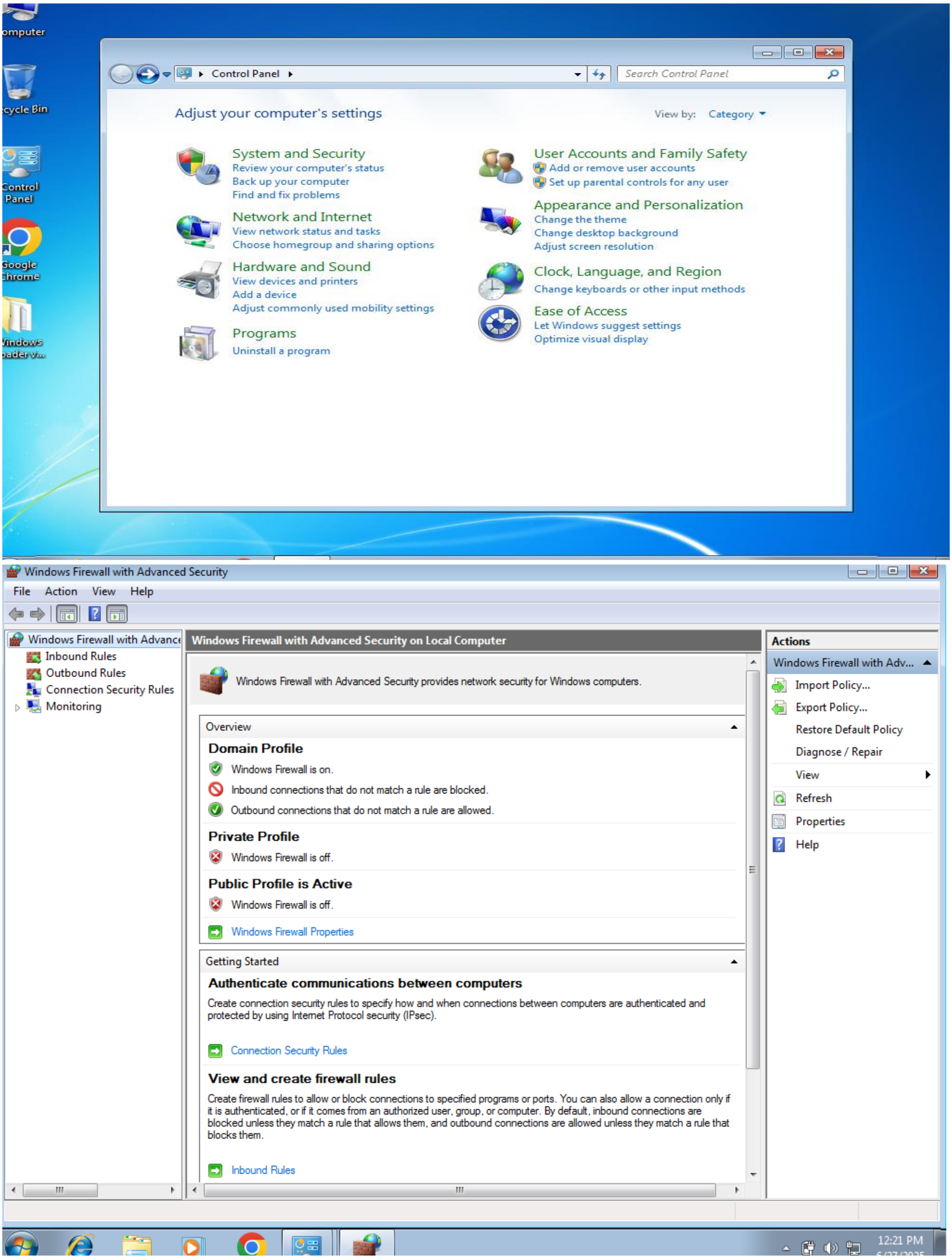
Setup and use a Firewall on Windows

Step 1: Open Windows Firewall with Advanced Security

1. Click Start → Search for Windows Firewall with Advanced Security and open it.
2. You'll see the main console with sections for Inbound Rules, Outbound Rules, etc.



Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Back up your computer
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program

User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user

Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution

Clock, Language, and Region
Change keyboards or other input methods

Ease of Access
Let Windows suggest settings
Optimize visual display

Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile
- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile
- Windows Firewall is off.

Public Profile is Active
- Windows Firewall is off.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

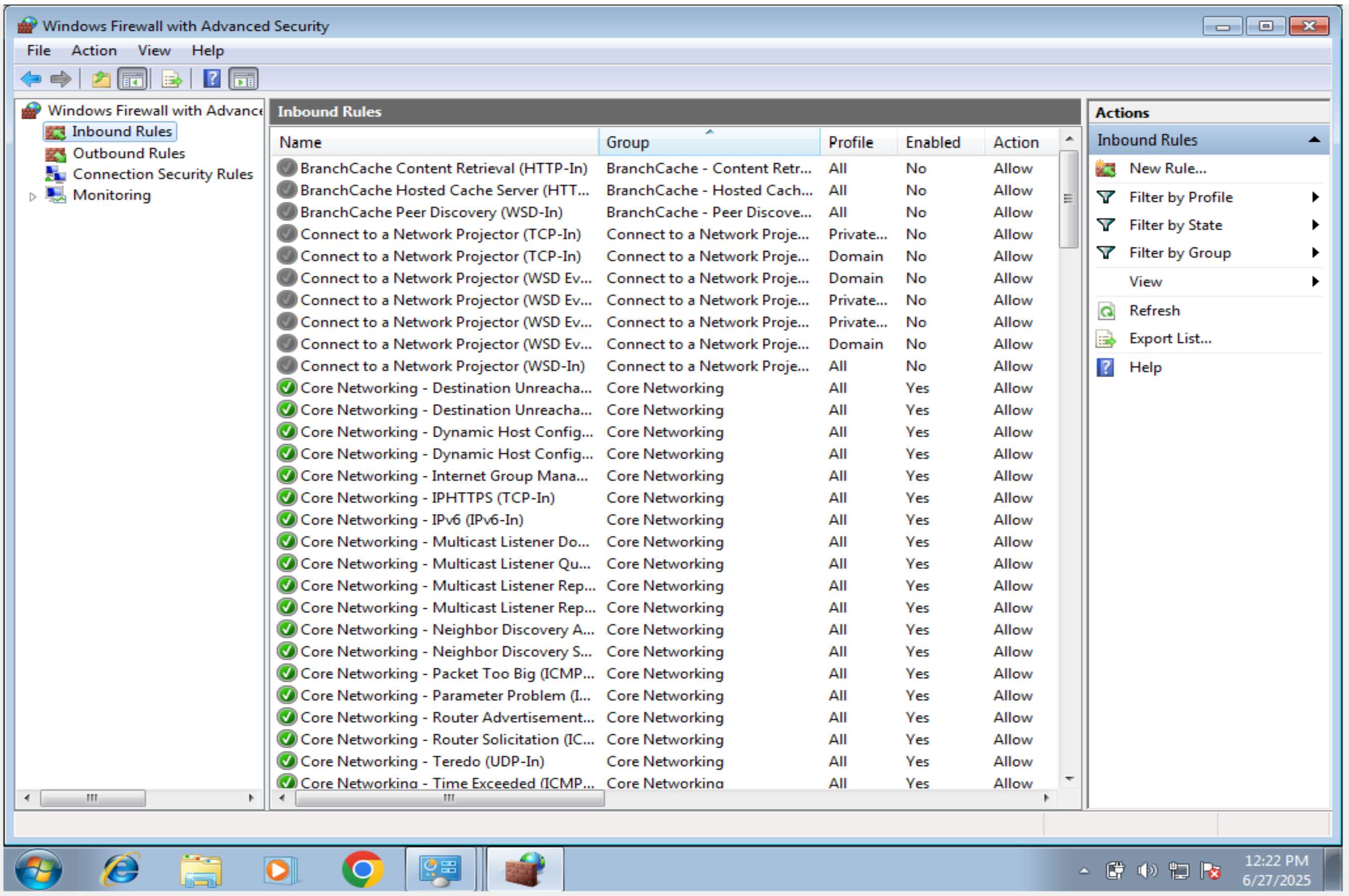
View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Step 2: Create a New Inbound Rule

1. On the left, click Inbound Rules.
2. On the right panel, click New Rule...



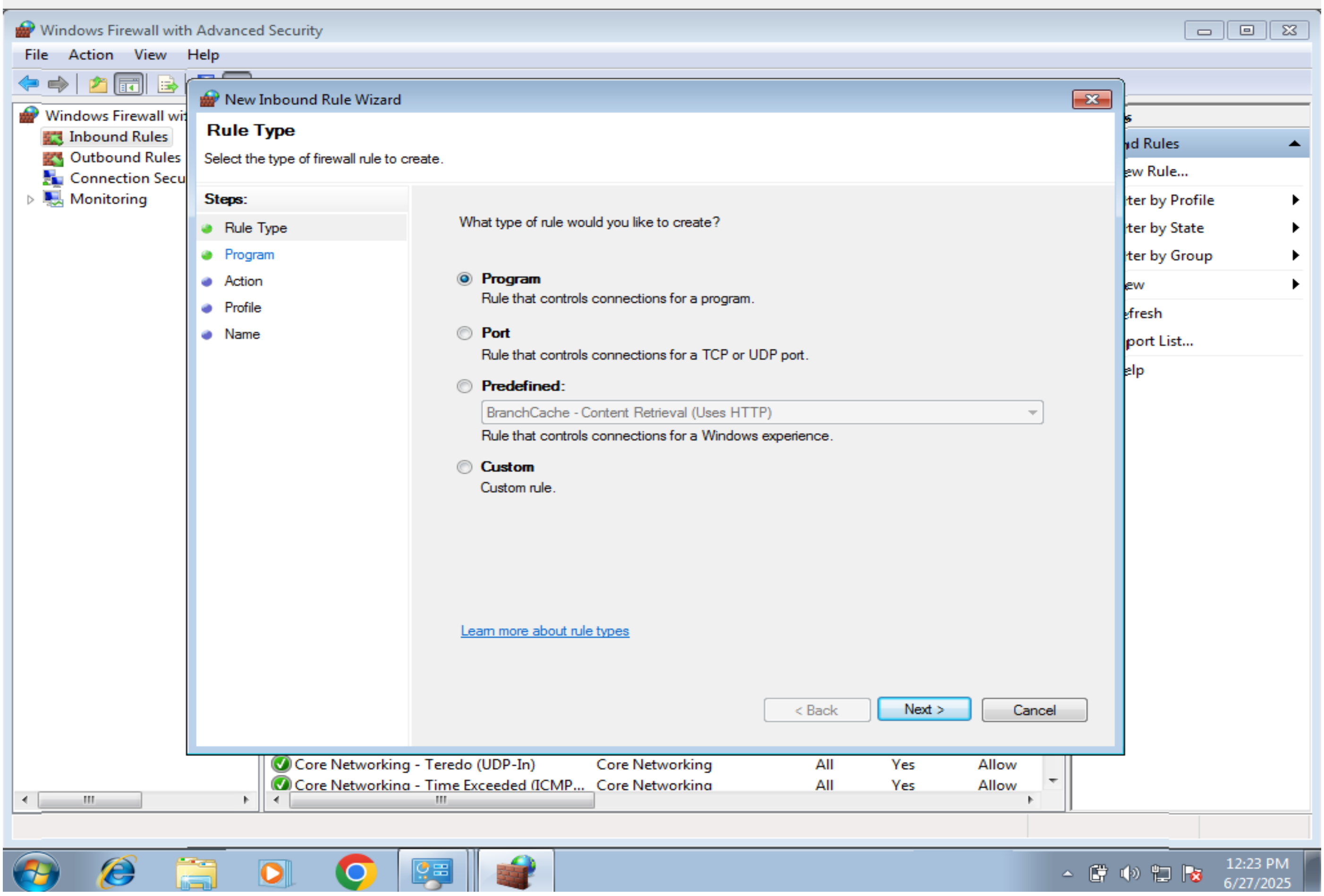
Inbound Rules

Name	Group	Profile	Enabled	Action
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	All	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow

Step 3: Configure the Rule

1. Rule Type: Select Port, click Next.
2. Protocol and Ports:
   - Select TCP.
   - Enter 23 in the "Specific local ports" field.
   - Click Next.
3. Action: Choose Block the connection. Click Next.
4. Profile: Keep all options checked (Domain, Private, Public). Click Next.
5. Name the Rule:
   - Name: Block Telnet Inbound
   - Description (optional): Blocks inbound TCP traffic on port 23 (Telnet)

- Click Finish.



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

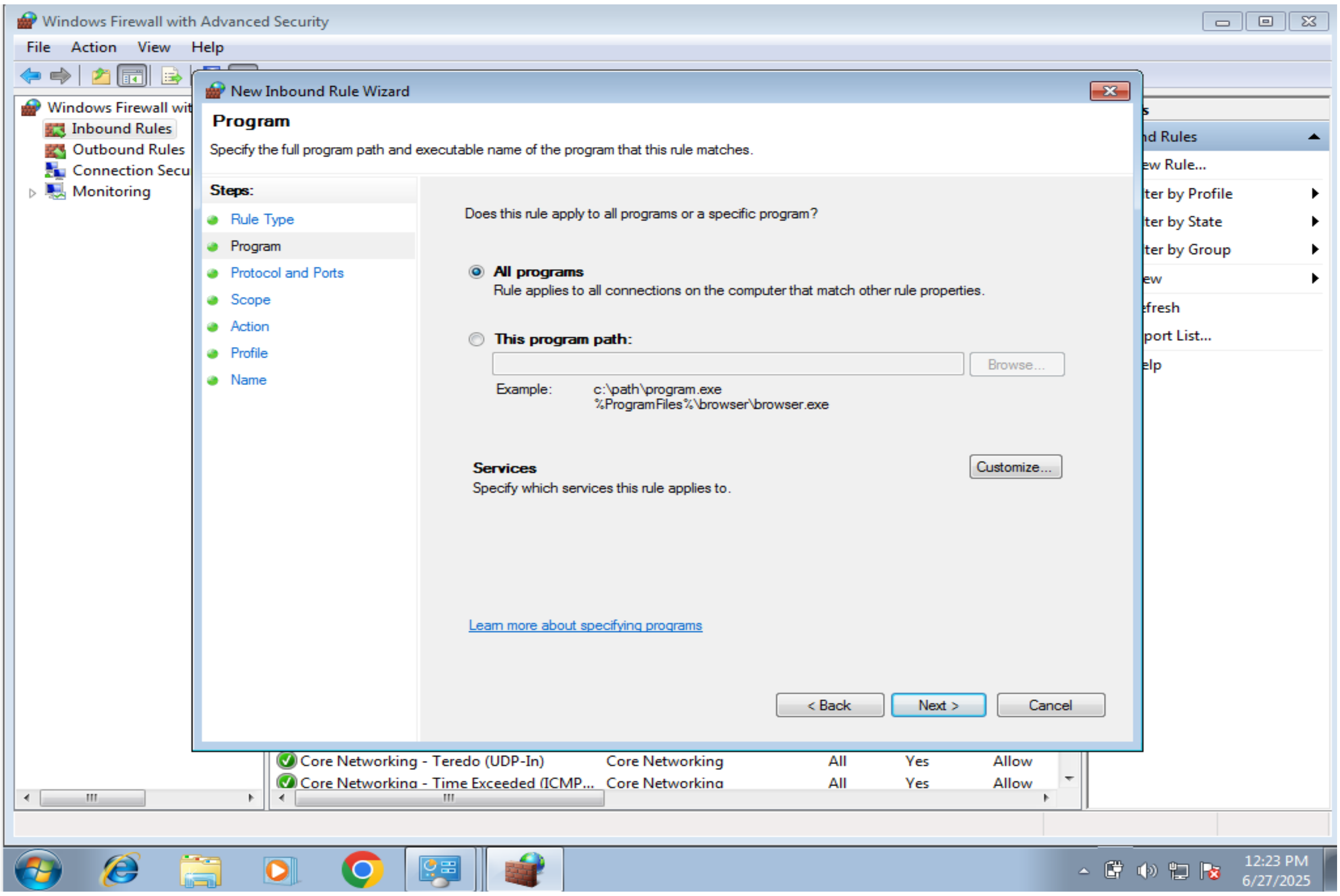
● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow



Program

Specify the full program path and executable name of the program that this rule matches.

Does this rule apply to all programs or a specific program?

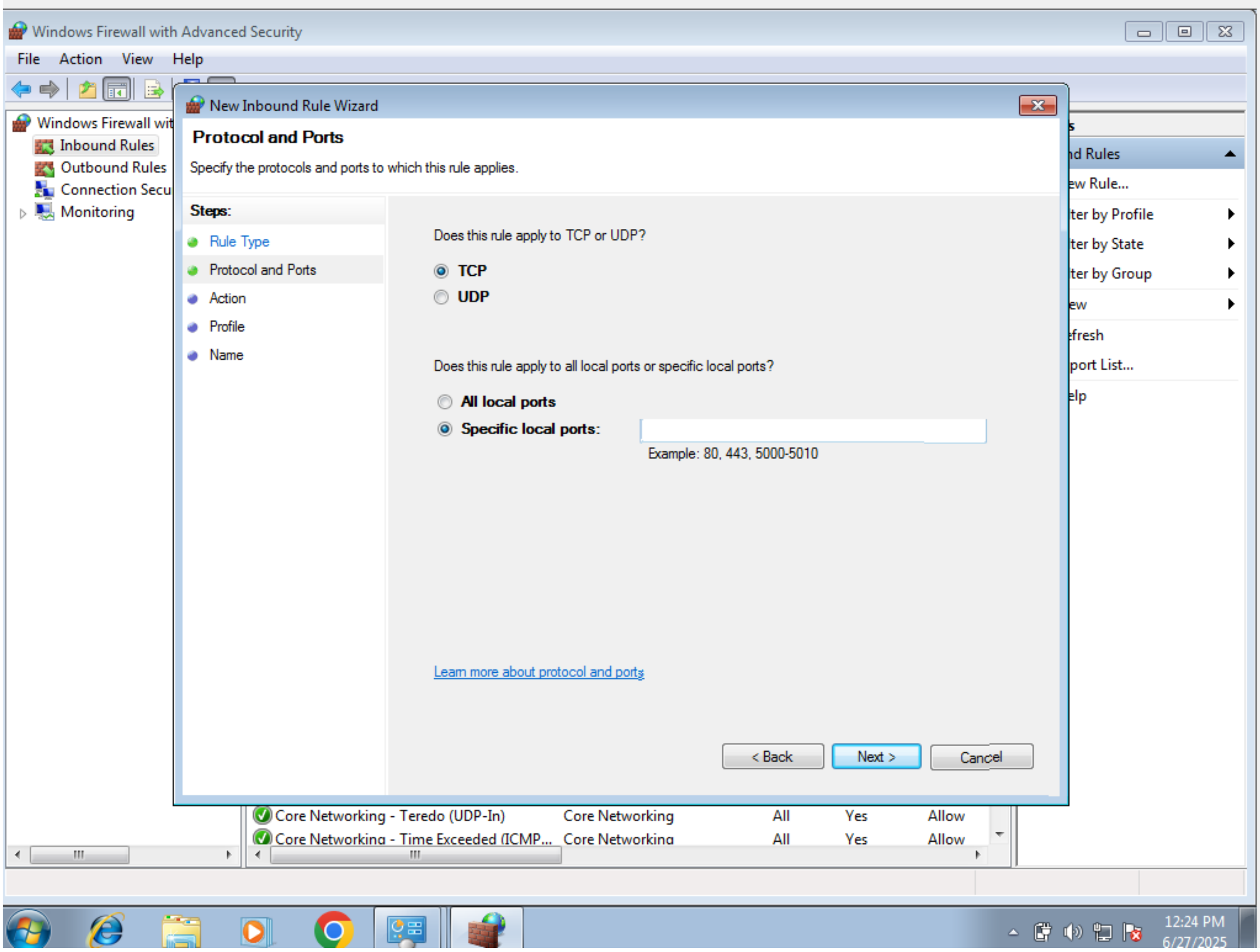
● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP

○ UDP

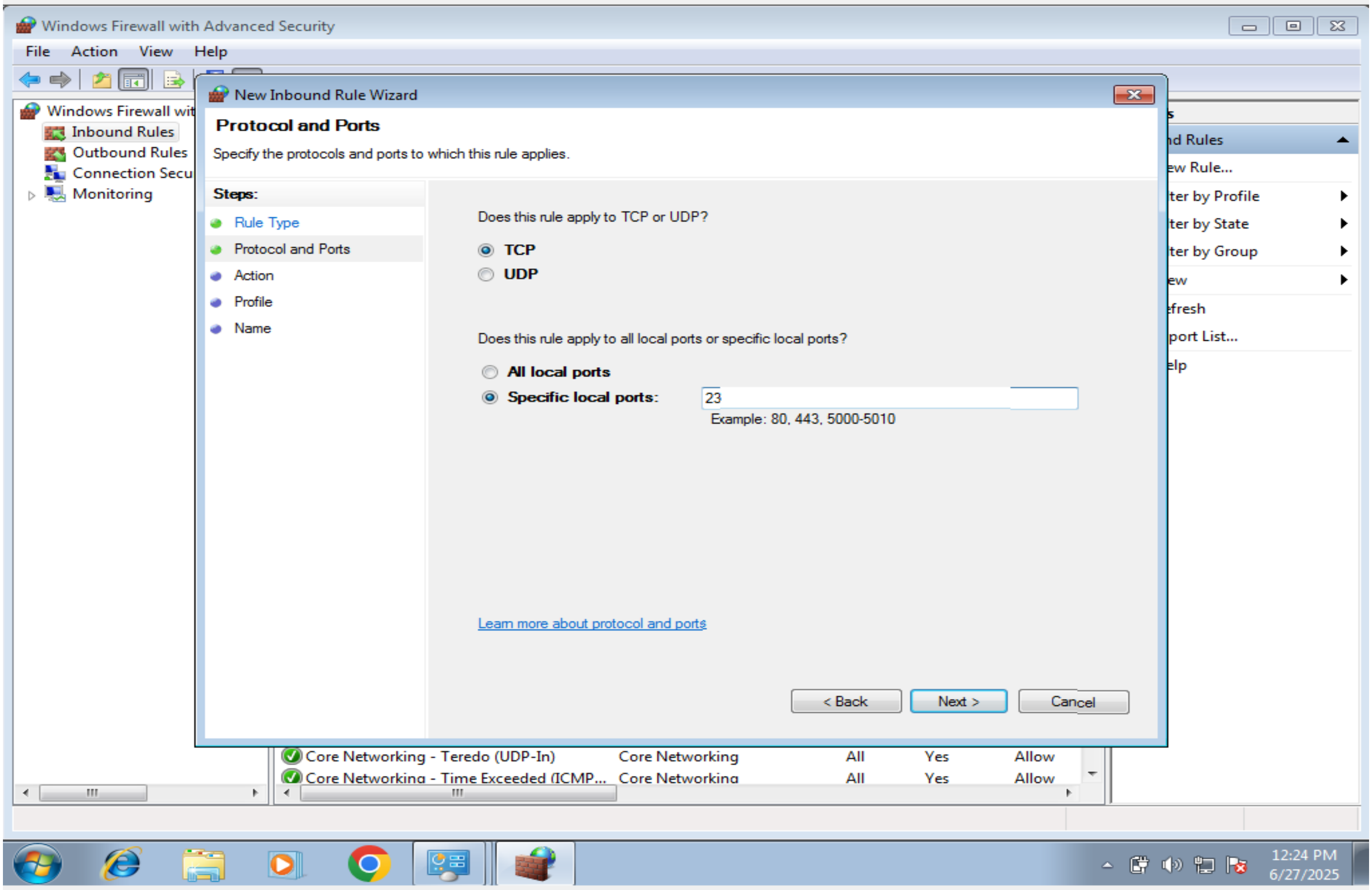
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports:

Example: 80, 443, 5000-5010

Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP

○ UDP

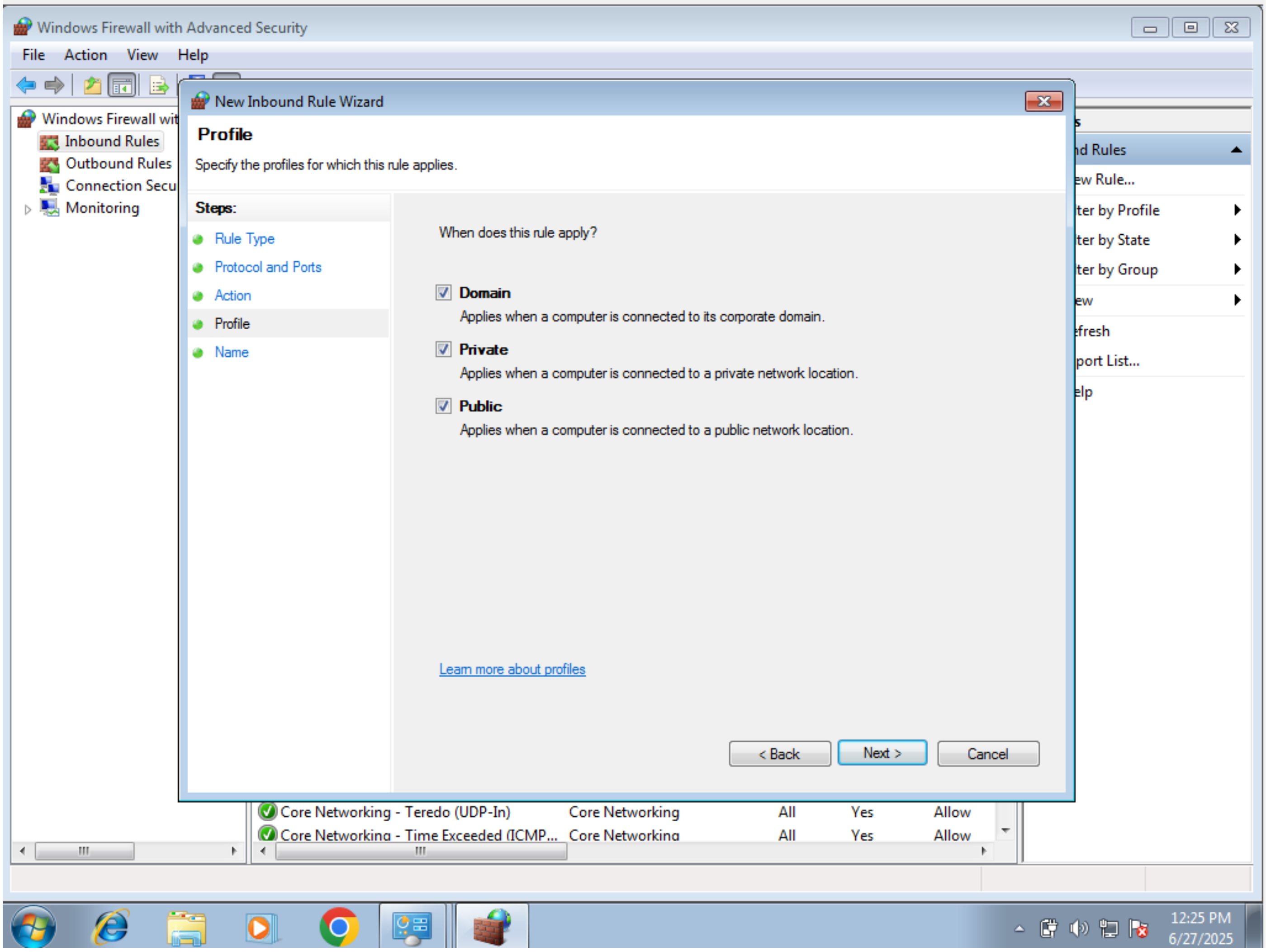
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 23

Example: 80, 443, 5000-5010

Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow



Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

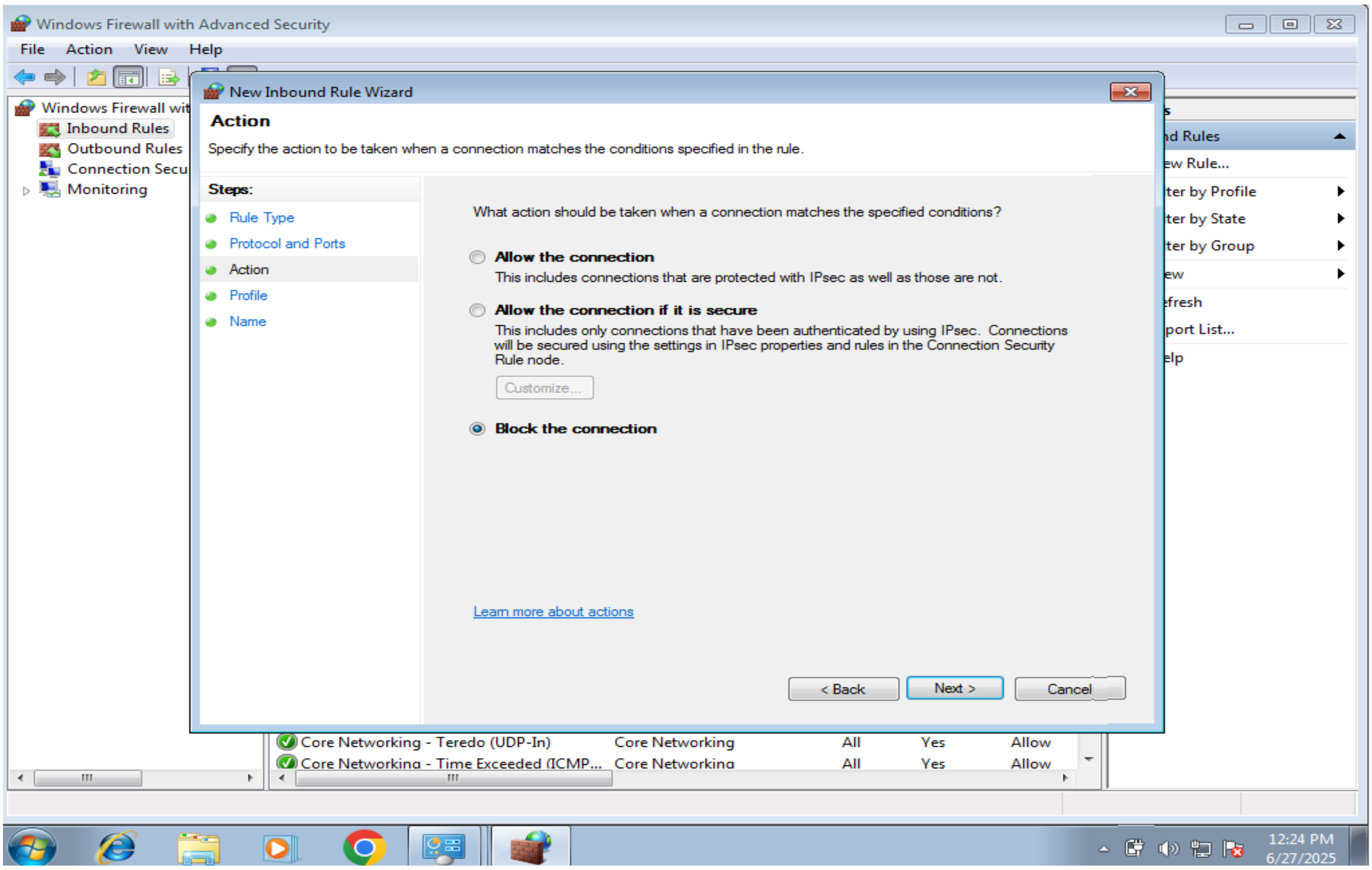
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Learn more about profiles

Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow



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?

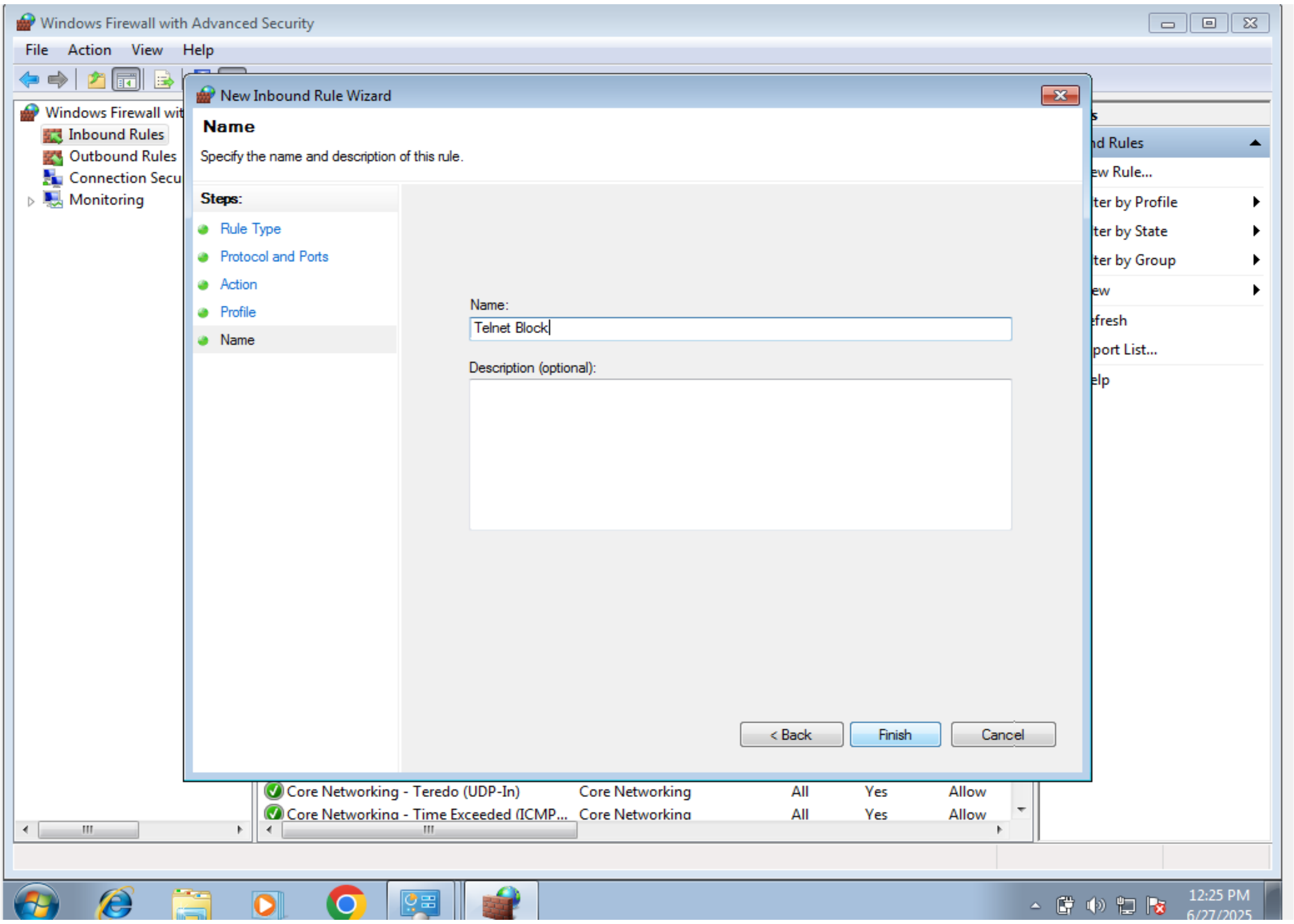
○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **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.

● **Block the connection**

Learn more about actions

Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

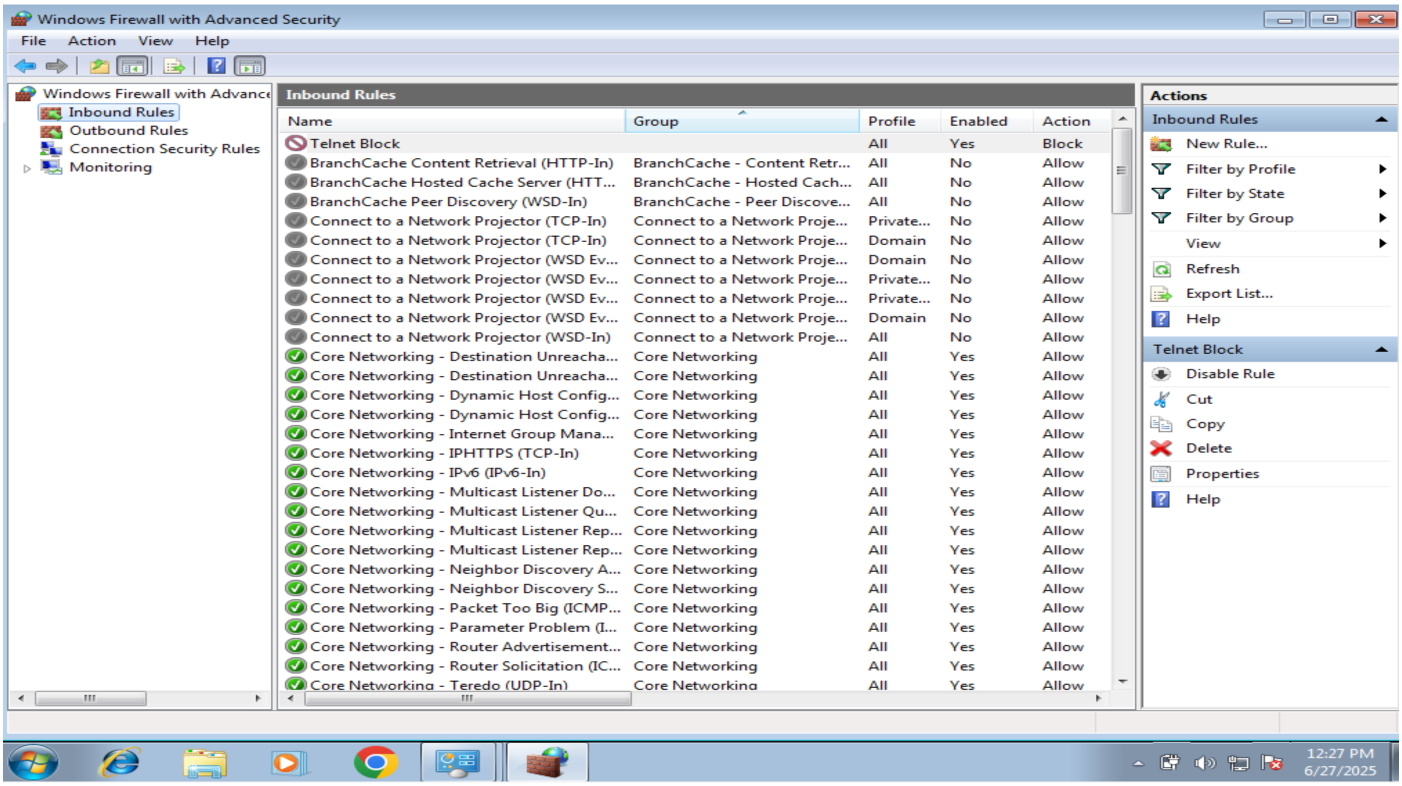
Name: Telnet Block

Description (optional):

Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow

Step 4: Confirm the Rule Is Active

1. You'll now see Block Telnet Inbound listed in Inbound Rules.
2. It should have a green check and block icon indicating it's active.

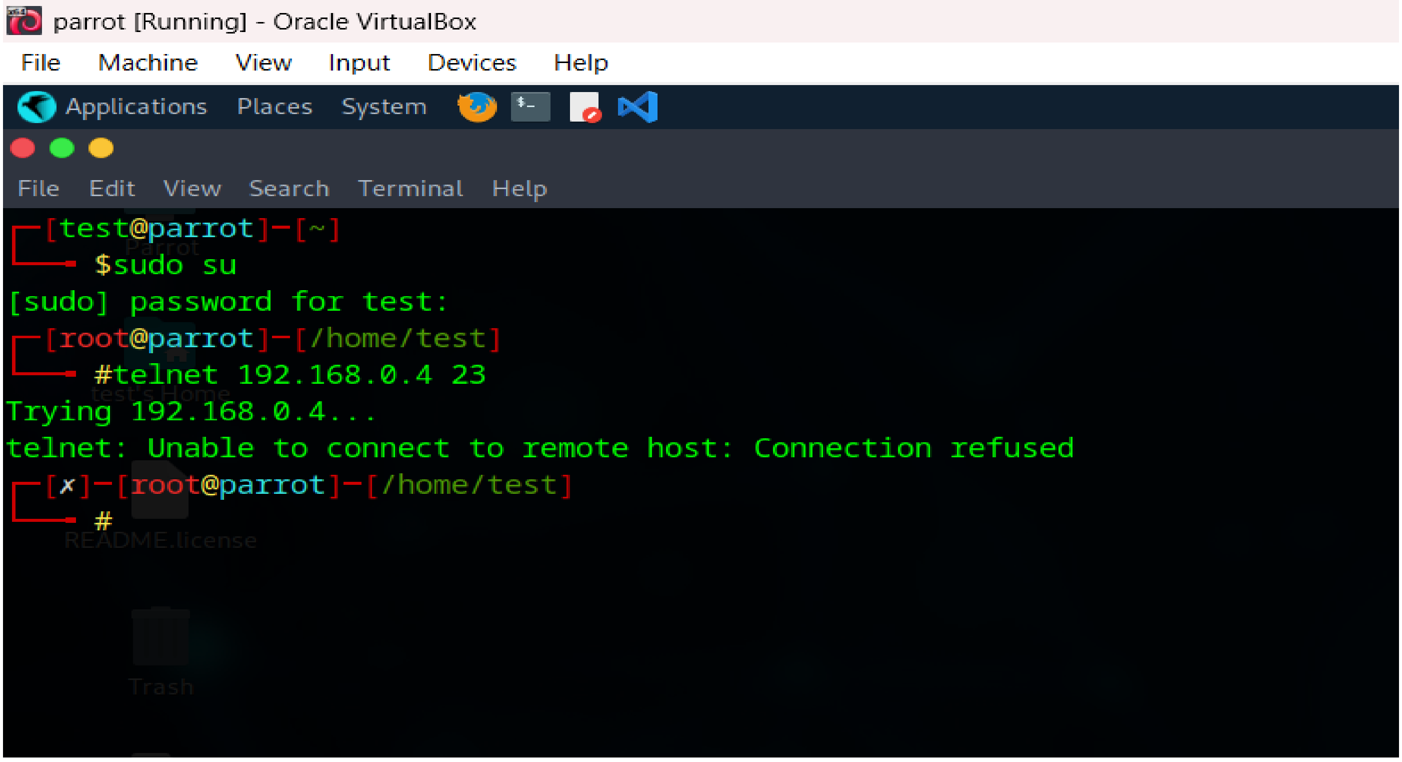


Inbound Rules

Name	Group	Profile	Enabled	Action
Telnet Block		All	Yes	Block
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	All	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow

Step 5: Test the Rule (Optional)

- Try running telnet 192.168.0.4 23 from another device.
- It should fail to connect, confirming the rule is working.



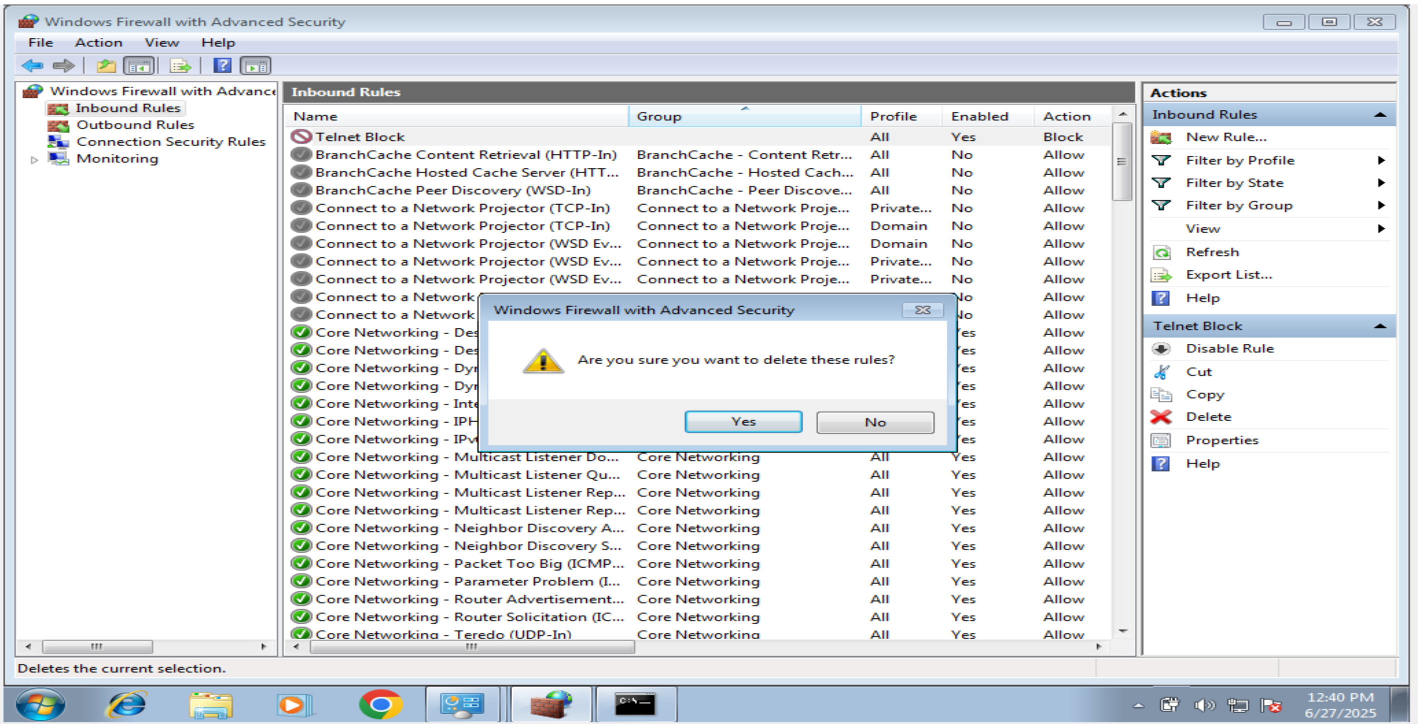
parrot [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
File Edit View Search Terminal Help

```
┌─[test@parrot]─[~]
└──╼ $sudo su
[sudo] password for test:
┌─[root@parrot]─[/home/test]
└──╼ #telnet 192.168.0.4 23
Trying 192.168.0.4...
telnet: Unable to connect to remote host: Connection refused
┌─[✗]─[root@parrot]─[/home/test]
└──╼ #
```

(Optional) Remove the Rule Later

If you want to restore the default state:

1. Right-click on Block Telnet Inbound.
2. Click 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
Telnet Block		All	Yes	Block
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network			No	Allow
Connect to a Network			No	Allow
Core Networking - Des			es	Allow
Core Networking - Des			es	Allow
Core Networking - Dyn			es	Allow
Core Networking - Dyn			es	Allow
Core Networking - Inte			es	Allow
Core Networking - IPH			es	Allow
Core Networking - IPv			es	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow

Windows Firewall with Advanced Security

Are you sure you want to delete these rules?

Deletes the current selection.

5. Allow SSH (Port 22) [Linux]

- SSH must remain accessible, especially if it's a remote server.

```
bash

sudo ufw allow 22
```

6. Remove the Test Block Rule

- **Windows:**
  - Go to *Inbound Rules*, right-click the rule → *Delete*.
- **Linux:**

```
bash

sudo ufw delete deny 23
```

7. Document Commands or GUI Steps Used

Example (Linux):

```
bash

# List current rules

sudo ufw status


# Block Telnet port

sudo ufw deny 23


# Allow SSH

sudo ufw allow 22


# Delete block rule

sudo ufw delete deny 23
```

8. Summary – How Firewall Filters Traffic

- A **firewall** acts like a gatekeeper.
- It uses **rules** to **allow** or **deny** traffic based on:
  - **Ports**
  - **Protocols (TCP/UDP)**
  - **IP addresses**
- Helps block **unauthorized access** and allows only **trusted communication**.

Concept	**Explanation**
Port	Logical endpoints for communication (e.g., 22 for SSH, 23 for Telnet).
Inbound vs Outbound	Inbound: from outside to your system; Outbound: from your system to outside.
Blocking vs Allowing	Blocking stops traffic; allowing permits traffic through the firewall.
UFW (Linux)	A command-line tool to manage firewall rules simply.
Windows Firewall	Built-in GUI tool for firewall rule management in Windows.