Example rules

- Log matches before blocking
- Block DDoS participants targeting your region
- Challenge a threat actor targeting the finance sector
- Filter by attacker country
- Combine with attack score
- Rate limit threat actors on API paths

Custom rule and rate limiting rule examples using threat intelligence fields. All fields are arrays — use `any()` with `[*]`.

:::caution Test rules with *Log* before enforcing. IP-based threat intelligence is a seven-day lookback over shared infrastructure — combine with other signals such as attack score before you block. :::

Log matches before blocking

Deploy with *Log* (Enterprise plans) to review matches before enforcing:

- **Expression:** `any(cf.intel.ip.attacker_names[*] != "")`
- **Action:** *Log*

Review matches in Security Events, then change the action to *Block* or *Managed Challenge*.

Block DDoS participants targeting your region

- **Expression:** `any(cf.intel.ip.target_countries[*] == "FR") and any(cf.intel.ip.datasets[*] == "ddos")`

- **Action:** *Block*

Challenge a threat actor targeting the finance sector

- **Expression:** `any(cf.intel.ip.target_industries[*] == "Banking & Financial Services") and any(cf.intel.ip.attacker_names[*] == "BLACKBASTA")`
- **Action:** *Managed Challenge*

Filter by attacker country

- **Expression:** `any(cf.intel.ip.attacker_countries[*] == "CN")`
- **Action:** *Block*

Combine with attack score

Block requests flagged by the WAF threat intelligence dataset that also have a low attack score:

- **Expression:** `any(cf.intel.ip.datasets[*] == "waf") and cf.waf.score lt 20`
- **Action:** *Block*

Rate limit threat actors on API paths

Rate limiting rule applying a stricter rate to flagged IPs on your API:

- **Expression:** `any(cf.intel.ip.datasets[*] == "ddos") and starts_with(http.request.uri.path, "/api/")`
- **Action:** *Block* when the rate is exceeded.

□□□ #2
□ □□□ □□□ 2026-11-01 05:13:49 UTC

□ □□□ □□□ 2026-11-01 05:13:51 UTC