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 lại 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 được
  - tạo ra từ máy chủ hướng tới internet
  - □ Inbound traffic theo hướng ngược lại

#### Windows Firewall with Advanced Security Console

<b>@</b>	Windows Firewall with Advanced Security	
File Action View Help		
←	Vindows Eirowall with Advanced Security on Jacal Computer	Actions
inbound Rules		
Outbound Rules		Windows Firewall with Advanced •
Connection Security Rules	Windows Rrewall with Advanced Security provides network security for Windows computers.	Import Policy
🛛 🖉 Monitoring		f!  Export Policy
• Firewall	Overview	Restore Default Policy
Connection Security Rules	Domain Profile is Active	Diagnose / Repair
Main Made	W ndows Rrewall is on.	View
QuickMode	No. hound connectors that do not match a rule are blocked.	View
Quotinouo	Outbound connections that do not match a rule are allowed	Refresh
		0
	Private Profile	Properties
	🧭 Windows Rrewall is on.	
	Nound connectors that do not match a rule are blocked.	0 Help
	Outbound connections that do not match a rule are allowed.	
	Public Profile	
	Windows Rrewall is on.	
	S hbound connecbns 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 riles to specify how and when connections between computers are authenticated and	
	protected by using hternet Protocol security (IPsec).	
	CJ Connection Security Rules	
	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 om es tro,man auth rized usg up. r computer. By def u .in.bo nd c? "necti? s are	v
	·	

### 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 chọn
  - cho việc ghi vết của Windows Firewall.

# 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

- 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.
- Name: bạn có thể nhập tên qui tắc và thông tin chú thích.

- \* 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.

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

		Serve	er Manager	- 0 ×
Server Ma	anager • Dashboard	i	-	()   Manage Tools View Help
III Dashboard	WELCOME TO SERVER MAN	AGER		Active Directory Domains and Trusts Active Directory Module for Windows PowerShell
Local Server  All Servers  AD DS  DNS  File and Storage Services	CLARCE STANT	Config 2 Add 3 Add 4 Crea	gure this local serve roles and features other servers to manag ite a server group	Active Directory Sites and Services Active Directory Users and Computers ADSI Edit Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management ISCSI Initiator Local Security Policy ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor
	ROLES AND SERVER GROUP Roles: 3   Server groups: 1   Se	<b>IS</b> mvers totak 7		Resource Monitor Security Configuration Wizard
	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 (58)

<b>2</b>	Windows Firewall with Advanced Security		_ <b>_</b> X
File Action View Help			
Windows Firewall with Advanced Security Income Advanced Security	Windows Firewall with Advanced Security on Local Computer		Actions
Connection Security Rules	Windows Firewall with Advanced Security provides network security for Windows computers.	^	Windows Firewall with Advanced  Import Policy Export Policy
I Firewall	Overview	•	Restore Default Policy
Connection Security Rules	Domain Profile is Active		Diagnose / Repair
Main Mode	Windows Firewall is on.		View
🔜 Quick Mode	S Inbound connections that do not match a rule are blocked.		Q Refresh
	Outbound connections that do not match a rule are allowed.		Properties
	Private Profile		Help
	Windows Firewall is on.	=	_
	Outbound connections that do not match a rule are allowed.		
	Public Profile		
	Windows Firewall is on.		
	S Inbound connections that do not match a rule are blocked.		
	Outbound connections that do not match a rule are allowed.		
	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		
	View and create firewall rules		
< III >	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 authorized user, group, or computer. By default, inbound connections are	~	

Right-clicking a rule will allow you toggle enable/disable.

			Windows Fin	ewall with Advanced S	ecurity				100
File Action View Help									
2 📅 🔒 🖬 📷									
Windows Firewall with Advance	Inbound F	Rules						Actions	-
🗱 Inbound Rules	Name			Group	Profile	Enabled	Action ^	Inhound Rules	
Cutbound Rules	SExample Inbound Block				All	Yes	Block	Mar New Pole	
Connection Security Rules	Active Directory Domain Controller - Ec			Active Directory Domain S	er All	Yes	Allow	TAEN RUIE	
Monitoring	Active	Directory Domain Co	ontroller - Ec	Active Directory Domain S	er All	Yes	Allow -	Filter by Profile	
	Active	Directory Domain Co	ontroller - LD	Active Directory Domain S	er All	Yes	Allow	Y Filter by State	
	Active Directory Domain Controller - LD			Active Directory Domain S	er All	Yes	Allow	Filter by Group	
				Active Directory Domain S	er All	Yes	Allow		
	Active	Directory Domain Co	ontroller - Net	Active Directory Domain Se	er All	Yes	Allow	View	
	Active Directory Domain Controller - SA.,     Active Directory Domain Controller - SA.,     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 Controller (RPC)     Active Directory Web Services (TCP-In)			Active Directory Domain S	er All	Yes	Allow	C Refresh	
				Active Directory Domain S	er All	Yes	Allow	Export List	
				Active Directory Domain Si	er All	Yes	Allow	E Mala	
				Active Directory Domain S	er All	Yes	Allow	I nep	
				Active Directory Domain S	er All	Yes	Allow	BranchCache Conte	nt.
				Active Directory Domain S	er All	Yes	Allow	O Enable Rule	
				Active Directory Domain Si	er All	Yes	Allow	Kon	
				Active Directory Web Servi	ces All	Yes	Allow	Cut	
	Brangels	Carlin Contant Bater		BranchCache - Content Re	an All	No	Allow	Copy	
	Bran	Enable Rule	er (HTT	BranchCache - Hosted Cao	ch All	No	Allow	X Delete	
	Brat	Cut ht	(nI-Gé	BranchCache - Peer Discov	e. All	No	Allow	Properties	
	CO1	Conv	iln)	COM+ Network Access	All	No	Allow	Theperoes	
	CO1	Delate	DCOM-In)	COM+ Remote Administra	ti All	No	Allow	Help	
	Cor	L'elete	nreacha	Core Networking	All	Yes	Allow		
	Cor	Properties	nreacha	Core Networking	All	Yes	Allow		
	Cor Cor	Help	t Config	Core Networking	All	Yes	Allow		
	Corera	etworking - oynamic	must Config	Core Networking	AI	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	r6-ln)	Core Networking	AII	Yes	Allow		
	Core N	letworking - Multicas	st Listener Do	Core Networking	All	Yes	Allow		
	HA Case M	Internation Adultion	+ Listener Per	Cam Maturahian		Nee	Aller		

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

<b>@</b>	Windows Fi	rewall with Adv	anced Security				_ <b>D</b> X
File Action View Help							
🗢 🔿 🔁 🖬 🔒							
In Windows Firewall with Advanced Security on Local Co	Inbound Rules						Actions
🗱 Inbound Rules	Name		Group	Profile	Enabled		Inbound Rules
Control Contro	File and Printer Sharing (Echo Rev	uest - ICMPv4-In)	File and Printer Sharing	All	No		New Pula
Connection Security Rules	File ar Enable Rule	uest - ICMPv6-In)	d Printer Sharing	All	Yes		
Monitoring	Sile ar Cut	DP-In)			Yes		Filter by Profile
	Sile ar	ram-In)	Pight click > chor		Yes		🐨 Filter by State 🔹 🕨
	Seletar Deleta	-In)	Right Click-> Chội	•	Yes		Filter by Group
	S File ar	n-ln)	Enable Pule		Yes		
	Sile ar Properties				Yes		view •
	SFile ar Help	ervice - RPC)	rile and Frinter Sharing	AU	Yes		🖸 Refresh
	Sile and Printer Snanng (Spooler	service - RPC-EPMA	AP) File and Printer Sharing	All	Yes		📑 Export List
	🔘 File and Printer Sharing over SMB	Direct (iWARP-In)	File and Printer Sharing over	All	No		2 Help
	🕗 File Replication (RPC)		File Replication	All	Yes		- Help
	🕑 File Replication (RPC-EPMAP)		File Replication	All	Yes		File and Printer Sharin 🔺
	🕑 File Server Remote Management	(DCOM-In)	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 Remote Management	(WMI-In)	File Server Remote Manage	All	Yes		
	🕑 FTP Server (FTP Traffic-In)		FTP Server	All	Yes	≡	Сору
	🕑 FTP Server Passive (FTP Passive T	raffic-In)	FTP Server	All	Yes		🔀 Delete
	🕑 FTP Server Secure (FTP SSL Traffi	c-ln)	FTP Server	All	Yes		Properties
	iSCSI Service (TCP-In)		iSCSI Service	All	No		
	🕑 Kerberos Key Distribution Center	- PCR (TCP-In)	Kerberos Key Distribution C	All	Yes		I Help
	🕑 Kerberos Key Distribution Center	- PCR (UDP-In)	Kerberos Key Distribution C	All	Yes		
	🕑 Kerberos Key Distribution Center	(TCP-In)	Kerberos Key Distribution C	All	Yes		
	🕑 Kerberos Key Distribution Center	(UDP-In)	Kerberos Key Distribution C	All	Yes		
	Key Management Service (TCP-Ir	n)	Key Management Service	All	No		
	🕑 Microsoft Key Distribution Servic	e	Microsoft Key Distribution S	All	Yes		
	🖉 Microsoft Key Distribution Servic	e	Microsoft Key Distribution S	All	Yes		
	🖉 Netlogon Service (NP-In)		Netlogon Service	All	No		
	Netlogon Service Authz (RPC)		Netlogon Service	All	No		
	🖉 Network Discovery (LLMNR-UDP	-ln)	Network Discovery	All	Yes		
	🥑 Network Discovery (NB-Datagran	n-ln)	Network Discovery	All	Yes		
	🖉 Network Discovery (NB-Name-In	)	Network Discovery	All	Yes		
	🖉 Network Discovery (Pub-WSD-Inj	)	Network Discovery	All	Yes	$\sim$	
	<				:	>	]

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

2	Windows Fir	rewall with Advanced Secu	inty				- 0	×
File Action View Help								
🕈 🔹 💼 🚉 🖬 📷								
Windows Firewall with Advance	Indound Rules						Actions	
Inbound Rules	Name	Group *	Profile	Enabled	Action	~	Inbound Rules	-
Cutbound Rules	Active Directory Domain Controller - Ec.	Active Directory Domain Ser_	All	Yes	Allow	177	En New Pole	
Manitoring	Active Directory Domain Controller - Ec	Active Directory Domain Ser	All	Yes	Allow		a constant	
	Q Active Directory Domain Controller - LD	Active Directory Domain Ser	All	Yes	Allow		Y Filter by Profile	- 23
	Active Directory Domain Controller - LD	Active Directory Domain Ser_	All	Yes	Allow		Y Filter by State	
	Active Directory Domain Controller - LD	Active Directory Domain Ser_	AB	Ves	Allow		P Filter by Group	
	Active Directory Domain Controller - Net	Active Directory Domain Ser	AH	Yes	Allow	110		-
	Active Directory Domain Controller - SA	Active Directory Domain Ser	All	Ves	Allow		Siew	
	Active Directory Domain Controller - SA	Active Directory Domain Ser	AB	Yes	Allow		G Refresh	
	Active Directory Domain Controller - Sec.	Active Directory Domain Ser_	BA	Yes	Allew		Export List_	
	Q Active Directory Domain Controller - Sec.	Active Directory Domain Ser_	BA	Ves	Allow		E	
	Q Active Directory Domain Controller - W3	Active Directory Domain Ser_	AB	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	All	Yes	Allow			
	Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Yes	Allow			
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No	Allow		1	
	BranchCache Hosted Cache Server (HTT_	BranchCache - Hosted Cach	All	No	Allow			
	BranchCache Peer Discovery (WSD-In)	ExanchCache - Peer Discove	All	No	Allow			
	COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow		1	
	COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati	AN	No	Allow		1	
	Core Networking - Destination Unvescha	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	Yes.	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	All	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	All	Yes	Allow	5		
( m )	6 101				2	1		

**Step 2: chọn Port** -> click **Next**.

<b>@</b>	New Inbound Rule Wizard	x
Rule Type Select the type of firewall rule to cre	eate.	
Steps: 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         Ustom rule.	

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

<u></u>	New Inbound Rule Wizard	X
Protocol and Ports Specify the protocols and ports to	which this rule applies.	
Steps: Protocol and Pots Action Profile Name	<ul> <li>Does this rule apply to TCP or UDP?</li> <li>TCP</li> <li>UDP</li> <li>Does this rule apply to all local ports or specific local ports?</li> <li>All local ports</li> <li>Specific local ports:</li> <li>80 Example: 80, 443, 5000-5010</li> </ul>	> Cancel

#### Step 4: Chon Allow the connection -> click Next.



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

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

<b>@</b>	New Inbound Rule Wizard	x
Name		
Specify the name and description	of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
a Name	Port 80	
	Description (optional):	
	Allow port 80 inbound on all connections	
	< Back Finish Cancel	

## 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**

2		Windows Firewall		<b>*</b>	Allowed apps					L	
🔄 🏵 🔹 🕇 🔐 🖌 Control Pa	Control Panel + System and Security + Windows Firewall v C			🛞 💿 👻 🕈 🔐 > Control Panel > System	and Security + Windows Firewall + Allowed apps		v C S	earch Control Panel	,P		
Control Panel Home	Help protect your PC with Wind Windows Firewall can help prevent hacke Internet or a network.	lows Firewall es 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 What are the risks of allowing an app to communicate?	ewall settings.	Chan	e settings			
through windows Firewall	🛛 🔮 Domain networks	Connected 📀			Allowed apps and features:						
Turn Windows Firewall on or off	Networks at a workplace that are attache	ed to a domain			Name	Domain	Private	Public ^			
<ul> <li>Restore defaults</li> <li>Advanced settings</li> </ul>	Windows Firewall state:	On			File Replication	2	2	2			
Troubleshoot my network	Incoming connections:	Block all connections to apps that are not on the list of allowed apps			FTP Server	Ø					
	Active domain networks:	domain41.com			Kerberos Key Distribution Center Key Management Service						
	Notification state:	Do not notify me when Windows Firewall blocks a new app			KMS Emulator Port			2			
	Private networks	Not connected 🕑			Microsoft Key Distribution Service	Ø					
	Guest or public network	ks Not connected 🕑			Network Discovery	Det	Ø	Remove			
						[	Allow and	ther app			

OK

Cancel

### **Firewall allow APP FTP**

2	W	indows Firewall with Adva	nced Sec	urity				L	. o x
File Action View Help									
💠 🔿 🗾 🕞 📓 🖬									
Windows Firewall with Advanced Security on Local Co	m Inbound Rules							Actions	
Conception Service Pulse	Name Ø DNS (UDP, Incoming)	Group DNS Service	Profile	Enabled Yes	Action	Override No	P ^ %	Inbound Rules	*
Monitoring Firewall Connection Security Rules Security Associations Main Mode Quick Mode	<ul> <li>RPC (TCP, Incoming)</li> <li>RPC Endpoint Mapper (TCP, Incoming)</li> <li>File and Printer Sharing (Echo Request - I</li> <li>File and Printer Sharing (Echo Request - I</li> <li>File and Printer Sharing (Echo Request - I</li> <li>File and Printer Sharing (LLMNR-UDP-In)</li> <li>File and Printer Sharing (NB-Datagram-In)</li> <li>File and Printer Sharing (NB-Name-In)</li> </ul>	DNS Service DNS Service File and Printer Sharing File and Printer Sharing	All Public Domai All All All	Yes Yes No Yes Yes Yes Yes	Allow Allow Block Block Allow Allow Allow	No No No No No No No	** < < < * * *	<ul> <li>✓ Filter by Profile</li> <li>✓ Filter by State</li> <li>✓ Filter by Group</li> <li>View</li> <li>☑ Refresh</li> <li>☑ Export List</li> </ul>	· · · · ·
	<ul> <li>File and Printer Sharing (NB-Session-In)</li> <li>File and Printer Sharing (SMB-In)</li> <li>File and Printer Sharing (Spooler Service</li> <li>File and Printer Sharing over SMBDirect (i</li> <li>File Replication (RPC)</li> <li>File Replication (RPC-EPMAP)</li> <li>File Server Remote Management (DCOM</li> <li>File Server Remote Management (SMB-In)</li> <li>File Server Remote Management (WMI-In)</li> </ul>	File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing over File Replication File Replication File Server Remote Manage File Server Remote Manage	AII AII AII AII AII AII AII AII AII	Yes Yes Yes No Yes Yes Yes Yes Yes	Allow Allow Allow Allow Allow Allow Allow Allow Allow	No No No No No No No	5'5'% A 5'% % % 5'9	Help	
ζ 111	<ul> <li>FTP Server (FTP Traffic-In)</li> <li>FTP Server Passive (FTP Passive Traffic-In)</li> <li>FTP Server Secure (FTP SSL Traffic-In)</li> <li>FTP Server Secure (FTP SSL Traffic-In)</li> <li>FSCSI Service (TCP-In)</li> <li>Kerberos Key Distribution Center - PCR (</li> <li>Kerberos Key Distribution Center - PCR (</li> <li>Kerberos Key Distribution Center (TCP-In)</li> <li>Kerberos Key Distribution Center (UDP-In)</li> <li>Key Management Service (TCP-In)</li> <li>Microsoft Key Distribution Service</li> <li>Microsoft Key Distribution Service</li> <li>Netlogon Service (NP-In)</li> <li>Netlogon Service Authz (RPC)</li> <li>Network Discovery (LLMNR-UDP-In)</li> </ul>	FTP Server FTP Server FTP Server ISCST Service Kerberos Key Distribution C Kerberos Key Distribution C Kerberos Key Distribution C Kerberos Key Distribution C Key Management Service Microsoft Key Distribution S Microsoft Key Distribution S Netlogon Service Netlogon Service Network Discovery	AII AII AII AII AII AII AII AII AII AII	Yes Yes Yes Yes Yes Yes Yes Yes No No No Yes	Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow	No No No No No No No No No No No No No	***********		

### **Firewall allow APP FTP**

· 🖌	Wi	indows Firewall with Adva	inced Sec	urity				_ <b>_</b> X
File Action View Help								
💠 🔿 🙇 📷 🔒 🖬 📷								
P Windows Firewall with Advanced Security on Local Com	Outbound Rules							Actions
<ul> <li>Windows Firewall with Advanced Security on Local Com</li> <li>Inbound Rules</li> <li>Outbound Rules</li> <li>Connection Security Rules</li> <li>Monitoring</li> <li>Firewall</li> <li>Connection Security Rules</li> <li>Security Associations</li> <li>Main Mode</li> <li>Quick Mode</li> </ul>	Outbound Rules Name Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I Core Networking - Router Advertisement Core Networking - Router Solicitation (IC Core Networking - Teredo (UDP-Out) Core Networking - Time Exceeded (ICMP DHCP Server Failover (TCP-Out) Distributed Transaction Coordinator (TC All Outgoing (TCP) All Outgoing (UDP) File and Printer Sharing (Echo Request - I File and Printer Sharing (Echo Request - I File and Printer Sharing (Echo Request - I File and Printer Sharing (LLMNR-UDP-Out) File and Printer Sharing (LLMNR-UDP-Out)	Group Core Networking Core Networking Core Networking Core Networking Core Networking DHCP Server Management Distributed Transaction Coo DNS Service DNS Service File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing	Profile All All All All All All All All All Domai Public All All All	Enabled Yes Yes Yes Yes Yes No Yes Yes No Yes Yes Yes Yes Yes Yes	Action Allow Allow Allow Allow Allow Allow Allow Allow Allow Block Block Allow Allow	Override No No No No No No No No No No No No No	P A A A & A % % % % A A A % 0	Actions         Outbound Rules         Image: New Rule         Image: Filter by Profile         Image: Filter by Profile         Image: Filter by State         Image: Filter by Group         Image: View         Image: Filter by Group         Image: Filter by Group
	File and Printer Sharing (NB-Datagram-O File and Printer Sharing (NB-Name-Out) File and Printer Sharing (NB-Session-Out) File and Printer Sharing (SMB-Out) FTP Server (FTP Traffic-Out)	File and Printer Sharing File and Printer Sharing File and Printer Sharing File and Printer Sharing FTP Server		Yes Yes Yes Yes Yes	Allow Allow Allow Allow	No No No No	5. 5. 5. 5. 5.	Copy Copy Properties
	<ul> <li>FTP Server Secure (FTP SSL Traffic-Out)</li> <li>iSCSI Service (TCP-Out)</li> <li>Network Discovery (LLMNR-UDP-Out)</li> <li>Network Discovery (NB-Datagram-Out)</li> <li>Network Discovery (NB-Name-Out)</li> <li>Network Discovery (Pub WSD-Out)</li> <li>Network Discovery (SDP-Out)</li> <li>Network Discovery (UPnPHost-Out)</li> <li>Network Discovery (WSD-Out)</li> <li>Network Discovery (WSD Events-Out)</li> <li>Network Discovery (WSD EventsSecure-O</li> <li>Network Discovery (WSD EventsSecure-O</li> <li>Network Discovery (WSD EventsSecure-O</li> <li>Network Discovery (WSD -Out)</li> <li>Retwork Discovery (WSD EventsSecure-O</li> <li>Network Discovery (WSD -Out)</li> <li>Routing and Remote Access (GRE-Out)</li> </ul>	FTP Server ISCSI Service Network Discovery Network Discovery Routing and Kemote Access Routing and Remote Access	All All All All All All All All All All	Yes No Yes Yes Yes Yes Yes Yes Yes No No	Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow	No No No No No No No No No No No No No N	************	Help
< III >	< 111						>	1

32