

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.

Revision #1

Created 2026-10-26 07:26:15 UTC by PBR_Documentation

Updated 2026-10-26 07:26:15 UTC by PBR_Documentation