Cloudflare Application Security

Partner Services Bootcamp - Course Syllabus

Course Overview

This four-day instructor-led bootcamp covers Cloudflare's application performance and security stack well beyond onboarding or certification prep. Day 1 covers the Cloudflare platform, DNS, and SSL. Day 2 pairs both CDN modules back-to-back and continues through smart routing, load balancing, and rules. Day 3 shifts entirely to security, walking through every layer from DDoS mitigation through API Shield. The morning of Day 4 is a capstone group project, and the afternoon closes with the Cloudflare Application Security Associate certification exam.

Format: Instructor-led with slides, live demos, lab exercises, and a capstone group presentation **Duration:** 4 days (3.5 days of instruction, labs, and presentations; half day certification exam) **Schedule:** 9 AM to 4 PM daily, one-hour lunch **Certification:** Day 4 afternoon includes the Cloudflare Application Security Associate exam

---

Who Should Attend

- Cloudflare partner engineers working with customers on application security deployments
- Solutions engineers preparing for the Cloudflare Application Security Associate certification
- Network and security engineers responsible for WAF, bot management, rate limiting, and API protection
- Engineers migrating customers from Akamai (or other CDN / WAF vendors) to Cloudflare

Prerequisites

- Familiarity with Cloudflare dashboard navigation
- Basic understanding of DNS and HTTP concepts
- Comfort reading command-line output (dig, nslookup, curl)

Daily Schedule

Day	Focus	Modules
Day 1	Foundations: Platform, DNS, and SSL	M00, M01, M02, M03
Day 2	CDN, Routing, and Load Balancing	M04, M05
Day 3	Security: DDoS through API Shield	M06, M07, M08
Day 4	Capstone Group Project (morning) / Cloudflare Application Security Associate certification exam (afternoon)	--

---

Module Descriptions

M00: Introduction and Bootcamp Overview

Bootcamp logistics, learning principles, and the four-day schedule. The instructor establishes the teaching methodology: theory immediately followed by hands-on application, every lab modeled on a real-world customer scenario, and the see-one-do-one-teach-one approach. Cloudflare University is introduced as a resource for continued learning.

M01: Application Performance

This module frames everything that follows. It covers how Cloudflare's global Anycast network operates, why every data center runs every service (the "single control plane" distinction from legacy CDN vendors), and the order of operations, the specific sequence in which a request passes through Cloudflare's modules. Understanding this flow is critical because it determines how DDoS mitigation, bot management, firewall rules, rate limiting, and API Shield interact with each other.

The module also covers compliance and data localization for regulated industries (GDPR, PII, the Anycast border-country edge case), multi-CDN architectures for financial institutions that require dual-CDN resiliency, and API automation fundamentals including Terraform, curl-to-Python workflows, and scoped API tokens with least-privilege permissions.

M02: DNS

DNS resolution from root servers through authoritative name servers, with dig, nslookup, DNS Checker, and Dig Web Interface as troubleshooting tools. Full authoritative vs. partial (CNAME) DNS setups, the security tradeoffs of each (in a partial setup the root domain is often left exposed unless CNAME flattening or registrar-level redirect rules are used), CNAME flattening, and proxy status (orange cloud

vs. gray cloud). Port limitations of the proxy for non-standard ports and the role of Cloudflare Spectrum for those cases.

M03: SSL/TLS

The two certificates in every proxied request (edge and origin), all five SSL modes, and why **Full (Strict)** is the required best practice for production security. Universal, Advanced, and custom certificate types, auto-renewal, DCV records for pre-cutover activation, certificate precedence, and the conflict-resolution rule: if a customer uploads a custom certificate, keep the Universal certificate active as a backup so a forgotten custom-cert expiration does not become an outage.

M04: CDN Part I

CDN fundamentals: pull vs. push CDN differences (relevant for Akamai migration conversations, since Cloudflare is a Pull CDN and pre-warming is generally unnecessary), how Cloudflare decides what to cache by default (based on file extension), verifying cache behavior with `cf-cache-status` headers, and why HTML isn't cached by default but often should be. Cache control directives, and the Cloudflare Trace tool for troubleshooting which rule matched a request.

M05: CDN Part II

Cache keys and cache sharding, TTL strategy, cache-purge risks, and using Cache Performance analytics to find optimization opportunities. **Tiered Caching** (generic vs. Smart Tiered Caching) as an always-on best practice for shielding the origin. **Argo Smart Routing** for dynamic traffic acceleration, and common mistakes like forgetting to enable Argo on Enterprise zones that purchased it (highly effective for global traffic, less useful for hyper-local traffic).

The **rules** section covers creating and managing rules from the dashboard: redirects, header manipulation, Host Header Override, and geo-redirection. Also introduces the "Last Match Wins" logic of Cache Rules (opposite of the top-down first-match Firewall Rules) that trips up new engineers.

Load balancing covers pools, monitors, steering policies (active-passive, dynamic Argo-based, geosteering), custom rules for path-based routing, session affinity, and common pitfalls like overly aggressive health-check intervals that cause origins to flag Cloudflare IPs as a DDoS attack, and configuring expected codes to include 301/302 redirects (not just 200 OK).

M06: Application Security

The largest module in the bootcamp, covering DDoS protection, WAF managed rulesets, the OWASP Core Ruleset, security analytics, and custom WAF rules.

- **DDoS Protection**: the automated always-on system that learns from ~20% of internet traffic, the difference between volumetric and signature-based detection, real customer scenarios where

thresholds don't trigger (and how to handle that conversation), and the strong recommendation to leave sensitivity settings at defaults unless explicitly advised by support.
- **WAF Managed Rules**: the 728+ rule managed ruleset, why default mode is the best practice, the logging-first deployment workflow, zero-day protection (Log4j, Spring4Shell), and why exceptions are rarely needed.
- **WAF OWASP Ruleset**: anomaly scoring, the four paranoia levels (PL1-PL4), and the clear recommendation to leave OWASP off unless compliance (usually PCI or SOC 2) forces it on. If enabled, PL1 is safe for most sites; PL4 will block legitimate traffic (the "paranoid chihuahua" analogy).
- **Security Analytics**: reading the events dashboard, sampling limitations, filtering by action and Ray ID, and why log push to a SIEM is the true source of truth. The total-traffic dashboard for establishing normal baselines.
- **Custom Rules**: the match-and-action model, challenge types (interactive, JS, managed, with Managed Challenge preferred over Interactive Challenge for most situations), the "Log" action as the first step for any new rule, and the "Skip" action for bypassing security modules on trusted traffic. Firewall rules execute top-down first-match-wins, the opposite of Cache Rules.

M07: Bot Management

The core lesson: bot management determines "automated vs. human," not "good vs. bad." That makes it the wrong tool for API traffic (everything scores 1) and the right tool for applications expecting human interaction. Bot score (1 = definite bot to 99 = definite human), the three scoring-engine components (heuristics, machine learning, behavioral analytics), the ML model's evolution to today's version 8 with strong bimodal distribution, and verified bots.

The three-step implementation process is the operational heart of the module: (1) deploy a safe base rule in Log mode (Bot Score < 30, action Log), (2) collaboratively analyze traffic with the customer to identify known good bots (partners, internal QA tools) that score low and need exceptions, (3) move the main rule from Log to Block or Managed Challenge only after the traffic looks clean (anywhere from two days to five weeks). Also covers rule stacking, managed IP lists, challenge solve rates, and textbook attack patterns for credential stuffing and content scraping.

M08: Protecting APIs: Rate Limiting and API Shield

Rate Limiting and API Shield as complementary tools for protecting API traffic that Bot Management can't help with.

- **Rate Limiting**: match criteria (IP, "IP with NAT support" to avoid blocking entire offices sharing a single public IP, origin response-code counting), threshold selection using the analysis tool or manual traffic review, the logging-first workflow, tiered rate-limit stacking, and distributed-counting tradeoffs.

- **API Shield**: six capabilities in order of complexity: Discovery and Endpoint Management for visibility into API traffic (often revealing deprecated endpoints customers didn't know existed), Schema Validation as the quickest win (JSON/OpenAPI drops malformed requests immediately), mTLS for mutual authentication, integrated Rate Limiting pre-populated from endpoint-management data, and Sequence Analysis / Sequence Mitigation for enforcing correct API call order using session identifiers (blocking thieves who skip directly from `/login` to `/transfer`). Implementation is a collaborative process with the customer's API developers, similar to bot management.

Day 4 Morning: Capstone Group Project

Four groups, each assigned a different industry vertical (fintech, global bank, e-commerce, media company) with fictitious sales notes, technical challenges, and infrastructure constraints. Groups have approximately three hours to design a full Cloudflare solution covering DNS, SSL, CDN, load balancing, and the complete security stack. Each group presents to the class, and the instructor challenges specific design decisions. Every participant gets exposure to four customer verticals and practices the solution-design thinking they'll use in real engagements.

Day 4 Afternoon: Cloudflare Application Security Associate Certification Exam

The bootcamp closes with the Cloudflare Application Security Associate certification exam. While there is no direct correlation between the bootcamp curriculum and the exam's scope, there is significant topical overlap. Three and a half days of hands-on configuration, troubleshooting, and solution design give participants a strong practical foundation heading into the exam.

Migration Methodology (Interwoven)

Akamai to Cloudflare migration considerations are threaded throughout the security modules rather than taught as a single unit. The core philosophy is **"Move and Improve," not "Lift and Shift":** legacy Akamai configurations are often bloated; the goal is to simplify the logic using Cloudflare's modern primitives. For large enterprise migrations (100+ zones), Terraform or API-driven scripts are used instead of the dashboard to ensure consistency and rollback.

What Students Leave With

- A working conceptual model of Cloudflare's application-security order of operations

- Hands-on experience with DNS, SSL, CDN, load balancing, WAF, Bot Management, Rate Limiting, and API Shield
- A group-designed customer solution architecture reviewed by the instructor and peers
- A completed Cloudflare Application Security Associate certification attempt

---

Cloudflare Products Covered

Product	Course Coverage
DNS	Full and partial (CNAME) setups, CNAME flattening, proxy status, port limitations
SSL/TLS	Universal, Advanced, and custom certificates; the five SSL modes; Full (Strict) as best practice; DCV records; auto-renewal
CDN	Default caching, cache-control directives, `cf-cache-status`, Tiered Caching, cache keys, TTL strategy, cache-purge safety
Argo Smart Routing	Dynamic-traffic acceleration; when it helps and when it doesn't
Rules	Redirects, header manipulation, Host Header Override, geo-redirection; Last-Match-Wins vs. Top-Down semantics
Load Balancing	Pools, monitors, steering policies, session affinity, health-check pitfalls
DDoS Protection	Automated volumetric and signature-based mitigation, threshold behavior
WAF Managed Rules	728+ rule ruleset, logging-first workflow, zero-day protection
WAF OWASP Ruleset	Anomaly scoring, paranoia levels, compliance-only enablement guidance
Security Analytics	Events dashboard, Ray ID filtering, sampling limits, SIEM Logpush
Custom Rules	Match-and-action model, challenge types, Skip action, top-down execution
Bot Management	Scoring (1-99), verified bots, three-step implementation, rule stacking
Rate Limiting	Match criteria (incl. "IP with NAT support"), threshold selection, tiered stacking
API Shield	Discovery + Endpoint Management, Schema Validation, mTLS, integrated Rate Limiting, Sequence Analysis

Cloudflare Spectrum	Mentioned for non-standard-port proxying (context)

Instructor

Mark Bowling Cloudflare Customer Success

Course materials developed 2026. Product names and dashboard paths reflect the current Cloudflare Application Security dashboard.