

Cato Networks

Cato Networks SASE at PBR: design, EdgeRouter IPsec/BGP site build standard, per-site builds, ZTNA and AI governance.

- [Cato Networks — Overview and Design](#)
- [EdgeRouter Site Build Standard \(IPsec IKEv2 + BGP to Cato\)](#)
- [Site: Gembrook \(PBR-R-G1\)](#)
- [Site: Cockatoo \(PBR-R-CK1\)](#)
- [Site: Gembrook West \(PBR-R-GW1\)](#)
- [Site: Mater Christi \(PBR-R-BS1\)](#)
- [Site: Emerald \(PBR-R-E1\) — deferred, via hubs](#)

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.

EdgeRouter Site Build Standard (IPsec IKEv2 + BGP to Cato)

Overview

Item	Value
Applies to	Ubiquiti EdgeRouter sites (EdgeOS 3.0.1): Gembrook, Cockatoo, Gembrook West, Mater Christi (Emerald deferred)
Design	Route-based IPsec IKEv2 VTIs to Cato Melbourne (primary) and Sydney (secondary) PoPs, eBGP to Cato ASN 64515
Status	Settled 26 Oct 2026 — fleet standard, proven at four sites
Owner	Mitch Fraser

This page is the build standard for connecting an EdgeRouter site to Cato. It records the settled design, the one-time strongSwan change the EdgeRouters need, the EdgeOS configuration template, the two-WAN-path variant, verification and recovery, and — because it cost a site outage — what **not** to do. Per-site values live on the site pages in this book.

Fleet standard (summary)

Cato side (site IPsec page)

- Site type IPsec IKEv2. Connection type **Responder Only** (the ER initiates). Destination type IPv4 (Melbourne 113.30.140.95 primary, Sydney 202.75.244.10 secondary).
- Authentication identifier = the **Cato-generated FQDN** shown on the site's IPsec page, `<catoSiteId>.23991.catonetworks.com`, on both tunnel rows. For a two-path site the WAN2 row uses `<catoSiteId>.23991.2.catonetworks.com`. (IPv4 = site WAN IP also works and is

mandatory if Bidirectional is ever used.)

- Init message parameters set explicitly: AES-CBC-256 / SHA-256 / PRF SHA-256 / DH14. Auth parameters AES-CBC-256 / SHA-256 / DH14. (Only matter for Bidirectional, harmless otherwise. "Automatic" makes the ER answer NO_PROPOSAL_CHOSEN.)
- Private IPs per the schema (site even / Cato odd). One BGP neighbour per tunnel: Cato ASN 64515, Peer ASN 6500<site>, Hold 90 / Keepalive 30, Advertise All routes.
- Last-mile bandwidth set to the real plan speeds; a fresh PSK per tunnel. Never paste a PSK into chat or a ticket — treat it as burned and regenerate.

EdgeOS side

- One-time drop-in `/etc/strongswan.d/zz-pbr-cato.conf` with `charon { ignore_acquire_ts = yes }` (see root cause). Survives reboot, **not firmware upgrade**.
 - Standard route-based VTI peers keyed by PoP IP, `connection-type initiate`, `authentication id @<fqdn>` (the `@` forces an FQDN identity), `remote-id <PoP IP>`, `ikev2-reauth no`.
 - VTIs `vti<site>00` / `vti<site>01`, /31 addresses, MTU 1400, OSPF passive, MSS clamp 1350 on vti.
 - BGP: export only the site's own prefixes (secondary prepends ASN twice), import allowlist 10.41.0.0/16 le 24 + 10.254.254.0/24 le 32 with local-pref 200 (primary) / 100 (secondary), administrative distance 115, keepalive 30 / hold 90, soft-reconfiguration inbound.
-

Root cause: why ER-initiated tunnels would not re-establish on their own (proven 26 Oct 2026)

Symptom: a manual `ipsec up` always worked, but after any drop (or reboot) the tunnels never came back by themselves, with Cato in Responder Only mode. Cato logged nothing useful; the ER log showed Cato replying `N(TS_UNACCEPT)` to `IKE_AUTH`.

- EdgeOS writes VTI peers to strongSwan as `auto=route` (a trap policy). Every automatic attempt is therefore *acquire-triggered* — by the BGP SYN or the UDP 10001 discovery broadcast heading into the VTI.
- strongSwan prepends the triggering packet's selector to the traffic selectors of an acquire-triggered initiation, after the log line "proposing traffic selectors" (so the log misleadingly shows only 0.0.0.0/0). On the wire the automatic `IKE_AUTH` was 416 bytes versus 384 for

a manual one: two extra 16-byte selectors, e.g. [10.254.6.60/32 tcp, 0.0.0.0/0] ↔ [10.254.6.61/32 tcp/179, 0.0.0.0/0]. This is the documented `charon.ignore_acquire_ts` behaviour (default no; pfSense ships it as yes).

- Cato's responder does not narrow per RFC 7296 §2.9 — it rejects any proposal carrying multiple traffic selectors. Cato KB "IPsec Tunnel Fails to Establish with TS_UNACCEPTABLE When Meraki VPN Health Check Is Enabled" states Cato "rejects the SA with a TS_UNACCEPTABLE notification when it receives multiple Traffic Selectors" and that Support can "apply a backend configuration". Cato's best practice note recommends "Initiate connection by Cato" for IKEv2 sites for this reason.
- **Confirmed by Cato Support (ticket reply 27 Oct 2026, Jerome Manalo):** their review of the Gembrook primary-tunnel capture found the failed proposals carried TSi 10.254.6.60/32 (TCP flow) + 0.0.0.0/0 and TSr 10.254.6.61/32 tcp/179 + 0.0.0.0/0, "two entries within each traffic-selector payload, which Cato rejects with TS_UNACCEPTABLE"; Cato expects exactly one 0.0.0.0/0 pair per tunnel. The 05:30:05 UTC success they cite is the first unattended re-establish after the drop-in.
- Why the PA-440s never hit this: PAN-OS proposes only its configured proxy-ID (0/0 ↔ 0/0).
- Eliminated by test: stale Cato state, simultaneous dual-PoP negotiation, crypto/DH choice, firewall/NAT, BGP configuration. The Cato per-site option "IKEv2 Send Single TS per payload" was tested and does not help — it governs how Cato encodes its own Network Ranges, not what it accepts.
- Fix: the `ignore_acquire_ts = yes` drop-in makes every ER attempt look exactly like a manual `ipsec up`. Proven at Gembrook 16:26: after `ipsec down`, the ER's own trap-triggered attempt sent a single-selector IKE_AUTH and established in about 1 second with Cato unable to initiate; both BGP neighbours returned unattended.

Alternative that also works: Bidirectional (fallback only)

Cato site Bidirectional, destination/identifier = the site WAN IPv4 on both rows, Init parameters explicit; ER peers `connection-type respond` with `authentication id <WAN IP>`. Cato then initiates every 60 s while down. EdgeOS still writes auto=route so the ER keeps trying in the background (harmless). Not the standard because Cato cannot initiate through NAT — which rules it out for every PTP/fibre path that NATs through a hub PA-440. Cockatoo was first built this way and has since been moved to the standard.

DO NOT DO: policy-based IPsec on an EdgeRouter (site outage, 26 Oct

2026 ~14:30)

The Cato AI assistant suggested removing `vti bind` and adding `tunnel 1 local prefix 10.6.0.0/16 remote prefix 0.0.0.0/0` on both Cato peers ("Cato requires policy-based"). Committing it took Gembrook offline: the kernel IPsec policy diverted **all** traffic from 10.6.0.0/16 into the Cato tunnel — overriding routing, including inter-site traffic to the hub — and removed the VTIs the BGP sessions ran over. Recovered by rebooting onto the saved config.boot. Cato's own IKEv2 site documentation supports route-based 0/0 tunnels; policy-based is the Meraki-specific KB workaround and does not even fix the multi-TS issue. **Never apply policy-based tunnels on any ER site.**

Build recipe (single-WAN site)

1. Audit the device: `show version`, `show interfaces`, `show ip route`, `show ip ospf neighbor`, `show configuration commands | grep -E 'firewall|nat|vpn|ospf'`. Note the WAN IP, LAN prefixes, loopback, hub VTIs, and that the WAN-local firewall already accepts IKE 500/4500 and ESP from any peer (all PBR ERs do, for the hub tunnels).
2. Create the Cato site (IPsec IKEv2, Responder Only, FQDN identifiers, IPv4 PoP destinations, explicit parameters, private IPs per schema, BGP neighbours, real bandwidth) and generate PSKs.
3. Apply the strongSwan drop-in (below). Hub tunnels bounce for about 2 seconds on `ipsec restart`.
4. Apply the EdgeOS template with the site values. Set the VTI /31 addresses and commit *before* adding the BGP neighbours (the validator rejects a neighbour that is not inside a configured VTI subnet; a /30 typo will do the same).
5. `commit-confirm 10`, verify, `confirm`, `save`.
6. Run the unattended re-establish proof (below). Only after that is the site "done".

EdgeOS template

Replace `<S>` with the site number, `<SITE>` with the site name, `<catoSiteId>` from the Cato page, and the WAN / loopback / legacy-range values from the audit. Quote PSKs.

```
# ---- One-time, outside EdgeOS config (survives reboot, NOT firmware upgrade) ----
sudo tee /etc/strongswan.d/zz-pbr-cato.conf >/dev/null <<'EOF'
# PBR: suppress acquire-derived traffic selectors so trap-triggered IKEv2
# initiations propose only the configured 0.0.0.0/0 (Cato rejects multi-TS).
# Not preserved by EdgeOS firmware upgrade - re-apply after upgrading.
```

```

charon {
    ignore_acquire_ts = yes
}
EOF

sudo ipsec restart      # hub tunnels bounce ~2 s

# ---- EdgeOS configuration (replace <...> values; PSKs in single quotes) ----
configure

# IKE / ESP groups
set vpn ipsec ike-group IKE-CAT0 key-exchange ikev2
set vpn ipsec ike-group IKE-CAT0 ikev2-reauth no
set vpn ipsec ike-group IKE-CAT0 lifetime 19800
set vpn ipsec ike-group IKE-CAT0 proposal 1 dh-group 14
set vpn ipsec ike-group IKE-CAT0 proposal 1 encryption aes256
set vpn ipsec ike-group IKE-CAT0 proposal 1 hash sha256
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection action restart
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection interval 30
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection timeout 30
set vpn ipsec esp-group ESP-CAT0 lifetime 3600
set vpn ipsec esp-group ESP-CAT0 mode tunnel
set vpn ipsec esp-group ESP-CAT0 pfs dh-group14
set vpn ipsec esp-group ESP-CAT0 proposal 1 encryption aes256
set vpn ipsec esp-group ESP-CAT0 proposal 1 hash sha256

# VTIs (site side even, Cato side odd; MUST be /31)
set interfaces vti vti<S>00 address 10.254.<S>.<S>0/31
set interfaces vti vti<S>00 description 'Cato Melbourne (primary)'
set interfaces vti vti<S>00 mtu 1400
set interfaces vti vti<S>01 address 10.254.<S>.<S>2/31
set interfaces vti vti<S>01 description 'Cato Sydney (secondary)'
set interfaces vti vti<S>01 mtu 1400
set protocols ospf passive-interface vti<S>00
set protocols ospf passive-interface vti<S>01
set firewall options mss-clamp interface-type vti
set firewall options mss-clamp mss 1350

# Peers (route-based VTI, ER initiates, FQDN identifier)
set vpn ipsec site-to-site peer 113.30.140.95 authentication mode pre-shared-secret

```

```
set vpn ipsec site-to-site peer 113.30.140.95 authentication pre-shared-secret '<PSK-PRIMARY>'
set vpn ipsec site-to-site peer 113.30.140.95 authentication id
@<catoSiteId>.23991.catonetworks.com
set vpn ipsec site-to-site peer 113.30.140.95 authentication remote-id 113.30.140.95
set vpn ipsec site-to-site peer 113.30.140.95 connection-type initiate
set vpn ipsec site-to-site peer 113.30.140.95 description 'Cato Melbourne PoP'
set vpn ipsec site-to-site peer 113.30.140.95 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 113.30.140.95 local-address <WAN-IP-PRIMARY-PATH>
set vpn ipsec site-to-site peer 113.30.140.95 vti bind vti<S>00
set vpn ipsec site-to-site peer 113.30.140.95 vti esp-group ESP-CAT0

set vpn ipsec site-to-site peer 202.75.244.10 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 202.75.244.10 authentication pre-shared-secret '<PSK-SECONDARY>'
set vpn ipsec site-to-site peer 202.75.244.10 authentication id
@<catoSiteId>.23991.catonetworks.com
set vpn ipsec site-to-site peer 202.75.244.10 authentication remote-id 202.75.244.10
set vpn ipsec site-to-site peer 202.75.244.10 connection-type initiate
set vpn ipsec site-to-site peer 202.75.244.10 description 'Cato Sydney PoP'
set vpn ipsec site-to-site peer 202.75.244.10 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 202.75.244.10 local-address <WAN-IP-SECONDARY-PATH>
set vpn ipsec site-to-site peer 202.75.244.10 vti bind vti<S>01
set vpn ipsec site-to-site peer 202.75.244.10 vti esp-group ESP-CAT0

# Routing policy
set policy prefix-list <SITE>-PREFIXES rule 10 action permit
set policy prefix-list <SITE>-PREFIXES rule 10 prefix 10.<S>.0.0/16
set policy prefix-list <SITE>-PREFIXES rule 10 le 24
set policy prefix-list <SITE>-PREFIXES rule 20 action permit
set policy prefix-list <SITE>-PREFIXES rule 20 prefix <legacy-range>/24
set policy prefix-list <SITE>-PREFIXES rule 90 action permit
set policy prefix-list <SITE>-PREFIXES rule 90 prefix <loopback>/32
set policy prefix-list CAT0-ALLOWED-IN rule 10 action permit
set policy prefix-list CAT0-ALLOWED-IN rule 10 prefix 10.41.0.0/16
set policy prefix-list CAT0-ALLOWED-IN rule 10 le 24
set policy prefix-list CAT0-ALLOWED-IN rule 20 action permit
set policy prefix-list CAT0-ALLOWED-IN rule 20 prefix 10.254.254.0/24
set policy prefix-list CAT0-ALLOWED-IN rule 20 le 32
```

```

set policy route-map CATO-CONNECTED rule 10 action permit
set policy route-map CATO-CONNECTED rule 10 match ip address prefix-list <SITE>-PREFIXES
set policy route-map CATO-OUT-PRI rule 10 action permit
set policy route-map CATO-OUT-PRI rule 10 match ip address prefix-list <SITE>-PREFIXES
set policy route-map CATO-OUT-SEC rule 10 action permit
set policy route-map CATO-OUT-SEC rule 10 match ip address prefix-list <SITE>-PREFIXES
set policy route-map CATO-OUT-SEC rule 10 set as-path-prepend '6500<S> 6500<S>'
set policy route-map CATO-IN-PRI rule 10 action permit
set policy route-map CATO-IN-PRI rule 10 match ip address prefix-list CATO-ALLOWED-IN
set policy route-map CATO-IN-PRI rule 10 set local-preference 200
set policy route-map CATO-IN-SEC rule 10 action permit
set policy route-map CATO-IN-SEC rule 10 match ip address prefix-list CATO-ALLOWED-IN
set policy route-map CATO-IN-SEC rule 10 set local-preference 100

# BGP
set protocols bgp 6500<S> parameters router-id <loopback>
set protocols bgp 6500<S> parameters distance prefix 0.0.0.0/0 distance 115
set protocols bgp 6500<S> redistribute connected route-map CATO-CONNECTED
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>1 remote-as 64515
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>1 description 'Cato Melbourne'
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>1 timers holdtime 90
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>1 timers keepalive 30
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>1 soft-reconfiguration inbound
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>1 route-map import CATO-IN-PRI
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>1 route-map export CATO-OUT-PRI
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 remote-as 64515
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 description 'Cato Sydney'
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 timers holdtime 90
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 timers keepalive 30
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 soft-reconfiguration inbound
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 route-map import CATO-IN-SEC
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 route-map export CATO-OUT-SEC

commit-confirm 10
# ... verify tunnels and BGP, then:
confirm
save

```

Verification

```

export VYATTA_PAGER=cat
show vpn ipsec status
show vpn ipsec sa                                # NOT 'show vpn ipsec state' - that prints live ESP
keys
sudo ipsec statusall | grep -E 'peer-(113|202)'
show vpn log | grep -E 'peer-(113|202)' | grep -E 'initiating|IKE_AUTH response|CHILD_SA .*
established|TS_UNACCEPT|AUTH_FAILED|NO_PROPOSAL'
show ip bgp summary
show ip bgp neighbors 10.254.<S>.<S>1 advertised-routes      # must be ONLY this site's
prefixes
show ip bgp neighbors 10.254.<S>.<S>1 received-routes        # ~127 offered
show ip route bgp                                            # must be ONLY 10.41.0.0/16 +
10.254.254.x at [115/...]
show ip route | grep -E '10\.(1|3|4|5|6|7|8|9|10|11|12)\.'   # inter-site routes must still be
OSPF [110/...] via hub VTIs
sudo ping -c 3 10.254.<S>.<S>1

```

Unattended re-establish proof

```

# Prove the ER re-establishes on its own (Cato is Responder Only, so it cannot help):
sudo ipsec down peer-113.30.140.95-tunnel-vti
# wait up to ~3 minutes, then:
show vpn log | grep peer-113.30.140.95 | grep -E 'initiating IKE_SA|sending
packet.*4500|IKE_AUTH response|CHILD_SA .* established'
# Expect: 'initiating IKE_SA' (not 'typed'), IKE_AUTH request 384 bytes (FQDN id) or 352 (IPv4
id),
# response '[ IDr AUTH SA TSi TSr ]' and 'CHILD_SA ... established'. 416 bytes +
N(TS_UNACCEPT) = drop-in missing.
show ip bgp summary

```

Two-WAN-path sites (one path per Cato HA role)

Sites with a PTP/fibre path through a hub plus an LTE path (Gembrook West, Mater Christi) use **two tunnels, one per path**: primary role = PTP/fibre path → Melbourne PoP, secondary role = LTE

path → Sydney PoP. Both are in BGP; the primary carries local-pref 200 and no prepend, the secondary local-pref 100 with the ASN prepended twice, and Cato itself double-prepends secondary-role routes and only uses the secondary role when every primary-role tunnel is down. This is exactly the shape Cato's own HA guides use for third-party routers (FortiGate, Cisco IOS, VMware Edge).

Why not four tunnels (both PoPs over both paths) like the KL1 PA-440: EdgeOS keys `site-to-site peer` by address and has a single routing table, so two tunnels to the same PoP IP from two paths would need hostname-keyed peers (EdgeOS refuses them for VTIs: "an ip address must be specified for VTIs") plus a persistent `ip rule` post-config script. The only clean alternative is a distinct PoP address per path, and the account's three IPsec IP licences are all allocated. Rejected as too complex; revisit only if licences change.

Extra configuration for a two-path site:

- Per-path host routes so each tunnel leaves by the right interface: `set protocols static route 113.30.140.95/32 next-hop <PTP next hop>` and `set protocols static route 202.75.244.10/32 next-hop <LTE gateway>`.
- Peer `local-address` = the address on that path (the PTP side uses the private transit address; the hub PA-440 NATs it, so the tunnel runs NAT-T on UDP 4500 — the hub's NAT and security policy must permit 500/4500 from the transit subnet).
- The LTE-local firewall ruleset on these sites is per-source, so add accept rules for the Sydney PoP (IKE 500/4500 and ESP). The PTP path enters an interface with no local ruleset.
- Cato page: WAN2 row identifier `<catoSiteId>.23991.2.catonetworks.com`; last-mile for the PTP row is its share of the hub's link.
- Do not export the transit /24 (e.g. 10.250.97.0/24, 192.168.127.0/24).

Operations

BGP neighbour reset (EdgeOS 3.0.1 has no working clear/reset command)

```
configure
set protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 shutdown
commit
delete protocols bgp 6500<S> neighbor 10.254.<S>.<S>3 shutdown
commit
exit
```

Recovery after a bad commit

```
# From a hub-side box (or via the site loopback 10.100.x.1 / hub VTI address if LAN replies
are being swallowed):
ssh <ER>
configure
load          # reloads the saved config.boot
commit
exit
# or, if the device is unreachable, power-cycle: it boots from config.boot (the last 'save').
```

EdgeOS 3.0.1 gotchas

- Any `set vpn ipsec` commit — including logging changes — restarts charon: all tunnels on the box (hub ones included) bounce for about 2 seconds. Do IPsec commits in a quiet window.
- `sudo ipsec stroke loglevel net 1 / enc 1` give live detail but are lost on every charon restart. `set vpn ipsec logging` is persistent but noisy — remove it after the build.
- `show vpn ipsec state` prints live ESP keys. Use `show vpn ipsec sa`. If keys were ever displayed or pasted, force a rekey.
- VTI addresses must be /31. A /30 makes the BGP validator reject the neighbour.
- `parameters distance global ...` is not accepted; use `parameters distance prefix 0.0.0.0/0 distance 115`. It applies to routes installed after the commit — reset the neighbour if the routes were already there.
- Site-to-site peers are keyed by IP; hostname peers are refused for VTIs.
- `config.boot` is in braces format — `grep` it by value, not by set-path. Commit "connecting to charon.ctl failed" on a logging change is the charon restart race and is harmless.
- Use `grep -E` rather than `match '\|'`; `sudo ping -c 3` rather than `ping count`; `export VYATTA_PAGER=cat` to stop the pager swallowing output.
- If a bad firewall or IPsec policy swallows LAN replies, the device is usually still reachable on its loopback 10.100.x.1 or a hub VTI address.

Post-firmware-upgrade runbook

1. Confirm `/etc/strongswan.d/zz-pbr-cato.conf` still exists; if not, re-create it and `sudo ipsec restart`.
 2. Run the unattended re-establish proof. A 416-byte IKE_AUTH followed by TS_UNACCEPT means the drop-in is missing.
-

Reference: Cato PoPs and schema

Item	Value
Melbourne PoP (primary)	113.30.140.95
Sydney PoP (secondary)	202.75.244.10
Cato ASN	64515
Site ASN	6500<site>
VTIs	vti<site>00 (primary), vti<site>01 (secondary)
/31s	10.254.<site>.<site>0/31 and .<site>2/31; site even, Cato odd
Identifier	<catoSiteId>.23991.catonetworks.com (WAN2: .23991.2.)
Import allowlist	10.41.0.0/16 le 24; 10.254.254.0/24 le 32
Known Cato site IDs	Gembrook 1000000006, Cockatoo 1000000007, Gembrook West 1000000008, Mater Christi 1000000009

Maintenance notes

Update this page if Cato support applies the backend multi-TS setting (the drop-in then becomes unnecessary but harmless), if PoP addresses or IP licences change, or after an EdgeOS firmware upgrade changes strongSwan behaviour. Keep the post-upgrade runbook in the fleet upgrade procedure.

Site: Gembrook (PBR-R-G1)

Overview

Item	Value
Site / device	Gembrook — PBR-R-G1, EdgeRouter PoE 5-port, EdgeOS 3.0.1 (Cavium MIPS64, 480 MB RAM, ~38 MB free; IPsec HW offload on)
Site number / ASN	6 / 65006
WAN	eth0 61.29.119.42/30 static (AAPT NBN), gateway 61.29.119.41
LAN	eth2 VLANs 10.6.{10,20,30,40,50,60,70,80,200}.0/24; legacy 10.1.7.0/24 on eth2.10
Loopback / OSPF	lo 10.100.7.1/32; area 0 = 10.254.0.0/16, area 7 = site networks (loopback/area numbering looks swapped with Gembrook West — tidy-up later)
Hub VTIs	vti100 Belgrave, vti800 KL1 NBN, vti810 KL1 Starlink (IKEv2 AES-256/SHA-256/DH14)
Firewall	eth0_aaptlocal accepts IKE 500/4500 + ESP from any peer; SSH/80/443 from WAN dropped (rule 160); NAT masquerade eth0; auto-firewall-nat-exclude on
Cato site ID / identifier	1000000006 — 1000000006.23991.catonetworks.com (both rows)

Status: ACTIVE — fleet standard, proven. Outstanding: quiet-window reboot test (cold start and drop-in persistence), `delete vpn ipsec logging`, confirm temporary firewall rule 5 is removed, `save`.

Built to the *EdgeRouter Site Build Standard* in this book (Responder Only on Cato, ER initiates, FQDN identifier, `ignore_acquire_ts` drop-in, route-based VTIs, BGP export of own prefixes only, import allowlist, distance 115). This page records the site-specific values and observations.

Cato site configuration

Item	Value
------	-------

Connection type	Responder Only; destinations IPv4 Melbourne 113.30.140.95 (PRIMARY1) / Sydney 202.75.244.10 (SECONDARY1), link NBN_TC4
Identifier	FQDN 1000000006.23991.catonetworks.com on both rows
Parameters	Init AES-CBC-256 / SHA-256 / PRF SHA-256 / DH14; Auth AES-CBC-256 / SHA-256 / DH14; 'IKEv2 Send Single TS per payload' On (harmless)
Private IPs	PRIMARY1 Cato 10.254.6.61 / Site 10.254.6.60; SECONDARY1 Cato 10.254.6.63 / Site 10.254.6.62
BGP	Cato ASN 64515, Peer ASN 65006, peers 10.254.6.60 and 10.254.6.62, Hold 90 / Keepalive 30, Advertise All routes
Last mile / PSK	AAPT plan speeds; PSKs regenerated per tunnel 26 Oct 2026 (an earlier PSK was exposed in chat and replaced)

EdgeOS configuration

Full configuration as applied (PSKs omitted). This is the reference build for the fleet; the template on the standard page is derived from it.

```
# ---- One-time, outside EdgeOS config (survives reboot, NOT firmware upgrade) ----
sudo tee /etc/strongswan.d/zz-pbr-cato.conf >/dev/null <<'EOF'
# PBR: suppress acquire-derived traffic selectors so trap-triggered IKEv2
# initiations propose only the configured 0.0.0.0/0 (Cato rejects multi-TS).
# Not preserved by EdgeOS firmware upgrade - re-apply after upgrading.
charon {
    ignore_acquire_ts = yes
}
EOF
sudo ipsec restart      # hub tunnels bounce ~2 s

# ---- EdgeOS configuration (replace <...> values; PSKs in single quotes) ----
configure

# IKE / ESP groups
set vpn ipsec ike-group IKE-CAT0 key-exchange ikev2
set vpn ipsec ike-group IKE-CAT0 ikev2-reauth no
set vpn ipsec ike-group IKE-CAT0 lifetime 19800
set vpn ipsec ike-group IKE-CAT0 proposal 1 dh-group 14
```

```
set vpn ipsec ike-group IKE-CAT0 proposal 1 encryption aes256
set vpn ipsec ike-group IKE-CAT0 proposal 1 hash sha256
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection action restart
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection interval 30
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection timeout 30
set vpn ipsec esp-group ESP-CAT0 lifetime 3600
set vpn ipsec esp-group ESP-CAT0 mode tunnel
set vpn ipsec esp-group ESP-CAT0 pfs dh-group14
set vpn ipsec esp-group ESP-CAT0 proposal 1 encryption aes256
set vpn ipsec esp-group ESP-CAT0 proposal 1 hash sha256

# VTIs (site side even, Cato side odd; MUST be /31)
set interfaces vti vti600 address 10.254.6.60/31
set interfaces vti vti600 description 'Cato Melbourne (primary)'
set interfaces vti vti600 mtu 1400
set interfaces vti vti601 address 10.254.6.62/31
set interfaces vti vti601 description 'Cato Sydney (secondary)'
set interfaces vti vti601 mtu 1400
set protocols ospf passive-interface vti600
set protocols ospf passive-interface vti601
set firewall options mss-clamp interface-type vti
set firewall options mss-clamp mss 1350

# Peers (route-based VTI, ER initiates, FQDN identifier)
set vpn ipsec site-to-site peer 113.30.140.95 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 113.30.140.95 authentication pre-shared-secret '<PSK-PRIMARY>'
set vpn ipsec site-to-site peer 113.30.140.95 authentication id
@10000000006.23991.catonetworks.com
set vpn ipsec site-to-site peer 113.30.140.95 authentication remote-id 113.30.140.95
set vpn ipsec site-to-site peer 113.30.140.95 connection-type initiate
set vpn ipsec site-to-site peer 113.30.140.95 description 'Cato Melbourne PoP'
set vpn ipsec site-to-site peer 113.30.140.95 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 113.30.140.95 local-address 61.29.119.42
set vpn ipsec site-to-site peer 113.30.140.95 vti bind vti600
set vpn ipsec site-to-site peer 113.30.140.95 vti esp-group ESP-CAT0

set vpn ipsec site-to-site peer 202.75.244.10 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 202.75.244.10 authentication pre-shared-secret '<PSK-SECONDARY>'
```

```
set vpn ipsec site-to-site peer 202.75.244.10 authentication id
@10000000006.23991.catonetworks.com
set vpn ipsec site-to-site peer 202.75.244.10 authentication remote-id 202.75.244.10
set vpn ipsec site-to-site peer 202.75.244.10 connection-type initiate
set vpn ipsec site-to-site peer 202.75.244.10 description 'Cato Sydney PoP'
set vpn ipsec site-to-site peer 202.75.244.10 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 202.75.244.10 local-address 61.29.119.42
set vpn ipsec site-to-site peer 202.75.244.10 vti bind vti601
set vpn ipsec site-to-site peer 202.75.244.10 vti esp-group ESP-CAT0
```

Routing policy

```
set policy prefix-list GEMBR00K-PREFIXES rule 10 action permit
set policy prefix-list GEMBR00K-PREFIXES rule 10 prefix 10.6.0.0/16
set policy prefix-list GEMBR00K-PREFIXES rule 10 le 24
set policy prefix-list GEMBR00K-PREFIXES rule 20 action permit
set policy prefix-list GEMBR00K-PREFIXES rule 20 prefix 10.1.7.0/24
set policy prefix-list GEMBR00K-PREFIXES rule 90 action permit
set policy prefix-list GEMBR00K-PREFIXES rule 90 prefix 10.100.7.1/32
set policy prefix-list CAT0-ALLOWED-IN rule 10 action permit
set policy prefix-list CAT0-ALLOWED-IN rule 10 prefix 10.41.0.0/16
set policy prefix-list CAT0-ALLOWED-IN rule 10 le 24
set policy prefix-list CAT0-ALLOWED-IN rule 20 action permit
set policy prefix-list CAT0-ALLOWED-IN rule 20 prefix 10.254.254.0/24
set policy prefix-list CAT0-ALLOWED-IN rule 20 le 32

set policy route-map CAT0-CONNECTED rule 10 action permit
set policy route-map CAT0-CONNECTED rule 10 match ip address prefix-list GEMBR00K-PREFIXES
set policy route-map CAT0-OUT-PRI rule 10 action permit
set policy route-map CAT0-OUT-PRI rule 10 match ip address prefix-list GEMBR00K-PREFIXES
set policy route-map CAT0-OUT-SEC rule 10 action permit
set policy route-map CAT0-OUT-SEC rule 10 match ip address prefix-list GEMBR00K-PREFIXES
set policy route-map CAT0-OUT-SEC rule 10 set as-path-prepend '65006 65006'
set policy route-map CAT0-IN-PRI rule 10 action permit
set policy route-map CAT0-IN-PRI rule 10 match ip address prefix-list CAT0-ALLOWED-IN
set policy route-map CAT0-IN-PRI rule 10 set local-preference 200
set policy route-map CAT0-IN-SEC rule 10 action permit
set policy route-map CAT0-IN-SEC rule 10 match ip address prefix-list CAT0-ALLOWED-IN
set policy route-map CAT0-IN-SEC rule 10 set local-preference 100
```

```
# BGP
set protocols bgp 65006 parameters router-id 10.100.7.1
set protocols bgp 65006 parameters distance prefix 0.0.0.0/0 distance 115
set protocols bgp 65006 redistribute connected route-map CATO-CONNECTED
set protocols bgp 65006 neighbor 10.254.6.61 remote-as 64515
set protocols bgp 65006 neighbor 10.254.6.61 description 'Cato Melbourne'
set protocols bgp 65006 neighbor 10.254.6.61 timers holdtime 90
set protocols bgp 65006 neighbor 10.254.6.61 timers keepalive 30
set protocols bgp 65006 neighbor 10.254.6.61 soft-reconfiguration inbound
set protocols bgp 65006 neighbor 10.254.6.61 route-map import CATO-IN-PRI
set protocols bgp 65006 neighbor 10.254.6.61 route-map export CATO-OUT-PRI
set protocols bgp 65006 neighbor 10.254.6.63 remote-as 64515
set protocols bgp 65006 neighbor 10.254.6.63 description 'Cato Sydney'
set protocols bgp 65006 neighbor 10.254.6.63 timers holdtime 90
set protocols bgp 65006 neighbor 10.254.6.63 timers keepalive 30
set protocols bgp 65006 neighbor 10.254.6.63 soft-reconfiguration inbound
set protocols bgp 65006 neighbor 10.254.6.63 route-map import CATO-IN-SEC
set protocols bgp 65006 neighbor 10.254.6.63 route-map export CATO-OUT-SEC

commit-confirm 10
# ... verify tunnels and BGP, then:
confirm
save
```

Verified state (26 Oct 2026)

- Both tunnels established, ER-initiated; unattended re-establish proven at 16:26:31 (single-selector IKE_AUTH 384 B, CHILD_SA in ~1 s, both BGP neighbours back).
- Exactly 11 Gembrook prefixes advertised; only 10.41.0.0/16 and 10.254.254.x installed from the ~127 offered; all hub OSPF routes untouched.

Incident record

26 Oct 2026 ~14:30: a policy-based tunnel configuration suggested by the Cato AI assistant was committed and took the site offline (all 10.6.0.0/16 traffic diverted into the Cato tunnel, VTIs removed). Recovered by rebooting onto the saved config.boot; BGP had to be re-entered and vti601 corrected from /30 to /31 before the neighbour would validate. See the DO-NOT-DO section of the standard page.

Maintenance notes

Update this page whenever the WAN address, prefixes, PSKs (date only — never the secret), Cato site parameters or tunnel layout change. Re-apply the strongSwan drop-in after any firmware upgrade and re-run the unattended re-establish proof.

Site: Cockatoo (PBR-R-CK1)

Overview

Item	Value
Site / device	Cockatoo — PBR-R-CK1, EdgeRouter PoE 5-port, EdgeOS 3.0.1 (~120 MB free; IPsec HW offload on)
Site number / ASN	5 / 65005
WAN	eth1 Optus 4G LTE, DHCP with fixed public IP 59.154.241.12/24; inbound IKE confirmed working
LAN	eth4 VLANs 10.5.10.0/24 (Infra), 10.5.60.0/24 (VoIP), 10.5.80.0/24 (SecOT); legacy 192.168.132.0/24 on switch0 (UniPi, station phone — OT); 10.1.6.0/24 on eth0 (link down)
Loopback / OSPF	lo 10.100.6.1/32; area 6 (old-scheme number); area 0 = 10.254.0.0/16; router-id 10.100.6.1, abr-type cisco; neighbours Belgrave vti100, KL1 vti800/vti810
Firewall	eth1local rules 30/31 accept IKE 500/4500 + ESP any peer; SSH/80/443 dropped (rule 96); NAT masquerade eth1; auto-firewall-nat-exclude on
Oddities	Stale static default <code>via 192.168.5.1 inactive</code> (default comes from DHCP) — delete when convenient
Cato site ID / identifier	1000000007 — 1000000007.23991.catonetworks.com (both rows)

Status: ACTIVE — fleet standard. Outstanding: set real LTE last-mile speeds on the Cato page; confirm the BGP distance line (prefix form) is present; delete the stale static default.

Built to the *EdgeRouter Site Build Standard* in this book (Responder Only on Cato, ER initiates, FQDN identifier, `ignore_acquire_ts` drop-in, route-based VTIs, BGP export of own prefixes only, import allowlist, distance 115). This page records the site-specific values and observations.

Cato site configuration

Item	Value
------	-------

Connection type	Responder Only; destinations IPv4 Melbourne 113.30.140.95 / Sydney 202.75.244.10; link OPTUSLTE_WAN
Identifier	FQDN 1000000007.23991.catonetworks.com on both rows
Parameters	Init AES-CBC-256 / SHA-256 / PRF SHA-256 / DH14; Auth AES-CBC-256 / SHA-256 / DH14
Private IPs	PRIMARY1 Cato 10.254.5.51 / Site 10.254.5.50; SECONDARY1 Cato 10.254.5.53 / Site 10.254.5.52
BGP	Cato ASN 64515, Peer ASN 65005, peers 10.254.5.50 and 10.254.5.52, Hold 90 / Keepalive 30, Advertise All routes
Last mile / PSK	To set: real Optus LTE speeds (page showed 100/100); fresh PSK per tunnel

EdgeOS configuration

Configuration as applied (PSKs omitted). Prefix list COCKATOO-PREFIXES: 10.5.0.0/16 le 24, 192.168.132.0/24, 10.1.6.0/24, 10.100.6.1/32.

```
# ---- One-time, outside EdgeOS config (survives reboot, NOT firmware upgrade) ----
sudo tee /etc/strongswan.d/zz-pbr-cato.conf >/dev/null <<'EOF'
# PBR: suppress acquire-derived traffic selectors so trap-triggered IKEv2
# initiations propose only the configured 0.0.0.0/0 (Cato rejects multi-TS).
# Not preserved by EdgeOS firmware upgrade - re-apply after upgrading.
charon {
    ignore_acquire_ts = yes
}
EOF
sudo ipsec restart      # hub tunnels bounce ~2 s

# ---- EdgeOS configuration (replace <...> values; PSKs in single quotes) ----
configure

# IKE / ESP groups
set vpn ipsec ike-group IKE-CAT0 key-exchange ikev2
set vpn ipsec ike-group IKE-CAT0 ikev2-reauth no
set vpn ipsec ike-group IKE-CAT0 lifetime 19800
set vpn ipsec ike-group IKE-CAT0 proposal 1 dh-group 14
set vpn ipsec ike-group IKE-CAT0 proposal 1 encryption aes256
```

```
set vpn ipsec ike-group IKE-CAT0 proposal 1 hash sha256
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection action restart
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection interval 30
set vpn ipsec ike-group IKE-CAT0 dead-peer-detection timeout 30
set vpn ipsec esp-group ESP-CAT0 lifetime 3600
set vpn ipsec esp-group ESP-CAT0 mode tunnel
set vpn ipsec esp-group ESP-CAT0 pfs dh-group14
set vpn ipsec esp-group ESP-CAT0 proposal 1 encryption aes256
set vpn ipsec esp-group ESP-CAT0 proposal 1 hash sha256

# VTIs (site side even, Cato side odd; MUST be /31)
set interfaces vti vti500 address 10.254.5.50/31
set interfaces vti vti500 description 'Cato Melbourne (primary)'
set interfaces vti vti500 mtu 1400
set interfaces vti vti501 address 10.254.5.52/31
set interfaces vti vti501 description 'Cato Sydney (secondary)'
set interfaces vti vti501 mtu 1400
set protocols ospf passive-interface vti500
set protocols ospf passive-interface vti501
set firewall options mss-clamp interface-type vti
set firewall options mss-clamp mss 1350

# Peers (route-based VTI, ER initiates, FQDN identifier)
set vpn ipsec site-to-site peer 113.30.140.95 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 113.30.140.95 authentication pre-shared-secret '<PSK-PRIMARY>'
set vpn ipsec site-to-site peer 113.30.140.95 authentication id
@1000000007.23991.catonetworks.com
set vpn ipsec site-to-site peer 113.30.140.95 authentication remote-id 113.30.140.95
set vpn ipsec site-to-site peer 113.30.140.95 connection-type initiate
set vpn ipsec site-to-site peer 113.30.140.95 description 'Cato Melbourne PoP'
set vpn ipsec site-to-site peer 113.30.140.95 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 113.30.140.95 local-address 59.154.241.12
set vpn ipsec site-to-site peer 113.30.140.95 vti bind vti500
set vpn ipsec site-to-site peer 113.30.140.95 vti esp-group ESP-CAT0

set vpn ipsec site-to-site peer 202.75.244.10 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 202.75.244.10 authentication pre-shared-secret '<PSK-SECONDARY>'
set vpn ipsec site-to-site peer 202.75.244.10 authentication id
```

@1000000007.23991.catonetworks.com

```
set vpn ipsec site-to-site peer 202.75.244.10 authentication remote-id 202.75.244.10
set vpn ipsec site-to-site peer 202.75.244.10 connection-type initiate
set vpn ipsec site-to-site peer 202.75.244.10 description 'Cato Sydney PoP'
set vpn ipsec site-to-site peer 202.75.244.10 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 202.75.244.10 local-address 59.154.241.12
set vpn ipsec site-to-site peer 202.75.244.10 vti bind vti501
set vpn ipsec site-to-site peer 202.75.244.10 vti esp-group ESP-CAT0
```

Routing policy

```
set policy prefix-list COCKAT00-PREFIXES rule 10 action permit
set policy prefix-list COCKAT00-PREFIXES rule 10 prefix 10.5.0.0/16
set policy prefix-list COCKAT00-PREFIXES rule 10 le 24
set policy prefix-list COCKAT00-PREFIXES rule 20 action permit
set policy prefix-list COCKAT00-PREFIXES rule 20 prefix 192.168.132.0/24
set policy prefix-list COCKAT00-PREFIXES rule 30 action permit
set policy prefix-list COCKAT00-PREFIXES rule 30 prefix 10.1.6.0/24
set policy prefix-list COCKAT00-PREFIXES rule 90 action permit
set policy prefix-list COCKAT00-PREFIXES rule 30 action permit
set policy prefix-list COCKAT00-PREFIXES rule 30 prefix 10.1.6.0/24
set policy prefix-list COCKAT00-PREFIXES rule 90 prefix 10.100.6.1/32
set policy prefix-list CAT0-ALLOWED-IN rule 10 action permit
set policy prefix-list CAT0-ALLOWED-IN rule 10 prefix 10.41.0.0/16
set policy prefix-list CAT0-ALLOWED-IN rule 10 le 24
set policy prefix-list CAT0-ALLOWED-IN rule 20 action permit
set policy prefix-list CAT0-ALLOWED-IN rule 20 prefix 10.254.254.0/24
set policy prefix-list CAT0-ALLOWED-IN rule 20 le 32

set policy route-map CAT0-CONNECTED rule 10 action permit
set policy route-map CAT0-CONNECTED rule 10 match ip address prefix-list COCKAT00-PREFIXES
set policy route-map CAT0-OUT-PRI rule 10 action permit
set policy route-map CAT0-OUT-PRI rule 10 match ip address prefix-list COCKAT00-PREFIXES
set policy route-map CAT0-OUT-SEC rule 10 action permit
set policy route-map CAT0-OUT-SEC rule 10 match ip address prefix-list COCKAT00-PREFIXES
set policy route-map CAT0-OUT-SEC rule 10 set as-path-prepend '65005 65005'
set policy route-map CAT0-IN-PRI rule 10 action permit
set policy route-map CAT0-IN-PRI rule 10 match ip address prefix-list CAT0-ALLOWED-IN
set policy route-map CAT0-IN-PRI rule 10 set local-preference 200
set policy route-map CAT0-IN-SEC rule 10 action permit
```

```
set policy route-map CAT0-IN-SEC rule 10 match ip address prefix-list CAT0-ALLOWED-IN
set policy route-map CAT0-IN-SEC rule 10 set local-preference 100

# BGP
set protocols bgp 65005 parameters router-id 10.100.6.1
set protocols bgp 65005 parameters distance prefix 0.0.0.0/0 distance 115
set protocols bgp 65005 redistribute connected route-map CAT0-CONNECTED
set protocols bgp 65005 neighbor 10.254.5.51 remote-as 64515
set protocols bgp 65005 neighbor 10.254.5.51 description 'Cato Melbourne'
set protocols bgp 65005 neighbor 10.254.5.51 timers holdtime 90
set protocols bgp 65005 neighbor 10.254.5.51 timers keepalive 30
set protocols bgp 65005 neighbor 10.254.5.51 soft-reconfiguration inbound
set protocols bgp 65005 neighbor 10.254.5.51 route-map import CAT0-IN-PRI
set protocols bgp 65005 neighbor 10.254.5.51 route-map export CAT0-OUT-PRI
set protocols bgp 65005 neighbor 10.254.5.53 remote-as 64515
set protocols bgp 65005 neighbor 10.254.5.53 description 'Cato Sydney'
set protocols bgp 65005 neighbor 10.254.5.53 timers holdtime 90
set protocols bgp 65005 neighbor 10.254.5.53 timers keepalive 30
set protocols bgp 65005 neighbor 10.254.5.53 soft-reconfiguration inbound
set protocols bgp 65005 neighbor 10.254.5.53 route-map import CAT0-IN-SEC
set protocols bgp 65005 neighbor 10.254.5.53 route-map export CAT0-OUT-SEC

commit-confirm 10
# ... verify tunnels and BGP, then:
confirm
save
```

Verified state (26 Oct 2026)

- First established 16:03 on Bidirectional, then converted to the fleet standard (Cato Responder Only + FQDN identifier; ER drop-in, `authentication id @1000000007.23991.catonetworks.com`, `connection-type initiate`).
- Advertised: 10.5.10/60/80 /24s, 192.168.132.0/24, 10.100.6.1/32 (10.1.6.0/24 absent while eth0 is down).

Maintenance notes

Update this page whenever the WAN address, prefixes, PSKs (date only — never the secret), Cato site parameters or tunnel layout change. Re-apply the strongSwan drop-in after any firmware upgrade and re-run the unattended re-establish proof.

Site: Gembrook West (PBR-R-GW1)

Overview

Item	Value
Site / device	Gembrook West — PBR-R-GW1, EdgeRouter 12-port, EdgeOS 3.0.1
Site number / ASN	7 / 65007
WAN paths	eth9 PTP 10.250.97.2/24 to Kings Rd KT1 (default via 10.250.97.1, OSPF area 0); eth8 Optus 4G LTE DHCP fixed 124.19.90.145/24 (default at distance 210); hub tunnels via /32 statics out LTE
LAN	10.7.40.0/24; legacy 172.16.2.0/24; radios 10.52.0.0/24; transit 10.250.97.0/24 (not exported)
Loopback / OSPF	lo 10.100.12.1/32, area 12, router-id 10.100.12.1; stale passive-interface vti1/vti2 (harmless)
Firewall	eth8local rules 30–33 KL1/Belgrave, 34–35 Cato Sydney PoP; PTP path on eth9 has no local ruleset; NAT masquerade eth8
Cato site ID / identifiers	1000000008 — 1000000008.23991.catonetworks.com (PTP row), 1000000008.23991.2.catonetworks.com (LTE row)

Status: ACTIVE — two-tunnel fleet standard. Optional: confirm/save, failover proof (`ipsec down` Melbourne → routes flip to vti701 → back), confirm device model.

Built to the *EdgeRouter Site Build Standard* in this book (Responder Only on Cato, ER initiates, FQDN identifier, `ignore_acquire_ts` drop-in, route-based VTIs, BGP export of own prefixes only, import allowlist, distance 115). This page records the site-specific values and observations.

Cato site configuration

Item	Value
Connection type	Responder Only; IPv4 destinations; two tunnel rows, one per path
PRIMARY1 (PTP_WAN)	→ Melbourne 113.30.140.95 from 10.250.97.2 (NAT-T through KT1 61.69.44.198; KT1 NAT/policy already permitted it); vti700 10.254.7.70/31 (Cato .71); last-mile = share of Kings NBN
SECONDARY (LTE_WAN)	→ Sydney 202.75.244.10 from 124.19.90.145; vti701 10.254.7.72/31 (Cato .73); last-mile = real Optus speeds
Parameters	Init AES-CBC-256 / SHA-256 / PRF SHA-256 / DH14; Auth AES-CBC-256 / SHA-256 / DH14
BGP	Cato ASN 64515, Peer ASN 65007, peers 10.254.7.70 and 10.254.7.72, Hold 90 / Keepalive 30, Advertise All routes
Failover	Cato uses the secondary role only when all primary tunnels are down; secondary routes double-prepended by Cato and by the ER

EdgeOS configuration

Two-path build (PTP primary, LTE secondary). PSKs omitted.

```
# One-time drop-in (see standard page), then:
configure

set protocols static route 113.30.140.95/32 next-hop 10.250.97.1      # Melbourne PoP via PTP
(eth9 -> KT1)
set protocols static route 202.75.244.10/32 next-hop 124.19.90.1      # Sydney PoP via LTE
(eth8)

# LTE-local firewall is per-source: allow Sydney PoP
set firewall name eth8local rule 34 action accept
set firewall name eth8local rule 34 description 'Cato Sydney IKE'
set firewall name eth8local rule 34 destination port 500,4500
set firewall name eth8local rule 34 protocol udp
set firewall name eth8local rule 34 source address 202.75.244.10
set firewall name eth8local rule 35 action accept
set firewall name eth8local rule 35 description 'Cato Sydney ESP'
set firewall name eth8local rule 35 protocol esp
```

```
set firewall name eth8local rule 35 source address 202.75.244.10

# IKE-CAT0 / ESP-CAT0 groups as per standard

set interfaces vti vti700 address 10.254.7.70/31
set interfaces vti vti700 description 'Cato Melbourne via PTP (primary)'
set interfaces vti vti700 mtu 1400
set interfaces vti vti701 address 10.254.7.72/31
set interfaces vti vti701 description 'Cato Sydney via LTE (secondary)'
set interfaces vti vti701 mtu 1400
set protocols ospf passive-interface vti700
set protocols ospf passive-interface vti701
set firewall options mss-clamp interface-type vti
set firewall options mss-clamp mss 1350

set vpn ipsec site-to-site peer 113.30.140.95 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 113.30.140.95 authentication pre-shared-secret '<PSK-PRIMARY>'
set vpn ipsec site-to-site peer 113.30.140.95 authentication id
@1000000008.23991.catonetworks.com
set vpn ipsec site-to-site peer 113.30.140.95 authentication remote-id 113.30.140.95
set vpn ipsec site-to-site peer 113.30.140.95 connection-type initiate
set vpn ipsec site-to-site peer 113.30.140.95 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 113.30.140.95 local-address 10.250.97.2
set vpn ipsec site-to-site peer 113.30.140.95 vti bind vti700
set vpn ipsec site-to-site peer 113.30.140.95 vti esp-group ESP-CAT0

set vpn ipsec site-to-site peer 202.75.244.10 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 202.75.244.10 authentication pre-shared-secret '<PSK-SECONDARY>'
set vpn ipsec site-to-site peer 202.75.244.10 authentication id
@1000000008.23991.2.catonetworks.com
set vpn ipsec site-to-site peer 202.75.244.10 authentication remote-id 202.75.244.10
set vpn ipsec site-to-site peer 202.75.244.10 connection-type initiate
set vpn ipsec site-to-site peer 202.75.244.10 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 202.75.244.10 local-address 124.19.90.145
set vpn ipsec site-to-site peer 202.75.244.10 vti bind vti701
set vpn ipsec site-to-site peer 202.75.244.10 vti esp-group ESP-CAT0

set policy prefix-list GEMWEST-PREFIXES rule 10 action permit
```

```
set policy prefix-list GEMWEST-PREFIXES rule 10 prefix 10.7.0.0/16
set policy prefix-list GEMWEST-PREFIXES rule 10 le 24
set policy prefix-list GEMWEST-PREFIXES rule 20 action permit
set policy prefix-list GEMWEST-PREFIXES rule 20 prefix 172.16.2.0/24
set policy prefix-list GEMWEST-PREFIXES rule 30 action permit
set policy prefix-list GEMWEST-PREFIXES rule 30 prefix 10.52.0.0/24
set policy prefix-list GEMWEST-PREFIXES rule 90 action permit
set policy prefix-list GEMWEST-PREFIXES rule 90 prefix 10.100.12.1/32
# CAT0-ALLOWED-IN, CAT0-CONNECTED, CAT0-OUT-PRI/SEC (prepend '65007 65007'), CAT0-IN-PRI/SEC
as per standard

set protocols bgp 65007 parameters router-id 10.100.12.1
set protocols bgp 65007 parameters distance prefix 0.0.0.0/0 distance 115
set protocols bgp 65007 redistribute connected route-map CAT0-CONNECTED
set protocols bgp 65007 neighbor 10.254.7.71 remote-as 64515
set protocols bgp 65007 neighbor 10.254.7.71 timers holdtime 90
set protocols bgp 65007 neighbor 10.254.7.71 timers keepalive 30
set protocols bgp 65007 neighbor 10.254.7.71 soft-reconfiguration inbound
set protocols bgp 65007 neighbor 10.254.7.71 route-map import CAT0-IN-PRI
set protocols bgp 65007 neighbor 10.254.7.71 route-map export CAT0-OUT-PRI
set protocols bgp 65007 neighbor 10.254.7.73 remote-as 64515
set protocols bgp 65007 neighbor 10.254.7.73 timers holdtime 90
set protocols bgp 65007 neighbor 10.254.7.73 timers keepalive 30
set protocols bgp 65007 neighbor 10.254.7.73 soft-reconfiguration inbound
set protocols bgp 65007 neighbor 10.254.7.73 route-map import CAT0-IN-SEC
set protocols bgp 65007 neighbor 10.254.7.73 route-map export CAT0-OUT-SEC

commit-confirm 10 ; confirm ; save
```

Verified state (26 Oct 2026 18:02)

- Melbourne SA from 10.250.97.2 via NAT-T, Sydney SA from 124.19.90.145; both BGP Established with 18 prefixes received, routes installed via vti700 at [115/100].
- Exactly 4 prefixes advertised: 10.7.40.0/24, 10.52.0.0/24, 10.100.12.1/32, 172.16.2.0/24 (transit 10.250.97.0/24 correctly absent).

Design decision: two tunnels, not four

Investigated 26 Oct 2026. Cato allows four tunnels to two PoP addresses (the KL1 PA-440 does this), but EdgeOS keys peers by address and has one routing table, so a second tunnel to the same PoP from the other path needs hostname-keyed peers (refused for VTIs) and a persistent `ip rule` script. A distinct PoP address per path would need a fourth IPsec IP licence (all three allocated). Rejected; one path per Cato HA role instead, matching Cato's own third-party HA guides. The hostname-peer refusal also means the "FQDN trick" is unavailable for the hub Starlink VTIs; `peer 0.0.0.0` (respond-only, matched on remote-id) is an untested alternative.

Maintenance notes

Update this page whenever the WAN address, prefixes, PSKs (date only — never the secret), Cato site parameters or tunnel layout change. Re-apply the strongSwan drop-in after any firmware upgrade and re-run the unattended re-establish proof.

Site: Mater Christi (PBR-R-BS1)

Overview

Item	Value
Site / device	Mater Christi — PBR-R-BS1, EdgeRouter 12, EdgeOS 3.0.1 (1 GB RAM; uptime 162 d at audit; boot-image upgrade prompt pending)
Site number / ASN	10 / 65010
WAN paths	eth9 airFiber PTP 192.168.127.79/24 to Belgrave (default [50] via 192.168.127.99, OSPF neighbour 10.100.1.1 at 192.168.127.1); eth8 LTE DHCP fixed 161.43.192.52/24 (default [210]); hub tunnels vti100 Belgrave, vti800 KL1, vti920 Kings LTE via LTE statics
LAN	10.10.40.0/24; legacy 172.16.0.0/24; transit 192.168.127.0/24 (not exported)
Loopback / OSPF	lo 10.100.10.1/32, router-id 10.100.10.1; area 0 = 10.254.0.0/16 (Cato VTIs passive)
Firewall	eth8local per-source: rules 36–37 added for Cato Sydney PoP; PTP path on eth9 has no local ruleset
Housekeeping	Orphaned <code>eth1local</code> ruleset incl. 'wan access to gui' accept-all-TCP (unattached — delete); clock a month behind — add au.pool.ntp.org servers
Cato site ID / identifier	1000000009 — 1000000009.23991.catonetworks.com (used on both rows)

Status: TUNNELS UP — confirm BGP Established and routes, fix NTP, then `confirm` and `save`.

Built to the *EdgeRouter Site Build Standard* in this book (Responder Only on Cato, ER initiates, FQDN identifier, `ignore_acquire_ts` drop-in, route-based VTIs, BGP export of own prefixes only, import allowlist, distance 115). This page records the site-specific values and observations.

Cato site configuration

Item	Value
Connection type	Responder Only; IPv4 destinations; two tunnel rows, one per path
PRIMARY1 (PTP_BELG)	→ Melbourne 113.30.140.95 from 192.168.127.79 (NAT-T through Belgrave B1 27.32.136.234 — B1 NAT + 500/4500 policy for 192.168.127.0/24 required); vti1000 10.254.10.100/31 (Cato .101)
SECONDARY (LTE_WAN)	→ Sydney 202.75.244.10 from 161.43.192.52; vti1001 10.254.10.102/31 (Cato .103)
Parameters	Init AES-CBC-256 / SHA-256 / PRF SHA-256 / DH14; Auth AES-CBC-256 / SHA-256 / DH14
BGP	Cato ASN 64515, Peer ASN 65010, peers 10.254.10.100 and 10.254.10.102, Hold 90 / Keepalive 30, Advertise All routes

EdgeOS configuration

Two-path build (airFiber PTP primary, LTE secondary). MATER-PREFIXES: 10.10.0.0/16 le 24, 172.16.0.0/24, 10.100.10.1/32. PSKs omitted.

```
# One-time drop-in (see standard page), then:
configure

set protocols static route 113.30.140.95/32 next-hop 192.168.127.99    # Melbourne PoP via
airFiber PTP (eth9 -> Belgrave)
set protocols static route 202.75.244.10/32 next-hop 161.43.192.1     # Sydney PoP via LTE
(eth8)

# LTE-local firewall is per-source: allow Sydney PoP
set firewall name eth8local rule 36 action accept
set firewall name eth8local rule 36 description 'Cato Sydney IKE'
set firewall name eth8local rule 36 destination port 500,4500
set firewall name eth8local rule 36 protocol udp
set firewall name eth8local rule 36 source address 202.75.244.10
set firewall name eth8local rule 37 action accept
```

```
set firewall name eth8local rule 37 description 'Cato Sydney ESP'
set firewall name eth8local rule 37 protocol esp
set firewall name eth8local rule 37 source address 202.75.244.10

# IKE-CAT0 / ESP-CAT0 groups as per standard

set interfaces vti vti1000 address 10.254.10.100/31
set interfaces vti vti1000 description 'Cato Melbourne via PTP (primary)'
set interfaces vti vti1000 mtu 1400
set interfaces vti vti1001 address 10.254.10.102/31
set interfaces vti vti1001 description 'Cato Sydney via LTE (secondary)'
set interfaces vti vti1001 mtu 1400
set protocols ospf passive-interface vti1000
set protocols ospf passive-interface vti1001
set firewall options mss-clamp interface-type vti
set firewall options mss-clamp mss 1350

set vpn ipsec site-to-site peer 113.30.140.95 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 113.30.140.95 authentication pre-shared-secret '<PSK-PRIMARY>'
set vpn ipsec site-to-site peer 113.30.140.95 authentication id
@1000000009.23991.catonetworks.com
set vpn ipsec site-to-site peer 113.30.140.95 authentication remote-id 113.30.140.95
set vpn ipsec site-to-site peer 113.30.140.95 connection-type initiate
set vpn ipsec site-to-site peer 113.30.140.95 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 113.30.140.95 local-address 192.168.127.79
set vpn ipsec site-to-site peer 113.30.140.95 vti bind vti1000
set vpn ipsec site-to-site peer 113.30.140.95 vti esp-group ESP-CAT0

set vpn ipsec site-to-site peer 202.75.244.10 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 202.75.244.10 authentication pre-shared-secret '<PSK-SECONDARY>'
set vpn ipsec site-to-site peer 202.75.244.10 authentication id
@1000000009.23991.catonetworks.com
set vpn ipsec site-to-site peer 202.75.244.10 authentication remote-id 202.75.244.10
set vpn ipsec site-to-site peer 202.75.244.10 connection-type initiate
set vpn ipsec site-to-site peer 202.75.244.10 ike-group IKE-CAT0
set vpn ipsec site-to-site peer 202.75.244.10 local-address 161.43.192.52
set vpn ipsec site-to-site peer 202.75.244.10 vti bind vti1001
set vpn ipsec site-to-site peer 202.75.244.10 vti esp-group ESP-CAT0
```

```
set policy prefix-list MATER-PREFIXES rule 10 action permit
set policy prefix-list MATER-PREFIXES rule 10 prefix 10.10.0.0/16
set policy prefix-list MATER-PREFIXES rule 10 le 24
set policy prefix-list MATER-PREFIXES rule 20 action permit
set policy prefix-list MATER-PREFIXES rule 20 prefix 172.16.0.0/24
set policy prefix-list MATER-PREFIXES rule 90 action permit
set policy prefix-list MATER-PREFIXES rule 90 prefix 10.100.10.1/32
# CAT0-ALLOWED-IN, CAT0-CONNECTED, CAT0-OUT-PRI/SEC (prepend '65010 65010'), CAT0-IN-PRI/SEC
as per standard

set protocols bgp 65010 parameters router-id 10.100.10.1
set protocols bgp 65010 parameters distance prefix 0.0.0.0/0 distance 115
set protocols bgp 65010 redistribute connected route-map CAT0-CONNECTED
set protocols bgp 65010 neighbor 10.254.10.101 remote-as 64515
set protocols bgp 65010 neighbor 10.254.10.101 timers holdtime 90
set protocols bgp 65010 neighbor 10.254.10.101 timers keepalive 30
set protocols bgp 65010 neighbor 10.254.10.101 soft-reconfiguration inbound
set protocols bgp 65010 neighbor 10.254.10.101 route-map import CAT0-IN-PRI
set protocols bgp 65010 neighbor 10.254.10.101 route-map export CAT0-OUT-PRI
set protocols bgp 65010 neighbor 10.254.10.103 remote-as 64515
set protocols bgp 65010 neighbor 10.254.10.103 timers holdtime 90
set protocols bgp 65010 neighbor 10.254.10.103 timers keepalive 30
set protocols bgp 65010 neighbor 10.254.10.103 soft-reconfiguration inbound
set protocols bgp 65010 neighbor 10.254.10.103 route-map import CAT0-IN-SEC
set protocols bgp 65010 neighbor 10.254.10.103 route-map export CAT0-OUT-SEC

commit-confirm 10 ; confirm ; save
```

State at last check (26 Oct 2026)

- Both tunnels established on first commit. BGP neighbours were still in Active about 25 s later — recheck `show ip bgp summary`, advertised routes (expect 10.10.40.0/24, 172.16.0.0/24, 10.100.10.1/32) and `show ip route bgp`.

Maintenance notes

Update this page whenever the WAN address, prefixes, PSKs (date only — never the secret), Cato site parameters or tunnel layout change. Re-apply the strongSwan drop-in after any firmware upgrade and re-run the unattended re-establish proof.

Site: Emerald (PBR-R-E1) — deferred, via hubs

Overview

Item	Value
Site / device	Emerald — PBR-R-E1, EdgeRouter Pro 8, EdgeOS 3.0.1 (2 GB RAM)
Site number / ASN	3 / 65003 (reserved)
Decision	26 Oct 2026 — no Cato tunnel for now . Emerald is reached through the KL1 and KT1 hub tunnels instead.
Links	Fibre to KL1 eth7 10.250.38.1/24 (default [1/0] via 10.250.38.2, OSPF nbr 10.100.8.1); PTP to Kings eth2 10.250.39.1/24 (default [3/0] via 10.250.39.2, OSPF nbr 10.100.11.1); fibre to Lakeside eth6 10.51.0.25/30 (OSPF nbr 10.100.5.1); NBN VDSL eth1 203.174.186.18/30 was DOWN at audit (hub tunnels CONNECTING)
Prefixes	10.3.0.0/16 /24s, legacy 10.1.3.0/24, loopback 10.100.3.1/32

Reaching Emerald via the hubs (to do on the PA-440s)

1. KL1 and KT1 currently export only their own connected prefixes to Cato (Redist_OSPF-BGP, filter type connect). Add Emerald's OSPF-learned prefixes (10.3.0.0/16 /24s, 10.1.3.0/24, 10.100.3.1/32) to the Cato export on both: KL1 as primary, KT1 as backup (lower local-pref / AS-path prepend), so Cato has two paths that follow the fibre and PTP.
2. Return path: Emerald has no route to 10.41.0.0/16. Preferred: KL1 and KT1 redistribute 10.41.0.0/16 (and 10.254.254.0/24) from BGP into OSPF as externals — this also covers any other non-Cato site. Alternative: static on E1 for 10.41.0.0/16 via 10.250.38.2 with a floating backup via 10.250.39.2.

3. Verify from an Emerald host to a ZTNA client address and from Cato to 10.3.x, then record the KL1/KT1 policy names here.

Retained design if an Emerald tunnel is ever wanted

Item	Value
PRIMARY1 FIBRE_KL1	→ Melbourne 113.30.140.95 from 10.250.38.1 (NAT-T via KL1); vti300 10.254.3.30/31 (Cato .31); static 113.30.140.95/32 via 10.250.38.2
SECONDARY PTP_KINGS	→ Sydney 202.75.244.10 from 10.250.39.1 (NAT-T via KT1); vti301 10.254.3.32/31 (Cato .33); static 202.75.244.10/32 via 10.250.39.2
Prefix list	EMERALD-PREFIXES: 10.3.0.0/16 le 24, 10.1.3.0/24, 10.100.3.1/32
BGP	router-id 10.100.3.1, Peer ASN 65003, peers 10.254.3.30 / .32; standard policies
MSS clamp	Existing pppoe/1412 clamp → change interface-type to vti, mss 1350 (or add a second clamp) — check before build
Identifier	<catoSiteId>.23991.catonetworks.com / .23991.2. — read from the Cato page when the site is created

Maintenance notes

Revisit if the Emerald NBN service is restored and a direct tunnel becomes worthwhile, or if the hub export/redistribution design changes. Update the Overview page status table when the hub-side work is done.