

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.

Revision #1

Created 2026-10-26 07:26:17 UTC by PBR_Documentation

Updated 2026-10-26 07:26:17 UTC by PBR_Documentation