CLOUDFLARE

Replacing Azure Application Gateway WAF with Cloudflare

HTTP DDoS Mitigation & Next-Generation Web Application Firewall

HTTP Layer 7 DDoS

WAF & Custom Rules

Bot & Challenge Management

Global Policy Control

The Challenge

Why Azure Application Gateway WAF is falling short

CLOUDFLARE

Azure AppGW + WAF: Four Critical Gaps

An active HTTP DDoS attack has exposed fundamental limitations in Azure's Application Gateway WAF. These aren't edge cases — they are architectural constraints.

⚠ GAP 1

CRS-Only WAF Rules

Rules are based on OWASP CRS with no Cloudflare-equivalent proprietary threat intelligence or ML-based attack scoring

⚠ GAP 2

No ASN Blocking

No native capability to block traffic by Autonomous System Number — impossible without custom scripting outside the WAF

⚠ GAP 3

CAPTCHA Requires Azure Front Door

Challenge/CAPTCHA capabilities are only available when routing through Azure Front Door — a significant architectural dependency

⚠ GAP 4

No Global Policy Management

Separate WAF policies per site means no way to push a global block or exclusion across all protected properties without scripting

Gap 1 — WAF Rules Limited to CRS

AZURE APPGW WAF

- **OWASP CRS v2.x** — older rule set, higher false positive rates, limited to signature matching only
- **NGINX + mod_security** architecture — essentially an Azure Portal wrapper around a commodity WAF stack
- **No proprietary threat intelligence** — rules are community-sourced, not informed by Cloudflare-scale traffic visibility
- **No ML-based attack scoring** — binary signature match only, unable to detect novel attack patterns

CLOUDFLARE WAF

- **Cloudflare Managed Ruleset** — proprietary, curated by Cloudflare's security team. Updated weekly + emergency releases for zero-days
- **OWASP CRS v3.x** — newer standard with paranoia levels (PL1–PL4), transparent scoring, lower false positive rates
- **WAF Attack Score (ML)** — machine learning scores every request for SQLi, XSS, and RCE independently of signatures
- **Per-rule overrides**, tag-based overrides, and granular rule customisation via dashboard or API

Gap 2 — No ASN Blocking

AZURE APPGW WAF

- **No native ASN blocking** — cannot block traffic from entire hosting networks or botnets using ASN
- **IP-only granularity** — blocking individual IPs during a distributed attack is operationally infeasible
- **Requires external scripting** to automate IP range extraction and WAF rule updates during an active DDoS
- **No expression-based logic** — cannot combine ASN with URI path, request method, or other signals in a single rule

CLOUDFLARE WAF

- **Native ASN blocking** via IP Access Rules or Custom Rules — no scripting required, available in the dashboard
- **Compound expressions** — combine ASN with country, URI path, bot score, rate, and more in a single rule
- Example:

```
(ip.src.asnum in {12345 67890}) and not cf.verified_bot
```

- **Account-scope application** — one IP Access Rule can block an ASN across all zones in the account simultaneously

Gap 3 — CAPTCHA Requires Azure Front Door

AZURE APPGW WAF

- **Architectural dependency** — challenge/CAPTCHA requires routing through Azure Front Door, a separate product with its own cost and configuration
- **Traditional CAPTCHA** — degrades user experience, increasingly bypassable by automated tools, accessibility concerns
- **Not available standalone** — no challenge capability on AppGW WAF without the full Front Door integration path
- **Limited under attack** — no rapid "challenge all" mode for immediate DDoS response without architectural changes

CLOUDFLARE

- **Managed Challenge** — available as an action on any WAF rule, DDoS override, or bot rule. No separate product required
- **No CAPTCHA** — Cloudflare has moved entirely to non-interactive challenges: invisible JS proofs, Private Access Tokens (Apple), button-click fallback
- **Under Attack Mode** — one-click site-wide JS challenge during an active attack. Disableable instantly once attack subsides
- **Turnstile** — embeddable CAPTCHA alternative for forms/logins. Works independently, no architectural dependency

Gap 4 — No Global Policy Management

AZURE APPGW WAF

- **Per-site WAF policies** — each Application Gateway has its own WAF policy, no shared global baseline
- **No cross-policy propagation** — adding a block for a new attack vector requires updating every WAF policy individually
- **Scripting required** — the only practical way to synchronise rules across all sites is through Azure CLI/PowerShell automation
- **No exclusion inheritance** — a false positive fix on one site must be manually replicated to every other site

CLOUDFLARE ENTERPRISE WAF

- **Account-level WAF** — define custom rules, rate limiting rules, and managed ruleset deployments once at the account level; apply to all zones
- **Account-level custom rulesets** — a single ruleset deployed globally with per-zone expression overrides for site-specific customisations
- **Account-level rate limiting** — define rate limits once and push to all Enterprise zones simultaneously
- **IP Access Rules (account scope)** — one click to apply an ASN or IP block across every zone in the account

The Cloudflare Solution

A layered defence purpose-built for HTTP DDoS and application security

Cloudflare — Every Service on Every Server

ONE GLOBAL ANYCAST NETWORK

Cloudflare operates **330+ cities across 120+ countries**. Unlike traditional vendors with centralised scrubbing centres, every Cloudflare location runs **every product simultaneously** — WAF, DDoS mitigation, CDN, bot management, and more.

TRAFFIC INSPECTED CLOSEST TO THE SOURCE

Attack traffic is identified and absorbed at the PoP **nearest to the attacker** — never backhauled to a remote scrubbing centre. This eliminates the latency penalty that traditional DDoS mitigation services impose during an active attack.

NO SPECIALISED HARDWARE — SOFTWARE-DEFINED

Every capability — WAF rules, rate limiting, bot scoring, DDoS mitigation — is delivered as **software running on commodity servers**. New rules and mitigations propagate globally in seconds, not hours.

EVERY SERVER IN EVERY CITY RUNS:

- **HTTP DDoS Protection**
- **WAF & Custom Rules**
- **Bot Management**
- **Rate Limiting**
- **Managed Challenges**
- **SSL/TLS Termination**
- **CDN & Caching**
- **DNS Resolution**

The result: Consistent protection with no single point of failure, no scrubbing centre latency, and capabilities that scale with Cloudflare's entire network capacity — not a single region's headroom.

Always-On HTTP DDoS Protection

Always enabled — no configuration needed. The HTTP DDoS Attack Protection managed ruleset cannot be turned off. It is active from the moment a zone is onboarded.

~3 second average time to mitigate. Cloudflare's Autonomous Edge detects attack fingerprints and installs ephemeral mitigation rules in real time — before traffic reaches Azure.

Unmetered and uncapped. No limits on attack size or duration. No per-GB or per-request pricing for DDoS mitigation traffic.

~3s
Avg. L7 mitigation time

∞
No attack size cap

330+
Cities — attack absorbed at edge

0
Manual intervention required

UNDER ATTACK MODE

One-click site-wide JS challenge. Activatable immediately from the dashboard or API during an active attack. Disable instantly when the attack subsides.

WAF: Far Beyond CRS

CLOUDFLARE MANAGED RULESET

Proprietary rules written by Cloudflare's security team. Covers known attack techniques, CVEs, and zero-day vulnerabilities. Updated **weekly** with emergency releases for critical threats. This is not CRS — it is informed by traffic across **millions of zones**.

CLOUDFLARE OWASP CORE RULESET (V3.X)

Cloudflare's implementation of OWASP CRS **v3.x** (vs Azure's v2.x). Features paranoia levels PL1–PL4 and a transparent threat scoring model. Tune sensitivity without blanket disables.

WAF ATTACK SCORE (ML)

Machine learning model that scores every request for **SQLi, XSS, and RCE** independently of signature matching. Catches novel attack patterns that no signature can anticipate. Combine with custom rules for surgical policies.

FULL CUSTOMISABILITY

Per-rule overrides, tag-based overrides (e.g. disable all WordPress rules on a non-WP site), WAF exceptions, and custom rules — all configurable via dashboard or API with full Terraform support.

ASN Blocking & Compound Custom Rules

IP ACCESS RULES — ASN BLOCKING

Block, allow, or challenge traffic by IP, IP range, country, or **ASN** — natively in the Cloudflare dashboard. Apply to a single zone or to **all zones in the account** with one rule.

CUSTOM RULES — EXPRESSION LANGUAGE

Full expression syntax. Combine any request signal — ASN, country, URI, headers, bot score, rate — in a single rule. Actions: Block, Managed Challenge, JS Challenge, Log, Skip.

EXAMPLE: BLOCK ATTACK ASNS

```
(ip.src.asnum in {12345 67890 11111})
```

EXAMPLE: BLOCK ASN EXCEPT VERIFIED BOTS

```
(ip.src.asnum eq 12345)
  and not cf.verified_bot
```

EXAMPLE: CHALLENGE ASN ON SPECIFIC PATH

```
(ip.src.asnum eq 12345)
  and (http.request.uri.path contains "/api")
```

Managed Challenges — No CAPTCHA Required

MANAGED CHALLENGE

Cloudflare's non-interactive challenge selects the appropriate verification method dynamically — **invisible JS proof**, Private Access Tokens (Apple devices), or a button click as a last resort. Available as an action on any WAF rule, DDoS override, or bot rule. No separate product. No Azure Front Door equivalent required.

TURNSTILE

Cloudflare's embeddable CAPTCHA alternative. Drop a widget into any login or form page. Visitors are challenged invisibly — no image puzzles. Works via client-side JS + server-side token validation. No routing through Cloudflare required for deployment.

UNDER ATTACK MODE

Activatable in seconds from the Cloudflare dashboard, API, or Terraform. Applies a JS Challenge to **all HTTP traffic** site-wide. The most effective immediate-response tool during an active HTTP DDoS flood — no architectural change needed.

BOT MANAGEMENT INTEGRATION

Combine challenges with Cloudflare Bot Management — challenge only traffic below a bot score threshold, whitelist verified crawlers, and build fine-grained rules using ML-derived signals alongside ASN, country, and URI conditions.

Account-Level WAF — Global Policy Control

ACCOUNT-LEVEL CUSTOM RULESETS

Define a set of custom rules **once at the account level** and deploy them across all zones. Use scope expressions to target all zones or specific subsets. Site-specific overrides layer on top without disrupting the global baseline.

ACCOUNT-LEVEL MANAGED RULESET DEPLOYMENT

Deploy the Cloudflare Managed Ruleset and OWASP Core Ruleset at account level with per-zone expression overrides. Different OWASP paranoia levels per application, different actions per hostname — all managed from a single place.

ACCOUNT-LEVEL RATE LIMITING

Create rate limiting rules once and **deploy to all Enterprise zones simultaneously**. A single update during an active attack propagates instantly to every protected site — no per-zone scripting.

TERRAFORM & API-FIRST

Every account-level WAF configuration is fully manageable via the Cloudflare API and official Terraform provider. Enables GitOps workflows — WAF policy changes reviewed, version-controlled, and deployed like code.

Adaptive DDoS Protection

TRAFFIC BASELINE LEARNING

Cloudflare builds a unique traffic profile for your zone over 7 days — measuring normal request rates by **country/region, User-Agent distribution, and origin error rates**. During an attack, Adaptive DDoS detects deviations from this baseline and automatically tightens mitigation thresholds.

EFFECTIVE AGAINST SOPHISTICATED ATTACKS

Particularly effective against **low-and-slow application layer attacks** that fall below static threshold rules but deviate significantly from the zone's normal traffic pattern. The profile self-updates as legitimate traffic evolves.

For Locations

Detects abnormal geo-distribution vs your 7-day baseline

For User-Agents

Flags unusual UA distribution across Cloudflare's entire network

For Origins

Mitigates floods that spike your origin error rate above profile

Self-Adapting

Profile updates continuously — no manual tuning needed

CLOUDFLARE

Why Cloudflare for WA Government?

IRAP assessed. Essential Eight aligned. Data sovereignty built in. Trusted by Australia's peak cyber authority.

The Australian Cyber Threat Landscape

Source: **ASD's ACSC Annual Cyber Threat Report 2024–25** · cyber.gov.au · Published October 2025

+280%
Rise in DDoS/DoS incidents — 200+ responded to in FY24–25

+83%
Increase in malicious cyber activity notifications to entities

+111%
Rise in critical infrastructure cyber activity notifications

$202K
Avg. cybercrime cost to large business — up 219%

Top Threats to Government (FY24–25)

37% — Compromised asset / network / infrastructure
16% — DoS / DDoS attacks — second highest threat type
15% — Malware infection
State-sponsored actors (PRC, Russia) actively targeting Australian government networks

Top Threats to Critical Infrastructure (FY24–25)

55% — Compromised asset / network / infrastructure
23% — DoS / DDoS — a top-3 threat for CI sectors
19% — Compromised accounts / credentials
ASD warns CI entities face increasing risk of disruptive attacks on essential services

Australia's Peak Cyber Authority — Trusted strategic industry partnership with Cloudflare. In March 2025, ASD's ACSC — in cooperation with **Cloudflare Pty Ltd** and NZ's NCSC — published the official Australian Government guidance: "Preparing for and Responding to Denial-of-Service Attacks" on **cyber.gov.au**.

The WA Government Context

WA state government departments face a unique and demanding set of challenges — all validated by the ACSC's 2024–25 Annual Cyber Threat Report.

Escalating Cyber Threats

DDoS against Australian organisations up **280%** — ACSC responded to 200+ incidents in FY24–25

State-sponsored actors (PRC, Russia) actively targeting government and CI networks

Ransomware, credential theft, and data breaches increasing year-on-year

Data Sovereignty Requirements

WA government data must remain in Australia

SOCI Act 2018 — cloud now classified as critical infrastructure

Privacy Act 1988 — APP 11 security obligations apply

Essential Eight Compliance

ACSC Essential Eight mandatory for Commonwealth; adopted at state level

ACSC published 26 PROTECT publications in FY24–25 including Essential Eight updates

Maturity Level 2+ now expected for sensitive workloads

Legacy IT Modernisation

ACSC recommends "replace legacy IT" as a key strategic priority for all organisations

Ageing VPNs are a primary attack vector — Zero Trust is the modern replacement

MPLS and on-premise firewalls not fit for cloud-first, hybrid work environments

Budget & Taxpayer Accountability

Avg. cybercrime cost to large organisations up **219%** — cost of inaction is rising

Vendor consolidation is a strategic priority to maximise taxpayer value

Prevention is measurably cheaper than breach response

Procurement & Trust

IRAP assessment is the mandatory government procurement credential

BuyICT / Cloud Marketplace panel arrangements shorten sales cycle

Cloudflare's co-authorship with ACSC demonstrates highest-level government trust

Cloudflare's Australian Government Credentials

Official ACSC Partner: Cloudflare co-authored the Australian Government's definitive DDoS guidance with ASD's ACSC (March 2025) — published on cyber.gov.au.

IRAP ASSESSED

Active IRAP assessment at **OFFICIAL** and **PROTECTED** classification levels — assessed against the ISM. The mandatory credential for government procurement. Agencies can issue an ATO using Cloudflare's IRAP report.

CERTIFICATIONS

ISO 27001 · SOC 2 Type II · FedRAMP Moderate · PCI DSS · GDPR · CSA STAR

DATA SOVEREIGNTY

PoPs in **Perth · Sydney · Melbourne · Brisbane · Adelaide**. Data Localisation Suite pins inspection, logs & keys to Australian nodes. Logpush to Australian storage (S3 Sydney / Azure Australia East). Supports 12–72 hour SOCI Act incident reporting to ASD/ACSC.

SOCI ACT COMPLIANCE

Mandatory incident reporting within 12–72 hours to ASD/ACSC. No dependency on adversarial nation infrastructure. Detailed log retention via Logpush supports all audit requirements.

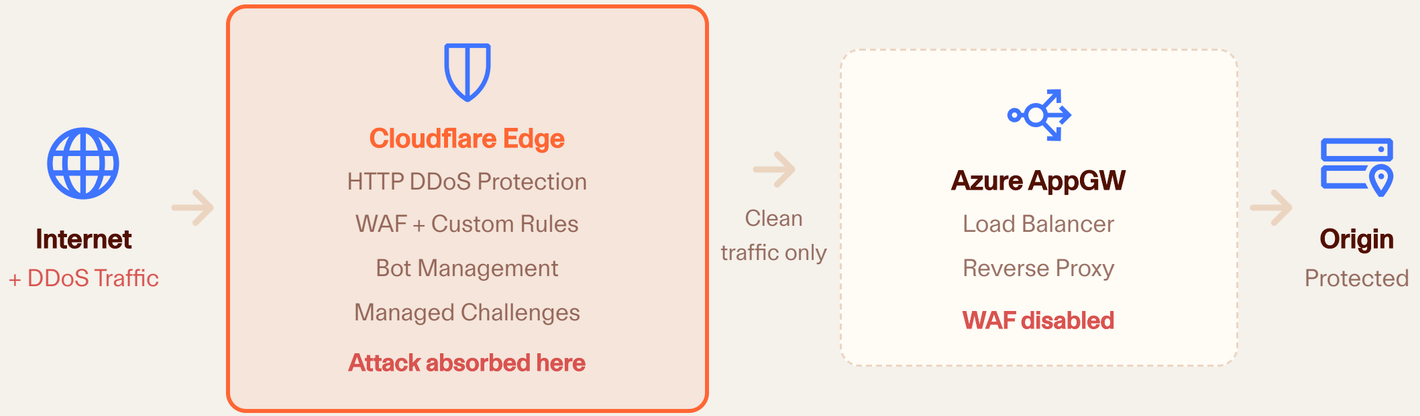
Essential Eight — Cloudflare Mapping

Cloudflare helps WA government agencies achieve Essential Eight maturity across all eight strategies:

ESSENTIAL EIGHT STRATEGY	CLOUDFLARE SOLUTION	MATURITY SUPPORT
Application Control	Zero Trust Gateway — enforce application access policies per user and device	ML 1–3
Patch Applications	WAF virtual patching — block exploits targeting unpatched vulnerabilities before patching occurs	ML 1–3
Configure MS Office Macros	Area 1 Email Security stops macro-laden phishing payloads + Remote Browser Isolation	ML 1–3
User Application Hardening	Remote Browser Isolation (RBI) — removes the browser attack surface entirely	ML 2–3
Restrict Admin Privileges	Cloudflare Access — least privilege, per-resource, time-limited access with MFA enforcement	ML 2–3
Patch Operating Systems	Zero Trust device posture checks — block non-compliant or unpatched OS versions at access time	ML 2–3
Multi-Factor Authentication	Cloudflare Access enforces MFA at the identity layer across all supported identity providers	ML 2–3
Regular Backups	R2 Object Storage — durable, zero egress fees, Australian region, supports backup workflows	ML 1–3

Simple High Level Implementation Design

Cloudflare sits in front of the existing Azure Application Gateway (retained as a load balancer and reverse proxy — WAF disabled). No changes to the internal Azure network architecture are required.



No re-architecture required

DNS change only — point the zone to Cloudflare nameservers. Azure AppGW remains in place as LB/proxy.

Origin IP protected

Cloudflare masks the Azure AppGW public IP. Lock AppGW to accept connections from Cloudflare IP ranges only.

Incremental rollout

Onboard sites one at a time in Log mode first — validate zero false positives before switching to Block.

CLOUDFLARE

Cloudflare Tunnel — Hardening Your Azure Origin

WHAT IS CLOUDFLARE TUNNEL?

A lightweight daemon (`cloudflared`) installed inside your Azure environment. It creates **outbound-only, post-quantum encrypted connections** to Cloudflare's global network — no inbound firewall rules, no open ports, no public IP required on your origin.

HOW IT DEPLOYS IN AZURE

Install `cloudflared` as a container in **AKS**, an **Azure Container Instance**, or directly on an **Azure VM**. Maintains 4 connections across 2+ Cloudflare data centres for automatic failover. No changes to existing Azure network routing required.

THE RESULT: A DARK ORIGIN

Once the Tunnel is active, your Azure NSG inbound rules can be set to **deny all internet traffic**. The AppGW public IP still exists but has no open ports — any attacker who discovers it hits nothing. There is no IP, no port, no attack surface to target.

TRAFFIC FLOW WITH TUNNEL ACTIVE

Internet + Attackers → **Cloudflare Edge**

WAF + DDoS + Bot applied here. Attack traffic dropped.

Cloudflare Edge → Tunnel (QUIC/PQ) → **Azure AppGW**

Clean traffic only. AppGW has no internet exposure.

Direct to Azure IP — Blocked — NSG denies all inbound

No public IP exposed
Origin unreachable from internet

Zero inbound ports
NSG: deny all inbound internet

Bypass attacks blocked
Can't reach origin even if CF is bypassed

Post-quantum encrypted
QUIC protocol, future-proof encryption

Cloudflare Tunnel — The Azure Cost Case

Bandwidth Alliance: Microsoft Azure is a **founding member** of the Cloudflare Bandwidth Alliance. Traffic between Azure and Cloudflare travels over private peering connections and 108+ public peering links — not paid transit — giving mutual customers **discounted egress fees** on Azure→Cloudflare traffic. Cloudflare customers see an **average 60% reduction in Azure bandwidth usage**. (Source: cloudflare.com/integrations/microsoft-azure)

COST AREA	WITHOUT CLOUDFLARE	WITH CLOUDFLARE + BANDWIDTH ALLIANCE
AppGW WAF_v2 Tier	Per-hour fixed charge + per-capacity-unit fees on top of Standard_v2 base. CU consumption spikes unpredictably during DDoS attacks — driving unplanned cost.	Downgrade AppGW to Standard_v2 (LB/proxy only). Cloudflare WAF replaces the WAF tier — included in Enterprise, no per-rule or per-CU charges.
Azure Egress Fees	Per-GB billing on all outbound data to the internet. During an attack, every flood request forces an origin response — egress volume spikes with no warning or cap. Normal traffic generates constant per-GB charges on all origin responses.	**Bandwidth Alliance discounted peering** — Azure→Cloudflare traffic travels over private PNI links, not paid transit, reducing the per-GB egress rate. On top of this, Cloudflare CDN caches content at the edge — Azure origin only responds to cache misses, delivering an average **60% reduction in Azure bandwidth consumption**.
Azure DDoS Protection	Substantial monthly base charge + per-protected-resource fees. Without it, Azure provides only basic best-effort mitigation — insufficient for a sustained application-layer attack.	Eliminated. Cloudflare's always-on, unmetered DDoS protection is included in Enterprise — no base charge, no per-resource fees, no caps on attack size or duration.
NSG Management	NSGs must maintain and refresh Cloudflare IP allowlists to lock down the AppGW — operational overhead every time Cloudflare's IP ranges change.	With Tunnel active, NSG rule is: deny all inbound from internet. No allowlist. No maintenance. IP range changes are irrelevant — the Tunnel handles all connectivity.

Why Cloudflare Resolves Every Gap

CONCERN	AZURE APPGW WAF	CLOUDFLARE ENTERPRISE
WAF Rule Quality	OWASP CRS v2.x only. No proprietary intelligence. No ML scoring.	Cloudflare Managed Ruleset (proprietary) + OWASP CRS v3.x + ML-based WAF Attack Score.
ASN Blocking	Not available. Requires external scripting to block IP ranges.	Native ASN blocking via IP Access Rules or Custom Rules. Compound expressions supported.
Challenges / CAPTCHA	Only available via Azure Front Door integration. Traditional CAPTCHA.	Managed Challenge (non-interactive) on any rule. Under Attack Mode. Turnstile. No Front Door equivalent needed.
Global Policy	Per-site WAF policies. No cross-site propagation without scripting.	Account-level WAF: custom rulesets, rate limiting, managed rulesets deployed globally from one place.
Active DDoS Response	No automatic mitigation. Manual rule updates required during attack.	Always-on autonomous mitigation. ~3s to act. Adaptive DDoS learns your traffic baseline for sophisticated attacks.

Cloudflare Enterprise — Addresses all five concerns out of the box. No supplementary products required.