

Cato Networks — Overview and Design

Overview

Item	Value
System	Cato Networks SASE (cloud PoPs; PBR uses IPsec sites, no Cato Sockets)
Owner	Mitch Fraser, IT Manager
Status	Active — site onboarding in progress (Oct 2026)
Cato ASN	64515
PBR site ASN	6500<site number> (e.g. Belgrave 65001, Kilvington 65008, Gembrook 65006)
Melbourne PoP (primary)	113.30.140.95
Sydney PoP (secondary)	202.75.244.10
Cato account IPsec IP licences	3 allocated, 0 free (limits per-path PoP addresses — see EdgeRouter standard)
Related pages	EdgeRouter Site Build Standard; per-site pages in this book

Cato Networks is PBR's SASE platform. It provides secure web / CASB and application control (including the AI application controls), Cato AI Security, ZTNA via the Cato Client (replacing the legacy VPN), and site connectivity. Cato is an **overlay** on top of the existing Palo Alto PA-440 hub-and-spoke network: it does not replace the site edge, and OSPF remains the internal source of truth for inter-site routing. Sites connect to the Cato cloud by IPsec IKEv2 tunnels — from the PA-440s at the hub/major sites and from Ubiquiti EdgeRouters at the smaller sites — with BGP presenting each site's own prefixes to Cato and learning the Cato-side ranges back.

Organisational context

PBR is a Victorian heritage railway with roughly 175 users across 8 sites in the Dandenong Ranges. Compliance drivers for the Cato work are the Essential Eight, VPDSS and the VG-CISO framework. Cato sits alongside Palo Alto PA-440 firewalls (onboarding to Strata Cloud Manager), ThreatLocker, Action1, Intune, Duo MFA, Huntress MDR and SCEPman PKI.

Licensing model

The licence is site-unlimited but **bandwidth-pooled**: no cap on sites, but every site tunnel and every Cato Client draws from one shared pool. This drives the design rule that on-site ZTNA clients must not hairpin through the site tunnel (PA-440 PBF rule, below), and that IPsec tunnels should carry only what needs to reach Cato.

Network integration design

Topology

- Kilvington Drive (KL1) is the OSPF hub with an Aruba 6300M VSX core. PA-440s at each major site; EdgeRouters at the small sites. Inter-site transport is Palo Alto / EdgeOS IPsec VTIs carrying OSPF (area 0 = 10.254.0.0/16 transit, one area per site).
- Each Cato-connected site builds its own IPsec IKEv2 tunnels to the Melbourne (primary) and Sydney (secondary) PoPs. Route-based (VTI) only.
- Addressing seen by Cato is the new 10.<site>.<vlan>.0/24 scheme plus any legacy ranges still in use at that site.

Routing boundary: BGP to Cato alongside internal OSPF

- Each site advertises **only its own connected prefixes** to Cato (export policy). Secondary-role tunnels prepend the site ASN twice so Cato prefers the primary.
- Each site **imports only** 10.41.0.0/16 (Cato / ZTNA client ranges) and 10.254.254.0/24 from Cato. Everything else Cato offers (about 127 prefixes including all other PBR sites) is dropped by the import allowlist. This guarantees Cato is never preferred for any internal route — OSPF over the hub VTIs stays the only inter-site path.
- Second guard on EdgeOS: BGP administrative distance is raised to 115 (above OSPF's 110), so even an accidental import loss would not beat OSPF.

- Redistribution is one-way per site (connected → BGP). Nothing is redistributed from BGP into OSPF today; see the Emerald note on the site pages for the proposed exception (KL1/KT1 redistributing 10.41.0.0/16 into OSPF so non-Cato sites can reach ZTNA clients).

Fleet schema (confirmed from the KL1 PA-440 build)

Element	Convention
Tunnel interface	Site's own number: vti<site>00 primary, vti<site>01 secondary (PA: tunnel.<site>00-03)
Tunnel /31	10.254.<site>.<site>0/31, .<site>2/31 (then .<site>4, .<site>6) — site side even, Cato side odd
Example (KL1, site 8)	tunnel.800-803 on 10.254.8.80 / .82 / .84 / .86
Example (Gembrook, site 6)	vti600 10.254.6.60/31 (Cato .61), vti601 10.254.6.62/31 (Cato .63)
Authentication identifier	Cato-generated FQDN <catoSiteId>.23991.catonetworks.com (WAN2 role: <catoSiteId>.23991.2.catonetworks.com)
Crypto	IKEv2, AES-CBC-256 / SHA-256 / PRF SHA-256 / DH14; ESP AES-CBC-256 / SHA-256, PFS DH14
BGP timers	Keepalive 30 / Hold 90
Import allowlist	10.41.0.0/16 le 24, 10.254.254.0/24 le 32

Site status (26 Oct 2026)

Site	Device	Site#	ASN	Paths	Status
Kilvington (hub)	KL1 PA-440	8	65008	NBN + Starlink, 4 tunnels	Active (reference build)
Belgrave	B1 PA-440	1	65001	—	Active — export policy over-advertises; tighten to own prefixes
Gembrook	PBR-R-G1 EdgeRouter PoE-5	6	65006	NBN (single)	Active — fleet standard
Cockatoo	PBR-R-CK1 EdgeRouter PoE-5	5	65005	Optus LTE (single)	Active — fleet standard

Site	Device	Site#	ASN	Paths	Status
Gembrook West	PBR-R-GW1 EdgeRouter 12	7	65007	PTP via KT1 (primary) + LTE (secondary)	Active
Mater Christi	PBR-R-BS1 EdgeRouter 12	10	65010	airFiber PTP via Belgrave (primary) + LTE (secondary)	Tunnels up; BGP/NTP to confirm
Emerald	PBR-R-E1 EdgeRouter Pro 8	3	65003	—	Deferred — reach via KL1/KT1 hubs

ZTNA (Cato Client) replacing the VPN

- Cato Client becomes the single remote-access path once cutover is complete; identity from M365 / Entra ID, Duo MFA already in place.
- Access rules are user/group based, mapped onto the SCM zone model (Z-CORP, Z-SERVERS, Z-VOIP, Z-SECOT, Z-GUEST, Z-RADIO) — OT and radio segments excluded from general remote access.
- On-site clients must bypass the site tunnel: a Policy-Based Forwarding rule on the PA-440s sends on-site client traffic to the Cato PoPs out the local internet link rather than into the IPsec tunnel, protecting the bandwidth pool. (Match criteria and failover monitor still to be finalised and documented.)

AI governance through Cato

- Cato AI Security consumes Claude Enterprise inference-hook / Compliance API telemetry; regular Claude chat is visible, Cowork sessions are not (known gap, open governance item).
 - Tenant restriction: Application Control header injection on the Claude domains to allow only PBR's Claude Enterprise organisation, same pattern as M365 tenant restrictions. Header details, org ID and enforce/monitor mode still to be recorded here.
 - Supports the AI governance policy (PBRB PO 082), the CEO approval paper and the VPDSS third-party tool assessment process.
-

Open items

1. Mater Christi: confirm BGP Established on both neighbours and expected routes; fix NTP (clock a month behind); commit-confirm and save.
2. Gembrook: quiet-window reboot test (cold start + drop-in persistence); remove verbose `vpn ipsec logging`; confirm temporary firewall rule 5 is gone; save.
3. Cockatoo: set real Optus LTE last-mile speeds on the Cato site page.
4. Emerald via hubs: add Emerald prefixes to the KL1 (primary) and KT1 (backup) Cato export policies; provide a return path for 10.41.0.0/16 from Emerald (preferred: KL1/KT1 redistribute 10.41.0.0/16 and 10.254.254.0/24 from BGP into OSPF).
5. Belgrave: tighten Cato export policy to its own prefixes (currently exports far more).
6. Optional Cato support ticket: backend setting so Cato narrows rather than rejects multiple traffic selectors (would make the EdgeOS drop-in unnecessary).
7. PA-440 PBF rule for on-site ZTNA clients: finalise, test, document.
8. Claude tenant-restriction rule: record header/org details and mode; resolve or formally accept the Cowork visibility gap.
9. NetBox: record Cato VTIs, /31s and client ranges. Housekeeping: loopback/area numbering mismatches (Gembrook lo 10.100.7.1 vs site 6, Cockatoo lo 10.100.6.1 vs site 5, Gembrook West area 12), BS1 orphaned `eth1local` ruleset, CK1 stale static default.

Maintenance notes

Update the site status table whenever a site is added or changed, and keep the per-site pages as the authoritative configuration record. When Cato support changes anything on the backend (multi-TS handling, PoP addresses, IP licences), update the EdgeRouter Site Build Standard page.

Revision #1

Created 2026-10-26 07:26:08 UTC by PBR_Documentation

Updated 2026-10-26 07:26:08 UTC by PBR_Documentation