Magic Transit, Cloudflare Network Firewall & Cloudflare WAN

Network Protection & Transformation for
University of Western Australia

Confidential April 2026

UWA's Current Network Environment

INTERNET UPLINK

AARNet — Australian Academic & Research Network

Advertising a public /16 IP range via AARNet BGP peering. AARNet provides transit.

COMPUTE & STORAGE

On-Premises Data Centres

Core research systems, student services & HPC workloads hosted on campus.

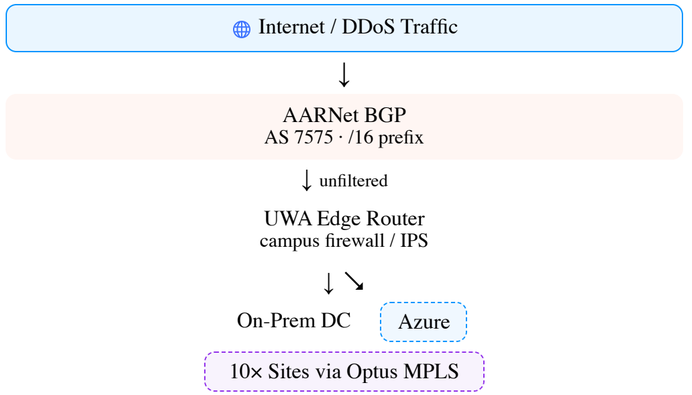
Microsoft Azure — cloud-native workloads & dev/test.

BRANCH WAN

10 campus sites connected via Optus MPLS

Private WAN connecting faculty buildings, satellite campuses & research stations.

CURRENT TOPOLOGY



The Challenge: Universities Are Prime Targets

THE RISK TODAY

- DDoS can saturate the AARNet uplink — attack & legitimate traffic compete for the same pipe
- AARNet provides transit, not scrubbing — attacks hit your edge directly
- Campus firewalls not designed for Tbps-scale floods
- Research, student portals & VoIP share the same IP space

31 Tbps+
largest DDoS in 2025 — beyond on-prem capacity

<1 sec
Cloudflare DDoS detection & mitigation time

ⓘ The gap: AARNet was never designed as DDoS mitigation — the campus edge gets hit first.

EDUCATION SECTOR TRENDS

- Education sector faces rapidly growing DDoS threat volumes (Cloudflare Radar)
- Exam & enrolment periods are prime attack windows
- Research IPs are publicly listed — easily targeted
- Hacktivist groups specifically target academic institutions
- AARNet carries nation-state traffic — complex threat landscape

Magic Transit

DDoS Protection & Traffic Engineering for UWA's Public IP Space

How Magic Transit Works

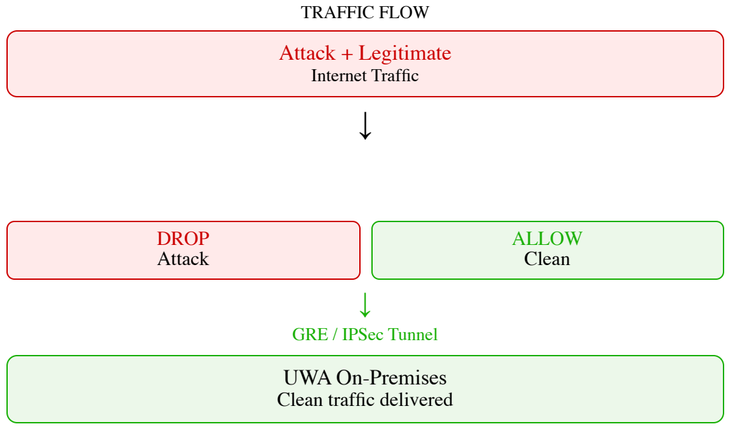
BGP Route Advertisement
Cloudflare announces UWA's IP prefixes to the internet from 330+ cities globally via anycast BGP. Internet traffic is attracted to Cloudflare's nearest PoP.

DDoS Scrubbing at the Edge
All traffic is inspected at Cloudflare's edge — 477 Tbps+ of mitigation capacity. L3/L4 attack traffic is dropped before it reaches UWA.

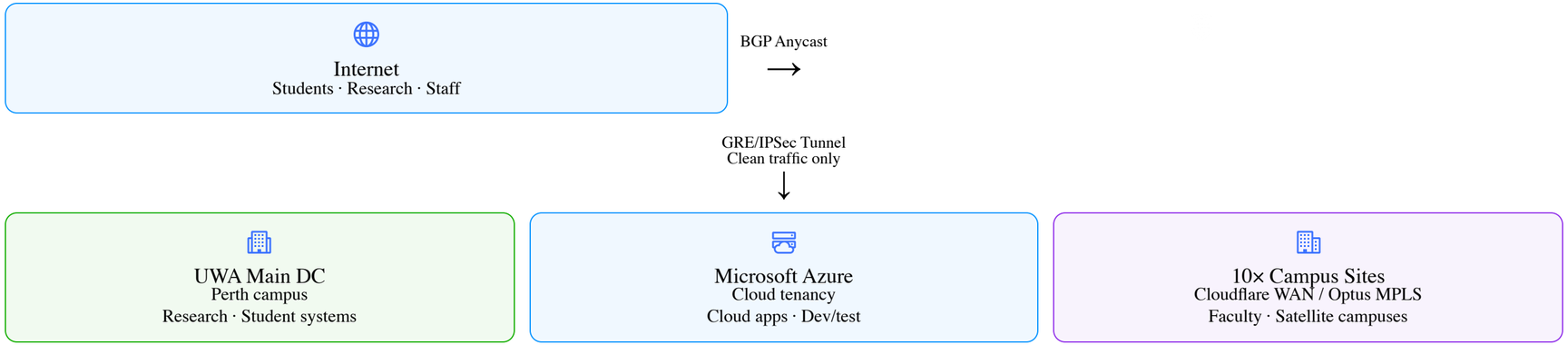
Clean Traffic via Tunnel
Legitimate traffic is encapsulated and forwarded to UWA's edge routers via GRE or IPSec tunnels. UWA retains full IP space ownership (BYOIP).

4

Always-On, Zero Diversion
Protection is active 24/7 — no scrubbing centre diversion required. No latency penalty during clean traffic due to Cloudflare's global backbone.



UWA Architecture with Magic Transit



BYOIP: UWA retains full ownership of the 130.95.0.0/16 prefix — no renumbering, no change to DNS or existing peering. AARNet retained as return-path or backup.

Migration: AARNet → Magic Transit

Phase 1

Onboarding & Provisioning

Cloudflare provisions UWA's IP prefixes. Letter of Authorisation (LOA) issued. IRR route objects validated.

Phase 2

Tunnel Establishment

GRE or IPSec tunnels configured from UWA edge routers to Cloudflare Anycast IPs. Static routes or eBGP for return-path.

Phase 3

Shadow Mode Testing

Cloudflare announces a /24 test prefix. Validate tunnel health, latency & traffic paths before full cutover.

Phase 4

Full BGP Cutover

Cloudflare advertises the full 130.95.0.0/16 from all PoPs globally. AARNet withdrawn or deprioritised via BGP communities.

Validation & Hardening

Cloudflare Network Firewall policies applied. DDoS sensitivity tuned. AARNet retained as standby / return path for redundancy.

TUNNEL OPTIONS

GRE
Higher throughput, lower overhead. Preferred for DC links.

IPSec
Encrypted. Required where ASD/compliance mandates in-transit encryption.

KEY CONSIDERATIONS

- AARNet retained as return path — asymmetric routing supported
- GRE MTU: set to 1476 bytes to avoid fragmentation
- Health checks per tunnel with automatic failover
- No impact to DNS, SSL or applications
- BGP cutover propagation: 15–30 minutes

Zero downtime migration — phased BGP shifts allow rollback at any point before full cutover.

Active/Backup DC — How Magic Transit Controls Traffic

STEP 1 — TUNNEL ESTABLISHMENT

Both DC1 and DC2 establish GRE or IPSec tunnels to Cloudflare's anycast endpoints. Each terminates on a different UWA border router — giving Cloudflare two independent paths into 130.95.0.0/16.

STEP 2 — ROUTE PRIORITY CONTROLS ACTIVE DC

Each tunnel is assigned a priority in Cloudflare's routing table. Lower value = preferred. All inbound traffic goes to the lowest-priority healthy tunnel.

DC1 Tunnels
100
Active — all traffic here

DC2 Tunnels
200
Standby — no traffic

STEP 3 — AUTOMATIC FAILOVER <1 SECOND

Cloudflare probes every tunnel continuously from all 330+ PoPs. If DC1 tunnels fail, a +1,000,000 priority penalty is applied, making DC2 the winner. No manual intervention needed.

OPTIONAL — BGP PEERING FOR DYNAMIC CONTROL

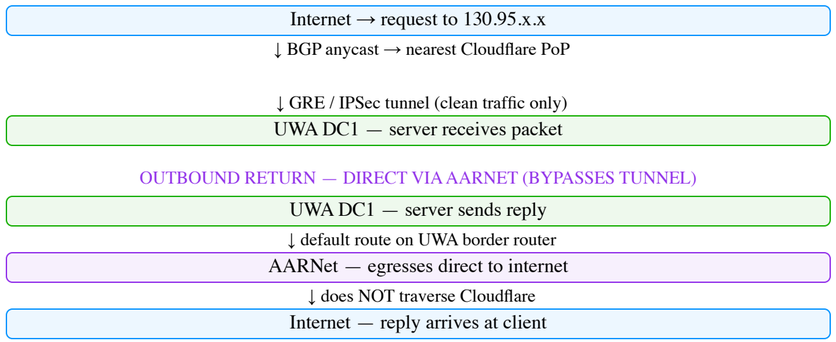
UWA can run eBGP sessions over the tunnels for dynamic, automated routing control:

- Planned maintenance: Withdraw BGP routes from DC1 — Cloudflare shifts to DC2 within ~20 seconds globally
- Traffic weighting: Advertise different MED values to bias traffic toward one DC
- BGP communities and AS prepending supported for fine-grained engineering

TRAFFIC CONTROL — SUMMARY

Static route priority	Dashboard / API — always-on, <1s failover
Tunnel health checks	Automatic detection — <1 second
BGP withdraw	Dynamic — ~20s global convergence
BGP communities / MED	Traffic engineering & weighting

Magic Transit Traffic Flow — Unidirectional by Default



THIS IS CALLED DIRECT SERVER RETURN (DSR)

Magic Transit processes inbound traffic only by default. The GRE/IPSec tunnel carries packets from Cloudflare to UWA — return traffic goes direct via AARNet and never enters the tunnel. This is the standard deployment model.

IMPLICATIONS FOR UWA'S DC DESIGN

- Stateful firewalls: Must handle asymmetric flows — inbound arrives via CF tunnel, return leaves via AARNet on a different interface
- Each DC is independent: Both DCs handle their own return traffic via their own AARNet uplinks — no cross-DC return path
- Source IPs preserved: No NAT — Cloudflare delivers the original client IP to UWA's servers
- DDoS doesn't affect AARNet outbound: Only clean traffic arrives — inbound attack absorption happens at Cloudflare

Optional — Magic Transit Egress: Routes outbound traffic back through Cloudflare via PBR at the DC edge, providing symmetric routing and outbound firewall filtering on the return path.

Magic Transit: Pros & Cons for UWA

Advantages

- Always-on protection — no human intervention required
- 477+ Tbps capacity — absorbs any realistic DDoS volume
- Sub-second mitigation — autonomous L3/L4 blocking
- BYOIP — UWA retains full IP ownership; no renumbering
- Perth PoP — local presence for low-latency ingress
- AARNet continuity — kept as return path or failover
- Unified platform — transit, firewall & WAN in one dashboard
- Reduces hardware — edge DDoS appliances no longer needed
- Compliance-ready — IPSec, audit logs, full flow analytics

Considerations

- Routing architecture change — BGP & tunnel config on edge devices
- MTU tuning required — GRE reduces MTU to 1476 bytes
- Asymmetric routing — return path via AARNet needs validation
- Subscription cost — priced on committed bandwidth capacity
- AARNet coordination — prefix withdrawal requires NOC engagement
- Tunnel redundancy — 2× tunnels per DC recommended for HA

Mitigating factor: All are standard network engineering tasks. Cloudflare's onboarding team provides full migration support throughout.

AARNet vs Magic Transit: Side by Side

DDoS Protection	None (transit only)	Always-on, 477 Tbps
Scrubbing Capacity	None	477 Tbps globally
L3/L4 Firewall	Not included	Cloudflare Network Firewall included
Global PoPs	AU & NZ focused	330+ cities, 120 countries
IP Ownership	UWA retains	UWA retains (BYOIP)
Mitigation Time	N/A — attack hits campus	<1 second (automated)
Analytics	Limited NetFlow	Full traffic analytics dashboard

AARNet and Magic Transit are complementary — AARNet can be retained for outbound routing & research network peering while Cloudflare handles all inbound protection.

Cloudflare Network Firewall

Network-Level Filtering at Cloudflare's Edge — Before Traffic Reaches UWA

Cloudflare Network Firewall: What It Does

WHAT IS MAGIC FIREWALL?

A cloud-delivered, stateless L3/L4 firewall enforcing network access control at Cloudflare's global edge — applied to Magic Transit traffic before it reaches your network.

RULE CAPABILITIES

- Filter on source/dest IP, CIDR, port, protocol
- Match on packet length, TTL, TCP flags, ICMP type
- Wireshark-syntax expressions for complex rules
- Apply globally or per-tunnel / per-prefix
- Evaluated at line rate — no performance penalty

MANAGEMENT

- Dashboard UI, API & Terraform supported
- Rule changes propagate globally in seconds
- Integrated with Magic Transit analytics

EXAMPLE RULES (Wireshark syntax)

magic-firewall.conf

```
# Block DNS floods from non-AU/NZ sources
ip.dst in { 130.95.0.0/16 } and
udp.dstport == 53 and
not ip.geoip.country in { "AU" "NZ" }

# Drop SYN floods to admin subnet
ip.dst == 130.95.128.0/24 and
tcp.flags.syn == 1 and
not ip.src in { 130.95.0.0/16 10.0.0.0/8 }
```

REPLACES / AUGMENTS

Before
On-prem ACLs — attack traffic still hits campus

After
Policies enforced at Cloudflare edge globally

Included with Magic Transit — no additional licensing for base L3/L4 filtering. Advanced IDS/IPS available as add-on.

Cloudflare Network Firewall: UWA Use Cases

USE CASE 1

Geo-Blocking

Block inbound traffic from high-risk countries to sensitive research subnets — enforced at Cloudflare's edge, not campus firewall.

USE CASE 2

Protocol Enforcement

Restrict ICMP floods, drop malformed UDP targeting HPC nodes, enforce port allowlists per subnet segment.

USE CASE 3

IP Reputation

Apply Cloudflare threat intelligence to block known botnet C2 IPs and scanner ASNs from reaching UWA IP space.

USE CASE 4

Exam Period Rules

Apply strict temporary rules during exam windows — deployed via API in seconds, rolled back instantly after.

USE CASE 5

Azure Subnet Isolation

Restrict which public IPs can reach UWA's Azure services — upstream enforcement complements Azure NSGs.

USE CASE 6

Site Segmentation

As MPLS migrates to Cloudflare WAN, firewall enforces inter-site access control — replacing hardware rules at branch edges.

Cloudflare WAN

Connecting UWA's 10 Sites via Cloudflare's Global Private Backbone

Cloudflare WAN: SD-WAN on Cloudflare's Backbone

WHAT IS MAGIC WAN?

Cloudflare WAN replaces or augments traditional MPLS by routing branch traffic through Cloudflare's private backbone — connecting sites, cloud & internet via a single fabric.

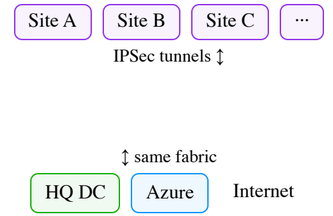
HOW SITES CONNECT

- IPSec tunnels from site routers to Cloudflare anycast endpoints
- Cloudflare One Connector — hardware or virtual for sites without IPSec
- BGP or static routing for prefix advertisement per site
- Traffic routed across Cloudflare's private backbone

INTERNET TRAFFIC OPTION

Branch internet can egress via Cloudflare Gateway (SWG) — DNS filtering, URL filtering & malware inspection for all branch users, replacing branch firewall stacks.

MAGIC WAN TOPOLOGY



All traffic policies managed from one dashboard

Cloudflare WAN: Replacing Optus MPLS for UWA

TODAY — OPTUS MPLS

- Fixed-cost circuits
- Long contract terms
- Limited bandwidth
- No cloud on-ramp
- Separate firewall/site
- Provider-managed routing

FUTURE — MAGIC WAN

- Any broadband / 4G / 5G
- Elastic bandwidth
- Native cloud on-ramp
- Centralised policy mgmt
- Built-in SWG & firewall
- UWA-controlled routing

MIGRATION APPROACH

- Deploy IPSec tunnels alongside existing MPLS — no disruption
- Migrate sites one-by-one with policy-based routing
- MPLS retained as backup / failover during transition

Azure: Connects via Cloudflare backbone — no ExpressRoute needed. Private routing across on-prem, sites & Azure on one fabric.

UWA — 10 SITES ON MAGIC WAN

Crawley Main campus	Claremont Sport campus
Nedlands Medical campus	Albany Regional campus
Broome Regional campus	+ 5 sites Research stations

↕ IPSec tunnels over any WAN

Why Cloudflare's Network Matters for UWA

321
cities in 120+ countries

477+
Tbps DDoS scrubbing capacity

<1s
median DDoS mitigation time

50ms
RTT for 95% of AU internet users

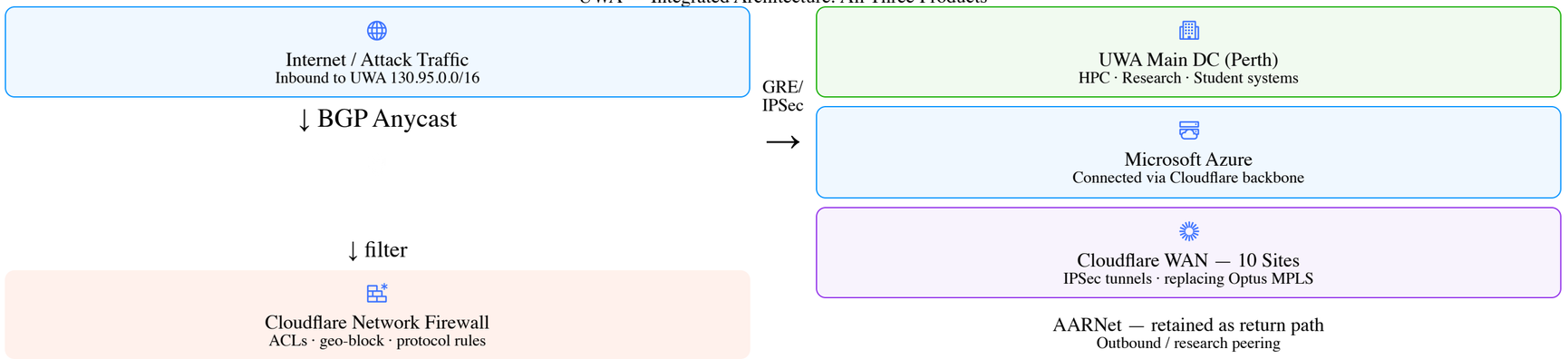
AUSTRALIA & NZ PRESENCE

- Perth — local PoP for low-latency UWA ingress
- Sydney, Melbourne, Brisbane, Adelaide, Canberra
- Auckland — NZ research partner access
- Direct peering with AARNet, Telstra, Optus, TPG

EDUCATION SECTOR EXPERIENCE

- Cloudflare protects multiple Group of Eight universities in Australia
- AARNet peering keeps academic traffic on trusted networks
- Supports HECVAT and ISO 27001 compliance requirements
- Project Galileo — free protection for at-risk research arms

UWA — Integrated Architecture: All Three Products



Why Cloudflare for UWA

SECURITY OUTCOMES

- Eliminate DDoS risk from AARNet uplink saturation
- Protect research & students during exam periods
- Network firewall before traffic hits campus
- Cloudflare threat intelligence on every packet

OPERATIONAL & COMMERCIAL

- Single platform for security + WAN + cloud
- Centralised policy — dashboard or Terraform
- Displace Optus MPLS costs with Cloudflare WAN
- AARNet relationship preserved & complementary
- Future-ready: extend to ZTNA, Gateway & DLP

COMPLIANCE & TRUST

- ISO 27001, SOC 2 Type II certified
- IRAP assessed — ASD-aligned assessment framework for AU Government workloads
- AU traffic stays in AU PoPs (Perth, SYD, MEL)
- Full audit logging & flow analytics

cities globally

Recommended Next Steps

Technical Discovery Workshop

Deep-dive with UWA network team — validate prefix sizes, tunnel endpoints, BGP config, MPLS topology & Azure requirements.

Proof of Concept — Magic Transit

30-day PoC: GRE tunnel, test prefix, validate health, latency & DDoS mitigation behaviour in shadow environment.

3

AARNet Coordination

Engage AARNet NOC on BGP withdrawal process, return-path options & peering during transition period.

4

Cloudflare WAN Site Assessment

Audit the 10 Optus MPLS sites — router models, broadband circuits & connectivity to plan migration timeline.

5

Commercial Engagement

Indicative pricing based on committed Mbps for Magic Transit, Cloudflare WAN site count & seats. Education pricing available.