

Prepare a comparable test

State one test question, keep the direct and proxied requests comparable, and define your criteria before measuring.

1 Define the test

Narrow test question and expected observation

Pass / fail criteria: required exit, request outcome, error share and timing limits

2 Record the environment

Client / runtime and exact version

Operating system

Test start time (UTC)

Client region

Required target region

Proxy protocol

Authentication method only

Timeout limit (seconds)

Proxy transport: HTTP or TLS

Approved destination URL without tokens, credentials or private identifiers

3 Keep the comparison consistent

Use the same destination, client, timeout, method, relevant headers and request body. Record redirect, retry, cache and concurrency settings. Change only the intended route; note any unavoidable differences.

Shared request settings, planned attempt count and direct / proxied route labels

Keep certificate verification enabled. An HTTPS destination does not imply TLS between the client and proxy. Record both boundaries separately.

Keep passwords, tokens, cookies and customer responses out of this worksheet.

Blank means not measured. Enter only observations you actually retain.

Diagnose the failing layer

Check the connection in order. Record the earliest failure supported by evidence, then repeat with one relevant setting changed.

Result vocabulary: pass, fail, inconclusive, not tested. Leave unmeasured observations blank.

1. Client configuration

Did the client receive the intended settings and select the intended route?

Result

2. DNS resolution

Which hostnames resolve locally or remotely? Record the resolver error or observed mode.

Result

3. TCP connection

Can the client reach the proxy host and port? Record refusal, timing or timeout stage.

Result

4. Authentication

Did the proxy accept the intended authentication method? Keep the challenge or error redacted.

Result

5. CONNECT and TLS

Record the proxy CONNECT result and destination TLS handshake separately. Verify certificates.

Result

6. Destination response

Record the target HTTP status, redirect behavior and safe response evidence.

Result

7. Application behavior

Did parsing, session handling and retries behave as expected after the response?

Result

Interpret the boundary before changing the endpoint

407 concerns proxy authentication. A target 401 or 403 concerns the destination response; confirm which server returned it.

A timeout alone does not prove a dead proxy. CONNECT success alone does not establish destination or application success.

Blank means not measured. Enter only observations you actually retain.

Record attempts and conclusions

Retain failed attempts as well as successful ones. Scope the conclusion to the environment, route, destination and observation window.

4 Keep the raw observations

Route	UTC timestamp	Elapsed ms	HTTP / error	Stage

Use direct or proxied route labels. Retain every attempt, timestamp, error and timeout in a redacted raw log. Latency is total request elapsed time; summarize finite measured samples and state the sample count.

5 Summarize each route and test window

Route	Attempts	Latency n	Median ms	p95 ms	Errors / timeouts
Direct					
Proxied					

Percentile method and sample population	Redacted raw-log reference and UTC window

Counts by destination HTTP status, transport errors and timeouts (each route)

Decision: pass / fail / inconclusive	Evidence: documentation / local / live	Observed exit (redacted as needed)

Supported conclusion, missing evidence and next test

Testing methodology Troubleshooting Client compatibility

Blank means not measured. Enter only observations you actually retain.