

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.

Revision #1

Created 2026-10-26 07:26:12 UTC by PBR_Documentation

Updated 2026-10-26 07:26:12 UTC by PBR_Documentation