

**BẢO MẬT HỆ THỐNG
VỚI
WINDOWS FIREWALL**

Tổng quan

1. Tổng quan về Windows Firewall.
2. Windows Firewall with Advanced Security.
3. Cấu hình các quy tắc Firewall.
4. Các quy tắc bảo mật nối kết.
5. Giám sát Windows Firewall with Advanced Security.

Tường lửa (Firewall) là gì?

- ❖ Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống.
- ❖ Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn
- ❖ Một khi bạn đã xem xét bảo vệ vật lý cho các máy chủ của bạn, bạn cần bắt đầu quan tâm tới các con đường chính có thể xâm nhập vào mạng của.

Tác dụng của tường lửa

- ❖ Một số mối nguy hiểm mà tường lửa có thể bảo vệ chống lại được như sau:
 - ❑ Ứng dụng mạng quét các cổng không có bảo vệ, để kẻ tấn công có thể sử dụng để truy cập vào hệ thống.
 - ❑ Ứng dụng trojan horse mở một kết nối tới một máy tính trên Internet, cho phép kẻ tấn công bên ngoài chạy chương trình và truy cập dữ liệu lưu trữ trên hệ thống.

Windows Server 2012 Firewall

- ❖ Windows Server 2012 bao gồm một chương trình tường lửa được gọi là Windows Firewall, được kích hoạt mặc định trên tất cả các hệ thống Windows Server 2012.
- ❖ Theo mặc định, Windows Firewall chặn hầu hết các giao thông mạng xâm nhập vào máy tính.
- ❖ Tường lửa hoạt động bằng cách kiểm tra các nội dung gói tin vào/ra của máy tính và so sánh thông tin với các quy tắc, từ đó xác định các gói tin được phép đi qua tường lửa và gói tin nào bị chặn.

Windows Firewall with Advanced Security

- ❖ Windows Firewall with Advanced Security là gì?
- ❖ Windows Firewall with Advanced Security Console
- ❖ Các loại firewall profile
- ❖ Cấu hình profile

Windows Firewall with Advanced Security là gì?

- ❖ Windows Firewall with Advanced Security là một sự kết hợp giữa firewall cá nhân (host firewall) và IPsec, cho phép bạn cấu hình để lọc các kết nối vào và ra trên hệ thống.
- ❖ Cung cấp một giao diện mạnh mẽ hơn để quản lý các chính sách tường lửa một cách chi tiết.
- ❖ Được sử dụng để quản lý Windows Firewall dựa trên cổng, dịch vụ, ứng dụng, và các giao thức.

Windows Firewall with Advanced Security Console

- ❖ Có thể được sử dụng để quản lý các lĩnh vực sau:
 - ❑ Các quy tắc vào (Inbound rules)
 - ❑ Các quy tắc ra (Outbound rules)
 - ❑ Các quy tắc bảo mật kết nối (Connection security rules)
 - ❑ Giám sát (Monitoring)
 - ❑ **Outbound traffic** (lưu lượng gửi đi) là lưu lượng truy cập được tạo ra từ máy chủ hướng tới internet
 - ❑ **Inbound traffic** theo hướng ngược lại

Windows Firewall with Advanced Security Console

The screenshot displays the Windows Firewall with Advanced Security console. The main window title is "Windows Firewall with Advanced Security". The left-hand navigation pane shows a tree view with the following items: Inbound Rules, Outbound Rules, Connection Security Rules, Monitoring, Firewall, Connection Security Rules, Security Associations, Main Mode, and Quick Mode. The main content area is titled "Windows Firewall with Advanced Security on localComputer" and shows the "Overview" tab for the "Domain Profile". A red rectangular box highlights the "Overview" section. The "Overview" section contains the following information:

- Domain Profile is Active**
 - 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 on.
 - Inbound connections that do not match a rule are blocked.
 - Outbound connections that do not match a rule are allowed.
- Public 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.

Below the overview, there is a link for "Windows Firewall Properties". The right-hand pane shows the "Actions" menu with the following options: Import Policy..., Export Policy..., Restore Default Policy, Diagnose / Repair, View, and Refresh. Below the actions, there is a "Properties" section with a "Help" link.

Các loại firewall profile

- ❖ Windows Server 2012 có ba loại firewall profile sau:
 - ❑ Domain: những lưu lượng mạng có thể phát hiện được bộ điều khiển miền (Domain control) và gia nhập vào miền.
 - ❑ Private: lưu lượng mạng đến và đi từ các server cục bộ hoặc mạng cục bộ
 - ❑ Public: lưu lượng mạng không phải từ mạng cục bộ (ví dụ mạng World Wide Web)

Cấu hình profile

- ❖ Khung State cấu hình các loại:
 - Firewall state
 - Inbound connections
 - Outbound connections
- ❖ Khung Settings bạn có thể cấu hình các thiết lập để điều khiển một số hành vi của tường lửa.
- ❖ Trong khung Logging bạn có thể cấu hình một số tùy

Các qui tắc bảo mật nổi kết

- ❖ Các thuộc tính của một qui tắc Firewall
 - Tạo một qui tắc Firewall
 - Demo: Tạo một qui tắc Firewall

Các thuộc tính của một qui tắc

- ❖ **Tab General**: cho phép bạn có thể thay đổi tên, mô tả, kích hoạt hoặc vô hiệu hóa và các Actions:
 - Allow the connections.
 - Allow only secure connections.
 - Block the connections.
- ❖ **Tab Programs and Services**: cho phép bạn có thể thay đổi chương trình hoặc dịch vụ trong qui tắc.
- ❖ **Tab Users and Computers**: cho phép bạn có thể cấu hình qui tắc để áp dụng cho người dùng nào đó hoặc máy tính cụ thể.

Các thuộc tính của một qui tắc

Firewall

- **Tab Protocols and Ports:** cho phép bạn có thể cấu hình loại giao thức và cổng cho qui tắc.
- ❖ **Tab Scope:** cho phép bạn có thể thiết lập địa chỉ IP nội bộ Local IP address và địa chỉ IP từ xa Remote IP address cho phạm vi qui tắc.
- ❖ **Tab Advanced:** cho phép bạn có thể thiết lập các profile và các loại kết nối (interface type) sẽ sử dụng trong firewall qui tắc này.

Tạo một qui tắc Firewall

- ❖ Rule Type: có thể cấu hình:
 - Program: cho phép kiểm soát truy cập vào và ra đối với một chương trình cụ thể.
 - Port: cho phép cấu hình qui tắc dựa trên số cổng TCP hoặc UDP.
 - Predefined.
 - Custom.
- ❖ Program: có thể cấu hình:
 - All programs.
 - The program path.
 - Services.

Tạo một qui tắc Firewall

- ❖ Protocol and Ports: có thể cấu hình:
 - Protocol type: thiết lập kiểu giao thức để áp dụng cho qui tắc này.
 - Protocol number.
 - Local Port: đây là cổng trên máy chủ mà qui tắc được sử dụng.
 - Remote port: đây là cổng trên máy tính khác.
 - Internet Control Message Protocol (ICMP) settings:
- ❖ Scope: bạn có thể thiết lập địa chỉ IP nội bộ và từ xa đến qui tắc áp dụng.

Tạo một qui tắc Firewall

- ❖ Action: có thể cấu hình:
 - Allow the connection: tạo qui tắc Allow.
 - Allow the connection if it is secure: cho phép kết nối nếu có một chính sách **IPSec** cho phép hai điểm endpoint thiết lập một kết nối an toàn.
 - Block the connection: tạo qui tắc Deny.
- ❖ Users and Computers: bạn có thể chọn người dùng hoặc máy tính có thể kết nối.
- ❖ Profile: thiết lập profile mà bạn muốn áp dụng cho qui tắc.

Tạo một qui tắc bảo mật nối kết

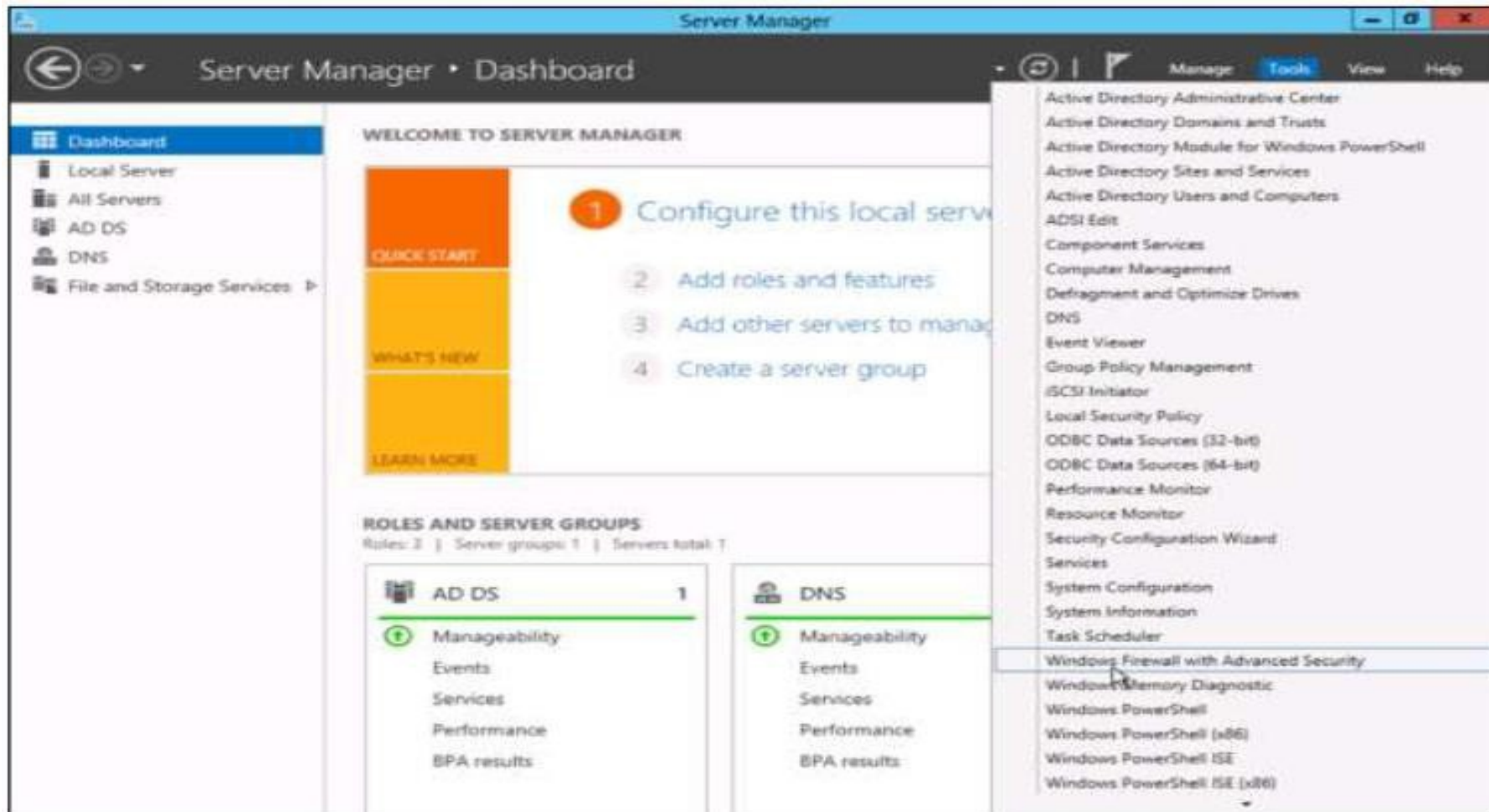
- ❖ **Rules Type:** chọn kiểu qui tắc bảo mật nối kết phù hợp.
- ❖ **Requirements:** xác định thời điểm muốn thực hiện thao tác xác thực.
- ❖ **Authentication Method:** chỉ định một phương pháp xác thực phù hợp.
- ❖ **Profile:** bạn chọn các profile phù hợp.
- ❖ **Name:** nhập tên của qui tắc bảo mật nối kết.

Giám sát Windows Firewall with Advanced Security.

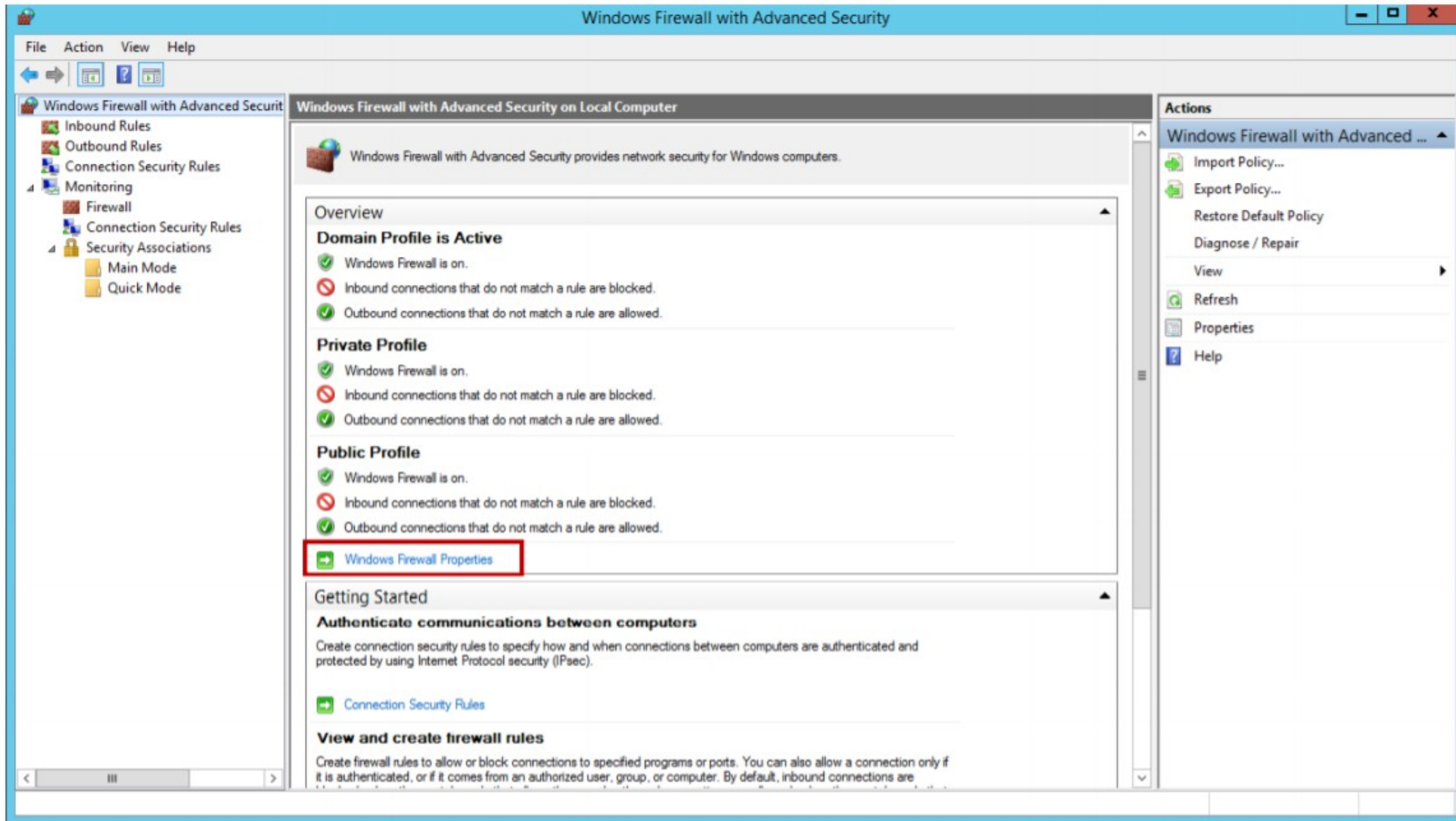
- ❖ Giám sát (Monitoring) là thành phần cho phép bạn theo dõi hoạt động của các quy tắc firewall và quy tắc bảo mật nối kết.
- ❖ Màn hình chính của Monitoring sẽ hiển thị thông tin chi tiết về các profile đang hoạt động.
- ❖ Còn nếu bạn chọn mục Connection Security Rules, danh sách các quy tắc bảo mật nối kết với thông tin chi tiết tương ứng sẽ xuất hiện.

Demo: Tạo một qui tắc bảo mật nối kết

- ❖ **Step 1:** Vào Server Manager -> click Tools và chọn Windows Firewall with Advanced Security.

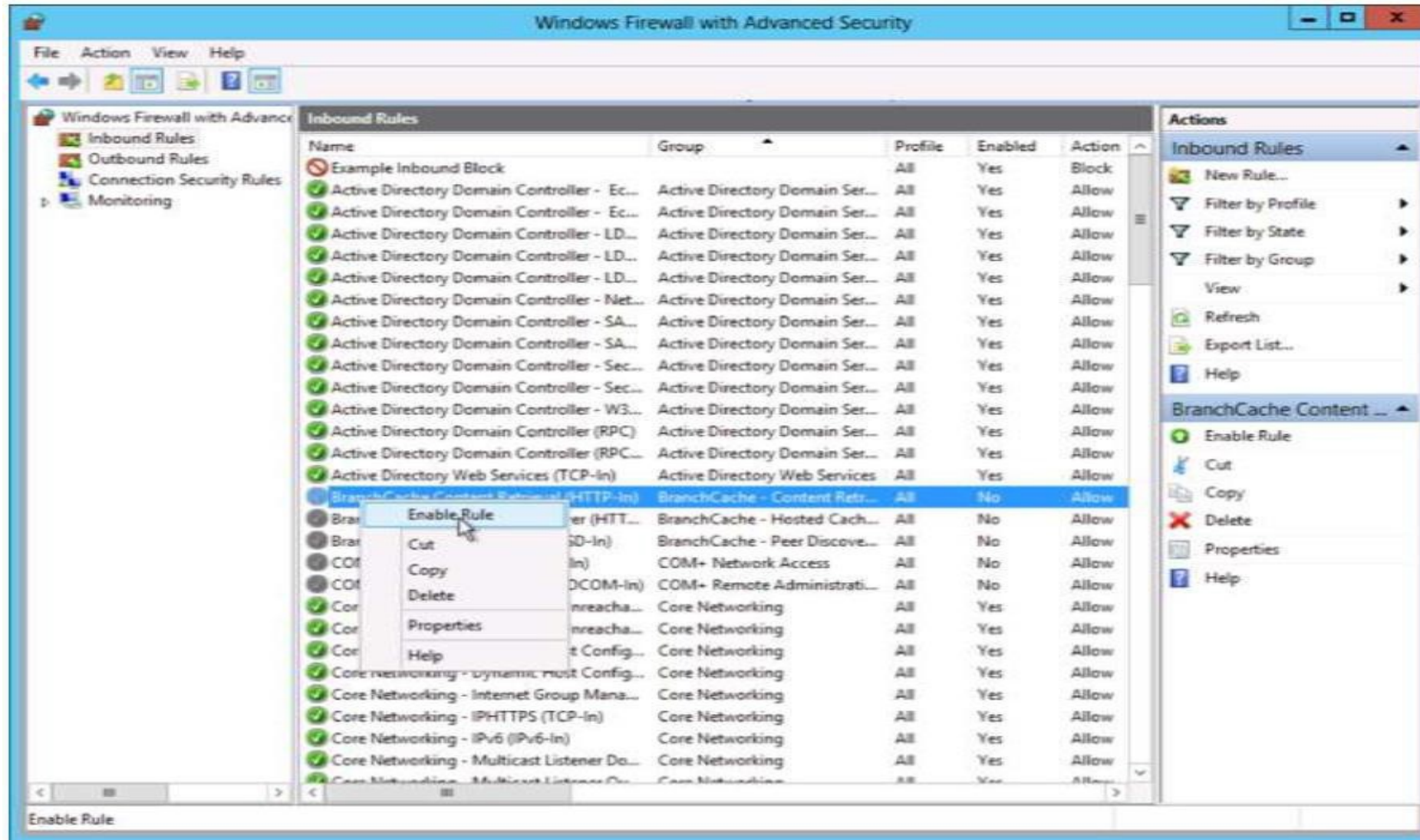


Demo: Tạo một qui tắc bảo mật nối kết



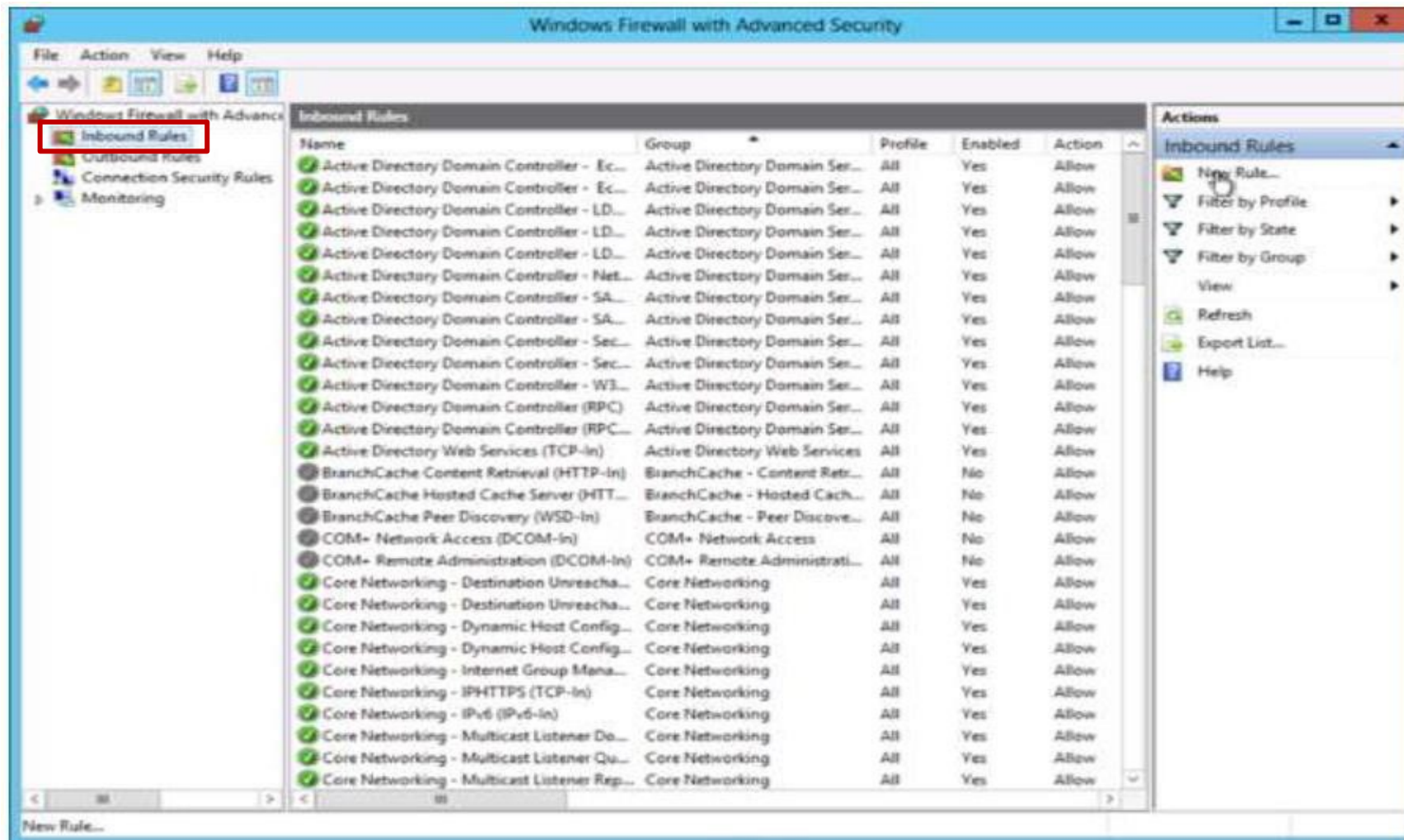
Demo: Tạo một qui tắc bảo mật nổi

❖ **kết** Right-clicking a rule will allow you toggle



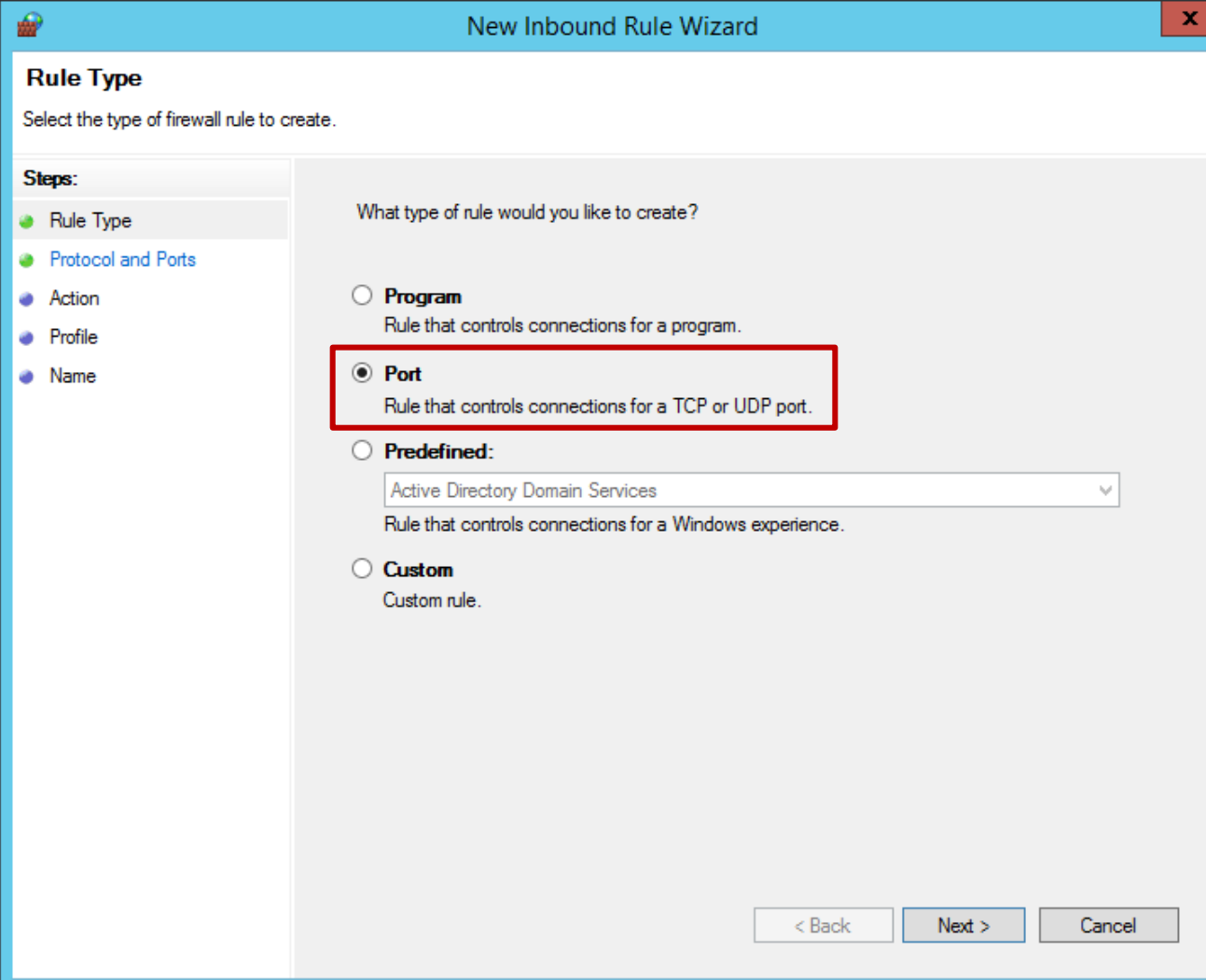
Demo: Tạo một qui tắc bảo mật nối

kết Step 1: Menu Inbound Rules /Outbound Rules – click “New Rule”.



Demo: Tạo một qui tắc bảo mật nổi

kết Step 2: chọn Port -> click
Next.



New Inbound Rule Wizard

Rule Type
Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- 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:
Active Directory Domain Services
Rule that controls connections for a Windows experience.

Custom
Custom rule.

< Back Next > Cancel

Demo: Tạo một qui tắc bảo mật nối kết

- ❖ **Step 3:** chọn TCP/UDP, điền Port cần mở (hoặc danh sách các Port) -> click Next

New Inbound Rule Wizard

Protocol and Ports
Specify the protocols and ports to which this rule applies.

Steps:

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

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:

80
Example: 80, 443, 5000-5010

< Back Next > Cancel

Mở Port Vượt Tường

❖ **Step 4: Chọn *Allow the connection* -> click Next**

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

< Back **Next >** Cancel

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

Step 5: chọn profiles cho rule -> click Next.

Demo: Tạo một qui tắc bảo mật nổi

kết Điền tên và mô tả của Rule -> click
Finish.

The screenshot shows a 'New Inbound Rule Wizard' window. On the left, a 'Steps' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name', with 'Name' selected. The main area has a 'Name' label above a text box containing 'Port 80'. Below it, a 'Description (optional):' label is above a text box containing 'Allow port 80 inbound on all connections'. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a blue border.

Bài Tập

- ❖ Tạo một qui tắc bảo mật nối kết cho các dịch vụ sau:
 - WWW (TCP: 80)
 - DNS (TCP:53, UDP: 53)
 - DHCP (UDP: 67, 68)
 - FTP (TCP: 20, 21)

Firewall allow APP FTP

Windows Firewall

Control Panel Home

Control Panel > System and Security > Windows Firewall

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Allow an app or feature through Windows Firewall

- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

Domain networks Connected

Networks at a workplace that are attached to a domain

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active domain networks: domain41.com

Notification state: Do not notify me when Windows Firewall blocks a new app

Private networks Not connected

Guest or public networks Not connected

See also

- Action Center
- Network and Sharing Center

Allowed apps

Control Panel > System and Security > Windows Firewall > Allowed apps

Search Control Panel

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate? [Change settings](#)

Allowed apps and features:

Name	Domain	Private	Public
<input type="checkbox"/> File and Printer Sharing over SMBDirect	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> File Replication	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> File Server Remote Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> FTP Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> iSCSI Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Kerberos Key Distribution Center	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Key Management Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> KMS Emulator Port	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> KMS Emulator: Service_KMS.exe	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Microsoft Key Distribution Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Netlogon Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Network Discovery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Details..](#) [Remove](#)

[Allow another app...](#)

[OK](#) [Cancel](#)

Firewall allow APP FTP

The screenshot displays the Windows Firewall with Advanced Security console. The 'Inbound Rules' list is visible, with three rules highlighted in a red box:

- FTP Server (FTP Traffic-In)
- FTP Server Passive (FTP Passive Traffic-In)
- FTP Server Secure (FTP SSL Traffic-In)

Name	Group	Profile	Enabled	Action	Override	P
DNS (UDP, Incoming)	DNS Service	All	Yes	Allow	No	%
RPC (TCP, Incoming)	DNS Service	All	Yes	Allow	No	%
RPC Endpoint Mapper (TCP, Incoming)	DNS Service	All	Yes	Allow	No	%
File and Printer Sharing (Echo Request - I...)	File and Printer Sharing	Public	Yes	Block	No	A
File and Printer Sharing (Echo Request - I...)	File and Printer Sharing	Domai...	No	Block	No	A
File and Printer Sharing (Echo Request - I...)	File and Printer Sharing	All	Yes	Allow	No	A
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Allow	No	%
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Allow	No	S
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Allow	No	S
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Allow	No	S
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Allow	No	S
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	All	Yes	Allow	No	%
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	All	Yes	Allow	No	A
File and Printer Sharing over SMBDirect (i...)	File and Printer Sharing over...	All	No	Allow	No	S
File Replication (RPC)	File Replication	All	Yes	Allow	No	%
File Replication (RPC-EPMAP)	File Replication	All	Yes	Allow	No	%
File Server Remote Management (DCOM...)	File Server Remote Manage...	All	Yes	Allow	No	%
File Server Remote Management (SMB-In)	File Server Remote Manage...	All	Yes	Allow	No	S
File Server Remote Management (WMI-In)	File Server Remote Manage...	All	Yes	Allow	No	%
FTP Server (FTP Traffic-In)	FTP Server	All	Yes	Allow	No	%
FTP Server Passive (FTP Passive Traffic-In)	FTP Server	All	Yes	Allow	No	C
FTP Server Secure (FTP SSL Traffic-In)	FTP Server	All	Yes	Allow	No	%
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow	No	%
Kerberos Key Distribution Center - PCR (...)	Kerberos Key Distribution C...	All	Yes	Allow	No	%
Kerberos Key Distribution Center - PCR (...)	Kerberos Key Distribution C...	All	Yes	Allow	No	%
Kerberos Key Distribution Center (TCP-In)	Kerberos Key Distribution C...	All	Yes	Allow	No	%
Kerberos Key Distribution Center (UDP-In)	Kerberos Key Distribution C...	All	Yes	Allow	No	%
Key Management Service (TCP-In)	Key Management Service	All	No	Allow	No	%
Microsoft Key Distribution Service	Microsoft Key Distribution S...	All	Yes	Allow	No	%
Microsoft Key Distribution Service	Microsoft Key Distribution S...	All	Yes	Allow	No	%
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow	No	S
Netlogon Service Authz (RPC)	Netlogon Service	All	No	Allow	No	%
Network Discovery (LLMNR-UDP-In)	Network Discovery	All	Yes	Allow	No	%

Firewall allow APP FTP

Windows Firewall with Advanced Security

File Action View Help

Windows Firewall with Advanced Security on Local Com

- Inbound Rules
- Outbound Rules**
- Connection Security Rules
- Monitoring
 - Firewall
 - Connection Security Rules
- Security Associations
 - Main Mode
 - Quick Mode

Name	Group	Profile	Enabled	Action	Override	P
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow	No	A
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow	No	A
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow	No	A
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow	No	A
Core Networking - Teredo (UDP-Out)	Core Networking	All	Yes	Allow	No	%
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow	No	A
DHCP Server Failover (TCP-Out)	DHCP Server Management	All	Yes	Allow	No	%
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	All	No	Allow	No	%
All Outgoing (TCP)	DNS Service	All	Yes	Allow	No	%
All Outgoing (UDP)	DNS Service	All	Yes	Allow	No	%
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domai...	No	Block	No	A
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Public	Yes	Block	No	A
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Allow	No	A
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	All	Yes	Allow	No	%
File and Printer Sharing (NB-Datagram-O...	File and Printer Sharing	All	Yes	Allow	No	S
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	All	Yes	Allow	No	S
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	All	Yes	Allow	No	S
File and Printer Sharing (SMB-Out)	File and Printer Sharing	All	Yes	Allow	No	S
FTP Server (FTP Traffic-Out)	FTP Server	All	Yes	Allow	No	%
FTP Server Secure (FTP SSL Traffic-Out)	FTP Server	All	Yes	Allow	No	%
iSCSI Service (TCP-Out)	iSCSI Service	All	No	Allow	No	%
Network Discovery (LLMNR-UDP-Out)	Network Discovery	All	Yes	Allow	No	%
Network Discovery (NB-Datagram-Out)	Network Discovery	All	Yes	Allow	No	S
Network Discovery (NB-Name-Out)	Network Discovery	All	Yes	Allow	No	S
Network Discovery (Pub WSD-Out)	Network Discovery	All	Yes	Allow	No	%
Network Discovery (SSDP-Out)	Network Discovery	All	Yes	Allow	No	%
Network Discovery (UPnPHost-Out)	Network Discovery	All	Yes	Allow	No	%
Network Discovery (UPnP-Out)	Network Discovery	All	Yes	Allow	No	S
Network Discovery (WSD Events-Out)	Network Discovery	All	Yes	Allow	No	S
Network Discovery (WSD EventsSecure-O...	Network Discovery	All	Yes	Allow	No	S
Network Discovery (WSD-Out)	Network Discovery	All	Yes	Allow	No	%
Routing and Remote Access (GRE-Out)	Routing and Remote Access	All	No	Allow	No	S
Routing and Remote Access (L2TP-Out)	Routing and Remote Access	All	No	Allow	No	S

Actions

- Outbound Rules
 - New Rule...
 - Filter by Profile
 - Filter by State
 - Filter by Group
 - View
 - Refresh
 - Export List...
 - Help
- FTP Server Secure (FTP SSL Traffic-Out)**
 - Disable Rule
 - Cut
 - Copy
 - Delete
 - Properties
 - Help