

Bài 7. Thực hành cấu hình tường lửa trên window 7

Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

NỘI DUNG

A. Cấu hình cơ bản

1. Bật tắt tường lửa qua giao diện hoặc lệnh

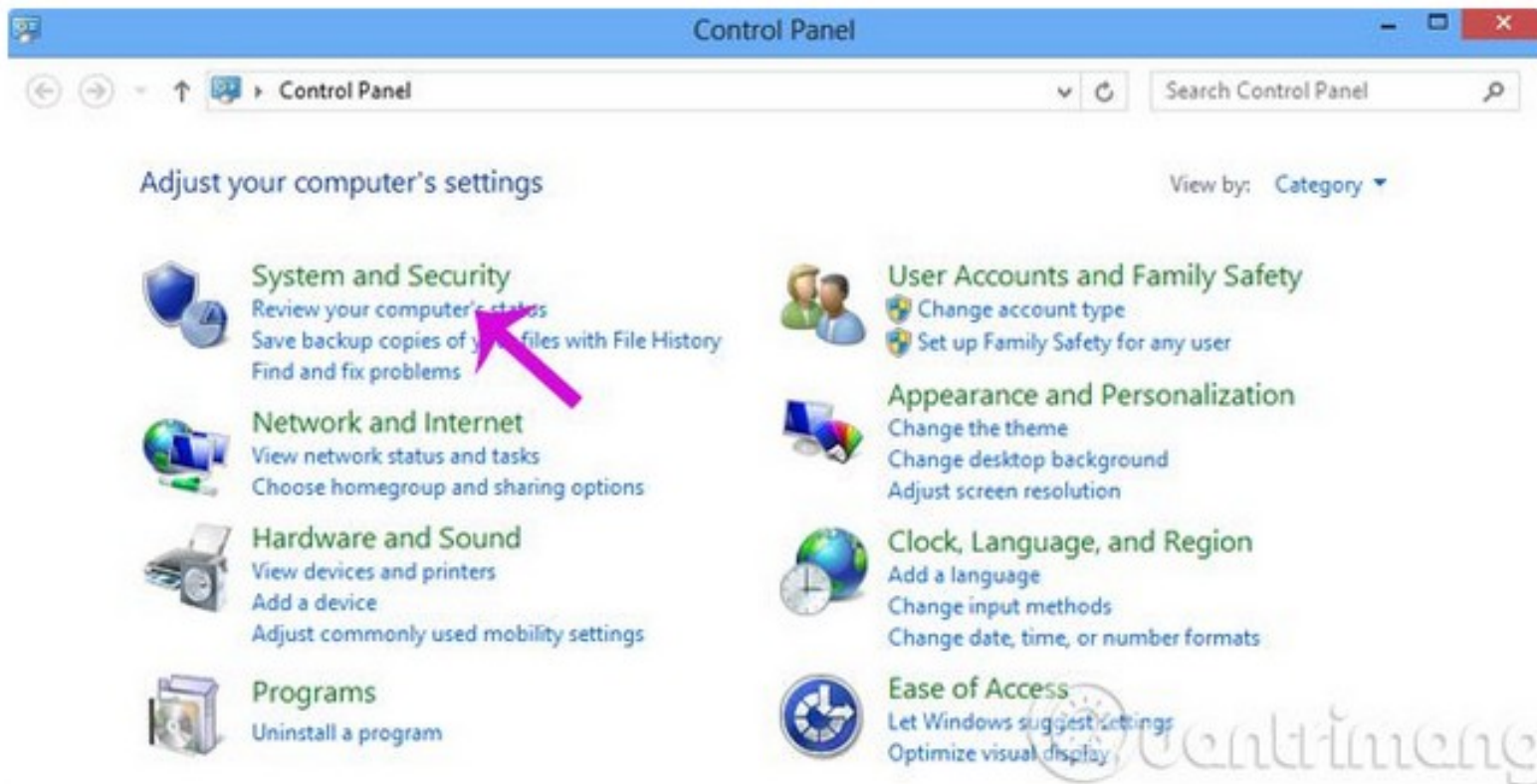
B. Cấu hình nâng cao

2. Giới thiệu các tính năng nâng cao
3. Cấu hình tường lửa ngăn chặn gói tin ICMP
4. Cấu hình tường lửa ngăn chặn truy cập ra ngoài mạng
5. Cấu hình chặn một ứng dụng sử dụng tường lửa

1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 1 - sử dụng giao diện

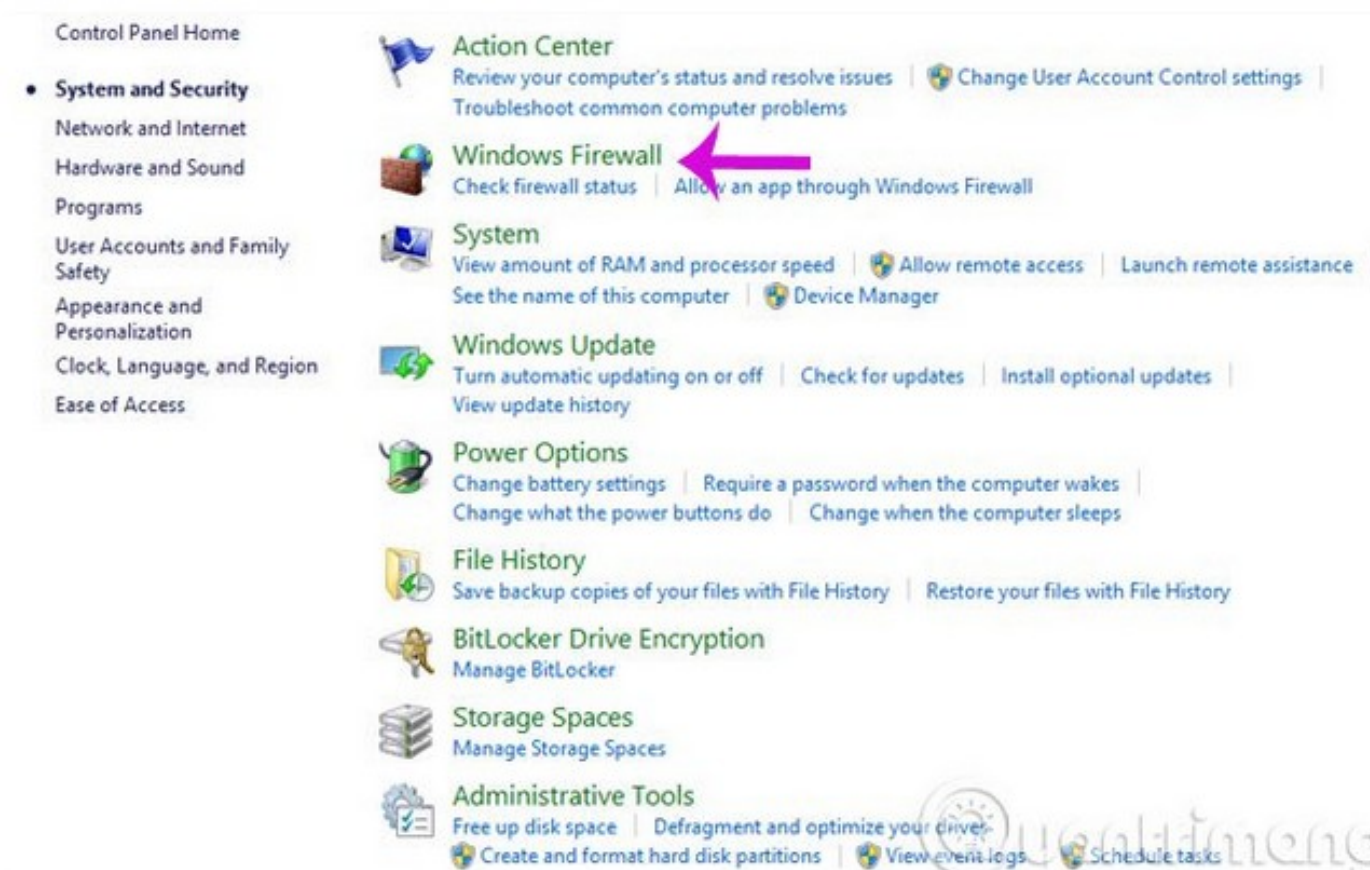
Bước 1: Đăng nhập máy tính với quyền administrator, truy cập theo đường dẫn Start > Control Panel > System and Security.



1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 1 - sử dụng giao diện

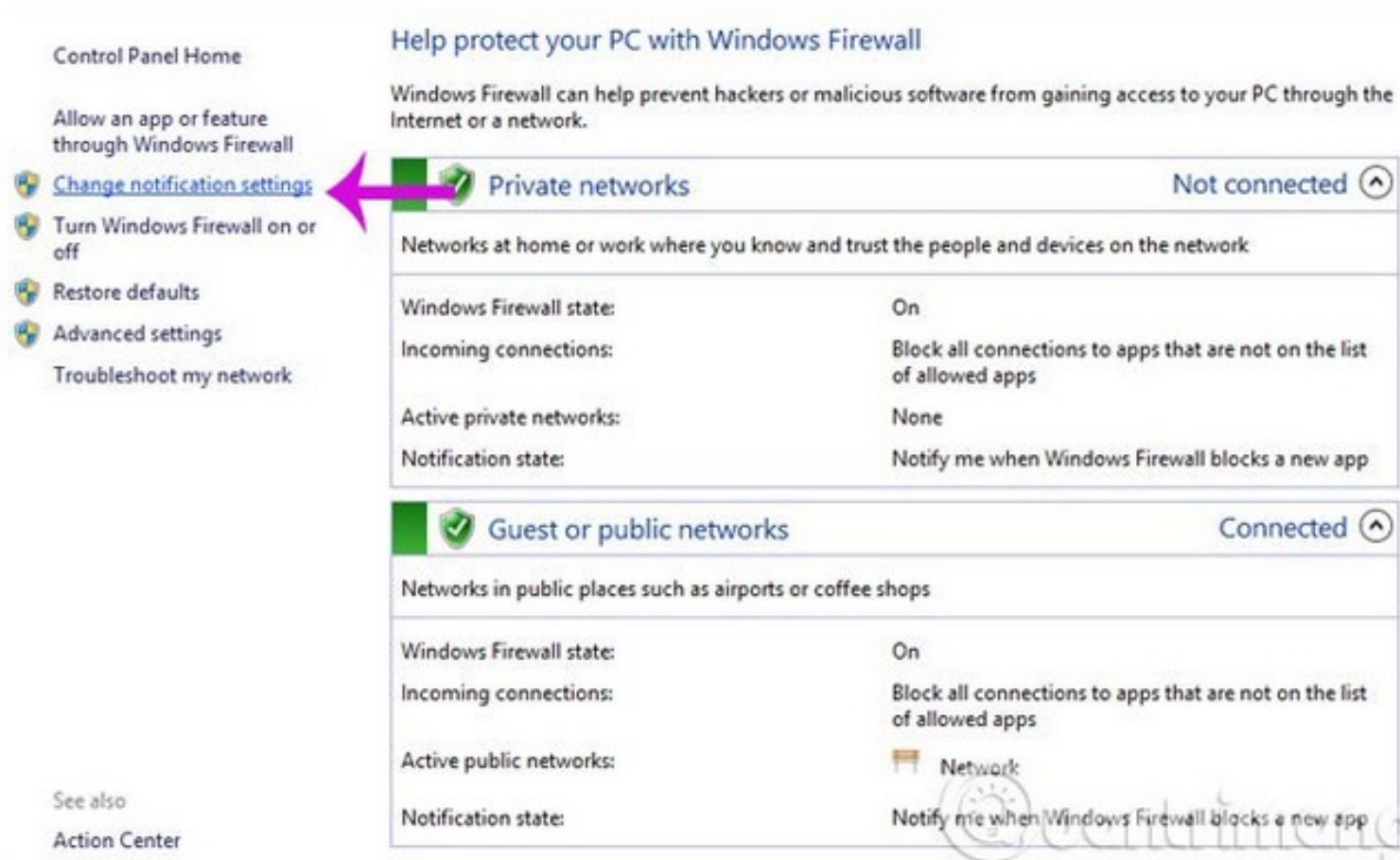
Bước 2: Trong cửa sổ System and Security, bạn click vào Windows Firewall.



1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 1 - sử dụng giao diện

Bước 3: Chọn Change notification settings để điều chỉnh cài đặt firewall.



1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 1 - sử dụng giao diện

Bước 4: Điều chỉnh bật hoặc tắt Firewall cho cả 2 chế độ Private và Public network

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

1



☒ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Firewall blocks a new app



☐ Turn off Windows Firewall (not recommended)

Public network settings

2



☒ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☒ Notify me when Windows Firewall blocks a new app



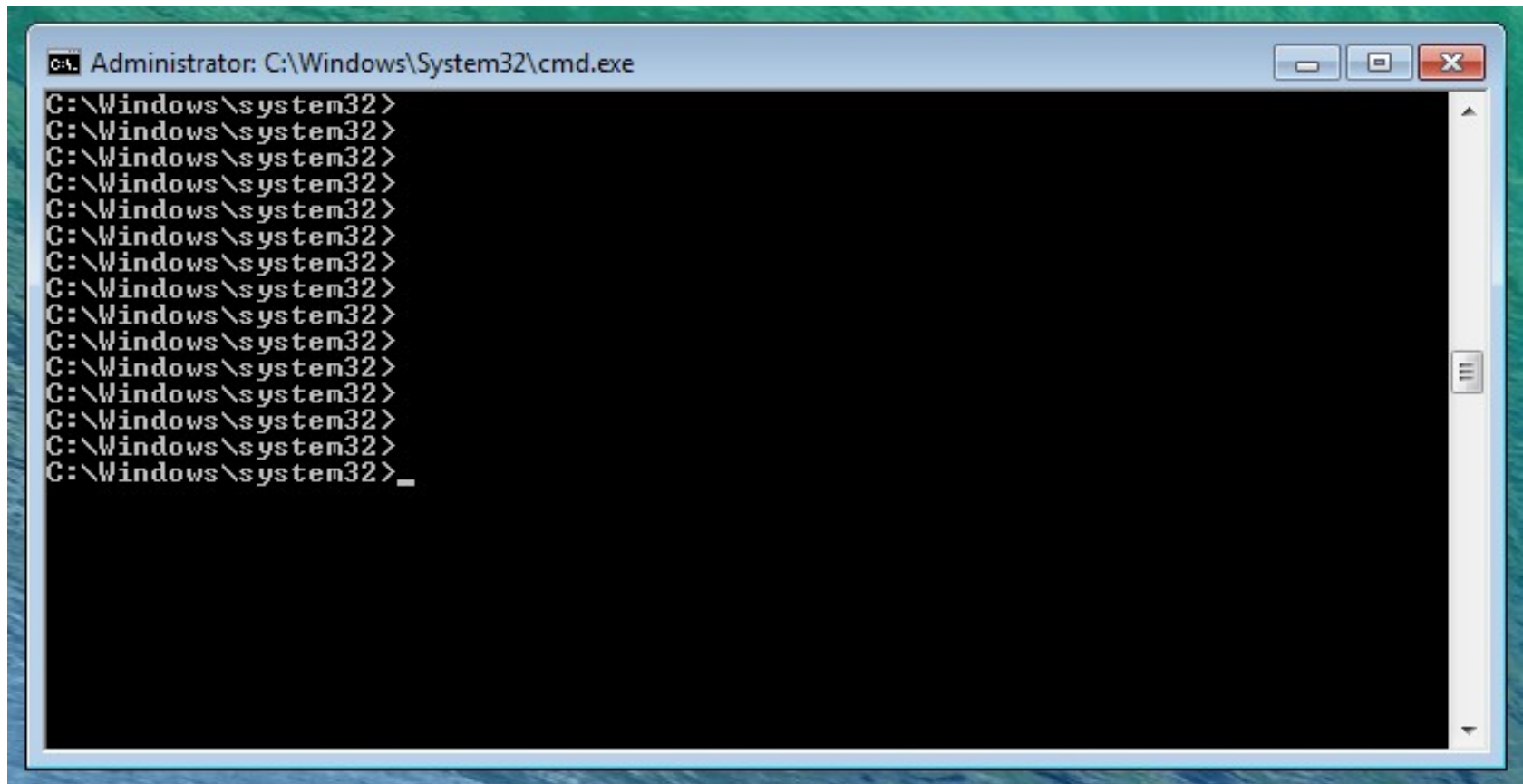
☐ Turn off Windows Firewall (not recommended)



1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 2 - sử dụng netsh

Bước 1: Bật command line dưới quyền administrative

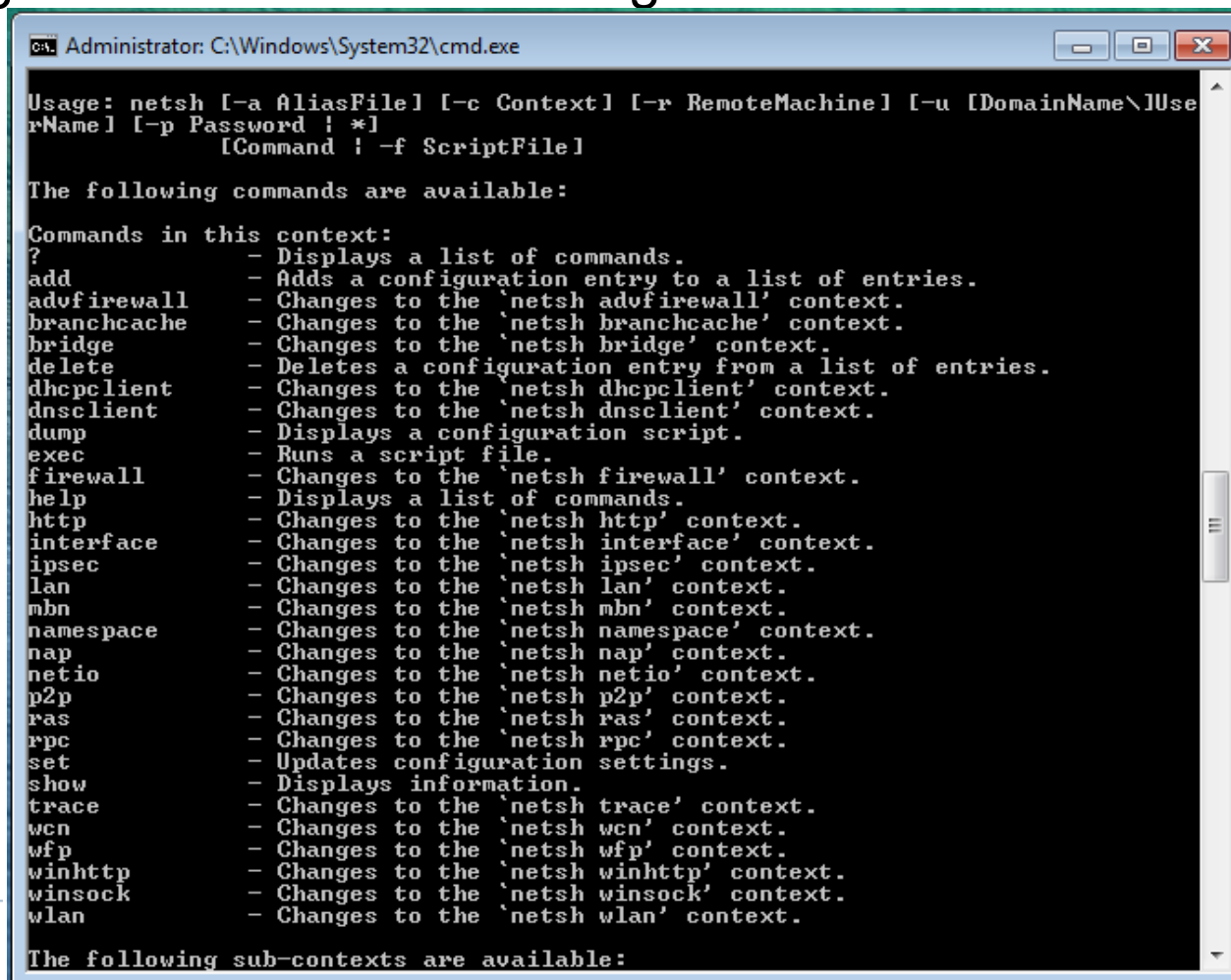


The image shows a screenshot of a Windows command prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The window has a blue title bar and standard Windows window controls (minimize, maximize, close). The command prompt area is black with white text. It displays a series of 14 identical prompts: "C:\Windows\system32>". The last prompt is followed by a cursor "_".

1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 2 - sử dụng netsh

Bước 2: gõ netsh ? để xem hướng dẫn



```
C:\Windows\System32\cmd.exe

Usage: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]User
rName] [-p Password !*]
        [Command] [-f ScriptFile]

The following commands are available:

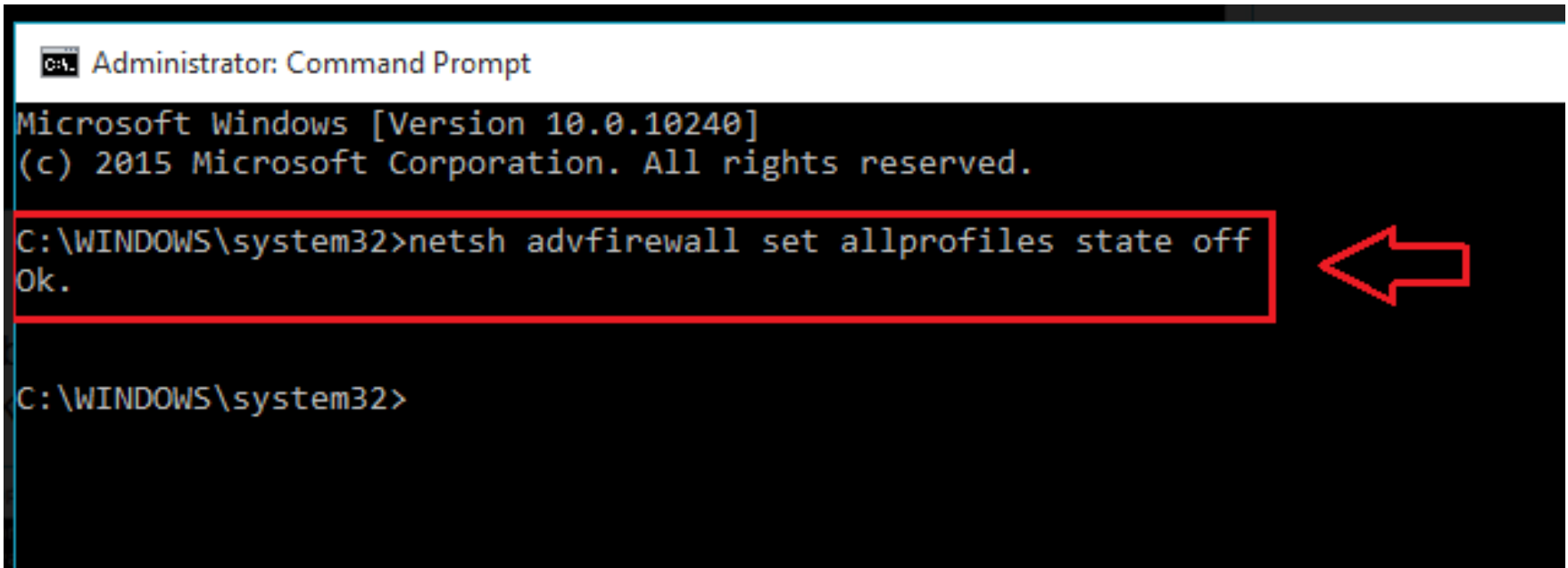
Commands in this context:
?           - Displays a list of commands.
add         - Adds a configuration entry to a list of entries.
advfirewall - Changes to the 'netsh advfirewall' context.
branchcache - Changes to the 'netsh branchcache' context.
bridge     - Changes to the 'netsh bridge' context.
delete     - Deletes a configuration entry from a list of entries.
dhcpcclient - Changes to the 'netsh dhcpcclient' context.
dnsclient  - Changes to the 'netsh dnsclient' context.
dump       - Displays a configuration script.
exec       - Runs a script file.
firewall   - Changes to the 'netsh firewall' context.
help       - Displays a list of commands.
http       - Changes to the 'netsh http' context.
interface  - Changes to the 'netsh interface' context.
ipsec      - Changes to the 'netsh ipsec' context.
lan        - Changes to the 'netsh lan' context.
mbn        - Changes to the 'netsh mbn' context.
namespace - Changes to the 'netsh namespace' context.
nap        - Changes to the 'netsh nap' context.
netio      - Changes to the 'netsh netio' context.
p2p        - Changes to the 'netsh p2p' context.
ras        - Changes to the 'netsh ras' context.
rpc        - Changes to the 'netsh rpc' context.
set        - Updates configuration settings.
show       - Displays information.
trace      - Changes to the 'netsh trace' context.
wcn        - Changes to the 'netsh wcn' context.
wfp        - Changes to the 'netsh wfp' context.
winhttp    - Changes to the 'netsh winhttp' context.
winsock    - Changes to the 'netsh winsock' context.
wlan       - Changes to the 'netsh wlan' context.

The following sub-contexts are available:
```


1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 2 - sử dụng netsh

Bước 3: tắt tường lửa netsh advfirewall set allprofiles state off



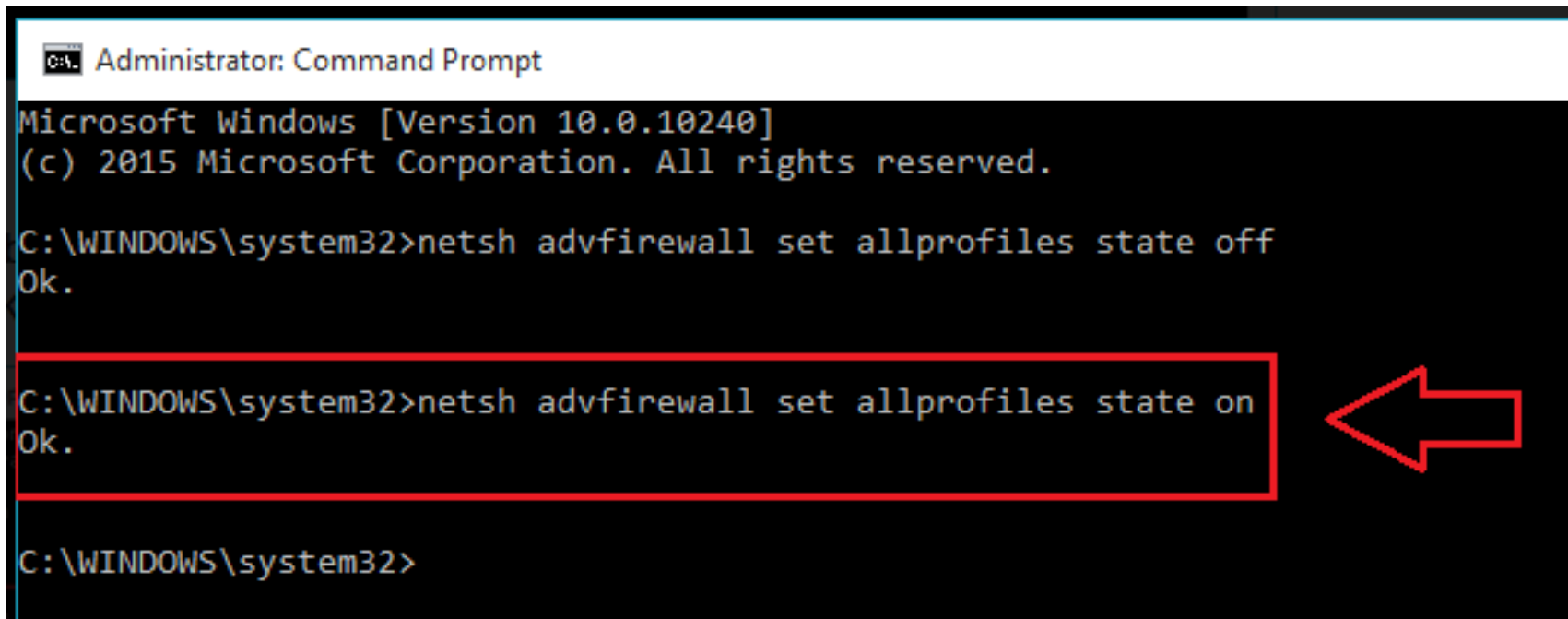
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>netsh advfirewall set allprofiles state off
Ok.
C:\WINDOWS\system32>
```

A red rectangular box highlights the command `netsh advfirewall set allprofiles state off` and its output `Ok.` in the Command Prompt. A red arrow points from the right side of the box towards the command text.

1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 2 - sử dụng netsh

Bước 3: bật tường lửa netsh advfirewall set allprofiles state on



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netsh advfirewall set allprofiles state off
Ok.

C:\WINDOWS\system32>netsh advfirewall set allprofiles state on
Ok.

C:\WINDOWS\system32>
```

A red rectangular box highlights the command `netsh advfirewall set allprofiles state on` and its output `Ok.` in the command prompt. A large red arrow points from the right side of the box towards the command text.

1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 2 - sử dụng netsh

- Khởi động (reset) lại Windows Firewall

netsh advfirewall reset

- Xem các luật đã được cấu hình

netsh advfirewall firewall show rule name=all

- Đặt lại đường dẫn của log

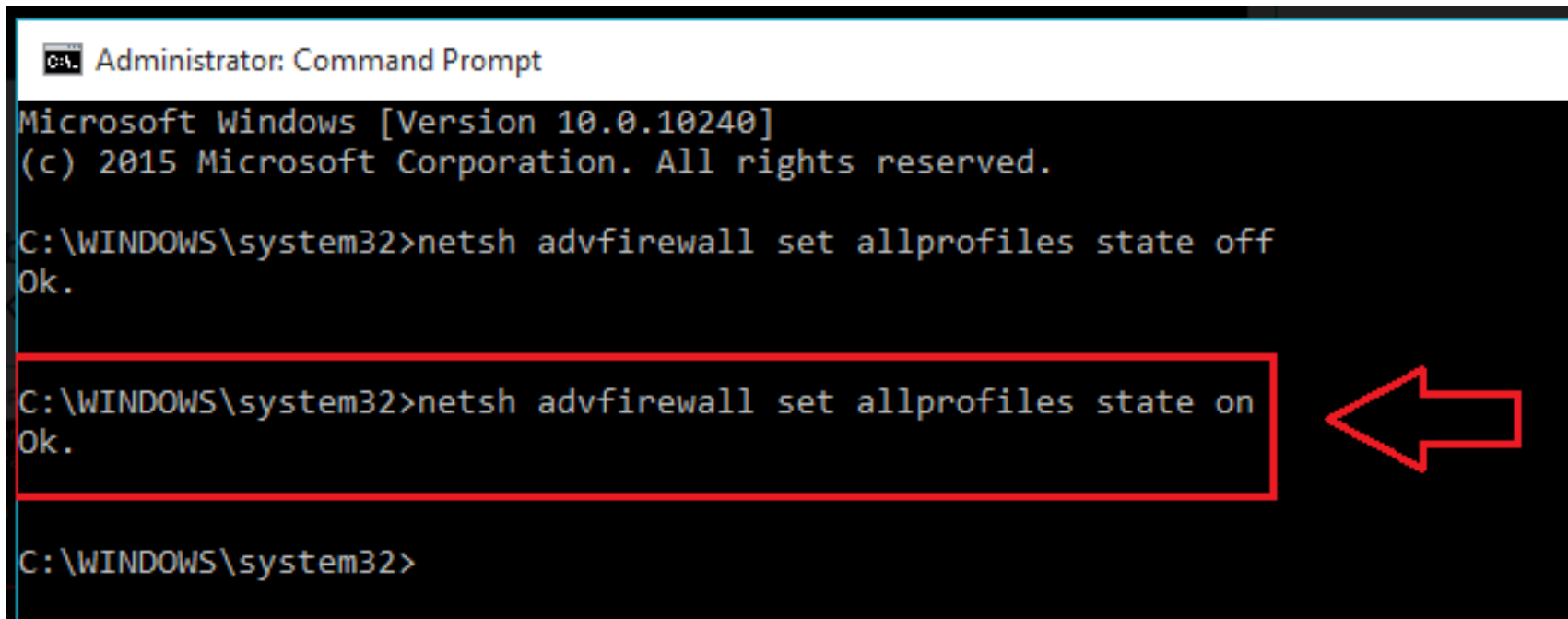
***netsh advfirewall firewall set currentprofile
logging filename "C:\temp\pfirewall.log"***

- Mặc định \Windows\system32\LogFiles\
Firewall\pfirewall.log

1. Bật tắt tường lửa qua giao diện, qua netsh

Cách 2 - sử dụng netsh

Bước 3: bật tường lửa `netsh advfirewall set allprofiles state on`



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netsh advfirewall set allprofiles state off
Ok.

C:\WINDOWS\system32>netsh advfirewall set allprofiles state on
Ok.

C:\WINDOWS\system32>
```

A red rectangular box highlights the command `netsh advfirewall set allprofiles state on` and its output `Ok.` in the command prompt. A red arrow points from the right towards this box.

2. Giới thiệu các tính năng nâng cao

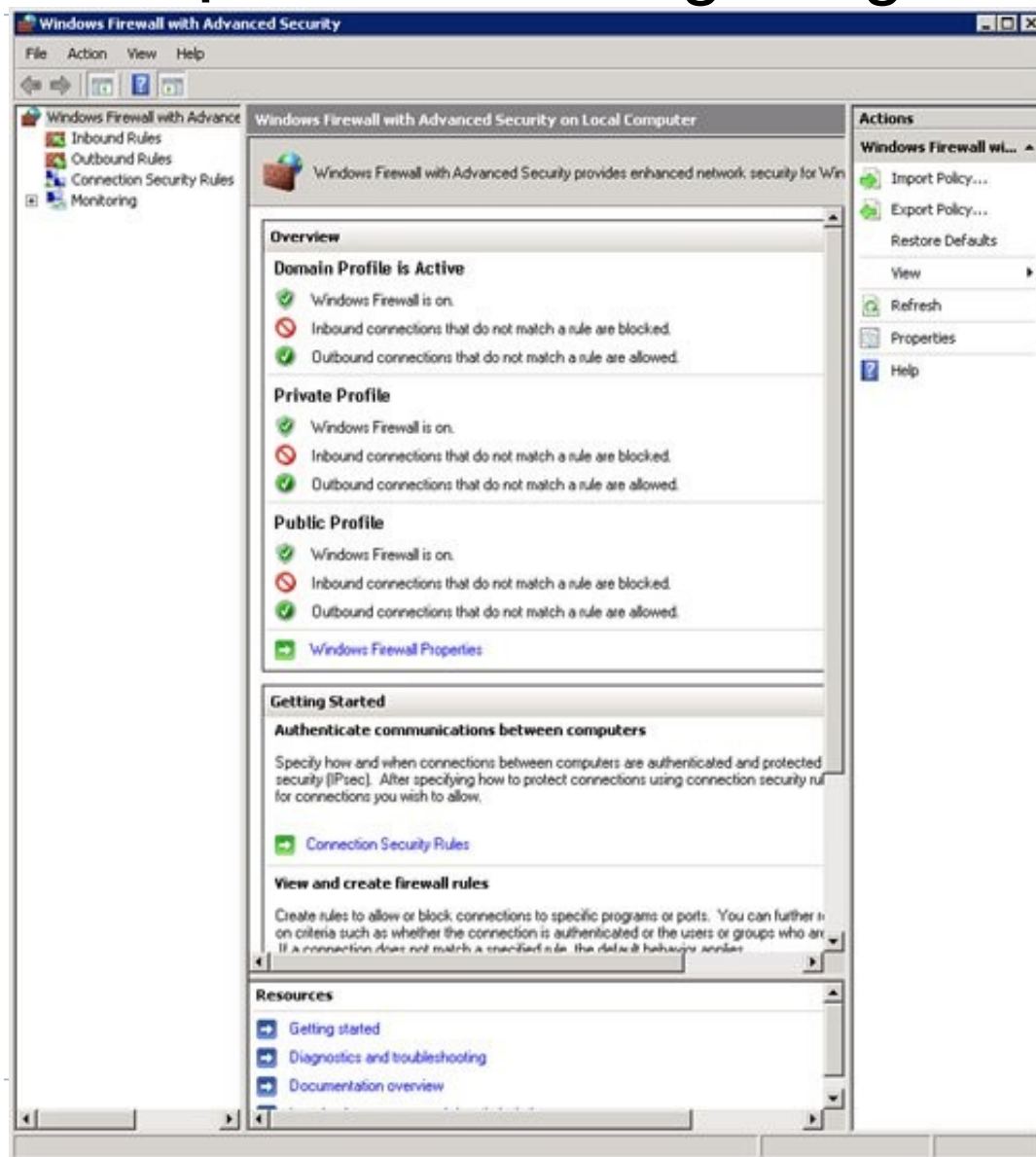
Inbound rules: các luật này sẽ kiểm soát mạng đi từ bên ngoài mạng vào bên trong mạng

Outbound rules: các luật này sẽ kiểm soát mạng đi từ bên trong mạng ra bên ngoài mạng

Connection security rules: luật bảo mật kết nối để thực thi thẩm định giữa hai máy tính ngang hàng trước khi chúng có thể thiết lập một kết nối và bảo đảm các thông tin được truyền tải giữa hai máy tính.

Monitoring: sử dụng giao diện kiểm tra để hiển thị các thông tin về các rule tường lửa hiện hành, các rule bảo mật kết nối và các vấn đề bảo mật liên quan.

2. Giới thiệu các tính năng nâng cao



2. Giới thiệu các tính năng nâng cao

Cấu trúc của 1 rule

Name	Group	Profile	Enabled	Action	Override
Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
Allowed Users	Allowed Computers				

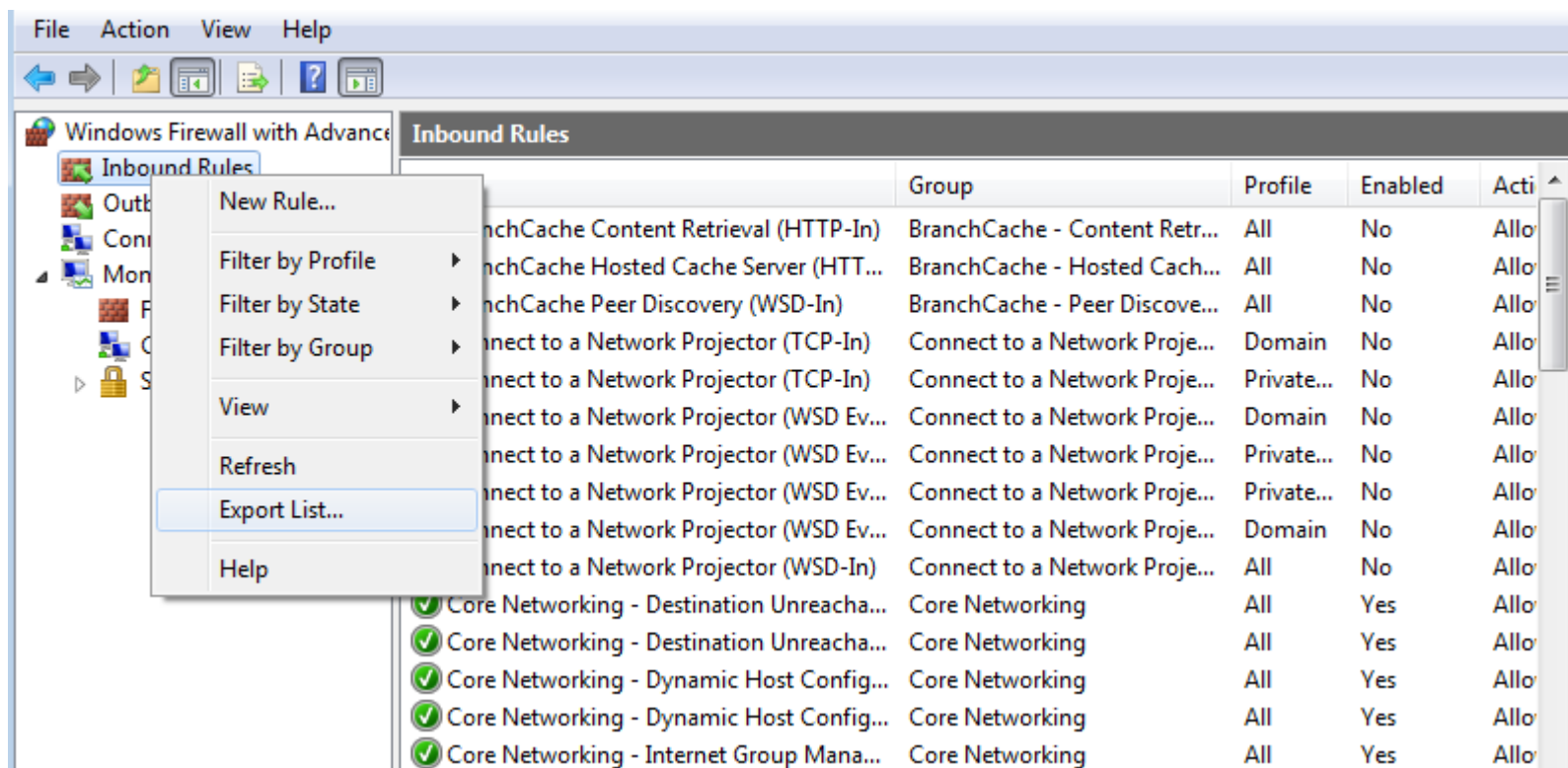
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Allowed Users	Allowed Computers
block icmp	rule	All	Yes	Allow	No	Any	Any	Any	ICMPv4	Any	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache	- Content Retrieval (Uses HTTP)	All	No	Allow	No	SYSTEM	Any	Any	TCP	80	Any	Any
BranchCache Hosted Cache Server (HTTP-In)	BranchCache	- Hosted Cache Server (Uses HTTPS)	All	No	Allow	No	SYSTEM	Any	Any	TCP	443	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache	- Peer Discovery (Uses WSD)	All	No	Allow	No	%systemroot%\system32\svchost.exe	Any	Local	subnet	UDP	3702	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Projector	Domain	No	Allow	No	%SystemRoot%\system32\netproj.exe	Any	Any	TCP	Any	Any	Any	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Projector	Private, Public	No	Allow	No	%SystemRoot%\system32\netproj.exe	Any	Local	subnet	TCP	Any	Any	Any
Connect to a Network Projector (WSD Events-In)	Connect to a Network Projector	Domain	No	Allow	No	System	Any	Any	TCP	5357	Any	Any	Any
Connect to a Network Projector (WSD Events-In)	Connect to a Network Projector	Private, Public	No	Allow	No	System	Any	Local	subnet	TCP	5357	Any	Any
Connect to a Network Projector (WSD EventsSecure-In)	Connect to a Network Projector	Private, Public	No	Allow	No	System	Any	Local	subnet	TCP	5358	Any	Any
Connect to a Network Projector (WSD EventsSecure-In)	Connect to a Network Projector	Domain	No	Allow	No	System	Any	Any	TCP	5358	Any	Any	Any
Connect to a Network Projector (WSD-In)	Connect to a Network Projector	All	No	Allow	No	%SystemRoot%\system32\netproj.exe	Any	Local	subnet	UDP	3702	Any	Any
Core Networking - Destination Unreachable (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any	Any
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any	Any

2. Giới thiệu các tính năng nâng cao

Cách inport export rules

netsh advfirewall export "C:\temp\WFconfiguration.wfw"

netsh advfirewall import "C:\temp\WFconfiguration.wfw"



2. Giới thiệu các tính năng nâng cao

Inbound rules

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

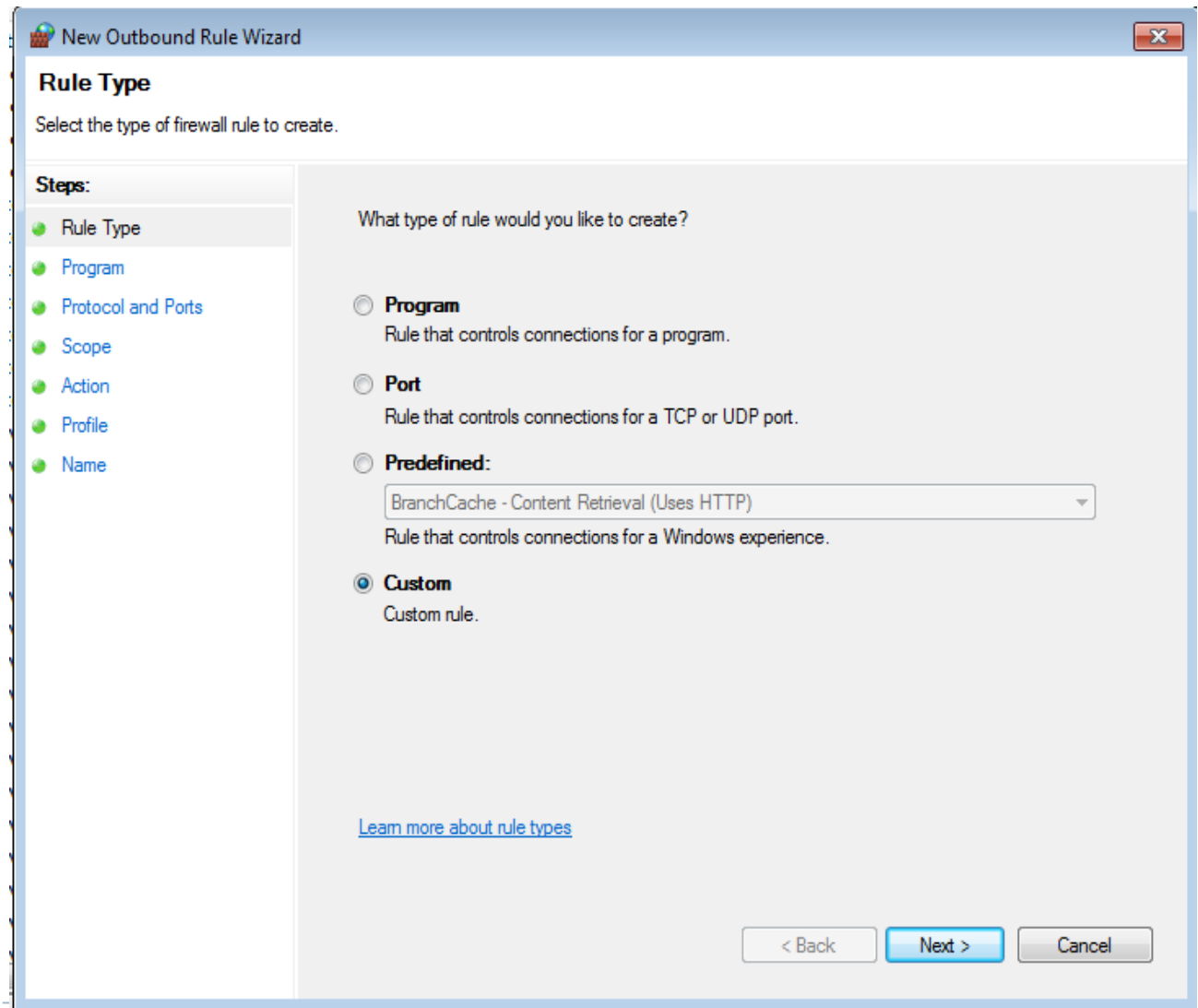
☒ **Custom**
Custom rule.

[Learn more about rule types](#)

< Back Next > Cancel

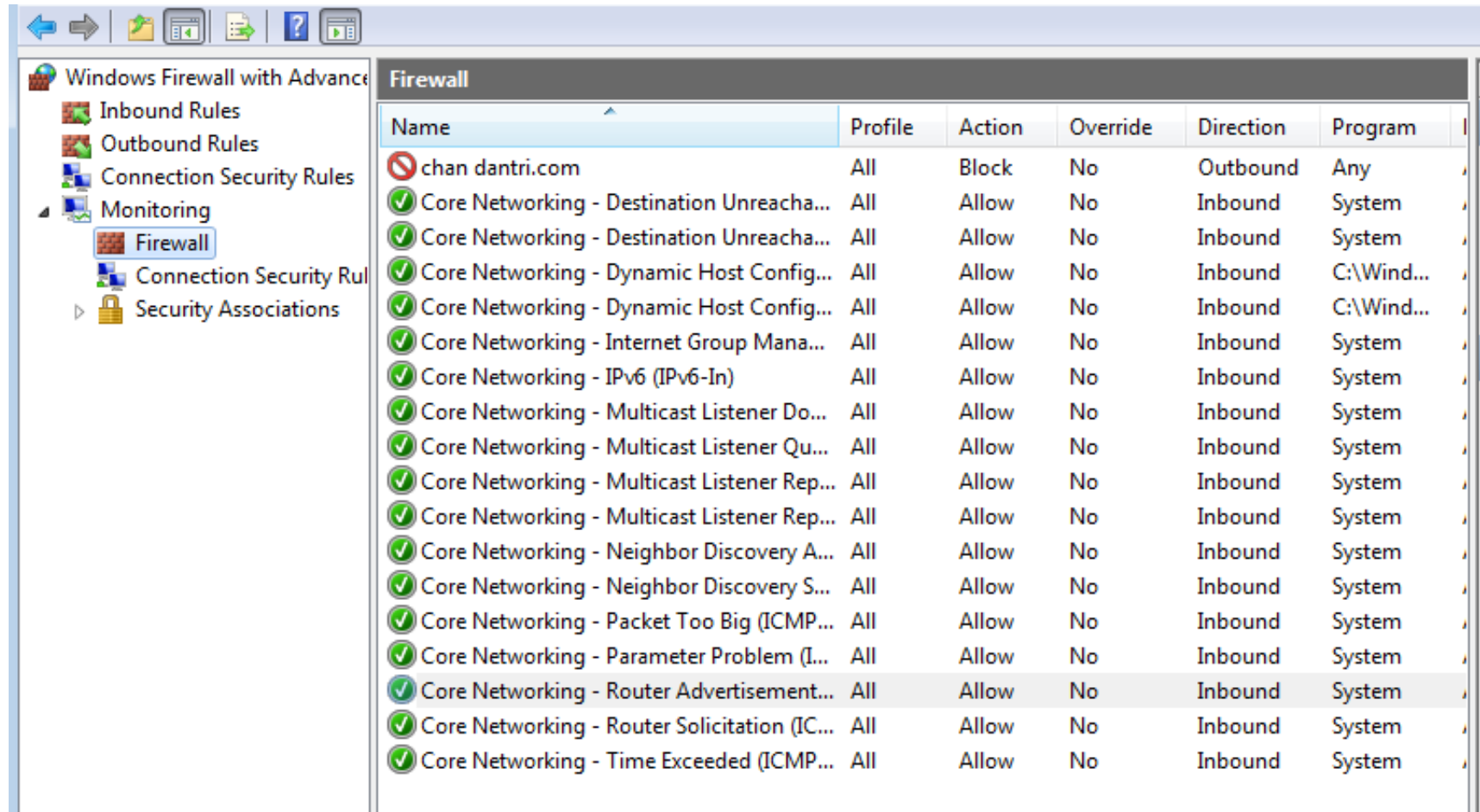
2. Giới thiệu các tính năng nâng cao

outbound rules



2. Giới thiệu các tính năng nâng cao

Monitoring



Name	Profile	Action	Override	Direction	Program
chan dantri.com	All	Block	No	Outbound	Any
Core Networking - Destination Unreach...	All	Allow	No	Inbound	System
Core Networking - Destination Unreach...	All	Allow	No	Inbound	System
Core Networking - Dynamic Host Config...	All	Allow	No	Inbound	C:\Wind...
Core Networking - Dynamic Host Config...	All	Allow	No	Inbound	C:\Wind...
Core Networking - Internet Group Mana...	All	Allow	No	Inbound	System
Core Networking - IPv6 (IPv6-In)	All	Allow	No	Inbound	System
Core Networking - Multicast Listener Do...	All	Allow	No	Inbound	System
Core Networking - Multicast Listener Qu...	All	Allow	No	Inbound	System
Core Networking - Multicast Listener Rep...	All	Allow	No	Inbound	System
Core Networking - Multicast Listener Rep...	All	Allow	No	Inbound	System
Core Networking - Neighbor Discovery A...	All	Allow	No	Inbound	System
Core Networking - Neighbor Discovery S...	All	Allow	No	Inbound	System
Core Networking - Packet Too Big (ICMP...	All	Allow	No	Inbound	System
Core Networking - Parameter Problem (I...	All	Allow	No	Inbound	System
Core Networking - Router Advertisement...	All	Allow	No	Inbound	System
Core Networking - Router Solicitation (IC...	All	Allow	No	Inbound	System
Core Networking - Time Exceeded (ICMP...	All	Allow	No	Inbound	System

3. Cấu hình tường lửa ngăn chặn gói tin ICMP

1. Tắt:

```
netsh advfirewall firewall add rule="ALL ICMP V4" dir=IN action  
= block protocol=icmpv4
```

2. Bật:

```
netsh advfirewall firewall add rule="ALL ICMP V4" dir=IN action  
= allow protocol=icmpv4
```

3. Kích hoạt port:

```
netsh advfirewall firewall add rule name="Open SQL Server Port  
1433" dir=in action=allow protocol=TCP localport=1433
```

4. Kích hoạt remote desktop

```
netsh advfirewall firewall set rule group="remote desktop"  
new enable=Yes
```

5. Import export

```
netsh advfirewall export "C:\temp\WFconfiguration.wfw"  
netsh advfirewall import "C:\temp\WFconfiguration.wfw"
```

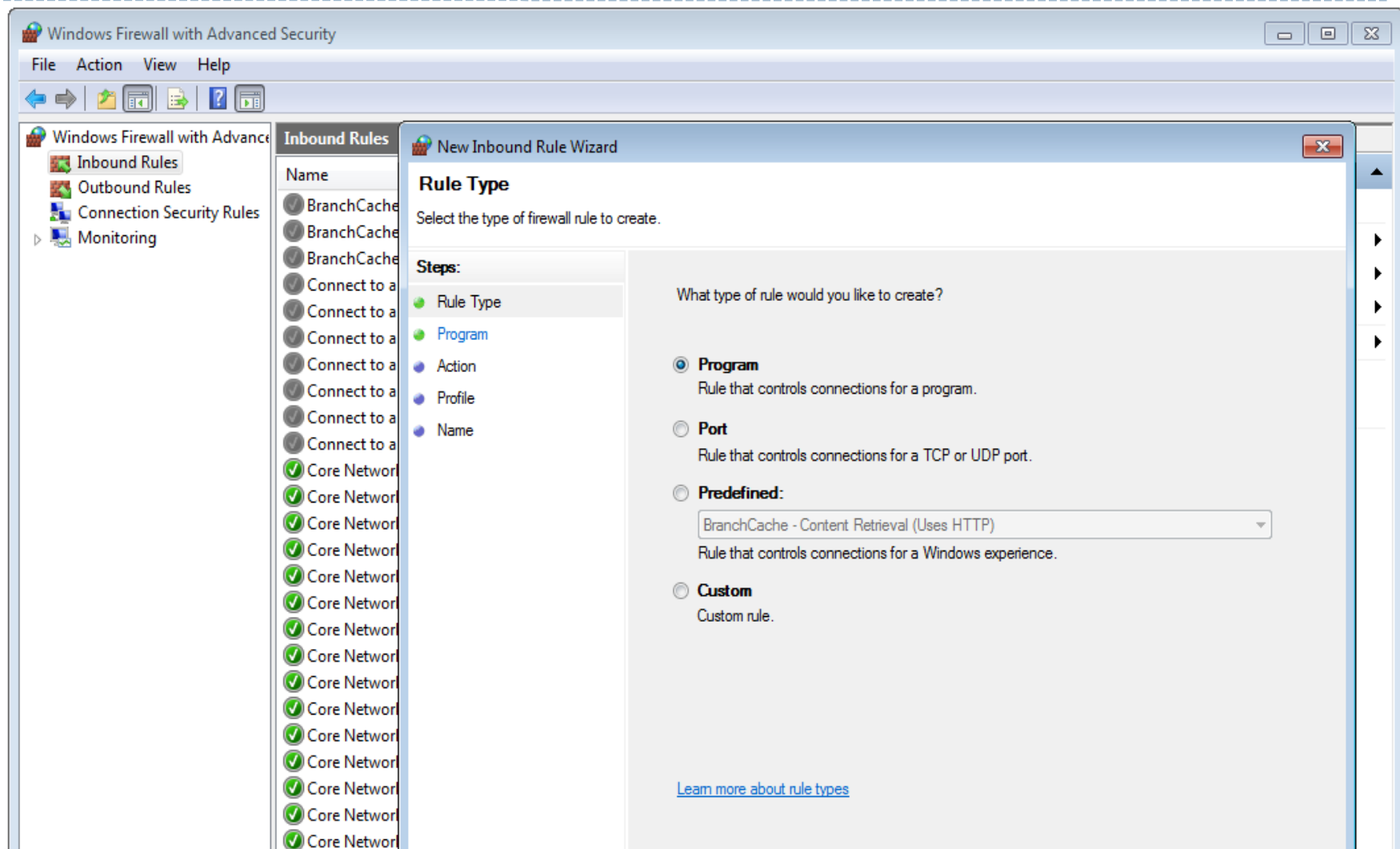
3. Cấu hình tường lửa ngăn chặn gói tin ICMP

Bước 1: Mở Rule cho gói ICMP bạn vào mở ***Control Pannel -> Windows Firewall -> Advanced setting -> chọn Inbound Rules.***

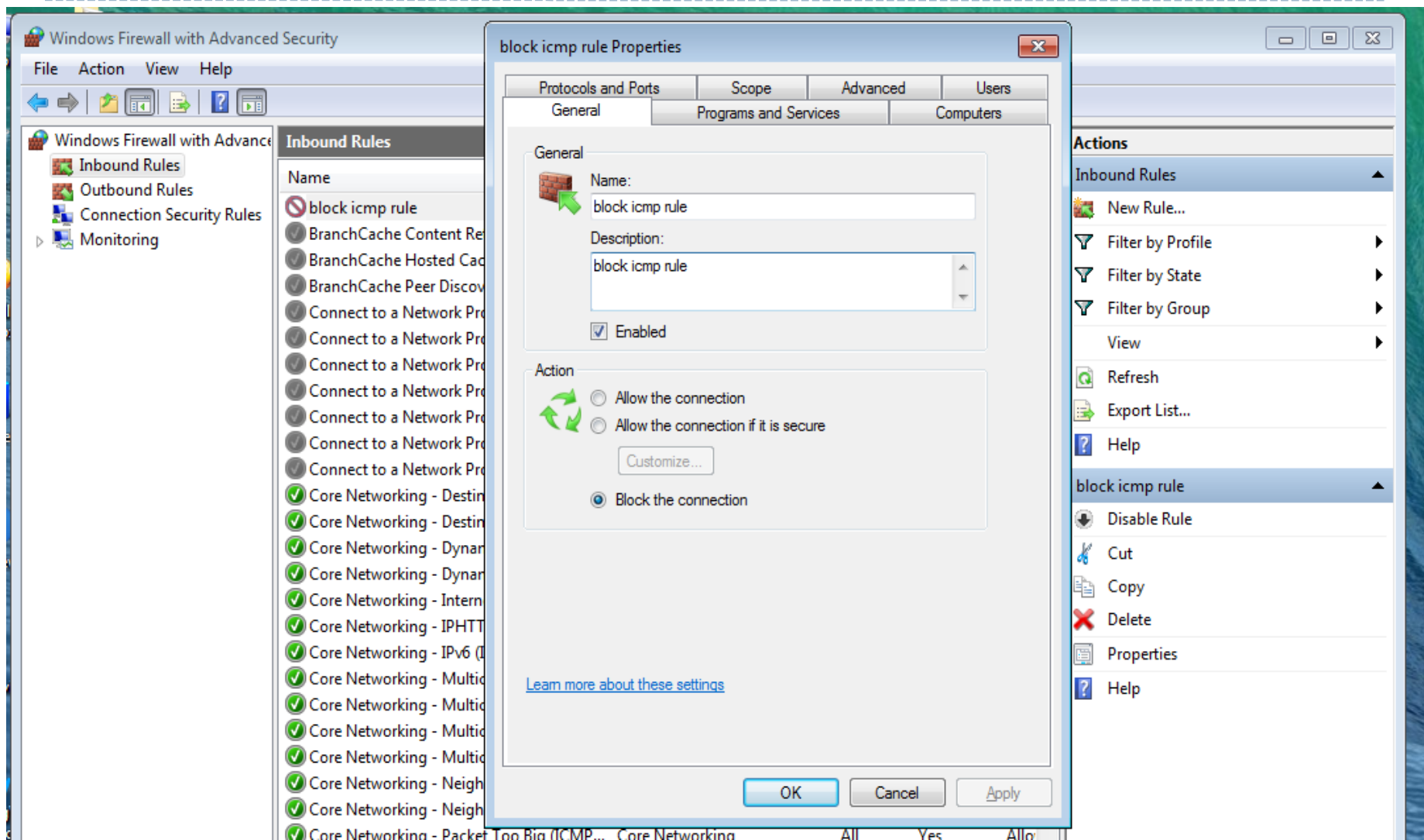
Bước 2: chọn **New rule** trong mục Actions -> trong của sổ New Inbound Rule chọn Custom rồi nhấn Next

Bước 3: chọn 1 chương trình nào hoặc All program rồi nhấn Next

3. Cấu hình tường lửa ngăn chặn gói tin ICMP



3. Cấu hình tường lửa ngăn chặn gói tin ICMP

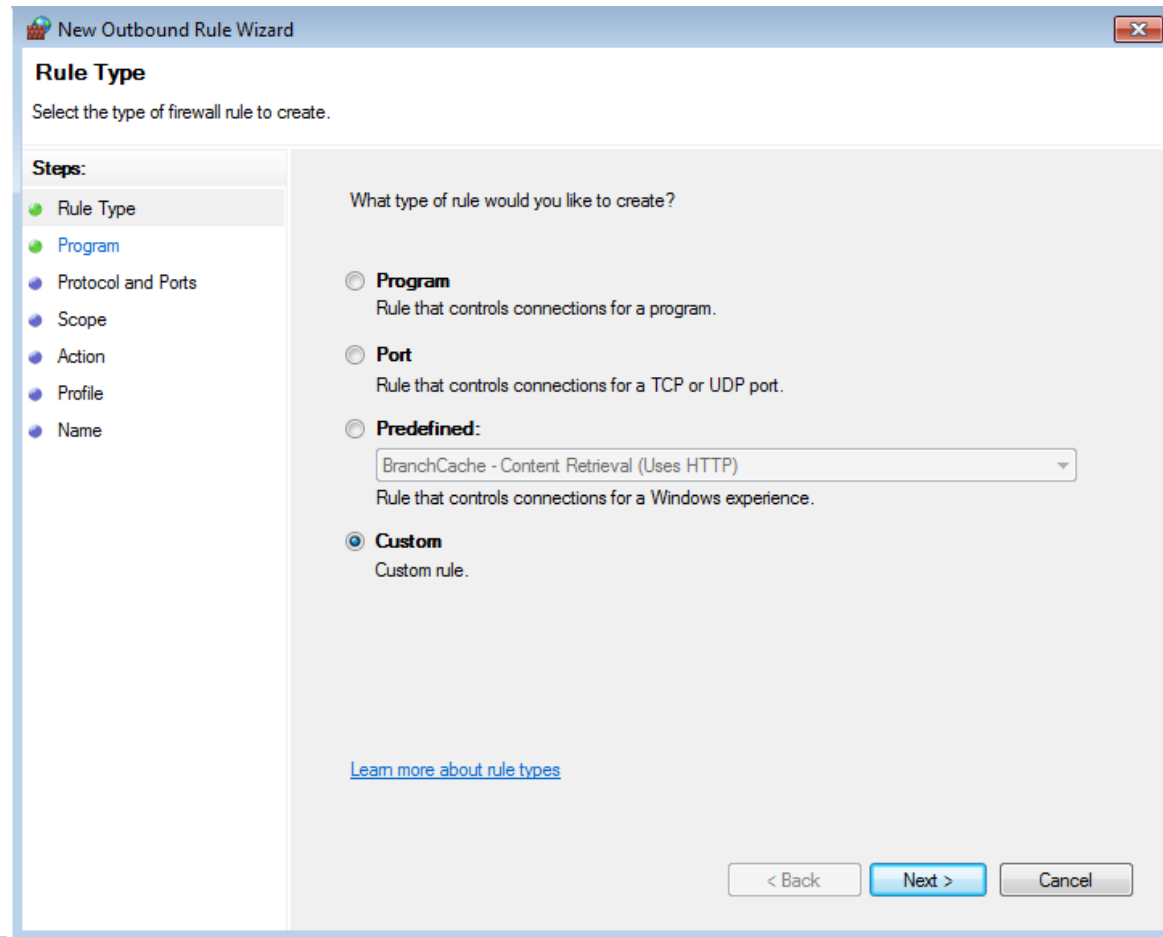


3. Cấu hình tường lửa ngăn chặn gói tin ICMP

```
phaivd@phaivd-Aspire-V5-471: ~  
File Edit View Search Terminal Help  
phaivd@phaivd-Aspire-V5-471:~$ ping 192.168.81.128  
PING 192.168.81.128 (192.168.81.128) 56(84) bytes of data.  
^C  
--- 192.168.81.128 ping statistics ---  
9 packets transmitted, 0 received, 100% packet loss, time 8192ms  
  
phaivd@phaivd-Aspire-V5-471:~$ ping 192.168.81.128  
PING 192.168.81.128 (192.168.81.128) 56(84) bytes of data.  
64 bytes from 192.168.81.128: icmp_seq=1 ttl=128 time=0.619 ms  
64 bytes from 192.168.81.128: icmp_seq=2 ttl=128 time=0.476 ms  
64 bytes from 192.168.81.128: icmp_seq=3 ttl=128 time=0.718 ms  
64 bytes from 192.168.81.128: icmp_seq=4 ttl=128 time=0.645 ms  
^C  
--- 192.168.81.128 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3073ms  
rtt min/avg/max/mdev = 0.476/0.614/0.718/0.091 ms  
phaivd@phaivd-Aspire-V5-471:~$ ping 192.168.81.128  
PING 192.168.81.128 (192.168.81.128) 56(84) bytes of data.  
█
```

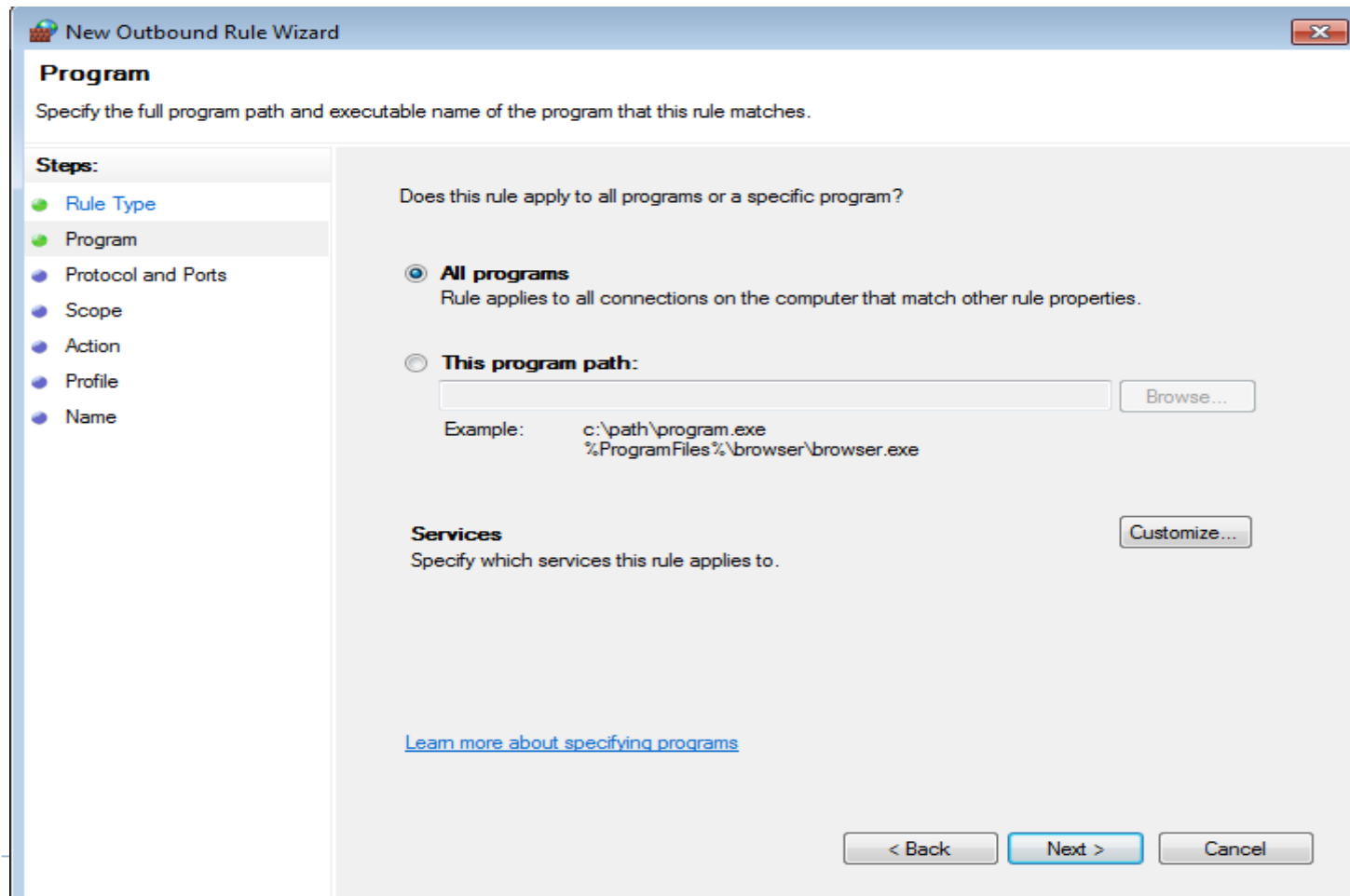
4. Cấu hình tường lửa ngăn chặn truy cập ra ngoài mạng

B1. Nhấn vào Outbound và tạo mới 1 rule



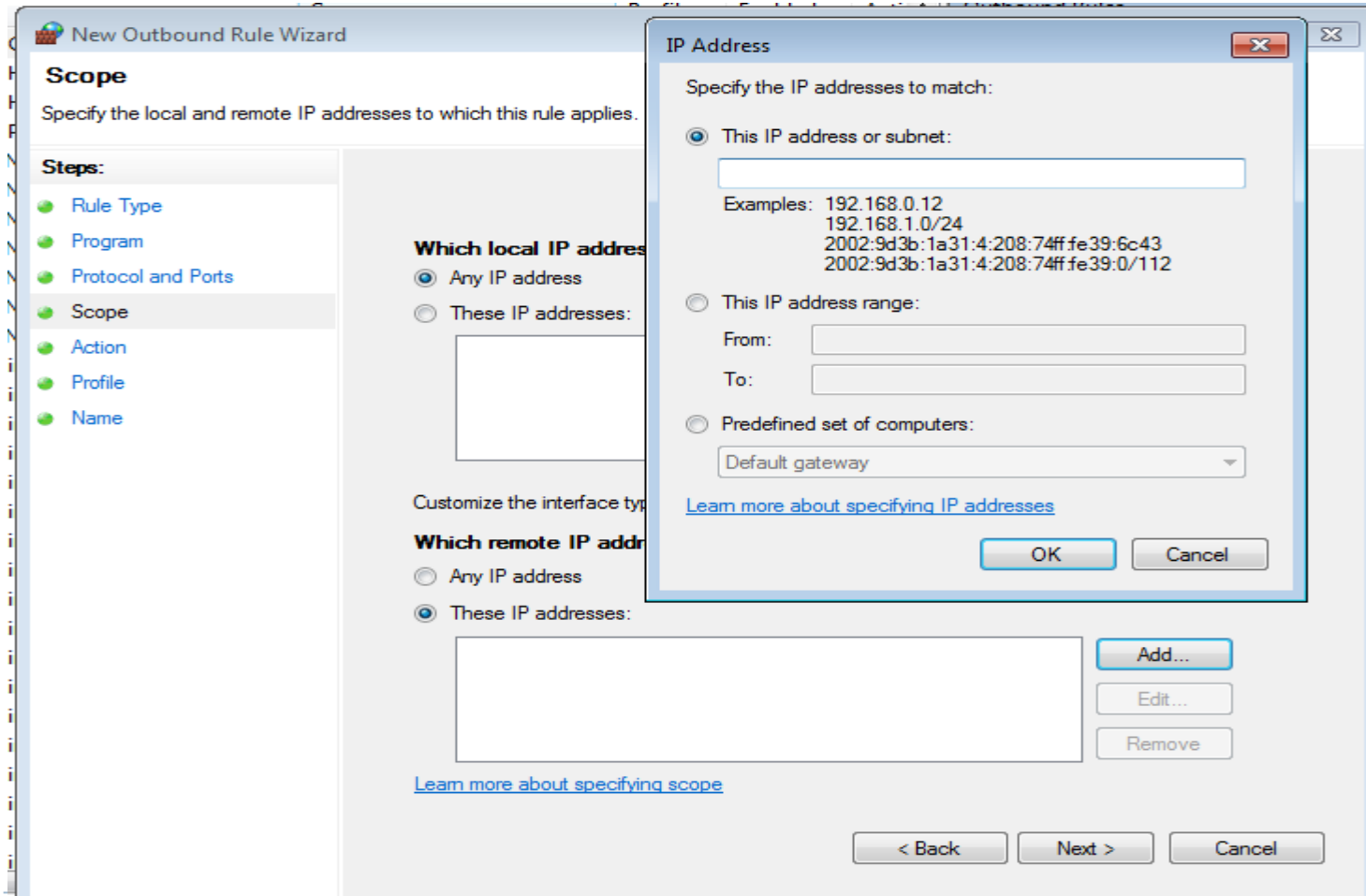
4. Cấu hình tường lửa ngăn chặn truy cập ra ngoài mạng

B2. chọn custom và nhấn Next



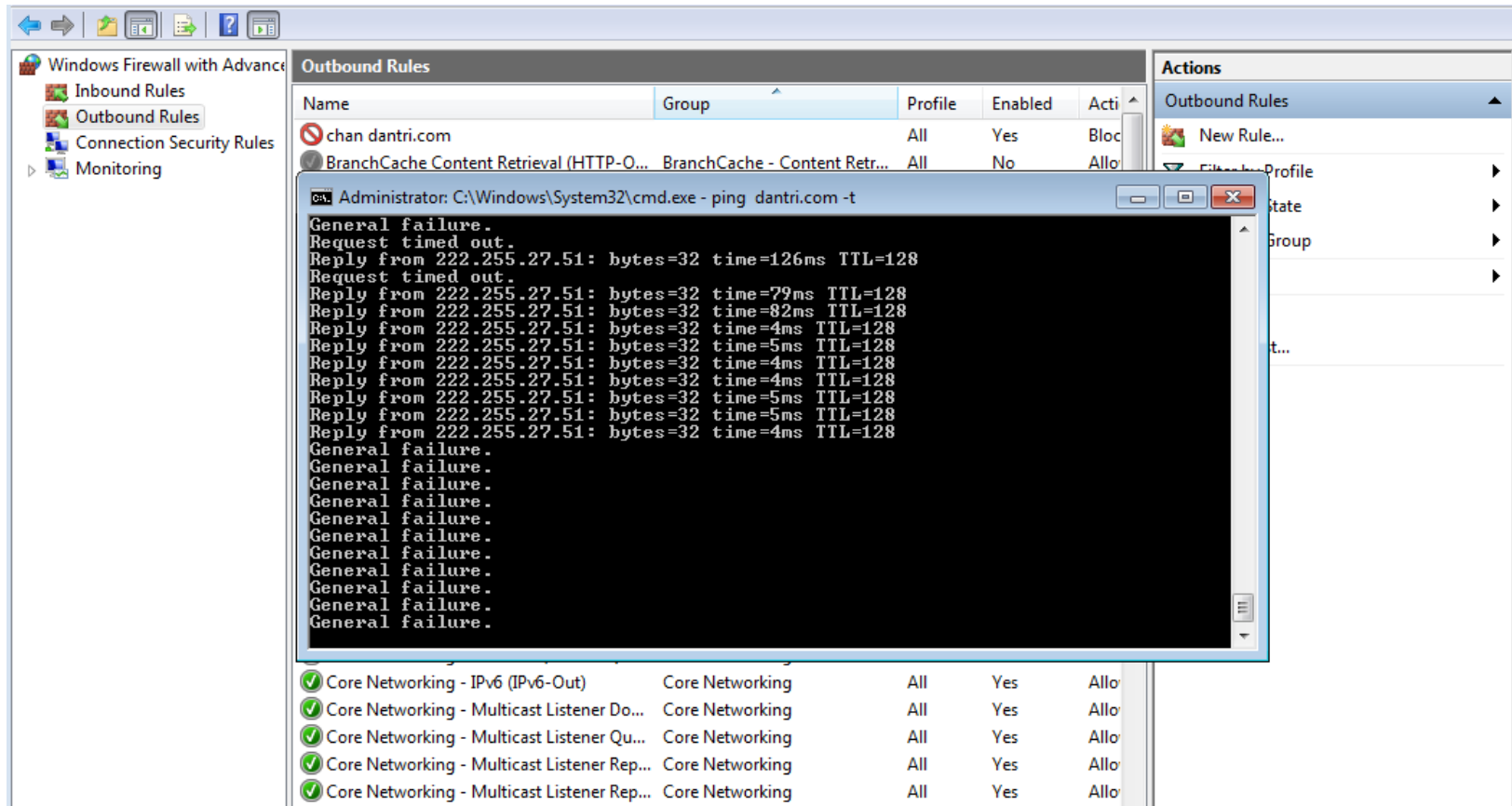
4. Cấu hình tường lửa ngăn chặn truy cập ra ngoài mạng

B3. Chọn scope rồi nhập địa chỉ IP cần chặn



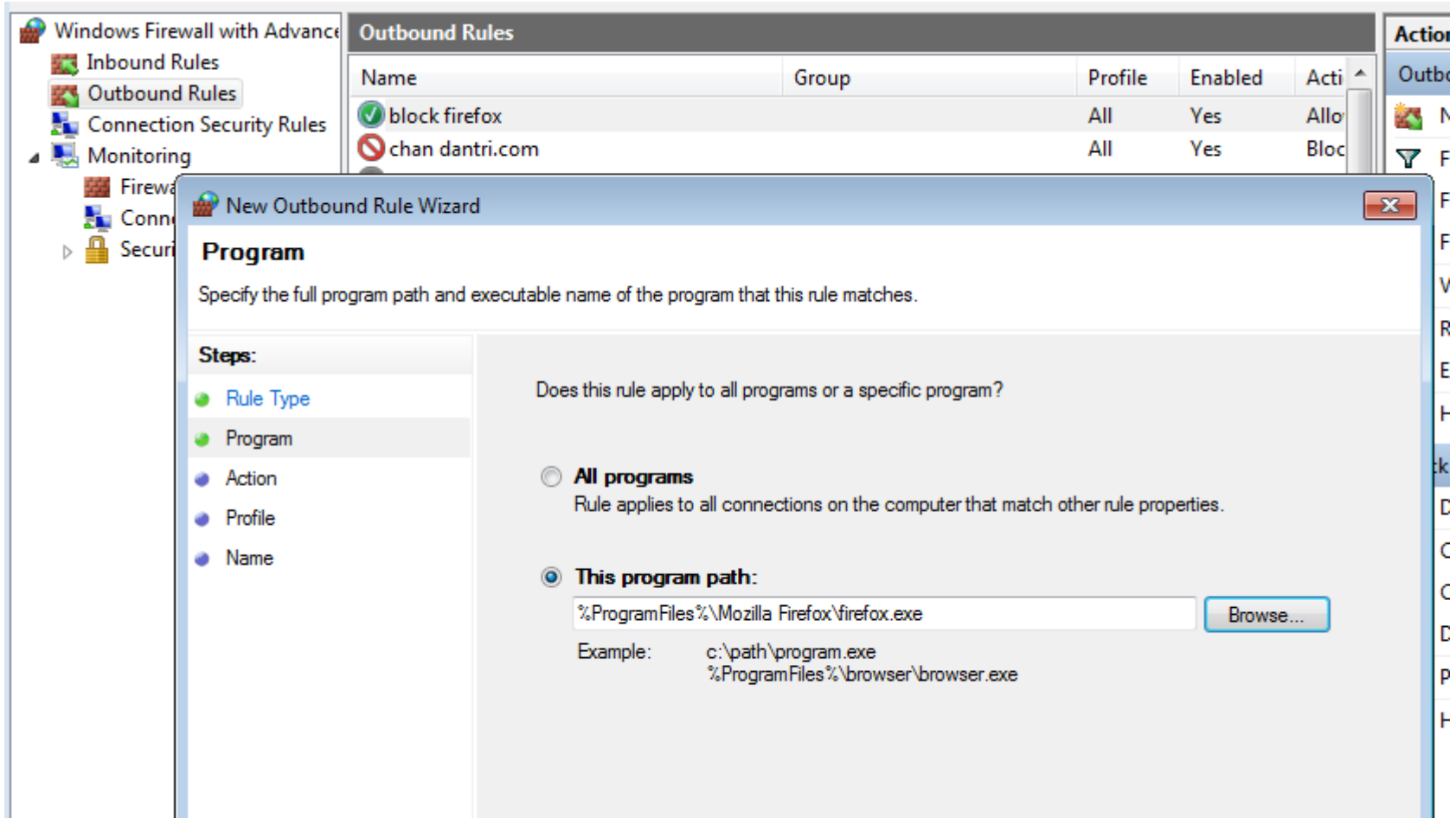
4. Cấu hình tường lửa ngăn chặn truy cập ra ngoài mạng

B4. Chọn chế độ block. Kết quả địa chỉ của Dantri bị chặn



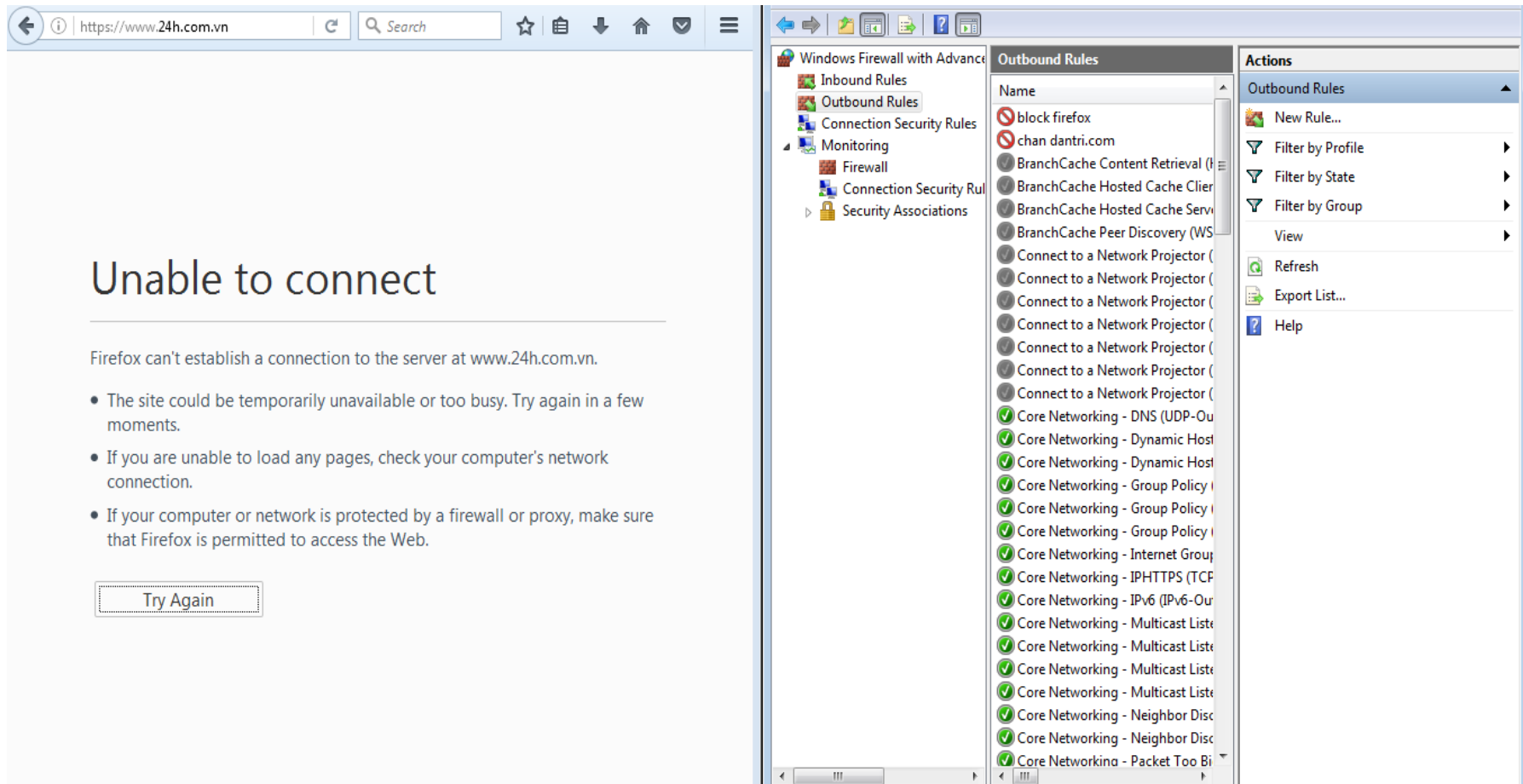
5. Cấu hình chặn một ứng dụng sử dụng tường lửa

Lựa chọn chương trình chạy qua tường lửa như sau



5. Cấu hình chặn một ứng dụng sử dụng tường lửa

Lựa chọn chương trình chạy qua tường lửa như sau



HỎI VÀ ĐÁP