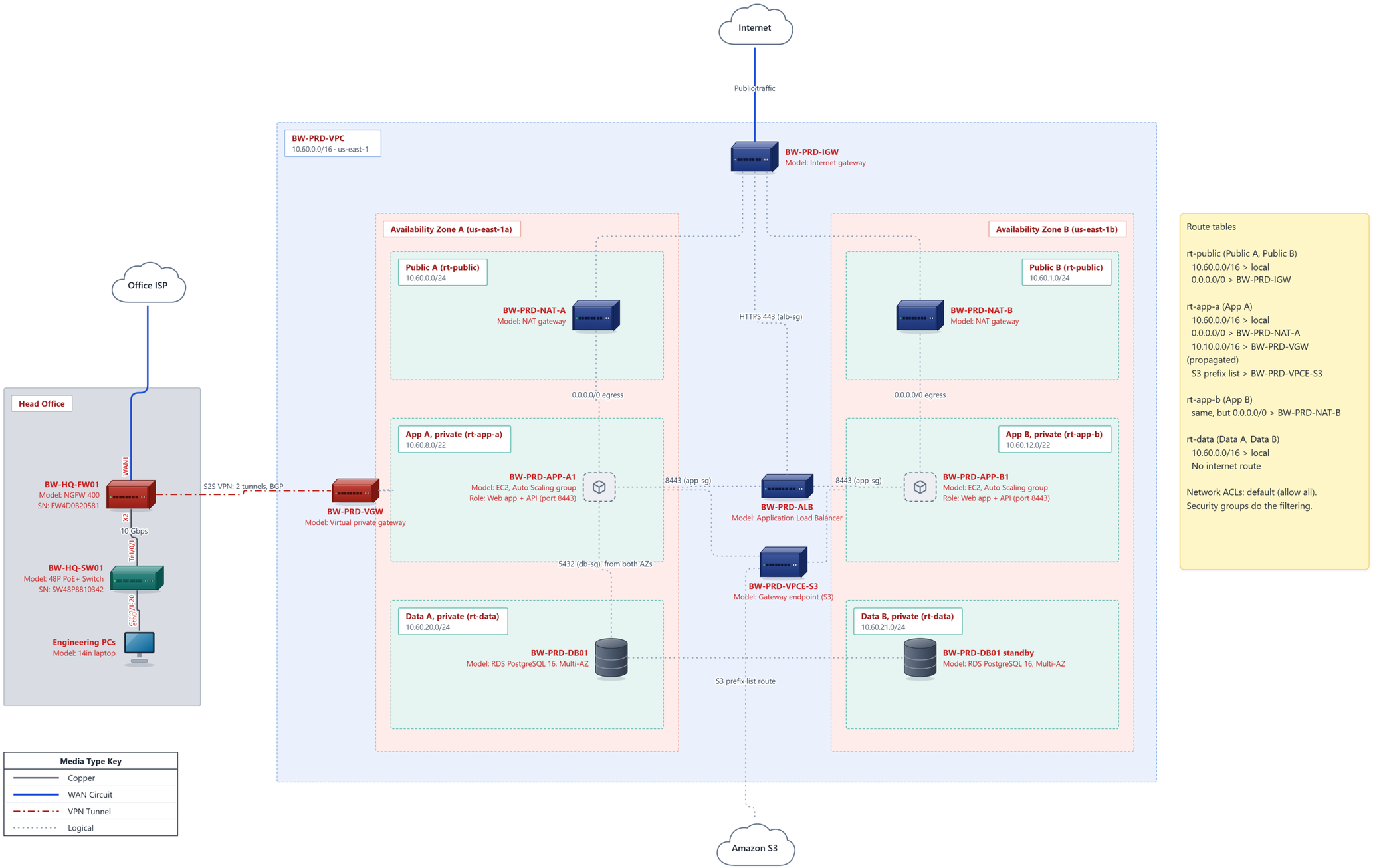

Route tables

rt-public (Public A, Public B)
10.60.0.0/16 > local
0.0.0.0/0 > BW-PRD-IGW

rt-app-a (App A)
10.60.0.0/16 > local
0.0.0.0/0 > BW-PRD-NAT-A
10.10.0.0/16 > BW-PRD-VGW
(propagated)
S3 prefix list > BW-PRD-VPCE-S3

rt-app-b (App B)
same, but 0.0.0.0/0 > BW-PRD-NAT-B

rt-data (Data A, Data B)
10.60.0.0/16 > local
No internet route

Network ACLs: default (allow all).
Security groups do the filtering.

DOCUMENT **Brightwater Analytics - AWS Production VPC** Brightwater Analytics · Production in us-east-1; head office 12 Quay Street, Springfield	SHEET TITLE **Production VPC**	VERSION 1.0	LAST CHANGED 2026-11-25	VERIFIED	SHEET **1** of 5
		DRAWN BY	LAST EDITOR	APPROVED	

Device Inventory 16 devices

Hostname	Type	Vendor / model	Serial	Mgmt IP	Area	Location	Page
Internet	Internet						Production VPC
Office ISP	ISP / Carrier						Production VPC
Amazon S3	Cloud Provider						Production VPC
BW-PRD-IGW	Router	AWS (managed service) Internet gateway			BW-PRD-VPC		Production VPC
BW-PRD-ALB	Load Balancer	AWS (managed service) Application Load Balancer			BW-PRD-VPC		Production VPC
BW-PRD-NAT-A	Router	AWS (managed service) NAT gateway		10.60.0.10	Public A (rt-public)		Production VPC
BW-PRD-NAT-B	Router	AWS (managed service) NAT gateway		10.60.1.10	Public B (rt-public)		Production VPC
BW-PRD-APP-A1	Virtual Machine	AWS (managed service) EC2, Auto Scaling group		10.60.8.21	App A, private (rt-app-a)	us-east-1a	Production VPC
BW-PRD-APP-B1	Virtual Machine	AWS (managed service) EC2, Auto Scaling group		10.60.12.21	App B, private (rt-app-b)	us-east-1b	Production VPC
BW-PRD-DB01	Database	AWS (managed service) RDS PostgreSQL 16, Multi-AZ		10.60.20.30	Data A, private (rt-data)	us-east-1a	Production VPC
BW-PRD-DB01 standby	Database	AWS (managed service) RDS PostgreSQL 16, Multi-AZ		10.60.21.30	Data B, private (rt-data)	us-east-1b	Production VPC
BW-PRD-VPCE-S3	Router	AWS (managed service) Gateway endpoint (S3)			BW-PRD-VPC		Production VPC
BW-PRD-VGW	VPN Gateway	AWS (managed service) Virtual private gateway			BW-PRD-VPC		Production VPC
BW-HQ-FW01	Firewall	Example Networks NGFW 400	FW4D0B20581	10.10.99.1	Head Office	Head office comms room, Rack 1, U10	Production VPC
BW-HQ-SW01	Switch	Example Networks 48P PoE+ Switch	SW48P8810342	10.10.99.2	Head Office	Head office comms room, Rack 1, U8	Production VPC
Engineering PCs	Workstation	Example Computers 14in laptop			Head Office		Production VPC

Link / Cabling Schedule 18 links

Cable ID	End A	Interface	End B	Interface	Media	Speed	VLANs	Length	Test	Label / notes	Page
	Internet		BW-PRD-IGW		WAN Circuit					Public traffic	Production VPC
	BW-PRD-IGW		BW-PRD-ALB		Logical					HTTPS 443 (alb-sg)	Production VPC
	BW-PRD-IGW		BW-PRD-NAT-A		Logical						Production VPC
	BW-PRD-IGW		BW-PRD-NAT-B		Logical						Production VPC
	BW-PRD-ALB		BW-PRD-APP-A1		Logical					8443 (app-sg)	Production VPC
	BW-PRD-ALB		BW-PRD-APP-B1		Logical					8443 (app-sg)	Production VPC
	BW-PRD-APP-A1		BW-PRD-NAT-A		Logical					0.0.0.0/0 egress	Production VPC
	BW-PRD-APP-B1		BW-PRD-NAT-B		Logical					0.0.0.0/0 egress	Production VPC
	BW-PRD-APP-A1		BW-PRD-DB01		Logical					5432 (db-sg), from both AZs	Production VPC
	BW-PRD-DB01		BW-PRD-DB01 standby		Logical						Production VPC
	BW-PRD-VPCE-S3		App A, private (rt-app-a)		Logical						Production VPC
	BW-PRD-VPCE-S3		App B, private (rt-app-b)		Logical						Production VPC
	BW-PRD-VPCE-S3		Amazon S3		Logical					S3 prefix list route	Production VPC
	BW-PRD-VGW		App A, private (rt-app-a)		Logical						Production VPC
	Office ISP		BW-HQ-FW01	WAN1	WAN Circuit						Production VPC
	BW-HQ-FW01		BW-PRD-VGW		VPN Tunnel					S2S VPN: 2 tunnels, BGP	Production VPC
BW-C001	BW-HQ-FW01	X2	BW-HQ-SW01	Te1/0/1	Copper	10 Gbps	10,99	1 m	Pass		Production VPC
BW-D001-020	BW-HQ-SW01	Gi1/0/1-20	Engineering PCs	eth0	Copper		10		Pass		Production VPC

VLAN / Subnet Table 6 VLANs

VLAN	Name	Subnet	Gateway	DHCP scope / helper	Devices	Page
	App A, private (rt-app-a)	10.60.8.0/22	10.60.8.1	AWS DHCP options set (AmazonProvidedDNS)	1	Production VPC
	App B, private (rt-app-b)	10.60.12.0/22	10.60.12.1	AWS DHCP options set (AmazonProvidedDNS)	1	Production VPC
	Data A, private (rt-data)	10.60.20.0/24	10.60.20.1	AWS DHCP options set (AmazonProvidedDNS)	1	Production VPC
	Data B, private (rt-data)	10.60.21.0/24	10.60.21.1	AWS DHCP options set (AmazonProvidedDNS)	1	Production VPC
	Public A (rt-public)	10.60.0.0/24	10.60.0.1	AWS DHCP options set (AmazonProvidedDNS)	1	Production VPC
	Public B (rt-public)	10.60.1.0/24	10.60.1.1	AWS DHCP options set (AmazonProvidedDNS)	1	Production VPC

Data Stores 2 stores

Data store	Stores	Class.	Sensitive data	Encrypted at rest	Kept for	Region	Owner	Boundary
BW-PRD-DB01	Customer accounts, orders	Confidential	Personal info	Yes	Automated backups 14 days	us-east-1	Engineering	
BW-PRD-DB01 standby	Customer accounts, orders	Confidential	Personal info	Yes	Automated backups 14 days	us-east-1	Engineering	