

Windows 8.0 Firewall Rule Reporting

This presentation shows using the command line to backup all the firewall rules. The presentation show how to export the Windows Firewall rules to a file. The presentation shows the location of the Firewall logging system. The presentation shows retrieving the Windows Firewall logs in Notepad

Preuss

3/12/2014

- Snuffy
- Oracle VM VirtualBox
- Computer
- Recuva
- Recycle Bin
- Control Panel
- Gpg4win Document...
- GPA
- Kleopatra

The presentation logs on as a full administrator.

Start


Snuffy 



Mail





Internet Explorer




Store 15

Trending
Kristian Nairn
Princeton Mo
Katie Couric d
Bing




People

The presentation goes to the Start Menu.





SkyDrive


Rio de J
Bing




Messaging



Obama Will Seek Broad Expansion of Overtime Pay




98.5 - Justin Verlander near perfect in spring training debut for the Tigers



Games


Desktop



Weather



2 NYC buildings collapse in explosion, 2 dead



Music

Apps



Paint



WordPad



Computer



Windows Easy Transfer Reports



Remote Desktop Connection



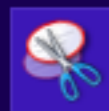
XPS Viewer



Control Panel

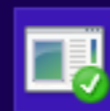


Windows PowerShell



Snipping Tool

Windows Ease of Access



Default Programs



Sound Recorder



Magnifier



File Explorer



Steps Recorder



Narrator



Help and Support



Sticky Notes



On-Screen Keyboard



Run



Windows Fax and Scan



Windows Speech Recognition



Windows Journal

Windows System



Windows Media Player



Command Prompt ✓



Pin to Start



Unpin from taskbar



Open new window



Run as administrator

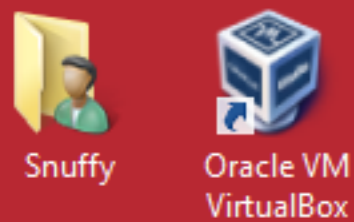


Open file location



All apps

The presentation selects the Command Prompt. The presentation selects Run as Administrator.



Administrator: Command Prompt

```
C:\Windows\system32>cd %HOMEPATH%  
C:\Users\Snuffy>_
```

The presentation changes the default directory to the current logon home directory.

GPA





Snuffy

Oracle VM
VirtualBox

Administrator: Command Prompt

```
C:\Windows\system32>cd %HOMEPATH%  
C:\Users\Snuffy>md temp  
C:\Users\Snuffy>cd temp  
C:\Users\Snuffy\temp>_
```

The presentation creates a temp directory for this project. The presentation changes the default directory to %HOMEPATH%\temp.

GPA



Kleopatra



ENG

11:28 AM
3/12/2014



Snuffy

Oracle VM
VirtualBox

Administrator: Command Prompt

```
C:\Windows\system32>cd %HOMEPATH%
```

```
C:\Users\Snuffy>md temp
```

```
C:\Users\Snuffy>cd temp
```

```
C:\Users\Snuffy\temp>netsh advfirewall export fw_backup01.txt  
Ok.
```

```
C:\Users\Snuffy\temp>
```

The command netsh advfirewall export will copy the current firewall configuration to the file fw_backup01.txt

You may choose another name other than fw_backup01.txt

GPA



Kleopatra



ENG

11:28 AM
3/12/2014



Snuffy

Oracle VM
VirtualBox

Administrator: Command Prompt

```
C:\Windows\system32>cd %HOMEPATH%
C:\Users\Snuffy>md temp
C:\Users\Snuffy>cd temp
C:\Users\Snuffy\temp>netsh advfirewall export fw_backup01.txt
Ok.
C:\Users\Snuffy\temp>dir
Volume in drive C has no label.
Volume Serial Number is CEEB-FF81

Directory of C:\Users\Snuffy\temp

03/12/2014  11:28 AM    <DIR>          .
03/12/2014  11:28 AM    <DIR>          ..
03/12/2014  11:28 AM                282,624 fw_backup01.txt
               1 File(s)                282,624 bytes
               2 Dir(s)      22,632,583,168 bytes free

C:\Users\Snuffy\temp>_
```

The presentation generates a directory listing of the folder to see the firewall backup is done.

GPA



Kleopatra



ENG

11:29 AM
3/12/2014

- Snuffy
- Oracle Virtu...
- Computer
- Recycle Bin
- Control Panel
- Gpg4win Document...
- GPA
- Kleopatra

All Control Panel Items

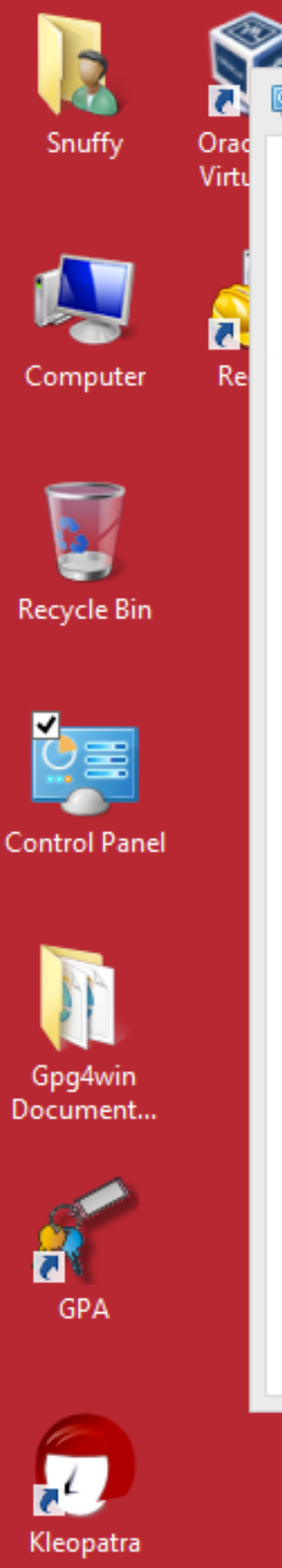
Control Panel > All Control Panel Items

Adjust your computer's settings

View by: Small icons

Action Center	Add features to Windows 8	Administrative Tools
AutoPlay	BitLocker Drive Encryption	Color Management
Credential Manager	Date and Time	Default Programs
Device Manager	Devices and Printers	Display
Ease of Access Center	Family Safety	File History
Flash Player (32-bit)	Folder Options	Fonts
HomeGroup	Indexing Options	Internet Options
Keyboard	Language	
Mail (32-bit)	Mouse	
Notification Area Icons	Pen and Touch	
Personalization	Phone and Modem	
Programs and Features	Recovery	
RemoteApp and Desktop Connections	Sound	
Storage Spaces	Sync Center	
Tablet PC Settings	Taskbar	
User Accounts	Windows 7 File Recovery	
Windows Firewall	Windows Update	

The presentation opens the Control Panel.



All Control Panel Items

Administrative Tools

File Home Share View

<< All Control Panel Items >> Administrative Tools

Search Administrative Tools

Name	Date modified	Type	Size
Component Services	7/25/2012 3:20 PM	Shortcut	2 KB
Computer Management	7/25/2012 3:17 PM	Shortcut	2 KB
Defragment and Optimize Drives	7/25/2012 3:16 PM	Shortcut	2 KB
Disk Cleanup	7/25/2012 3:20 PM	Shortcut	2 KB
Event Viewer		Shortcut	2 KB
Indexing Control Panel		Shortcut	2 KB
Localized System Information		Shortcut	2 KB
Localized System Configuration		Shortcut	2 KB
Localized System Information		Shortcut	2 KB
Performance Monitor	7/25/2012 3:15 PM	Shortcut	2 KB
Print Management	7/25/2012 3:28 PM	Shortcut	2 KB
Resource Monitor	7/25/2012 3:15 PM	Shortcut	2 KB
Services	7/25/2012 3:17 PM	Shortcut	2 KB
System Configuration	7/25/2012 3:16 PM	Shortcut	2 KB
System Information	7/25/2012 3:16 PM	Shortcut	2 KB
Task Scheduler	7/25/2012 3:18 PM	Shortcut	2 KB
Windows Firewall with Advanced Security	7/25/2012 3:28 PM	Shortcut	2 KB
Windows Memory Diagnostic	7/25/2012 3:15 PM	Shortcut	2 KB
Windows PowerShell (x86)	7/26/2012 1:44 AM	Shortcut	3 KB
Windows PowerShell ISE (x86)	7/25/2012 3:18 PM	Shortcut	2 KB
Windows PowerShell ISE	7/25/2012 3:18 PM	Shortcut	2 KB

The presentation opens the Administrative Tools in the Control Panel.

The presentation open the MMC, Windows Firewall with Advance Security.

Windows Firewall with Advanced Security

File Action View Help



Windows Firewall with Advan

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

The presentation selects the Inbound Rule. This will show all the inbound rules for the firewall.

Group	Profile	Enabled	Action	
	Public	Yes	Allow	
	Public	Yes	Allow	
	Public	Yes	Allow	
	Public	Yes	Allow	
	Public	Yes	Allow	
@{Microsoft.Reader_6.2.920...	Domain...	Yes	Allow	
@{microsoft.windowscom...	Domain...	Yes	Allow	
@{microsoft.windowsphoto...	All	Yes	Allow	
Bing	Domain...	Yes	Allow	
Bing	Domain...	Yes	Allow	
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
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	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
Core Networking - IPHTTPS (TCP-In)	Core Networkin	All	Yes	Allow

Actions

Inbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Windows Firewall with Advanced Security

File Action View Help



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

Inbound Rules

Name	Group	Profile	Enabled	Action
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-I)	BranchCache - Peer Discov...	All	No	Allow
Connect to a Network Projector (TCP)				Allow
Connect to a Network Projector (TCP)				Allow
Connect to a Network Projector (WS				Allow
Connect to a Network Projector (WS				Allow
Connect to a Network Projector (WS				Allow
Connect to a Network Projector (WS				Allow
Connect to a Network Projector (WS				Allow
Connect to a Network Projector (WS				Allow
Connect to a Network Projector (WS				Allow
Distributed Transaction Coordinator				Allow
Distributed Transaction Coordinator				Allow
Distributed Transaction Coordinator				Allow
Distributed Transaction Coordinator (RP...	Distributed Transaction Co...	Private...	No	Allow
Distributed Transaction Coordinator (TC...	Distributed Transaction Co...	Private...	No	Allow
Distributed Transaction Coordinator (TC...	Distributed Transaction Co...	Domain	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	Domain	No	Allow
HomeGroup In	HomeGroup	Private	No	Allow

The presentation selects the enabled tab. This sorts all the firewall rules by enabled status.

Actions

Inbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Windows Firewall with Advanced Security

File Action View Help



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

Inbound Rules

Name	Group	Profile	Enabled	Action
Windows Media Player x86 (UDP-In)	Windows Media Player	Private	Yes	Allow
Windows Media Player Network Sharing ...	Windows Media Player Net...	Private	Yes	Allow
Windows Media Player Network Sharing ...	Windows Media Player Net...	Private	Yes	Allow
Windows Media Player Network Shar				Allow
Windows Media Player Network Shar				Allow
Windows Media Player Network Shar				Allow
Windows Media Player Network Shar				Allow
Windows Media Player Network Shar				Allow
Windows Media Player Network Shar				Allow
Windows Media Player Network Shar				Allow
Windows Media Player (UDP-In)				Allow
Store				Allow
Remote Assistance (TCP-In)				Allow
Remote Assistance (SSDP UDP-In)				Allow
Remote Assistance (SSDP TCP-In)				Allow
Remote Assistance (RA Server TCP-In)	Remote Assistance	Domain	Yes	Allow
Remote Assistance (PNRP-In)	Remote Assistance	Domai...	Yes	Allow
Remote Assistance (DCOM-In)	Remote Assistance	Domain	Yes	Allow
Reader	Reader	Domai...	Yes	Allow
Reader	Reader	Domai...	Yes	Allow
Proximity sharing over TCP (TCP sharing...	Proximity Sharing	All	Yes	Allow
Play To UPnP Events (TCP-In)	Play To functionality	Public	Yes	Allow
Play To streaming server (RTSP-Streamin...	Play To functionality	Domain	Yes	Allow
Play To streaming server (RTSP-Streamin...	Play To functionality	Private	Yes	Allow
Play To streaming server (RTSP-Streamin...	Play To functionality	Public	Yes	Allow
Play To streaming server (RTCP-Streamin...	Play To functionality	Public	Yes	Allow
Play To streaming server (RTCP-Streamin...	Play To functionality	Domain	Yes	Allow

Actions

- Inbound Rules
 - New Rule...
 - Filter by Profile
 - Filter by State
 - Filter by Group
 - View
 - Refresh
 - Export List...
 - Help

The presentation selects the enabled tab again. The presentation prefers the reverse alphabetical order.

Windows Firewall with Advanced Security

File Action View Help



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

Inbound Rules

Save in: temp

Name	Date modified	Type
No items match your search.		

File name: inbound_rules.csv

Save as type: Text (Comma Delimited) (*.csv)

Save Only Selected Rows

Actions

- Inbound Rules
 - New Rule...
 - Filter by Profile
 - Filter by State
 - Filter by Group
 - View
 - Refresh
 - Export List...
 - Help

Name	Action	Profile	Enabled
Play To streaming server (RTSP-Streamin...	Play To functionality	Private	Yes
Play To streaming server (RTSP-Streamin...	Play To functionality	Public	Yes
Play To streaming server (RTCP-Streamin...	Play To functionality	Public	Yes
Play To streaming server (RTCP-Streamin...	Play To functionality	Domain	Yes

The presentation names the file inbound_rules.csv.

The presentation selects Save as Type: Text (Comma Delimited) (*.csv)

The presentation saves the file.

Windows Firewall with Advanced Security

File Action View Help



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

The presentation wishes to review the firewall log settings. The presentation selects the Windows Firewall with Advanced Security.



Overview

Domain Profile



Private Profile



Public Profile is Active



[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).

Actions

Windows Firewall with Advanced Security

Import Policy...

Export Policy...

Restore Default Policy

Diagnose / Repair

View

Refresh

Properties

Help

Windows Firewall with Advanced Security

File Action View Help

Windows Firewall with Advanced Security on Local Computer

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

- Import Policy...
- Export Policy...
- Restore Default Policy
- Diagnose / Repair
- View
- Refresh
- Properties
- Help

Private Profile

- Windows Firewall (On)
- Inbound connections (Blocked)
- Outbound connections (Allowed)

Public Profile

- Windows Firewall (On)
- Inbound connections (Blocked)
- Outbound connections (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).

Actions

- Import Policy...
- Export Policy...
- Restore Default Policy
- Diagnose / Repair
- View
- Refresh
- Properties
- Help

The presentation right clicks on Windows Firewall with Advance Security. The presentation selects Properties.

Windows Firewall with Advanced Security

File Action View Help

Navigation icons: back, forward, home, help, refresh

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

Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security on Local Co...

Domain Profile Private Profile Public Profile IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Specify settings that control Windows Firewall behavior. Customize...

Specify logging settings for troubleshooting. Customize...

OK Cancel Apply

Actions

- Windows Firewall wit...
 - Import Policy...
 - Export Policy...
 - Restore Default Policy
 - Diagnose / Repair
 - View
 - Refresh
 - Properties
 - Help

The presentation will review the log settings for each profile tab.

The presentation selects customize button to review the firewall log settings.

Administrator: Command Prompt

```
Microsoft Windows [Version 6.2.9200]  
(c) 2012 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>cd %HOMEPATH%\temp  
C:\Users\Snuffy\temp>
```

The presentation returns to the Command prompt running as Administrator.

The presentation changes to the directory made earlier in this document.

Gpg4win Document...



GPA



Kleopatra



ENG

11:37 AM
3/12/2014

Administrator: Command Prompt

```
Microsoft Windows [Version 6.2.9200]  
(c) 2012 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>cd %HOMEPATH%\temp  
C:\Users\Snuffly\temp>netsh advfirewall show allprofiles
```

The presentation runs the netsh advfirewall show allprofiles command to get the firewall log location.

Gpg4win Document...



GPA



Kleopatra

Administrator: Command Prompt

```

MaxFileSize                4096

Public Profile Settings:
-----
State                       ON
Firewall Policy             BlockInbound,AllowOutbound
LocalFirewallRules          N/A (GPO-store only)
LocalConSecRules            N/A (GPO-store only)
InboundUserNotification    Enable
RemoteManagement           Disable
UnicastResponseToMulticast Enable

Logging:
LogAllowedConnections       Enable
LogDroppedConnections       Enable
FileName                    %systemroot%\system32\LogFiles\Firewall\pfi
firewall.log
MaxFileSize                  4096

```

Ok.

```

C:\Users\Snuffy\temp>notepad %systemroot%\system32\logfiles\firewall\pfi
firewall.log_

```

The presentation will open the firewall log for the Public Profile. Note, sometimes all the profiles log to the same file. It is good to scroll and check.

The presentation enters the command to open the log file.

```
notepad %systemroot%\system32\logfiles\firewall\pfi
firewall.log
```



GPA



Kleopatra



pfirewall.log - Notepad

File Edit Format View Help

```

#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2014-03-04 19:45:51 DROP UDP 10.11.116.187 239.255.255.250 1900 1900 515 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP fe80::c4ef:fbff:d0ac:8c7e ff02::c 1900 1900 543 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP 10.11.116.187 239.255.255.250 1900 1900 463 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP fe80::c4ef:fbff:d0ac:8c7e ff02::c 1900 1900 491 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP 10.11.116.187 239.255.255.250 1900 1900 529 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP fe80::c4ef:fbff:d0ac:8c7e ff02::c 1900 1900 557 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP 10.11.116.187 239.255.255.250 1900 1900 527 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP fe80::c4ef:fbff:d0ac:8c7e ff02::c 1900 1900 555 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP 10.11.116.187 239.255.255.250 1900 1900 543 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP fe80::c4ef:fbff:d0ac:8c7e ff02::c 1900 1900 571 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP 10.11.116.187 239.255.255.250 1900 1900 472 - - - - - - - RECEIVE
2014-03-04 19:45:51 DROP UDP fe80::c4ef:fbff:d0ac:8c7e ff02::c 1900 1900 500 - - - - - - - RECEIVE
2014-03-04 19:46:15 DROP UDP 10.11.108.220 239.255.255.250 61739 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:16 DROP UDP 10.11.108.220 224.0.0.252 51699 5355 52 - - - - - - - RECEIVE
2014-03-04 19:46:16 DROP UDP 10.11.108.220 224.0.0.252 51699 5355 52 - - - - - - - RECEIVE
2014-03-04 19:46:18 DROP UDP 10.11.108.220 239.255.255.250 61739 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:19 DROP UDP 10.11.118.162 224.0.0.252 65177 5355 51 - - - - - - - RECEIVE
2014-03-04 19:46:19 DROP UDP 10.11.118.162 224.0.0.252 65177 5355 51 - - - - - - - RECEIVE
2014-03-04 19:46:20 DROP UDP 10.11.118.162 224.0.0.252 51959 5355 55 - - - - - - - RECEIVE
2014-03-04 19:46:20 DROP UDP 10.11.118.162 239.255.255.250 57092 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:20 DROP UDP 10.11.118.162 224.0.0.252 51959 5355 55 - - - - - - - RECEIVE
2014-03-04 19:46:21 DROP UDP 10.11.108.220 239.255.255.250 61739 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:22 DROP UDP 10.11.118.162 224.0.0.252 62313 5355 51 - - - - - - - RECEIVE
2014-03-04 19:46:22 DROP UDP 10.11.118.162 224.0.0.252 62313 5355 51 - - - - - - - RECEIVE
2014-03-04 19:46:23 DROP UDP 10.11.118.162 239.255.255.250 57092 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:24 DROP UDP 10.11.108.220 239.255.255.250 61739 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:26 DROP UDP 10.11.118.162 239.255.255.250 57092 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:27 DROP UDP 10.11.108.220 239.255.255.250 61739 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:29 DROP UDP 10.11.118.162 239.255.255.250 57092 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:30 DROP UDP 10.11.118.176 239.255.255.250 50888 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:30 DROP UDP 10.11.108.220 239.255.255.250 61739 1900 161 - - - - - - - RECEIVE
2014-03-04 19:46:32 DROP UDP 10.11.118.162 239.255.255.250 57092 1900 161 - - - - - - - RECEIVE

```

The presentation reviews the Windows Firewall log in notepad.

