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 qui tắc Firewall.
- 4. Các qui 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 lai được như sau:
 - Úng dụng mạng quét các cổng không có bảo vệ, để kẻ tấn
 công
 - có thể sử dụng để truy cập vào hệ thống.
 - Úng 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 đươc tạo ra từ máy chủ hướng tới internet □ Inbound traffic theo hƯớng ngược lại

Windows Firewall with Advanced Security Console

@	Windows Firewall with Advanced Security	
File Action View Help 	Windows Firewall with Advanced Security Vindows Firewall with Advanced Security on localComputer Windows Rrewall with Advanced Security provides network security for Windows computers . Overview Domain Profile is Active Image: Windows Rrewall is on. Image: Inbound connections that do not match a rule are blocked . Image: Private Profile Image: Windows Rrewall is on. Image: Ima	Actions <u>Windows Firewa II wi th</u> <u>Advanced •</u> f!! Intrapolicy Diagnose / Repa ir View Refresh O Properties Kalo
	 Windows Rrewall 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 Rrewall is on. Inbound connections that do not match a rule are blocked . Outbound connections that do not match a rule are blocked . Outbound connections that do not match a rule are blocked . Outbound connections that do not match a rule are blocked . Outbound connections that do not match a rule are blocked . Outbound connections that do not match a rule are allowed . CJ windows Rrewall 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). CJ Connection Security Rules 	Properties 6 Help
>	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 .is_ut_enl_cate?.or if	,

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: Iưu lượng mạng không phải từ mạng cục bộ (ví dụ mạng World Wide Web)

Cấu hình profile

- * Khung State cấu hình các loại:
 - \cdot \Box Firewall state
 - \cdot \Box Inbound connections
 - $\cdot \Box$ 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

11

Các qui tắc bảo mật nối 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

- **Firewall** 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

- **Firewal** rotocols 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 qui tắc firewall và qui 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 qui 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.

		Serv	er Manager	- 0 ×
€ Server Ma	anager • Dashboa	ird		C Manage Took View Help
Dashboard	WELCOME TO SERVER M	ANAGER		Active Directory Domains and Trusts Active Directory Module for Windows PowerShell
Local Server All Servers All Servers AD DS DNS File and Storage Services	CLICCESTANT WHAT'S NEW	2 Add 3 Add 4 Cre	gure this local serve d roles and features d other servers to manag ate a server group	Active Directory Sites and Services Active Directory Users and Computers ADSI Edit Component Services Computer Management Defragment and Optimice Drives DNS Event Viewer Group Policy Management (SCSI Initiator Local Security Policy ODBC Data Sources (S2-bit) ODBC Data Sources (64-bit) Performance Monitor
	ROLES AND SERVER GRO Roles 3 Server groups 1	Gervers total	T	Resource Monitor Security Configuration Wizard Services
	AD DS	1	A DNS	System Configuration System Information
	Manageability Events Services Performance BPA results		Manageability Events Services Performance BPA results	Task Scheduler Windows Firewall with Advanced Security Windows PowerShell Windows PowerShell (x86) Windows PowerShell (x86) Windows PowerShell (x86)

Demo: Tạo một qui tắc bảo mật nối kết

*	Windows Firewall with Advanced Security		_ D X
File Action View Help			
Windows Firewall with Advanced Securi	Windows Firewall with Advanced Security on Local Computer		Actions
 Inbound Rules Outbound Rules Connection Security Rules Monitoring 	Windows Firewall with Advanced Security provides network security for Windows computers.	^	Windows Firewall with Advanced Windows Firewall with Advanced Key Structure Policy Key Structure Policy
Firewall	Overview	•	Restore Default Policy
A Gecurity Associations	Domain Profile is Active		Diagnose / Repair
Main Mode	Windows Firewall is on.		View
Quick Mode	V Inbound connections that do not match a rule are blocked.		Refresh
	Outbound connections that do not match a rule are allowed.		Properties
	Private Profile Image: Windows Firewall is on. Image: Inbound connections that do not match a rule are blocked. Image: Outbound connections that do not match a rule are allowed.	=	7 Help
	Public Profile Image: Windows Firewall is on. Image: Inbound connections that do not match a rule are blocked. Image: Outbound connections that do not match a rule are allowed. Image: 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		
2 Jun 19	View and create tirewall 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 authenticated user group, or come too. Buildon it is buildon and connection only if		

Demo: Tạo một qui tắc bảo mật nối

* **Ref**ght-clicking a rule will allow you toggle

Windows Firewall with Advanced Security									100
File Action View Help									
- 🔶 🙇 🔟 🕞 🛃 🗔									
Windows Firewall with Advance	Inbound I	Rules					10	Actions	
1 Inbound Rules	Name			Group	Denfile	Enabled	Action 0	Johnund Dular	
Cutbound Rules	S Example Inbound Block				48	Yes	Block	moound rules	_
Connection Security Rules	Active	Directory Domain Co	ontroller - Ec	Active Directory Domain Ser	All	Yes	Allow	New Rule	
p 🍯 Monitoring	Active	Directory Domain Co	ontroller - Ec.	Active Directory Domain Ser.	All	Yes	Allow	Y Filter by Profile	
	Active	Directory Domain Co	ontroller - LD	Active Directory Domain Ser.	All	Yes	Allow	Y Filter by State	
	Active	Directory Domain Co	ontroller - LD	Active Directory Domain Ser	All	Yes	Allow	V Elter by Group	
	Active Directory Domain Controller - LD			Active Directory Domain Ser	All	Yes	Allow	Y The by Group	
	 Active Directory Domain Controller - Net Active Directory Domain Controller - Net Active Directory Domain Controller - SA Active Directory Domain Controller - SA Active Directory Domain Controller - Sec Active Directory Domain Controller - Sec Active Directory Domain Controller - Sec Active Directory Domain Controller - W3 Active Directory Domain Controller (RPC) Active Directory Domain Controller (RPC) 			Active Directory Domain Ser	All	Yes	Allow	View	
				Active Directory Domain Ser	AL	Yes	Allow	Refresh	
				Active Directory Domain Ser	All	Yes	Allow	Expect List	
				Active Directory Domain Ser	All	Yes	Allow		
				Active Directory Domain Ser.	All	Yes	Allow	Help	
				Active Directory Domain Ser	All	Yes	Allow	BranchCache Conte	at.
				Active Directory Domain Ser	All	Yes	Allow	O Enable Rule	
				Active Directory Domain Ser	All	Yes	Allow		
	Active	Directory Web Service	es (TCP-in)	Active Directory Web Services	All	Yes	Allow	Cut Copy	
	Geratut	Carlin Comment Bar	and (HTTP-In)	BranchCache - Content Retr	(48)	No	Allow		
	Brai	Enable Rule	er (HTT_	BranchCache - Hosted Cach	All	No	Allow	X Delete	
	Brat	Cut ht	(nl-Qi	BranchCache - Peer Discove	AL	No	Allow	Descention	
	CO1	Com	(In)	COM+ Network Access	All	No	Allow	Properors	
	CO1	Copy	DCOM-In)	COM+ Remote Administrati	AE	No	Allow	Help	
	Cor	Delete	nreacha	Core Networking	All	Yes	Allow		
	Cor	Properties	nreacha	Core Networking	All	Yes	Allow		
	Cor Cor	Help	t Config	Core Networking	All	Yes	Allow		
	Corers	etworking - oynemi	must Config	Core Networking	All	Yes	Allow		
	Core N	letworking - Internet	Group Mana	Core Networking	All	Yes	Allow		
	Core N	letworking - IPHTTPS	S (TCP-In)	Core Networking	All	Yes	Allow		
	Core N	letworking - IPv6 (IPv	(6-lm)	Core Networking	All	Yes	Allow		
	Core N	letworking - Multicas	t Listener Do_	Core Networking	All	Yes	Allow		
	Re Cambi	in the second	+ Listener Per	Cam Maturahian		Ver	Aller		

Inbound Rules: Printer Sharing (Echo Request-ICMPv4-In)

@		Windows Fir	ewall with Adva	nced Security				_ D X		
File Action View Help										
🗢 🔿 🛃 🗟 🖬										
P Windows Firewall with Advanced Security on Local Co	Inbound Rules							Actions		
🔣 Inbound Rules	Name			Group	Profile	Enabled		Inbound Rules		
Cutbound Rules	File and Drin	ter Sharing (Echo Reg	File and Printer Sharing	All	No		Mary Pulo			
Connection Security Rules	🕜 File ar	Enable Rule	uest - ICMPv6-In)	od Printer Sharing	All	Yes		New Rule		
Monitoring	🕜 File ar	Cut	DP-In)		A.1	Yes		🐨 Filter by Profile 🔹 🕨		
	🕑 File ar	Conv	ram-In)	Dight click >		Yes		🛛 🍸 Filter by State 🛛 🕨		
	🕑 File ar	Delete	-ln) n-ln)			Yes		🕎 Filter by Group		
	🕜 File ar 🚽	Delete		chon		Yes		Viau		
	🕜 File ar	Properties		CHŲH		Yes				
	🕑 File ar	Help	ervice - RPC)			Yes		Refresh		
	🕑 File and Prin	iter snanng (spooler s	ervice - RPC-EPMA	P) Flee and Global det sharing I C	All	Yes		📑 Export List		
	File and Prin	iter Sharing over SMBI	Direct (iWARP-In)	File and Printer Sharing over	All	No		12 Help		
	🕢 File Replicati	ion (RPC)		File Replication	All	Yes				
	File Replication (RPC-EPMAP)			File Replication	All	Yes		File and Printer Sharin 🔺		
	V File Server Re	emote Management (File Server Remote Manage	All	Yes		O Enable Rule			
	🕜 File Server Remote Management (SMB-In)			File Server Remote Manage	All	Yes		K Cut		
	🛛 🕑 File Server Re	emote Management (WMI-In)	File Server Remote Manage	All	Yes				
	FTP Server (F	FTP Traffic-In)		FTP Server	All	Yes	≡	Copy		
	FTP Server P	assive (FTP Passive Tr	affic-In)	FTP Server	All	Yes		🔀 Delete		
	FTP Server Se	ecure (FTP SSL Traffic	-ln)	FTP Server	All	Yes		Properties		
	SCSI Service	: (TCP-In)		iSCSI Service	All	No				
	🛛 🥑 Kerberos Key	y Distribution Center -	PCR (TCP-In)	Kerberos Key Distribution C	All	Yes		И нер		
	🛛 🥑 Kerberos Key	y Distribution Center -	PCR (UDP-In)	Kerberos Key Distribution C	All	Yes		4 7		
	🛛 🥑 Kerberos Key	y Distribution Center (TCP-In)	Kerberos Key Distribution C	All	Yes		1 7		
	🛛 🥑 Kerberos Key	y Distribution Center ((UDP-In)	Kerberos Key Distribution C	All	Yes		4 7		
	🖉 Key Manage	ment Service (TCP-In))	Key Management Service	All	No		1 7		
	🛛 🔮 Microsoft Ke	ey Distribution Service	£	Microsoft Key Distribution S	All	Yes		1 7		
	🛛 🔮 Microsoft Ke	ey Distribution Service	£	Microsoft Key Distribution S	All	Yes		1		
	🖉 Netlogon Se	rvice (NP-In)		Netlogon Service	All	No		1 7		
	🖉 🔘 Netlogon Se	rvice Authz (RPC)		Netlogon Service	All	No		1		
	🛛 🕑 Network Dis	covery (LLMNR-UDP-	ln)	Network Discovery	All	Yes		1		
	🛛 🥑 Network Dis	covery (NB-Datagram	ı-In)	Network Discovery	All	Yes		1		
	🛛 🥑 Network Dis	covery (NB-Name-In)	ł.	Network Discovery	All	Yes		1 7		
	🛛 🕑 Network Dis	covery (Pub-WSD-In)		Network Discovery	All	Yes	\sim	(
< III >	<	Ш				2	>			

Demo: Tạo một qui tắc bảo mật nối

kếttep 1: Menu Inbound Rules /Outbound Rules – click "New Rule".

2	Windows Fit	rewall with Advanced Secu	inty				- 0	×
File Action View Help								
🕈 🔹 📰 📑 🖬 📷								
Windows Firewall with Advance	Indexend Roles						Actions	_
inbound Rules	Name	Group *	Picfile	Enabled	Action	~	Inbound Rules	
Cutbound Rules	Active Directory Domain Controller - Ec	Active Directory Domain Ser_	All	Yes	Allow		ET New Pole	
Connection Security Rules	Active Directory Domain Controller - Ec	Active Directory Domain Ser_	All	Yes	Allow		and when	
Monitoring	Active Directory Domain Controller - LD	Active Directory Domain Ser	All	Yes	Allow		V Fitter by Profile	
	Active Directory Domain Controller - LD	Active Directory Domain Ser_	AB.	Yes	Allow		Y Filter by State	
	Q Active Directory Domain Controller - LD	Active Directory Domain Ser_	AB	Ves	Allow		Y Filter by Group	
	Active Directory Domain Controller - Net	Active Directory Domain Ser	AB	Yes	Allow			
	Active Directory Domain Controllier - SA.	Active Directory Domain Ser	All	Ves	Allow	Π	Siew	
	Active Directory Domain Controller - SA	Active Directory Domain Ser	AB	Yes	Allow		C Refresh	
	Active Directory Domain Controller - Sec.	Active Directory Domain Ser_	BA	Ves	Allew		Export List-	
	Active Directory Domain Controller - Sec	Active Directory Domain Ser_	All	Ves	Allow		E Hote	
	Q Active Directory Domain Controller - W3	Active Directory Domain Ser_	All	Ves.	Allow		La riep	
	Active Directory Domain Controller (RPC)	Active Directory Domain Ser	All	Ves	Allow			
	Active Directory Domain Controller (RPC	Active Directory Domain Ser	AB	Yes	Allow			
	Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Ves	Allow			
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	Nio	Allow			
	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No	Allow			
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	Allow			
	COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow			
	COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati	AN	No	Allow			
	Core Networking - Destination Unreacha	Core Networking	AB	Ves	Allow			
	O Core Networking - Destination Unreacha	Core Networking	All	Ves	Allow			
	Core Networking - Dynamic Host Config.	Core Networking	4.8	Ves	Allow			
	Core Networking - Dynamic Host Config.	Core Networking	AB	Ves.	Allow			
	Core Networking - Internet Group Mana_	Core Networking	All	Yes	Allow			
	Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Ves	ABow			
	Core Networking - IPv6 (IPv6-In)	Core Networking	AB	Ves	Allow			
	Core Networking - Multicast Listener Do-	Core Networking	All	Ves	ABow			
	Core Networking - Multicast Listener Du	Core Networking	All	Ves	ABpw			
	Core Networking - Multicest Listener Rep.	Core Networking	Ait	Ves	Allew	9		
	< III				2			

New Rule

Demo: Tạo một qui tắc bảo mật nối

kếttep 2: chọn Port -> click

Next.

@	New Inbound Rule Wizard
Rule Type Select the type of firewall rule to creat	te.
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. Pot Rule that controls connections for a TCP or UDP pot. Predefined: Active Directory Domain Services Rule that controls connections for a Windows experience. Custom Custom rule.

Demo: Tạo một qui tắc bảo mật nối kết

* Step 3: chọnTCP/UDP, điền Port cần mở (hoặc danh sách các Port) -> click Next______

<i>[•]</i>	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 	 Does this rule apply to TCP or UDP? TCP UDP 	Mở Port
 Name 	Does this rule apply to all local ports or specific local ports? All local ports Specific local ports: 80 Example: 80, 443, 5000-5010 All local ports 80 Example: 80, 443, 5000-5010 80 80 80 80 80 80 80 80 <	Cancel

*

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

< Back

Next >

Cancel

What action should be taken when a connection matches the specified conditions?

Allow the connection

Nort

This includes connections that are protected with IPsec as well as those are not

O 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 ...

O Block the connection

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.

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

< Back

Next >

Cancel

Demo: Tạo một qui tắc bảo mật nối

kếtiền tên và mô tả của Rule -> click

Finish.

2	New Inbound Rule Wizard	x
Name Specify the name and description o	of this rule.	
Steps:		
Rule TypeProtocol and PortsAction		
Profile	Name:	
Name	For ou	
	Description (optional): Allow pot 80 inbound on all connections < Back Finish Cance	4

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)
 - **G** FTP (TCP: 20, 21)

Firewall allow APP FTP

2		Windows Firewall		¥	Allowed apps				Ŀ	- 0 X
🕞 🏵 🔹 🕆 🔮 🖌 Control P	anel 🔸 System and Security 🔸 Windows F	irewall	v Č	€ 💿 ▼ ↑ 🔐 + Control Panel + Syste	m and Security + Windows Firewall + Allowed apps			۷ (5 Search Control Panel	٩,
Control Panel Home Allow an app or feature through Windows Firewall	Help protect your PC with Wir Windows Firewall can help prevent hack Internet or a network.	ndows Firewall kers or malicious software from gaining access to your PC through the			Allow apps to communicate through Windows Fire To add, change, or remove allowed apps and ports, click Change s What are the risks of allowing an app to communicate?	wall ettings.	😚 Change setti	ings		
💡 Change notification settings	🔮 Domain networks	Opmain 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: Immain domain41.com Netification state: Do not notify me when Windows Firewall blocks a			Allowed apps and features:					
 Turn Windows Firewall on or off Restore defaults Advanced settings Troubleshoot my network N 	Networks at a workplace that are attac Windows Firewall state: Incoming connections: Active domain networks: Notification state:				Name □ File and Printer Sharing over SMBDirect ☑ File Replication ☑ File Server Remote Management ☑ FTP Server □ iSCSI Service ☑ Kerberos Key Distribution Center □ Key Management Service ☑ KMS Emulator Part	Private Public				
	Implementation state Implementation state	Not connected $③$			 MMS Emulator Port MMS Emulator: Service_KMS.exe Microsoft Key Distribution Service Netlogon Service Network Discovery 	Detr	I V V V V V V Allow another ap	v Ive pp		

See also Action Center Network and Sharing Center

Cancel

OK

Firewall allow APP FTP

Windows Firewall with Advanced Security									_ 🗆 X
File Action View Help									11.11
← ⇒ 2 🖬 🗟 🖬									
P Windows Firewall with Advanced Security on Local Com	Inbound Rules							Actions	
🗱 Inbound Rules	Name	Group	Profile	Enabled	Action	Override	P ^	Inbound Rules	-
Cutbound Rules	ONS (UDP, Incoming)	DNS Service	All	Yes	Allow	No	%	Man New Pule	
Connection Security Rules	@ RPC (TCP, Incoming)	DNS Service	All	Yes	Allow	No	91		
A Monitoring	RPC Endpoint Mapper (TCP, Incoming)	DNS Service	All	Yes	Allow	No	%	Filter by Profile	•
Connection Security Rules	SFile and Printer Sharing (Echo Request - I	File and Printer Sharing	Public	Yes	Block	No	A	Filter by State	•
A Security Associations	SFile and Printer Sharing (Echo Request - I	File and Printer Sharing	Domai	No	Block	No	A	Filter by Group	,
Main Mode	SFile and Printer Sharing (Echo Request - I	File and Printer Sharing	All	Yes	Allow	No	A	View	
Quick Mode	G File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Allow	No	%	VIEW	
	File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Allow	No	S	C Refresh	
	G File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Allow	No	S	Export List	
	G File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Allow	No	S	Help	
	File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Allow	No	S		
	General 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		
	Sile Replication (RPC)	File Replication	All	Yes	Allow	No	%		
	Sile Replication (RPC-EPMAP)	File Replication	All	Yes	Allow	No	%≡		
	G File Server Remote Management (DCOM	File Server Remote Manage	All	Yes	Allow	No	%		
	G 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	92		
	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		
	SFTP Server Secure (FTP SSL Traffic-In)	FTP Server	All	Yes	Allow	No	%		
	USCSI Service (TCP-In)	ISCSI Service	All	No	Allow	No	2		
	Werberos Key Distribution Center - PCR (Kerberos Key Distribution C	All	Yes	Allow	No	%		
	W 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	%		
	W Kerberos Key Distribution Center (UDP-In)	Kerberos Key Distribution C	All	Ves	Allow	No	%		
	Key Management Service (TCP-In)	Key Management Service	All	No	Allow	No	91		
	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		
	Wetlogon Service Authz (RPC)	Netlogon Service	All	No	Allow	No	%		
	Whetwork Discovery (LLMNR-UDP-In)	Network Discovery	All	Yes	Allow	No	%~		
< III >	< III						>]]	

Firewall allow APP FTP

· 🖌	Wi	indows Firewall with Adva	nced Sec	urity					
File Action View Help									
(+ +) (2 (C) (+) (2 (C) (+) (-) (-) (-) (-) (-) (-) (-) (-) (-) (-									_
Windows Firewall with Advanced Security on Local Com	Outbound Rules							Actions	-
Inbound Rules	Name	Group	Profile	Enabled	Action	Override	P ^	Outhound Rules	
Cutbound Rules	Ocore Networking - Packet Too Big (ICMP	Core Networking	All	Yes	Allow	No	A	Man New Puls	
Connection Security Rules	Ocore Networking - Parameter Problem (I	Core Networking	All	Yes	Allow	No	A	New Rule	
A Monitoring	Core Networking - Router Advertisement	Core Networking	All	Yes	Allow	No	A	Filter by Profile	٠
Firewall	Core Networking - Router Solicitation (IC	Core Networking	All	Yes	Allow	No	A	Tilter by State	٠
A Security Associations	Core Networking - Teredo (UDP-Out)	Core Networking	All	Yes	Allow	No	%	Y Filter by Group	
Main Mode	Core Networking - Time Exceeded (ICMP	Core Networking	All	Yes	Allow	No	A		-
Quick Mode	ODHCP Server Failover (TCP-Out)	DHCP Server Management	All	Yes	Allow	No	%	View	•
	Distributed Transaction Coordinator (TC	Distributed Transaction Coo	All	No	Allow	No	%	G Refresh	
	All Outgoing (TCP)	DNS Service	All	Yes	Allow	No	%	Export List	
	All Outgoing (UDP)	DNS Service	All	Yes	Allow	No	%	17 Help	
	SFile and Printer Sharing (Echo Request - I	File and Printer Sharing	Domai	No	Block	No	A	II Help	_
	SFile and Printer Sharing (Echo Request - I	File and Printer Sharing	Public	Yes	Block	No	A	FTP Server Secure (FTP SSL Traffic-Out)	-
	SFile and Printer Sharing (Echo Request - I	File and Printer Sharing	All	Yes	Allow	No	A	Disable Rule	_
	Sile and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	All	Yes	Allow	No	%	Ken	
	File and Printer Sharing (NB-Datagram-O	File and Printer Sharing	All	Yes	Allow	No	S	a Cut	
	SFile and Printer Sharing (NB-Name-Out)	File and Printer Sharing	All	Yes	Allow	No	S	Сору	
	SFile and Printer Sharing (NB-Session-Out)	File and Printer Sharing	All	Yes	Allow	No	S	🔀 Delete	
	File and Printer Sharing (SMB-Out)	File and Printer Sharing	All	Yes	Allow	No	S.	Bronatian	
	SFTP Server (FTP Traffic-Out)	FTP Server	All	Yes	Allow	No	%	Fioperues	
	FTP Server Secure (FTP SSL Traffic-Out)	FTP Server	All	Yes	Allow	No	× .	I Help	
	SCSI 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		
	Wetwork Discovery (NB-Name-Out)	Network Discovery	All	Yes	Allow	No	S		
	Wetwork Discovery (Pub WSD-Out)	Network Discovery	All	Yes	Allow	No	%		
	Wetwork Discovery (SSDP-Out)	Network Discovery	All	Yes	Allow	No	%		
	Wetwork Discovery (UPnPHost-Out)	Network Discovery	All	Yes	Allow	No	%		
	W 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		
	Wetwork Discovery (WSD-Out)	Network Discovery	All	Yes	Allow	No	%		
	Routing and Remote Access (GRE-Out)	Kouting and Remote Access	All	No	Allow	No	5		
	Routing and Remote Access (L2TP-Out)	Routing and Remote Access	All	No	Allow	No	S v		
< III >	< III						>	J	_

32