

Open in app ↗

Sign up Sign in

Medium

 Write 

[Misc Series #4] Forensics on EDRSilencer Events

 GhouLSec · [Follow](#)



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Table of Descriptions by Event ID

Event ID	Brief Description
5152	Windows Filtering Platform blocked a packet
5154	Windows Filtering Platform permitted an application or service to listen on a port for incoming connections
5156	Windows Filtering Platform allowed a connection
5157	Windows Filtering Platform blocked a connection
5158	Windows Filtering Platform permitted a bind to a local port
5159	Windows Filtering Platform blocked a bind to a local port

Medium

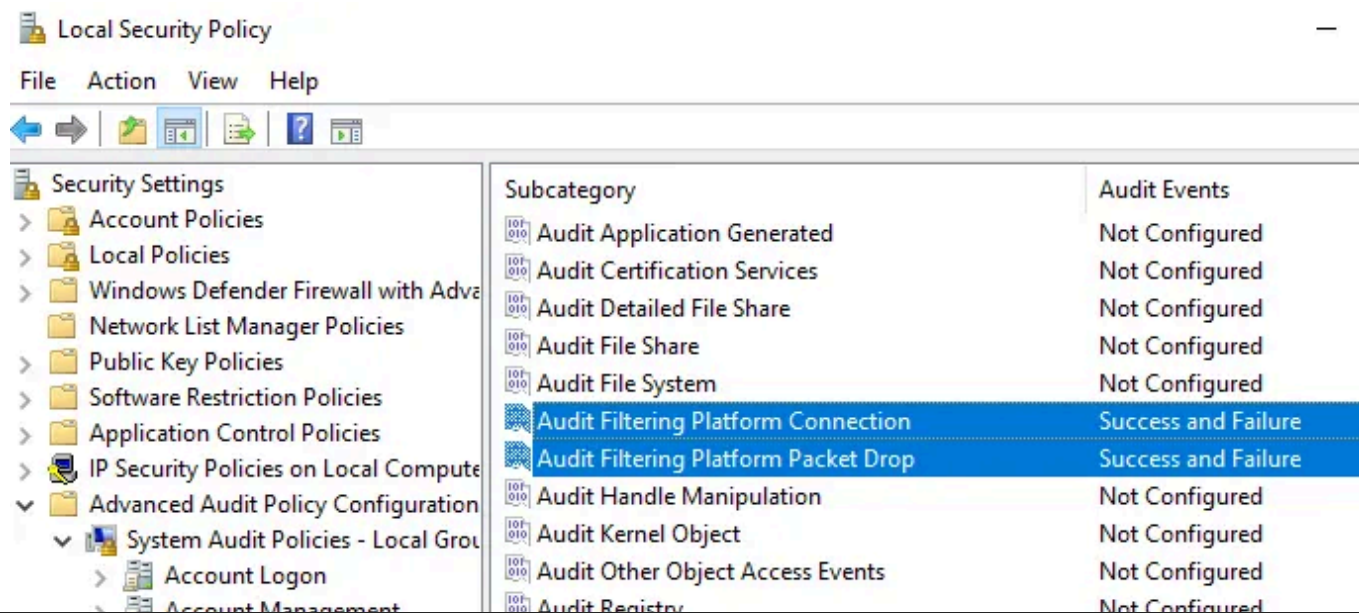
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Medium

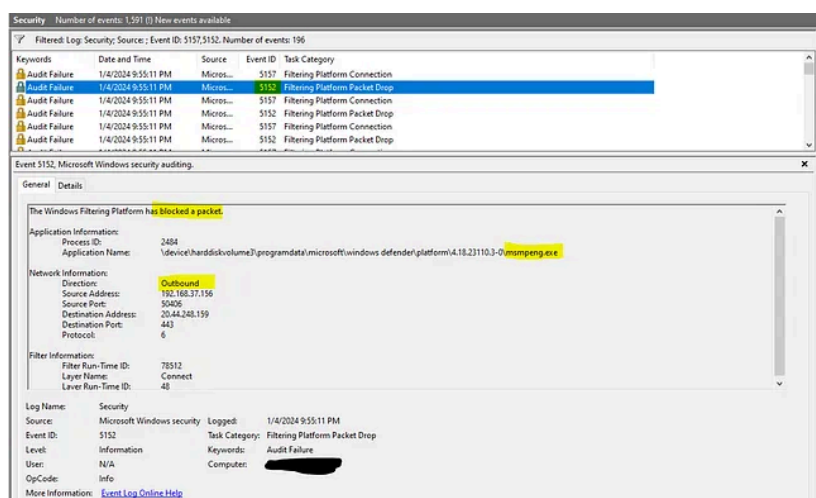
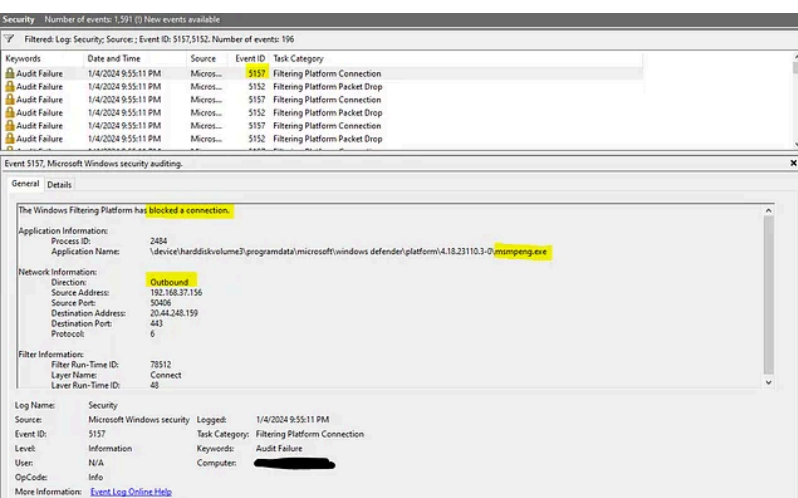
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

As we can see in `netevents.xml`, the string in the `<asString>` tag is in UTF16-LE format while the `<data>` tag is the hex representation of string in `<asString>` tag.

```
<item>
  <header>
    <timeStamp>2024-01-04T14:59:07.302Z</timeStamp>
    <flags numItems="9">
      <item>FWPM_NET_EVENT_FLAG_IP_PROTOCOL_SET</item>
      <item>FWPM_NET_EVENT_FLAG_LOCAL_ADDR_SET</item>
      <item>FWPM_NET_EVENT_FLAG_REMOTE_ADDR_SET</item>
      <item>FWPM_NET_EVENT_FLAG_LOCAL_PORT_SET</item>
      <item>FWPM_NET_EVENT_FLAG_REMOTE_PORT_SET</item>
      <item>FWPM_NET_EVENT_FLAG_APP_ID_SET</item>
      <item>FWPM_NET_EVENT_FLAG_USER_ID_SET</item>
      <item>FWPM_NET_EVENT_FLAG_IP_VERSION_SET</item>
      <item>FWPM_NET_EVENT_FLAG_PACKAGE_ID_SET</item>
    </flags>
    <ipVersion>FWP_IP_VERSION_V4</ipVersion>
```

Medium

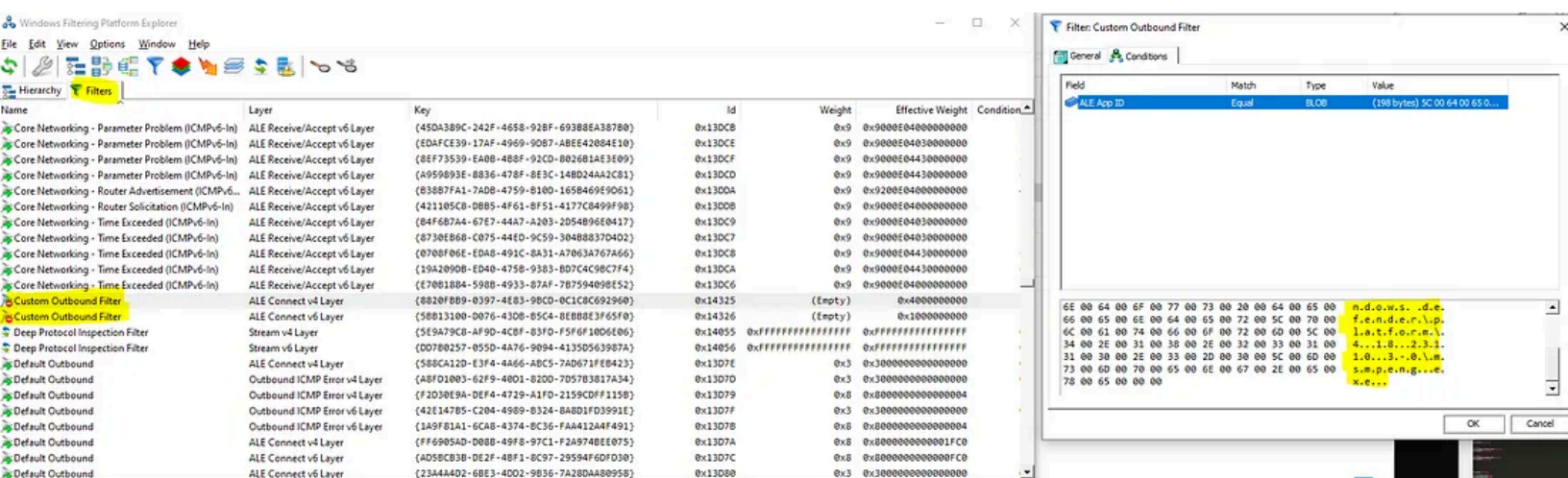
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Medium

Sign up to discover human stories that deepen your understanding of the world.

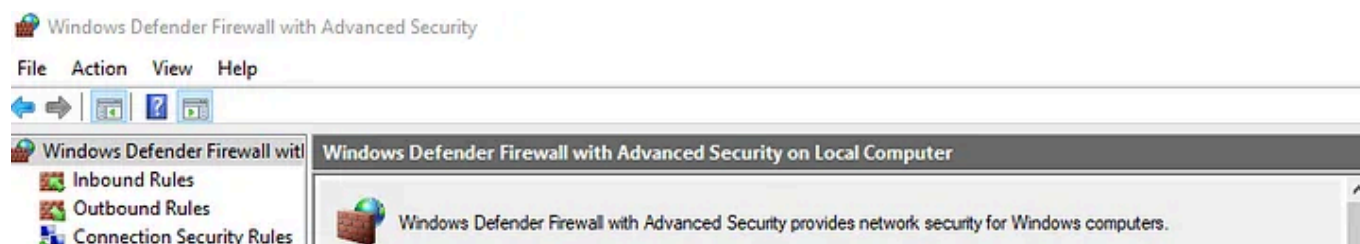
Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Same with WFP event logs, the windows firewall doesn't log those packet drop events by default. We have to enable it based on the network profile the we are using.



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

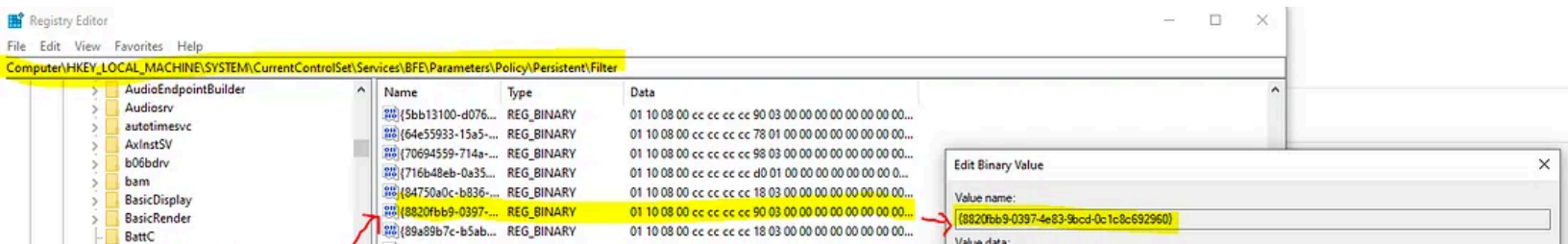
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The WFP filter data of the EDRSilencer can be found in the service registry key Base Filtering Engine (BFE) which is located as

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

EDRSilencer.exe	4916	CreateFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\MsMpEng.exe	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: SYNCHRONIZING_IO,...
EDRSilencer.exe	4916	QueryNameInfo	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\MsMpEng.exe	BUFFER OVERFLOW	
EDRSilencer.exe	4916	QueryNameInfo	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\MsMpEng.exe	SUCCESS	Name: \ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\
EDRSilencer.exe	4916	CloseFile	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\MsMpEng.exe	SUCCESS	
EDRSilencer.exe	4916	Thread Create		SUCCESS	Thread ID: 364
EDRSilencer.exe	4916	Thread Exit		SUCCESS	Thread ID: 364, User Time: 0.00000000, Kernel Time: 0.00000000
EDRSilencer.exe	4916	Thread Exit		SUCCESS	Thread ID: 7456, User Time: 0.00000000, Kernel Time: 0.00000000
EDRSilencer.exe	4916	Thread Exit		SUCCESS	Thread ID: 8036, User Time: 0.00000000, Kernel Time: 0.01562500
EDRSilencer.exe	4916	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.00000000 seconds, Kernel Time: 0.01562500 seconds

EDR process file has been loaded by EDRSilenacer before apply the WFP block rule.

Once it was succeed, we can see the the `TCP Disconnect` events from the `msmpeng.exe` and once the WFP block rule disabled, the event data flow to server gets back to normal (`TCP Send` & `TCP Receive`). However, this part will

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Collect Windows Filtering Platform (WFP) events

This topic describes how to collect Windows Filtering Platform (WFP) events in SEM.

documentation.solarwinds.com

Windows Security Log Event ID 5156 - The Windows Filtering Platform has allowed a connection

5156: The Windows Filtering Platform has allowed a connection On
this page This event documents each time WFP allows a

[illegible]

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

blog.quarkslab.com



Cybersecurity

Threat Hunting

Computer Forensics

Digital Forensics

Blue Team



--



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app