How to Monitor Network Activity with the Windows Security & Firewall Logs to Detect Inbound and Outbound Attacks

Sponsored by solarwinds

Thanks to

- Made possible by solarwinds LOG & EVENT MANAGER www.solarwinds.com

Mav Turner, Director of Product Marketing and Business Strategy

Preview of Key Points

- What kinds of activity can you audit?
- Use cases
- 2 options
  - Windows Firewall auditing
  - Windows Firewall logging
- Auditing
  - How to enable
  - Event IDs
- Logging
  - How to enable
  - Reading the logs

Windows Firewall monitoring

- 2 options
  - Auditing
    - Security log
    - Easy to understand messages
    - Includes local process name, filter info
    - Inflates the size of the Security log
  - Logging
    - %systemroot%\system32\LogFiles\Firewall\pfirewall.log
    - W3C Extended Log File Format
      - Space delimited text file
      - With file name headers
    - No local process name
    - No Security log overhead
    - After max size reached
      - File renamed to pfirewall.log.old
      - Existing old deleted

Windows Firewall Text File Logging

- Enable for each profile
- Group policy available
- Only actions logged
  - Allow
  - Drop
- No logging if profile "off"

```
#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

2014-12-10 07:36:21 ALLOW TCP 192.168.10.2 132.245.88.194 51329 443 0 - 0 0 0 - - - SEND
2014-12-10 07:36:22 ALLOW UDP 192.168.10.2 200.32.248.1 53799 53 0 - - - - - - - SEND
2014-12-10 07:36:22 ALLOW UDP 127.0.0.1 127.0.0.1 61444 61444 0 - - - - - - - SEND
2014-12-10 07:36:26 ALLOW UDP 192.168.10.2 83.23.207.210 58384 29911 0 - - - - - - - SEND
2014-12-10 07:36:26 ALLOW UDP 192.168.10.2 188.186.163.240 58384 43927 0 - - - - - - - SEND
2014-12-10 07:36:26 ALLOW UDP 192.168.10.2 82.204.201.110 58384 9527 0 - - - - - - - SEND
2014-12-10 07:36:26 ALLOW UDP 192.168.10.2 189.54.112.10 58384 2454 0 - - - - - - - SEND
2014-12-10 07:36:27 ALLOW UDP 192.168.10.2 64.4.23.158 58384 443 0 - - - - - - - SEND
2014-12-10 07:36:29 ALLOW TCP 192.168.10.2 157.56.240.137 51334 80 0 - 0 0 0 - - - SEND
```

Windows Auditing

- Audit policy subcategories
  - Filtering Platform Packet Drop
  - Filtering Platform Connection
  - Group policy available
- Windows Firewall configuration
  - Events logged whether Firewall is on or off
  - Don't shutdown the Windows Firewall service

Filtering Platform Connection

- These are the 2 core events
- Interesting for both inbound and outbound
  - 5156 The Windows Filtering Platform has allowed a connection
  - 5157 The Windows Filtering Platform has blocked a connection
- Acting as a server
  - Filter on **inbound**
- Acting as a client
  - Filter on **outbound**

Filtering Platform Connection

- Can this computer accept inbound connections initiated from remote computers?
  - Windows 5154 - The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections
    - Event is pretty much redundant if because of 5156
  - ~~Windows 5155 - The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections~~
    - Doesn't get logged
    - Instead look at 5157 inbound

Filtering Platform Connection

- Not observed:
- ~~5151 A more restrictive Windows Filtering Platform filter has blocked a packet.~~
- ~~5150 The Windows Filtering Platform has blocked a packet~~
  - See 5152

Filtering Platform Packet Drop

- 5152: The Windows Filtering Platform has blocked a packet
- Can probably ignore altogether unless you are worried about stateful attacks
- Ignore for outbound
  - Already covered by other events

Filtering Platform Packet Drop

- ~~5031 The Windows Firewall Service blocked an application from accepting incoming connections on the network.~~
  - Not logged
- ~~5153 A more restrictive Windows Filtering Platform filter has blocked a packet~~
  - Not logged

Use cases

- Do you have Windows firewall turned on with actual traffic restrictions?
  - Monitoring security log for denials and drops
    - Something/someone trying to misuse network
    - Be alerted to broken end-user experience
  - Outbound
    - Malware on local system?
  - Inbound
    - Malware on some other system on network?

Use cases

- Monitor outbound connections
  - To Internet addresses
    - Compare against blacklists
  - To internal addresses
    - Look for port and address scan patterns
    - Look for new addresses accessed for the first time

Bottom line

- Firewall logging generates a lot of data
- Analysis requires heavy duty search and correlation
- Firewall log data should be correlated with other types of log data
  - Problematic without categorization
- Check out SolarWinds Log and Event Manager