Lesson 19: Configuring Windows Firewall

MOAC 70-410: Installing and Configuring Windows Server 2012



WILEY

Overview

- Exam Objective 6.4: Configure Windows Firewall
- Building a Firewall
- Using the Windows Firewall Control Panel
- Using the Windows Firewall with Advanced Security Console

Building a Firewall

Lesson 19: Configuring Windows Firewall

© 2013 John Wiley & Sons, Inc.

Building a Firewall

- A **firewall** is a software program that protects a computer or a network by allowing certain types of network traffic in and out of the system while blocking others.
- A firewall is essentially a series of filters that examine the contents of packets and the traffic patterns to and from the network to determine which packets they should allow to pass through the filter.

Firewalls Protect Against:

- Network scanner applications that probe systems for unguarded ports, which are essentially unlocked doors that attackers can use to gain access to the system.
- Trojan horse applications that open a connection to a computer on the Internet, enabling an attacker on the outside to run programs or store data on the system.
- Attackers that obtain passwords by illicit means, such as social engineering, and then use remote access technologies to log on to a computer from another location and compromise its data and programming.
- Denial of service attacks that use authorized access points to bombard a system with traffic, preventing legitimate traffic from reaching the computer.

Firewall Settings

The three most important criteria that firewalls can use in their rules are:

- IP addresses: Identify specific hosts on the network. You can use IP addresses to configure a firewall to allow only traffic from specific computers or networks in and out.
- **Protocol numbers:** Specify whether the packet contains TCP or UDP (User Datagram Protocol) traffic. You can filter protocol numbers to block packets containing certain types of traffic.
- **Port numbers:** Identify specific applications running on the computer. The most common firewall rules use port numbers to specify the types of application traffic the computer is allowed to send and receive.

Firewall Settings

Firewall rules can function in two ways:

- Admit all traffic, except that which conforms to the applied rules
- Block all traffic, except that which conforms to the applied rules

- The **Windows Firewall control panel** provides a simplified interface that enables you to avoid the details of rules and port numbers.
- For full access to firewall rules and more sophisticated functions, you must use the Windows Firewall with Advanced Security console.
- Many of the roles and features included in Windows Server 2012 automatically open the appropriate firewall ports when you install them.
- The system warns you of firewall issues.

👽 🔂 📗 =	Network	- 🗆 X
File Network Vie	2W	v 😯
🔄 🍥 🔻 🕈 🖣 🕨 N	letwork v C Search Network	م
Network discovery and file s	haring are turned off. Network computers and devices are not visible. Click to change	×
✓ ★ Favorites ■ Desktop ▶ Downloads ₩ Recent places	This folder is empty.	
Libraries		
Þ 🖳 Computer		
🗅 🗣 Network		
0 items		8== 🖿

Windows Explorer with Network Discovery and File Sharing turned off

Advanced sharing settings	_ 🗆 X
() ▼ ↑ 🗟 ≪ Network and Sharing Center ➤ Advanced sharing settings ∨ ♥	anel 🔎
Change sharing options for different network profiles	
Windows creates a separate network profile for each network you use. You can choose specific options for each profile.	
Private (9
Guest or Public	9
Domain (current profile) ($\overline{\mathbf{O}}$
Network discovery	
When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.	
Turn on network discovery	
 Turn off network discovery 	
File and printer sharing	-
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.	
 Turn on file and printer sharing Turn off file and printer sharing 	
le run on nie and princer sharing	
All Networks (*	•)
Save changes Cancel	

The Advanced Sharing Settings page of the Network and Sharing Center control panel

<i>2</i>	Allowed apps					_	□ X
€ ⊚ -	↑ 🔗 ≪ System and Security ト Windows Firewall ト Allowed apps	~ ¢	Sear	ch Contro	l Pane	el	Q
	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?		🛞 Chaj	nge settin	gs		
	Allowed apps and features:						
	Name	Domain	Private	Public	^		
	ISCSI Service Key Management Service						
	Netlogon Service						
	Network Discovery						
	Performance Logs and Alerts						
	Remote Desktop				≡		
	Remote Event Log Management						
	Remote Scheduled Tasks Management						
	Remote Service Management						
	Remote Shutdown						
	Remote volume Management Resition and Remote Access						
					~		
		Det	ai <u>l</u> s	Re <u>m</u> ov	e		
			Allow an	iothe <u>r</u> apj	o		
			ОК	Cano	el		

The Network Discovery application in the Allowed apps dialog box

© 2013 John Wiley & Sons, Inc.

2	Windows Firewall with Adva	inced Security		_ □	x
File Action View Help					
🗢 🄿 🙇 🖬 🔒					
Windows Firewall with Advance	Inbound Rules		A	ctions	
🗱 Inbound Rules	Name	Group	~	nbound Rules	▲ <u>^</u>
Connection Security Rules	Netlogon Service (NP-In)	Netlogon Service	1	🚦 New Rule	
Monitoring	Network Discovery (LLMNR-UDP-In)	Network Discovery		Filter by Profile	•
	Network Discovery (NB-Datagram-In)	Network Discovery		Filter by State	
	Wetwork Discovery (NB-Name-In)	Network Discovery		Filter by Group	•
	Wetwork Discovery (Pub-WSD-In)	Network Discovery		View	•
	Wetwork Discovery (SSDP-In)	Network Discovery			=
	Wetwork Discovery (UPnP-In)	Network Discovery	≡ Ľ	Refresh	
	Wetwork Discovery (WSD Events-In)	Network Discovery		🗼 Export List	
	Network Discovery (WSD EventsSecure-In)	Network Discovery		? Help	
	Performance Logs and Alerts (DCOM-In)	Performance Logs and Ale	ſ	Network Discovery	•
	Performance Logs and Alerts (DCOM-In)	Performance Logs and Ale		Enable Rule	
	Performance Logs and Alerts (TCP-In)	Performance Logs and Ale		🖌 Cut	_
	Remote Desktop - User Mode (TCP-In)	Remote Desktop		🖹 Сору	
< III >		> · · · · · · · · · · · · · · · · · · ·		🕻 Delete	~

Network Discovery rules in the Windows Firewall with Advanced Security console

Using the Windows Firewall Control Panel

Lesson 19: Configuring Windows Firewall

© 2013 John Wiley & Sons, Inc.

Using the Windows Firewall Control Panel



The Windows Firewall control panel window

Using the Windows Firewall Control Panel

@	Customize Settings	□ X
€ 🗇 ד ↑ 🔗 «	Windows Firewall Customize Settings V C Search Control Panel	Q
Custor You can Domain V	mize settings for each type of network modify the firewall settings for each type of network that you use. network settings In the intervention of 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)	
Drivate r		
Ø	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)	
W		
Public n V	 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) 	
	OK Cancel	

The Customize Settings dialog box for Windows Firewall

Allowing Applications

Allowed apps		_ D X
	✓ C Search Control Pa	nel 🔎
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? Allowed apps and features: Name BranchCache - Content Retrieval (Uses HTTP) BranchCache - Hosted Cache Client (Uses HTTPS) BranchCache - Hosted Cache Server (Uses HTTPS) BranchCache - Peer Discovery (Uses WSD) COM+ Network Access COM+ Remote Administration Core Networking Distributed Transaction Coordinator File and Printer Sharing File and Printer Sharing over SMBDirect SCSI Service Key Management Service	Domain Private Public Omain Private Public Omain Omain Image: Stress of the str	
	OK Cancel]

The Allowed Apps dialog box for Windows Firewall

Using the Windows Firewall with Advanced Security Console

Lesson 19: Configuring Windows Firewall

© 2013 John Wiley & Sons, Inc.

Using the Windows Firewall with Advanced Security Console



The Windows Firewall with Advanced Security console

Configuring Profile Settings

- The default Windows Firewall configuration calls for the same basic settings for all three profiles:
 - The firewall is turned on.
 - Incoming traffic is blocked unless it matches a rule.
 - Outgoing traffic is allowed unless it matches a rule.

Configuring Profile Settings

Windows Fire	ewall with Adv	anced	Sec	urity on Loc	al Co 🗙
Domain Profile	Private Profile P	ublic Pro	file	IPsec Settings	
Specify beha domain. State	avior for when a co	mputer is	conn	ected to its corp	orate
🚽 🔒 R	irewall state:	Or	n (reco	ommended)	~
	Inbound connecti	ions:		Block (default)	~
	Outbound connect	ctions:		Allow (default)	~
	Protected network	k connec	ctions	Custor	mize
Settings	pecify settings that irewall behavior.	control \	Windo	ws Custor	mize
Logging S tr	pecify logging settir oubleshooting.	ngs for		Custor	mize
		ОК		Cancel	<u>A</u> pply

The Windows Firewall with Advanced Security on Local Computer dialog box

© 2013 John Wiley & Sons, Inc.

2	Windows Firewall wi	th Advanced Security			_ D X
File Action View Help	5				
(= =) 🖄 🖬 🔒 🛛					
Pindows Firewall with A	Inbound Rules				Actions
🗱 Inbound Rules	Name	Group [▲]	Profile	Enabled ^	Inbound 🔺
Cutbound Rules	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No	Mar New
Connection Security	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No _	ivew
Monitoring	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	🕎 Filter 🕨
	COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	🝸 Filter 🕨
	COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati	All	No	🕎 Filter 🕨
	🕑 Core Networking - Destination Unreacha	Core Networking	All	Yes	View
	🕢 Core Networking - Destination Unreacha	Core Networking	All	Yes	
	🔇 Core Networking - Dynamic Host Config	Core Networking	All	Yes	Refresh
	🔇 Core Networking - Dynamic Host Config	Core Networking	All	Yes	📑 Export
	🕑 Core Networking - Internet Group Mana	Core Networking	All	Yes	7 Help
	🕑 Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	- neip
	🕑 Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Network 🔺
	🕑 Core Networking - Multicast Listener Do	Core Networking	All	Yes	Enabl
	Ore Networking - Multicast Listener Qu	Core Networking	All	Yes	K Cut
	🔮 Core Networking - Multicast Listener Rep	Core Networking	All	Yes	
	Ore Networking - Multicast Listener Rep	Core Networking	All	Yes	🕒 Сору
	Ore Networking - Neighbor Discovery A	Core Networking	All	Yes	🗙 Delete
	Ocre Networking - Neighbor Discovery S	Core Networking	All	Yes	Prope
	Core Networking - Packet Too Big (ICMP	Core Networking	All	Yes	- ·
	Core Networking - Parameter Problem (I	Core Networking	All	Yes 🗸	l Help
< III >	< <u> </u>			>	

The Inbound Rules list in the Windows Firewall with Advanced Security console

@	New Inbound Rule Wizard	x
Rule Type Select the type of firewall rule to c	reate.	
Steps: Program Action Profile Name	What type of rule would you like to create? • Program Rule that controls connections for a program. • Pgt Rule that controls connections for a TCP or UDP port. • Prgdefined: BranchCache - Content Retrieval (Uses HTTP) v Rule that controls connections for a Windows experience. • Custom Custom rule.	

The Rule Type page in the New Inbound Rule Wizard

@	New Inbound Rule Wizard	x
Program Specify the full program path and e	executable name of the program that this rule matches.	
Steps: Program Action Profile Name	Does this rule apply to all programs or a specific program? All programs Rule applies to all connections on the computer that match other rule properties. Image: This program path: Example: c:\path\program.exe YProgram Files %\browser\browser.exe	

The Program page in the New Inbound Rule Wizard

@	New In	nbound Rule Wizard
Protocol and Ports		
Specify the protocols and ports to	which this rule applies.	
Steps:		
a Rule Type	To which ports and prot	ocols does this rule apply?
Program		
Protocol and Ports	Protocol type:	Any 🗸
Scope	Protocol number:	0
Action		
Profile	Local port:	All Ports v
Name		
	Dt-	Example: 80, 443, 5000-5010
	Remote port:	All Ports
		Example: 80, 443, 5000-5010
	Internet Control Messag (ICMP) settings:	ge Protocol Customize < Back Next > Cancel

The Protocols and Ports page in the New Inbound Rule Wizard

@	New Inbound Rule Wizard					
Predefined Rules						
Select the rules to be created for	this experience.					
Steps:						
Rule Type	Which rules would you like to create?					
Predefined Rules	The following rules define network connectivity re	quirements for the se	lected predefin	ed group.		
 Action 	the existing rule will be overwritten.	ready exists and is cl	iecked, the co	ILCIILS OF		
	Rules:	Rule Exists	Profile	Desc		
	BranchCache Content Retrieval (HTTP-In)	Already exists	All	Inbou		
	< 111			>		
		< Back	Next >	Cancel		

The Predefined Rules page in the New Inbound Rule Wizard

@	New Inbound Rule Wizard	x
Scope		
Specify the local and remote IP ad	ddresses to which this rule applies.	
Steps:		
Rule Type		
Program	Which local IP addresses does this rule apply to?	
Protocol and Ports	 Any IP address 	
Scope	O These IP addresses:	
Action	Add	
Profile	Edit	
Name	Remove	
	Customize the interface types to which this rule applies: Customize	
	Which remote IP addresses does this rule apply to?	
	Any IP address	
	O These IP addresses:	
	Add	
	Edit	
	Remove	
	< Back Next > Cancel	

The Scope page of the New Inbound Rule Wizard

@	New Inbound Rule Wizard	×
Action		
Specify the action to be taken v	when a connection matches the conditions specified in the rule.	
Steps:		
Steps: Rule Type Program Protocol and Ports Scope Action Profile Name	What action should be taken when a connection matches the specified conditions? Image: Contract Cont	
	< Back Next > Cancel	

The Action page of the New Inbound Rule Wizard

@	New Inbound Rule Wizard	x
Profile		
Specify the profiles for which this	rule applies.	
Steps:		
Rule Type	When does this rule apply?	
Program		
Protocol and Ports	Domain Applies when a computer is connected to its corporate domain.	
Scope Action		
 Profile 	Applies when a computer is connected to a private network location, such as a home	
• Name	or work place. ✓ Public Applies when a computer is connected to a public network location. <back next=""> Cancel</back>	

The Profile page of the New Inbound Rule Wizard

@	New Inbound Rule Wizard	x
Name		
Specify the name and description	of this rule.	
Steps:		
Rule Type		
Program		
Protocol and Ports	News	
Scope	Name:	
Action		
Profile	Description (optional):	
Name		
	< Back Finish Cancel	

The Name page of the New Inbound Rule Wizard

Importing and Exporting Rules

- The process of creating and modifying rules in the Windows Firewall with Advanced Security console can be time consuming.
- The console makes it possible for you to save the rules and settings you create by exporting them to a policy file.
- A policy file is a file with a .wfw extension that contains all the property settings in a Windows Firewall installation, as well as all of its rules, including the preconfigured rules and the ones you created or modified.

Creating Rules Using Group Policy

- Windows Firewall is an application designed to protect a single computer from intrusion
- Administrators can distribute firewall settings to computers throughout the network by using Group Policy.

Creating Rules Using Group Policy



The Windows Firewall with Advanced Security node in a Group Policy object

© 2013 John Wiley & Sons, Inc.

Using Filters

- The **filter** feature enables you to display inbound or outbound rules according to:
 - The profile they apply to
 - Their current state
 - The group to which they belong

- The IP Security (IPsec) standards are a collection of documents that define a method for securing data while it is in transit over a TCP/IP network.
- IPsec includes a connection establishment routine, during which computers authenticate each other before transmitting data, and a technique called **tunneling**, in which data packets are encapsulated within other packets, for their protection.
- Windows Server 2012 also includes a feature that incorporates IPsec data protection into the Windows Firewall.

<i>\</i>	New Connection Security Rule Wizard	x
Rule Type Select the type of connection sec	urity rule to create.	
Steps: Paule Type Requirements Authentication Method Profile Name	What type of connection security rule would you like to create? Image: Solution Restrict connections based on authentication criteria, such as domain membership or health status. Image: Authentication exemption Do not authenticate connections from the specified computers. Image: Server-to-server Authenticate connection between the specified computers. Image: Server To Server Authenticate connections between the specified computers. Image: Server To Server Authenticate connections between two computers. Image: Server To Server Authenticate connections between two computers. Image: Server To Server Authenticate connections between two computers. Image: Server To Server Authenticate connections between two computers. Image: Server To Server Authenticate connections between two computers. Image: Server To Server Authenticate connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule. Seak Net > Cancel	

The Rule Type page in the New Connection Security Rule Wizard

<i>@</i>	New Connection Security Rule Wizard	x
Endpoints		
Specify the computers between v	which secured connections will be established using IPsec.	
Steps:		
Rule Type	Create a secured connection between computers in Endpoint 1 and Endpoint 2.	
Endpoints	Which computers are in Endpoint 1?	
Requirements	 Any IP address 	
Authentication Method	O These IP addresses:	
Profile	Add	
Name	Edit	
	Bemove	
	Customize the interface types to which this rule applies: Customize	
	Which computers are in Endpoint 2?	
	 Any IP address 	
	O These IP addresses:	
	Add	
	Edit	
	Bemove	
	I TEHIOVE	
	< Back Next > Cance	

The Endpoints page in the New Connection Security Rule Wizard

<i>@</i>	New Connection Security Rule Wizard	×
Requirements Specify the authentication require	ments for connections that match this rule.	
Steps: Rule Type Endpoints Requirements Authentication Method Profile Name	When do you want authentication to occur? • Request authentication for inbound and outbound connections Authenticate whenever possible but authentication is not required. • Require authentication for inbound connections and request authentication for outbound connections Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required. • Require authentication for inbound and outbound connections are authenticated whenever possible but authentication is not required. • Require authentication for inbound and outbound connections Both inbound and outbound connections must be authenticated to be allowed. • Require authentication for inbound and outbound connections Both inbound and outbound connections must be authenticated to be allowed. • Back • Next > • Cancel	

The Requirements page in the New Connection Security Rule Wizard

@	New Connection Security Rule Wizard	x
Authentication Method	omed for connections that match this rule.	
Steps: Rule Type Endpoints Requirements Authentication Method Profile Name	What authentication method would you like to use? • Computer certificate Restrict communications to connections from computers that have a certificate from this certification authority (CA). Signing Algorithm: RSA (default) v Certificate store type: Root CA (default) v CA name: CA name: Restrict certificates Restrict certificates are issued by Network Access Protection health certificate servers. Methods Accept only health certificates Restrict cates are issued by Network Access Protection health certificate servers.	
	< Back Next > Cance	I

The Authentication Method page in the New Connection Security Rule Wizard

Lesson Summary

- A firewall is a software program that protects a computer by allowing certain types of network traffic in and out of the system while blocking others.
- A firewall is essentially a series of filters that examine the contents of packets and the traffic patterns to and from the network to determine which packets they should allow to pass through the filter.
- The default rules preconfigured into the firewall are designed to admit the traffic used by standard Windows networking functions, such as file and printer sharing. For outgoing network traffic, Windows Firewall allows all traffic to pass the firewall except that which conforms to a rule.
- The Windows Firewall control panel is designed to enable administrators to perform basic firewall configuration tasks as needed.
- For full access to the Windows Firewall configuration settings, you
 must use the Windows Firewall with Advanced Security snap-in for
 the Microsoft Management console.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.



