Defense Algorithm Implementations

This section provides pseudocode for the six core CIF defense algorithms. Configuration parameters are documented separately in sec:config-params. Framework API reference, deployment considerations, and integration examples are provided in supplementary materials.

> ***Cross-Reference Note**: All algorithms implement formal definitions from Part 1. We cite specific theorems using "(Part 1, Theorem N)" notation to enable traceability from implementation to theoretical foundations.*
>
> ***Reproducibility**: Algorithm implementations are in `src/core/`. Run `pytest tests/` to verify behavior (191 tests, 100% pass rate).*

Algorithm 1: Cognitive Firewall Classification

The cognitive firewall classifies incoming messages using a multi-stage detection pipeline. This implements the formal Cognitive Firewall definition from Part 1, Section 5.1, specifying three-stage filtering ($F_{sig} \rightarrow F_{sem} \rightarrow F_{anom}$) with combined threat scoring (Part 1, Definition 5.1).