

Windows Firewall with Advanced Security Troubleshooting Guide: Diagnostics and Tools

Microsoft Corporation

Published: February 2010

Abstract

This document describes how Windows Firewall with Advanced Security and IPsec works, what the common troubleshooting situations are, and which tools you can use for troubleshooting.



The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

The Windows Firewall with Advanced Security Design Guide and Deployment Guide are for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft Windows Server, Windows 7, Windows Vista, and Windows XP are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Windows Firewall with Advanced Security Troubleshooting Guide: Diagnostics and Tools 5](#_Toc254332391)

[Topics in this article 5](#_Toc254332392)

[Tools and Procedures Used to Troubleshoot Windows Firewall 5](#_Toc254332393)

[Using Monitoring in Windows Firewall with Advanced Security 6](#_Toc254332394)

[Troubleshooting considerations for firewall rules 6](#_Toc254332395)

[Viewing Firewall and IPsec Events in Event Viewer 7](#_Toc254332396)

[Enabling Audit Events for Windows Firewall with Advanced Security 8](#_Toc254332397)

[Enable audit events for Windows Firewall with Advanced Security 8](#_Toc254332398)

[Viewing firewall and IPsec audit events in Event Viewer 9](#_Toc254332399)

[Configuring Firewall Log Files 10](#_Toc254332400)

[Configure the firewall log file for a profile 10](#_Toc254332401)

[Create netstat and tasklist text files 13](#_Toc254332402)

[Sample output of Tasklist.txt and Netstat.txt 14](#_Toc254332403)

[Verifying that Key Firewall and IPsec Services are Working 14](#_Toc254332404)

[Resetting the Defaults in Windows Firewall with Advanced Security 15](#_Toc254332405)

[Capturing Firewall and IPsec Events with Netsh WFP 16](#_Toc254332406)

[Common Troubleshooting Situations using Windows Firewall with Advanced Security 17](#_Toc254332407)

[Windows Firewall Troubleshooting Situations 18](#_Toc254332408)

[Windows Firewall Is Blocking a Program 18](#_Toc254332409)

[Verify that Windows Firewall is enabled for your network location 18](#_Toc254332410)

[There is no active "allow" rule for the traffic 19](#_Toc254332411)

[There is an active "block" rule for the traffic 21](#_Toc254332412)

[Rules are evaluated in a specific order 21](#_Toc254332413)

[Group Policy does not allow local rules to be applied 23](#_Toc254332414)

[Rules that require connection security might be blocking traffic 23](#_Toc254332415)

[Mixed policies might cause dropped traffic 24](#_Toc254332416)

[Peer computer policy might cause dropped traffic 27](#_Toc254332417)

[Windows Firewall Is Turned off Every Time I Start My Computer 27](#_Toc254332418)

[Settings are managed by Group Policy 28](#_Toc254332419)

[Windows Live OneCare is installed 28](#_Toc254332420)

[Another (non-Microsoft) firewall program is installed 29](#_Toc254332421)

[Another program is stopping Windows Firewall 30](#_Toc254332422)

[I Need to Disable Windows Firewall 31](#_Toc254332423)

[I Cannot Configure Windows Firewall with Advanced Security 33](#_Toc254332424)

[Nobody Can Ping My Computer 33](#_Toc254332425)

[Nobody Can Access My Local File and Printer Shares 34](#_Toc254332426)

[I Cannot Remotely Administer Windows Firewall 35](#_Toc254332427)

[IPsec Troubleshooting Situations 35](#_Toc254332428)

[My IPsec-protected Computer Cannot Get an IP Address from DHCP 36](#_Toc254332429)

[IPsec Exemption for DHCPv4 36](#_Toc254332430)

[IPsec Exemption for DHCPv6 37](#_Toc254332431)

# Windows Firewall with Advanced Security Troubleshooting Guide: Diagnostics and Tools

Windows Firewall with Advanced Security, a Microsoft Management Console (MMC) snap-in, in Windows® 7, Windows Vista®, Windows Server® 2008 R2 and Windows Server® 2008 is a stateful, host-based firewall that filters incoming and outgoing connections based on its configuration. Windows Firewall with Advanced Security also supports an RFC-compliant implementation of Internet Protocol security (IPsec), IPsec and firewall configuration can now be done together in this snap-in. This article describes how Windows Firewall with Advanced Security works, what the common troubleshooting situations are, and which tools you can use for troubleshooting.

For a downloadable version of this article, go to the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=184045) at http://go.microsoft.com/fwlink/?LinkId=184045.

## Topics in this article

 [Tools and Procedures Used to Troubleshoot Windows Firewall](#ze53bd0a2c6054c869e81e77186619faa)

 [Common Troubleshooting Situations using Windows Firewall with Advanced Security](#z6d72b831d4c24158874a04e9e9d37c43)

# Tools and Procedures Used to Troubleshoot Windows Firewall

This section discusses tools and procedures used to troubleshoot Windows Firewall common situations. Topics include:

 [Using Monitoring in Windows Firewall with Advanced Security](#z06ea0ed2aa1a4f21ac2d09602e7f64d1)

 [Viewing Firewall and IPsec Events in Event Viewer](#z988f926069e7482f8fb5e9da33ea9634)

 [Enabling Audit Events for Windows Firewall with Advanced Security](#z934019e232624cf5a1b4805b3d7ef7d3)

 [Configuring Firewall Log Files](#zfabecbf98dd24b699b19f57268b3ae56)

 [Verifying that Key Firewall and IPsec Services are Working](#z172162311031486d929d0df598d65556)

 [Resetting the Defaults in Windows Firewall with Advanced Security](#z8451be41641c4dcfab7c8e0d143e236c)

 [Capturing Firewall and IPsec Events with Netsh WFP](#zfeab0be0a8a6445e945b92740dea8375)

# Using Monitoring in Windows Firewall with Advanced Security

The first step you typically take in troubleshooting a Windows Firewall or IPsec problem is to view which rules are currently being applied to the computer. Using the Monitoring node in Windows Firewall with Advanced Security enables you to see the rules currently being applied both locally and by Group Policy.

To open the Monitoring node in Windows Firewall with Advanced Security

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security MMC snap-in, in the navigation tree, select and then expand Monitoring.2. In the navigation tree, select Firewall to view the currently active inbound and outbound rules. You can double-click a rule to view its details.3. In the navigation tree, select Connection Security Rules to view the currently active connection security rules that implement IPsec requirements on network traffic. You can double-click a rule to view its details.4. For either Firewall or Connection Security Rules, you can determine where a rule came from. In the Actions pane, click View, and then click Add/Remove Columns. In the Available columns list, select Rule Source, click Add, position it in the Displayed columns list by clicking Move Up or Move Down, and then click OK. It can take a few seconds for the list to appear with the new information.5. In the navigation tree, expand Security Associations, and then select either Main Mode or Quick Mode to view the currently active security associations that are established between the local computer and various remote computers.6. In each |

## Troubleshooting considerations for firewall rules

 Only one firewall rule is used to determine if a network packet is allowed or dropped. If the network packet matches multiple rules, then the rule that is used is selected using the following precedence:

 Rules that specify the action Allow if Secure and also the option Block Override

 Rules that specify the action Block

 Rules that specify the action Allow

 Only currently active rules are displayed in the Monitoring node. Rules might not appear in the list if:

 The rule is disabled.

 If the default inbound or outbound firewall behavior is configured to allow traffic that is not blocked by a rule, then allow rules of the specified direction are not displayed.

 By default, the firewall rules in the groups identified in the following list are enabled. Additional rules might be enabled when you install certain Windows Features or programs.

 Core Networking – all profiles

 Remote Assistance – DCOM and RA Server TCP rules for domain profile only, other rules for both domain and private profiles

 Network Discovery – private profile only

# Viewing Firewall and IPsec Events in Event Viewer

Note

This topic applies to computers that are running Windows 7 and Windows Server 2008 R2 only. To view firewall and IPsec events on computers that are running previous versions of Windows, see [Enabling Audit Events for Windows Firewall with Advanced Security](#z934019e232624cf5a1b4805b3d7ef7d3)

Windows 7 and Windows Server 2008 R2 automatically log significant firewall and IPsec events in the computer’s event log. You can view events in the log by using Event Viewer.

To view events for Windows Firewall with Advanced Security in Event Viewer

|  |
| --- |
| 1. Event Viewer is available as part of Computer Management. Click Start, right-click Computer, and then click Manage. Under System Tools, click Event Viewer.2. In the navigation tree, expand Event Viewer, expand Applications and Services, expand Microsoft, expand Windows, and then expand Windows Firewall with Advanced Security.3. There are four views of operational events provided: ConnectionSecurity. This log maintains events that relate to the configuration of IPsec rules and settings. For example, when a connection security rule is added or removed or the settings of IPsec are modified, an event is added here. ConnectionSecurityVerbose. This log maintains events that relate to the operational state of the IPsec engine. For example, when a connection security rule become active or when crypto sets are added or removed, an event is added here. This log is disabled by default. To enable this log, right-click ConnectionSecurityVerbose, and then click Enable Log. Firewall. This log maintains events that relate to the configuration of Windows Firewall. For example, when a rule is added, removed, or modified, or when a network interface changes its profile, an event is added here. FirewallVerbose. This log maintains events that relate to the operational state of the firewall. For example, when a firewall rule become active, or when the settings of a profile are changed, an event is added here. This log is disabled by default. To enable this log, right-click FirewallVerbose, and then click Enable Log.4. Each event includes a General tab that summarizes the information contained in the event. For more information about an event, click Event Log Online Help to open a web page in the Windows Server Technical Library that contains detailed information and prescriptive guidance.The event also includes a Details tab that displays the raw data associated with the event. You can copy and paste the information in the Details tab by selecting the text (CTRL+A selects it all) and then pressing CTRL-C. |

# Enabling Audit Events for Windows Firewall with Advanced Security

Important

The information in this topic is useful mainly to computers that are running Microsoft® Windows Vista® and Windows Server® 2008. Although the audit events are available in Windows® 7 or Windows Server® 2008 R2, it is more effective to use the operational event logging supported by those versions of Windows. For more information, see [Viewing Firewall and IPsec Events in Event Viewer](#z988f926069e7482f8fb5e9da33ea9634).

By default, Windows Firewall with Advanced Security in Windows Vista and Windows Server 2008 does not log anything in the Event Viewer log. The events that can be logged by Windows Firewall with Advanced Security are called “audit” events, and must be enabled. Once enabled, the events generated by Windows Firewall with Advanced Security can be viewed in Event Viewer.

 [Enable audit events in Windows Firewall with Advanced Security](#z1)

 [Viewing firewall and IPsec audit events in Event Viewer](#z2)

For more information about events that are generated by Windows Firewall with Advanced Security, see Event IDs Used by Windows Firewall with Advanced Security

## Enable audit events for Windows Firewall with Advanced Security

To enable audit events, use auditpol.exe, a command-line tool that modifies audit polices of the local computer. You can use the auditpol command-line tool to enable or disable the various categories and subcategories of events and then view the events in the Event Viewer snap-in.

 To get the list of event categories recognized by the auditpol tool, type the following at the command prompt:

auditpol.exe /list /category

 To get the list of subcategories under a category (this example uses the category Policy Change), type the following at the command prompt:

auditpol.exe /list /category:"Policy Change"

 To set a category and a subcategory to enable, type the following at the command prompt:

auditpol.exe /set /category:"CategoryName" /SubCategory:"SubcategoryName"

An example of setting a category and subcategory to enable is:

auditpol.exe /set /category:"Policy Change" /subcategory:"MPSSVC rule-level Policy Change" /success:enable /failure:enable

The events generated by Windows Firewall with Advanced Security span several categories and subcategories. Consider creating a batch file with the auditpol commands that you want that you can use to enable and disable audit events as needed. The following table lists event categories and subcategories that are relevant to troubleshooting Windows Firewall with Advanced Security.

|  |  |
| --- | --- |
| Category | Subcategories |
| Policy Change | **** MPSSVC rule-level policy change**** Filtering Platform policy change |
| Logon/Logoff | **** IPsec Main Mode**** IPsec Quick Mode **** IPsec Extended Mode  |
| System | **** IPsec Driver**** Other system events  |
| Object Access | **** Filtering Platform packet drop **** Filtering Platform connection  |

When you change audit policy settings, for changes to take effect, you must either restart the computer or force a manual policy refresh. You can force a manual refresh by typing the following command at the command prompt:

gpupdate /force

After you are done troubleshooting, you can disable the events by changing the enable settings above to disable and rerunning the commands.

## Viewing firewall and IPsec audit events in Event Viewer

Once the audit events are enabled, use Event Viewer to view the events in the Security event log.

To view firewall and IPsec audit events in Event Viewer

|  |
| --- |
| 1. Click Start, click Control Panel, click System and Maintenance (on Windows Vista and Windows Server 2008) or System and Security (on Windows 7 and Windows Server 2008 R2), and then under Administrative Tools click View event logs.2. In Event Viewer, expand Windows Logs and then click Security. In the details pane, you can view the security-related audit events. The list of logged events is displayed at the top of the details pane. Clicking an event in the list displays more detailed information in the bottom of the Details pane. The General tab gives a description of the event in friendly text. The Details tab gives you the option to view the details of the event in either Friendly View or XML View. If you need more information about an event, on the General tab, click Event Log Online Help. |

# Configuring Firewall Log Files

You can enable logging in Windows Firewall with Advanced Security to create a text file that contains information about which network connections the firewall allows and drops. You can create the following types of log files:

 [Configure the firewall log file for a profile](#z3)

 Create netstat and tasklist text files

## Configure the firewall log file for a profile

Before you can view firewall logs, you must configure Windows Firewall with Advanced Security to create log files.

To configure logging for a Windows Firewall with Advanced Security profile

|  |
| --- |
| 1. In the console tree of the Windows Firewall with Advanced Security snap-in, click Windows Firewall with Advanced Security, and then click Properties in the Actions pane.2. Click the tab of the profile for which you want to configure logging (Domain, Private, or Public), and then click Customize.3. Specify a name and location.4. Specify a log file size limit (Between 1 and 32767 Kbytes).5. Click Yes for Log dropped packets.6. Click Yes for Log successful connections and then click OK. |

To view the firewall log file

Open Explorer to the path and filename you chose in the previous procedure, "To configure logging for a profile". To access the firewall log, you must be an administrator of the local computer.Windows Firewall with Advanced Security

You can view the log file in Notepad or any program that can open a text file.

Interpreting the firewall log file

The following log information is collected. Some data in the log file applies to only certain protocols (TCP flags, ICMP type and code, etc.), and some data applies only to dropped packets (size).

|  |  |  |
| --- | --- | --- |
| Fields | Description | Example |
| Date | Displays the year, month, and day that the recorded transaction occurred. Dates are recorded in the format YYYY-MM-DD, where YYYY is the year, MM is the month, and DD is the day. | 2006-3-27 |
| Time | Displays the hour, minute, and second when the recorded transaction occurred. Times are recorded in the format: HH:MM:SS, where HH is the hour in 24-hour format, MM is the minute, and SS is the second. | 21:36:59 |
| Action | Indicates the operation that was observed by the firewall. The actions available to the firewall are OPEN, CLOSE, DROP, and INFO-EVENTS-LOST. An INFO-EVENTS-LOST action indicates the number of events that occurred but that were not recorded in the log. | OPEN |
| Protocol | Displays the protocol that was used for the communication. A protocol entry can also be a number for packets that are not using TCP, UDP, or ICMP. | TCP |
| src-ip | Displays the IP address of the sending computer. | XXX.XXX.X.XX |
| dst-ip | Displays the IP address of the destination computer. | XXX.XXX.X.XX |
| src-port | Displays the source port number of the sending computer. A src-port entry is recorded in the form of a whole number, between 1 and 65,535. Only TCP and UDP display a valid src-port entry. All other protocols display a src-port entry of -. | 4039 |
| dst-port | Displays the port number of the destination computer. A dst-port entry is recorded in the form of a whole number, between 1 and 65,535. Only TCP and UDP display a valid dst-port entry. All other protocols display a dst-port entry of -. | 53 |
| size | Displays the packet size in bytes. | - |
| tcpflags | Displays the TCP control flags that are found in the TCP header of an IP packet:**** Ack. Acknowledgment field significant**** Fin. No more data from sender**** Psh. Push function**** Rst. Reset the connection**** Syn. Synchronize sequence numbers**** Urg. Urgent Pointer field significant A flag appears as a single uppercase initial of the flagname. For example, the Fin flag appears as F, the single uppercase initial of the flagname. | AFP |
| tcpsyn | Displays the TCP sequence number in the packet. | 1315819770 |
| tcpack | Displays the TCP acknowledgment number in the packet. | 0 |
| tcpwin | Displays the TCP window size of the packet in bytes. | 64240 |
| icmptype | Displays a number that represents the Type field of the ICMP message. | 8 |
| icmpcode | Displays a number that represents the Code field of the ICMP message. | 0 |
| info | Displays an information entry that depends on the type of action that occurred. For example, an INFO-EVENTS-LOST action creates an entry for the number of events that occurred but were not recorded in the log since the time of the last occurrence of this event type. | 23 |

Note

A hyphen (-) is used for fields where no information is available for an entry.

## Create netstat and tasklist text files

You can create two custom log files, one to view network statistics (lists all listening ports) and the other to view the task list of either programs or services. The task list will provide the process identifier (PID) of the event which you can look up in the network statistics file for details. The procedure to create these two files is as follows:

To create network statistics and task list text files

|  |
| --- |
| 1. At the command prompt, type netstat -ano > netstat.txt, and then press ENTER.2. At the command prompt, type tasklist > tasklist.txt, and then press ENTER. If you want to create a text file for services rather than programs, at the command prompt, type tasklist /svc > tasklist.txt.3. Open the tasklist.txt and the netstat.txt files. 4. In the tasklist.txt file, write down the Process Identifier (PID) for the process you are troubleshooting. Compare the PID with that in the Netstat.txt file. Write down the protocol that is used. The information about the protocol used can be useful when reviewing the information in the firewall log file. |

### Sample output of Tasklist.txt and Netstat.txt

Netstat.txt

Proto Local Address Foreign Address State PID

TCP 0.0.0.0:XXX 0.0.0.0:0 LISTENING 122

TCP 0.0.0.0:XXXXX 0.0.0.0:0 LISTENING 322

Tasklist.txt

Image Name PID Session Name Session# Mem Usage

==================== ======== ================ =========== ============

svchost.exe 122 Services 0 7,172 K

XzzRpc.exe 322 Services 0 5,104 K

Note

The actual IP addresses have been changed to (X), and RPC service to (z).

# Verifying that Key Firewall and IPsec Services are Working

For Windows Firewall with Advanced Security to operate correctly, the following services must be started:

 Base Filtering Engine

 Group Policy Client

 IKE and AuthIP IPsec Keying Modules

 IP Helper

 IPsec Policy Agent

 Network Location Awareness

 Network List Service

 Windows Firewall

To open the Services snap-in and verify that services are started

|  |
| --- |
| 1. Click Start and click Control Panel.2. Click System and Maintenance.3. Scroll to and click Administrative Tools.4. Double-click Services.5. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.6. Verify that the services listed above are started. If one or more of the services are not started, right-click the service name in the list, and then click Start. |

# Resetting the Defaults in Windows Firewall with Advanced Security

As a last resort, you may want to restore Windows Firewall with Advanced Security defaults. When you restore default settings, you lose all settings, all firewall rules, and all IPsec connection security rules configured locally on the computer after Windows was installed. Group Policy applied rules and settings are not disturbed. The loss of locally defined rules might cause some programs to stop working that depend on certain rules or settings. Also, if you are remotely managing this computer, the connection is lost when you restore defaults.

Before resetting the Windows Firewall with Advanced Security defaults, make sure that you save the current firewall state. This allows you to restore your settings if necessary.

The steps to save the firewall state and reset Windows Firewall with Advanced Security to its default configuration are as follows:

To save the current firewall state

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security MMC snap-in, click Export Policy in the Actions pane.2. In the Save As property sheet, provide a name and path for the export file.3. Click Save. |

Note

You can use the Import Policy option in the Actions pane to reapply your saved configuration.

To restore Windows Firewall with Advanced Security to its default configuration

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security snap-in, click Restore Defaults in the Actions pane.2. At the Windows Firewall with Advanced Security prompt, click Yes to restore firewall defaults.  |

# Capturing Firewall and IPsec Events with Netsh WFP

Windows 7 and Windows Server 2008 R2 introduce the new netsh wfp context that enables you to capture diagnostic trace sessions of the behavior of the Windows Filtering Platform which is the base engine that implements your firewall and connection security rules. Starting a capture session, reproducing the problem, and then stopping the capture results in a log that can help you or Microsoft Customer Support Services (CSS) troubleshoot connectivity problems on your computers.

To capture a Netsh WFP diagnostics session

|  |
| --- |
| 1. Open a command prompt with Administrator permissions.2. At the command prompt, change the current folder to your desktop by running the command: cd %userprofile%\desktop3. To start the capture, run the command netsh wfp capture start.4. Reproduce the networking problem whose cause you are trying to diagnose.5. To complete the capture, run the command netsh wfp capture stop. The output file is stored in the current folder. |

To view the WFP diagnostic data

|  |
| --- |
| 1. In Explorer, double-click the .cab file that you created in the previous procedure.2. The .cab file contains an .xml file and an .etl file. The .etl file is a binary file that is intended for use by CSS. The .xml file can be loaded and read locally. Because of the size of the .xml files produced by this process we recommend that you acquire an XML Reader program, instead of using a Web browser or Notepad to open the file. Several good ones are available for free download on the Web.3. Drag the wfpdiag.xml file from the .cab file to the desktop.4. Open the file with your XML reader of choice and examine the contents. Note the main sections: sysInfo – This section contains information about the computer on which the trace was captured. initialState – This section contains information about the state of the WFP and the currently configured rules before the problem was reproduced. Events – This section contains information about things that occurred while the capture session was running. finalState – This section contains the same information as initialState, but was captured when you ran the wfp capture stop command. You can directly compare the two sections to look for differences that might relate to the connection problem you are trying to diagnose. |

Similarly, you can use the netsh trace and netsh trace stop commands to capture a variety of diagnostic information customized to a selected scenario, such as wfp-ipsec.

To capture a Netsh Trace diagnostics section

|  |
| --- |
| 1. At an Administrator: Command Prompt, run the command netsh trace start scenario=wfp-ipsec tracefile=%userprofile%\desktop\SampleTrace.cabSubstitute a path a filename appropriate to your environment.2. The output of the command shows you that the trace is running, the file to which the data is written, and details of other possible parameters.3. Reproduce the problem whose cause you are trying to diagnose.4. run the command netsh trace stop.The computer takes a few moments to compile the collected trace data into a .cab file at your specified location.5. Open Windows Explorer, browse to the folder you specified, and double-click the .cab file, and examine its contents. A variety of text files, .xml files, event log files, and other types are included. |

# Common Troubleshooting Situations using Windows Firewall with Advanced Security

The following are common problems encountered when using Windows Firewall with Advanced Security. Select the description that most closely matches your problem.

 [Windows Firewall Is Blocking a Program](#z9c9fbd4c3a014a8d903a7e4f2ecae627)

 [Windows Firewall Is Turned off Every Time I Start My Computer](#z54d58a7adf444c68b26f499180af5dbe)

 [I Need to Disable Windows Firewall](#zc96976ff4bce4c3b9bf869f686117982)

 [I Cannot Configure Windows Firewall with Advanced Security](#z6845184392db49c487708fcae0bf8845)

 [Nobody Can Ping My Computer](#z5a8f9b091fed4878b7a7d46944f181bc)

 [Nobody Can Access My Local File and Printer Shares](#z62c9f18750144332a9fd5d83e71c3b85)

 [I Cannot Remotely Administer Windows Firewall](#zb56b15c5e11d4e3cb7f2174a74e45a5c)

 [My IPsec-protected Computer Cannot Get an IP Address from DHCP](#ze3ae18d6da61414bb56d7f0d9e3fa699)

# Windows Firewall Troubleshooting Situations

# Windows Firewall Is Blocking a Program

One of the most common problems when using a network firewall is that it sometimes blocks network traffic that you want to allow. The following sections discuss reasons that the firewall might be blocking traffic.

## Verify that Windows Firewall is enabled for your network location

The first step in diagnosing dropped or blocked traffic situations is to determine if the firewall is turned on and which network location profile is active: domain, private, or public.

To verify that the firewall is enabled for the current network location profile

|  |
| --- |
|  Perform either of the following: At a command prompt, run the command:netsh advfirewall show currentprofileThe first line of the output indicates the currently active network location profile. The second line of the output indicates if the firewall is on or off for the currently active network location profile. For example:C>netsh advfirewall show currentprofileDomain Profile Settings:-------------------------------------------------------State ONFirewall Policy BlockInbound,AllowOutbound… Click Start, click Control Panel, click Network and Internet, and then click Windows Firewall. The details pane indicates if the firewall is on or off. The entry for Network location indicates the currently active network location profile. |

Most of the procedures that follow use the Windows Firewall with Advanced Security MMC snap-in, rather than the Windows Firewall Control Panel program.

To start the Windows Firewall with Advanced Security MMC snap-in

|  |
| --- |
|  Do one of the following: Click Start, click All Programs, click Administrative Tools, and then click Windows Firewall with Advanced Security. At a command prompt, run the command:wf.msc |

## There is no active "allow" rule for the traffic

By default, Windows Firewall with Advanced Security blocks all unsolicited inbound network traffic, and allows all outbound network traffic. For unsolicited inbound network traffic to reach your computer, you must create an allow rule to permit that type of network traffic. If a network program cannot get access, verify that in the Windows Firewall with Advanced Security snap-in there is an active allow rule for the current profile. To verify that there is an active allow rule, double-click Monitoring and then click Firewall .If there is no active allow rule for the program, go to the Inbound Rules node and create a new rule for that program. Create either a program rule, or a service rule, or search for a group that applies to the feature and make sure all the rules in the group are enabled.

To permit the traffic, you must create a rule for the program that needs to listen for that traffic. If you know the TCP or UDP port numbers required by the program, you can additionally restrict the rule to only those ports, reducing the vulnerability of opening up all ports for the program.

Note

By default on Windows Vista, when the firewall detects a new program trying to listen on a network port, the firewall displays a pop-up message asking if the user wants to permit the program to listen. If the user approves, and has either Administrator or Network Operator permissions, then the program exception rule is created automatically with no further action from the user. On Windows Server 2008, the pop-up message does not display by default, and so the administrator must manually create or enable the appropriate inbound rules for the program.

To add an inbound rule for a program by using the Windows Firewall Control Panel program

|  |
| --- |
| 1. Click Start, click Control Panel, and then under Security, click Allow a program through Windows Firewall.2. On the Exceptions tab, check the list to see if an exception for your program already exists and just needs to be enabled. If you find one, select the box next to it, and then click OK. 3. If a rule does not already exist, click Add program.4. In the Add a Program dialog box, either select your program from the list, or click the Browse button to enter the path to the executable file.5. If the program should only be accessed from certain network addresses, click Change Scope, and enter the appropriate subnet addresses or individual IP addresses. Click OK to return to the Add a Program dialog box.6. Click OK to return to the Windows Firewall Settings dialog box. Your new exception is displayed in the list in alphabetical order with a check mark in the box next to it. Click OK to save your new exception rule.7. Test your rule by running the network program that needs to be able to receive unsolicited network traffic. |

To add an inbound rule for a program by using the Windows Firewall with Advanced Security MMC snap-in

|  |
| --- |
| 1. Click Start, click All Programs, click Administrative Tools, and then click Windows Firewall with Advanced Security.2. Click Inbound Rules and examine the list to see if an allow rule that meets your requirements already exists and just needs to be enabled. Disabled rules have a grey icon next to them, while enabled rules are red, green or yellow. The Enabled column also indicates Yes or No.3. If you find a rule in the list, enable it by right-clicking the rule name, and then clicking Enable rule.4. If a rule does not already exist, then create a new rule for your program by following these steps:a. In the navigation pane, select Inbound Rules.b. In the Actions pane, click New Rule.c. On the Rule Type page, select Program, and then click Next.d. On the Program page, select This program path, then click Browse, and navigate to the program you want to be able to receive inbound network traffic. Click Next to continue.e. On the Action page, select Allow the connection, and then click Next.f. On the Profile page, select the profiles to which this rule should apply, and then click Next.g. On the Name page, type a name and a description for the rule.The rule is created and automatically enabled.h. Test your rule by running the network program that needs to be able to receive unsolicited network traffic. |

## There is an active "block" rule for the traffic

By default, Windows Firewall with Advanced Security blocks all unsolicited inbound network traffic, and allows all outbound network traffic. For network programs on your computer to send information to the network, you typically do not need to do anything. The default configuration of the firewall permits all outbound traffic. If a block rule is active, it can prevent network packets that match its criteria from being sent. A block rule can be present in either the Inbound Rules or Outbound Rules lists.

To check if an active block rule exists, and disable it if found

|  |
| --- |
| 1. Click Start, click All Programs, click Administrative Tools, and then click Windows Firewall with Advanced Security.2. Double-click Monitoring, and then click Firewall.The list of currently defined and active rules is displayed.3. If you find a rule that you suspect is interfering with required network traffic, note the value in the Direction column, Inbound or Outbound.4. In the navigation pane, click Inbound Rules or Outbound Rules, depending on the value you found in step 3.5. Right-click the suspect rule in the list, and then click Disable rule. We recommend that you do not disable the rule until you verify that it indeed was the offending rule, and that disabling it did not adversely affect other network traffic. |

## Rules are evaluated in a specific order

Windows Firewall with Advanced Security evaluates its rules in a specific order. A network packet might match several rules, and the order in which the rules are evaluated determines which rule applies to the packet.

|  |  |  |
| --- | --- | --- |
| Order number | Rule type | Description |
| 1 | Windows Service Hardening | This type of rule restricts services from establishing connections. Service restrictions are configured out-of-the-box so that Windows Services can only communicate in specific ways (i.e., restricting allowable traffic through a specific port) but until you create a firewall rule, traffic is not allowed.Independent software vendors can make use of public Windows Service Hardening APIs to restrict their own services. |
| 2 | Connection security rules  | This type of rule defines how and in which circumstances computers authenticate using IPsec. Connection security rules are used in establishing server and domain isolation, as well as in enforcing Network Access Protection (NAP) policy. |
| 3 | Authenticated bypass rules | This type of rule allows the connection of particular computers if the traffic is protected with IPsec, regardless of other inbound rules in place. Specified computers are allowed to bypass inbound rules that block traffic: examples of this are vulnerability scanners, programs that scan other programs, computers, and networks for weaknesses. |
| 4 | Block rules | This type of rule explicitly blocks a particular type of incoming or outgoing traffic. |
| 5 | Allow rules | This type of rule explicitly allows a particular type of incoming or outgoing traffic. |
| 6 | Default rules | These rules define the action that takes place when a connection does not meet any of the parameters of a higher order rule. Out-of-the-box, the inbound default is to block connections, and the outbound default is to allow connections. |

Within each rule category listed in the preceding table, rules are matched by the degree of their specificity. For example, rule 1 and rule 2 are both in the same category. If rule 1 has parameters A and B specified and rule 2 has parameters A, B, and C specified, then rule 2 will be evaluated first. The first rule that is evaluated and matches all criteria is the rule applied to the network packet.

## Group Policy does not allow local rules to be applied

When configuring the Windows Firewall with Advanced Security policy through Group Policy, the administrator can specify whether or not firewall or connection security rules created by local administrators are applied. If you have created a local firewall or connection security rule and it is not appearing in the corresponding monitoring node, this may be the reason.

To verify why local firewall and connection security rules do not appear in Monitoring

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security snap-in, click Properties.2. Click the tab corresponding to the active profile.3. Click Customize in the Settings section.4. The Rule Merge section will tell you if local rules are applied. |

## Rules that require connection security might be blocking traffic

When you create an inbound or outbound firewall rule, one of the options for action is to Allow only secure connections. When you specify this option, you need to have a connection security rule or separate IPsec policy that causes the traffic to be secured. Otherwise, the traffic is always dropped.

To verify whether the rule or rules for your program require security

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security snap-in, click the Inbound Rules in the tree. Select the rule you wan to verify and then click Properties in the Actions pane. 2. Click the General tab and under Action verify that Allow only secure connections is selected.3. If the rule has the action Allow only secure connections, click Monitoring in the tree and then Connection Security Rules. Verify whether there are appropriate connection security rules in place to secure the traffic specified by the firewall rule.Warning If you have an active IP Security Policies policy, ensure that policy secures the desired traffic. Do not create connection security rules because the IP Security Policies policy and the connection security rules can conflict. |

An outbound connection isn't being allowed.

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security snap-in, click Monitoring. Expand the section for the active profile and verify under Firewall State that outbound connections that do not match a rule are allowed.2. Under Monitoring, click Firewall to verify that the outbound connection you want to allow does not have a block rule.  |

## Mixed policies might cause dropped traffic

There are several interfaces in Windows that allow you to configure firewall and IPsec settings. Creating policies in multiple places can lead to conflicts that block traffic. The following configuration points are available:

 Windows Firewall with Advanced Security. This policy is configured through the Windows Firewall with Advanced Security snap-in either locally or as part of a Group Policy. This policy configures both firewall and IPsec settings for computers running Windows Vista and Windows Server 2008.

 Windows Firewall Administrative Template. This policy is configured through the Group Policy Management Editor under Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall. This interface contains the Windows Firewall settings that were available prior to Windows Vista and Windows Server 2008 and should be used when configuring a Group Policy object that controls earlier versions of Windows. These settings can be applied to computers running Windows Vista or Windows Server 2008, but it is recommended that you use the Windows Firewall with Advanced Security policy instead as it offers more flexibility and security. Note that some of the domain profile settings are shared between the Windows Firewall Administrative Template and the Windows Firewall with Advanced Security policy, so you can expect to see settings here if you have configured domain profiles settings in the Windows Firewall with Advanced Security snap-in.

 IP Security Policies. This policy is configured through the IP Security Policies snap-in either locally or through the Group Policy Management Editor under Computer Configuration\Windows Settings\Security Settings\IP Security Policies. This policy configures IPsec settings that can be understood by earlier versions of Windows as well as Windows Vista and Windows Server 2008. You should not apply this policy and connection security rules from the Windows Firewall with Advanced Security policy on the same computer.

To view all these settings in their appropriate snap-ins create a custom MMC snap-in and add the Windows Firewall with Advanced Security snap-in, Group Policy Management snap-in, and the IP Security Monitor snap-in.

To create a custom MMC snap-in console

|  |
| --- |
| 1. Click Start, click All Programs, click Accessories, and then click Run.2. In the Open text box, type mmc, and then press ENTER.3. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.4. On the File menu, click Add/Remove Snap-in.5. In the Available snap-ins list box, click Windows Firewall with Advanced Security, then click Add.6. Click OK.7. Repeat steps 1 through 6 to add Group Policy Management snap-in and IP Security Monitor.8. Before you close the snap-in, save and name the custom console for future use. |

To verify which policies are active for the active profile, use the following procedure.

To verify which policies are applied

|  |
| --- |
| 1. At the command prompt, type mmc, and then press ENTER.2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.3. On the File menu, click Add/Remove Snap-in.4. In the Available snap-ins list box, click Group Policy Management, then click Add.5. Click OK.6. In the tree, click the subnode (usually the forest in which the local computer resides) and click double-click Group Policy Results in the Detail pane.7. In the Actions pane, click More Actions and click Group Policy Results Wizard.8. Click Next. Click This computer or Another computer (type the computer name and path or click browse to locate it). Click Next again.9. Click Display policy settings for either Current user or Click a specific user. If you do not want to display settings for user policy and want to display computer policy settings only, click Do not display user policy settings in the results (display computer policy settings only), click Next, and Next again.10. Click Finish. Group Policy Results will generate a report in the Details pane. The report tabs include: Summary, Settings, and Policy Events.11. To make sure there is not a conflicting IP Security Policies policy, after the reports are generated, use the Settings tab and locate Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory. If that last node is not present, then there is no policy from the IPsec Policy Agent. If the last node is present, the policy name, description, and Group Policy object (GPO) from which the policy originated is displayed. If you have both an IP Security Policies policy and a Windows Firewall with Advanced Security policy using connection security rules, then your connectivity issue could be a result of policy conflicts. We recommend using one policy or the other, but not both. It is fine to use IP Security Policies and Inbound or Outbound rules from Windows Firewall with Advanced Security. Policy conflicts can arise and troubleshooting can become more difficult if settings are configured in one place and not considered when configured in another.There could still be conflicting policies from local Group Policy objects or from scripts your IT department may have run. Verify all IPsec policies using IP Security Monitor or at the command prompt type the following command:netsh ipsec dynamic show all12. To see the settings applied by the Windows Firewall Administrative Template, see Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall.13. In the same console, you can look at the Policy Events tab to see if there have been any recent issues applying policy.14. To see which policy is applied by Windows Firewall with Advanced Security, open the snap-in for the computer you are troubleshooting and review the settings in Monitoring.  |

To view Administrative Templates, open the Group Policy Management snap-in and under Group Policy Results, verify if any legacy settings are being applied that might be causing traffic to be blocked.

To view IP Security Policies, open the IP Security Monitor snap-in. Click the local computer in the tree. In the Detail pane, click either Active Policy, Main Mode or Quick Mode. Search for any competing policies that might be causing traffic to be blocked.

By using Monitoring in the Windows Firewall with Advanced Security snap-in, you can see rules that are currently being applied from both local and Group Policy. See "Use monitoring in the Windows Firewall with Advanced Security snap-in" later in this document for more details.

If there are no IPsec rules configured in Windows Firewall with Advanced Security, stop IPsec Policy Agent. This will allow you to see if dropped traffic results from IPsec or Windows Firewall.

To stop IPsec Policy Agent

|  |
| --- |
| 1. Click Start and click Control Panel.2. Click System and Maintenance and click Administrative Tools.3. Double-click Services and at the User Account Control prompt, supply the correct credentials if required. Click Continue.4. Locate IPsec Policy Agent in the list of services and verify in the Status column that the service is started. 5. If the IPsec Policy Agent is started, right click IPsec Policy Agent, and then click Stop. Alternatively, you can stop the IPsec Policy Agent at the command prompt by typing net stop policy agent. |

## Peer computer policy might cause dropped traffic

For communications to be established using IPsec, both computers must have compatible IPsec policies. This policy can be specified through connection security rules in Windows Firewall with Advanced Security, through the IP Security Policies snap-in, or through another IPsec provider.

Peer computer may not have a complimentary policy

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security snap-in, click Monitoring and Connection Security Rules to verify whether both peers have an IPsec policy configured. 2. If a peer computer is running an earlier version of Windows than Windows Vista, verify that at least one Main Mode cryptographic suite and one Quick Mode cryptographic suite use algorithms that are supported on both peers. a. Click Main Mode, click the connection you want to check in the Details pane, then click Properties in the Actions Pane. View the connection details for both peers to verify that they are compatible.b. Repeat step 2a, this time substituting Quick Mode. View the connection details for both peers to verify that they are compatible.3. If Kerberos V5 authentication is used, verify that the peer is in the same domain or in a trusted domain.4. If a certificate is used, verify that it has the appropriate flags. Certificates that use Internet Key Exchange (IKE) only require digital signature as a usage type. Certificates that use AuthIP need client authentication (and depending on the scenario server authentication) as a usage type. For more details on AuthIP certificates see "AuthIP in Windows Vista" (<http://go.microsoft.com/fwlink/?LinkId=76867>) on the Microsoft Web site. |

# Windows Firewall Is Turned off Every Time I Start My Computer

It is important to have a software-based firewall running on any computer that is connected to a network. Windows Firewall is included in the Windows Vista and Windows Server 2008 operating systems. If Windows Firewall is not running, and you think it should be, the following are possible causes:

 [Settings are managed by Group Policy](#z5)

 [Windows Live OneCare is installed](#z6)

 [Another (non-Microsoft) firewall program is installed](#z7)

 [Another program is stopping Windows Firewall](#z8)

## Settings are managed by Group Policy

If your computer is connected to an organization’s network, then the network administrator might be managing some of the settings on your computer. For example, on a network that uses Active Directory Domain Services (AD DS), the administrator can use Group Policy to centrally configure computer settings. This means the user typically cannot change the settings. If Windows Firewall is managed on your network in this way, then the Windows Firewall Control Panel and the Windows Firewall with Advanced Security Microsoft Management Console (MMC) snap-in both display a banner similar to the following:

The banner displayed when settings are controlled by Group Policy



For more information, contact your network administrator about Group Policy settings that affect Windows Firewall.

## Windows Live OneCare is installed

When Windows Live OneCare is installed, it disables Windows Firewall and uses a firewall that is included with and managed by OneCare instead. OneCare registers this firewall with the Windows Security Center as the firewall provided for your computer. You cannot enable Windows Firewall while the OneCare firewall is installed. Use Windows Security Center to confirm that a firewall program is installed and operating on your computer.

To use Windows Security Center to confirm that a firewall is running

|  |
| --- |
|  The Windows Security Center runs in the background and monitors the state of security software on your computer. Start the Windows Security Center by clicking Start, and then typing Security Center in the Start Search box. Double-click Security Center when it appears on the Start menu.If Windows Security Center detects that a firewall is not present or is not turned on, then the Firewall section of the window is expanded, and displays a red banner with a warning that a firewall program was not detected.If Windows Security Center detects that a firewall is present and is not turned on, then the Firewall section of the window is highlighted in green, and is not expanded by default. If you click the green banner to expand the Firewall section, it displays information about the state of the currently active firewall program, similar to the following:The banner displayed when Windows Live OneCare is installedNote The Windows Security Center only runs on client versions of the Windows operating system, such as Windows XP with Service Pack 2 (SP2) and Windows Vista with SP1. |

## Another (non-Microsoft) firewall program is installed

Windows Firewall is an important component in a “defense-in-depth” strategy in which multiple components are used in layers to help protect your computer. However, the use of multiple firewalls can cause problems. If the exception rules on both firewalls do not match exactly, then network traffic can be blocked, and programs will not work as expected. If you install a non-Microsoft firewall program, or if one was installed on your computer by the manufacturer, then that firewall program can disable Windows Firewall to prevent a conflict. If you want to continue to use the non-Microsoft firewall program, then keep Windows Firewall turned off.

If you want to continue to use the non-Microsoft firewall program and Windows Firewall together, then contact the program’s vendor to inquire if side-by-side use of these firewalls is supported, and if so, how to prevent the program from turning off Windows Firewall.

If you want to use Windows Firewall instead, uninstall the non-Microsoft firewall program, and then follow the steps in either of the following procedures.

To enable Windows Firewall by using Control Panel

|  |
| --- |
| 1. To remove the non-Microsoft firewall program, click Start, click Control Panel, and then in Control Panel Home, click Uninstall a Program. Click the non-Microsoft firewall program in the list, and then click Uninstall. Follow the directions on your screen to finish uninstalling the program.2. On the main Control Panel window, click Security, and then click Turn Windows Firewall on or off.3. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.4. In the Windows Firewall Settings dialog box, on the General tab, click On (recommended), and then click OK. |

To enable Windows Firewall by using the Windows Security Center

|  |
| --- |
| 1. The Windows Security Center runs in the background and monitors the state of security software on your computer. If the Windows Security Center detects a problem, it displays a red shield icon in the notification area of the Start menu. Double-click the shield to open the Windows Security Center program. If the red shield icon does not appear, you can start the Windows Security Center by clicking Start, and then typing Security Center in the Start Search box. Click Security Center when it appears on the Start menu.Note The Windows Security Center only runs on client versions of the Windows operating system, such as Windows XP with Service Pack 2 (SP2) and Windows Vista with SP1.2. If Windows Security Center detects that a firewall is not present or is not turned on, then the Firewall section of the window is expanded, and a Turn on now button appears. Do one of the following: To turn on Windows Firewall, click Turn on now, and then in the User Account Control dialog box, click Continue. To find a firewall program from another software maker, click Show me my available options, and then click Go online to get a different firewall program.Internet Explorer will open to a page that displays links to security vendors that offer firewall software programs. To turn off the warning (not recommended), click Show me my available options, and then click I have a firewall program that I’ll monitor myself. In the User Account Control dialog box, click Continue to approve the change. |

## Another program is stopping Windows Firewall

If you do not have another firewall program installed on your computer, you can enable security auditing to help identify what is turning Windows Firewall off. When security auditing is enabled, Windows generates additional events in the Event Viewer Security log. You can use this log to trace certain types of activity on your computer.

Before you can view the security auditing events, you must enable Windows to generate them. They are turned off by default. For more information, see [Enable IPsec and Windows Firewall Audit Events](http://go.microsoft.com/fwlink/?linkid=114217).

To view the security auditing events

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Click Start, and in the Start Search box, start typing Event Viewer. Double-click Event Viewer when it appears in the Programs list.2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.3. In the navigation page, expand Windows Logs, and then click Security.4. Look for events with numbers in the range of 4900 to the low 5000s that indicate that the firewall service (MpsSvc) was stopped. Open the event, and then click the Event Log Online Help link to determine why the service stopped, and how to get it started again.Some of these events are shown in the following table:

|  |  |
| --- | --- |
| Event ID | Event text |
| 5029 | The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy. Error Code: %1 |
| 5030 | The Windows Firewall Service failed to start. Error Code: %1 |
| 5025 | The Windows Firewall Service has been stopped. |

If one of these events appears in the Security log: In Event Viewer, click the Event Log Online Help link at the bottom of the event description window. For many events, additional information, including diagnostic and troubleshooting procedures specific to that event, is available. Examine other events that are logged immediately before and after the event you found, including events that are found in the other logs. Other events that happened at or near the same time can sometimes indicate reasons for the failure. Use the Filter Current View option to see events that were logged within a specified time window from some or all of the logs. |

# I Need to Disable Windows Firewall

Because Windows Firewall with Advanced Security plays an important part in helping to protect your computer from security threats, we recommend that you do not disable it unless you install another firewall from a reputable vendor that provides an equivalent level of protection.

You cannot uninstall Windows Firewall with Advanced Security; you can only disable the firewall functionality.

If you must disable the firewall functionality, follow one the procedures shown here.

Note

To modify any setting for Windows Firewall with Advanced Security, you must either be a member of the Administrators group or the Network Operators group on the local computer.

To disable the firewall portion of Windows Firewall with Advanced Security from a command prompt

|  |
| --- |
| 1. Open an Administrator: Command Prompt. To do so, click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.2. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.3. At the command prompt, type the following command:netsh advfirewall set profiles state offwhere profiles is AllProfiles, CurrentProfile, DomainProfile, PrivateProfile, or PublicProfile. |

To disable the firewall portion of Windows Firewall with Advanced Security by using the Windows Firewall Control Panel program

|  |
| --- |
| 1. Click Start, click Control Panel, click Network and Internet, and then under Windows Firewall, click Turn Windows Firewall on or off.2. On the General tab of the Windows Firewall Settings dialog box, select Off (not recommended), and then click OK. |

To disable the firewall portion of Windows Firewall with Advanced Security by using the Windows Firewall with Advanced Security MMC snap-in

|  |
| --- |
| 1. Click Start, click All Programs, click Administrative Tools, and then click Windows Firewall with Advanced Security.2. In the navigation pane, right-click Windows Firewall with Advanced Security on Local Computer, and then click Properties.3. On each of the Domain Profile, Private Profile, and Public Profile tabs, change the Firewall state option to Off (not recommended).4. Click OK to save your changes. |

Caution

Do not disable Windows Firewall by stopping the service. Instead, use one of the preceding procedures (or an equivalent Group Policy setting) to turn the firewall off. If you turn off the Windows Firewall with Advanced Security service, you lose other benefits provided by the service, such as the ability to use Internet Protocol security (IPsec) connection security rules, Windows Service Hardening, and network protection from attacks that employ network fingerprinting. For more information about Windows Service Hardening, see <http://go.microsoft.com/fwlink/?linkid=104976>. Non-Microsoft firewall software that is compatible with Windows Vista and Windows Server 2008 can programmatically disable only the parts of Windows Firewall with Advanced Security that need to be disabled for compatibility. You should not disable the firewall yourself for this purpose. Stopping the service associated with Windows Firewall with Advanced Security is not supported by Microsoft.

If your computer is managed by a network administrator, the ability to disable Windows Firewall can be disabled by using Group Policy.

# I Cannot Configure Windows Firewall with Advanced Security

If all the settings for the properties of Windows Firewall with Advanced Security are not available (appear grayed out), then your computer is either:

 Part of a managed network and the network administrator has used Group Policy to configure Windows Firewall with Advanced Security behavior. In this case, you would see a "For your security, some settings are controlled by Group Policy" message at the top of the Windows Firewall with Advanced Security snap-in. Your network administrator has configured policy that prevents you from changing the Windows Firewall with Advanced Security configuration.

 Running Windows Vista or Windows Server 2008 and is not a part of a managed network, but local Group Policy settings have been set to configure Windows Firewall with Advanced Security behavior.

To edit local Group Policy settings for Windows Firewall with Advanced Security, use the Local Computer Policy snap-in. To open the local Computer Policy snap-in, type secpol at the command prompt. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue. Navigate to Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security to configure the Windows Firewall with Advanced Security policy.

# Nobody Can Ping My Computer

A common step in troubleshooting connectivity situations is to use the Ping tool to ping the IP address of the computer to which you are trying to connect. When you ping, you send an ICMP Echo message (also known as an ICMP Echo Request message) and get an ICMP Echo Reply message in response. By default, Windows Firewall does not allow incoming ICMP Echo messages, and therefore the computer cannot send an ICMP Echo Reply in response.

Enabling incoming ICMP Echo messages will allow others to ping your computer. However, it also leaves your computer vulnerable to the types of attacks that use ICMP Echo messages. Therefore, we recommended that you enable the Allow incoming echo request setting temporarily, and then disable it when it is no longer needed.

To enable ICMP Echo messages, create new inbound custom rules to allow ICMPv4 and ICMPv6 Echo Request packets.

To enable ICMP Echo Request for ICMPv4 and ICMPv6

|  |
| --- |
| 1. In the Windows Firewall with Advanced Security snap-in, click Inbound Rules in the tree, and click New Rule in the Actions Pane.2. Click Custom and click Next.3. Click All programs and click Next.4. For Protocol type, select ICMPv4.5. Click Customize for Internet Control Message Protocol (ICMP) settings.6. Click Echo Request, click OK, and then click Next.7. Under Which local IP address does this rule match? and for Which remote IP address does this rule match click either Any IP address or These IP Addresses. If you click These IP addresses, specify the IP addresses and click Add, then click Next.8. Click Allow the connection, and then click Next.9. Under When does this rule apply?, click the active profile, any or all profiles (Domain, Private, Public) to which you want this rule to apply, and then click Next.10. For Name type a name for this rule and for Description an optional description. Click Finish.11. Repeat steps for ICMPv6, selecting ICMPv6 for Protocol Type instead of ICMPv4. |

If you have active connection security rules, it is also helpful for troubleshooting purposes to exempt ICMP from the IPsec requirements temporarily. To do this, in the Windows Firewall with Advanced Security snap-in, in the Properties dialog box, click the IPsec Settings tab and click Yes to Exempt ICMP from IPsec. This step is only necessary if you have active connection security rules on the computer that you are trying to ping.

Note

Only administrators or network operators can change Windows Firewall settings.

# Nobody Can Access My Local File and Printer Shares

If you cannot access file or printer shares on a computer that has Windows Firewall enabled, verify that all the rules in the File and Printer Sharing group that apply to the active profile are enabled. In the Windows Firewall with Advanced Security snap-in, click Inbound Rules in the tree and scroll to the rules with the group name File and Printer Sharing. Verify that these rules are enabled. For each rule that is not enabled, select the rule and click Enable Rule in the Actions Pane.

Warning   Enabling File and Printer Sharing for any computer that is directly attached to the Internet is strongly discouraged because malicious users can attempt to obtain access to file shares and compromise your personal files.

# I Cannot Remotely Administer Windows Firewall

If you cannot remotely administer a computer that has Windows Firewall enabled, verify that all the rules in the predefined Windows Firewall Remote Management group that apply to the active profile on the computer you want to manage are enabled. In the Windows Firewall with Advanced Security snap-in, click Inbound Rules in the tree and scroll to the rules associated with the group Remote Administration. Verify that these rules are enabled. For each rule that is not enabled, select the rule and click Enable Rule in the Actions Pane. In addition, verify that the IPsec Policy Agent service is enabled. This service is required to remotely manage the Windows Firewall.

To verify that IPsec Policy Agent is started

|  |
| --- |
| 1. Click Start and click Control Panel.2. Click System and Maintenance and click Administrative Tools.3. Double-click Services.4. If the User Account Control dialog box appears, confirm that the action it displays is what you want, and then click Continue.5. Locate IPsec Policy Agent in the list of services and verify in the Status column that the service is started. 6. If the IPsec Policy Agent is not started, right click IPsec Policy Agent and click Start. Alternatively, you can start the IPsec Policy Agent at the command prompt by typing net start policy agent. |

Note

The IPsec Policy Agent service is enabled by default. Unless you have stopped this service, it should be running.

# IPsec Troubleshooting Situations

# My IPsec-protected Computer Cannot Get an IP Address from DHCP

When you implement a server isolation or domain isolation solution on your network, the computers in the domain receive connection security rules that block unsolicited inbound network traffic that is not IPsec-protected. DHCP network traffic is typically not IPsec-protected, but because a DHCP exchange is initiated by the client computer, replies from the DHCP server are typically permitted because they are responses to client requests.

However, in some environments where the DHCP infrastructure is not fully RFC compliant, the DHCP servers and relay agents reply to the client-initiated broadcast packet with a unicast response. Because the incoming unicast packet from DCHP does not match the broadcast packet that was sent, the packet is viewed by the firewall as unsolicited, and is dropped. For this reason, DHCP network traffic is typically exempted from IPsec authentication requirements.

Notes

This problem affects only computers that are running Windows Vista or Windows Server 2008.

By default, computers that are running Windows 7 or Windows Server 2008 R2 help to simplify connection security and firewall rule configuration by exempting DHCPv4 and DHCPv6 traffic from IPsec authentication requirements. The DHCP client service on these versions of Windows comes with rules that exempt the DHCPv4 and DHCPv6 packet from authentication during communication with a DHCP server. The DHCP client service automatically enables these exemption rules as needed, and then removes the exemptions when the DHCP exchange is complete. This setting can be configured by using the netsh advfirewall set global ipsec defaultexemptions command. For more information, see the article [DHCP Broadcast flag handling in Windows 7](http://go.microsoft.com/fwlink/?linkid=143684) (http://go.microsoft.com/fwlink/?linkid=143684) on the Microsoft Windows DHCP Team Blog.

In addition to client computers in an environment with non-RFC-compliant DHCP servers, this symptom can also occur on computers that have the following registry key value set to 0.

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interface\{GUID}\DhcpConnForceBroadCastFlag

## IPsec Exemption for DHCPv4

To resolve this problem for computers that are running earlier versions of Windows and using IPv4-based DHCP, create a connection security rule that exempts this “unsolicited” inbound DHCPv4 traffic from any authentication requirements. The rule must have the following characteristics:

|  |  |
| --- | --- |
| Parameter | Value |
| Rule type | Custom |
| Endpoint 1 | Any |
| Endpoint 2 | Any |
| Authentication requirements | Do not authenticate |
| Protocol | UDP (17) |
| Endpoint 1 port | 68 |
| Enpoint 2 port | 67 |

To create this connection security rule by using the Netsh command-line tool, use commands similar to the following at an administrator command prompt:

netsh

netsh>advfirewall

netsh advfirewall>set store gpo = <domain>\<gponame>

In the previous command, <domain> and <gponame> represent the actual domain name and name of the Group Policy object (GPO) you want to modify.

netsh advfirewall>consec add rule name=”DHCPv4 Exemption” endpoint1=any endpoint2=any port1=68 port2=67 protocol=UDP action=noauthentication

Deploy this rule to all of the members of your server or domain isolation groups.

## IPsec Exemption for DHCPv6

To resolve this problem for computers that are running earlier versions of Windows and using IPv6-based DHCP, create a connection security rule that exempts this “unsolicited” inbound DHCPv6 traffic from any authentication requirements. The rule must have the following characteristics:

|  |  |
| --- | --- |
| Parameter | Value |
| Rule type | Custom |
| Endpoint 1 | Any |
| Endpoint 2 | Any |
| Authentication requirements | Do not authenticate |
| Protocol | UDP (17) |
| Endpoint 1 port | 546 |
| Enpoint 2 port | 547 |

To create this connection security rule by using the Netsh command-line tool, use commands similar to the following at an administrator command prompt:

netsh

netsh>advfirewall

netsh advfirewall>set store gpo = <domain>\<gponame>

In the previous command, <domain> and <gponame> represent the actual domain name and name of the Group Policy object (GPO) you want to modify.

netsh advfirewall>consec add rule name=”DHCPv6 Exemption” endpoint1=any endpoint2=any port1=546 port2=547 protocol=UDP action=noauthentication

Deploy this rule to all of the members of your server or domain isolation groups.