[Misc Series #4] Forensics on EDRSilencer Events

GhouLSec · Follow
5 min read · Jan 4, 2024

--

EDRSilencer by netero1010 is a tool that utilizing Windows Filtering Platform (WFP) to block EDR agent to send out its event data to its server by adding both **IPv4** and **IPv6** WFP outbound block rule (Administrator access required). That is bad as most of the defenders are heavily depends on the event data from EDR to perform their operation task. In this blog, here are some of the indicators that we can go for if the EDR event data flow has been "blocked" due to any security events (e.g. red teaming or threat actor).

Event Logs

As usual, **Security event logs** contain event that is related to WFP and now we are focusing on the WFP **block** events which are EID `5152` and `5157`

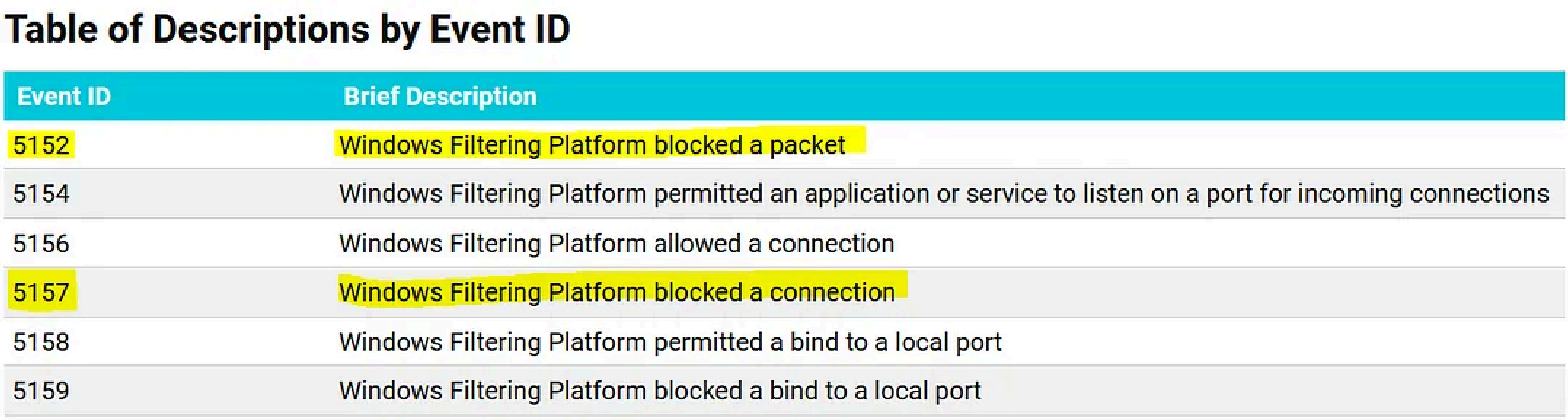
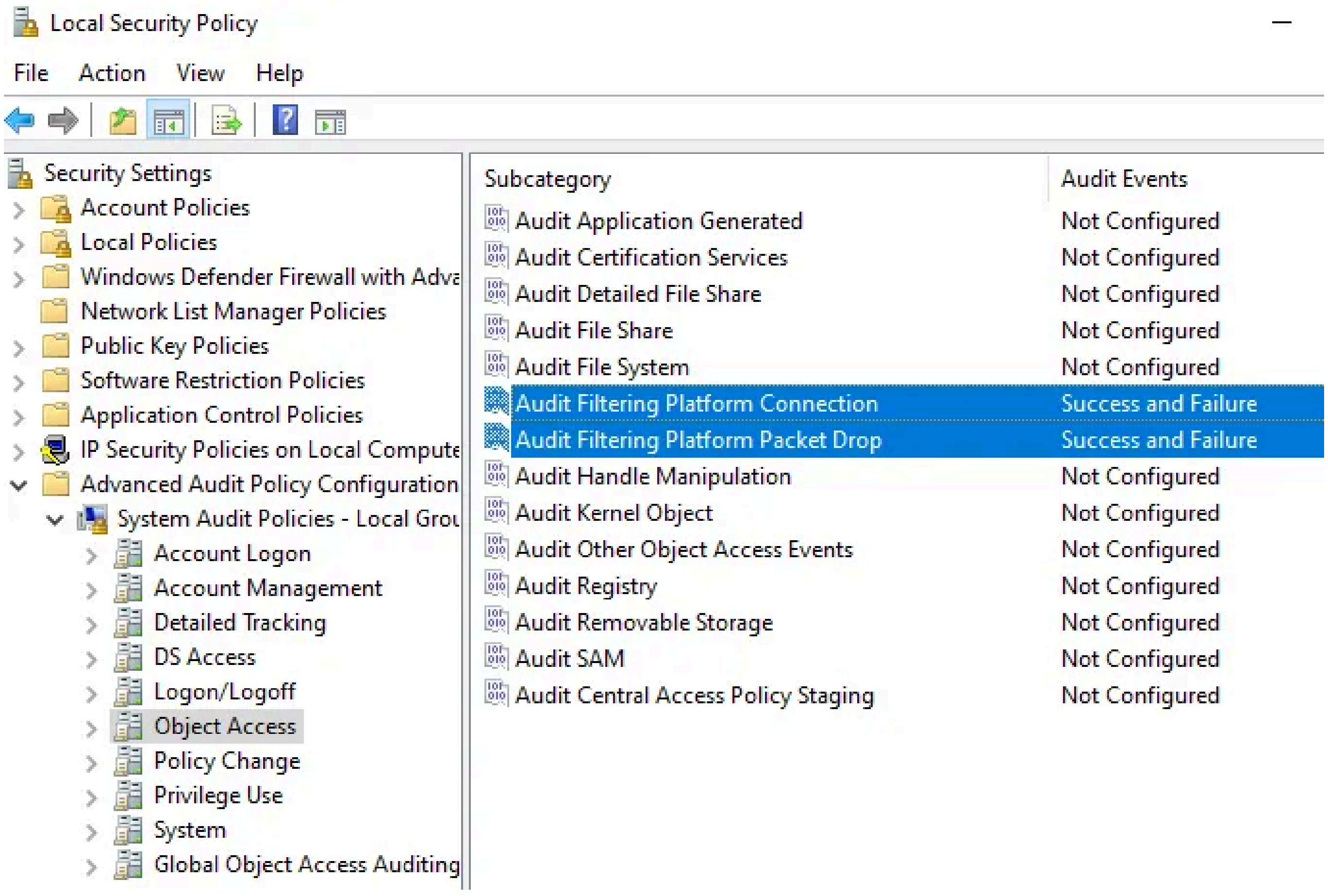


Table of Descriptions by Event ID

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

Taken from documentation.solarwinds.com

However, it is not enable by default as enabling it may cause event flood and thus leading to performance issue.

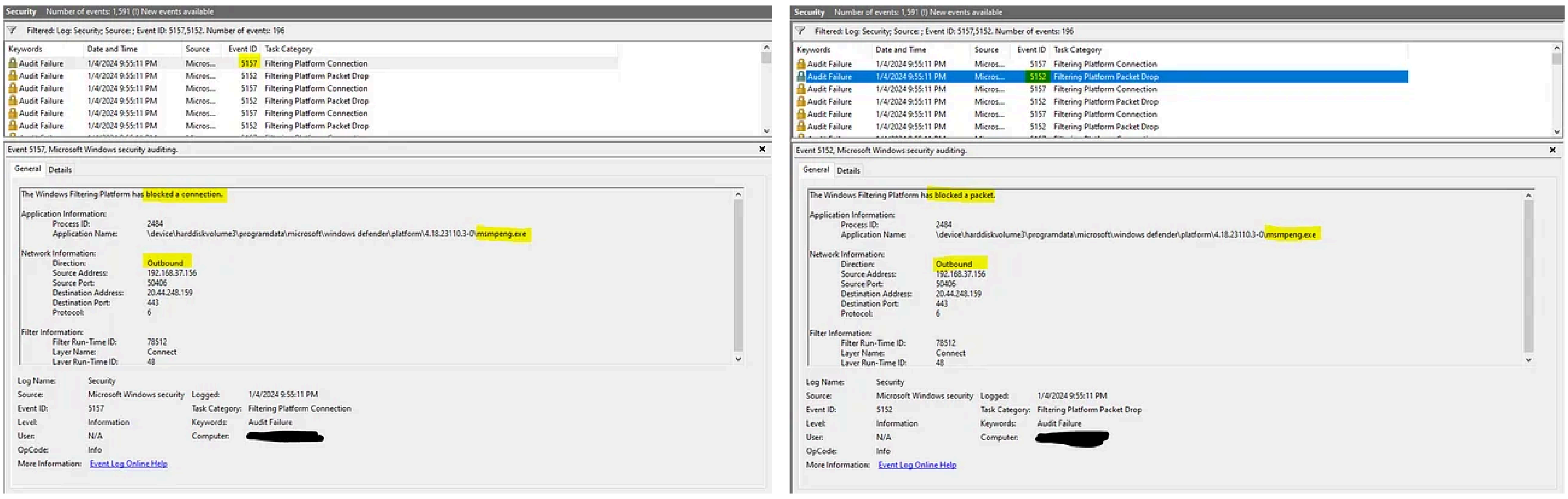


Security Settings
- Account Policies
- Local Policies
- Windows Defender Firewall with Adva
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Compute
- Advanced Audit Policy Configuration
  - System Audit Policies - Local Grou
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing

Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Not Configured
Audit File Share	Not Configured
Audit File System	Not Configured
Audit Filtering Platform Connection	Success and Failure
Audit Filtering Platform Packet Drop	Success and Failure
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

Enabling WFP Audit

There is a down side on this audit as it won't immediately log the WFP filter rule add event from EDRSilencer once the EDRSilencer added the WFP rule to block the outbound connection of the EDR process. Those WFP events **only log if the user execute any files (e.g. Laucnhing mimikatz.exe) that will trigger EDR to send out event data to its server.**



Filtered: Log: Security; Source: ; Event ID: 5157,5152. Number of events: 196

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5157	Filtering Platform Connection
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5152	Filtering Platform Packet Drop
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5157	Filtering Platform Connection
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5152	Filtering Platform Packet Drop
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5157	Filtering Platform Connection
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5152	Filtering Platform Packet Drop

Event 5157, Microsoft Windows security auditing.

```
The Windows Filtering Platform has blocked a connection.

Application Information:
        Process ID:             2484
        Application Name:       \device\harddiskvolume3\programdata\microsoft\windows defender\platform\4.18.23110.3-0\msmpeng.exe

Network Information:
        Direction:              Outbound
        Source Address:         192.168.37.156
        Source Port:            50406
        Destination Address:    20.44.248.159
        Destination Port:       443
        Protocol:               6

Filter Information:
        Filter Run-Time ID:     78512
        Layer Name:             Connect
        Layer Run-Time ID:      48
```

Log Name: Security
Source: Microsoft Windows security
Logged: 1/4/2024 9:55:11 PM
Event ID: 5157
Task Category: Filtering Platform Connection
Level: Information
Keywords: Audit Failure
User: N/A
Computer: [redacted]
OpCode: Info
More Information: Event Log Online Help

Security Number of events: 1,591 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 5157,5152. Number of events: 196

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5157	Filtering Platform Connection
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5152	Filtering Platform Packet Drop
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5157	Filtering Platform Connection
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5152	Filtering Platform Packet Drop
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5157	Filtering Platform Connection
Audit Failure	1/4/2024 9:55:11 PM	Micros...	5152	Filtering Platform Packet Drop

Event 5152, Microsoft Windows security auditing.

```
The Windows Filtering Platform has blocked a packet.

Application Information:
        Process ID:             2484
        Application Name:       \device\harddiskvolume3\programdata\microsoft\windows defender\platform\4.18.23110.3-0\msmpeng.exe

Network Information:
        Direction:              Outbound
        Source Address:         192.168.37.156
        Source Port:            50406
        Destination Address:    20.44.248.159
        Destination Port:       443
        Protocol:               6

Filter Information:
        Filter Run-Time ID:     78512
        Layer Name:             Connect
        Layer Run-Time ID:      48
```

Log Name: Security
Source: Microsoft Windows security
Logged: 1/4/2024 9:55:11 PM
Event ID: 5152
Task Category: Filtering Platform Packet Drop
Level: Information
Keywords: Audit Failure
User: N/A
Computer: [redacted]
OpCode: Info
More Information: Event Log Online Help

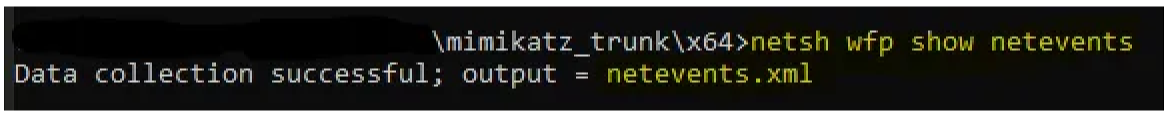
EID 5157 & 5152

Screenshots above are the events EID `5157` & `5152` that the outbound connection from `msmpeng.exe` being blocked by the WFP rule (I don't have EDR in my environment, so I'm just using it as example 🤣)

Thanks for the blog from Soren, there is another event log for the MDE agent which is **Microsoft-Windows-SENSE/Operational** that will log any failed connection from MDE to the server as EID `5`. Probably different EDR will have different ways of logging this kind of event.

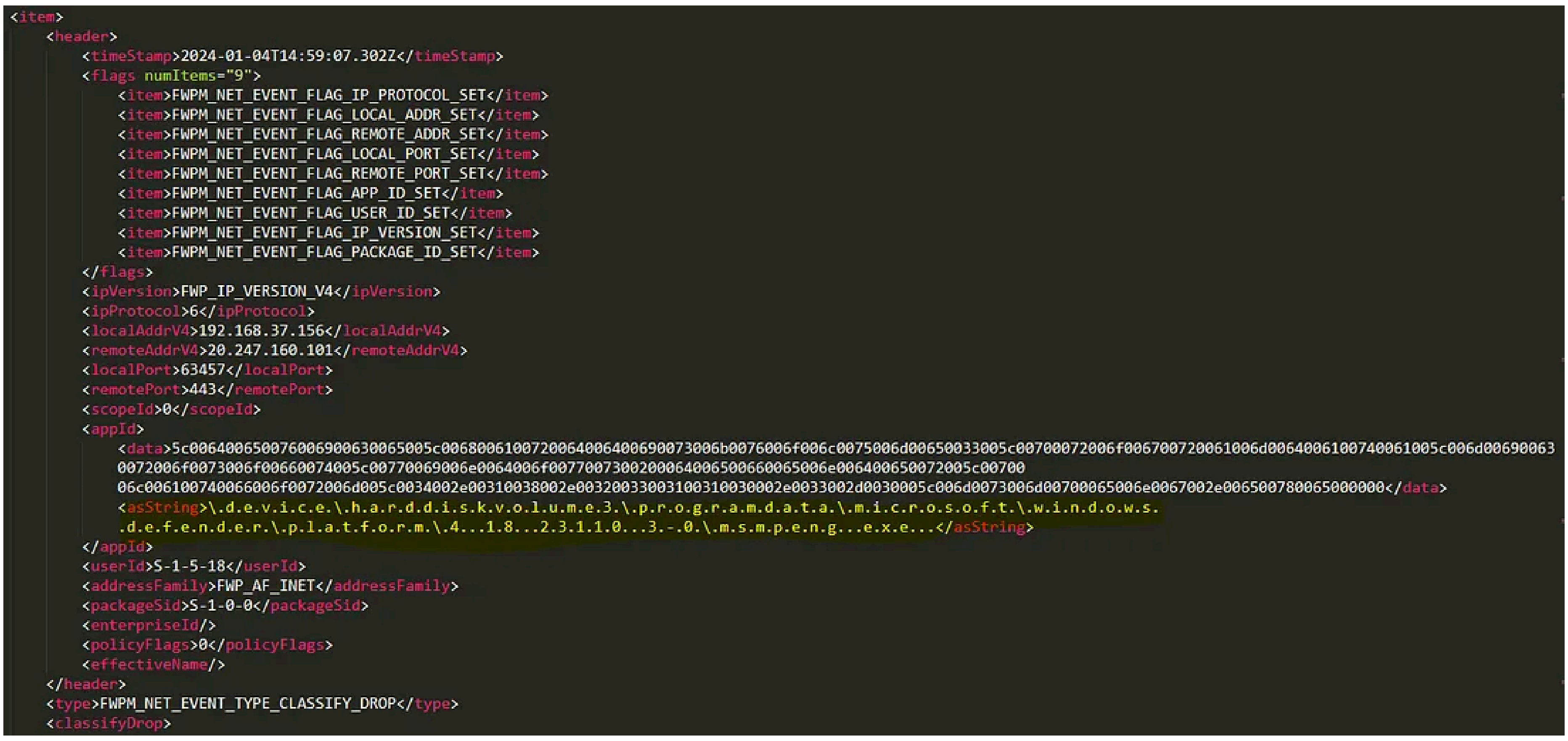
Netsh

We also can leverage `netsh wfp show netevents` command to get the WFP events in `xml` form.



```
[redacted]\mimikatz_trunk\x64>netsh wfp show netevents
Data collection successful; output = netevents.xml
```

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.



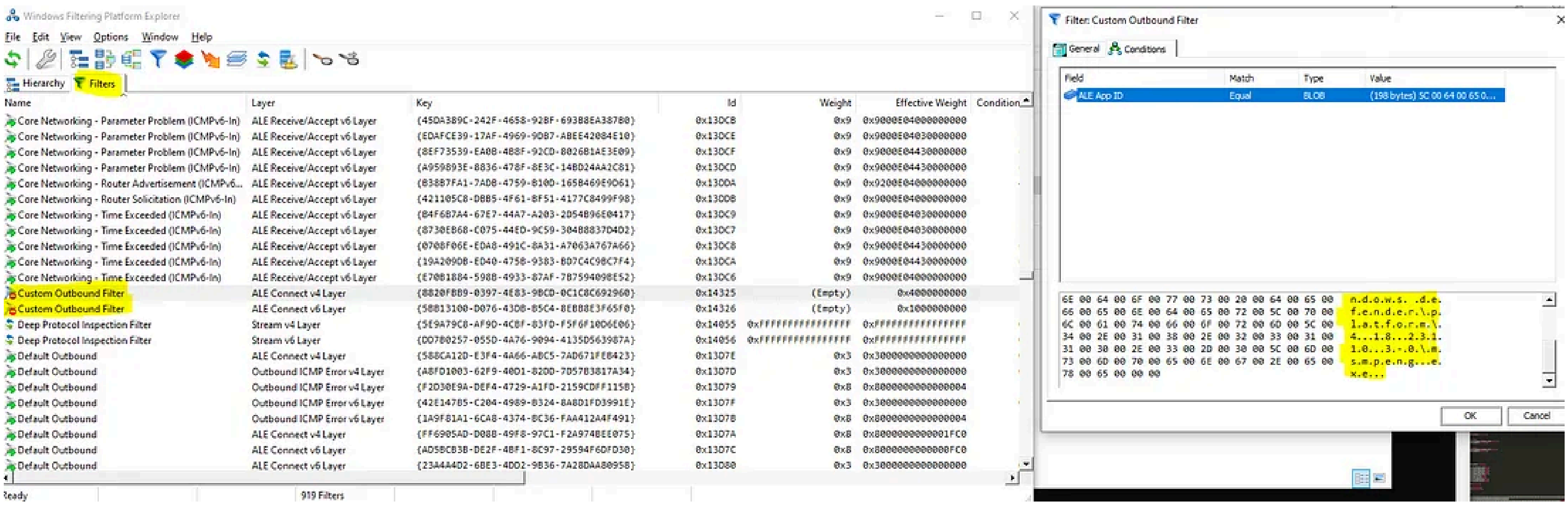
```
<item>
    <header>
        <timeStamp>2024-01-04T14:59:07.302Z</timeStamp>
        <flags numItems="9">
            <item>FWPM_NET_EVENT_FLAG_IP_PROTOCOL_SET</item>
            <item>FWPM_NET_EVENT_FLAG_LOCAL_ADDR_SET</item>
            <item>FWPM_NET_EVENT_FLAG_REMOTE_ADDR_SET</item>
            <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>
        <ipProtocol>6</ipProtocol>
        <localAddrV4>192.168.37.156</localAddrV4>
        <remoteAddrV4>20.247.160.101</remoteAddrV4>
        <localPort>63457</localPort>
        <remotePort>443</remotePort>
        <scopeId>0</scopeId>
        <appId>
            <data>5c006400650076006900630065005c006800610072006400640069007300b0076006f006c0075006d00650033005c00700072006f006700720061006d006400610074061005c006d00690063
            0072006f0073006f00660074005c00770069006e0064006f00770073002000640065006600650006e006400650072005c00700
            06c006100740066006f0072006d005c0034002e00310038002e0032003300310031000002e0033002d0030005c006d0073006d00700065006e0067002e006500780065000000</data>
            <asString>\.d.e.v.i.c.e.\.h.a.r.d.d.i.s.k.v.o.l.u.m.e.3.\.p.r.o.g.r.a.m.d.a.t.a.\.m.i.c.r.o.s.o.f.t.\.w.i.n.d.o.w.s.
            .d.e.f.e.n.d.e.r.\.p.l.a.t.f.o.r.m.\.4...1.8...2.3.1.1.0...3.-.0.\.m.s.m.p.e.n.g...e.x.e...</asString>
        </appId>
        <userId>S-1-5-18</userId>
        <addressFamily>FWP_AF_INET</addressFamily>
        <packageSid>S-1-0-0</packageSid>
        <enterpriseId/>
        <policyFlags>0</policyFlags>
        <effectiveName/>
    </header>
    <type>FWPM_NET_EVENT_TYPE_CLASSIFY_DROP</type>
    <classifyDrop>
```

netviews.xml

WFPExplorer

WFPExplorer from zodiacon is a GUI tools that can look for the WFP objects. Look for the `Filters` and we can find the hard coded filter name from EDRSilencer, `Custom Outbound Filter` in there.

Note that, the `ALE App ID` bytes in WFPExplorer the matches with the App ID in `netviews.xml` (`<appId> > <data>` tag)



Windows Filtering Platform Explorer
File Edit View Options Window Help
Hierarchy
Filters

Name	Layer	Key	Id	Weight	Effective Weight	Condition
Core Networking - Parameter Problem (ICMPv6-In)	ALE Receive/Accept v6 Layer	{45DA389C-242F-4658-928F-69388EA38780}	0x13DCB	0x9	0x9000E04000000000	
Core Networking - Parameter Problem (ICMPv6-In)	ALE Receive/Accept v6 Layer	{EDAFCE39-17AF-4969-9D87-ABEE42084E10}	0x13DCE	0x9	0x9000E04030000000	
Core Networking - Parameter Problem (ICMPv6-In)	ALE Receive/Accept v6 Layer	{8EF73539-EA08-488F-92CD-8026B1AE3E09}	0x13DCF	0x9	0x9000E04430000000	
Core Networking - Parameter Problem (ICMPv6-In)	ALE Receive/Accept v6 Layer	{A959893E-8836-478F-8E3C-148D24AA2C81}	0x13DCD	0x9	0x9000E04430000000	
Core Networking - Router Advertisement (ICMPv6...	ALE Receive/Accept v6 Layer	{83887FA1-7AD8-4759-8100-165B469E9D61}	0x13DDA	0x9	0x9200E04000000000	
Core Networking - Router Solicitation (ICMPv6-In)	ALE Receive/Accept v6 Layer	{421105C8-D8B5-4F61-8F51-4177C8499F98}	0x13DD8	0x9	0x9000E04000000000	
Core Networking - Time Exceeded (ICMPv6-In)	ALE Receive/Accept v6 Layer	{84F6B7A4-67E7-44A7-A203-2D54B96E0417}	0x13DC9	0x9	0x9000E04030000000	
Core Networking - Time Exceeded (ICMPv6-In)	ALE Receive/Accept v6 Layer	{8730EB68-C075-44ED-9C59-30488837D4D2}	0x13DC7	0x9	0x9000E04030000000	
Core Networking - Time Exceeded (ICMPv6-In)	ALE Receive/Accept v6 Layer	{0708F06E-EDA8-491C-8A31-A7063A767A66}	0x13DC8	0x9	0x9000E04430000000	
Core Networking - Time Exceeded (ICMPv6-In)	ALE Receive/Accept v6 Layer	{19A209DB-ED40-4758-9383-BD7C4C98C7F4}	0x13DCA	0x9	0x9000E04430000000	
Core Networking - Time Exceeded (ICMPv6-In)	ALE Receive/Accept v6 Layer	{E7081884-5988-4933-87AF-787594098E52}	0x13DC6	0x9	0x9000E04000000000	
Custom Outbound Filter	ALE Connect v4 Layer	{8820FBB9-0397-4E83-9BCD-0C1C8C692960}	0x14325	(Empty)	0x4000000000	
Custom Outbound Filter	ALE Connect v6 Layer	{58813100-D076-43D8-85C4-8EB88E3F65F0}	0x14326	(Empty)	0x1000000000	
Deep Protocol Inspection Filter	Stream v4 Layer	{5E9A79C8-AF9D-4C8F-83FD-F5F6F10D6E06}	0x14055	0xFFFFFFFFFFFFFFFF	0xFFFFFFFFFFFFFFFF	
Deep Protocol Inspection Filter	Stream v6 Layer	{DD780257-055D-4A76-9094-4135D563987A}	0x14056	0xFFFFFFFFFFFFFFFF	0xFFFFFFFFFFFFFFFF	
Default Outbound	ALE Connect v4 Layer	{588CA12D-E3F4-4A66-ABC5-7AD671FE8423}	0x13D7E	0x3	0x3000000000000000	
Default Outbound	Outbound ICMP Error v4 Layer	{A8FD1003-62F9-40D1-820D-7D57B3817A34}	0x13D7D	0x3	0x3000000000000000	
Default Outbound	Outbound ICMP Error v4 Layer	{F2D30E9A-DEF4-4729-A1FD-2159CDFF115B}	0x13D79	0x8	0x8000000000000004	
Default Outbound	Outbound ICMP Error v6 Layer	{42E147B5-C204-4989-B324-8A8D1FD3991E}	0x13D7F	0x3	0x3000000000000000	
Default Outbound	Outbound ICMP Error v6 Layer	{1A9F81A1-6CA8-4374-8C36-FAA412A4F491}	0x13D7B	0x8	0x8000000000000004	
Default Outbound	ALE Connect v4 Layer	{FF6905AD-D08B-49F8-97C1-F2A974BEE075}	0x13D7A	0x8	0x80000000000001FC0	
Default Outbound	ALE Connect v6 Layer	{AD58C83B-DE2F-48F1-8C97-29594F6DFD30}	0x13D7C	0x8	0x8000000000000FC0	
Default Outbound	ALE Connect v6 Layer	{23A4A4D2-6BE3-4DD2-9B36-7A28DAA8095B}	0x13D80	0x3	0x3000000000000000	

Ready 919 Filters

Filter: Custom Outbound Filter

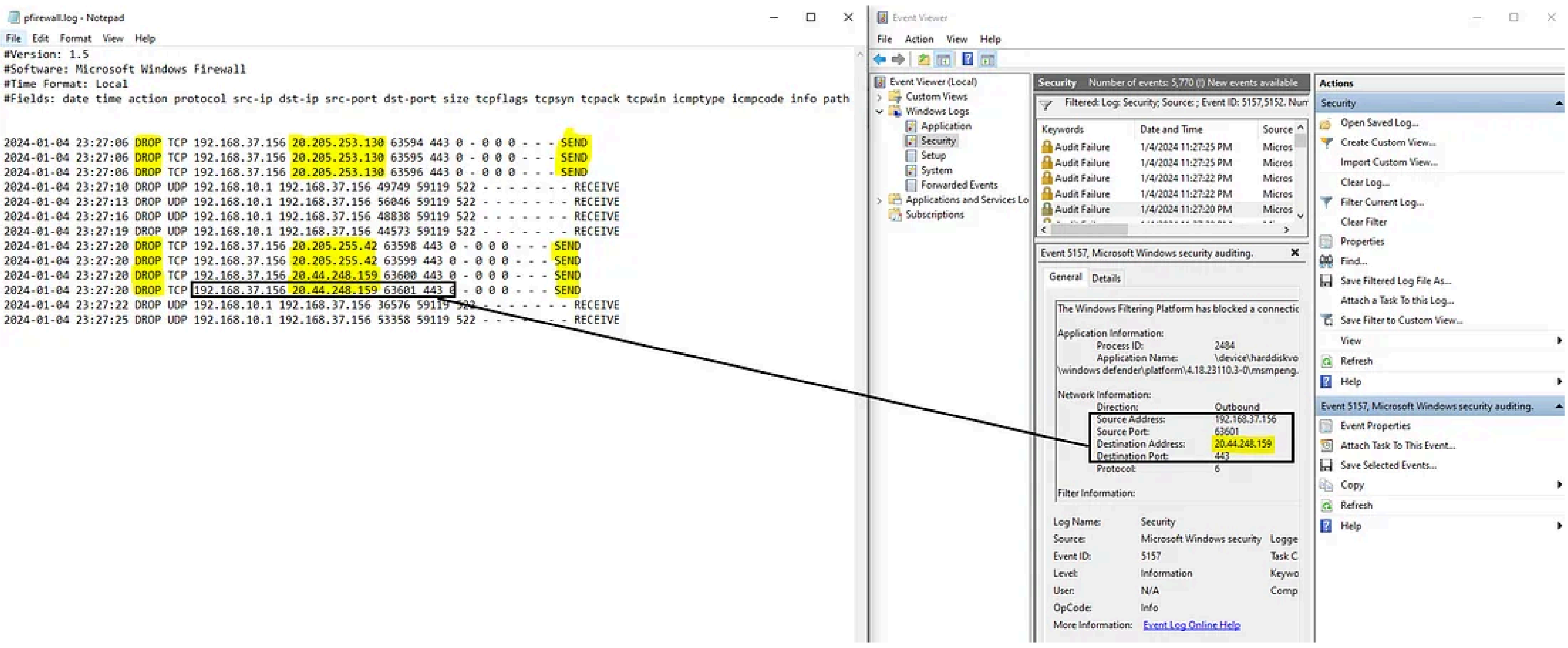
Field	Match	Type	Value
ALE App ID	Equal	BLOB	(198 bytes) 5C 00 64 00 65 0...

```
6E 00 64 00 6F 00 77 00 73 00 20 00 64 00 65 00    n.d.o.w.s. .d.e.
66 00 65 00 6E 00 64 00 65 00 72 00 5C 00 70 00    f.e.n.d.e.r.\.p.
6C 00 61 00 74 00 66 00 6F 00 72 00 6D 00 5C 00    l.a.t.f.o.r.m.\.
34 00 2E 00 31 00 38 00 2E 00 32 00 33 00 31 00    4...1.8...2.3.1.
31 00 30 00 2E 00 33 00 2D 00 30 00 5C 00 6D 00    1.0...3.-.0.\.m.
73 00 6D 00 70 00 65 00 6E 00 67 00 2E 00 65 00    s.m.p.e.n.g...e.
78 00 65 00 00 00                                  x.e...
```

EDRSilencer filter on WFPExplorer

Firewall Logs

Firewall logs also contains some useful information (Src & Dest IPs, packet size etc) to support further support the events stored in security event log.



```
#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


2024-01-04 23:27:06 DROP TCP 192.168.37.156 20.205.253.130 63594 443 0 - 0 0 0 - - - SEND
2024-01-04 23:27:06 DROP TCP 192.168.37.156 20.205.253.130 63595 443 0 - 0 0 0 - - - SEND
2024-01-04 23:27:06 DROP TCP 192.168.37.156 20.205.253.130 63596 443 0 - 0 0 0 - - - SEND
2024-01-04 23:27:10 DROP UDP 192.168.10.1 192.168.37.156 49749 59119 522 - - - - - - - RECEIVE
2024-01-04 23:27:13 DROP UDP 192.168.10.1 192.168.37.156 56046 59119 522 - - - - - - - RECEIVE
2024-01-04 23:27:16 DROP UDP 192.168.10.1 192.168.37.156 48838 59119 522 - - - - - - - RECEIVE
2024-01-04 23:27:19 DROP UDP 192.168.10.1 192.168.37.156 44573 59119 522 - - - - - - - RECEIVE
2024-01-04 23:27:20 DROP TCP 192.168.37.156 20.205.255.42 63598 443 0 - 0 0 0 - - - SEND
2024-01-04 23:27:20 DROP TCP 192.168.37.156 20.205.255.42 63599 443 0 - 0 0 0 - - - SEND
2024-01-04 23:27:20 DROP TCP 192.168.37.156 20.44.248.159 63600 443 0 - 0 0 0 - - - SEND
2024-01-04 23:27:20 DROP TCP 192.168.37.156 20.44.248.159 63601 443 0 - 0 0 0 - - - SEND
2024-01-04 23:27:22 DROP UDP 192.168.10.1 192.168.37.156 36576 59119 522 - - - - - - - RECEIVE
2024-01-04 23:27:25 DROP UDP 192.168.10.1 192.168.37.156 53358 59119 522 - - - - - - - RECEIVE
```

Security Number of events: 5,770 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 5157,5152. Num

Keywords	Date and Time	Source
Audit Failure	1/4/2024 11:27:25 PM	Micros
Audit Failure	1/4/2024 11:27:25 PM	Micros
Audit Failure	1/4/2024 11:27:22 PM	Micros
Audit Failure	1/4/2024 11:27:22 PM	Micros
Audit Failure	1/4/2024 11:27:20 PM	Micros

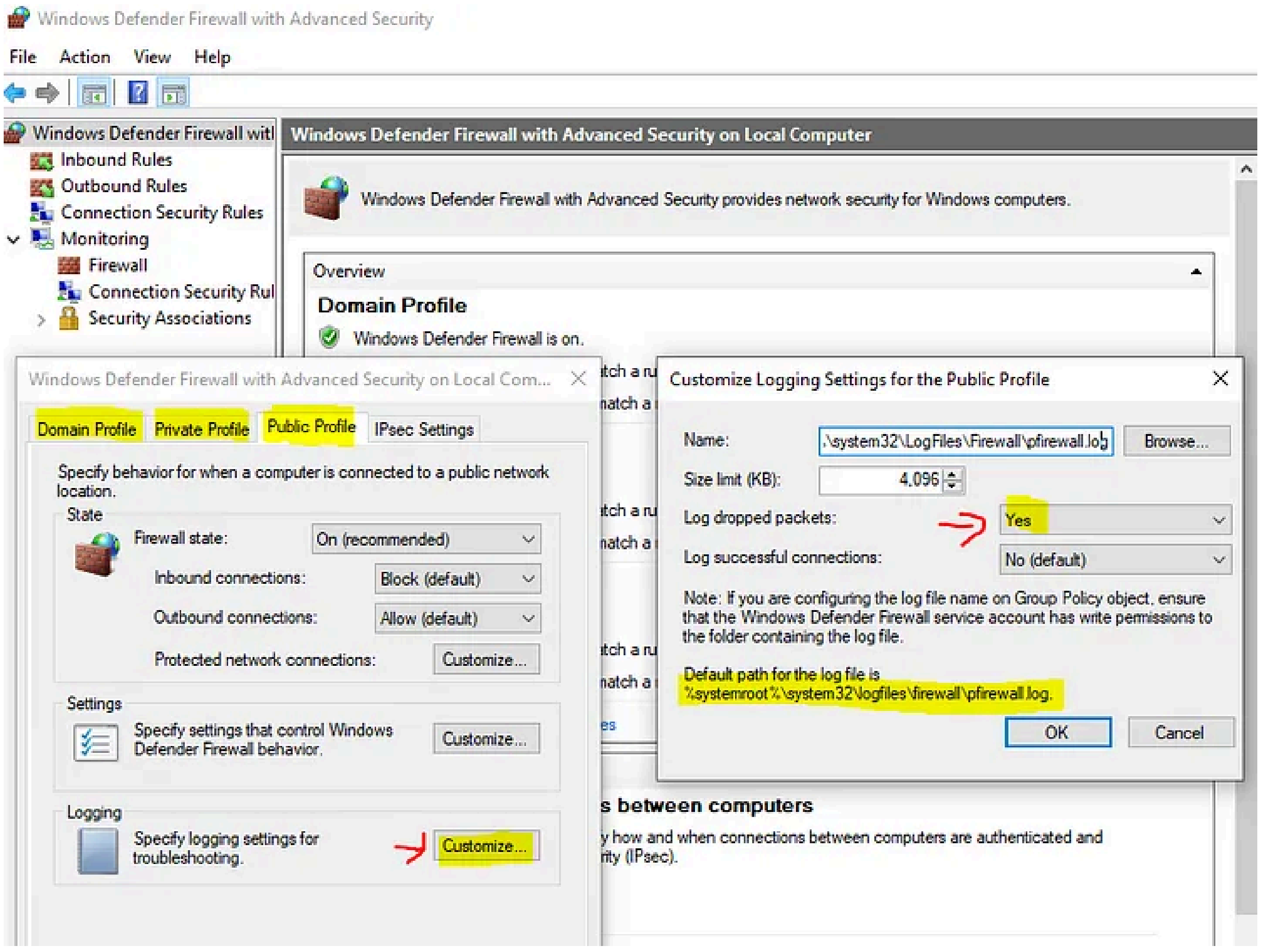
Event 5157, Microsoft Windows security auditing.

```
The Windows Filtering Platform has blocked a connectic

Application Information:
        Process ID:             2484
        Application Name:       \device\harddiskvo
\windows defender\platform\4.18.23110.3-0\msmpeng.

Network Information:
        Direction:              Outbound
        Source Address:         192.168.37.156
        Source Port:            63601
        Destination Address:    20.44.248.159
        Destination Port:       443
        Protocol:               6

Filter Information:
```

Log Name: Security
Source: Microsoft Windows security Logge
Event ID: 5157 Task C
Level: Information Keywo
User: N/A Comp
OpCode: Info
More Information: Event Log Online Help

Dropped packet data in pfirewall.log that supports events in security event log

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.


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Windows Defender Firewall with Advanced Security on Local Computer
Overview
Domain Profile
Windows Defender Firewall is on.
s between computers
Windows Defender Firewall with Advanced Security on Local Com...
Domain Profile
Private Profile
Public Profile
IPsec Settings
State
Settings
Logging
Customize...
Customize Logging Settings for the Public Profile
Browse...
OK
Cancel

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

Specify behavior for when a computer is connected to a public network location.

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Specify settings that control Windows Defender Firewall behavior.

Specify logging settings for troubleshooting.

Name: \system32\LogFiles\Firewall\pfirewall.log

Size limit (KB): 4,096

Log dropped packets: Yes

Log successful connections: No (default)

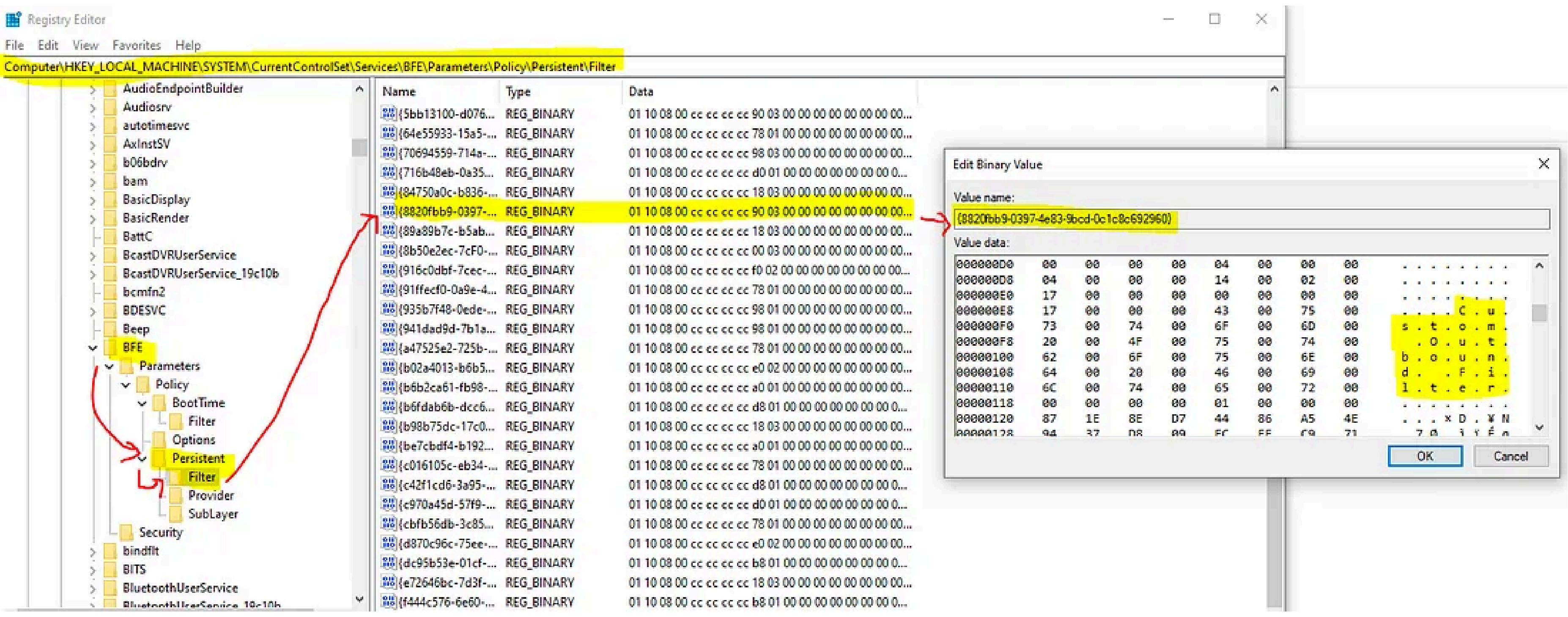
Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

Once enabled the `Log dropped packets`, any dropped packet will be logged in `%systemroot%\system32\logfiles\firewall\pfirewall.log`

Registry Key

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`



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

AudioEndpointBuilder
Audiosrv
autotimesvc
AxInstSV
b06bdrv
bam
BasicDisplay
BasicRender
BattC
BcastDVRUserService
BcastDVRUserService_19c10b
bcmfn2
BDESVC
Beep
BFE
  Parameters
    Policy
      BootTime
        Filter
      Options
      Persistent
        Filter
        Provider
        SubLayer
  Security
bindflt
BITS
BluetoothUserService
BluetoothUserService_19c10b
```

```
Name                Type         Data
{5bb13100-d076-...  REG_BINARY   01 10 08 00 cc cc cc cc 90 03 00 00 00 00 00 00 00 00...
{64e55933-15a5-...  REG_BINARY   01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{70694559-714a-...  REG_BINARY   01 10 08 00 cc cc cc cc 98 03 00 00 00 00 00 00 00 00...
{716b48eb-0a35...   REG_BINARY   01 10 08 00 cc cc cc cc d0 01 00 00 00 00 00 00 00 0...
{84750a0c-b836-...  REG_BINARY   01 10 08 00 cc cc cc cc 18 03 00 00 00 00 00 00 00 00...
{8820fbb9-0397-...  REG_BINARY   01 10 08 00 cc cc cc cc 90 03 00 00 00 00 00 00 00 00...
{89a89b7c-b5ab...   REG_BINARY   01 10 08 00 cc cc cc cc 18 03 00 00 00 00 00 00 00 00...
{8b50e2ec-7cF0-...  REG_BINARY   01 10 08 00 cc cc cc cc 00 03 00 00 00 00 00 00 00 00...
{916c0dbf-7cec-...  REG_BINARY   01 10 08 00 cc cc cc cc f0 02 00 00 00 00 00 00 00 00...
{91ffecf0-0a9e-4... REG_BINARY   01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{935b7f48-0ede-...  REG_BINARY   01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{941dad9d-7b1a...   REG_BINARY   01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{a47525e2-725b-...  REG_BINARY   01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{b02a4013-b6b5...   REG_BINARY   01 10 08 00 cc cc cc cc e0 02 00 00 00 00 00 00 00 00...
{b6b2ca61-fb98-...  REG_BINARY   01 10 08 00 cc cc cc cc a0 01 00 00 00 00 00 00 00 00...
{b6fdab6b-dcc6...   REG_BINARY   01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{b98b75dc-17c0...   REG_BINARY   01 10 08 00 cc cc cc cc 18 03 00 00 00 00 00 00 00 00...
{be7cbdf4-b192...   REG_BINARY   01 10 08 00 cc cc cc cc a0 01 00 00 00 00 00 00 00 00...
{c016105c-eb34-...  REG_BINARY   01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{c42f1cd6-3a95-...  REG_BINARY   01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{c970a45d-57f9-...  REG_BINARY   01 10 08 00 cc cc cc cc d0 01 00 00 00 00 00 00 00 0...
{cbfb56db-3c85...   REG_BINARY   01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{d870c96c-75ee-...  REG_BINARY   01 10 08 00 cc cc cc cc e0 02 00 00 00 00 00 00 00 00...
{dc95b53e-01cf-...  REG_BINARY   01 10 08 00 cc cc cc cc b8 01 00 00 00 00 00 00 00 0...
{e72646bc-7d3f-...  REG_BINARY   01 10 08 00 cc cc cc cc 18 03 00 00 00 00 00 00 00 00...
{f444c576-6e60-...  REG_BINARY   01 10 08 00 cc cc cc cc b8 01 00 00 00 00 00 00 00 0...
```

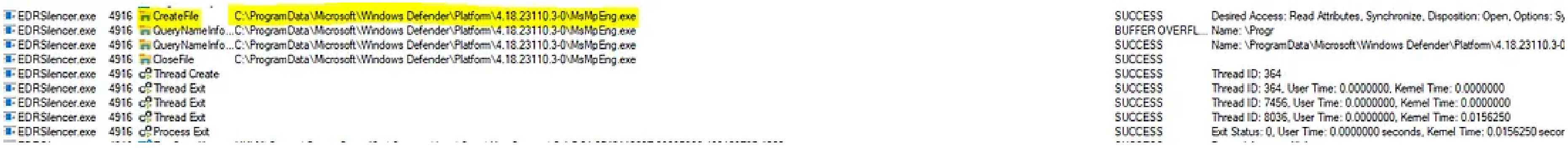
```
Edit Binary Value

Value name:
{8820fbb9-0397-4e83-9bcd-0c1c8c692960}

Value data:
000000D0  00 00 00 00 04 00 00 00   . . . . . . . .
000000D8  04 00 00 00 14 00 02 00   . . . . . . . .
000000E0  17 00 00 00 00 00 00 00   . . . . . . . .
000000E8  17 00 00 00 43 00 75 00   . . . . C . u .
000000F0  73 00 74 00 6F 00 6D 00   s . t . o . m .
000000F8  20 00 4F 00 75 00 74 00     . O . u . t .
00000100  62 00 6F 00 75 00 6E 00   b . o . u . n .
00000108  64 00 20 00 46 00 69 00   d .   . F . i .
00000110  6C 00 74 00 65 00 72 00   l . t . e . r .
00000118  00 00 00 00 01 00 00 00   . . . . . . . .
00000120  87 1E 8E D7 44 86 A5 4E   . . . . x D . ¥ N
```

Some extra reading on the WFP from QuarksLab.

Host Events

EDRSilencer have to load the `msmpeng.exe` in order to pass EDR process into the WFP filter function (Relevant **code**). So theoretically, the loading process will still get log by EDR.

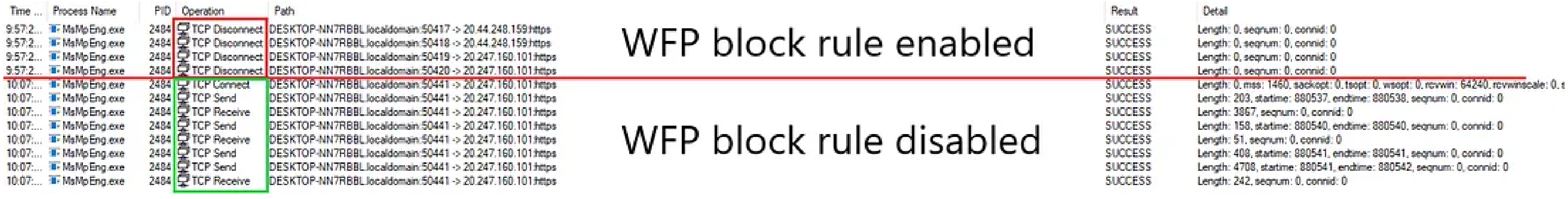
However, this is just a clue for the investigator that a EDR process has been loaded.



```
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: Sy
EDRSilencer.exe  4916  QueryNameInfo...   C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23110.3-0\MsMpEng.exe  BUFFER OVERFL...  Name: \Progr
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: 0.0000000, Kernel Time: 0.0000000
EDRSilencer.exe  4916  Thread Exit                                                                                       SUCCESS          Thread ID: 7456, User Time: 0.0000000, Kernel Time: 0.0000000
EDRSilencer.exe  4916  Thread Exit                                                                                       SUCCESS          Thread ID: 8036, User Time: 0.0000000, Kernel Time: 0.0156250
EDRSilencer.exe  4916  Process Exit                                                                                      SUCCESS          Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0156250 secor
```

EDR process file has been loaded by EDRSilencer 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 be not visible in EDR since the WFP block rule has been applied on the EDR process.



```
Time ...  Process Name  PID   Operation       Path                                                         Result   Detail
9:57:2... MsMpEng.exe   2484  TCP Disconnect  DESKTOP-NN7RBBL.localdomain:50417 -> 20.44.248.159:https     SUCCESS  Length: 0, seqnum: 0, connid: 0
9:57:2... MsMpEng.exe   2484  TCP Disconnect  DESKTOP-NN7RBBL.localdomain:50418 -> 20.44.248.159:https     SUCCESS  Length: 0, seqnum: 0, connid: 0
9:57:2... MsMpEng.exe   2484  TCP Disconnect  DESKTOP-NN7RBBL.localdomain:50419 -> 20.247.160.101:https    SUCCESS  Length: 0, seqnum: 0, connid: 0
9:57:2... MsMpEng.exe   2484  TCP Disconnect  DESKTOP-NN7RBBL.localdomain:50420 -> 20.247.160.101:https    SUCCESS  Length: 0, seqnum: 0, connid: 0
10:07:... MsMpEng.exe   2484  TCP Connect     DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, rcvwin: 64240, rcvwinscale: 0, s
10:07:... MsMpEng.exe   2484  TCP Send        DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 203, startime: 880537, endtime: 880538, seqnum: 0, connid: 0
10:07:... MsMpEng.exe   2484  TCP Receive     DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 3867, seqnum: 0, connid: 0
10:07:... MsMpEng.exe   2484  TCP Send        DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 158, startime: 880540, endtime: 880540, seqnum: 0, connid: 0
10:07:... MsMpEng.exe   2484  TCP Receive     DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 51, seqnum: 0, connid: 0
10:07:... MsMpEng.exe   2484  TCP Send        DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 408, startime: 880541, endtime: 880541, seqnum: 0, connid: 0
10:07:... MsMpEng.exe   2484  TCP Send        DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 4708, startime: 880541, endtime: 880542, seqnum: 0, connid: 0
10:07:... MsMpEng.exe   2484  TCP Receive     DESKTOP-NN7RBBL.localdomain:50441 -> 20.247.160.101:https    SUCCESS  Length: 242, seqnum: 0, connid: 0
```

Difference on the TCP events when WFP block enabled and disabled by EDRSilencer

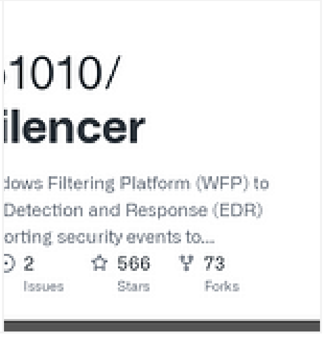
Hopefully, this quick blog post helps and remember check both **IPv4** and **IPv6** WFP rules, cheers !!

References

GitHub - netero1010/EDRSilencer: A tool uses Windows Filtering Platform (WFP) to block Endpoint…

A tool uses Windows Filtering Platform (WFP) to block Endpoint Detection and Response (EDR) agents from reporting…

github.com


1010/
ilencer
lows Filtering Platform (WFP) to
Detection and Response (EDR)
orting security events to...
2
Issues
566
Stars
73
Forks

Collect Windows Filtering Platform (WFP) events

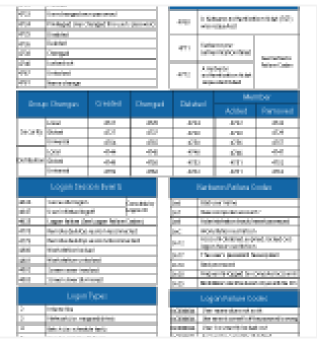
This topic describes how to collect Windows Filtering Platform (WFP) events in SEM.

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…

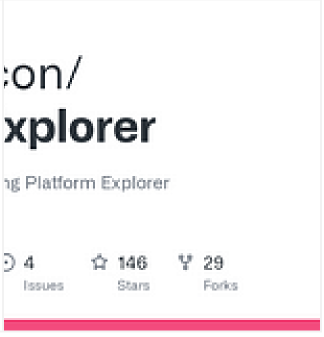
www.ultimatewindowssecurity.com



GitHub - zodiacon/WFPExplorer: Windows Filtering Platform Explorer

Windows Filtering Platform Explorer. Contribute to zodiacon/WFPExplorer development by creating an account on…

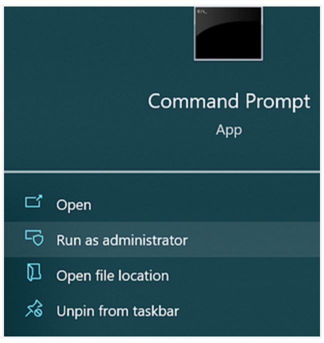
github.com



Windows is Blocking Traffic!

In this blog, I'd like to show you some of the techniques I use to troubleshoot when the only thing that makes sense is…

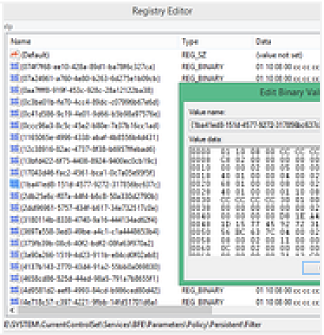
www.lookingpoint.com



Windows Filtering Platform: Persistent state under the hood

Since Windows XP SP2, the Windows firewall is deployed and enabled by default in every Microsoft Windows operating…

blog.quarkslab.com



Cybersecurity

Threat Hunting

Computer Forensics

Digital Forensics

Blue Team

--

Written by GhouLSec

Follow

218 Followers

Typical memes addict 🐿️ from Malaysia. GitHub: https://github.com/ghoulgy 🍕 Support my work: https://www.buymeacoffee.com/GhoulSec

Help Status About Careers Press Blog Privacy Terms Text to speech Teams