How to view the Windows 7 firewall log file for block ports

This howto will show two ways to view Windows 7 firewall blocking two ports. The howto believes your system has been exposed to the network for some time and Windows 7 firewall logging is enabled.

Preuss
2/12/2012

win7_x64 - VMware Player File Virtual Machine Help

Recycle Bin

Adobe Reader X

LibreOffice 3.4

Mozilla Firefox

Once the logging is enabled and the system is on the network for some time, log as administrator to view the log entries.

4:54 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Local Security Policy

File Action View Help

- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Sec
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Failure
Audit directory service access	No auditing
Audit logon events	Failure
Audit object access	Failure
Audit policy change	Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	No auditing

This is the Local Security Policy | Audit Policy settings for this howto.

Administrative Tools

Size

2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
3 KB

Troubleshooting
User Accounts
VMware Tools
Windows Anytime Upgrade
Windows CardSpace
Windows Defender
Windows Firewall
Windows Update

4:57 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Logs
  - Subscriptions

Security Number of events: 554 (!) New events available

Level	Date and Time	Source	Ev...	Task Category
Information	2/12/2012 5:03:19 PM	Microsoft Wind...	4656	File System
Information	2/12/2012 5:03:18 PM	Microsoft Wind...	4656	File System
Information	2/12/2012 5:03:09 PM	Microsoft Wind...	4673	Sensitive Privilege Use
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...

Event 4656, Microsoft Windows security auditing.

t was requested.

PREUSS-WIN7-X64\nxt
me: nxt
main: PREUSS-WIN7-X64
0x12b5cc

ecurity
Microsoft Windows security
656
Information
User: N/A
OpCode: Info
More Information: Event Log Online Help

Logged: 2/12/2012 5:03:19 PM
Task Category: File System
Keywords: Audit Failure
Computer: preuss-win7-x64

One place to find entries is Event Viewer | Windows Logs | Security.

Actions

Security
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 4656, Microsoft Wind...
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

5:03 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

win7_x64 - VMware Player File Virtual Machine Help

Event Viewer

File Action View Help

Event Viewer (Local)

Custo

Windo

Ap

Se

Se

Sy

Fo

Applic

Subsc

Event Properties - Event 5152, Microsoft Windows security auditing.

General Details

Network Information:

Direction:	Inbound
Source Address:	192.168.10.136
Source Port:	137
Destination Address:	192.168.10.2
Destination Port:	137
Protocol:	17

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/12/2012 5:02:23 PM
Event ID:	5152	Task Category:	Filtering Platform Packet Drop
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	preuss-win7-x64
OpCode:	Info		

More Information: Event Log Online Help

Copy Close

This is a log entry showing a dropped packet. Use the copy command to get the complete log file.

Save All Events As...

Attach a Task To this L...

View

Refresh

Help

Event 5152, Microsoft Wind...

Event Properties

Attach Task To This Ev...

Copy

Save Selected Events...

Refresh

Help

Level: Information Keywords: Audit Failure
User: N/A Computer: preuss-win7-x64
OpCode: Info
More Information: Event Log Online Help

5:13 PM
2/12/2012

vmware

win7_x64 - VMware Player File Virtual Machine Help

Event Viewer

File Action View Help

Untitled - Notepad

File Edit Format View Help

```
Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Date:          2/12/2012 5:02:23 PM
Event ID:      5152
Task Category: Filtering Platform Packet Drop
Level:         Information
Keywords:      Audit Failure
User:          N/A
Computer:      preuss-win7-x64
Description:
The Windows Filtering Platform has blocked a packet.

Application Information:
        Process ID:             892
        Application Name:       \device\harddiskvolume2\windows\system32\svchost.exe

Network Information:
        Direction:              Inbound
        Source Address:         192.168.10.136
        Source Port:            137
        Destination Address:    192.168.10.2
        Destination Port:               137
        Protocol:               17

Filter Information:
        Filter Run-Time ID:     68189
        Layer Name:             Receive/Accept
        Layer Run-Time ID:      44
Event Xml:
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
```

This is most of the complete log entry. The network information shows the packet header information of the dropped packet.

OpCode: Info

More Information: Event Log Online Help

Help

5:13 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Windows Firewall with Advanced Security

File Action View Help

Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

For your security, some settings are controlled by Group Policy

Domain Profile

Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Private Profile

Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Public Profile is Active

Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

Actions

Windows Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Firewall with Advance Security also shows dropped packets.

5:14 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Windows Firewall with Advanced Security

File Action View Help

Windows Firewall with Advance
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Monitoring

For your security, some settings are controlled by Group Policy

Domain Profile

Private Profile

Public Profile is Active

Active Networks

Network 4

Firewall State

Windows Firewall is on.

Inbound connections that do not match a

Outbound connections that do not match

General Settings

Display a notification when a program is blocke

Apply local firewall rules:

Apply local connection security rules: Yes

Logging Settings

File name: %systemroot%\system32\LogFiles\Firewall\pfirewall.lo

File maximum size (KB): 4096

Log dropped packets: Yes

Log successful connections: Yes

Click on the Monitoring option to the left, then click on %systemroot%\system32\LogFiles\F

Actions

Monitoring
- View
- Refresh
- Help

5:14 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Windows Firewall with Advanced Security

File Action View Help

pfirewall - Notepad

File Edit Format View Help

```
2012-02-12 17:07:59 ALLOW UDP 192.168.10.1                                    - SEND
2012-02-12 17:08:01 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:01 ALLOW UDP fe80::ed42:2                                    65220 53 0 - - - - - - - - SEND
2012-02-12 17:08:01 ALLOW ICMP fe80::ed42                                      - - - 135 0 - SEND
2012-02-12 17:08:08 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:12 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:12 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:12 ALLOW UDP 192.168.10.1                                    - SEND
2012-02-12 17:08:15 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:19 ALLOW UDP 192.168.10.1                                    - SEND
2012-02-12 17:08:22 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:24 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:26 ALLOW UDP 192.168.10.1                                     SEND
2012-02-12 17:08:26 ALLOW UDP fe80::ed42:2                                    57880 53 0 - - - - - - - - SEND
2012-02-12 17:08:26 ALLOW ICMP fe80::ed42                                      - - - 135 0 - SEND
2012-02-12 17:08:38 ALLOW UDP 192.168.10.136 192.168.10.2 56430 53 0 - - - -  - SEND
2012-02-12 17:09:19 ALLOW UDP 192.168.10.136 192.168.10.2 62019 53 0 - - - -  - SEND
2012-02-12 17:09:40 ALLOW UDP fe80::ed42:2de7:fb11:a7af ff02::1:2 546 547 0 -  - - - - - - SEND
2012-02-12 17:09:42 DROP UDP 192.168.10.1 192.168.10.255 138 138 238 - - - - - - - - RECEIVE
2012-02-12 17:09:55 ALLOW UDP fe80::ed42:2de7:fb11:a7af ff02::1:2 546 547 0 - - - - - - - - SEND
2012-02-12 17:09:58 ALLOW UDP 192.168.10.136 192.168.10.2 51186 53 0 - - - - - - - - SEND
2012-02-12 17:10:11 ALLOW UDP fe80::ed42:2de7:fb11:a7af ff02::1:2 546 547 0 - - - - - - - - SEND
2012-02-12 17:10:22 ALLOW UDP 192.168.10.136 192.168.10.2 137 137 0 - - - - - - - - SEND
2012-02-12 17:10:38 ALLOW UDP 192.168.10.136 192.168.10.2 62564 53 0 - - - - - - - - SEND
2012-02-12 17:10:43 ALLOW UDP fe80::ed42:2de7:fb11:a7af ff02::1:2 546 547 0 - - - - - - - - SEND
2012-02-12 17:11:13 ALLOW UDP 192.168.10.136 192.168.10.2 59496 53 0 - - - - - - - - SEND
2012-02-12 17:11:46 ALLOW UDP 192.168.10.136 192.168.10.2 60893 53 0 - - - - - - - - SEND
2012-02-12 17:12:17 ALLOW UDP 192.168.10.136 192.168.10.2 59963 53 0 - - - - - - - - SEND
2012-02-12 17:12:22 ALLOW UDP 192.168.10.136 192.168.10.2 137 137 0 - - - - - - - - SEND
2012-02-12 17:12:57 ALLOW UDP 192.168.10.136 192.168.10.2 52503 53 0 - - - - - - - - SEND
2012-02-12 17:13:34 ALLOW UDP 192.168.10.136 192.168.10.2 63781 53 0 - - - - - - - - SEND
2012-02-12 17:14:08 ALLOW UDP 192.168.10.136 192.168.10.2 65245 53 0 - - - - - - - - SEND
2012-02-12 17:14:22 ALLOW UDP 192.168.10.136 192.168.10.2 137 137 0 - - - - - - - - SEND
```

Highlighted is a dropped packet. You must identify the packet for the lab.

e name: %systemroot%\system32\LogFiles\Firewall\pfirewall.log

e maximum size (KB): 4096

g dropped packets: Yes

g successful connections: Yes

5:15 PM
2/12/2012

vmware

win7_x64 - VMware Player File Virtual Machine Help

Windows Firewall with Advanced Security

File Action View Help

pfirewall - Notepad

File Edit Format View Help

```
2012-02-12 17:04:46 ALLOW TCP fe80::ed42:2de7:fb11:a7af fe80::ed42:2de7:fb11:a7af 49164 135 0 - 0 0 0 - - - SEND
2012-02-12 17:04:46 ALLOW TCP fe80::ed42:2de7:fb11:a7af fe80::ed42:2de7:fb11:a7af 49164 135 0 - 0 0 0 - - - RECEIVE
2012-02-12 17:04:54 ALLOW UDP 192.168.10.136 192.168.10.255 137 137 0 - - - - - - - - SEND
2012-02-12 17:04:56 ALLOW UDP 192.168.10.136 192.168.10.2 58889 53 0 - - - - - - - - SEND
2012-02-12 17:04:56 ALLOW UDP fe80::ed42:2de7:fb11:a7af fe80::e291:f5ff:feff:b10e 49678 53 0 - - - - - - - - SEND
2012-02-12 17:04:56 ALLOW ICMP fe80::ed42:2de7:fb11:a7af ff02::1:ffff:b10e - - 0 - - - - 135 0 - SEND
2012-02-12 17:05:07 ALLOW UDP 192.168                                                    - - - SEND
2012-02-12 17:05:09 ALLOW UDP 192.168                                                    - - SEND
2012-02-12 17:05:09 ALLOW UDP fe80::e                                                    10e 61934 53 0 - - - - - - - - SEND
2012-02-12 17:05:09 ALLOW ICMP fe80::                                                    0 - - - - 135 0 - SEND
2012-02-12 17:05:18 ALLOW UDP 192.168                                                    - - SEND
2012-02-12 17:05:25 ALLOW UDP 192.168                                                    - - - SEND
2012-02-12 17:05:27 ALLOW UDP 192.168                                                    - - SEND
2012-02-12 17:05:27 ALLOW UDP fe80::e                                                    10e 57924 53 0 - - - - - - - - SEND
2012-02-12 17:05:27 ALLOW ICMP fe80::                                                    0 - - - - 135 0 - SEND
2012-02-12 17:05:38 ALLOW UDP 192.168                                                    - - SEND
2012-02-12 17:05:38 ALLOW TCP 192.168                                                    - - - SEND
2012-02-12 17:05:38 ALLOW TCP 192.168                                                    - - - SEND
2012-02-12 17:05:39 ALLOW UDP 192.168                                                    - - SEND
2012-02-12 17:05:39 ALLOW UDP 192.168                                                    - - - SEND
2012-02-12 17:05:42 ALLOW UDP 192.168                                                    - - SEND
2012-02-12 17:05:46 ALLOW UDP 192.168                                                    - - - SEND
2012-02-12 17:05:48 ALLOW UDP 192.168                                                    - - SEND
2012-02-12 17:05:51 ALLOW UDP 192.168.10.136 192.168.10.2 63087 53 0 - -                 - - - SEND
2012-02-12 17:05:52 ALLOW UDP 192.168.10.136 192.168.10.2 64608 53 0 - -                 - - - SEND
2012-02-12 17:05:53 ALLOW UDP 192.168.10.136 192.168.10.2 54701 53 0 - - - - - - - - SEND
2012-02-12 17:05:54 DROP UDP 192.168.10.1 192.168.10.255 138 138 229 - - - - - - - - RECEIVE
2012-02-12 17:05:55 ALLOW UDP 192.168.10.136 192.168.10.2 54105 53 0 - - - - - - - - SEND
2012-02-12 17:05:55 ALLOW UDP fe80::ed42:2de7:fb11:a7af fe80::e291:f5ff:feff:b10e 54036 53 0 - - - - - - - - SEND
2012-02-12 17:05:55 ALLOW ICMP fe80::ed42:2de7:fb11:a7af ff02::1:ffff:b10e - - 0 - - - - 135 0 - SEND
2012-02-12 17:06:11 ALLOW UDP 192.168.10.136 192.168.10.255 137 137 0 - - - - - - - - SEND
2012-02-12 17:06:13 ALLOW UDP 192.168.10.136 192.168.10.2 61913 53 0 - - - - - - - - SEND
2012-02-12 17:06:13 ALLOW UDP fe80::ed42:2de7:fb11:a7af fe80::e291:f5ff:feff:b10e 60604 53 0 - - - - - - - - SEND
2012-02-12 17:06:13 ALLOW ICMP fe80::ed42:2de7:fb11:a7af ff02::1:ffff:b10e - - 0 - - - - 135 0 - SEND
```

This is another dropped packet. You must identify the packet for the lab.

e name: %systemroot%\system32\LogFiles\Firewall\pfirewall.log

e maximum size (KB): 4096

g dropped packets: Yes

g successful connections: Yes

5:15 PM
2/12/2012

vmware