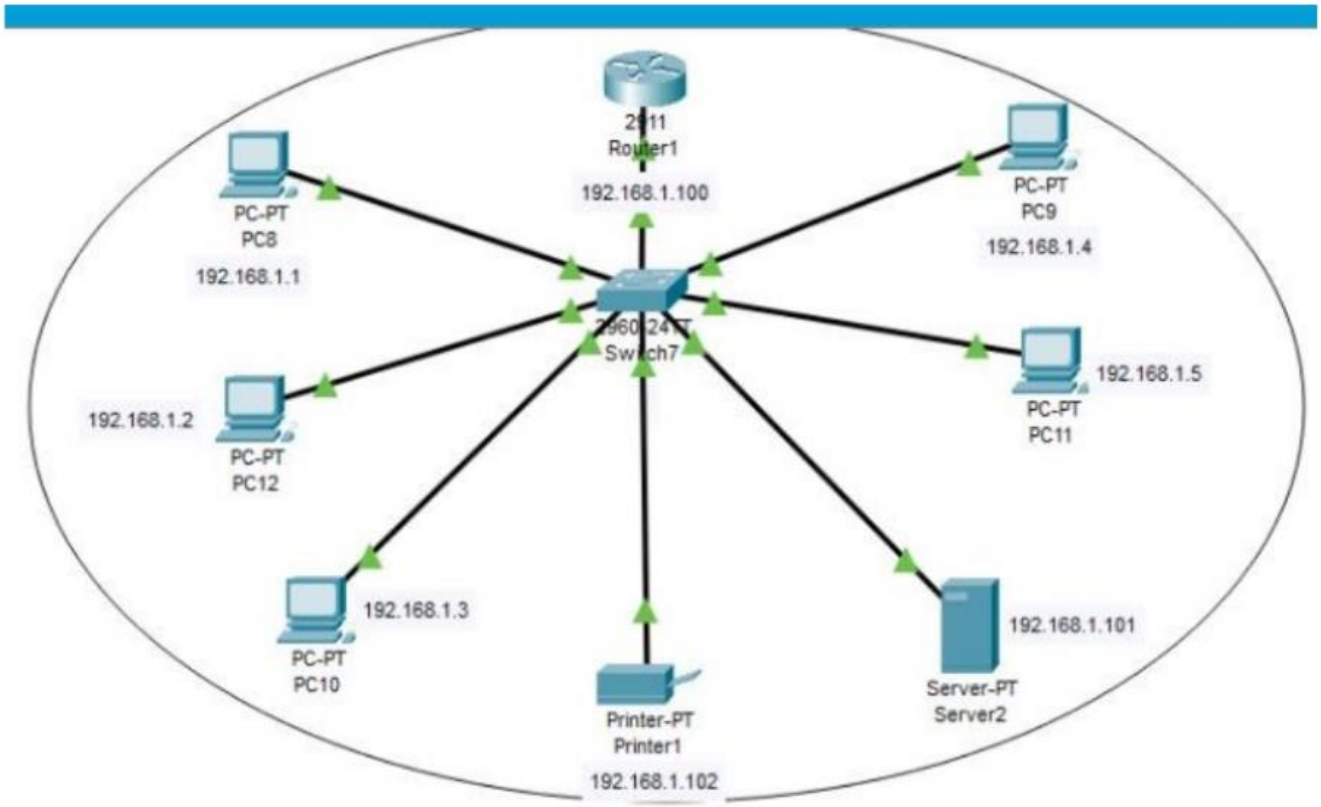
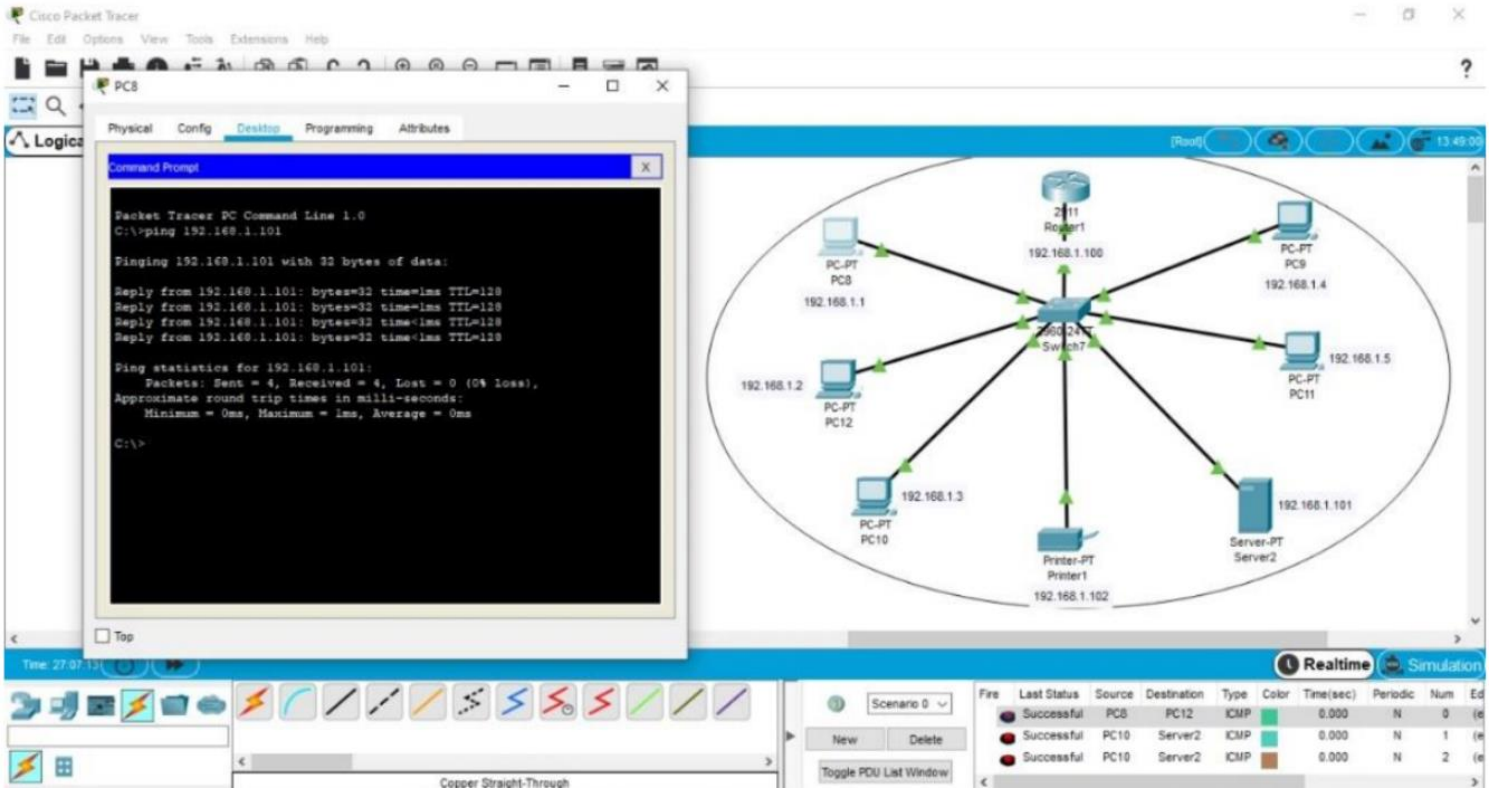
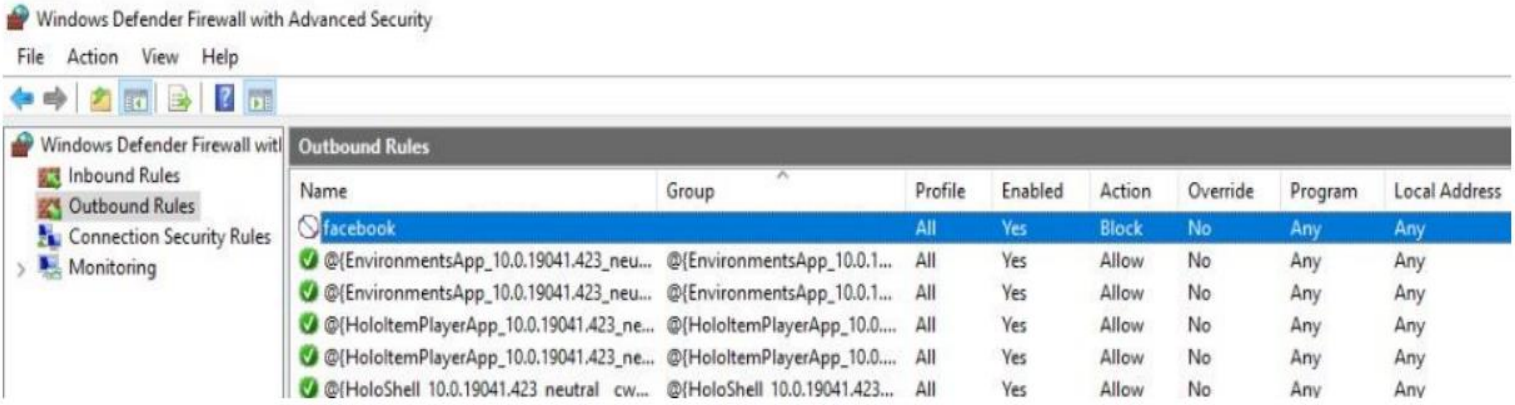
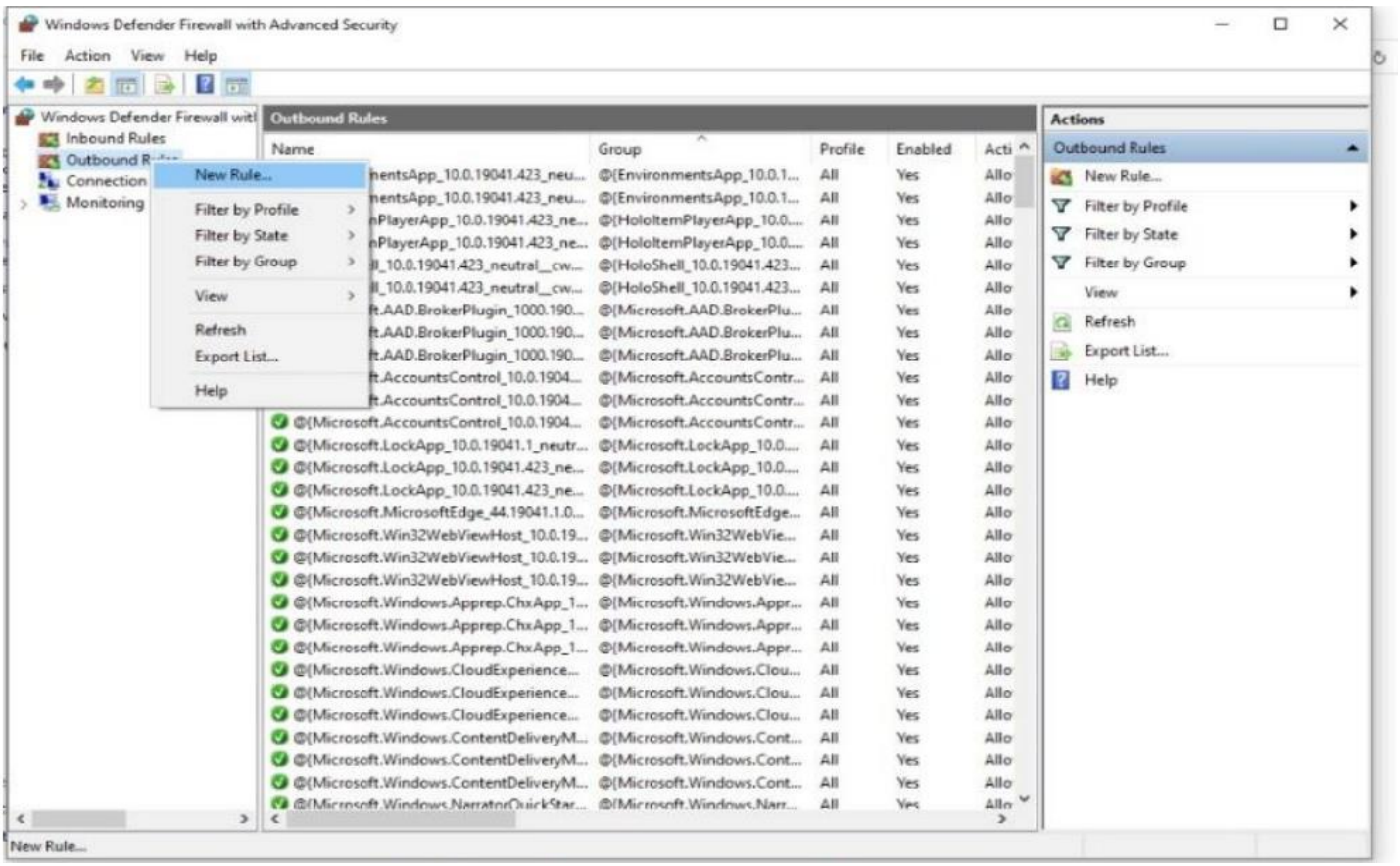
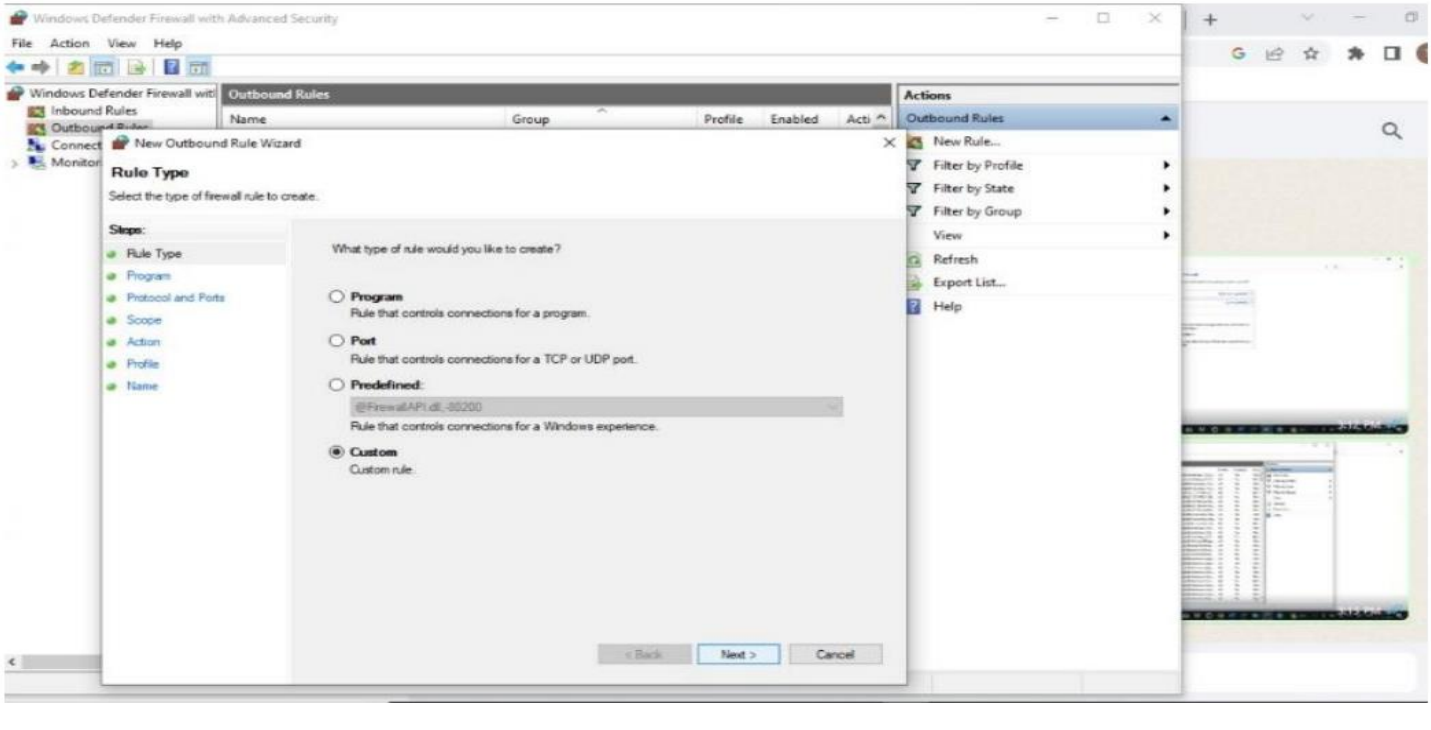

2811
Router1
192.168.1.100
PC-PT
PC8
192.168.1.1
PC-PT
PC9
192.168.1.4
2960-24TT
Switch7
192.168.1.5
PC-PT
PC11
192.168.1.2
PC-PT
PC12
192.168.1.3
PC-PT
PC10
192.168.1.101
Server-PT
Server2
Printer-PT
Printer1
192.168.1.102

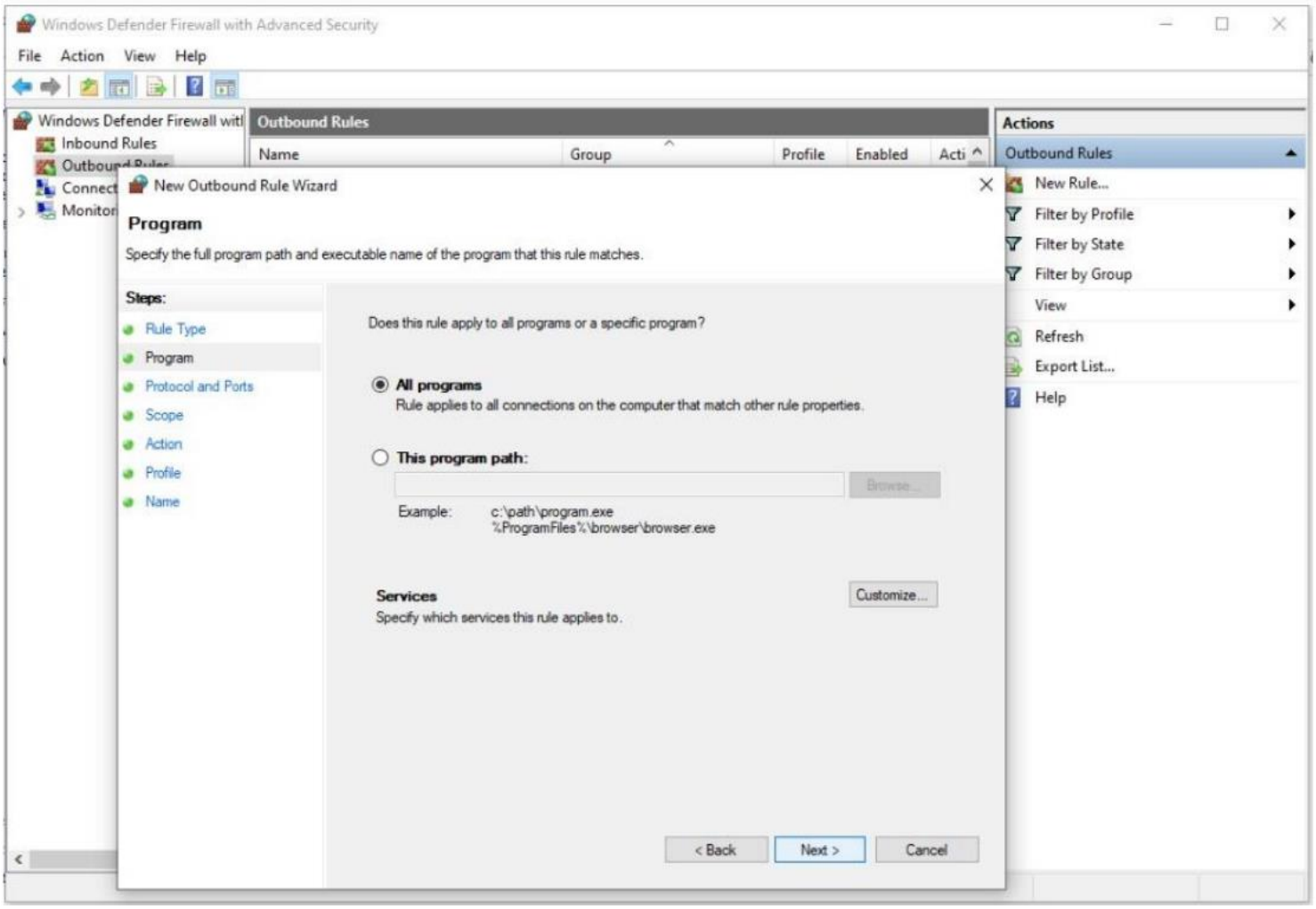

Cisco Packet Tracer
PC8
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.101
Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Copper Straight-Through

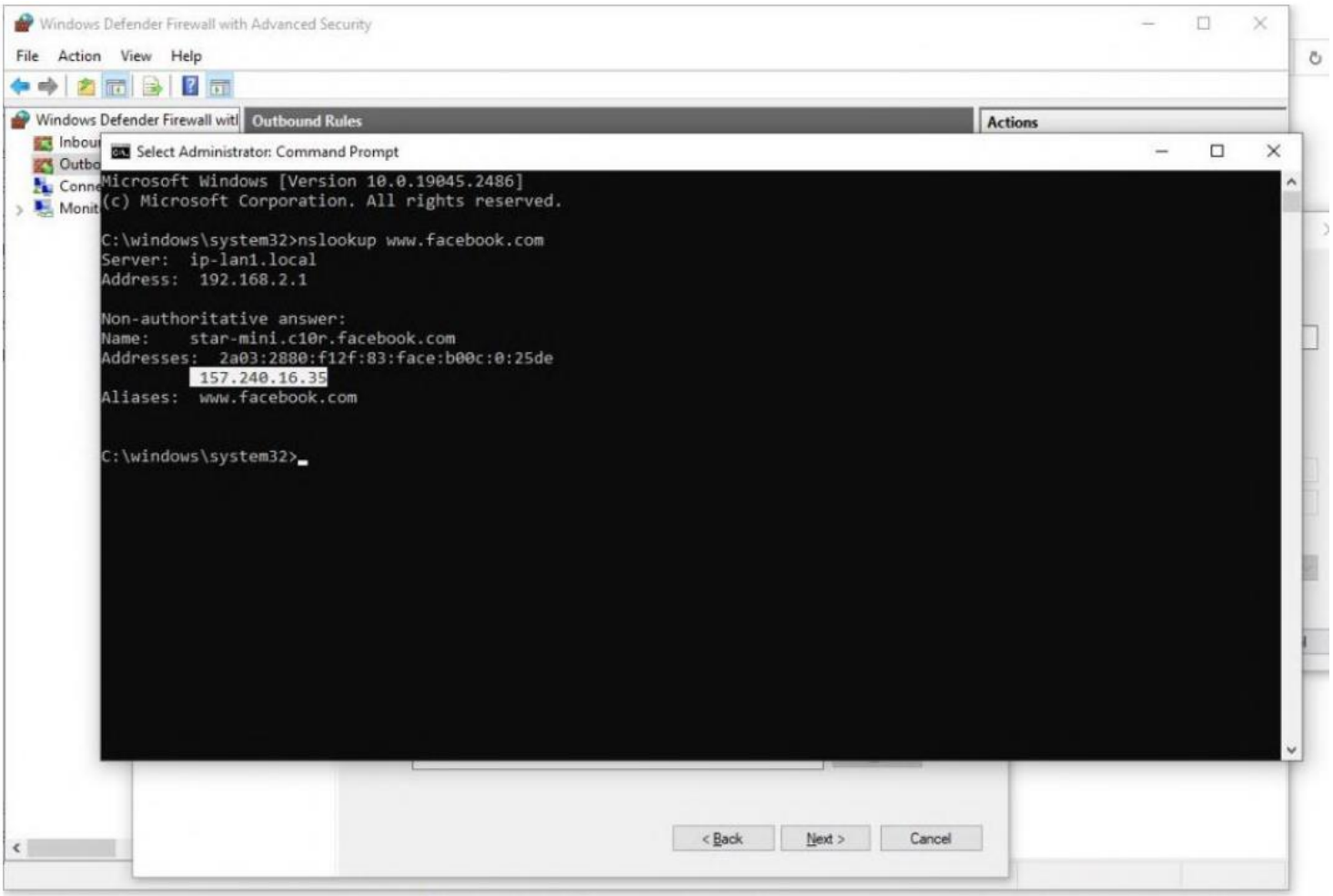

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Action
Override
Program
Local Address
facebook
All
Yes
Block
No
Any
Any
@{EnvironmentsApp_10.0.19041.423_neu...
@{EnvironmentsApp_10.0.1...
All
Yes
Allow
No
Any
Any
@{EnvironmentsApp_10.0.19041.423_neu...
@{EnvironmentsApp_10.0.1...
All
Yes
Allow
No
Any
Any
@{HoloItemPlayerApp_10.0.19041.423_ne...
@{HoloItemPlayerApp_10.0....
All
Yes
Allow
No
Any
Any
@{HoloItemPlayerApp_10.0.19041.423_ne...
@{HoloItemPlayerApp_10.0....
All
Yes
Allow
No
Any
Any
@{HoloShell 10.0.19041.423 neutral cw...
@{HoloShell 10.0.19041.423...
All
Yes
Allow
No
Any
Any

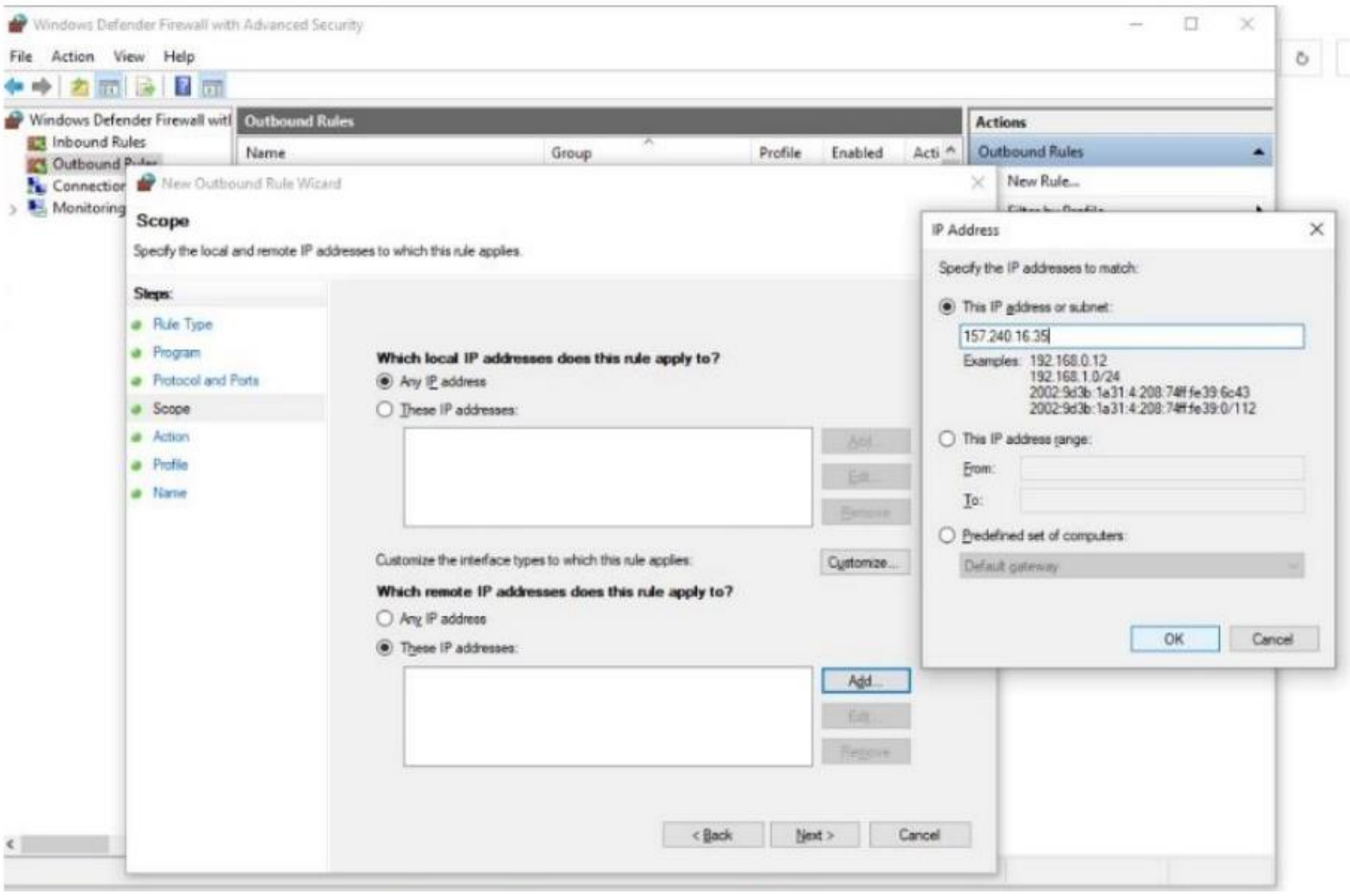
Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Defender Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
KLEBCA1
Notification state:
Notify me when Windows Defender Firewall blocks a new app

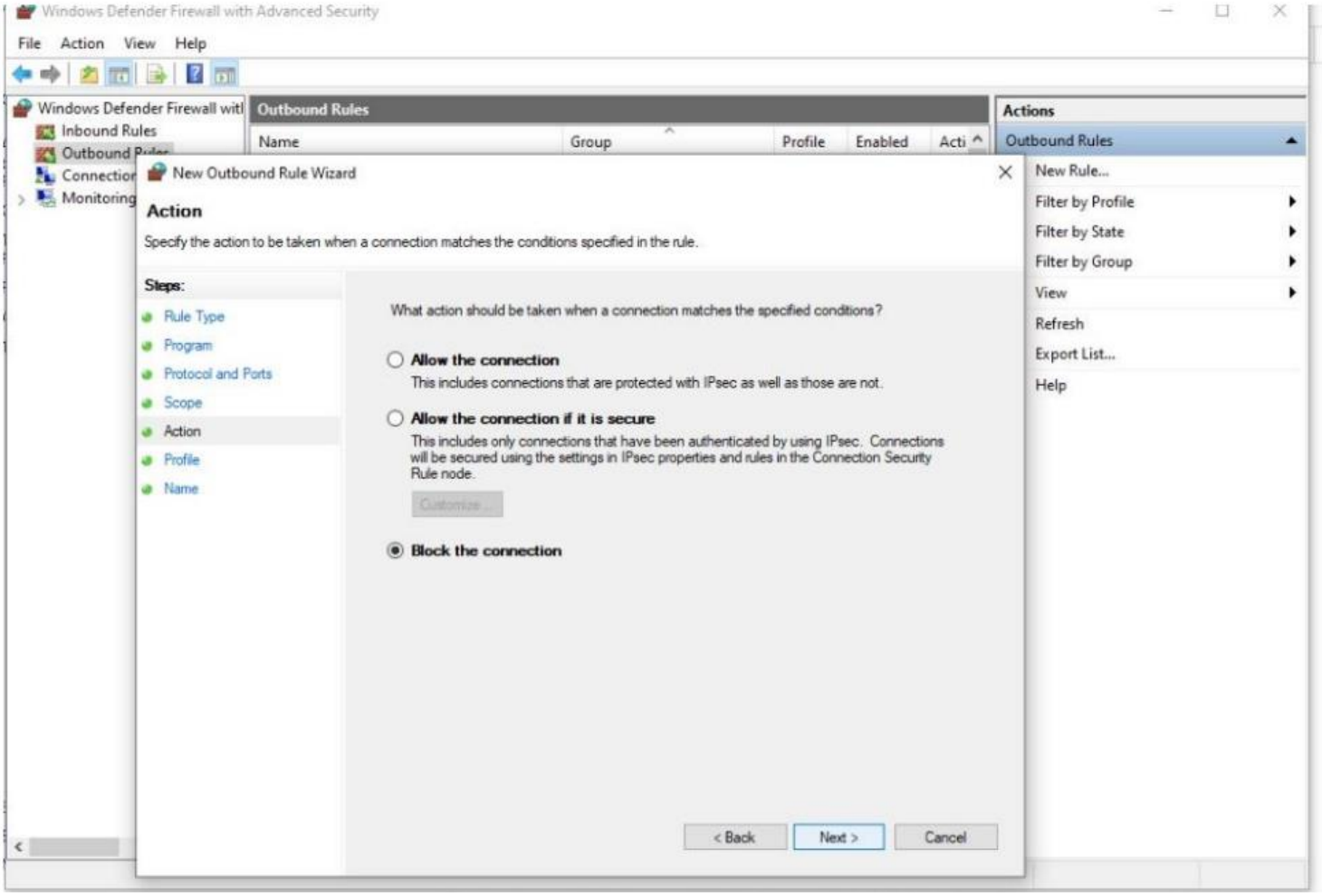

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Actions
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Rule...

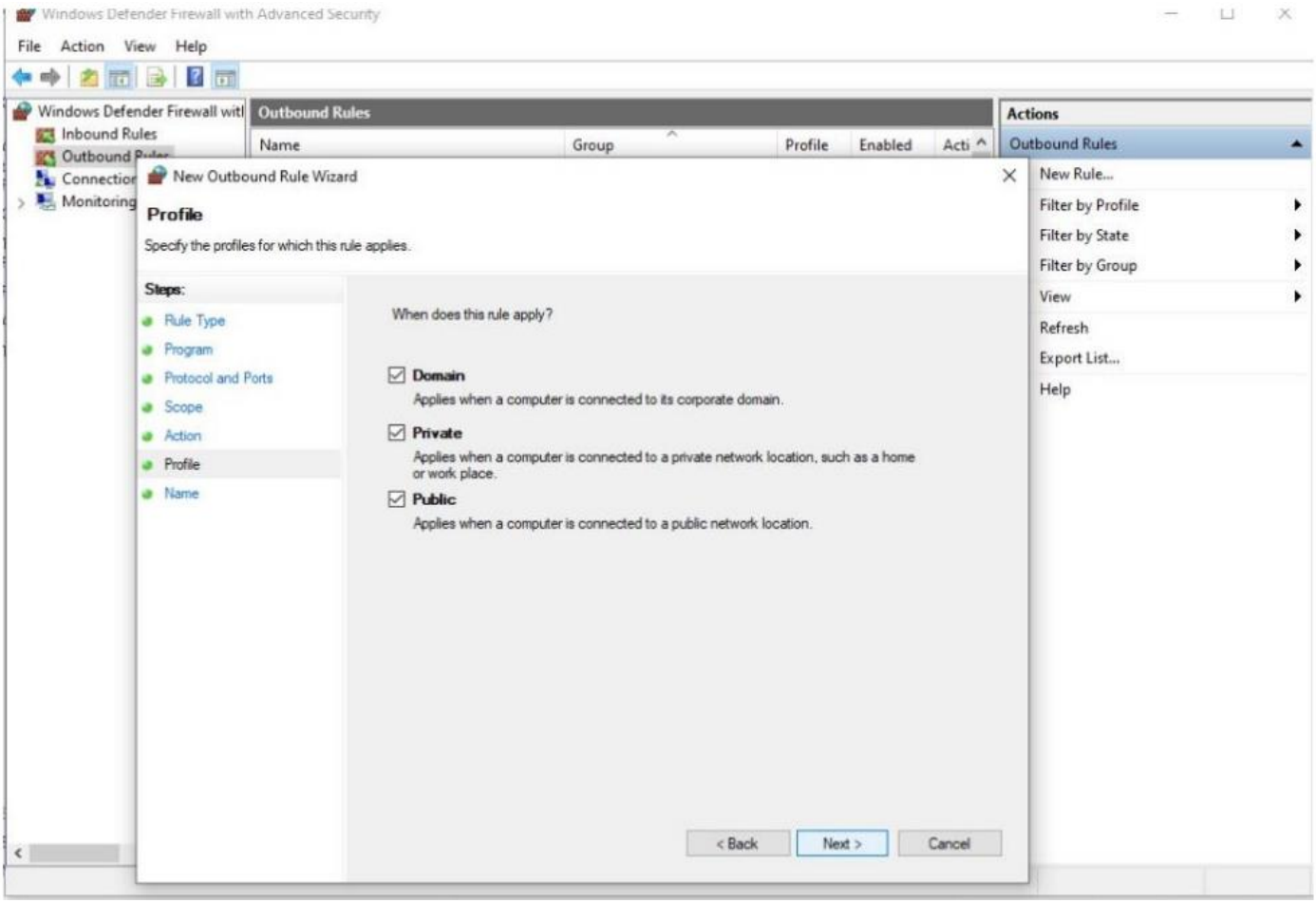

New Outbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

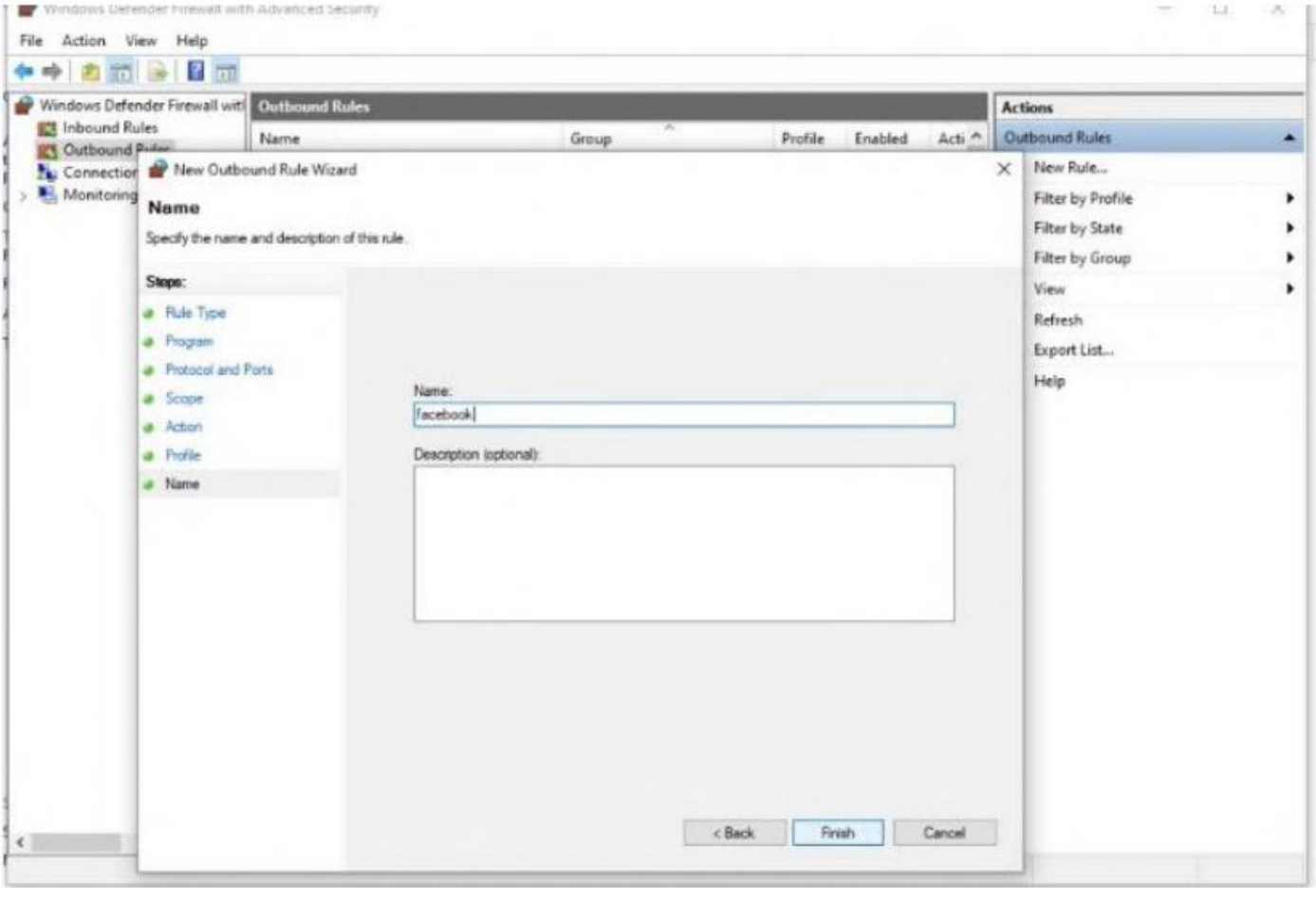

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connect
Monitor
Outbound Rules
Name
Group
Profile
Enabled
Acti
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Outbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
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:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
Cancel

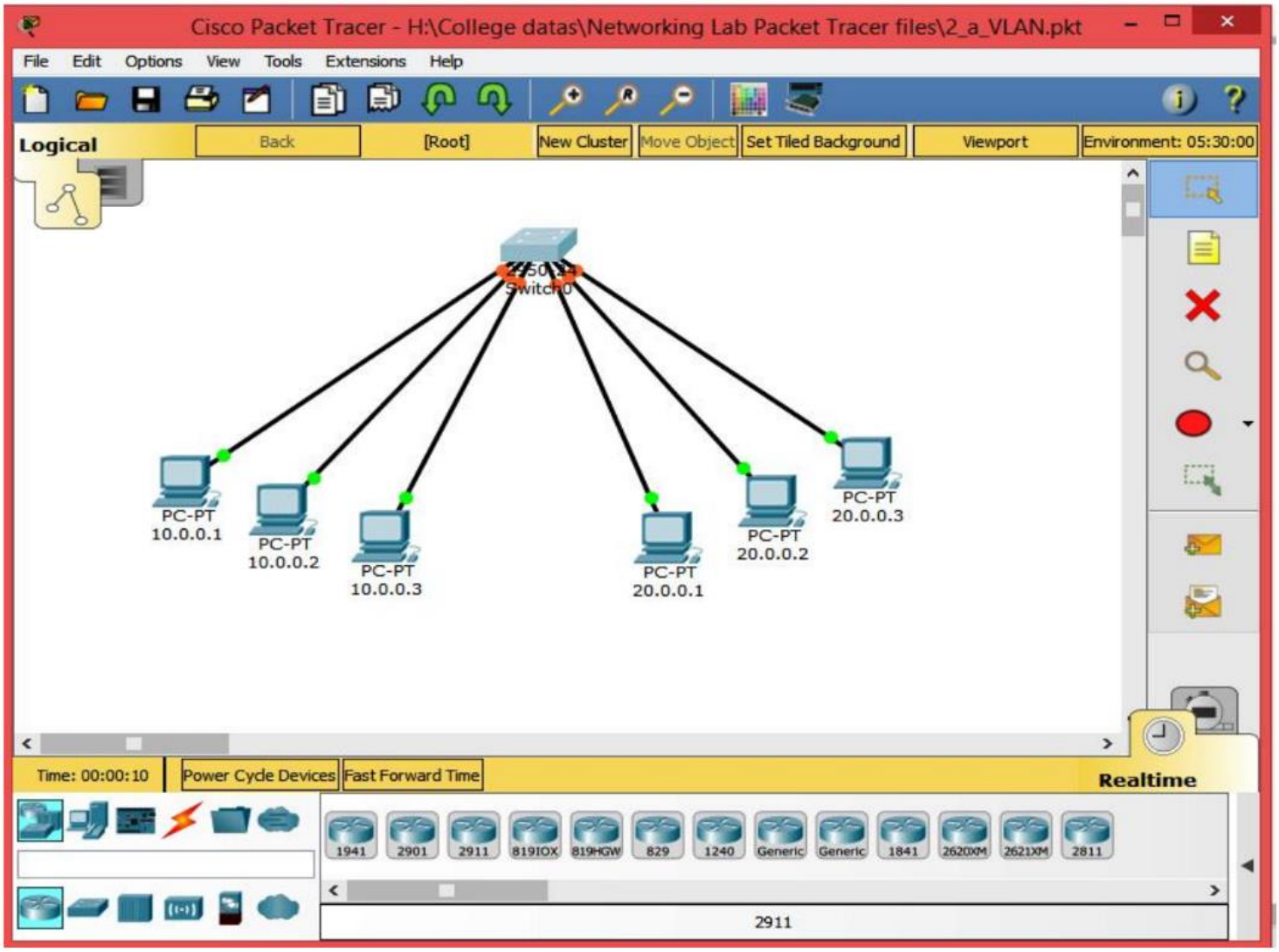

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Outbound Rules
Actions
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.
C:\windows\system32>nslookup www.facebook.com
Server: ip-lan1.local
Address: 192.168.2.1
Non-authoritative answer:
Name: star-mini.c10r.facebook.com
Addresses: 2a03:2880:f12f:83:face:b00c:0:25de
157.240.16.35
Aliases: www.facebook.com
C:\windows\system32>
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connectior
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Acti
Actions
Outbound Rules
New Rule...
New Outbound Rule Wizard
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:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
< Back
Next >
Cancel
IP Address
Specify the IP addresses to match:
This IP address or subnet:
157.240.16.35
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112
This IP address range:
From:
To:
Predefined set of computers:
Default gateway
OK
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connectior
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Acti
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Outbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
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.
Customize...
Block the connection
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connectior
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Acti
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Outbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
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.
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connectior
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Acti
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Outbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
facebook
Description (optional):
< Back
Finish
Cancel

MAC- ADDRESS TABLE:

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------      -------------------------------------------

Vlan    Mac Address       Type        Ports      Vlan    Mac Address       Type        Ports
----    -----------       --------    -----      ----    -----------       --------    -----

  10    0009.7c61.c0d0    DYNAMIC     Fa0/1        20    0060.3e8d.3936    DYNAMIC     Fa0/5
  10    000d.bdc2.3317    DYNAMIC     Fa0/2        20    00d0.bcb6.54aa    DYNAMIC     Fa0/6
  10    0090.0ce6.60c9    DYNAMIC     Fa0/3        20    00e0.a371.aec7    DYNAMIC     Fa0/4
```