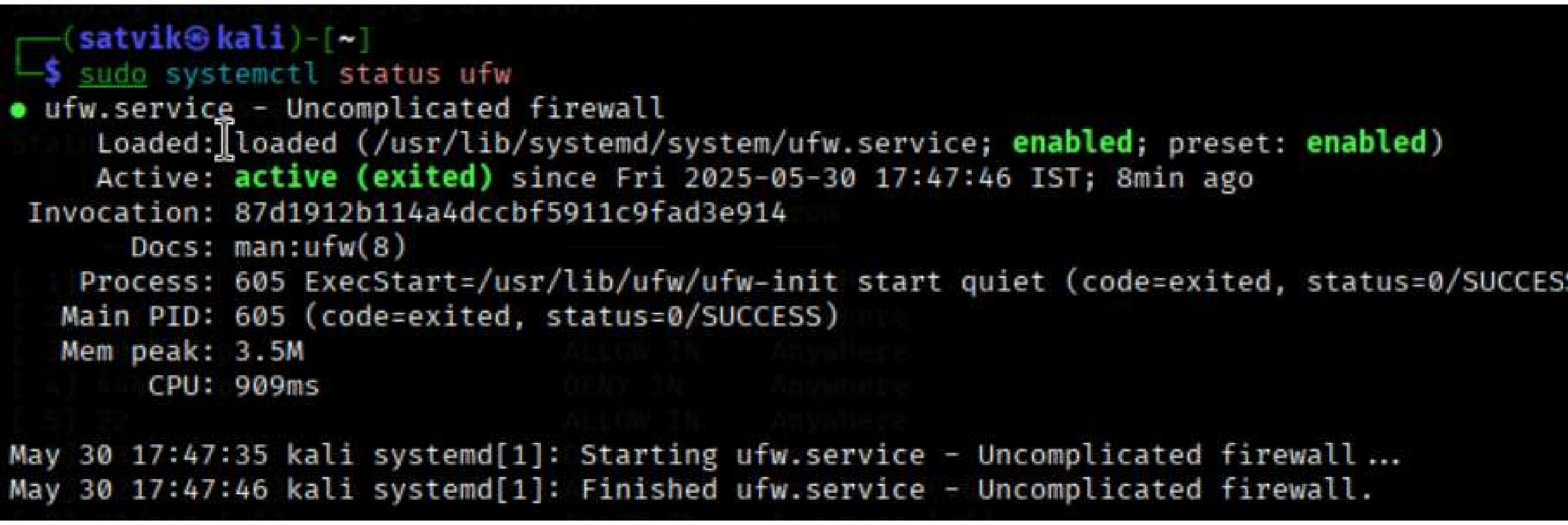
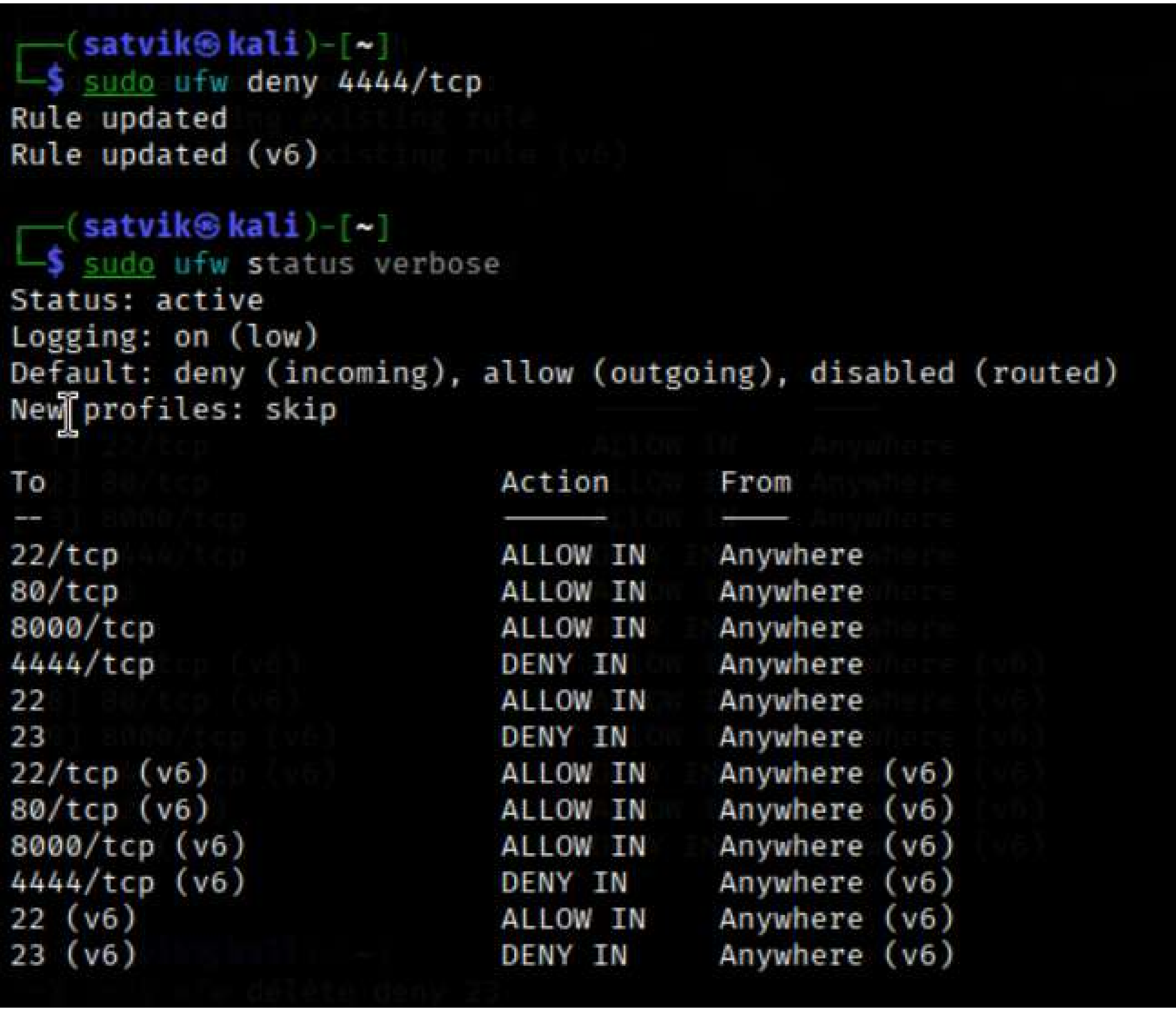
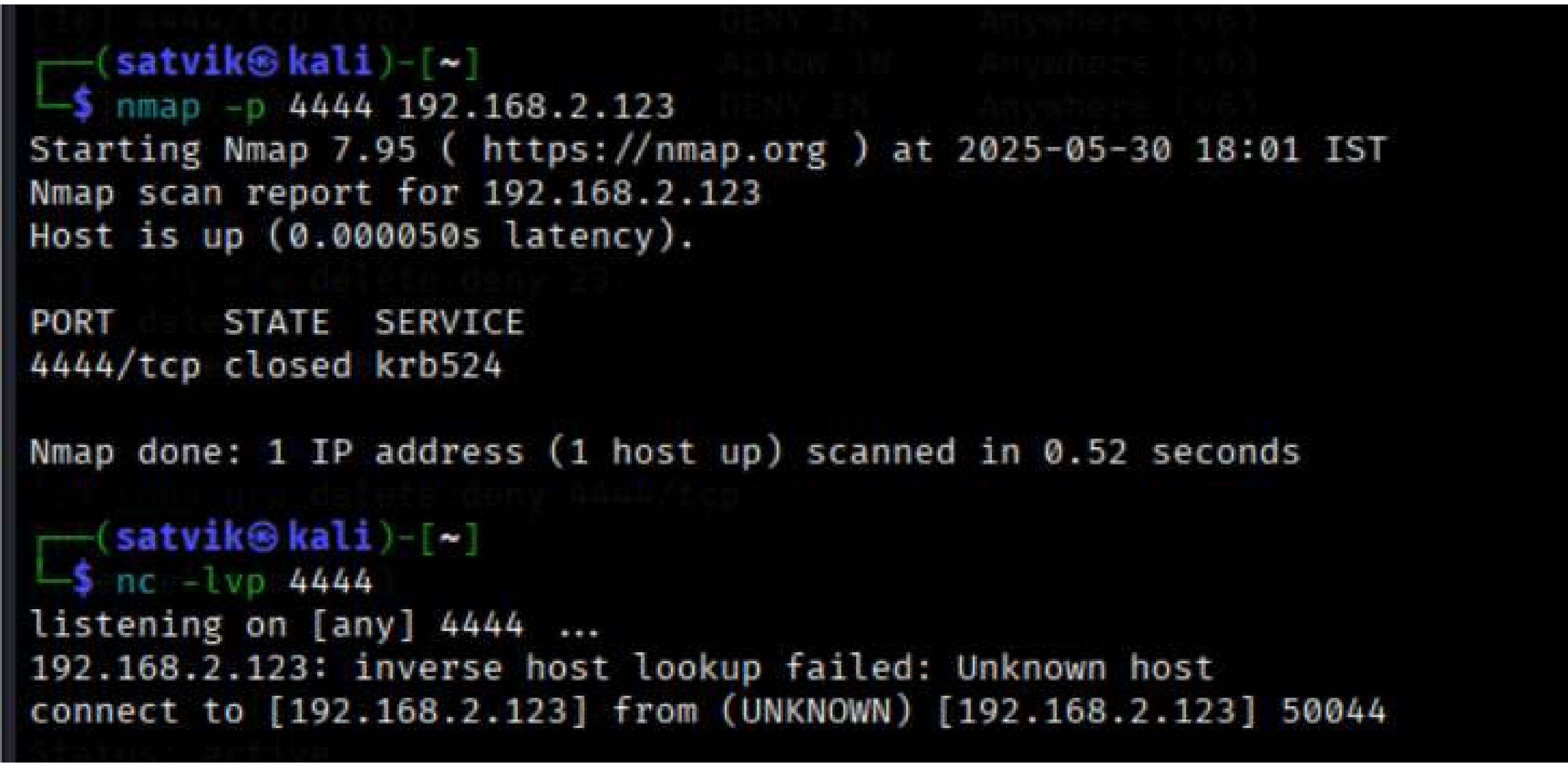


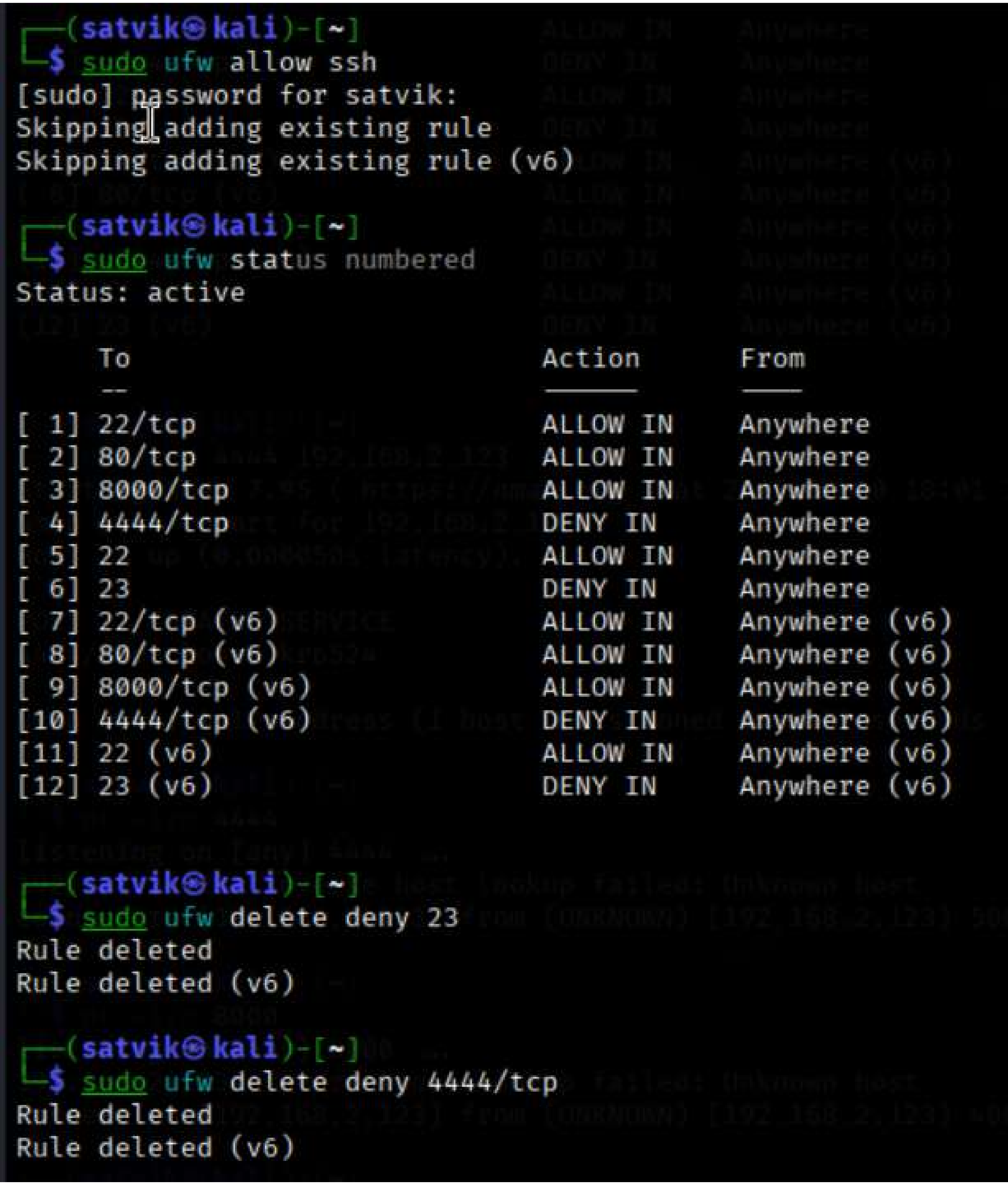
```
┌──(satvik㉿kali)-[~]
└─$ sudo systemctl status ufw
● ufw.service - Uncomplicated firewall
     Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: enabled)
     Active: active (exited) since Fri 2025-05-30 17:47:46 IST; 8min ago
 Invocation: 87d1912b114a4dccbf5911c9fad3e914
       Docs: man:ufw(8)
    Process: 605 ExecStart=/usr/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCES
   Main PID: 605 (code=exited, status=0/SUCCESS)
   Mem peak: 3.5M
        CPU: 909ms

May 30 17:47:35 kali systemd[1]: Starting ufw.service - Uncomplicated firewall...
May 30 17:47:46 kali systemd[1]: Finished ufw.service - Uncomplicated firewall.
```



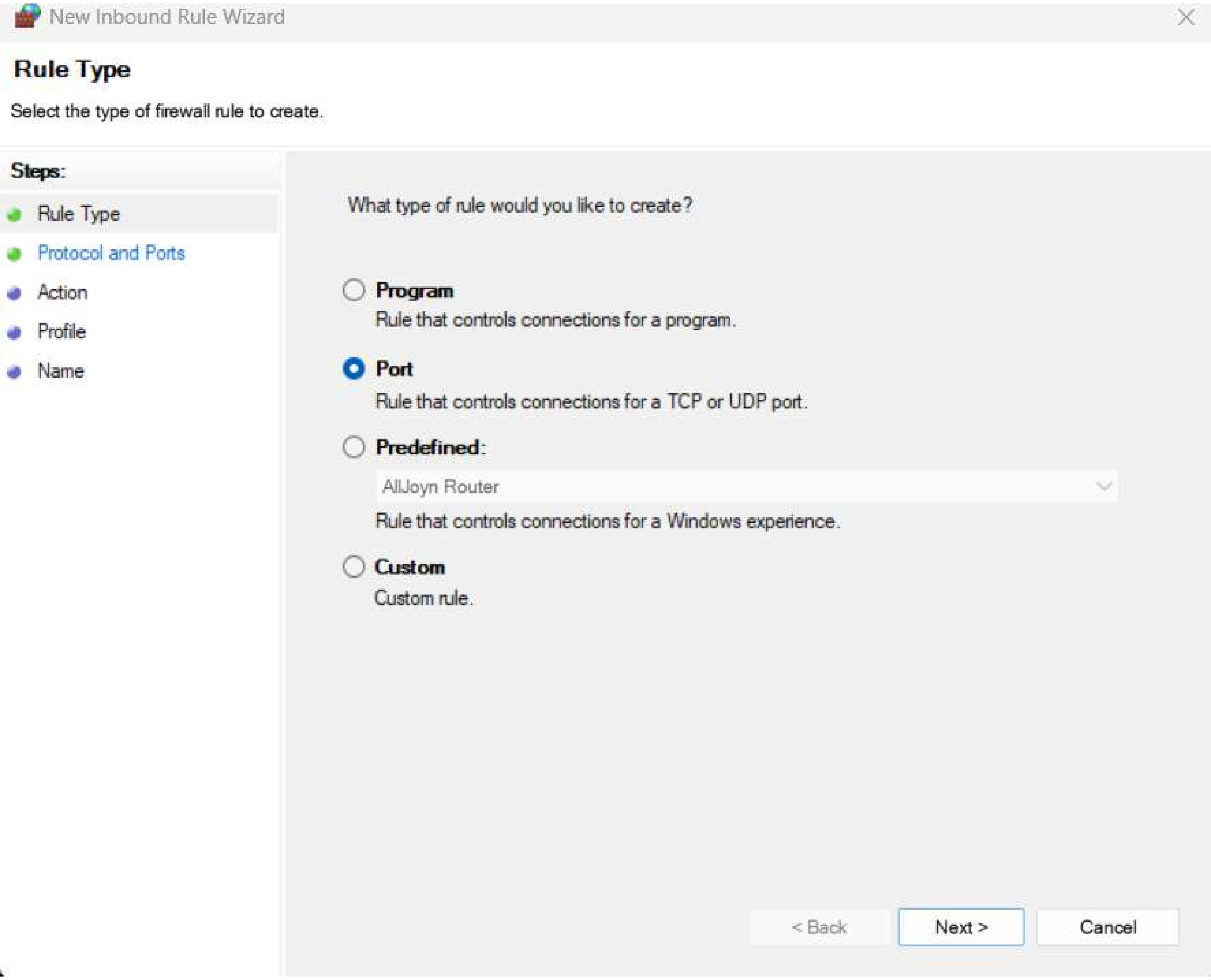
```
┌──(satvik㉿kali)-[~]
└─$ sudo ufw deny 4444/tcp
Rule updated
Rule updated (v6)

┌──(satvik㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
8000/tcp                   ALLOW IN    Anywhere
4444/tcp                   DENY IN     Anywhere
22                         ALLOW IN    Anywhere
23                         DENY IN     Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
8000/tcp (v6)              ALLOW IN    Anywhere (v6)
4444/tcp (v6)              DENY IN     Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
23 (v6)                    DENY IN     Anywhere (v6)
```



```
┌──(satvik㉿kali)-[~]
└─$ nmap -p 4444 192.168.2.123
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 18:01 IST
Nmap scan report for 192.168.2.123
Host is up (0.000050s latency).

PORT      STATE  SERVICE
4444/tcp closed krb524

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

┌──(satvik㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.2.123: inverse host lookup failed: Unknown host
connect to [192.168.2.123] from (UNKNOWN) [192.168.2.123] 50044
```



```
┌──(satvik㉿kali)-[~]
└─$ sudo ufw allow ssh
[sudo] password for satvik:
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(satvik㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 8000/tcp                   ALLOW IN    Anywhere
[ 4] 4444/tcp                   DENY IN     Anywhere
[ 5] 22                         ALLOW IN    Anywhere
[ 6] 23                         DENY IN     Anywhere
[ 7] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 8] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 9] 8000/tcp (v6)              ALLOW IN    Anywhere (v6)
[10] 4444/tcp (v6)              DENY IN     Anywhere (v6)
[11] 22 (v6)                    ALLOW IN    Anywhere (v6)
[12] 23 (v6)                    DENY IN     Anywhere (v6)


┌──(satvik㉿kali)-[~]
└─$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)

┌──(satvik㉿kali)-[~]
└─$ sudo ufw delete deny 4444/tcp
Rule deleted
Rule deleted (v6)
```



Rule Type

Select the type of firewall rule to create.

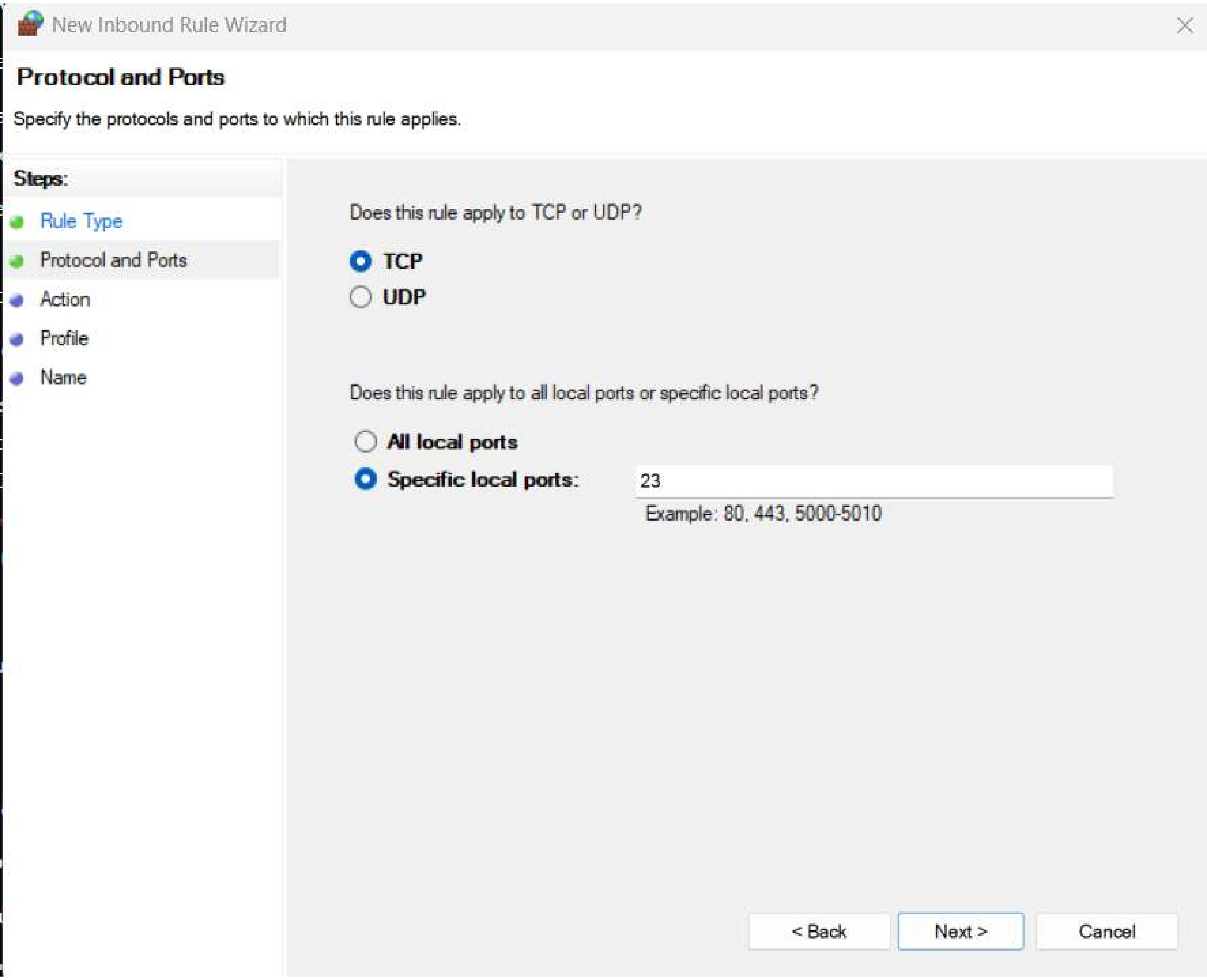
What type of rule would you like to create?

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

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

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● **TCP**

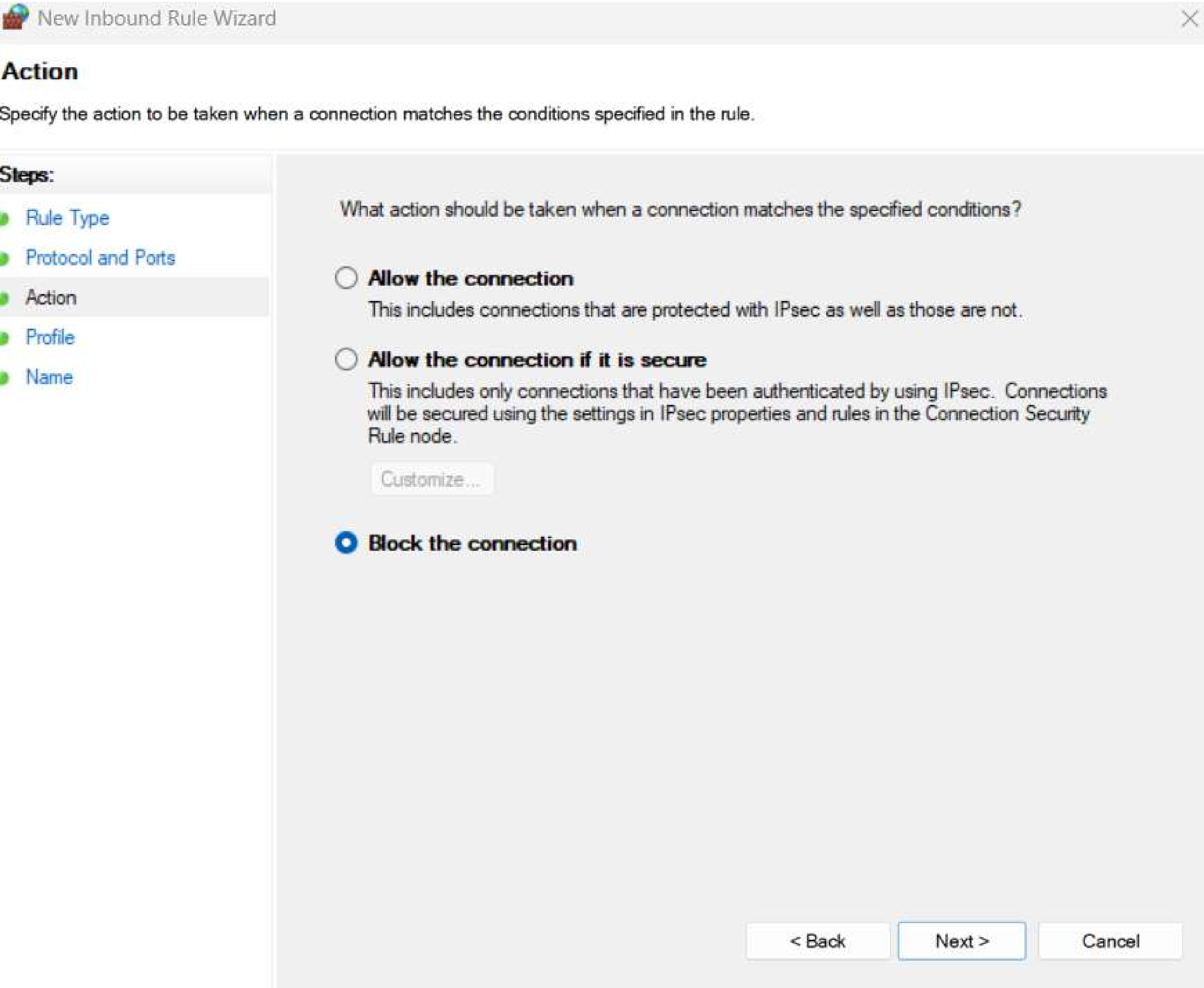
○ **UDP**

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

○ **All local ports**

● **Specific local ports:** 23

Example: 80, 443, 5000-5010



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?

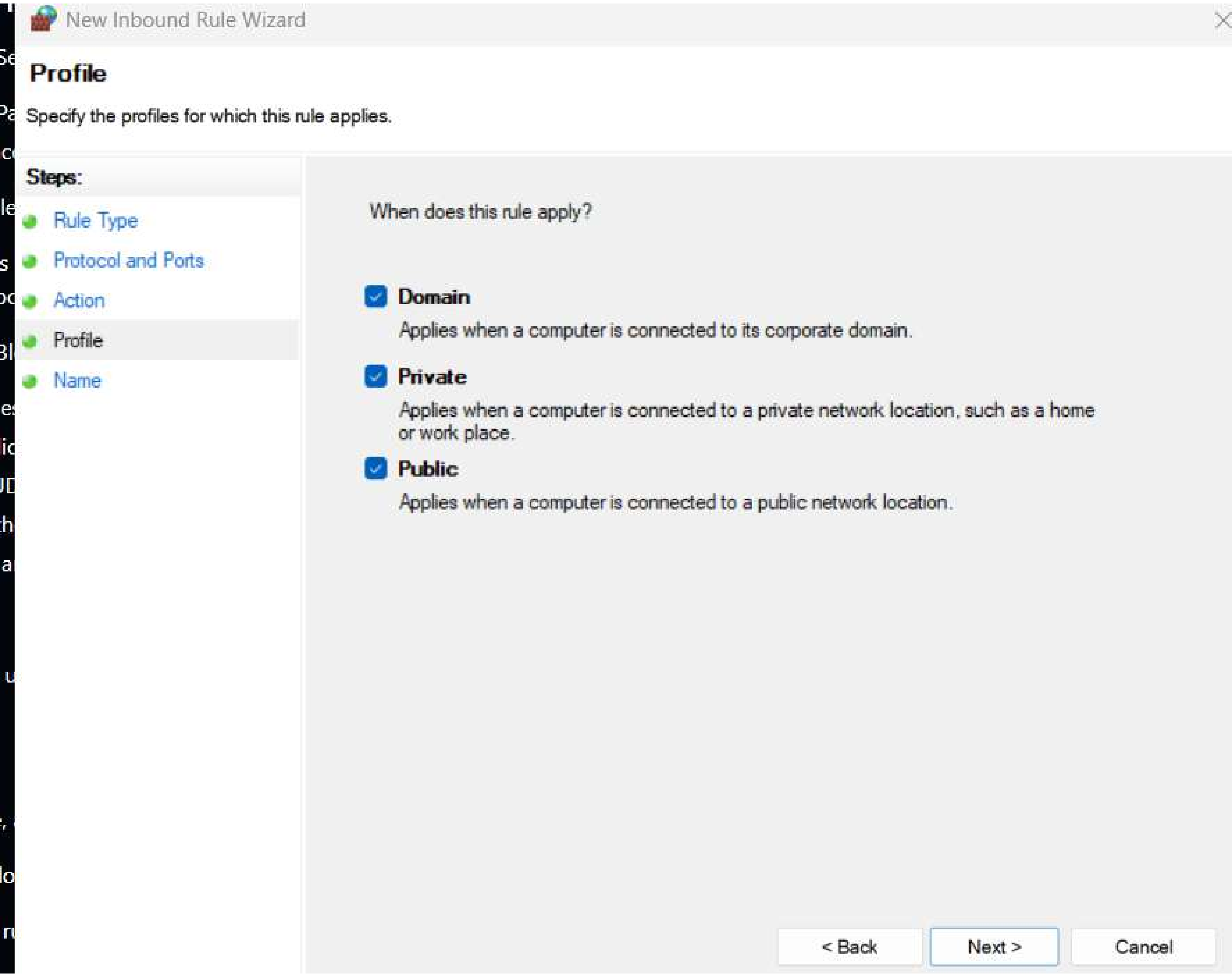
○ **Allow the connection**

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.

● **Block the connection**



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

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

When does this rule apply?

☑ **Domain**

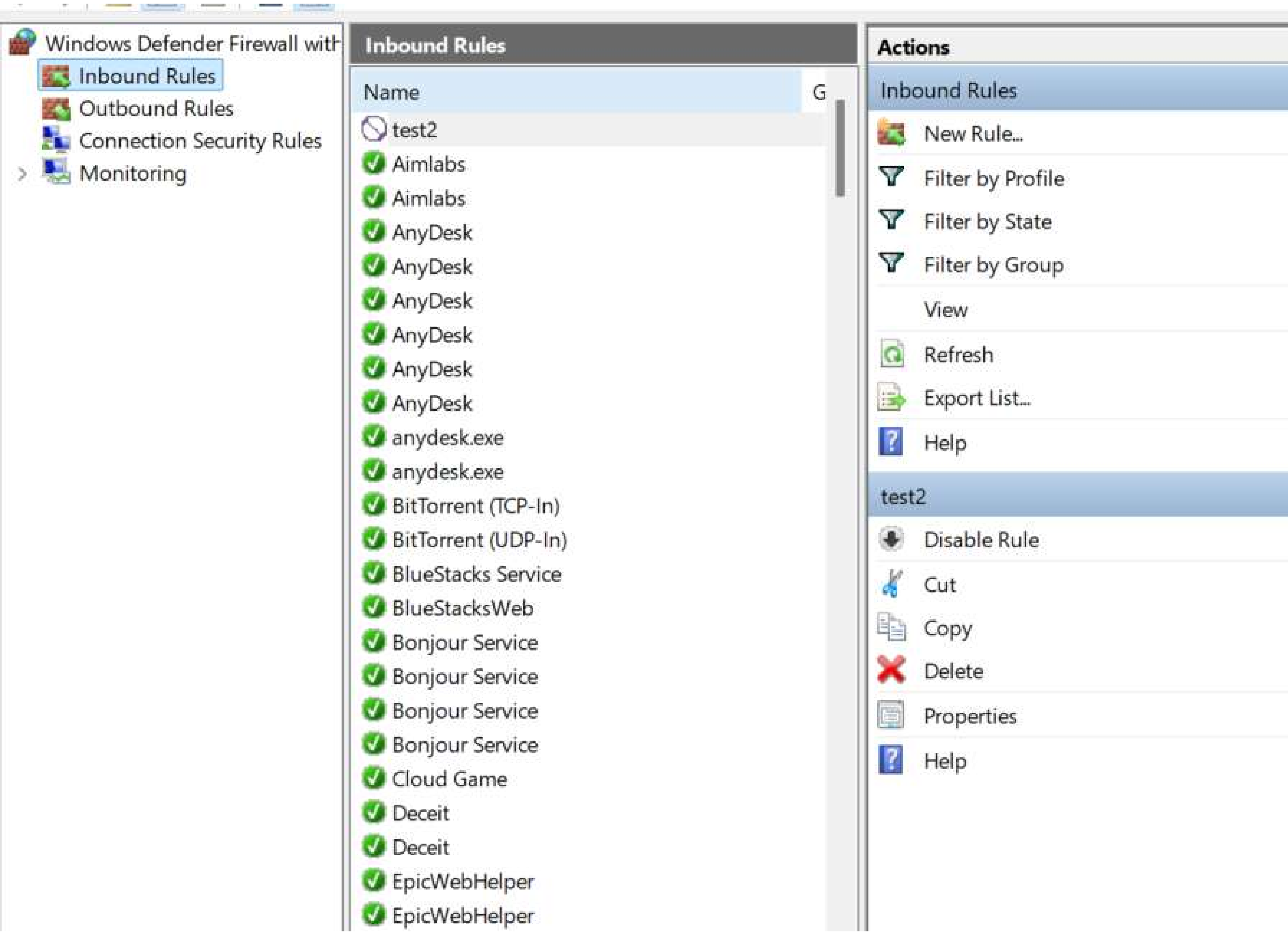
Applies when a computer is connected to its corporate domain.

☑ **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.



Inbound Rules

Name	G
test2	
✓ Aimlabs	
✓ Aimlabs	
✓ AnyDesk	
✓ AnyDesk	
✓ AnyDesk	
✓ AnyDesk	
✓ AnyDesk	
✓ AnyDesk	
✓ anydesk.exe	
✓ anydesk.exe	
✓ BitTorrent (TCP-In)	
✓ BitTorrent (UDP-In)	
✓ BlueStacks Service	
✓ BlueStacksWeb	
✓ Bonjour Service	
✓ Bonjour Service	
✓ Bonjour Service	
✓ Bonjour Service	
✓ Cloud Game	
✓ Deceit	
✓ Deceit	
✓ EpicWebHelper	
✓ EpicWebHelper	