

Cloudflare Zero Trust and SASE

Partner Services Bootcamp - Course Syllabus

Course Overview

This five-day instructor-led bootcamp teaches Cloudflare Zero Trust and SASE architecture through a combination of lecture, live demonstration, and hands-on lab exercises taught in chronological build order. Students build a working Zero Trust deployment from scratch using a dedicated Cloudflare Enterprise lab environment, progressing from identity and endpoint configuration through private networking, application access, content filtering, and site connectivity. The labs follow the "AcmeCorp" scenario: the student is hired to run AcmeCorp's Zero Trust rollout and rebuilds the inside of the company around one rule, trust nothing by default and verify every user and every device, every time.

Day 5 is a full-day individual capstone lab where students apply the full stack to a single end-to-end deployment, submitted to an automated grader.

Format: Instructor-led, in-person or virtual **Duration:** 4 days lecture + labs, 1 full day capstone lab **Lab environment:** Individual Cloudflare Enterprise pods with dedicated Windows client and Ubuntu origin server **Lab exercises:** ~100 hands-on exercises across 18 labs (Lab 9 runs as two parts, 9a and 9b)

Who Should Attend

- Cloudflare partner engineers preparing for Zero Trust customer deployments
- Network and security architects evaluating SASE platforms
- IT operations engineers responsible for deploying and managing Cloudflare One
- Security engineers designing identity-aware access controls and content filtering policies

Prerequisites

- Familiarity with TCP/IP networking (DNS, HTTP, TLS, routing)
 - Basic understanding of identity providers (SAML, SSO concepts)
 - Comfort with Windows and Linux command-line interfaces
 - No prior Cloudflare experience required
-

Daily Schedule

Day	Focus	Modules	Labs
Day 1	Foundation: Identity, Endpoints, and the Client	Modules 1-3	Labs 1-5: Identity & Account Baseline, Device Profile & Enrollment Setup, Deploy the Cloudflare One Client, Posture & DEX & warp-diag, Internal DNS & Profile Lockdown (29 exercises)
Day 2	Connectivity: Tunnels, Access, and Private Networking	Modules 4-5	Labs 6-13: Cloudflare Tunnel & Routing, DNS Location for Server-Side Filtering, Self-Hosted Web & SSH Apps, Browser-Rendered RDP & Pre-Login (9a), Multi-User SSH (9b), Intranet App, Public-IP Lockdown, App Launcher & JWT & Policy Tester, Private-Network ZTNA & Posture-Based Blocking (44 exercises)
Day 3	Policy: Gateway Filtering, RBI, DLP, and DNS	Modules 6-7	Labs 14-17: DNS & HTTP Policies with Browser Isolation, TLS Bypass & Cert Handling & Network Policies, Order-of-Enforcement & DLP Basics & Mode-Switch Prediction, SWG Advanced (24 exercises)
Day 4	Architecture: WAN, Mesh, Operations, and Project Delivery	Modules 8-10	Lab 18: Cloudflare Mesh (3 exercises)
Day 5	Capstone Lab	--	Full-day individual capstone: build and defend a complete Zero Trust deployment, checked by an automated grader

Module Descriptions

Module 1 - What Cloudflare Zero Trust Actually Does

~45 minutes

Sets the foundation: why the perimeter model broke, the four use cases that drive every deployment (secure remote access, SWG, site connectivity, application security), the Cloudflare One reference architecture, the five SASE service categories, and the component vocabulary students will use for the rest of the course. Includes a guided tour of the Cloudflare One dashboard.

Module 2 - Cloudflare One Client: Architecture and Configuration

~45 minutes

Deep dive into the endpoint agent: how the Cloudflare One Client connects to Cloudflare's edge, the five operational modes (Gateway with WARP, Gateway with DoH, Secure Web Gateway, Proxy Only, Device Information Only), Managed Networks for location-aware behavior, device profiles and split tunnel configuration, and production deployment via MDM/MSI with the `mdm.xml` override file.

Module 3 - Cloudflare One Client: Posture, Monitoring, and Troubleshooting

~45 minutes

Device posture checks (OS version, disk encryption, firewall state, domain membership), Digital Experience Monitoring (DEX) for synthetic probing and fleet health, captive portal detection and third-party agent coexistence, and the `warp-diag` troubleshooting toolkit for support escalations.

Module 4 - Cloudflare Tunnel

~45 minutes

How cloudflared works as a proxy (not a router), scaling with replicas and load balancing, creating tunnels via the dashboard and CLI, global vs. per-datacenter tunnel architecture, hostname-based routing with CGNAT addressing, and tunnel diagnostics with `cloudflared tunnel diag`.

Module 5 - Cloudflare Access

~45 minutes

The three Access deployment patterns (self-hosted, SaaS, Infrastructure), Access policy evaluation logic, the CF_Authorization JWT cookie and how it enables SSO, service tokens for machine-to-machine authentication, the App Launcher for end-user discovery, Independent MFA, and Access for Infrastructure (browser-rendered SSH and RDP with command logging).

Module 6 - Cloudflare Gateway: Filtering and Inspection

~45 minutes

How Access and Gateway divide responsibility, the three enforcement layers (DNS, Network, HTTP), building an HTTP policy stack with recommended baselines, TLS decryption and Do Not Inspect bypass rules, Remote Browser Isolation for grey-area content, Data Loss Prevention with built-in and custom detection profiles, CASB integration, and antivirus sandboxing.

Module 7 - Cloudflare Gateway: DNS, Egress, and Network Routing

~45 minutes

DNS resolver policies and DNS Override, egress policies with dedicated IPs and virtual networks, Protective DNS and DNS Locations for clientless branch-office security, Gateway troubleshooting methodology, and solving the overlapping-IP problem in M&A scenarios.

Module 8 - Cloudflare WAN, Cloudflare Mesh, and the Off-Ramp Choice

~45 minutes

Architectural comparison of cloudflared tunnels, Cloudflare Mesh (formerly WARP Connector), and Cloudflare WAN (formerly Magic WAN). When to use each, how the routing tables interact, CGNAT addressing across accounts, WARP-to-WARP direct device communication, and SCIM provisioning that ties the identity layer to the network layer.

Module 9 - Operations: Logs, Monitoring, and Troubleshooting

~45 minutes

What the dashboard shows and what it hides, Gateway logs (DNS, HTTP, Network) and the Logs dashboard, Network Session Logs and Log Explorer for SQL-style queries, Logpush for long-term retention to R2 or third-party SIEMs, tunnel diagnostics, and the "start from the beginning of the connection" troubleshooting methodology that works for every escalation.

Module 10 - Delivering a SASE Project

~25 minutes

The six-phase project lifecycle (initiation, design, pilot, production, automation, validation), pre-sales to post-sales handover, High-Level Design documentation, pilot testing strategy, production rollout with phased enforcement, Terraform and API automation at scale, and RBAC roles for multi-team management. Sets up the Day 5 capstone lab, where students apply the full stack end to end.

Lab Exercises

Each student receives a dedicated Cloudflare Enterprise lab environment with:

- A Windows 11 client VM
- An Ubuntu origin server with 5 Docker services (web server, intranet, DNS, FTP, SMB)
- A Cloudflare Enterprise account with Zero Trust Premier Bundle
- A dedicated DNS zone and Access organization

- A shared SAML identity provider

Lab 1 - Identity & Account Baseline

6 exercises / 30-45 minutes

Lay the foundation: identify your team name, integrate a SAML identity provider through the shared lab IdP and add it to your Zero Trust account, test SAML authentication end-to-end, enable account-wide baseline settings (TLS decryption, protocol detection, malware scanning, AV inspection), and confirm log visibility on the Cloudflare One Logs page.

Lab 2 - Device Profile & Enrollment Setup

6 exercises / 30-45 minutes

Configure how the Cloudflare One Client will behave before installing it: set global Client settings, create a dedicated device profile, adjust local domain fallback to route everything through Gateway, configure split tunnel rules, and set device enrollment permissions so only the right users can join the organization.

Lab 3 - Deploy the Cloudflare One Client

7 exercises / 30-45 minutes

Install and prove out the endpoint: sign in to the Windows desktop, uninstall any pre-existing client, install Cloudflare One Client via MSI with the `organization` parameter, authenticate via SAML, confirm the device shows up in the dashboard, verify Gateway is processing the client's internet traffic, and lock down behavior with an `mdm.xml` MDM override file.

Lab 4 - Posture, DEX & warp-diag

6 exercises / 30-45 minutes

Layer on posture and observability: create device posture checks (OS version, disk encryption, firewall state), build DEX synthetic tests for fleet health, configure DEX notifications for alerting, collect a warp-diag bundle remotely from the dashboard, collect one locally on the device, and analyze the bundle with online troubleshooting tools.

Lab 5 - Internal DNS & Profile Lockdown

4 exercises / 25-35 minutes

Build the lab's private namespace: create an internal DNS zone (`cf1pslabs.int`) with records for `web` and `ssh` , create a DNS view scoped to Cloudflare One Client users, create a Gateway resolver policy that routes queries for the internal zone to that view, and verify the device-profile lock-down behaviors that prevent users from disconnecting the client.

Lab 6 - Cloudflare Tunnel & Routing

9 exercises / 45-60 minutes

Build private connectivity: plan and create a Cloudflare Tunnel, install cloudflared on the Ubuntu origin server, add a private network route for the lab's CIDR, test IP-level connectivity from the Windows client, verify IPv6 is disabled on the client adapter so internal DNS resolves over IPv4, test FQDN-based connectivity through the internal DNS zone, configure a tunnel health alert, and enable debug-level cloudflared logging.

Lab 7 - DNS Location for Server-Side Filtering

1 exercise / 20-30 minutes

Bring Gateway DNS filtering to a host that can't run the Cloudflare One Client: create a Gateway DNS location for the Ubuntu Server, point `dnsproxy` at the DoH endpoint, and confirm queries from the server appear in the DNS query logs filtered by the new location.

Lab 8 - Self-Hosted Web & SSH Apps

8 exercises / 60-90 minutes

Publish the first two Access-protected applications: build a reusable baseline Access policy for lab users, configure an Access HTTPS app for the Ubuntu web service, publish the web service through the tunnel, test the HTTPS app end-to-end, configure a browser-rendered SSH Access app, publish SSH through the tunnel, test browser-rendered SSH, and confirm the Access decisions in the logs.

Lab 9a - Browser-Rendered RDP & Pre-Login

6 exercises / 45-60 minutes

Stand up Access for Infrastructure RDP and the pre-login device-authentication story: set up browser-rendered RDP through the Get Started wizard, test the RDP session in the browser, create a service token for pre-login, add an enrollment policy that accepts the service token, update `mdm.xml` with

the service token credentials, and walk through the pre-login flow where the device authenticates before any human user logs in.

Lab 9b - Multi-User SSH on the Ubuntu Server

3 exercises / 25-35 minutes

See per-user identity and log attribution in action: create local users on the Ubuntu Server, log in as each user through the browser-rendered SSH app, and confirm that each user appears distinctly in the Access logs.

Lab 10 - Intranet App Through the Tunnel

4 exercises / 25-35 minutes

Demonstrate the one-tunnel / many-services production pattern: publish the intranet service on port 8000 through the existing tunnel, create a second self-hosted Access app for it, test that the intranet renders distinct content from the public website (both routed through the same tunnel), and confirm the intranet Access decision in the logs.

Lab 11 - Public-IP Lockdown: Proving the Tunnel Is the Only Path

Guided demonstration / 10-15 minutes

Prove the tunnel is now the only inbound path to the origin. The Ubuntu Server's public IP is locked down at the pod-network level, so students confirm that direct-to-origin access is gone and that every path to internal services runs through the Cloudflare Tunnel established in Lab 6.

Lab 12 - App Launcher, JWT Inspection & Policy Tester

3 exercises / 25-35 minutes

Make Access discoverable and verifiable: enable the App Launcher for end-user discovery of published applications, inspect the `CF_Authorization` JWT to see what claims Cloudflare actually issues after authentication, and use the Policy Tester to dry-run a policy against a specific identity and posture state.

Lab 13 - Private-Network ZTNA & Posture-Based Blocking

10 exercises / 60-90 minutes

Apply Access policies to private-network traffic and tie them to posture: configure a Gateway Network policy that lets Access evaluate private traffic, enable WARP Authentication Identity for silent SSO, create two private-network ZTNA Access apps, test access from a Cloudflare One Client device, tear them down, deploy a three-policy posture stack (posture-fail block, cleanup allow, implicit deny) as

Gateway Network policies, test the access path with posture passing, run a posture-failure exercise by disabling Windows Firewall and watching the block, explore block events in the Logs page, and optionally configure Infrastructure Access SSH with full command logging.

Lab 14 - DNS & HTTP Policies with Browser Isolation

7 exercises / 45-60 minutes

Stack the first two enforcement tiers with isolated testing: deploy DNS recommended policies, test them, disable them, deploy HTTP recommended policies, test them, create a Browser Isolation list and policy, and test that isolation triggers as expected.

Lab 15 - TLS Bypass, Cert Handling & Network Policies

7 exercises / 45-60 minutes

Cover the messy real-world parts of HTTP inspection and the Network tier: test the untrusted-certificate policy, configure a TLS inspection bypass list with certificate verification, confirm TLS bypass actually skips decryption, disable HTTP policies, deploy Network recommended policies, test them, and create a targeted SMTP block on port 25.

Lab 16 - Order-of-Enforcement, DLP Basics & Mode-Switch Prediction

4 exercises / 45-60 minutes

Force students to reason about the full policy stack: enable all DNS, HTTP, and Network policies simultaneously and predict the order of enforcement on specific test traffic, build a DLP policy for financial-data detection, test the DLP policy, and run the mode-switch prediction exercise across Gateway with WARP / DoH / Traffic-only modes.

Lab 17 - SWG Advanced

6 exercises / 60-90 minutes

Cover the advanced SWG patterns customers actually ask about: create a custom Gateway block page, enable clientless Remote Browser Isolation, create a custom DLP detection entry with regex pattern matching and payload encryption, decrypt and inspect a DLP payload match from the logs, create a Gateway Authorization Proxy with a PAC file for agentless devices, and configure tenant control policies that gate SaaS access by corporate tenant via custom HTTP header injection.

Lab 18 - Cloudflare Mesh on the Ubuntu Server

3 exercises / 30-45 minutes

Deploy Cloudflare Mesh: create a dedicated device profile for the Mesh connector identity, install Cloudflare Mesh on the Ubuntu origin server alongside the existing tunnel, and verify that Gateway security policies (DNS and HTTP blocks) apply to the server's own internet traffic.

Day 5: Capstone Lab

The course finishes with a full-day, individual, hands-on capstone lab (roughly six hours). Working solo in their own lab pod, each student rebuilds AcmeCorp's Zero Trust posture end to end: identity and device posture, private connectivity with no inbound ports opened, an access decision in front of every internal application, layered Gateway filtering, and a sealed perimeter with accountable logging. Submissions are checked by an automated grader that inspects both the configuration and the live behavior of the student's account, so success is measured by a working deployment rather than a slide presentation. It is the practical exam for everything built across Labs 1-18.

What Students Leave With

- A working Cloudflare Zero Trust deployment built from scratch in their lab environment
 - Hands-on experience with ~100 configuration exercises across 18 labs spanning identity, networking, access control, content filtering, and operations
 - Understanding of when to use each Cloudflare One component (Cloudflare One Client, Tunnel, Access, Gateway, Mesh, WAN)
 - A troubleshooting methodology applicable to any Cloudflare One escalation
 - A completed individual capstone deployment, built solo and validated by an automated grader
 - Familiarity with the May 2026 Cloudflare One dashboard navigation and product names
-

Cloudflare Products Covered

Product	Course Coverage
Cloudflare One Client	Deployment, configuration, 5 modes, device profiles, split tunnel, MDM, posture, DEX, multi-user, pre-login
Cloudflare Tunnel	Creation, private routes, public hostnames, replicas, diagnostics, debug logging

Cloudflare Access	Self-hosted apps, browser-rendered SSH, private-network ZTNA, App Launcher, service tokens, Infrastructure Access, JWT inspection, Policy Tester
Cloudflare Gateway	DNS/HTTP/Network policies, recommended baselines, TLS decryption, Do Not Inspect, Browser Isolation (client and clientless), DLP (built-in and custom), custom block pages, proxy endpoints, PAC files, tenant control
Cloudflare Mesh	Connector deployment, device profile configuration, server-side Gateway policy enforcement
Cloudflare WAN	Architecture comparison, when to use vs. Tunnel/Mesh (lecture)
Internal DNS	Zones, views, resolver policies
DEX	Synthetic tests, remote diagnostics, alerting
Notifications	DEX alerts, tunnel health alerts
DLP	Built-in profiles, custom detection entries, regex patterns, payload encryption and decryption
CASB	Overview and integration patterns (lecture)

Instructor

Mark Bowling Cloudflare Customer Success

Course materials developed May 2026. Product names and dashboard paths reflect the May 2026 Cloudflare One dashboard.