Cloudflare Zero Trust — Training Doc

What Is Cloudflare Zero Trust?

Cloudflare Zero Trust (also called Cloudflare One) is Cloudflare's SASE/SSE platform. It replaces VPNs, firewalls, and legacy security appliances with a cloud-native architecture where every request is verified — no implicit trust.

The three pillars:

- **Access (ZTNA)** — Identity-aware proxy that protects applications. No VPN needed.
- **Gateway (SWG)** — Secure Web Gateway that filters DNS and HTTP traffic.
- **Tunnel** — Encrypted connector that exposes internal services without open ports.

Plus advanced capabilities: WARP (device client), Browser Isolation (RBI), CASB, DLP, and Email Security.

What We Built on saltwaterbrc.com

1. Cloudflare Access (ZTNA)

- **Identity Provider:** Google Workspace (saltwaterbrc.com domain)
- **Application:** Self-hosted app protecting `saltwaterbrc.com/admin`
- **Policy:** Allow emails `brandon@saltwaterbrc.com` and `brandon.r.crowe@gmail.com`
- **Session duration:** 24 hours
- Replaces VPN for remote access to internal apps
- No hardware. No agents required for web apps. No firewall rules.
- Identity-based — not network-based. Works from any device, any network.
- Every request is logged and auditable
- Competitors: Zscaler Private Access, Palo Alto Prisma Access, Cisco Duo

2. Cloudflare Gateway (Secure Web Gateway)

DNS Policies:

- **Block Security Threats** — Blocks malware, phishing, spam, spyware, command & control, DGA domains
- **Block Adult & Gambling** — Blocks adult themes, gambling, questionable content categories

HTTP Policies:

- **Block Risky File Downloads** — Blocks .exe file downloads
- DNS filtering catches threats before the connection is even established
- HTTP inspection sees inside encrypted traffic (with TLS decryption)
- No appliances to deploy. No backhauling traffic to a datacenter.
- Replaces: Cisco Umbrella, Zscaler Internet Access, Palo Alto URL Filtering
- Integrates with DLP for data loss prevention in transit

3. Cloudflare Tunnel

- **Tunnel name:** `saltwaterbrc-dev`
- **Tunnel ID:** `5ecd6f3c-454d-4b37-8b5b-f4f1880aa126`
- **Hostname:** `dev.saltwaterbrc.com` → `http://127.0.0.1:4321`
- **Config file:** `~/.cloudflared/config.yml`
- Replaces VPN concentrators, bastion hosts, and reverse proxies
- Zero inbound connections — the tunnel is outbound-only
- Works behind NAT, firewalls, any network — your machine initiates the connection
- Combine with Access policies to control who can reach the tunnel
- Use cases: expose internal dashboards, dev environments, on-prem apps to remote teams
- Competitors: Zscaler App Connector, Palo Alto GlobalProtect, traditional VPN

How to Demo the Tunnel

The tunnel requires two terminal processes running simultaneously:

```
cd ~/Documents/Claude/saltwaterbrc-astro && npm run dev -- --host 0.0.0.0
```

This starts the Astro site on `localhost:4321`, exposed to all network interfaces.

```
cloudflared tunnel run saltwaterbrc-dev
```

This connects your machine to Cloudflare's network and routes `dev.saltwaterbrc.com` to your local server.

- "This is my local machine. No public IP. No ports open. No firewall rules."
- "The tunnel is outbound-only — my machine initiated the connection to Cloudflare."
- "I can add an Access policy to control who can reach this. Identity-based, not network-based."
- "This replaces VPN for accessing internal tools, dev environments, on-prem apps."

4. WARP / Cloudflare One Client

- Device enrollment permissions with "Allow Enrollment" policy (both emails)
- Default device profile with WireGuard protocol
- Captive portal detection enabled
- Allow device to leave organization enabled
- Same architecture for 1 device or 10,000 — scales with zero additional infrastructure
- Works on macOS, Windows, Linux, iOS, Android
- Gateway policies enforced consistently across all enrolled devices
- Replaces: traditional VPN clients, endpoint security agents for web filtering
- Feb 2026 rebrand: WARP → Cloudflare One Client
- mDNSResponder conflict on macOS: caused by Docker, VMware, or Internet Sharing binding to port 53. Use `sudo lsof -iTCP:53 -iUDP:53 -n -P` to diagnose
- Enrollment failing: check that the policy is ATTACHED to device enrollment permissions (not just created as a reusable policy)

5. Browser Isolation (RBI)

- Clientless Web Isolation enabled
- "Allow Remote Browsing" policy created and attached
- Login method: Google Workspace
- **Clientless (what we built):** Direct URL, no WARP needed. Anyone with the link + auth can use it. Great for contractors, BYOD, demos.
- **Gateway-triggered:** WARP connected, HTTP policy with "Isolate" action. Risky sites automatically open in isolation — no special URL needed. Admin controls which sites get isolated.
- Contractor access: third parties view sensitive apps without installing anything
- BYOD: personal devices access corporate apps without corporate software
- Phishing protection: suspicious email links open in isolation automatically
- Data exfiltration prevention: admin can disable copy/paste, downloads, printing, keyboard input
- Replaces: virtual desktop infrastructure (VDI), Citrix, VMware Horizon for web apps

6. CASB (Cloud Access Security Broker)

- Google Workspace integration (CASB + Email mode)
- GCP service account: cloudflare-casb@saltwaterbrc-cloudflare.iam.gserviceaccount.com
- Domain-wide delegation in Google Admin console
- Read-Write policy (enables auto-remediation)
- Shadow IT discovery: find SaaS apps employees are using without approval
- Misconfiguration detection: catch "shared to anyone with the link" on sensitive Google Docs
- Compliance: automated scanning for HIPAA, PCI, SOX requirements
- Supported integrations: Google Workspace, Microsoft 365, Salesforce, GitHub, Slack, Box, Dropbox, and more
- Replaces: standalone CASB products like Netskope, McAfee MVISION Cloud

7. DLP (Data Loss Prevention)

- Detection profiles enabled: Financial Information (credit cards, IBAN, SWIFT), Credentials & Secrets (API keys, tokens), Social Security/Tax/Insurance Numbers
- HTTP policy: Block action when DLP Profile matches any enabled profile
- TLS decryption: ON
- Prevent employees from uploading credit card databases to personal cloud storage
- Block API keys from being pasted into ChatGPT or other AI tools
- Detect sensitive data in transit before it leaves the corporate network
- Combine with CASB for data-at-rest scanning (files already in SaaS apps)
- Regulatory compliance: PCI-DSS (credit cards), HIPAA (health data), SOX (financial data)
- Replaces: Symantec DLP, Forcepoint DLP, Digital Guardian

Architecture Summary

```
Public Internet ■ Cloudflare Edge ■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■ ■ ■ Access (ZTNA) ■ ■ →
Authenticates users ■ ■ → Checks policies ■ ■ → Protects /admin ■ ■ ■ ■ Gateway (SWG) ■ ■ → Filters DNS queries ■
■ → Inspects HTTP traffic ■ ■ → Blocks threats & content ■ ■ ■ ■ Tunnel ■ ■ → Encrypted connector ■ ■ → Routes to
local machine ■ ■ → No open ports needed ■ ■ ■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■ Your Machine
(cloudflared) ■ Local Dev Server (:4321)
```

The Full Stack (Updated)

saltwaterbrc.com now runs on **16 Cloudflare products**:

Layer	Product	Status
Registrar	Cloudflare Registrar	Live
DNS	Cloudflare DNS	Live
Hosting	Cloudflare Pages	Live
Framework	Astro (Cloudflare)	Live
Edge Logic	Cloudflare Workers	Live
State	Durable Objects	Live
Storage	Cloudflare R2	Live
AI	Workers AI + Vectorize	Live
AI Control	AI Gateway	Live
Containers	Sandbox SDK	Live
Video	Cloudflare Stream	Live
ZTNA	Cloudflare Access	Live
SWG	Cloudflare Gateway	Live
Connector	Cloudflare Tunnel	Live
Device Client	WARP	Live
Isolation	Browser Isolation	Live
SaaS Security	CASB	Live
Data Protection	DLP	Live

Sales Talking Points

- "I built Zero Trust on my own site in a single afternoon. No hardware. No agents for web apps. Identity-based access at the edge."
- "Every request to my admin panel is authenticated before it reaches the origin. That's ZTNA — not a VPN, not a firewall rule."
- "My Gateway policies block malware domains and risky file downloads for any enrolled device. That's your Secure Web Gateway — no appliance."
- "The tunnel exposes my local dev environment with zero inbound connections. That replaces your VPN concentrator."
- "My contractors can access internal tools through an isolated browser. No agent install. No VPN. Identity-verified, pixel-streamed, and I can disable copy/paste."
- "CASB found misconfigurations in my Google Workspace within hours of connecting. No agent. API-based scan."
- "DLP blocks credit card numbers and API keys from leaving enrolled devices. Same policy engine as the firewall."
- "Cloudflare Tunnel is outbound-only. No firewall changes. No public IPs. Works behind any NAT."
- "Gateway gives you DNS filtering, HTTP inspection, and DLP in one place. No backhauling to a datacenter."
- "Access integrates with your existing IdP — Google Workspace, Okta, Azure AD, anything SAML/OIDC."
- "Browser Isolation replaces VDI for web app access. No Citrix licenses. No virtual desktops."
- "CASB is API-based — connects to Google Workspace, M365, Salesforce, GitHub. No inline proxy needed for SaaS scanning."
- "DLP profiles are built-in. Credit cards, SSNs, API keys — toggle them on. No regex writing required."
- vs Zscaler: Single vendor for both app security (WAF/DDoS/Bot) AND Zero Trust. Zscaler can't do that.
- vs Palo Alto Prisma: Cloud-native from day one. No acquired/stitched-together products.
- vs Cisco: Modern architecture. No hardware dependency. Faster time to value.