CHECKLIST

Windows 10 Defender Firewall Audit Logs Investigation Checklist

A practical checklist for validating, reading, and documenting Windows 10 Defender Firewall audit logs during security investigations.

Windows 10 Defender Firewall Audit Logs for Security Investigations

Purpose

Use this checklist to quickly validate whether Windows 10 Defender Firewall audit logs can support an investigation, and to avoid overclaiming what the logs prove.

When to use this checklist

- Suspected unauthorized access
- Lateral movement investigation
- Unexpected inbound or outbound connection attempts
- Policy enforcement or drift validation
- Service reachability issues that may involve host firewall rules

1) Confirm the log source is reliable

- [ ] Verify firewall auditing is enabled for the relevant firewall profile.
- [ ] Confirm the affected host is the correct endpoint in scope.
- [ ] Record the hostname, IP address, and any asset identifier.
- [ ] Note the system time, time zone, and whether the clock appears synchronized.
- [ ] Check whether log retention is sufficient for the investigation window.
- [ ] Identify whether the host is managed by local policy, Group Policy, or both.

2) Define the investigative question

- [ ] State the exact question you are trying to answer.
- [ ] Decide whether the issue is about allow/deny enforcement, connection failure, or suspicious communication.
- [ ] Identify the relevant source IP, destination IP, port, protocol, and direction.
- [ ] Set a time window around the event of interest.

3) Retrieve and preserve the evidence

- [ ] Export or copy the firewall log from the affected host.
- [ ] Preserve any supporting event logs from the same time window.
- [ ] Capture nearby security, system, and application events for correlation.
- [ ] Record the acquisition method and the time of collection.
- [ ] Note any missing records, gaps, or log rotation limits.

4) Review the firewall log entries

- [ ] Filter for the source and destination addresses of interest.
- [ ] Filter for the relevant port and protocol.
- [ ] Check the direction of traffic: inbound or outbound.

- [ ] Determine whether the action was allowed or blocked.
- [ ] Look for repeated attempts that suggest scanning, retry logic, or persistence.
- [ ] Compare timestamps to the incident timeline.

5) Correlate with host context

- [ ] Verify the active firewall profile at the time of the event.
- [ ] Check for recent rule changes or policy updates.
- [ ] Correlate with process creation, service changes, logon activity, and endpoint alerts.
- [ ] Confirm whether the behavior matches expected application or service traffic.
- [ ] Look for clock skew or time normalization issues across sources.

6) Interpret the findings carefully

- [ ] Treat firewall logs as enforcement records, not packet captures.
- [ ] Avoid claiming attacker intent based on the log alone.
- [ ] Do not assume an allow record means the traffic was benign or successful.
- [ ] Do not assume a block record proves malicious activity.
- [ ] Consider whether another device or policy could have affected the connection first.

7) Validate policy behavior

- [ ] Compare the observed action with the expected policy outcome.
- [ ] Check whether the host was on the expected profile when the event occurred.
- [ ] Confirm that local and centralized policy sources do not conflict.
- [ ] Identify whether the observed behavior reflects an exception, a rule scope issue, or a profile mismatch.
- [ ] Document any differences between expected and actual enforcement.

8) Document your conclusion

- [ ] Summarize what the firewall log does show.
- [ ] Summarize what it does not show.
- [ ] Note the confidence level of the finding.
- [ ] Include the supporting evidence used for correlation.
- [ ] Record any limitations: missing logs, incomplete retention, or uncertain time alignment.
- [ ] State the next action: containment, remediation, policy correction, or deeper analysis.

Quick interpretation guide

- Inbound blocked on expected service port: host firewall likely prevented the connection.
- Inbound allowed but service still failed: investigate the application, service binding, or upstream filtering.
- Outbound blocked to an unexpected destination: possible policy enforcement, misconfiguration, or attempted unauthorized communication.
- Repeated blocked administrative connections: may indicate scanning, probing, or failed lateral movement attempts.
- No relevant log entry: may indicate logging gaps, wrong host, wrong time window, or traffic that never reached the firewall.

Common pitfalls to avoid

- Reading the firewall log in isolation.
- Confusing host enforcement with network-wide visibility.
- Assuming the log is complete when retention is limited.

- Ignoring firewall profile changes.
- Overstating what a single record proves.

Minimal evidence package for an investigation note

- [ ] Hostname and asset ID
- [ ] Relevant time window
- [ ] Source and destination IPs
- [ ] Port, protocol, and traffic direction
- [ ] Allow or block outcome
- [ ] Correlated security or system events
- [ ] Policy/profile status at the time
- [ ] Evidence gaps or limitations

Final check

Before relying on the logs in production or for incident reporting, confirm:

- [ ] Logging was enabled
- [ ] The timestamp is trustworthy
- [ ] The affected host was correctly identified
- [ ] The relevant profile and policy source are known
- [ ] Supporting evidence was reviewed
- [ ] The conclusion stays within what the logs can actually prove

---

This checklist is intended to help investigators validate firewall behavior on a Windows 10 host and use audit logs as part of a broader evidence set.