CLOUDFLARE

Network Transformation

Powered by Cloudflare

ACME Corp · Network Demo Track · 2026

Three Deadlines. One Window.

MPLS Expiring

Nov 2026

AT&T non-renewal notice due September

- $340K/yr for 4 circuits
- Singapore: 280ms round-trip
- All SaaS traffic hairpins through Chicago
- No alternative currently scoped

DC Exit Programme

18 months

to exit Chicago DC and Dallas DR

- 140 apps migrating to AWS
- Core banking stays on-prem (colo)
- BGP prefix 185.12.44.0/24 must be retained
- Hybrid connectivity needed during migration

VPN at Breaking Point

152%

capacity — 380 sessions on a 250-seat box

- $180K/yr Cisco AnyConnect licence
- 180ms+ latency for remote users
- No per-app access policies
- Perimeter trust — once in, fully trusted

Cloudflare is the **single network fabric** that solves all three simultaneously — replacing MPLS, bridging the DC migration, and eliminating the VPN.

CLOUDFLARE

ACME CORP

The Network Reality

Current state — and what needs to change

ACME Corp — Current Network

DATA CENTRES

Chicago (Primary): Palo Alto PA-5220, 10Gbps internet (x2)

Dallas (DR): Palo Alto PA-3220, 2x 1Gbps internet

Both DCs: exiting over 18 months → AWS us-east-1

WAN – AT&T MPLS ($340K/YR)

Chicago ↔ Dallas: 1Gbps — $80K/yr

Chicago ↔ Sydney: 100Mbps — $120K/yr — 180ms

Chicago ↔ London: 100Mbps — $90K/yr — 95ms

Chicago ↔ Singapore: 50Mbps — $50K/yr — 280ms

BRANCH CPE

Sydney: Meraki MX67 (Magic WAN compatible)

London: FortiGate 60F (IPsec underlay capable)

Singapore: Meraki MX67 (Magic WAN compatible)

TRAFFIC PROBLEMS

All M365, Salesforce, Workday traffic **hairpins through Chicago DC** before reaching the internet

AWS traffic from branches also hairpins through Chicago — even post-migration

Remote users: VPN → Chicago → app. 180ms+ for East Coast users on a **good** day

What the AI Reads — What Needs Fixing

DDoS — 48 Gbps attack took the portal offline for 2.5 hours

$140K revenue lost. $28K ISP scrubbing bill. ISP null-routing is the only mitigation. No L7 WAF.

MPLS — $340K/yr, Singapore at 280ms, all SaaS traffic hairpins

AT&T non-renewal notice must be submitted by **September 2026**. No alternative currently in place.

VPN — 152% capacity, $180K/yr, 180ms+ latency, no Zero Trust

380 concurrent sessions on a 250-seat Cisco ASA. Once on VPN, fully trusted. No per-app policies.

DC Exit — hybrid connectivity gap during 18-month migration

Core banking app (on-prem) must reach 12 downstream services migrating to AWS — without a VPN tunnel between clouds.

CLOUDFLARE

LIVE DEMONSTRATION

Five Network Scenarios

Architecture decisions — validated live against your environment data

1 Replacing $340K of MPLS

CLOUDFLARE

AT&T MPLS – THE PROBLEM

$340K/yr — Chicago↔Dallas ($80K), Sydney ($120K), London ($90K), Singapore ($50K)

September 2026 hard deadline — AT&T requires 90-day non-renewal notice. No alternative scoped.

Singapore at **280ms** — APAC team can't hold a video call. All SaaS traffic hairpins Chicago.

Meraki MX67 (Sydney/Singapore) and FortiGate 60F (London) — both capable as Magic WAN underlay

MAGIC WAN – THE OUTCOME

Cost: AT&T $340K/yr → Magic WAN ~$180K/yr = **$160K annual saving**. September deadline met.

Latency: Singapore 280ms → **<30ms** via Cloudflare Singapore PoP. London, Sydney similarly improved.

SaaS direct: M365, Salesforce, Workday break out to internet at the branch — no more Chicago hairpin.

Underlay: Meraki + FortiGate connect via IPsec to Cloudflare edge. No CPE replacement required.

Magic WAN | Gateway HTTP

2 DC Migration — Zero Disruption

THE MIGRATION CHALLENGE

Core banking app (on-prem) must reach **12 downstream services** being migrated to AWS — without a VPN tunnel between clouds

BGP prefix `185.12.44.0/24` embedded in financial institution whitelists — cannot change IPs post-exit

AWS and on-prem must coexist for 18 months — apps migrating one-by-one, some staying in colo permanently

CLOUDFLARE AS THE MIGRATION FABRIC

- **WARP Connector** — exposes on-prem `10.44.0.0/16` to Cloudflare. Core banking reaches AWS services transparently — zero app changes.
- **Cloudflare Tunnel** — AWS workloads expose APIs back to on-prem via cloudflared sidecars. Bidirectional. No VPC peering.
- **Magic Transit** — absorbs `185.12.44.0/24` into Cloudflare anycast. Chicago DC exits; IPs stay. Financial institution whitelists unchanged.
- **Zero Trust throughout:** Every cross-environment call is identity-aware. No implicit trust during migration.

Cloudflare Tunnel | WARP Connector | Magic Transit

3 VPN Eliminated — Zero Trust Everywhere

CISCO ANYCONNECT – THE PROBLEM

Cisco ASA 5515-X running at **152% capacity** — 380 concurrent sessions on a 250-seat box. Replacement cycle approaching.

$180K/yr in Cisco licencing. East Coast remote users averaging **180ms+** round-trip to Chicago.

Perimeter trust — once authenticated to VPN, users have broad network access. No per-app segmentation.

WARP + ACCESS – THE OUTCOME

- **$180K eliminated:** Cisco AnyConnect licence gone. VPN helpdesk tickets: **40/month → 0**.
- **Zero Trust:** Every app access gated by identity + device posture. Split tunnel routes `10.44.0.0/16` through Cloudflare; SaaS goes direct.
- **Performance:** Remote users connect to the nearest Cloudflare PoP — not Chicago. Latency drops dramatically.
- **DNS:** All lookups inspected by **Gateway DNS**. Threat categories blocked before traffic leaves the device.

WARP Client | Access (ZTNA) | Gateway DNS

4 48 Gbps DDoS — Absorbed, Not Nullrouted

APRIL 16 – WHAT HAPPENED

48Gbps Peak attack volume	**2.5hr** Portal offline
$140K Revenue lost	**$28K** Scrubbing bill

ISP scrubbing (metered) is the **only mitigation**. No L7 protection. Null-routing takes the portal offline. No WAF.

MAGIC TRANSIT – THE OUTCOME

- **Unmetered:** No more $28K scrubbing bills. Magic Transit absorbs attacks at Cloudflare's network — before they reach your infrastructure.
- **Sub-3 seconds:** DDoS mitigation SLA. The portal stays up. Transactions continue. Revenue protected.
- **L7 WAF:** Application-layer attacks (SQLi, XSS, credential stuffing) blocked at the edge. ISP scrubbing sees none of this.
- **BGP retained:** `185.12.44.0/24` announced via Cloudflare. Financial institution whitelists unchanged. Portal stays at the same IPs.

Magic Transit | WAF | DDoS Managed Rules

5 Client Portal — Built for Global Scale

CLOUDFLARE

THE MONOLITH PROBLEM

portal.acmecorp.com is a Java/Tomcat monolith — the same system that went down during the 48 Gbps DDoS because there was no elastic capacity

Peak traffic: **800 req/sec** (~1.5B requests/month). All hitting a single Chicago DC origin.

ASIC (AU) and SEC (US) regulations require **data residency control** — certain data cannot leave specific jurisdictions

Cold-start latency for international users: unacceptable. Sydney users experience 300ms+ page loads.

CLOUDFLARE WORKERS – THE OUTCOME

- **Global, elastic, zero cold-start:** Auth layer and API gateway run in Workers — deployed to 300+ PoPs globally in seconds. No single origin to hit.
- **Real-time:** Trade notifications via **Durable Objects** — WebSocket state managed at the edge, no origin required.
- **Data residency:** Jurisdiction-pinned Durable Objects — AU session data stays in AU, US data stays in US. ASIC and SEC compliance.
- **DDoS-proof by design:** No monolith to null-route. Attacks absorbed by Cloudflare's network before reaching any compute.

Workers | Durable Objects | D1 | Access

CLOUDFLARE

THE RESULT

One Network Fabric

Zero Trust. Zero incidents. $640K consolidated saving.

Before & After — Network Track

~~$340K/yr~~ **~$180K** AT&T MPLS → Magic WAN	~~$180K/yr~~ **$0** Cisco AnyConnect	~~280ms~~ **<30ms** Singapore latency	~~$28K/mo~~ **$0** Metered scrubbing bill

SEPTEMBER 2026

AT&T non-renewal committed. Magic WAN running in parallel. September decision made.

NOVEMBER 2026

AT&T circuits terminated. Magic WAN is sole WAN. $340K annual saving realised.

MONTH 18 – OCTOBER 2027

Chicago DC dark. Dallas DR exited. Cloudflare is the network backbone. Full hybrid migration complete.

The Network Transformation Roadmap

CLOUDFLARE

Phase 1 · Now → Sept 2026

FOUNDATION

- Magic Transit live on 185.12.44.0/24
- WAF protecting portal.acmecorp.com
- WARP + Access (ZTNA) — 600 users
- Gateway DNS — threat blocking
- Magic WAN parallel to MPLS

$208K+ saving immediate

Phase 2 · Sept → Nov 2026

MPLS EXIT

- Traffic shifted to Magic WAN per-app policies
- SaaS direct-to-internet from all branches
- AT&T non-renewal notice submitted
- Branch CPE validated (Meraki + FortiGate)
- AT&T circuits terminated Nov 2026

$340K/yr → $180K/yr locked in

Phase 3 · 2027

DC EXIT COMPLETE

- WARP Connector bridging AWS ↔ colo
- Cloudflare Tunnel for all migrated apps
- BGP prefix retained post-DC exit
- Workers — new portal.acmecorp.com live
- Chicago DC dark. Dallas DR exited.

One network fabric. Zero DCs.

Cloudflare One

One network fabric.
Zero trust. Zero incidents.

IMMEDIATE

Magic WAN scoping — confirm Meraki + FortiGate compatibility, run latency benchmarks

JUNE 10

Magic WAN Deep-Dive — IPsec config, BGP design, per-app routing policies

BEFORE SEPT 2026

AT&T non-renewal committed. Magic WAN running in parallel.