### Description

This article will detail how to perform the most common tasks with the windows firewall on Windows Server 2012. This includes managing the firewall settings and creating custom inbound and outbound firewall rules.

### Contents

- <u>Managing Firewall Settings</u>
- Applying Custom Rules

# **Managing Firewall Settings**

The Windows Firewall with Advanced Security is a host-based firewall that runs on Windows Server 2012 and is turned on by default. Firewall settings within Windows Server 2012 are managed from within the Windows Firewall MMC (Microsoft Management Console). To review and set Firewall settings perform the following:

1. Open the Server Manager from the task bar.

2. Click the Tools menu and select Windows Firewall with Advanced Security.



3. First review the current configuration settings by selecting **Windows Firewall Properties** from the MMC landing page. This **allows access to modify the settings** for each of the three firewall profiles, **Domain, Private, and Public** as well as IPSec settings.



### **Applying Custom Rules**

Custom Rules allow the finest level of control over inbound and outbound traffic to your Windows Server 2012.

1. If you have not done so already load the Windows Firewall MMC by opening the **Server Manager** from the task bar, clicking the **Tools menu**, and selecting **Windows Firewall with Advanced Security**.

2. Select either **Inbound Rules** or **Outbound Rules** under **Windows Firewall with Advanced Security** on the left side of the management console.

Note: This will provide a listing on each of the currently configured firewall rules. Rules that are currently enabled are denoted by green checkbox icon, while disabled rules display a grey checkbox icon. Rightclicking a rule will allow you toggle enable/disable.

<b>@</b>	Windows I	irewall with Advanced Secu	rity				_ <b>_</b> ×
File Action View Help							
🗢 🏟 🖄 🗊 🗟 🖬							
Windows Firewall with Advance	Inbound Rules						Actions
Inbound Rules	Name	Group	Profile	Enabled	Action	~	Inbound Rules
Cutbound Rules	SExample Inbound Block		All	Yes	Block		Max Rule
Connection Security Rules	Active Directory Domain Controller - Ec.	Active Directory Domain Ser	All	Yes	Allow		
Monitoring	Active Directory Domain Controller - Ec.	. Active Directory Domain Ser	All	Yes	Allow	_	Filter by Profile
	Active Directory Domain Controller - LD.	Active Directory Domain Ser	All	Yes	Allow	-	Filter by State
	Active Directory Domain Controller - LD.	Active Directory Domain Ser	All	Yes	Allow		Filter by Group
	Active Directory Domain Controller - LD.	Active Directory Domain Ser	All	Yes	Allow		Minu
	🖉 Active Directory Domain Controller - Net	Active Directory Domain Ser	All	Yes	Allow		view
	🐼 Active Directory Domain Controller - SA.	Active Directory Domain Ser	All	Yes	Allow		🕼 Refresh
	Active Directory Domain Controller - SA.	Active Directory Domain Ser	All	Yes	Allow		Export List
	🖉 Active Directory Domain Controller - Sec	Active Directory Domain Ser	All	Yes	Allow		17 Help
	🖉 Active Directory Domain Controller - Sec	Active Directory Domain Ser	All	Yes	Allow		The p
	Active Directory Domain Controller - W3	Active Directory Domain Ser	All	Yes	Allow		BranchCache Content +
	🐼 Active Directory Domain Controller (RPC	) Active Directory Domain Ser	All	Yes	Allow		C Enable Rule
	Active Directory Domain Controller (RPC	Active Directory Domain Ser	All	Yes	Allow		K c.
	Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Yes	Allow		a Cut
	BranchCache Content Retrieval (HTTP-In	) BranchCache - Content Retr	All	No	Allow		Сору
	Brar Enable Rule er (HTT.	BranchCache - Hosted Cach	All	No	Allow	1	💥 Delete
	Brar Cut SD-In)	BranchCache - Peer Discove	All	No	Allow		Properties
	COI Conv In)	COM+ Network Access	All	No	Allow		Fiopenies
	COI Delete DCOM-I	n) COM+ Remote Administrati	All	No	Allow		? Help
	Or Delete nreacha	Core Networking	All	Yes	Allow		
	Or Properties nreacha	Core Networking	All	Yes	Allow		
	🐼 Cor Help t Config	Core Networking	All	Yes	Allow		
	Core retworking - Dynamic Host Config	Core Networking	All	Yes	Allow		
	🐼 Core Networking - Internet Group Mana.	Core Networking	All	Yes	Allow		
	🔇 Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow		
	🔇 Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow		
	🖉 Core Networking - Multicast Listener Do.	Core Networking	All	Yes	Allow		
< III >	Care Naturking Multicast Listoner Ou	Caro Natworking	AU	Ver	Allow	~	
Enable Rule	1						

3. From the right side of either the Inbound Rules or Outbound Rules tab click New Rule.

File Action View Help								
🕨 🔿 💆 📰 🗟 🔽 🛅								
Windows Firewall with Advance	Inbound 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		May Puls	
Connection Security Rules	Active Directory Domain Controller - Ec	Active Directory Domain Ser	All	Yes	Allow		Nally Vole	
Monitoring	Active Directory Domain Controller - LD	Active Directory Domain Ser	All	Yes	Allow	_	Filter by Profile	
	Active Directory Domain Controller - LD	Active Directory Domain Ser	All	Yes	Allow	=	T Filter by State	
	Active Directory Domain Controller - LD	Active Directory Domain Ser	All	Yes	Allow		Filter by Group	
	Active Directory Domain Controller - Net	Active Directory Domain Ser	All	Yes	Allow		1	
	Active Directory Domain Controller - SA	Active Directory Domain Ser	All	Yes	Allow		View	
	Active Directory Domain Controller - SA	Active Directory Domain Ser	All	Yes	Allow		a Refresh	
	Active Directory Domain Controller - Sec	Active Directory Domain Ser	All	Yes	Allow		🔒 Export List	
	Active Directory Domain Controller - Sec	Active Directory Domain Ser	All	Yes	Allow			
	Active Directory Domain Controller - W3	Active Directory Domain Ser	All	Yes	Allow		Пер	
	Active Directory Domain Controller (RPC)	Active Directory Domain Ser	All	Yes	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			
	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	All	No	Allow			
	Ore Networking - Destination Unreacha	Core Networking	All	Yes	Allow			
	Ore Networking - Destination Unreacha	Core Networking	All	Yes	Allow			
	Ore Networking - Dynamic Host Config	Core Networking	All	Yes	Allow			
	Ore Networking - Dynamic Host Config	Core Networking	All	Yes	Allow			
	Ore Networking - Internet Group Mana	Core Networking	All	Yes	Allow			
	Ocore Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow			
	Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow			
	Ore Networking - Multicast Listener Do	Core Networking	All	Yes	Allow			
	Ore Networking - Multicast Listener Qu	Core Networking	All	Yes	Allow			
	Ore Networking - Multicast Listener Rep	Core Networking	All	Yes	Allow	~		
III >	<				>			

4. Select **Custom** from the Rule Type radial button and click **Next**.

<b>a</b>	New Inbound Rule Wizard	)
Rule Type Select the type of firewall rule to c	reate.	
Steps: Program Protocol and Ports Scope Action Profile Name	What type of rule would you like to create?         Program         Rule that controls connections for a program.         Port         Rule that controls connections for a TCP or UDP port.         Predefined:         Active Directory Domain Services         Rule that controls connections for a Windows experience.         O Custom         Custom rule.	cel

5. **Select the Program association** for the Custom Firewall Rule either All programs or the path to a program and click **Next**.

<b>@</b>	New Inbound Rule Wizard
<b>Program</b> Specify the full program path and e	executable name of the program that this rule matches.
Steps: Program Protocol and Ports Scope 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.             This program path:

6. From the Protocol type field **select the protocol type** and click **Next**.

Note: This walkthrough uses TCP on port 80 (HTTP) for example purposes.

<b>@</b>	New In	nbound Rule Wizard
Protocol and Ports		
Specify the protocols and ports to	which this rule applies.	
Steps:		
Rule Type	To which ports and prot	ocols does this rule apply?
Program		
Protocol and Ports	Protocol type:	TCP v
Scope	Protocol number:	6
<ul> <li>Action</li> <li>Bestle</li> </ul>		
Profile	Local port:	Specific Ports
Juanie Name		80 Example: 90, 442, 5000, 5010
	Remote port:	All Ports
		Example: 80, 443, 5000-5010
	Internet Control Messag (ICMP) settings:	ge Protocol Customize
		< Back Next Cancel

7. Select an IP address association for both local and remote addresses and click Next.

<i><sup>•</sup></i>	New Inbound Rule Wizard
Scope	
Specify the local and remote IP	addresses 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	Ado
Profile	Edi
Name	Rem
	Customize the interface types to which this rule applies: Custom
	Which remote IP addresses does this rule apply to?
	Any IP address
	O These IP addresses:
	Add
	Edi
	Rem
	< Back Next

8. Select an action to take on matching traffic and click **Next**.

<b>@</b>	New Inbound Rule Wizard
Action	
Specify the action to be taken v	when a connection matches the conditions specified in the rule.
Steps:	
Rule Type	What action should be taken when a connection matches the specified conditions?
Program	Allow the connection
Protocol and Ports	This includes connections that are protected with IPsec as well as those are not.
Scope	Allow the connection if it is secure
<ul> <li>Action</li> </ul>	This includes only connections that have been authenticated by using IPsec. Con will be accurred using the acttings in IPsec properties and rules in the Connection St
Profile	Rule node.
<ul> <li>Name</li> </ul>	Customize
	Riack the connection
	< Back Next >
	hE

9. Select the profiles associated with the custom rule and click Next.

# New Inbound Rule Wizard Profile Specify the profiles for which this rule applies. Steps: When does this rule apply? Rule Type Program Domain Protocol and Ports Applies when a computer is connected to its corporate domain. Scope Private Action Applies when a computer is connected to a private network location, such as a ho Profile or work place. Name ✓ Public Applies when a computer is connected to a public network location. Ne < Back

10. Provide a name for your Firewall rule and an optional description and click **Finish**.

2	New Inbound Rule Wizard
Name Specify the name and description	of this rule.
Name Specify the name and description Steps: Program Protocol and Ports Scope Action Profile Name	of this rule.          Name:         Example Inbound Block         Description (optional):         This rule will block incoming connections on port 80.]
	< Back

11. Once created the rule will be enabled. The firewall rule can be found on the corresponding Rule tab, either inbound or outbound depending on the type created. To disable or delete the rule find the rule in the MMC, right-click it, and select either Disable Rule or Delete.

Windows I	Windows Firewall with Advanced Security					
File Action View Help						
Windows Firewall with Advance Inbound Rules	Inbound Rules Act					
Name Name	Name Group		Enabled	Action ^	Inbo	
Custound Rules Security Pulses		All	Yes	Block		
Monitoring	Disable Rule n S	er All	Yes	Allow		
Active Directory Domain Controller -	Cut n S	er All	Yes	Allow =	Y I	
🕢 Active Directory Domain Controller - L	Copy n S	er All	Yes	Allow		
🕢 Active Directory Domain Controller - L	Delete n S	er All	Yes	Allow	TF	
🕢 Active Directory Domain Controller - L	n S	er All	Yes	Allow		
🕢 Active Directory Domain Controller - N	Properties n S	er All	Yes	Allow		
🕢 Active Directory Domain Controller - S	Help n S	er All	Yes	Allow	QF	
🕢 Active Directory Domain Controller - SA.	. Active Directory Domain S	er All	Yes	Allow	📑 E	
🕢 Active Directory Domain Controller - Sec	Active Directory Domain S	er All	Yes	Allow	2	
🕢 Active Directory Domain Controller - Sec	Active Directory Domain S	er All	Yes	Allow		
🕢 Active Directory Domain Controller - W3	Active Directory Domain S	er All	Yes	Allow	Exar	
🕢 Active Directory Domain Controller (RPC	) Active Directory Domain S	er All	Yes	Allow		
Active Directory Domain Controller (RPC)	Active Directory Domain S	er All	Yes	Allow	N .	
Active Directory Web Services (TCP-In)	Active Directory Web Servi	ces All	Yes	Allow	68	
💿 BranchCache Content Retrieval (HTTP-Ir	) BranchCache - Content Re	tr All	No	Allow	B (	
BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Ca	ch All	No	Allow	X	
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Disco	e All	No	Allow		
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow		
OM+ Remote Administration (DCOM-I	n) COM+ Remote Administra	ti All	No	Allow	?	
🔇 Core Networking - Destination Unreacha	Core Networking	All	Yes	Allow		
🔇 Core Networking - Destination Unreacha	Core Networking	All	Yes	Allow		
🕖 Core Networking - Dynamic Host Config	Core Networking	All	Yes	Allow		
🕜 Core Networking - Dynamic Host Config	Core Networking	All	Yes	Allow		
🕑 Core Networking - Internet Group Mana	Core Networking	All	Yes	Allow		
Ore Networking - IPHTTPS (TCP-In)	Core Networking	AII	Yes	Allow		
🕑 Core Networking - IPv6 (IPv6-In)	Core Networking	AII	Yes	Allow		
🕑 Core Networking - Multicast Listener Do	Core Networking	All	Yes	Allow		
< III > Cara Naturaking Multicast Listanar Ou	Cara Natworking	0.0	Var	Allow		
				>		