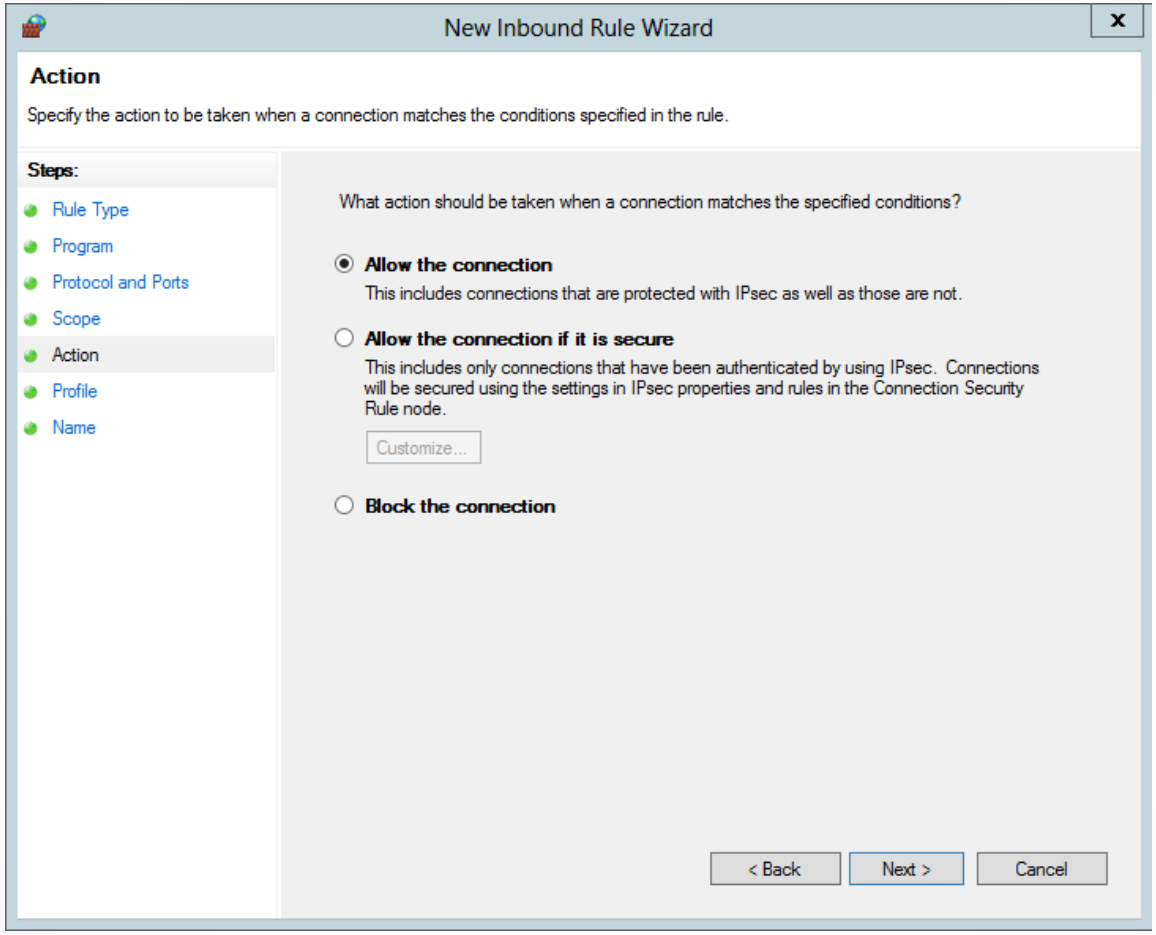
The Predefined Rules page in the New Inbound Rule Wizard

Creating Rules



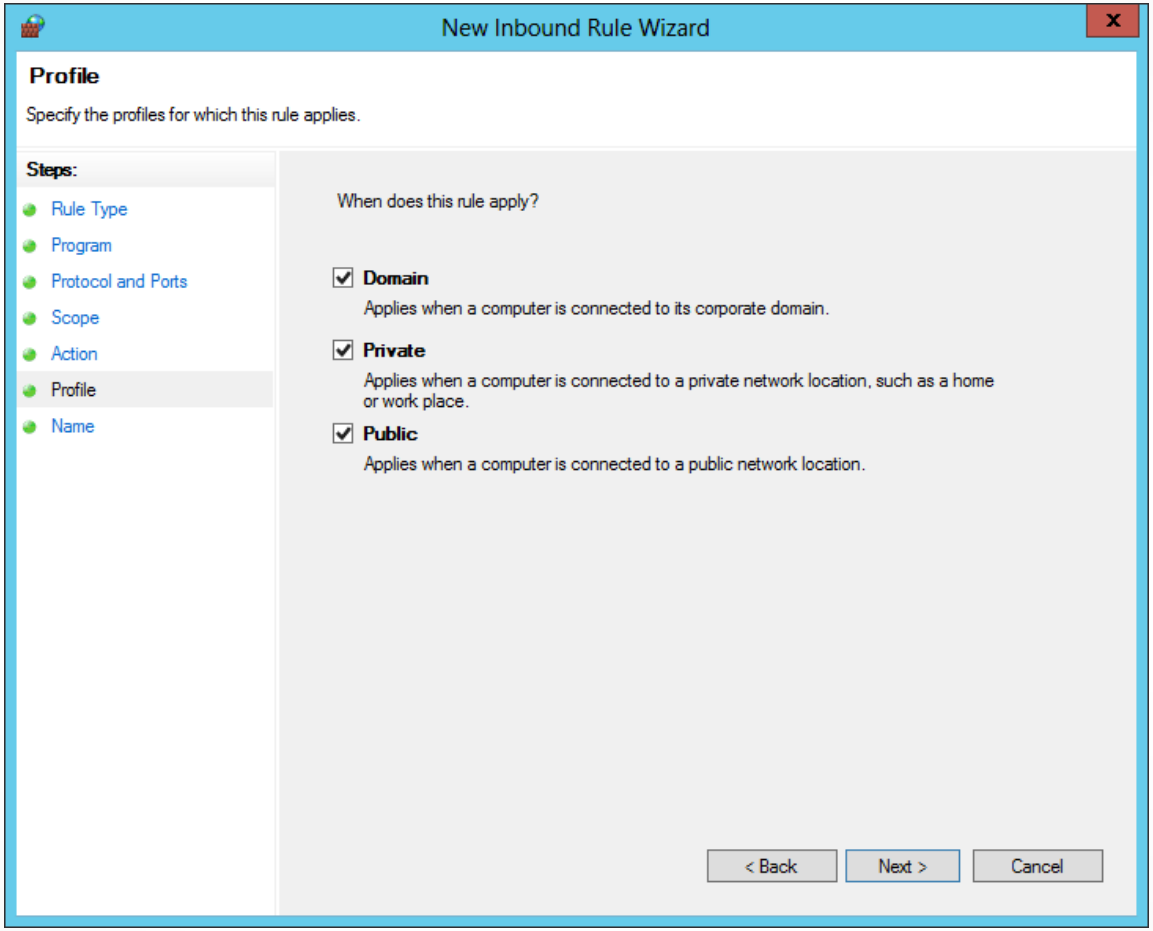
The Scope page of the New Inbound Rule Wizard

Creating Rules



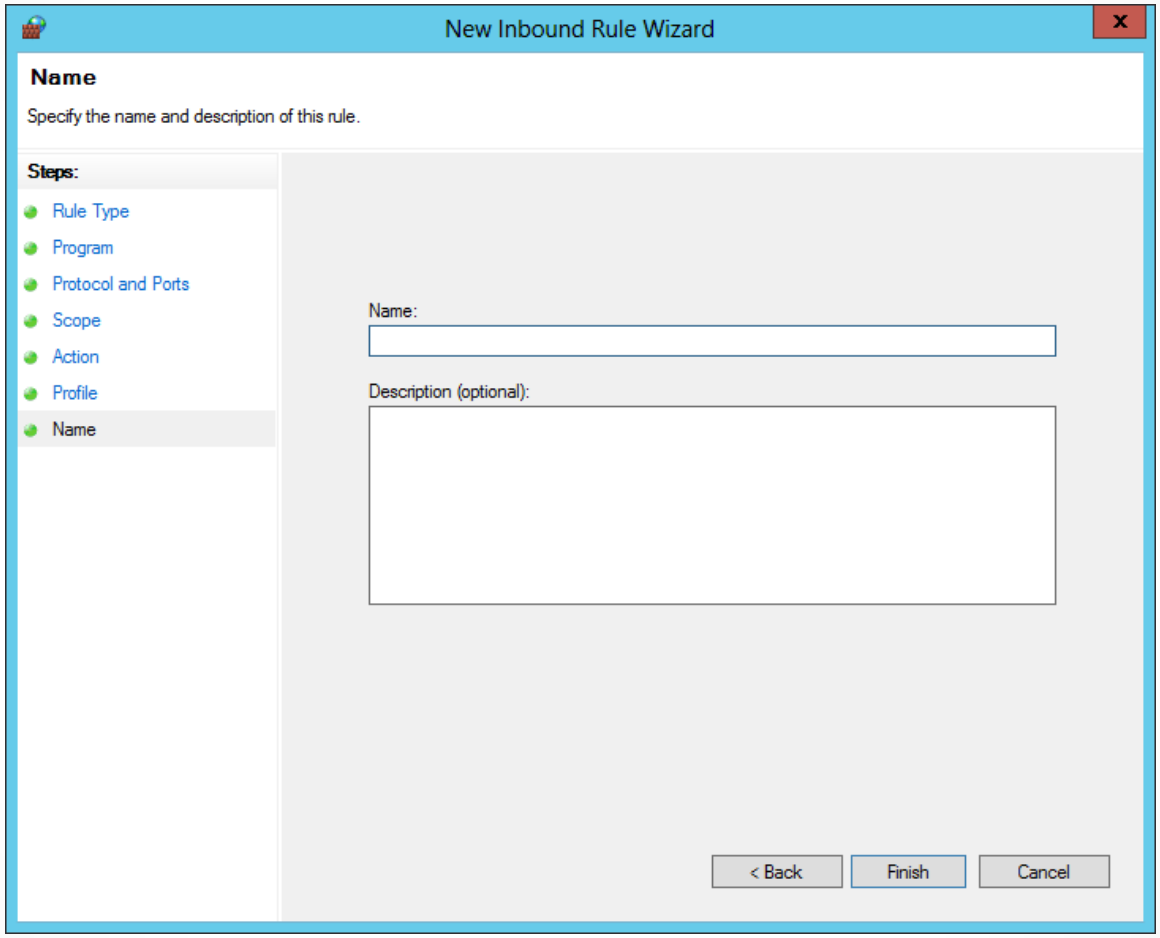
The Action page of the New Inbound Rule Wizard

Creating Rules



The Profile page of the New Inbound Rule Wizard

Creating Rules



The Name page of the New Inbound Rule Wizard

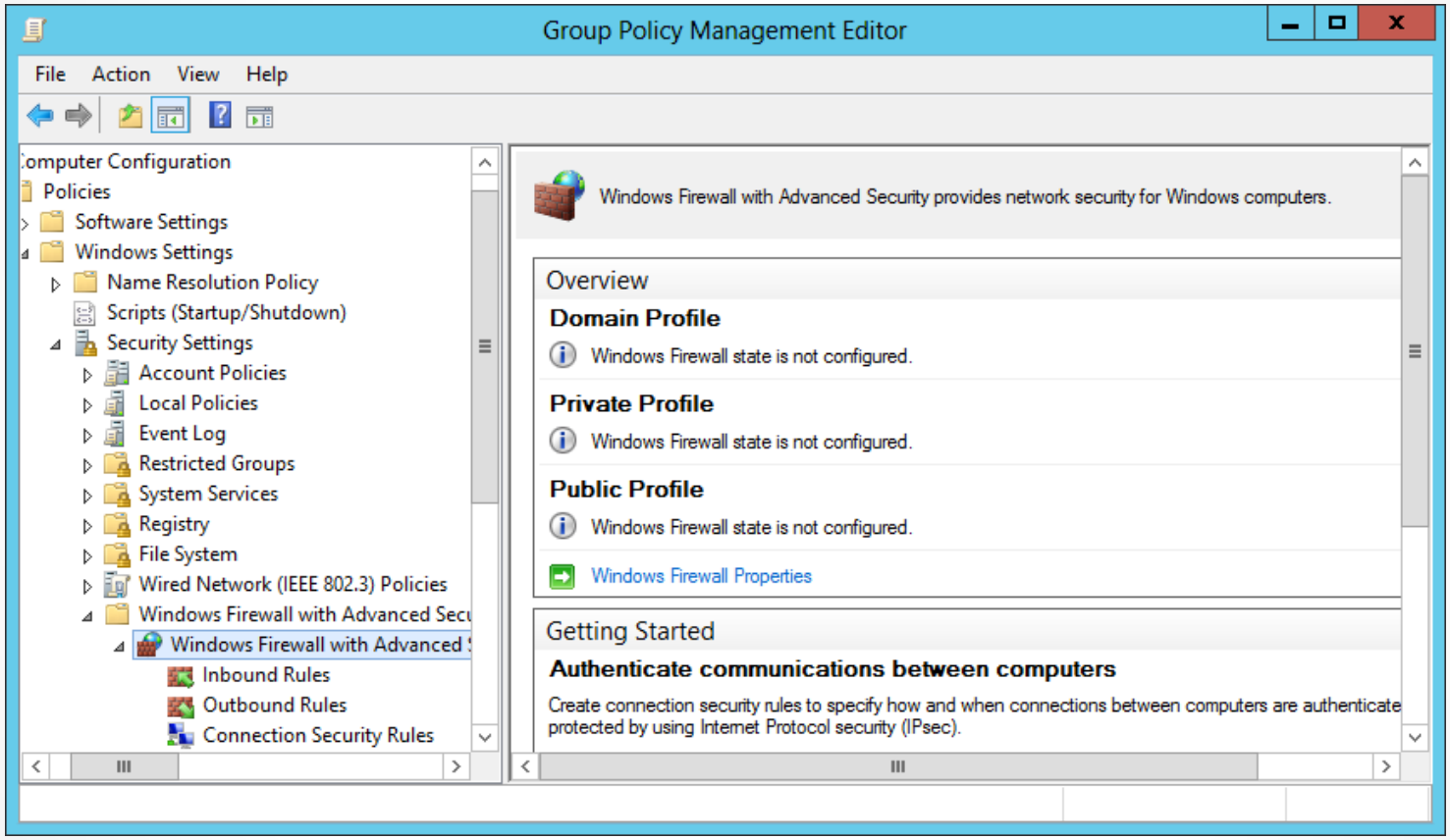
Importing and Exporting Rules

- 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

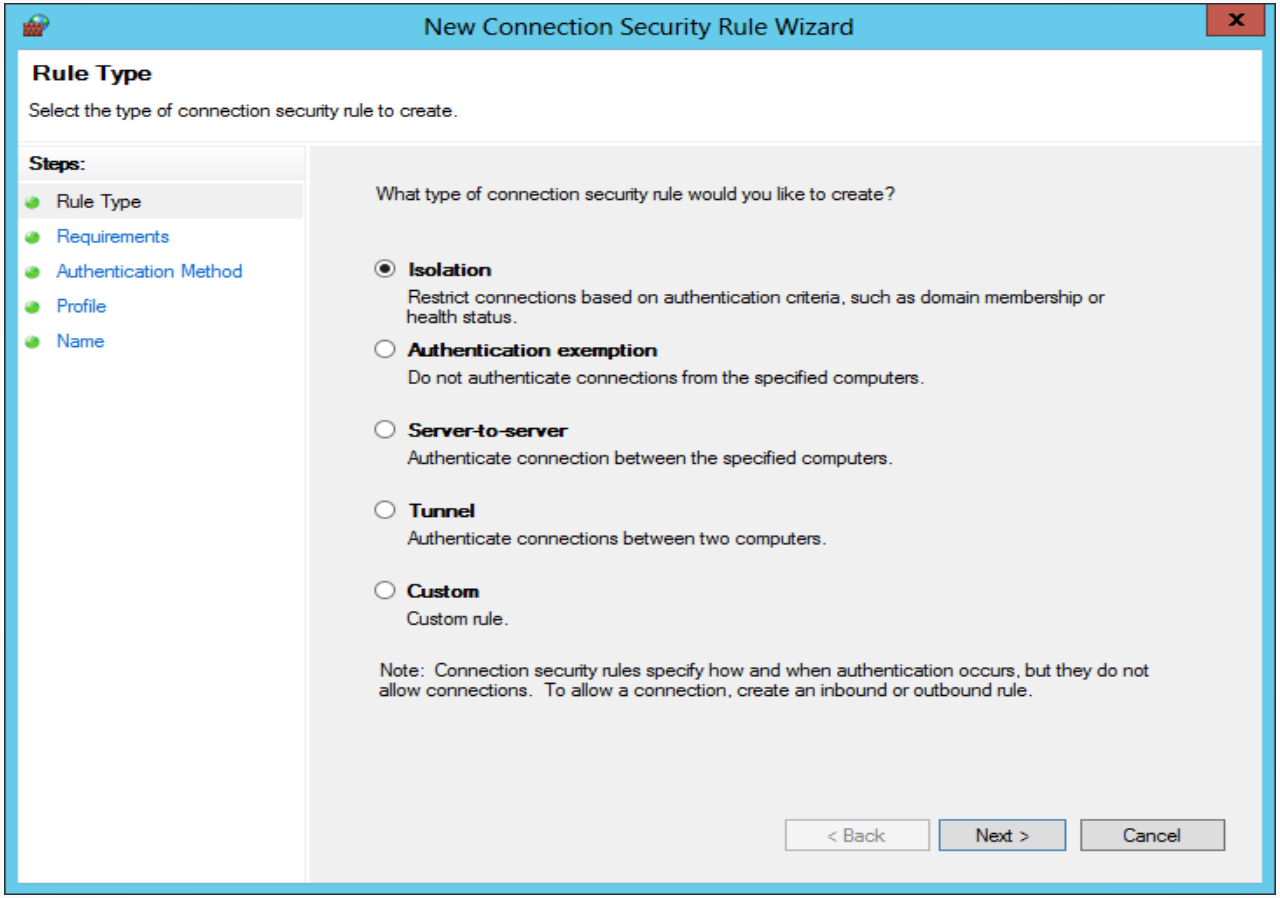
Using Filters

- 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

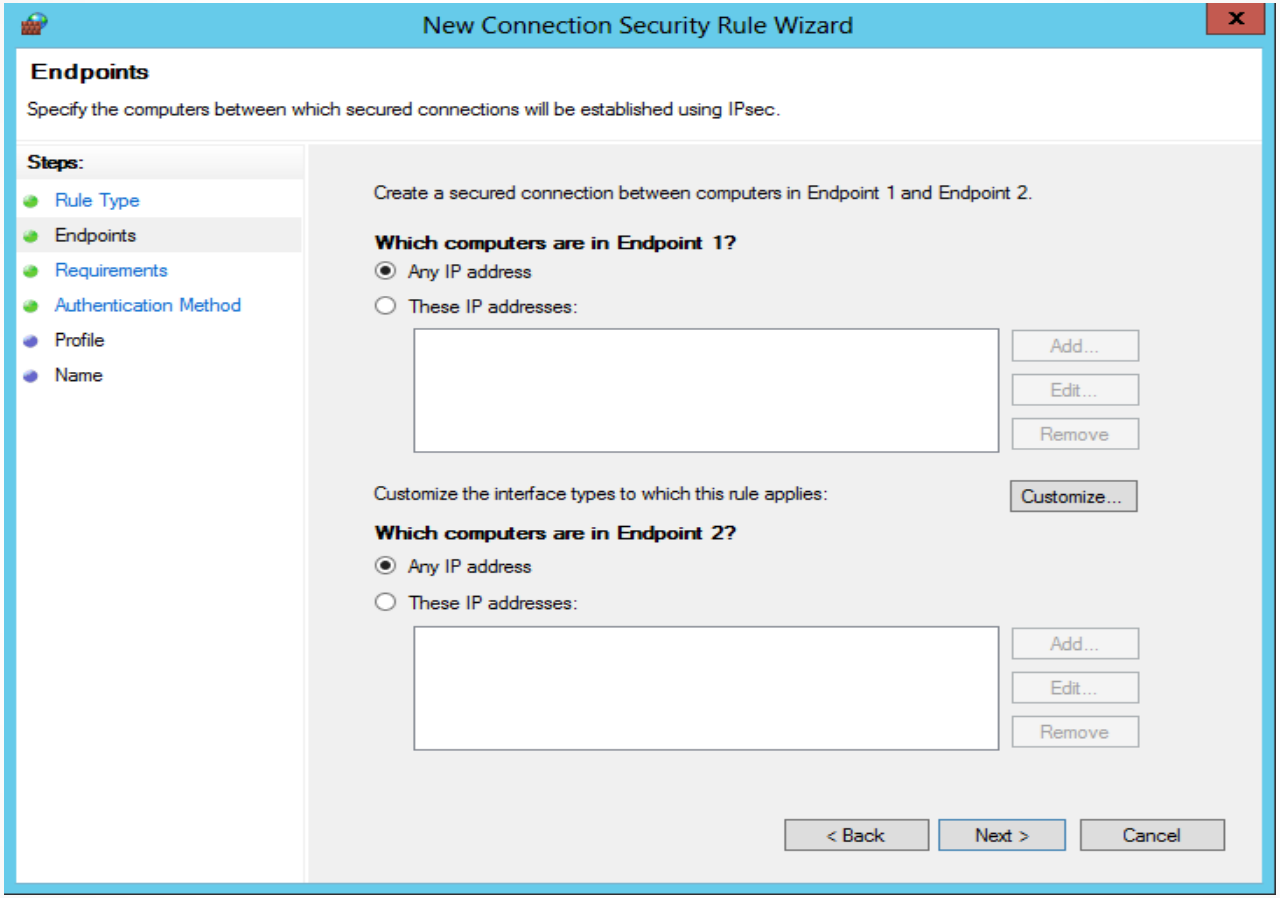
- The IP Security (IPsec) standards are a collection of documents that define a method for securing data while it is in transit over a TCP/IP network.
- IPsec includes a connection establishment routine, during which computers authenticate each other before transmitting data, and a technique called **tunneling**, 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



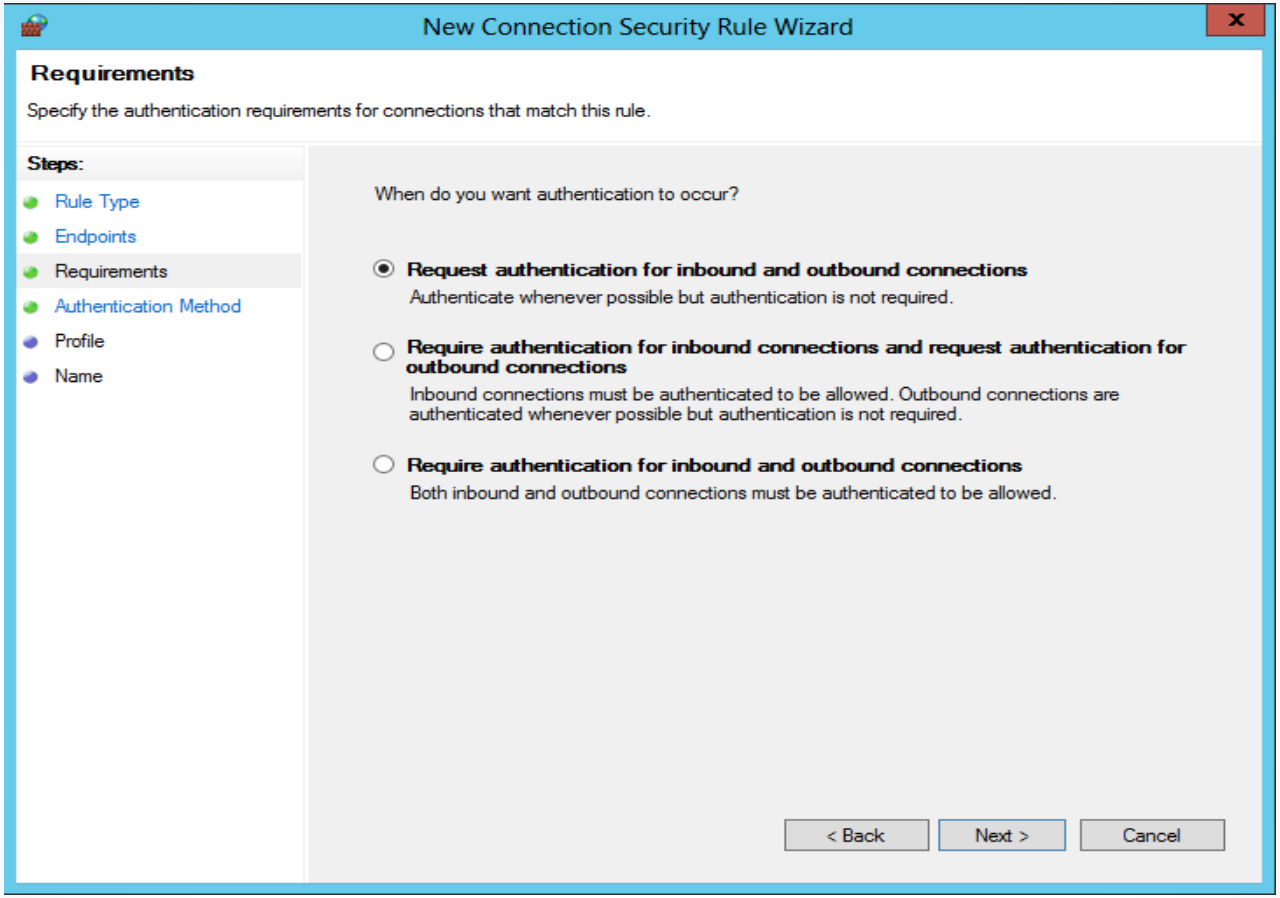
The Rule Type page in the New Connection Security Rule Wizard

Creating Connection Security Rules



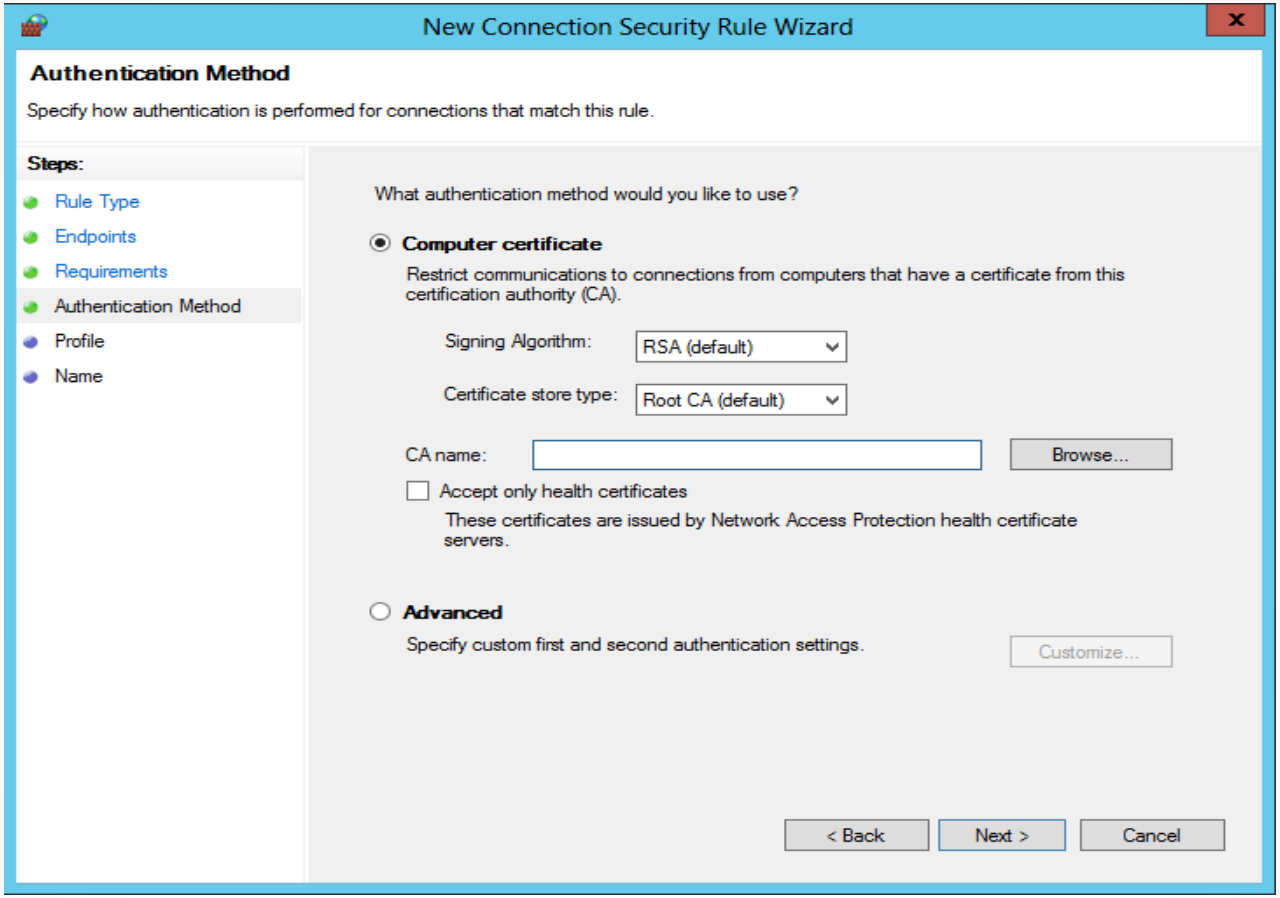
The Endpoints page in the New Connection Security Rule Wizard

Creating Connection Security Rules



The Requirements page in the New Connection Security Rule Wizard

Creating Connection Security Rules



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.