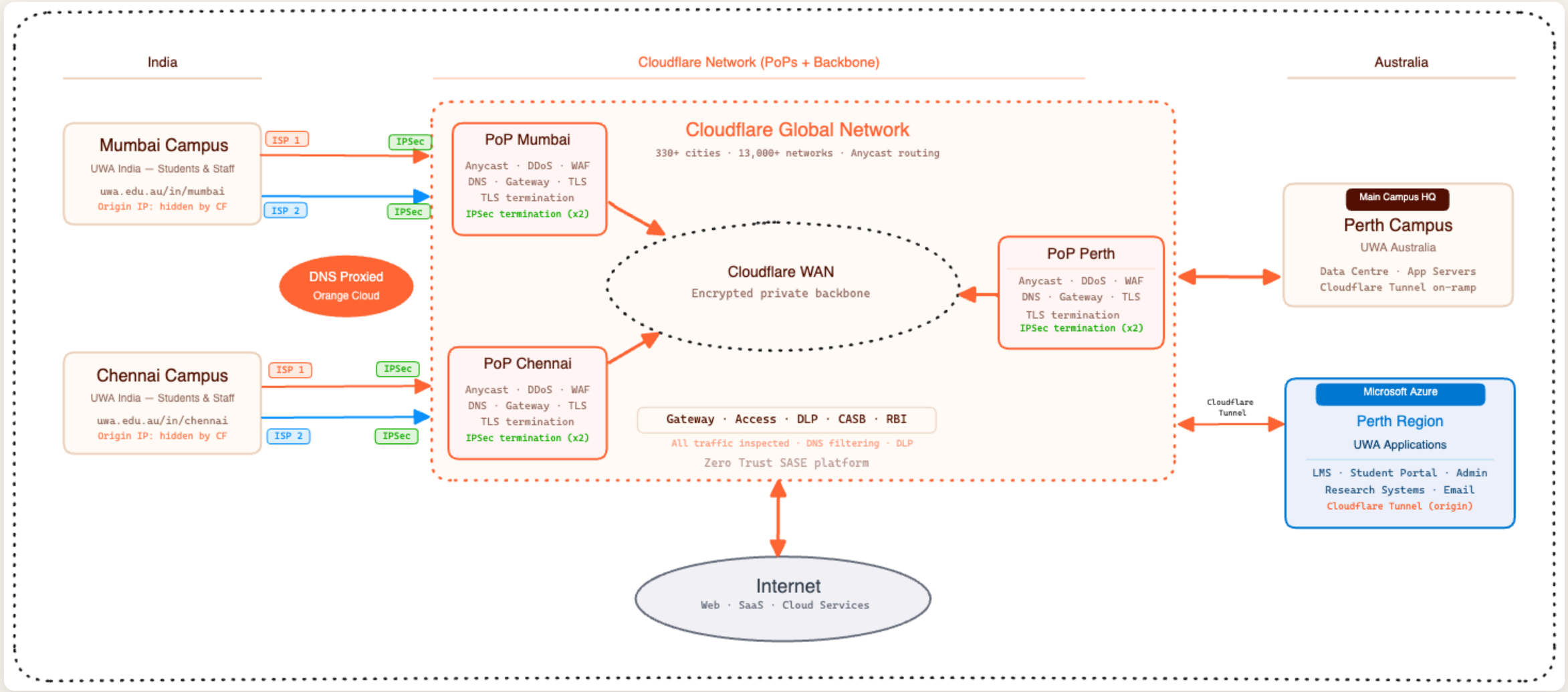
UWA India Campus

Cloudflare WAN Architecture

A Phased Approach to Secure Connectivity

Complete Architecture Overview



Technical Implementation

Phase 1: DNS Protection

Orange-cloud DNS proxy with DDoS mitigation, WAF rules, and bot management. Traffic inspected at Cloudflare's edge before reaching origin.

Phase 2: Cloudflare WAN

Encrypted IPSec tunnels from India campus to Cloudflare's global backbone. Secure, private connectivity to Perth and beyond.

Phase 3: Full SASE

Cloudflare Access for identity, Gateway for SWG, DLP for data protection. Complete Zero Trust architecture.

Global Integration

Unified policy across 330+ cities. Anycast routing ensures optimal performance from Mumbai to Perth and beyond.

Business Outcomes

Security First

Protection against DDoS, bots, and web attacks from day one

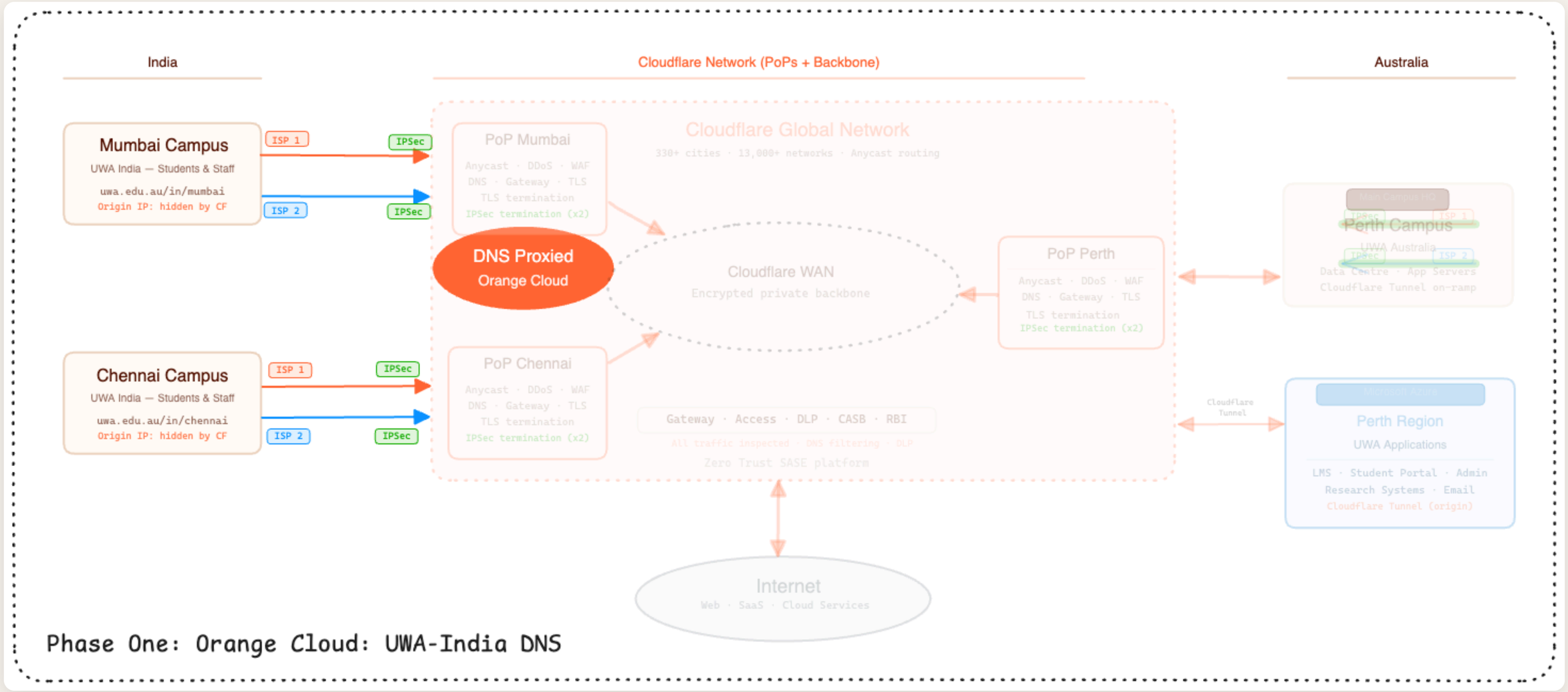
Global Reach

Low-latency connectivity to Perth and worldwide campuses

Zero Trust

Identity-based access and comprehensive data protection

Phase 1: Orange Cloud DNS



Phase 1 Technical Details

Objective: Protect UWA-India public-facing applications and websites

DNS Proxy

- Orange-cloud all DNS records
- Traffic routed through Cloudflare's edge
- Global Anycast network (330+ cities)

DDoS Protection

- Unmetered L3/L4/L7 mitigation
- Automatic attack detection
- Always-on protection

WAF & Bot Management

- OWASP Core Rule Set
- Managed rule sets
- Bot detection and mitigation

SSL/TLS

- Universal SSL certificates
- Automatic HTTPS rewrites
- TLS 1.3 support

Phase 1 Business Value

> *"Protect student portals and academic systems from day one. No hardware, no latency penalty."*

Immediate Benefits

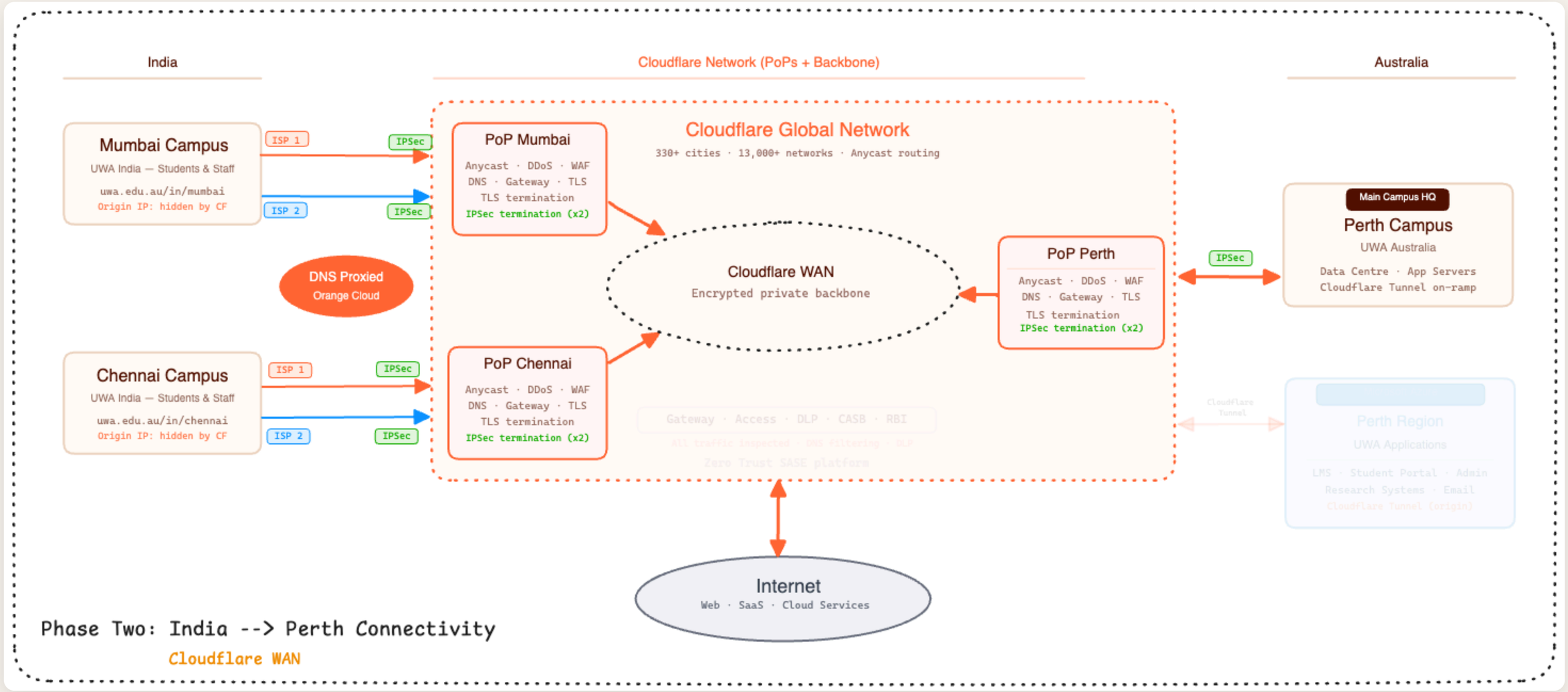
- Sub-50ms latency globally
- 99.9% uptime SLA
- Zero CAPEX deployment

Timeline

Week 1-2 DNS cutover

Week 3-4 WAF tuning

Phase 2: India → Perth Connectivity



Phase 2 Technical Details

Objective: Establish secure, private connectivity between Mumbai campus and Perth HQ

IPSec Tunnels

- Site-to-site IPSec from India firewall
- Cloudflare Tunnel endpoints
- AES-256 encryption in transit

Cloudflare WAN

- Cloudflare's private global backbone
- Anycast routing for optimal paths
- Automatic failover and load balancing

BGP Peering

- Dynamic route advertisement
- Automatic path selection
- Sub-50ms convergence

Traffic Inspection

- All inter-site traffic scanned
- Magic Firewall rules
- DLP for sensitive data

Phase 2 Business Value

> *"Mumbai to Perth in under 100ms with encryption that doesn't slow you down."*

Performance Gains

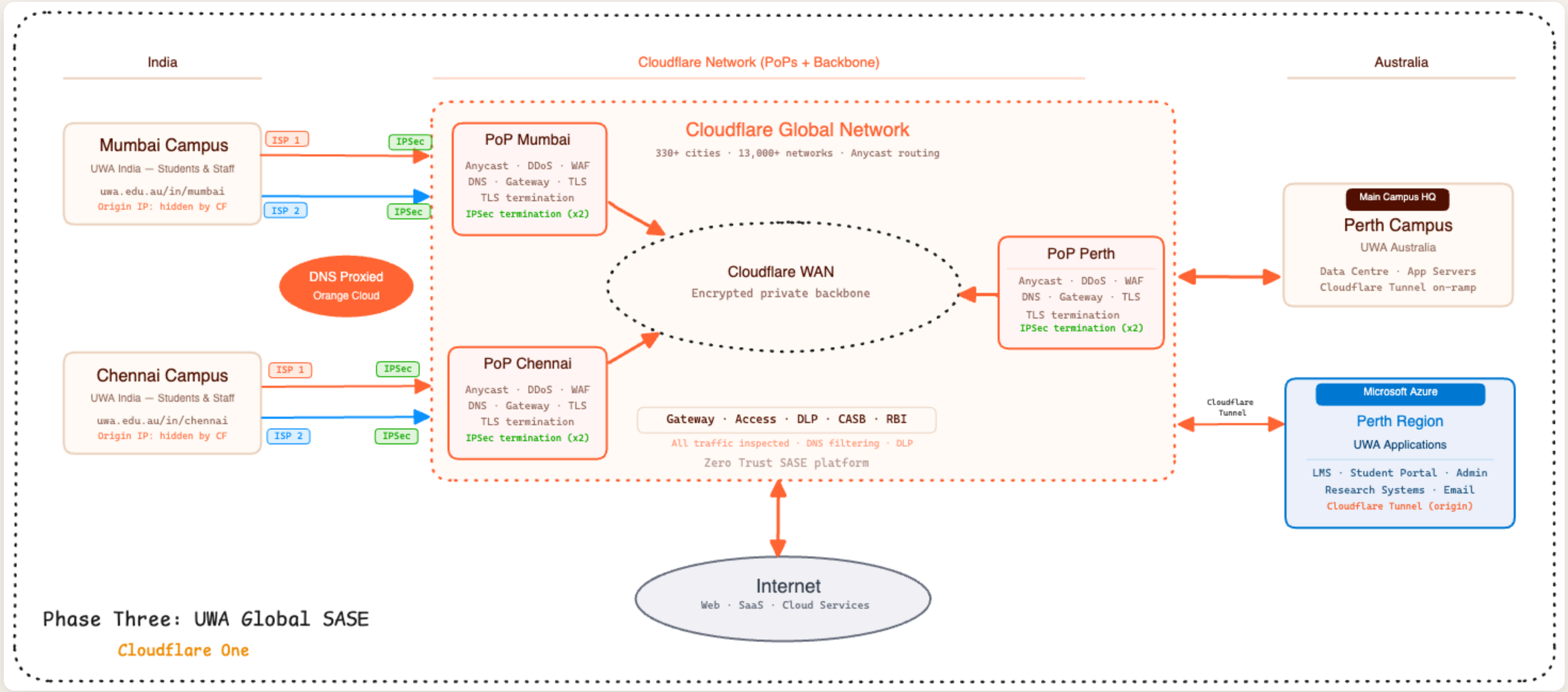
- ~40% latency reduction vs public internet
- Jitter-free video conferencing
- Consistent file transfer speeds

Deployment

Week 1 Tunnel configuration

Week 2 BGP peering

Phase 3: UWA Global SASE



Phase 3 Technical Details

Objective: Complete Zero Trust SASE architecture for all users and devices

Cloudflare Access

- Identity-aware proxy for all apps
- SSO integration (SAML/OIDC)
- Device posture checks

Secure Web Gateway

- DNS, HTTP, and TLS filtering
- URL categorization
- Anti-phishing protection

DLP & CASB

- Data loss prevention policies
- Cloud app visibility
- Shadow IT detection

Browser Isolation

- Zero-day threat protection
- Clientless isolation
- Granular policy control

Phase 3 Business Value

> *"One platform for identity, security, and connectivity. Simplify while strengthening."*

Transformation Outcomes

- Single vendor, single pane of glass
- Consistent policy everywhere
- Reduced security complexity

Rollout Phases

Month 1 WARP deployment

Month 2 Access policies

Month 3 Gateway & DLP

Implementation Roadmap

Phase 1

Orange Cloud DNS

Immediate protection

Weeks 1-4

Phase 2

Cloudflare WAN

Private connectivity

Weeks 5-8

Phase 3

Full SASE

Zero Trust complete

Months 3-6

One platform. Global reach. Zero Trust security.