# Description

This article will detail how to perform the most common tasks with the windows firewall on Windows Server 2012. This includes managing the firewall settings and creating custom inbound and outbound firewall rules.

# Contents

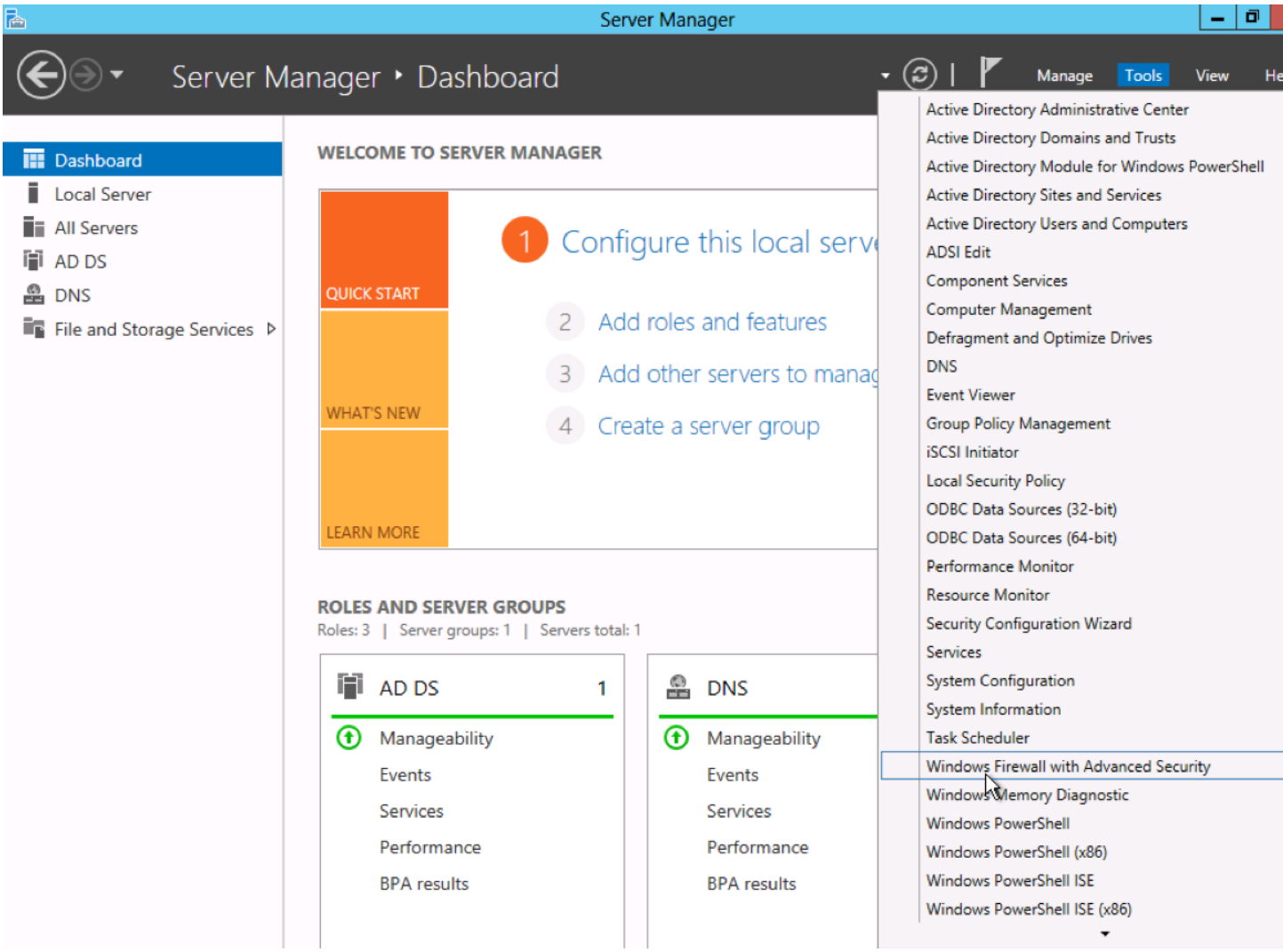


# Managing Firewall Settings

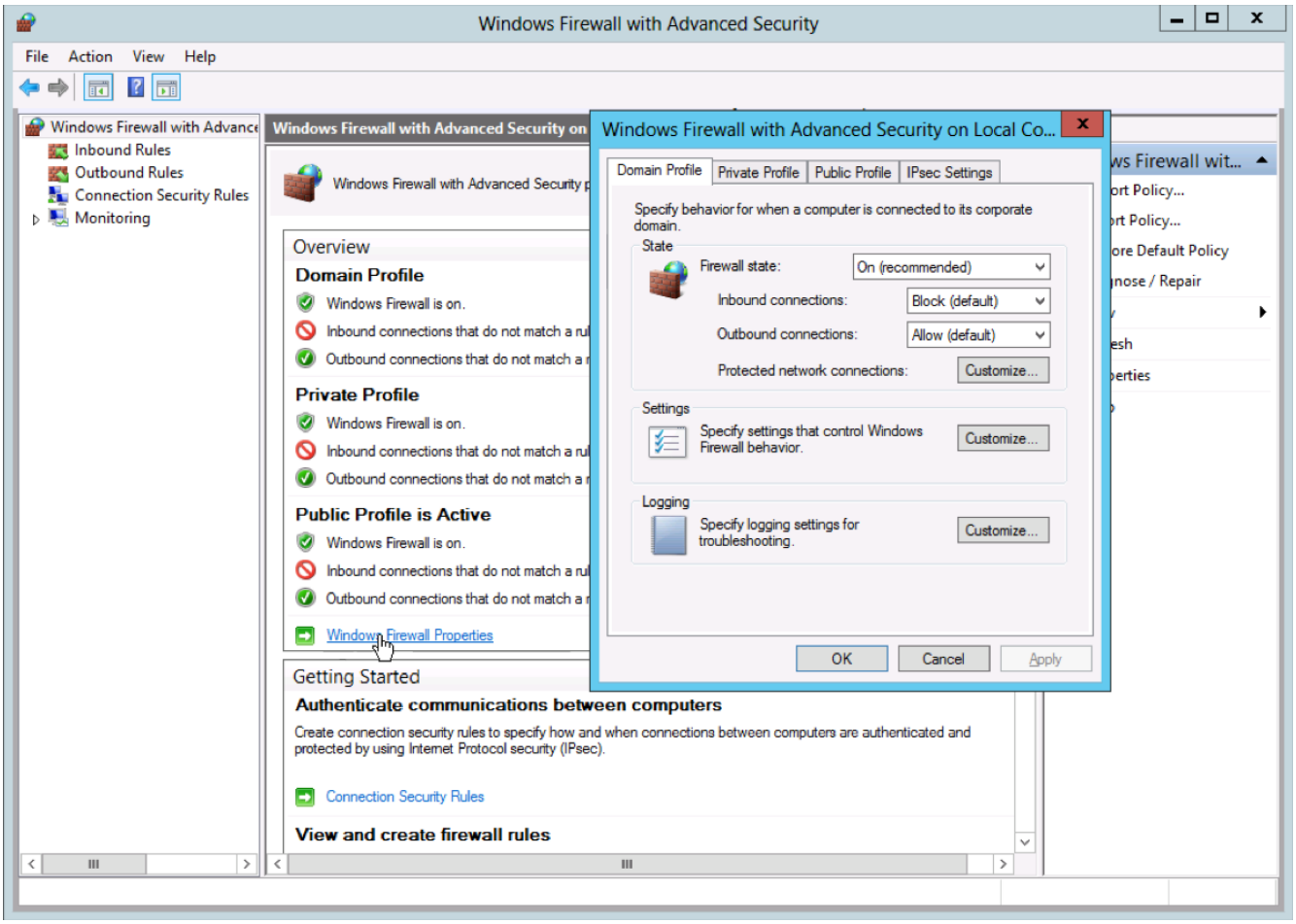
The Windows Firewall with Advanced Security is a host-based firewall that runs on Windows Server 2012 and is turned on by default. Firewall settings within Windows Server 2012 are managed from within the Windows Firewall MMC (Microsoft Management Console). To review and set Firewall settings perform the following:

1. Open the **Server Manager** from the task bar.

2. Click the **Tools menu** and select **Windows Firewall with Advanced Security**.




3. First review the current configuration settings by selecting **Windows Firewall Properties** from the MMC landing page. This **allows access to modify the settings** for each of the three firewall profiles, **Domain, Private, and Public** as well as IPSec settings.



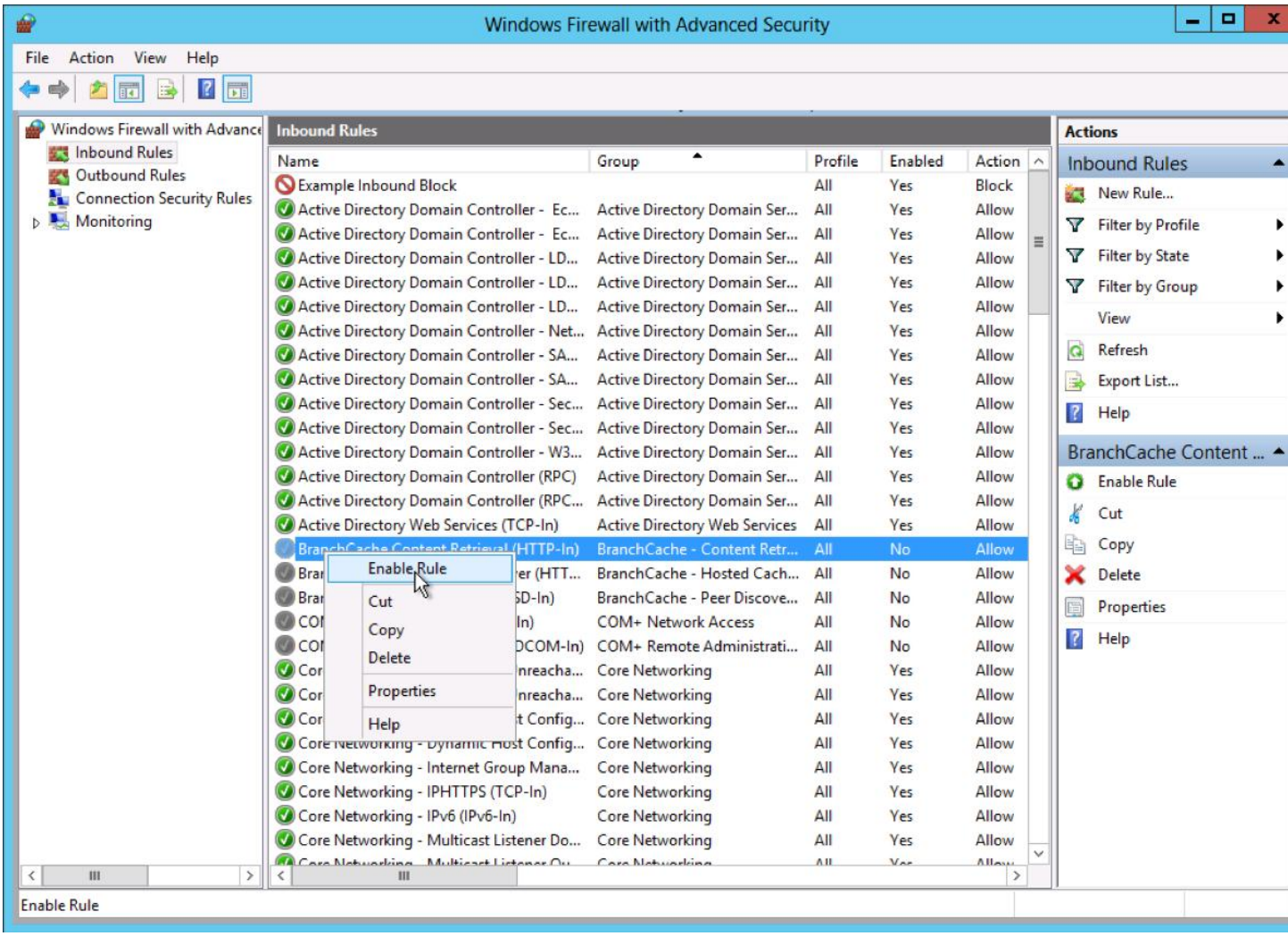

# Applying Custom Rules

Custom Rules allow the finest level of control over inbound and outbound traffic to your Windows Server 2012.

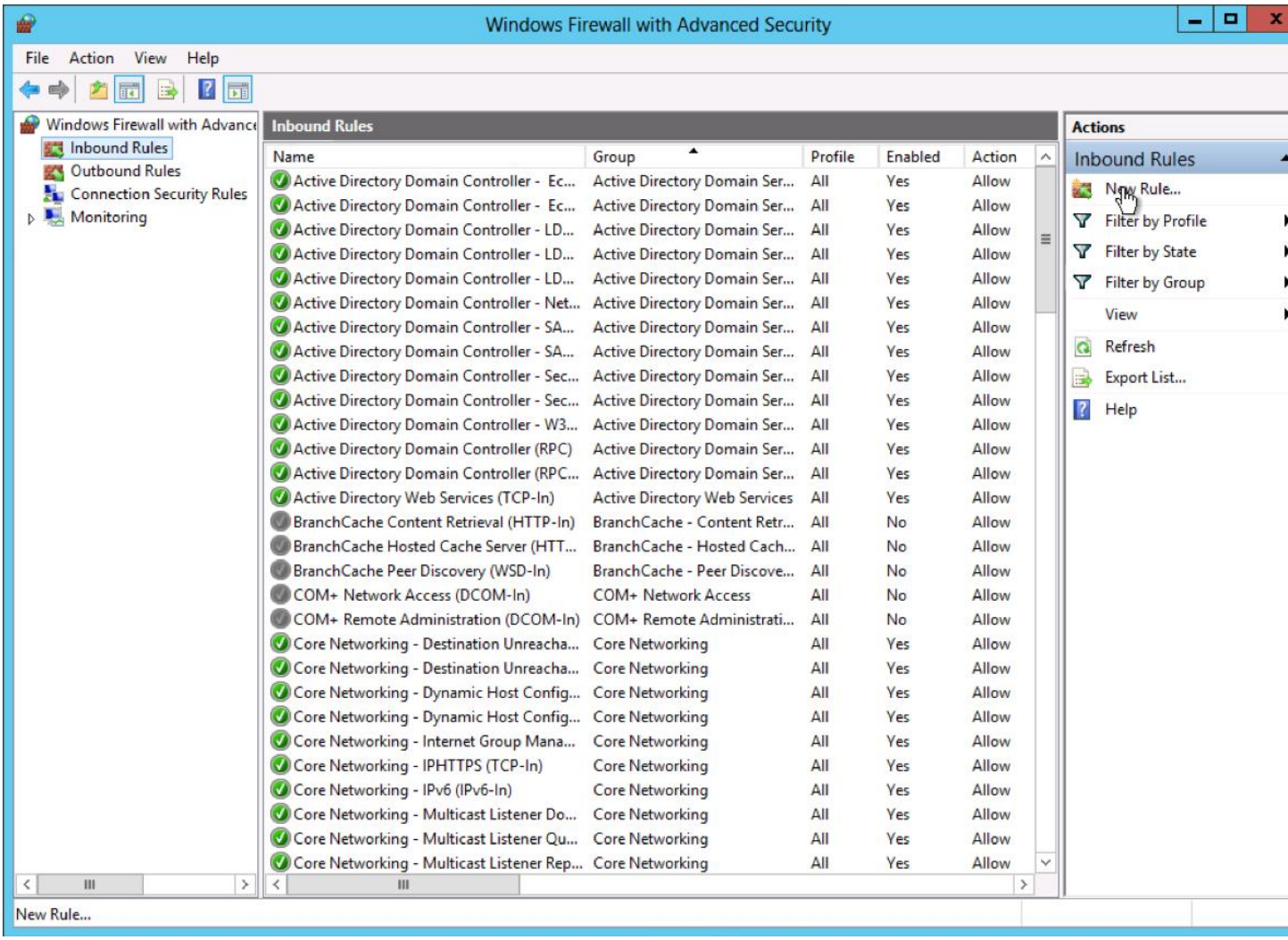
1. If you have not done so already load the Windows Firewall MMC by opening the **Server Manager** from the task bar, clicking the **Tools menu**, and selecting **Windows Firewall with Advanced Security**.

2. Select either **Inbound Rules** or **Outbound Rules** under **Windows Firewall with Advanced Security** on the left side of the management console.

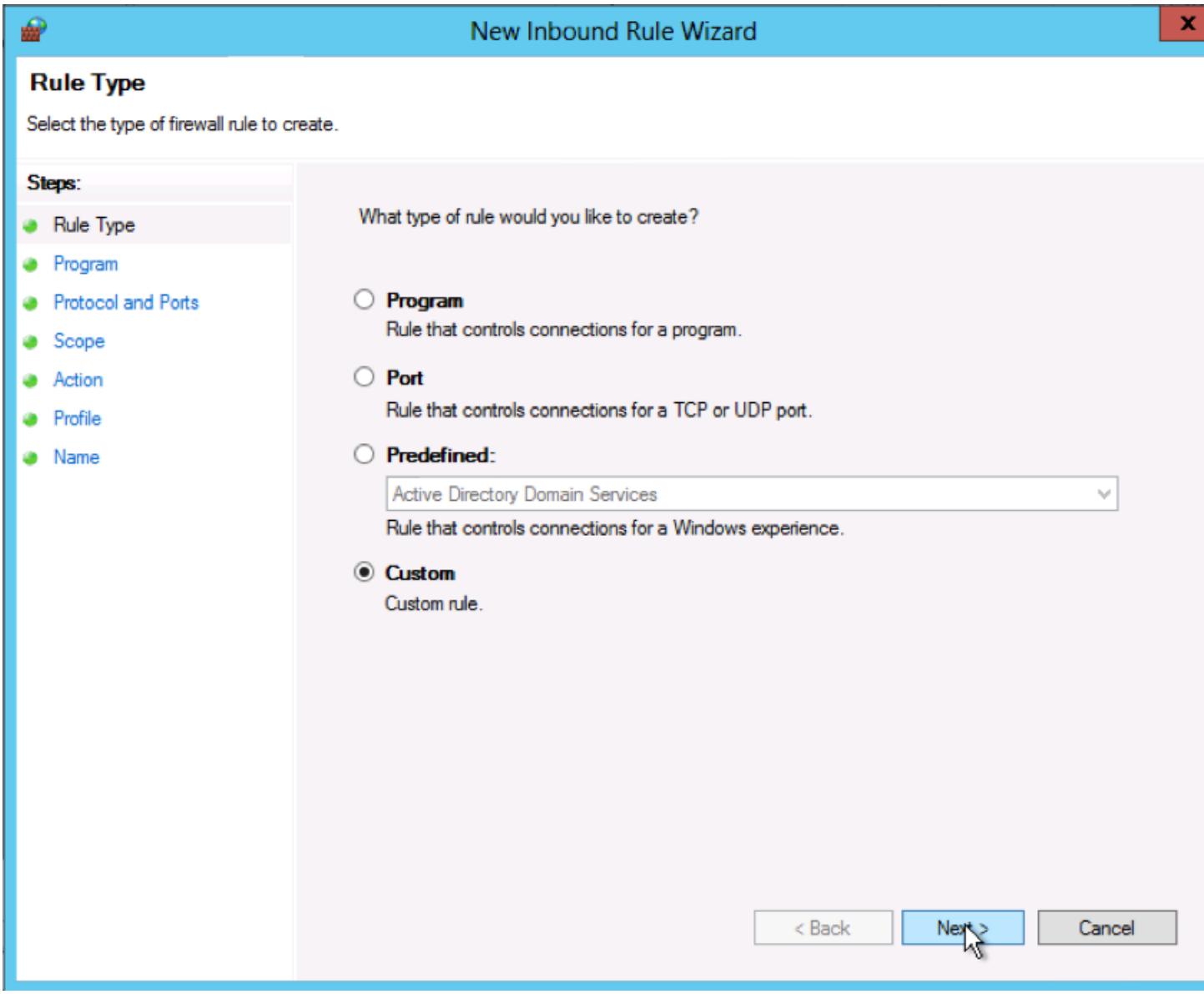
*Note: This will provide a listing on each of the currently configured firewall rules. Rules that are currently enabled are denoted by green checkbox icon, while disabled rules display a grey checkbox icon. Rightclicking a rule will allow you toggle enable/disable.*



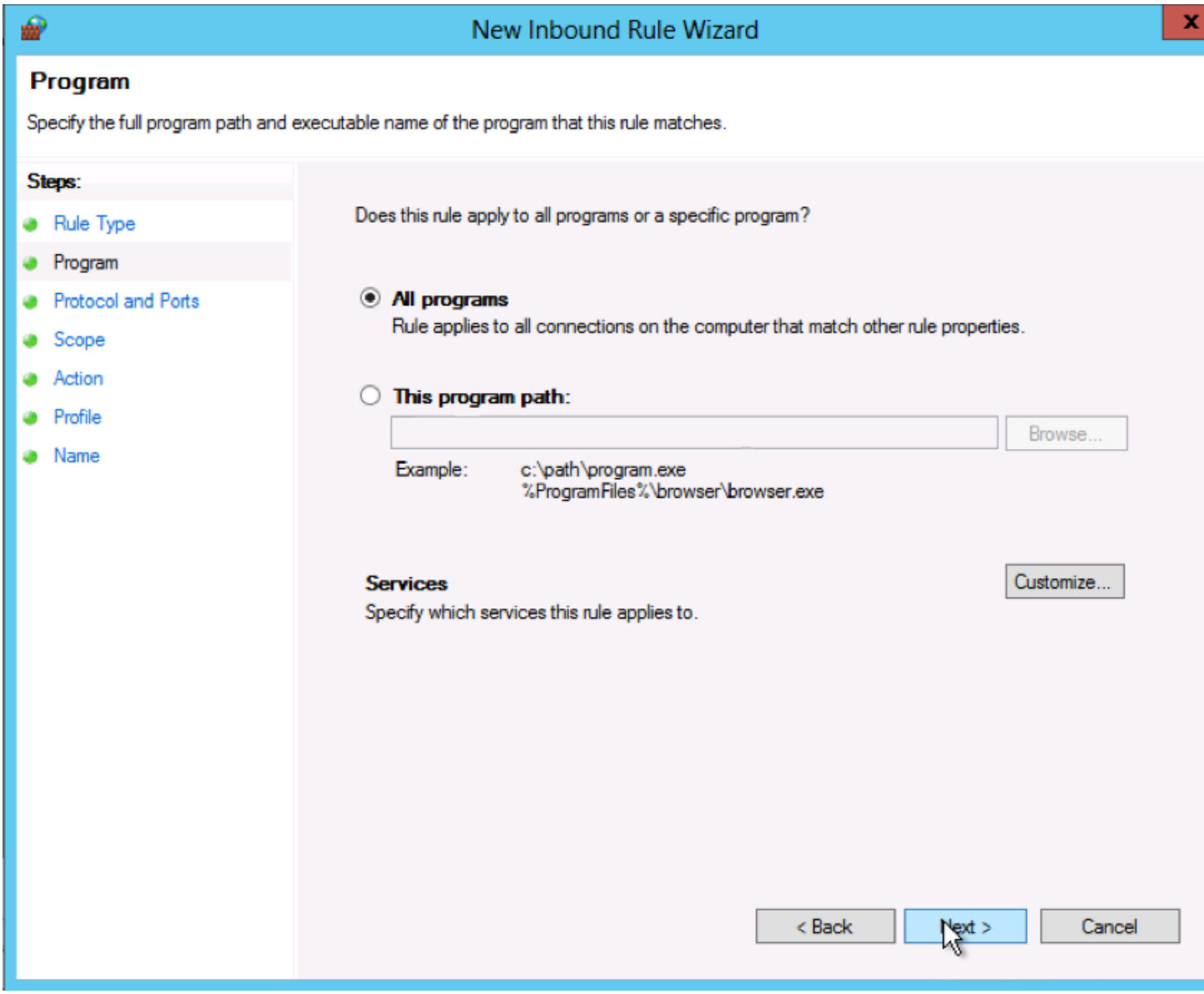

3. From the right side of either the **Inbound Rules** or **Outbound Rules** tab click **New Rule**.




4. Select **Custom** from the Rule Type radial button and click **Next**.

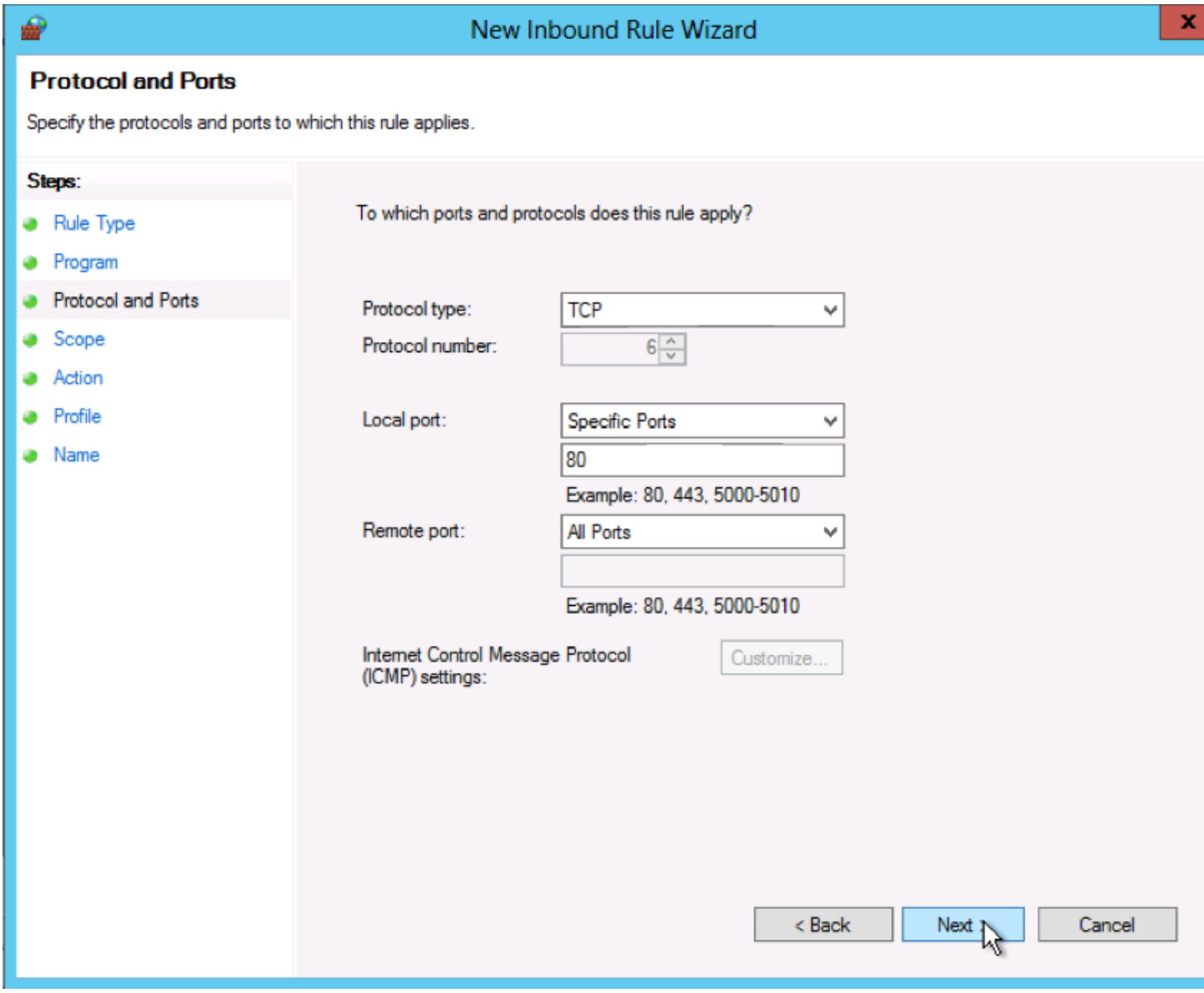



5. **Select the Program association** for the Custom Firewall Rule either All programs or the path to a program and click **Next**.

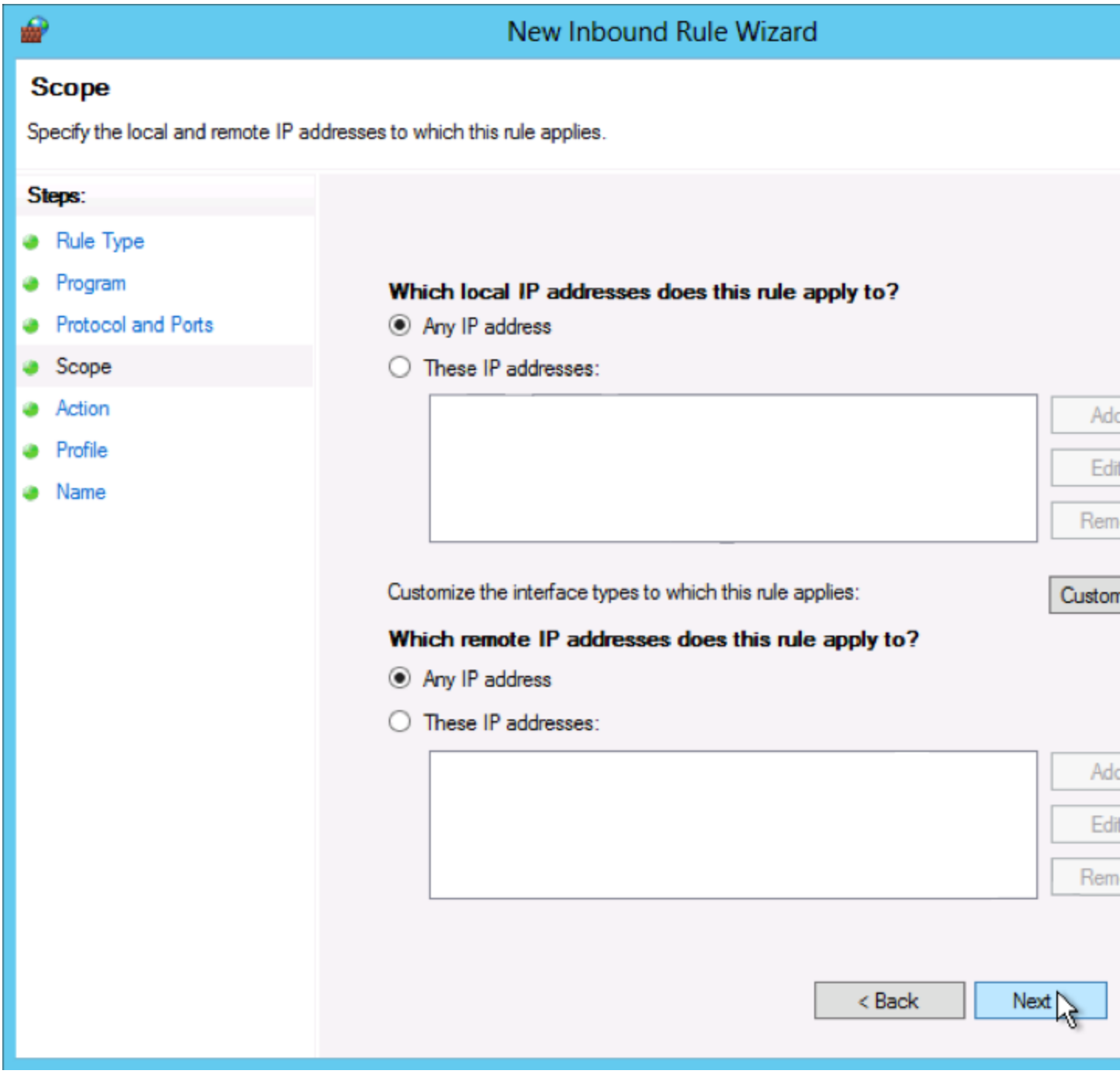



6. From the Protocol type field **select the protocol type** and click **Next**.

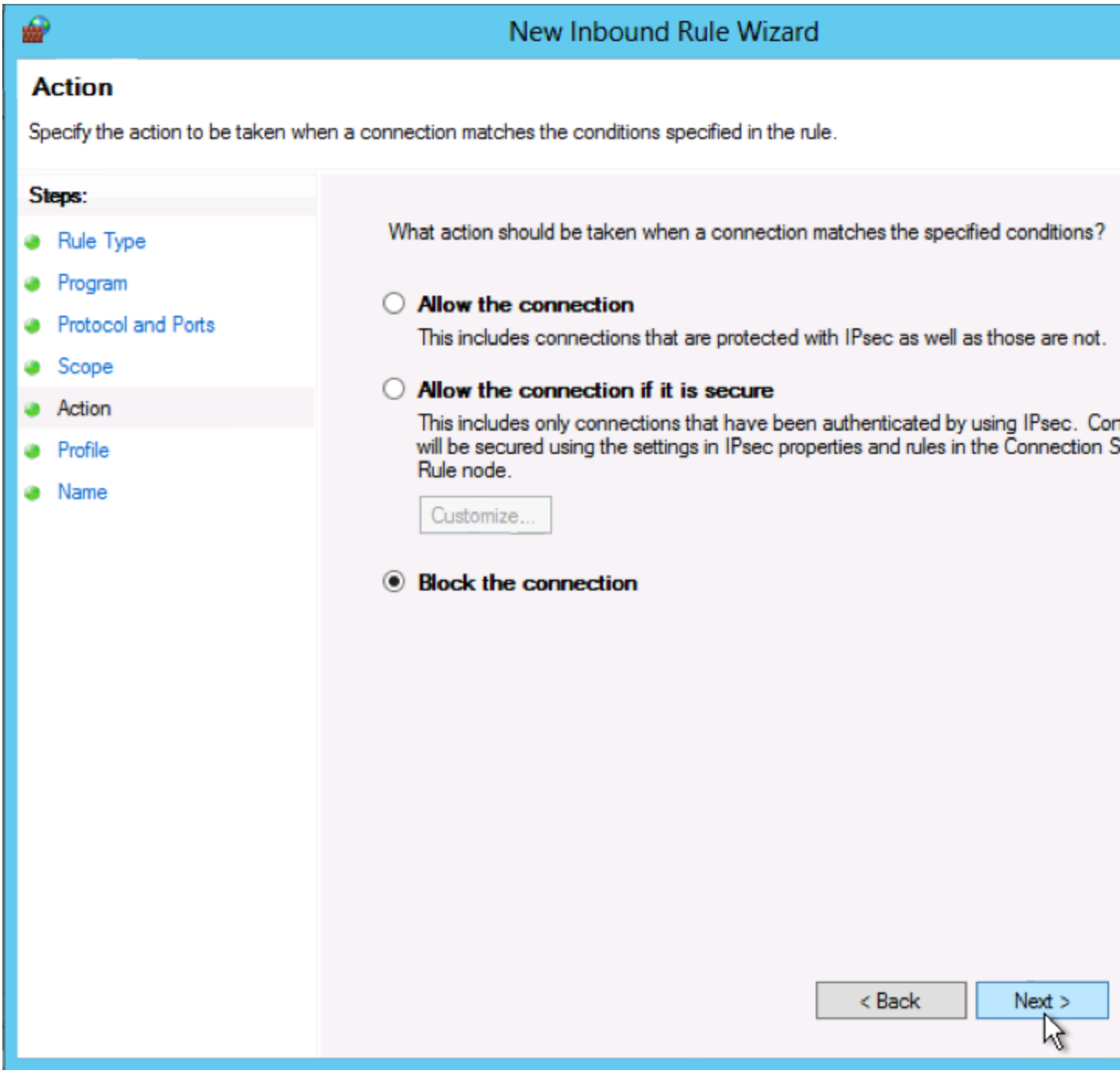
*Note: This walkthrough uses TCP on port 80 (HTTP) for example purposes.*



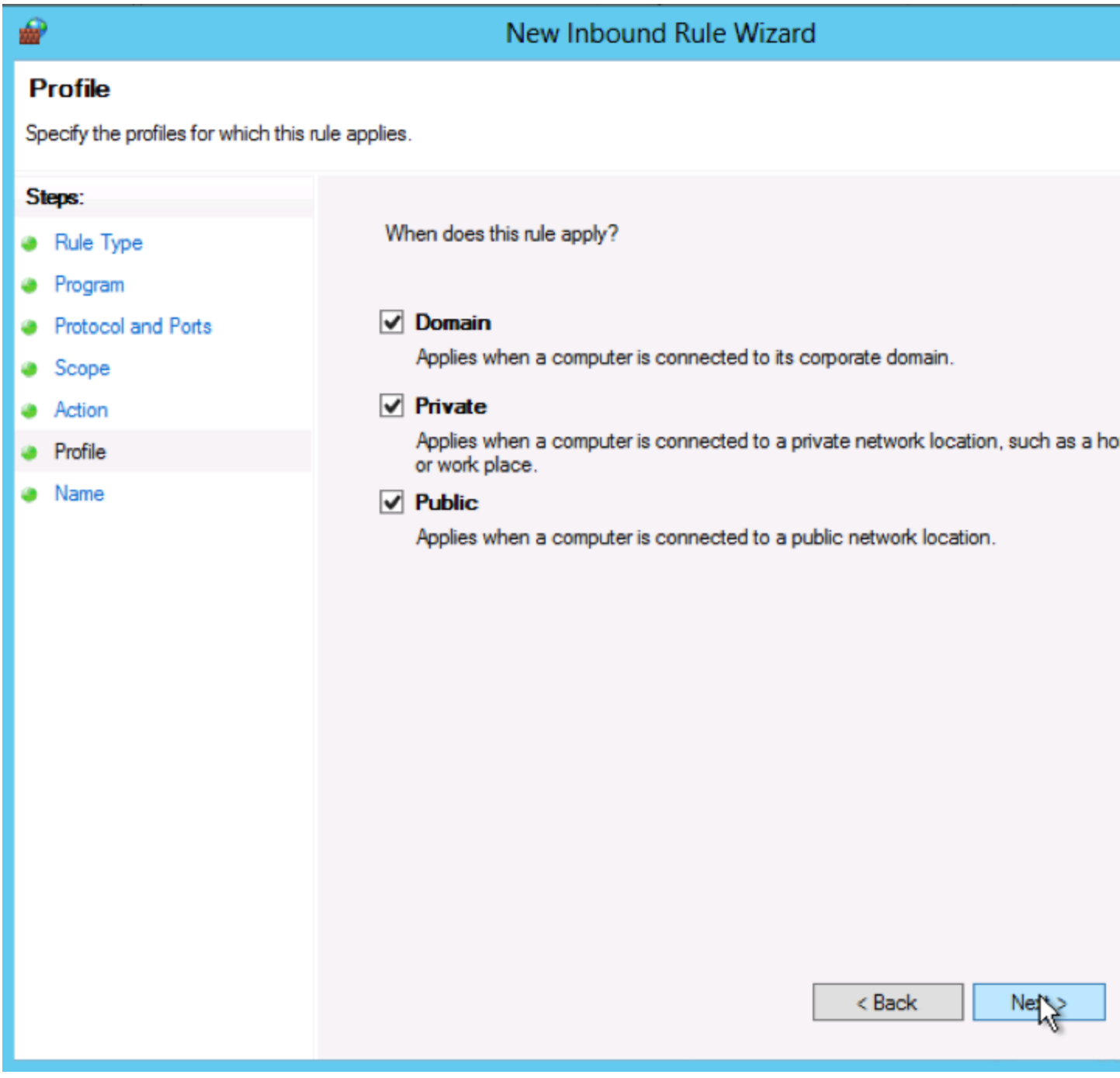

7. **Select an IP address association** for both local and remote addresses and click **Next**.



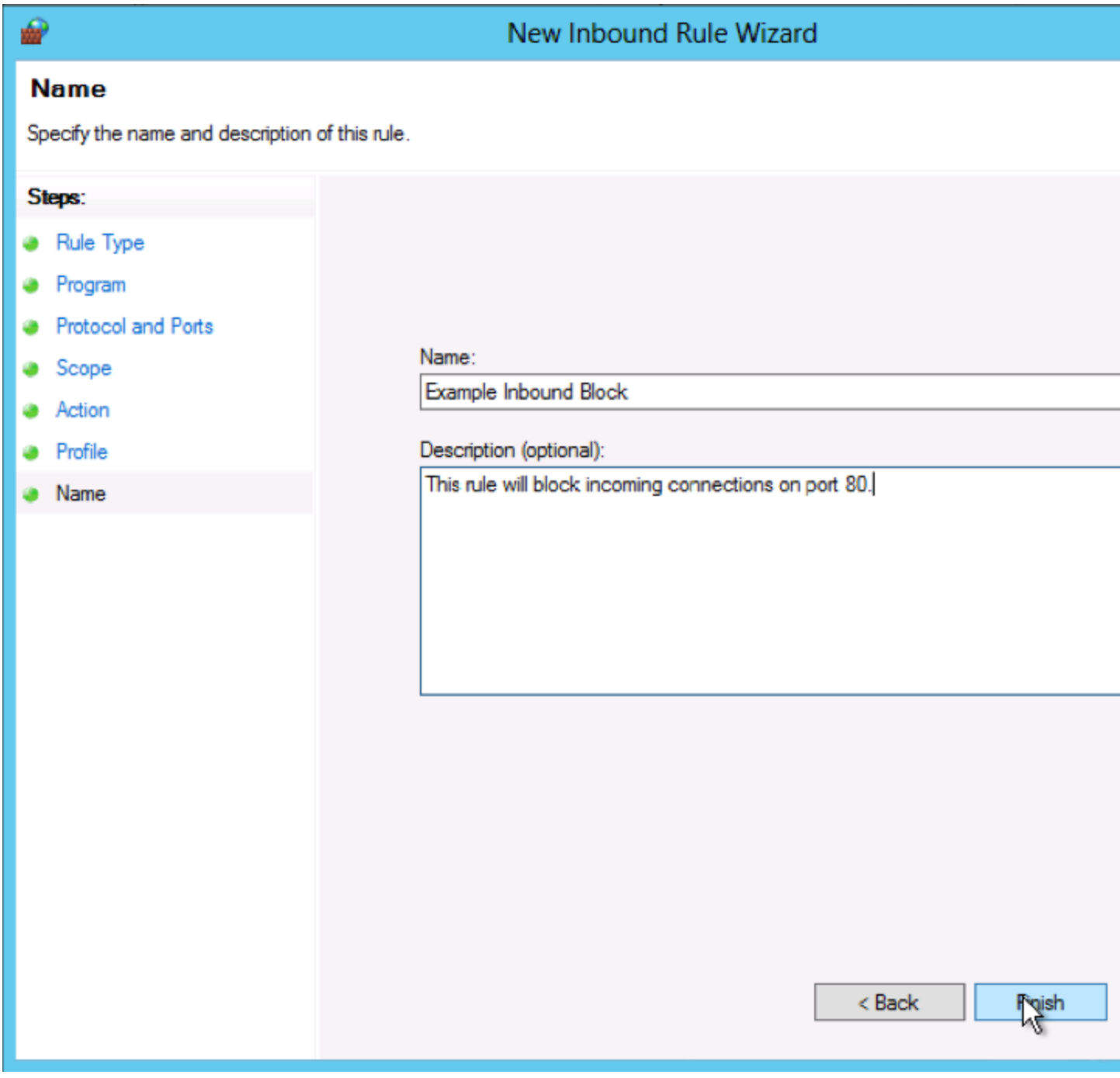

8. Select an action to take on matching traffic and click **Next**.



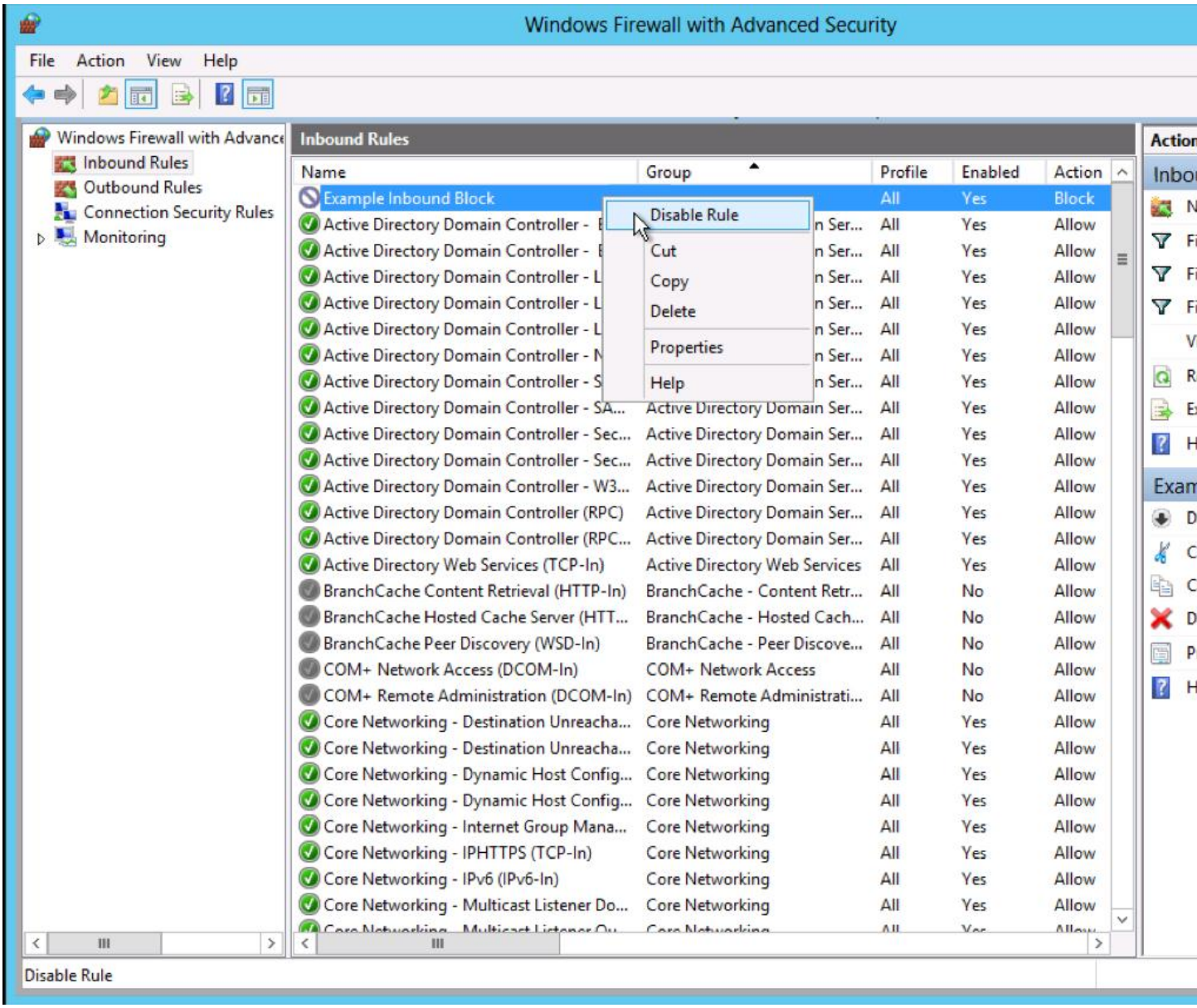

9. Select the profiles associated with the custom rule and click **Next**.




10. Provide a name for your Firewall rule and an optional description and click **Finish**.




11. Once created the rule will be enabled. The firewall rule can be found on the corresponding Rule tab, either inbound or outbound depending on the type created. To disable or delete the rule find the rule in the MMC, right-click it, and select either Disable Rule or Delete.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Example Inbound Block
All
Yes
Block
Disable Rule
Cut
Copy
Delete
Properties
Help
Active Directory Domain Controller - E
Active Directory Domain Controller - E
Active Directory Domain Controller - L
Active Directory Domain Controller - L
Active Directory Domain Controller - L
Active Directory Domain Controller - N
Active Directory Domain Controller - S
Active Directory Domain Controller - SA...
Active Directory Domain Controller - Sec...
Active Directory Domain Controller - Sec...
Active Directory Domain Controller - W3...
Active Directory Domain Controller (RPC)
Active Directory Domain Controller (RPC...
Active Directory Web Services (TCP-In)
BranchCache Content Retrieval (HTTP-In)
BranchCache Hosted Cache Server (HTT...
BranchCache Peer Discovery (WSD-In)
COM+ Network Access (DCOM-In)
COM+ Remote Administration (DCOM-In)
Core Networking - Destination Unreacha...
Core Networking - Destination Unreacha...
Core Networking - Dynamic Host Config...
Core Networking - Dynamic Host Config...
Core Networking - Internet Group Mana...
Core Networking - IPHTTPS (TCP-In)
Core Networking - IPv6 (IPv6-In)
Core Networking - Multicast Listener Do...
Active Directory Domain Ser...
Active Directory Web Services
BranchCache - Content Retr...
BranchCache - Hosted Cach...
BranchCache - Peer Discove...
COM+ Network Access
COM+ Remote Administrati...
Core Networking
All
Yes
No
Allow
Disable Rule