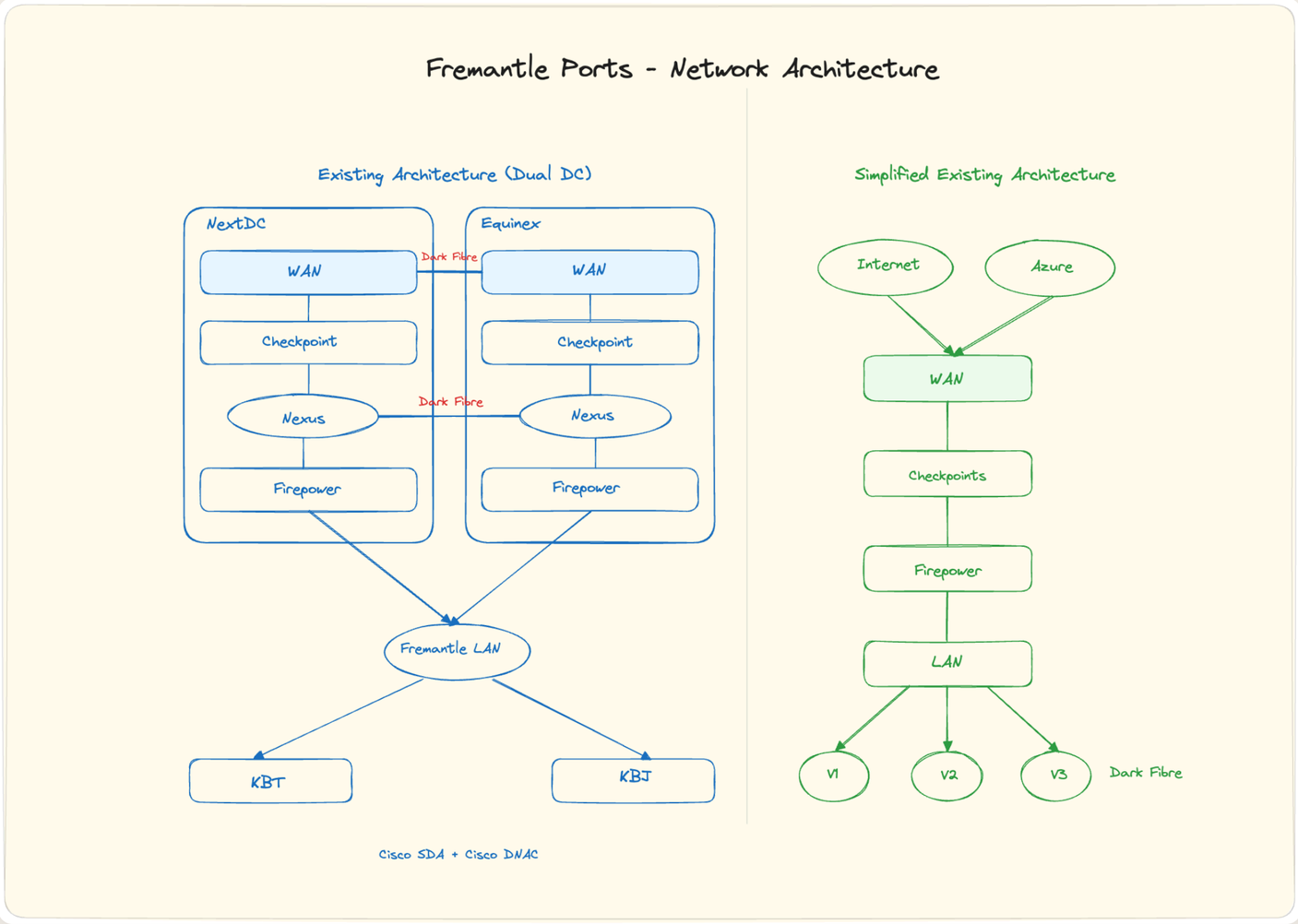
Fremantle Ports & Cloudflare

Network Security & Cloud Transformation Roadmap

Jason Clarke — Senior Solutions Engineer

April 2026 · Confidential

Current Infrastructure



Existing Cloudflare Usage

CDN freemanports.com.au — 20 TB/month

WAF App Security Advanced + Core (live)

DDoS Advanced DDoS — 20 TB global cap

Traffic Snapshot March 2026

45.4M

monthly requests on freemanports.com.au

42M of those are **automated bots**

= 92% of all traffic is non-human

Renewal

Expires **29 May 2026** · Quote Q-597277

Reseller: Datacom · Distributor: Dicker Data

Drivers for Change

🔒 Security Gaps

- 92% of web traffic is bots — no dedicated bot product
- API endpoints visible but unprotected
- Email relies solely on Microsoft Defender
- TCP/UDP port apps have no DDoS coverage

☁️ Cloud Migration

- Applications moving to Microsoft Azure
- Need secure, scalable cloud connectivity
- VPN complexity for remote workers
- Azure egress fees from current architecture

💰 Cost & Complexity

- Checkpoint firewall renewal approaching
- Dual DC Cisco hardware maintenance costs
- Multiple point security products to manage
- Opportunity to consolidate under Cloudflare

🏗️ Architecture Modernisation

- Replace on-prem firewall with CF Tunnel for cloud apps
- Move from VPN to Zero Trust ZTNA
- Simplify egress from Azure workloads

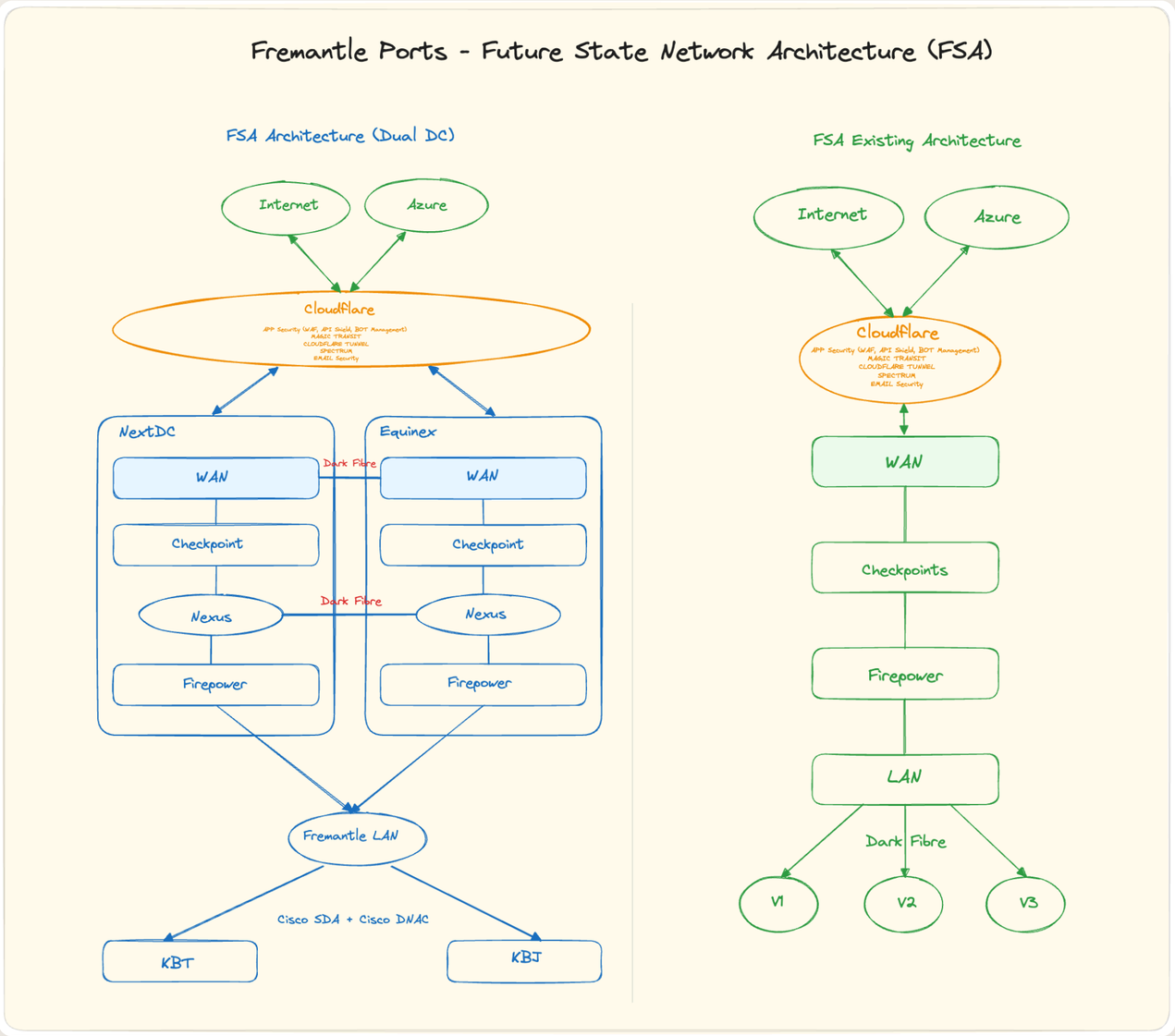
🚢 Critical Infrastructure Risk

- Fremantle Ports is critical national infrastructure
- OT & port systems need L3/L4 protection
- High-value target — regulatory obligations

Future State Architecture

How Cloudflare transforms the Fremantle Ports security posture

Future State — Architecture Overview



Zero Trust Posture

Verify every user and device. Identity-aware policies replace implicit network trust.

DDoS at Every Layer

L3/L4 via Spectrum, L7 via WAF. 321 Tbps capacity absorbs attacks at the edge.

API-First Security

Positive security model blocks schema violations at edge. Already activated free.

Bot Intelligence

ML scoring on every request. 42M monthly bots managed without affecting real users.

Email Protection

Phishing, BEC and malware stopped before M365. Retroactive post-delivery remediation.

Origin Concealment

Azure and port system IPs never exposed. Attack surface reduced to Cloudflare's network.

Future State — Business Benefits

$ Cost Reduction

- Checkpoint firewall licensing eliminated for cloud apps
- Reduced Azure egress costs via Tunnel optimisation
- Single vendor consolidation across 6 security domains
- Renewal pricing with expanded BoM discounts

Operational Efficiency

- Zero Trust replaces complex VPN for remote access
- Single Cloudflare dashboard across all security products
- API Shield auto-discovers endpoints — no manual config
- Bot rules reduce helpdesk noise from fake traffic

Cloud Enablement

- Azure migration secured end-to-end via CF Tunnel
- No public IPs required on any Azure server
- On-prem infra unchanged — zero forklift migration
- Works across multi-cloud and hybrid environments

Business Resilience

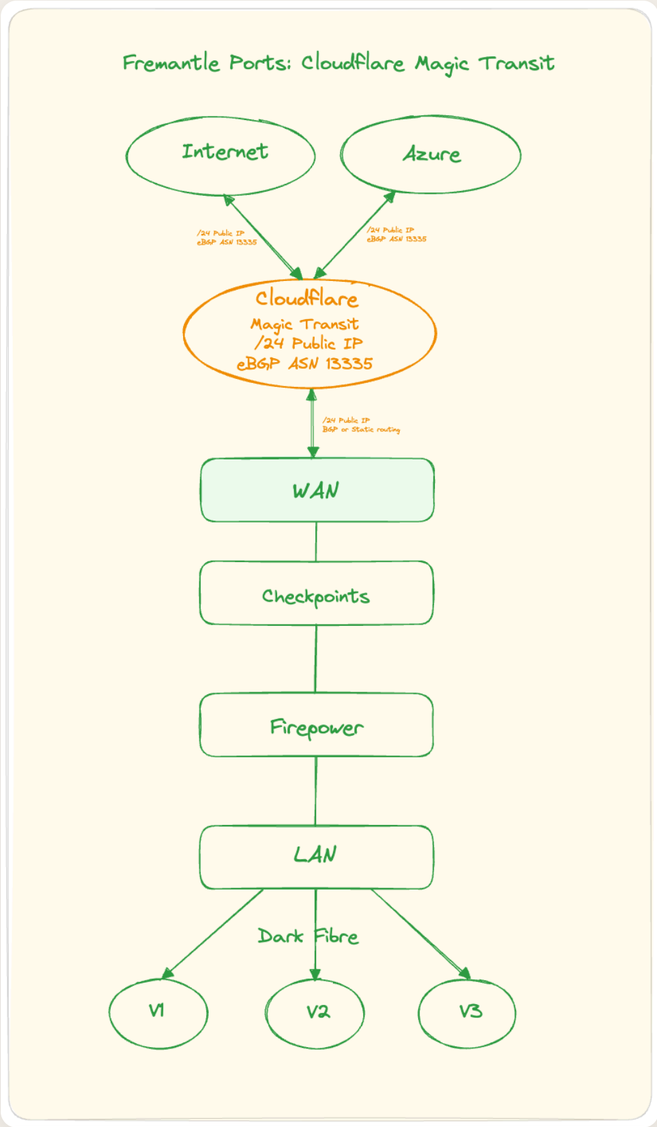
- Port operations protected from DDoS disruption
- Email phishing stopped before reaching staff inboxes
- BEC financial fraud protection for high-value transactions
- Continuous uptime for critical port systems

CLOUDFLARE

Magic Transit

Network-level DDoS protection for Fremantle Ports IP infrastructure

Magic Transit — Architecture & Benefits



Network-Level DDoS Protection

L3/L4 mitigation for the entire Fremantle IP prefix — volumetric attacks absorbed at Cloudflare's edge before ever reaching the network.

BGP Prefix Advertisement

Cloudflare announces Fremantle's IP ranges via anycast. Traffic is automatically routed to the nearest CF point of presence globally.

321 Tbps Absorption Capacity

The world's largest DDoS mitigation network. Even the largest volumetric attacks are absorbed without impacting port operations.

No Infrastructure Changes

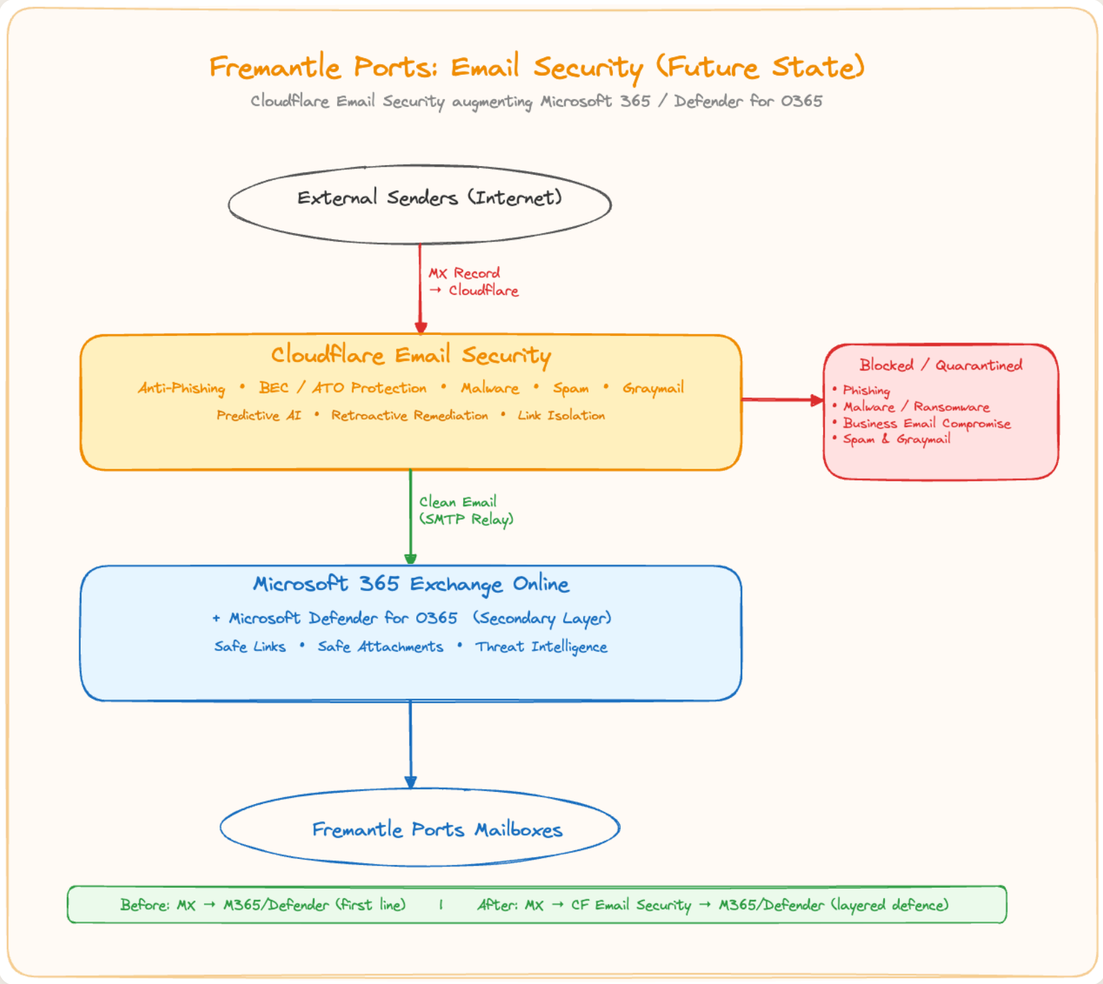
Works alongside existing NextDC and Inland Feunix infrastructure. Clean traffic returned to Fremantle via GRE tunnel or CNI.

Email Security

Cloudflare Email Security augmenting Microsoft 365

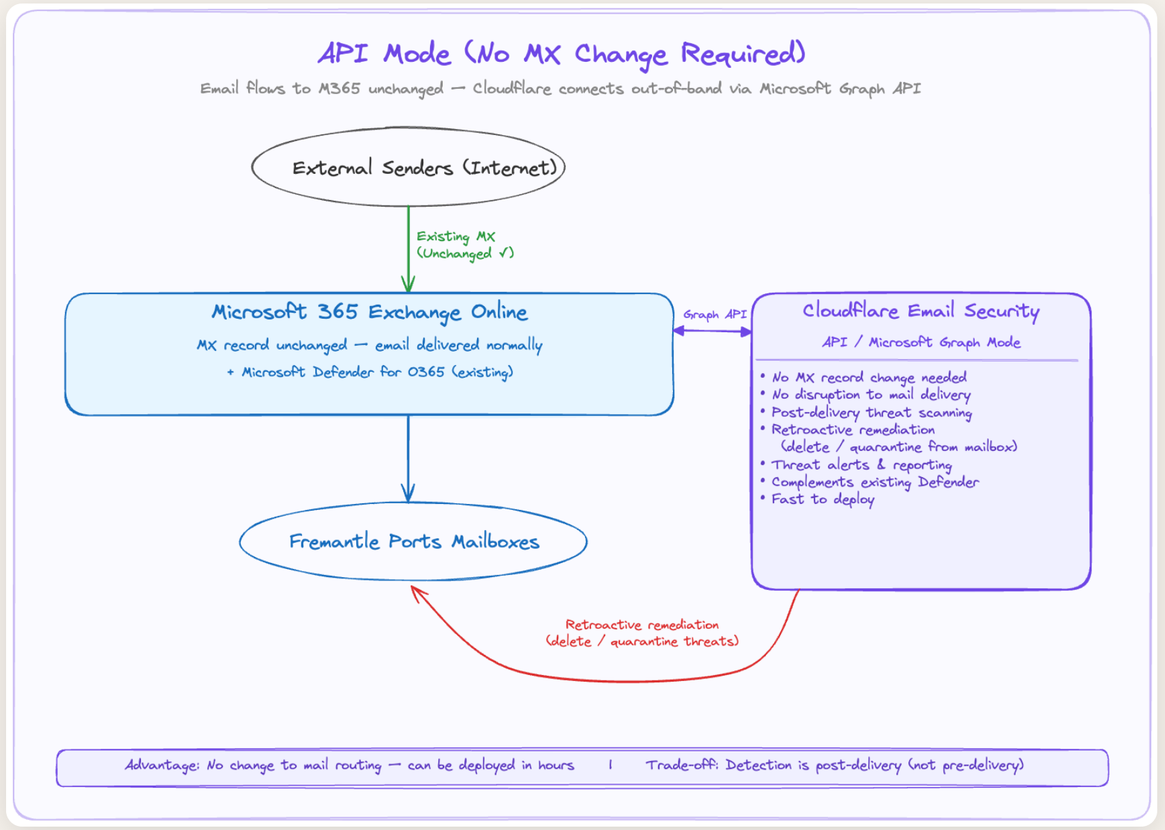
Email Security — Two Deployment Options

OPTION 1 — INLINE (MX CHANGE REQUIRED)



Pre-delivery blocking — threats never enter M365

OPTION 2 — API MODE (NO MX CHANGE)



Zero disruption — deploy in hours via Microsoft Graph API

Email Security — Technical Capabilities

Threat Detection Engine

- Predictive AI trained on billions of emails globally
- Phishing — payload, link & display-name analysis
- Business Email Compromise (BEC) detection
- Malware & ransomware attachment scanning
- Graymail categorisation & filtering

API Mode — Microsoft Graph

- Native M365 integration — no agent required
- Retroactive remediation from delivered mailboxes
- Auto-move / delete malicious emails post-delivery
- Works alongside existing Defender rules

Link & Attachment Protection

- URL rewriting & time-of-click scanning
- Malicious link isolation in CF Browser
- Sandboxed attachment detonation
- QR code phishing detection

Deployment Flexibility

- API mode: live in hours with no MX change
- Inline mode: full pre-delivery blocking
- Both complement — not replace — existing Defender
- Full audit trail and admin dashboard

Email Security — Business Value for Fremantle Ports

92%
of payload-based phishing attacks blocked by Cloudflare

<24h
to deploy via API mode with zero change management

$0
disruption to mail delivery with API mode deployment

Why Fremantle Ports Is a Target

Fremantle Ports handles high-value cargo movements, vessel scheduling, and government reporting — all prime BEC targets. A single phishing compromise can trigger wire fraud, regulatory breach, or operational disruption.

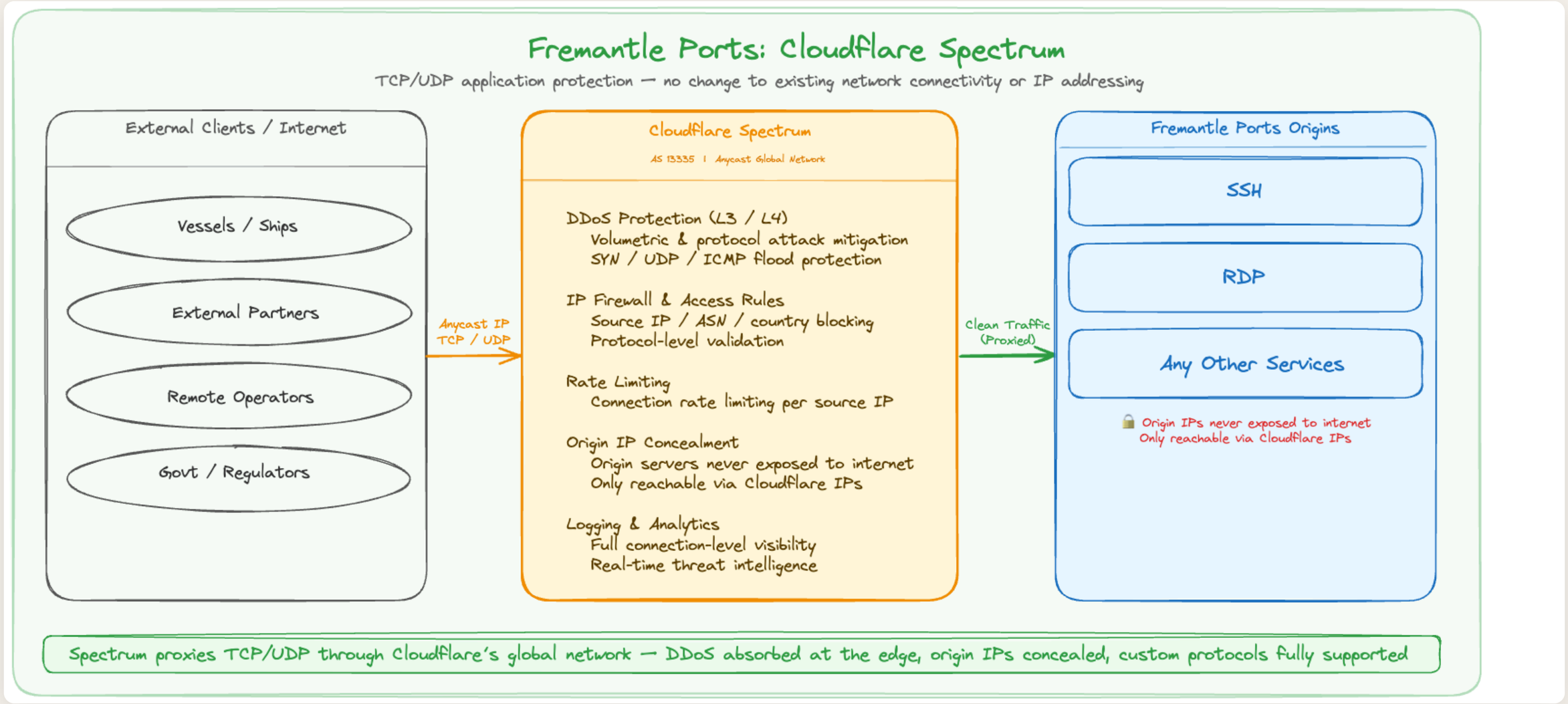
Recommended Approach

Start with **API mode** — immediate visibility, no disruption. Analyse threat data for 30 days, then evaluate inline mode for full pre-delivery protection. Complements and strengthens the existing Microsoft Defender investment.

Cloudflare Spectrum

TCP/UDP application protection for port operations systems

Spectrum — Architecture



Spectrum — Technical Capabilities

DDoS Protection (L3/L4)

- Volumetric attack mitigation (up to 321 Tbps capacity)
- SYN, UDP, ICMP flood protection
- TCP amplification attack blocking
- Always-on — no manual activation required

IP Firewall & Access Rules

- Block by source IP, ASN, or country
- Allow only known partners and systems
- Protocol-level validation
- Custom allow/block lists

Origin IP Concealment

- Fremantle origin IPs never exposed to internet
- Attackers can only reach Cloudflare IPs
- Dramatically reduces the attack surface
- Works for any TCP/UDP service on any port

Rate Limiting & Logging

- Connection rate limiting per source IP
- Burst protection for operational systems
- Full connection-level logs to SIEM
- Real-time attack telemetry dashboard

Spectrum — Business Value for Fremantle Ports

321Tbps
Cloudflare network capacity
to absorb DDoS attacks

100%
origin IP concealment
for PSL, R2S & RASA

Any
TCP/UDP protocol
no HTTP requirement

Why Fremantle Ports Needs This

Port management systems (PSL, R2S, RASA) operate on custom TCP/UDP protocols not covered by traditional web WAFs. A DDoS attack on these systems could halt vessel scheduling, cargo tracking, or regulatory reporting — with direct financial and operational impact.

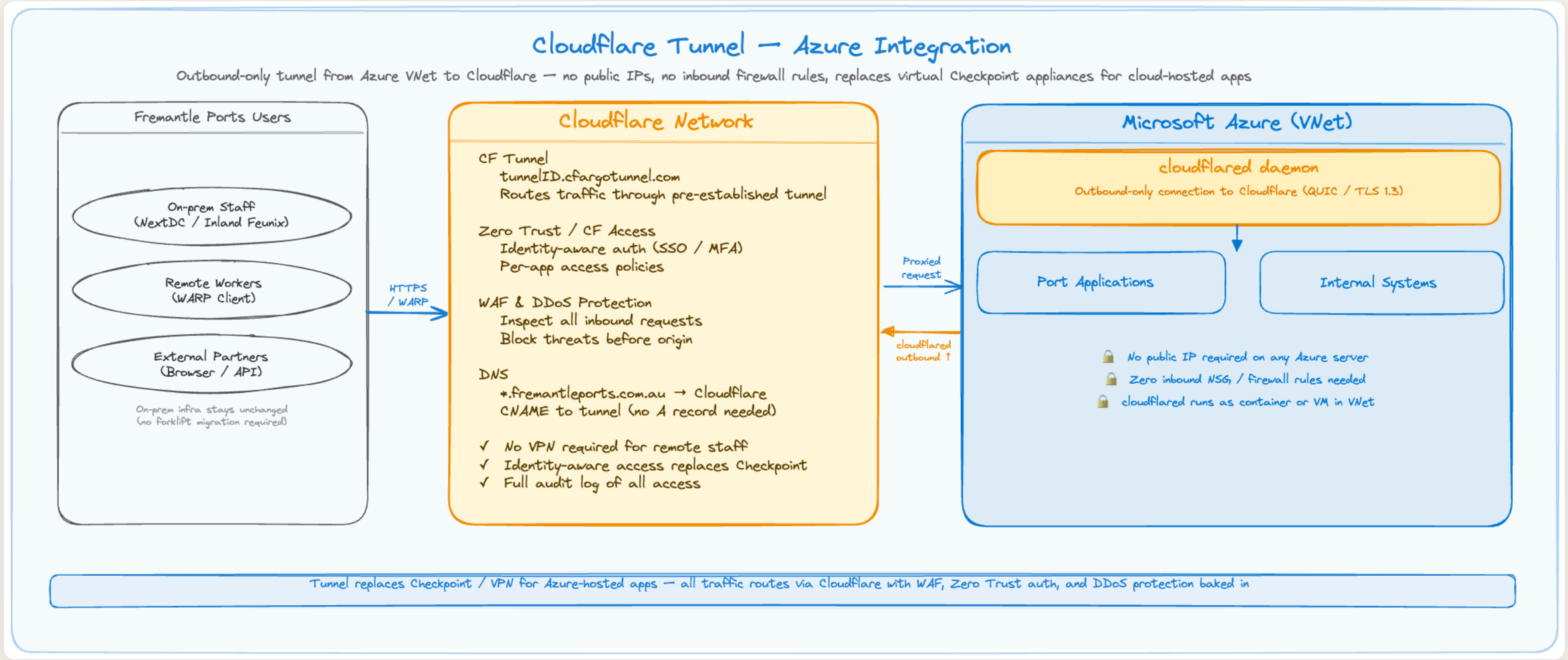
Critical Infrastructure Protection

As critical national infrastructure, Fremantle Ports is a high-value target. Spectrum provides DDoS resilience and IP concealment with no changes to existing server configurations — protecting core port systems while maintaining full operational continuity.

Cloudflare Tunnel

Secure Azure connectivity — no public IPs, no inbound firewall rules

Cloudflare Tunnel — Architecture



Cloudflare Tunnel — Technical Capabilities

Outbound-Only Tunnel

- cloudflared runs in Azure as container or VM
- Establishes persistent outbound QUIC/TLS 1.3 connection
- CF routes inbound requests through established tunnel
- No public IP or inbound port ever required

Zero Trust / CF Access

- SSO + MFA enforced per application
- Device posture checks (managed devices only)
- Per-app access policies — not network-wide
- Full audit log of every access request

WARP Client (Remote Workers)

- Lightweight client replaces traditional VPN
- Private apps accessed without exposing IPs
- Split tunnelling: internet vs private traffic
- Works on any device, any network

WAF & DNS in the Path

- All tunnel traffic inspected by Cloudflare WAF
- DNS filtering via CF Gateway for users
- DDoS protection on all tunnelled applications
- TLS inspection available for full visibility

Cloudflare Tunnel — Business Value for Fremantle Ports

Zero
public IPs required
on any Azure server

Zero
inbound NSG / firewall
rules to manage in Azure

↓ Cost
Checkpoint VPN eliminated
for all Azure-hosted apps

Enables the Azure Migration

As Fremantle Ports migrates applications to Azure, Cloudflare Tunnel provides the secure connectivity layer — without public IPs, complex firewall rules, or expensive dedicated circuits. On-prem infrastructure continues working unchanged during migration.

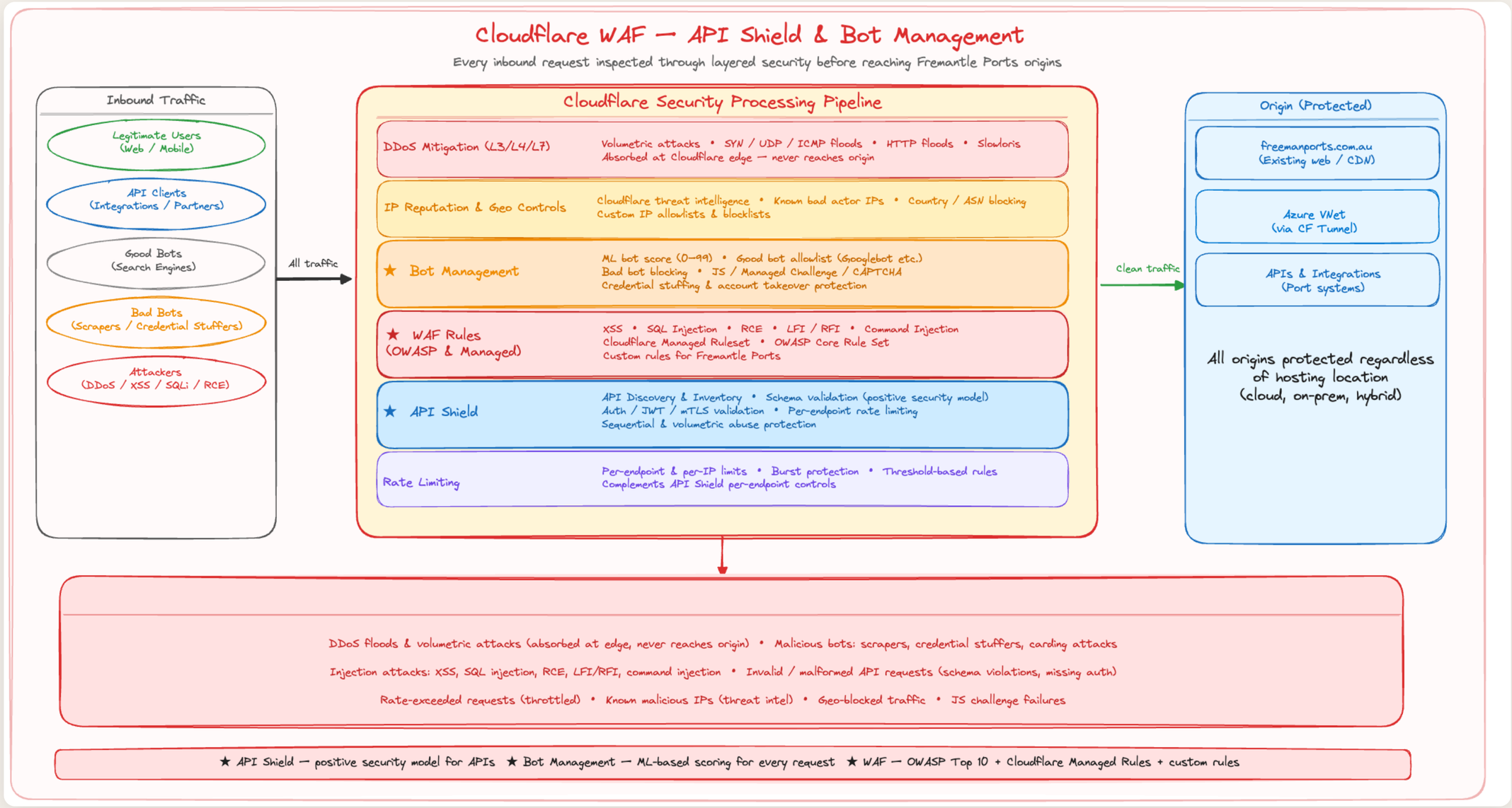
Secure Remote Access Without VPN

Port staff working remotely connect through WARP to access Azure applications securely — no VPN client, no split tunnelling headaches, no hardware to manage. Identity-aware policies ensure only the right people reach the right systems.

WAF · API Shield · Bot Management

Layered application security — already protecting freemanports.com.au

WAF — Security Processing Pipeline



WAF — Technical Capabilities

OWASP & Managed Rulesets

- Cloudflare Managed Ruleset (updated continuously)
- OWASP Core Rule Set — Top 10 full coverage
- XSS, SQL injection, RCE, LFI/RFI protection
- Custom rules tailored for Fremantle traffic patterns

Custom Rules & Transform Rules

- Wildcard and regex-based custom rule engine
- Header and URL rewrite via Transform Rules
- Page Shield detects JavaScript supply chain attacks
- Security Events dashboard — full attack history

L7 DDoS Protection

- HTTP flood mitigation at Cloudflare edge
- Slowloris and slow POST attack blocking
- Challenge-based mitigation (JS / Managed / CAPTCHA)
- Zero impact to legitimate user traffic

Already Live at Fremantle Ports

- App Security Advanced & Core — already active
- Advanced DDoS — 20 TB global cap in current contract
- Opportunity: tune rules using the March traffic data
- API Shield activated — endpoint inventory ready to review

API Shield — Deep Dive

API Discovery Already Active

- Auto-discovers all API endpoints from live traffic
- Surfaces undocumented & shadow APIs instantly
- Classifies by method, path, content type, and auth
- **Already enabled on freemanports.com.au**

Auth & JWT Validation

- Validate JWT tokens at Cloudflare edge (not origin)
- Block requests with expired or invalid tokens
- mTLS support for machine-to-machine API calls
- Leaked credential detection for ATO prevention

Schema Validation (Positive Security)

- Upload OpenAPI schema — CF enforces it at edge
- Any request deviating from schema is blocked
- Prevents injection attacks via API parameters
- No changes required to origin application code

> *"API traffic identification was raised as a high priority by the Fremantle cyber team. API Shield is already activated — the endpoint data is ready to review together."*
>
> Ian Hogben, Account Manager — 17 April 2026

Bot Management — Deep Dive

The Fremantle Ports Bot Problem

42M of 45.4M monthly requests are bots

= **92% of all traffic** is non-human. Consuming origin resources, skewing analytics, and creating credential stuffing and scraping risk with no dedicated bot product in place today.

How Bot Management Works

- ML bot score (0–99) assigned to every request
- Good bots (Googlebot etc.) automatically allowlisted
- Bad bots: blocked, challenged, or rate-limited
- JS Challenge / Managed Challenge / CAPTCHA options
- Leaked credential detection — stops account takeover

Protect Origin Performance

Eliminate junk traffic load. Reduce origin infrastructure costs and improve real-user page speed significantly.

Accurate Analytics

With bots filtered, analytics reflect real human traffic — enabling better data-driven decisions for the business.

Stop Account Takeover

Credential stuffing uses leaked passwords. Bot Management + Leaked Credentials detection stops ATO before it succeeds.

Summary — Cloudflare for Fremantle Ports

Email Security

Stops phishing, BEC, and malware before they reach staff inboxes — augments Microsoft Defender with no disruption to mail flow via API mode.

Spectrum

L3/L4 DDoS protection and origin IP concealment for port operations systems (PSL, R2S, RASA) running on custom TCP/UDP protocols.

Cloudflare Tunnel

Secure connectivity to Azure-hosted apps with no public IPs or inbound firewall rules. Replaces Checkpoint VPN and enables Zero Trust remote access.

WAF + API Shield

OWASP Top 10 protection plus a positive security model for APIs. Already active — endpoint discovery data is ready to tune with the cyber team.

Bot Management

ML-based scoring eliminates the 42M monthly bot requests consuming origin resources, skewing analytics, and creating credential stuffing risk.

Magic Transit

Network-level DDoS protection for Fremantle's entire IP prefix. Announces BGP routes via Cloudflare — volumetric attacks absorbed at the edge before reaching the network.

Jason Clarke · jclarke@cloudflare.com · +61 413 290 245

Ian Hogben · ihogben@cloudflare.com · +61 467 975 757