# Trusted JA4 Fingerprints From the Ingress

STATE
committed
TYPE
Architectural Specification
CREATED
2026-10-16
SUMMARY
Sibuna reads a JA4 TLS fingerprint that a trusted ingress computes and forwards in a request header, validates it, and lets policy rules, incidents and the console use it; it never terminates TLS itself.

STATUS
Committed
AUTHORS
Vikrant Rathore
UPDATED
2026-10-16

DISCUSSION
No external discussion URL assigned

LABELS
security, bots, policy

**Record status**

The catalog defines the review process and the meaning of each state. This numbered record forms part of the catalog.

## Contents

1. Abstract ..... 1
2. Motivation and scope ..... 2
3. Specification ..... 2
4. Rationale and alternatives ..... 3
5. Security and operational considerations ..... 3
6. Backwards compatibility ..... 3
7. Acceptance criteria and implementation status ..... 3
8. Resolved questions ..... 4
9. Review history ..... 4
10. References ..... 4

## 1. Abstract

A JA4 fingerprint summarises how a client opens a TLS connection: protocol, version, cipher suites, extensions and the first ALPN value. Browsers, libraries and bots differ in it, and a client cannot change it from inside its HTTP requests, which makes it one of the strongest signals for telling automation from browsers. Sibuna runs behind a TLS ingress and never sees the TLS handshake, so it cannot compute JA4 itself. We let an ingress that does compute it forward the value in a request header. Sibuna reads that header only from a trusted forwarder, checks its format, and makes the fingerprint available to policy rules, incident records and the console. An operator observes a new option, `--ja4-header`, a new rule field, `ja4`, and the fingerprint beside each recorded incident.

## 2. Motivation and scope

Hosted edges use JA4 for bot management: Cloudflare exposes JA3 and JA4 to Enterprise customers with Bot Management and can send `cf-ja4` to the origin. Sibuna's User-Agent and header signatures are easy to forge; a TLS fingerprint is not, because it is fixed by the client's TLS library before any HTTP byte is sent. Computing JA4 requires the ClientHello, so the component that terminates TLS must compute it. We considered making Sibuna that component and rejected it (see Rationale): the front door that browsers reach must speak HTTP/2 and HTTP/3, which Sibuna does not. Several ingresses already compute JA4 and pass it on:

- Cloudflare: the managed transform "Add bot protection headers" sends `cf-ja4` (Enterprise plan with Bot Management).
- Apache Traffic Server: the `ja4_fingerprint` plugin adds a `ja4` request header.
- nginx: the `ja4-nginx-module` of FoxIO exposes `$http_ssl_ja4` (it needs a ClientHello capture patch, nginx 1.26 or later); `proxy_set_header X-JA4 $http_ssl_ja4;` forwards it.
- HAProxy: a community Lua plugin.

No official Caddy or Envoy support was found when this record was written. This record covers JA4 only; JA4H (HTTP), JA4T (TCP) and the other JA4+ fingerprints are out of scope.

## 3. Specification

- **Option.** `--ja4-header <name>` names the request header that carries the fingerprint (for example `cf-ja4`, `ja4` or `x-ja4`). It is off by default, and it has no default value: the operator always names the header. The name must be a header token of 1 to 64 characters. It must not be a field Sibuna itself sets or strips: `X-Forwarded-*`, `X-Real-IP`, `X-Sibuna-*` and `Forwarded`, also when written with _ in place of `-`. Sibuna stores the name in lower case and matches it case-insensitively. When the option is set, the startup banner prints a `JA4:` line that names the header and says whether it is trusted or ignored.
- **Trust.** The header is read only when the request's forwarded headers are trusted, by the same decision that governs `X-Forwarded-For`: `--trust-forwarded`, or forward-auth mode when that option is absent (SID 0002). From an untrusted peer the header is ignored and counted in neither counter.
- **Origin.** In reverse-proxy mode, when forwarded headers are not trusted, Sibuna removes every field of the configured name from the request it sends to the origin, including spellings with _ in place of `-`. A client therefore cannot hand the origin a forged value under that name. When forwarded headers are trusted, only the exact spelling of the name (in any letter case) passes, unchanged; an alias with _ is still removed.
- **Validation.** A value is accepted only if it has the JA4 form `a_b_c` of 36 bytes: `a` is ten characters (one of `t`, `q` or `d`; a two-character version of lowercase letters or digits; `d` or `i`; a two-digit cipher count; a two-digit extension count; a two-character ALPN code of ASCII letters and digits), and `b` and `c` are twelve lowercase hexadecimal characters each. Exactly one field of the configured name must be present. A malformed value, or a repeated field, is treated as absent and counted in `sibuna_ja4_invalid_total`. Accepted values are counted in `sibuna_ja4_present_total`.
- **Policy.** A rule may carry `"ja4": "<value>"` (exact match) or `"ja4": "<prefix>*"` (prefix match; for example `"t13d*"` for TLS 1.3 over TCP with SNI). The pattern `"*"` alone matches any fingerprint. A request without a fingerprint never matches a `ja4` rule. The loader refuses a pattern that no fingerprint could match, with the error `InvalidJa4` (title "INVALID POLICY JA4"). Console management documents carry the same `ja4` field and are refused with `InvalidJa4` likewise. Matching is a byte comparison on the request path and allocates nothing.
- **Records.** Core storage migration 2 adds two nullable text columns on SQLite and PostgreSQL (SID 0011). `policies.ja4_pattern` holds a managed rule's criterion, at most 37 bytes (a fingerprint and `*`). `security_incidents.ja4` holds the fingerprint of the incident's request, exactly 36 bytes. Incidents of every kind (WAF denials, honeypot hits and audit findings) store the fingerprint when one was accepted, and incident search hits carry it. The console shows it in the incident evidence as "JA4 fingerprint", with the value or "Not recorded"; the Events filters accept a value or a prefix; the managed-rule editor has a JA4 field; and the policy test form takes a fingerprint.

- **No reputation keyed by JA4.** Bans and reputation stay keyed by address. A JA4 value names a client library, which many legitimate clients share, so banning by it would be too broad; rules decide what to do with it.

## 4. Rationale and alternatives

- **Native TLS termination in Sibuna** (with rustls, which the console already admits, SID 0012) would let Sibuna compute JA4 itself, but it would make Sibuna the front door. Browsers there negotiate HTTP/2 and HTTP/3; a front door that offers only HTTP/1.1 costs asset-heavy sites their multiplexing. Rejected.
- **HTTP/2 in Sibuna** would remove that objection but adds a binary protocol with a record of severe denial-of-service and inspection-bypass bugs (Rapid Reset, CVE-2023-44487; CONTINUATION floods; HTTP/2 to HTTP/1.1 downgrade smuggling; CVE-2026-13763, where a WAF behind a load balancer inspected only part of a body split across HTTP/2 frames). The established deployments, including AWS WAF behind CloudFront or a load balancer and Coraza inside Envoy or Caddy, keep HTTP/2 in the terminating proxy and inspect the decoded request. Rejected.
- **Reading the ClientHello in a TCP pass-through in front of the ingress** would need a way to attach the fingerprint to the decrypted requests downstream (for example PROXY protocol extensions the ingress forwards as headers), which common ingresses do not offer. Rejected.

## 5. Security and operational considerations

The fingerprint is only as trustworthy as the trust boundary: the configured header is honoured only from forwarders Sibuna already trusts, and an operator who enables `--ja4-header` must make the ingress overwrite any client-supplied copy of that header. A JA4 value identifies a TLS library and configuration, not a person or a device; it is stored with incidents under the same retention as the other incident fields. Clients can imitate a browser's ClientHello with specialised libraries, so JA4 raises the cost of automation rather than proving identity, and rules should combine it with other signals.

## 6. Backwards compatibility

The option is off by default, so behaviour does not change until an operator sets it. Without the option, a field that happens to carry the same name is an ordinary field and reaches the origin as before. The tables `policies` and `security_incidents` each gain one nullable column. Databases created before this change are migrated on start by core migration 2, which adds both columns and leaves every existing row valid.

## 7. Acceptance criteria and implementation status

1. With `--ja4-header` set and forwarding trusted, a `ja4` rule matches a request whose header carries a valid fingerprint, exactly and by prefix. Met: `cmd/sibuna/tests/ja4.rs` (`trusted_fingerprints_match_rules_exactly_and_by_prefix`); the pattern grammar in `crates/policy/src/ja4.rs`; the rule field and its refusal in `crates/policy/src/loader/tests.rs` (`ja4_patterns_compile_or_reject_the_file`).
2. The same header from an untrusted peer is ignored and, in reverse-proxy mode, removed from the request sent to the origin. Met: `cmd/sibuna/tests/ja4.rs` (`an_untrusted_fingerprint_is_ignored_and_removed_before_the_origin`) and `crates/net/src/request.rs` (`the_ja4_field_passes_only_when_trusted`).
3. Malformed and repeated values are ignored and counted. Met: `cmd/sibuna/tests/ja4.rs` (`malformed_and_repeated_values_are_counted_and_ignored`) and the form checks in `crates/policy/src/ja4.rs` (`fingerprints_have_the_ja4_form`).
4. Incidents record the fingerprint on SQLite and PostgreSQL, and the console shows and filters it. Met for the daemon and storage: `cmd/sibuna/tests/ja4.rs` (`incidents_carry_the_accepted_fingerprint`) and `crates/storage/src/worker/tests/ja4.rs` (`incidents_keep_the_fingerprint_their_request_carried`, `migration_two_adds_nullable_columns_to_a_version_one_database`). Met for the console: on both backends `crates/console-storage/tests/invariants/ja4.rs` (`ja4_rules_round_trip_through_edits_reads_and_imports`, `ja4_patterns_no_fingerprint_could_match_are_refused`,

`private_tests_and_replays_match_the_fingerprint`, `events_carry_and_filter_ja4_fingerprints_on_both_backends`, `the_live_feed_carries_the_fingerprint`); `crates/console/tests/policies.rs` (`ja4_rules_round_trip_and_values_no_fingerprint_could_match_are_refused`) and `crates/console/tests/events.rs` (`ja4_fingerprints_reach_pages_filters_and_csv_exports`); and in the interface `cmd/console-ui` (`incident_evidence_shows_the_recorded_ja4_fingerprint_or_not_recorded`, `the_ja4_filter_narrows_the_query_and_has_no_live_rows`, `the_rule_editor_carries_a_ja4_pattern_and_refuses_an_invalid_one`, `applied_rules_and_the_tester_show_the_ja4_fields`).
The Events filter takes the rule grammar: a whole fingerprint, a prefix followed by `*`, or `*` for any incident with a fingerprint. Both backends evaluate it as `substr(ja4, 1, n) = prefix`, never as `LIKE`, beside the existing filters and within their work bound. While a JA4 filter is set the Events page does not subscribe to live rows, as for the campaign and incident filters; the live events themselves carry the fingerprint. The CSV export gains a `ja4` column after `user_agent`.

5. A warm request still makes no heap allocation. Met: `cmd/sibuna/tests/steady_state.rs` now sends a fingerprint with every request and holds a `ja4` rule that each request is compared with.
6. The book gives recipes for Cloudflare, nginx and Apache Traffic Server. Met: the operations chapter, section “JA4 Fingerprints From the Ingress”.

Status: implemented and released in 1.0.0-beta.2; committed on 2026-10-16.

## 8. Resolved questions

- **Header name.** The header name is always explicit. `--ja4-header` takes a value and has no default, so no ingress’s naming is preferred and no header is read by accident.
- **Sets of fingerprints.** A rule carries one value or one prefix. Matching a set of fingerprints from a file, such as an allow list of known clients, is left for later; an operator who needs several values writes several rules.

## 9. Review history

- 2026-10-16: drafted for the maintainer’s review after deciding not to terminate TLS or HTTP/2 in Sibuna.
- 2026-10-16: accepted by the maintainer with the proposed answers to both open questions, now under “Resolved questions”.
- 2026-10-16: implemented for 1.0.0-beta.2. The implementation refined the specification. The reserved header names include `Forwarded` and spellings with _ for `-`. With trust, only the exact spelling of the header passes to the origin. The pattern `*` alone matches any fingerprint. Managed rules carry their criterion in `policies.ja4_pattern`. The stored criterion is at most 37 bytes and the incident column exactly 36 bytes. The counters are not bumped for untrusted peers.

## 10. References


- FoxIO, JA4+ network fingerprinting: https://github.com/FoxIO-LLC/ja4
- FoxIO, ja4-nginx-module: https://github.com/FoxIO-LLC/ja4-nginx-module
- Cloudflare, JA3/JA4 fingerprint: https://developers.cloudflare.com/bots/additional-configurations/ja3-ja4-fingerprint/
- Cloudflare, managed transforms: https://developers.cloudflare.com/rules/transform/managed-transforms/reference/
- Apache Traffic Server, JA4 fingerprint plugin: https://docs.trafficserver.apache.org/admin-guide/plugins/ja4_fingerprint.en.html
- CVE-2023-44487 (HTTP/2 Rapid Reset); CVE-2026-13763 (AWS ALB with WAF, HTTP/2 body inspection)
- SID 0002 (forwarded identity), SID 0003 (policy schema), SID 0007 (console evidence), SID 0011 (storage), SID 0012 (rustls)

### *Lifecycle event*

> 2026-10-16: prediscussion -> discussion. Assigned a permanent number and
> opened for discussion.

### *Lifecycle event*

> 2026-10-16: discussion -> accepted. Accepted by the maintainer on 2026-10-16
> with the proposed answers; implemented for 1.0.0-beta.2

### *Lifecycle event*

> 2026-10-16: accepted -> committed. Implemented and released in Sibuna
> 1.0.0-beta.2 on 2026-10-16. All six acceptance criteria met by the tests the
> record names (cmd/sibuna/tests/ja4.rs, steady_state.rs,
> crates/storage/src/worker/tests/ja4.rs,
> crates/console-storage/tests/invariants/ja4.rs, the console and interface
> tests); CI run 38872753827; release v1.0.0-beta.2, whose published
> linux-amd64 executable denied a TLS 1.2 fingerprint by prefix and admitted a
> TLS 1.3 one