AWS Certified CloudOps Engineer - Associate Cheat Sheet

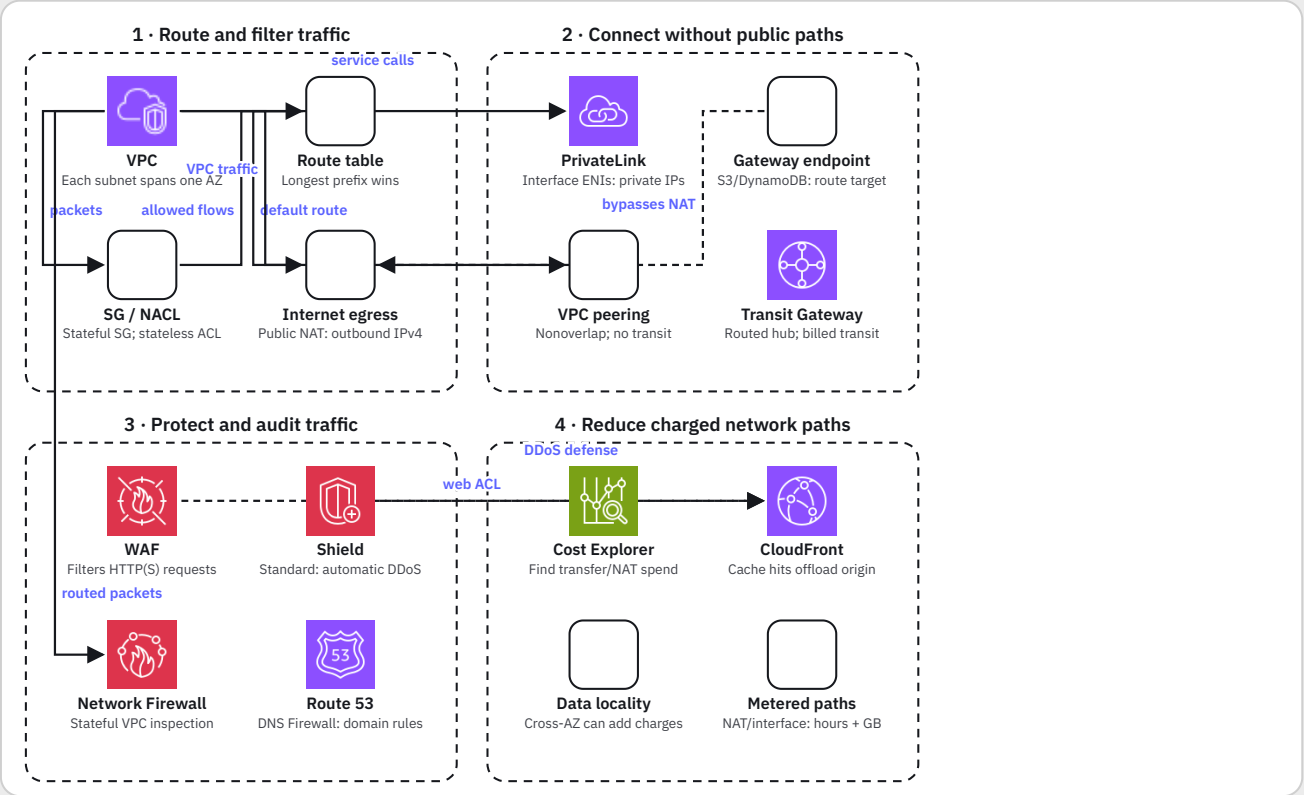
SOA-C03 · Domain 5 of 5

BlowStack

DOMAIN 5 · NETWORKING AND CONTENT DELIVERY · 18% OF THE EXAM · TASK STATEMENT 5.1

Implement and optimize networking features and connectivity

Route, isolate, protect, optimize



1 Route and filter traffic

Public IPv4 needs an IGW route and public address. Private IPv4 internet egress uses public NAT in a public subnet with an IGW route. Outbound-only IPv6 uses an egress-only IGW.

2 Connect without public paths

Interface endpoints use ENIs and security groups; private DNS resolves service names to endpoint IPs when enabled. Gateway endpoints use route tables, not security groups. Transit Gateway provides transitive routing.

3 Protect and audit traffic

AWS Config evaluates **configuration compliance**, not packet contents. Audit WAF, Resolver query, and Network Firewall logs for actions. Network Firewall requires symmetric routing through its endpoints.

4 Reduce charged network paths

Gateway endpoints for S3/DynamoDB have no endpoint charge and bypass NAT. Compare interface endpoint hourly/GB costs. Per-AZ NAT avoids cross-AZ traffic but adds hourly cost; cache hits reduce origin load.

Exam traps

- **Security groups have no deny rules** and automatically permit return traffic. NACLs support allow/deny rules, use first-match rule order, and need explicit return-path rules, including ephemeral ports.
- **PrivateLink is service access**, not full network connectivity; overlapping consumer/provider CIDRs are supported. VPC peering requires nonoverlapping CIDRs and cannot transit another VPC's NAT or IGW.
- **DNS Firewall is not a packet firewall**: it filters Resolver DNS queries, not direct-IP traffic. WAF filters web requests; Shield handles DDoS; Network Firewall inspects traffic routed through it.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

AWS Certified CloudOps Engineer - Associate Cheat Sheet

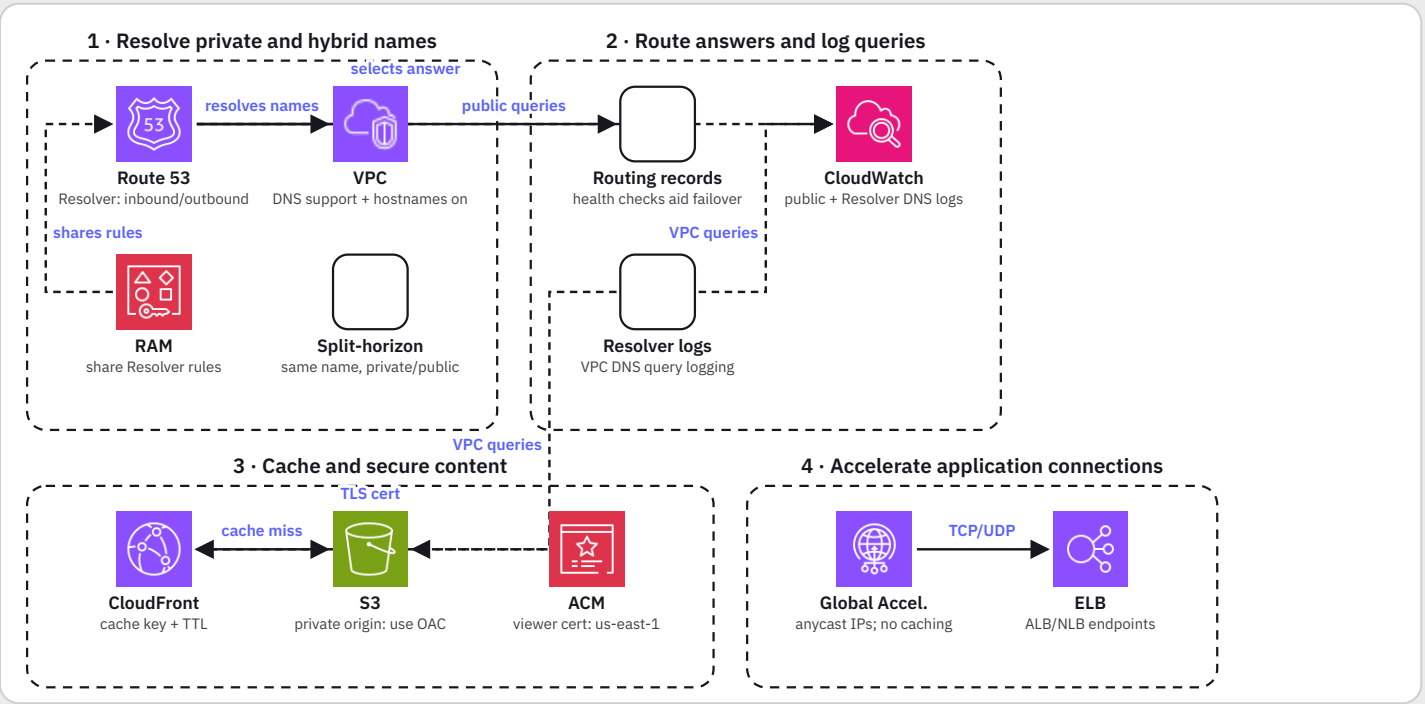
SOA-C03 · Domain 5 of 5

BlowStack

DOMAIN 5 · NETWORKING AND CONTENT DELIVERY · TASK STATEMENT 5.2

Configure domains, DNS services, and content delivery

Resolve, route, cache, accelerate



1 Resolve private and hybrid names

Resolver **inbound** endpoints accept on-premises DNS queries; outbound endpoints and forwarding rules reach on-premises DNS from VPCs. A matching private zone wins; missing records return NXDOMAIN, not public fallback.

2 Route answers and log queries

Use **failover** for active/passive, weighted for traffic splits, latency for lowest-latency Region, and multivalue for up to 8 healthy answers. Public query logs use CloudWatch; Resolver logs support CloudWatch or S3.

3 Cache and secure content

The **cache key** determines reuse through selected headers, cookies, and query strings; forwarding alone does not add them to the key. TTL controls freshness; invalidation or versioned names publish changes.

4 Accelerate application connections

Static anycast IPs favor Global Accelerator for TCP/UDP applications; it neither caches content nor terminates TLS. Health checks steer new connections to healthy endpoints; traffic dials adjust traffic by Region.

Exam traps

- A **zone-apex CNAME** is invalid. Route 53 alias records support the apex and selected AWS targets, including CloudFront distributions and ELB load balancers.
- DNS **failover is not instant**: health detection takes time, and clients can retain an earlier answer until its cached TTL expires.
- **Geolocation** routes by the client's location; geoproximity uses resource locations and optional bias. Neither is latency-based routing, which selects the lowest-latency AWS Region.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

AWS Certified CloudOps Engineer - Associate Cheat Sheet

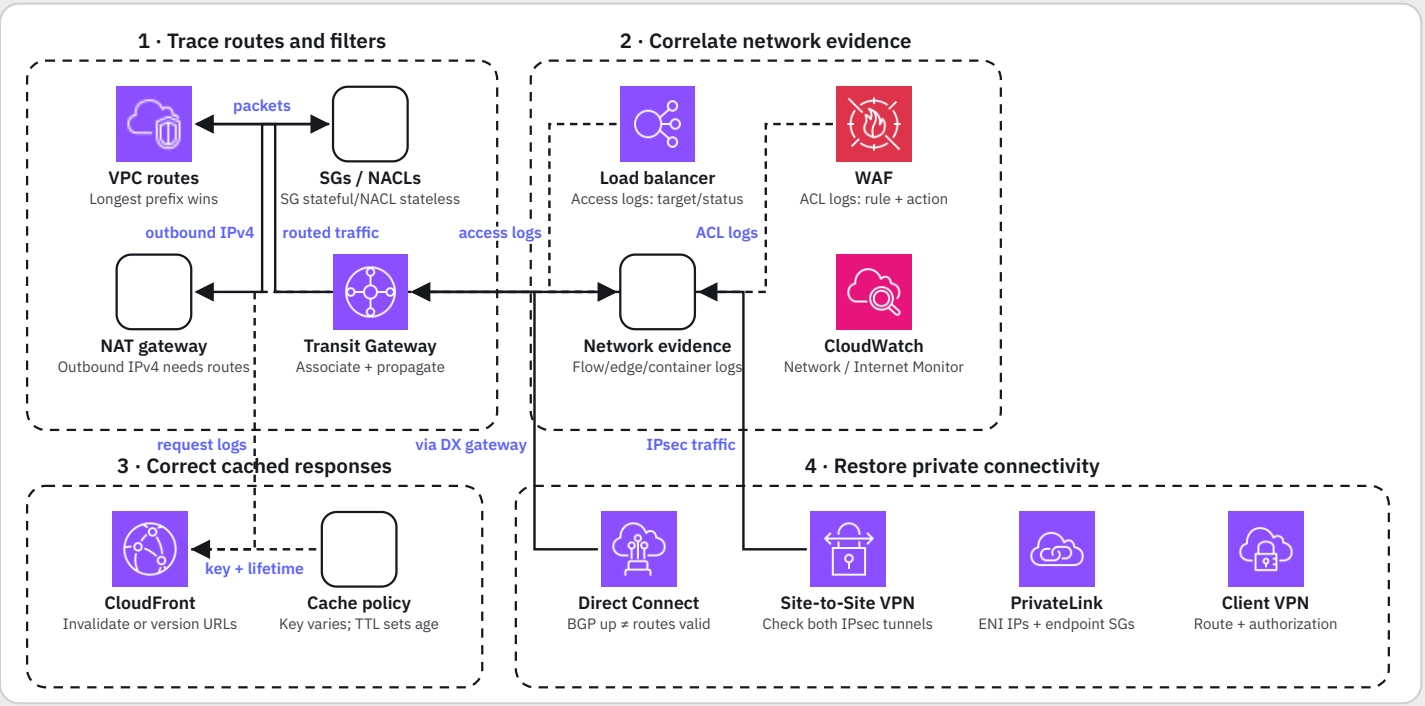
SOA-C03 · Domain 5 of 5

BlowStack

DOMAIN 5 · NETWORKING AND CONTENT DELIVERY · TASK STATEMENT 5.3

Troubleshoot network connectivity issues

Trace, correlate, refresh, reconnect



1 Trace routes and filters

For **timeouts**, check routes both ways, subnet associations, SGs, and NACLs. NACLs need return ephemeral ports; SGs allow replies. TGW attachment association selects its route table; propagation adds routes.

2 Correlate network evidence

Use **Network Monitor** for hybrid RTT/loss probes; Internet Monitor for internet health. Correlate timestamps, 5-tuples, and request IDs across logs; VPC Flow Logs show ACCEPT/REJECT, not payloads.

3 Correct cached responses

For **stale content**, invalidate existing paths or use versioned filenames; lowering TTL does not evict cached objects. Include response-varying query strings, headers, or cookies in the cache key.

4 Restore private connectivity

For **hybrid reachability**, verify nonoverlapping CIDRs, BGP prefixes, and return routes. PrivateLink needs endpoint SG access and correct private DNS resolution; Client VPN needs authorization plus routes.

Exam traps

- A **public NAT gateway** needs an internet gateway route; private subnets need a route to NAT. NAT does not allow unsolicited inbound traffic. Asymmetric paths can break NAT or stateful inspection.
- **Missing logs** do not prove no traffic: logging must be enabled, delivery can lag, and coverage varies. Flow Log ACCEPT means network filters allowed traffic, not that the application answered.
- A **minimum TTL > 0** can cache despite no-cache/no-store/private. An origin request policy forwards values but does not, by itself, add them to the cache key.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

AWS Certified CloudOps Engineer - Associate Cheat Sheet

SOA-C03 · Domain 5 of 5

BlowStack

DOMAIN 5 · NETWORKING AND CONTENT DELIVERY · WHAT TO REMEMBER

Concepts and services of Networking and Content Delivery

Concepts to know

IP Routing

Routes select next hops by destination; **longest-prefix match wins**. Check subnet route-table associations and return paths; an internet gateway route alone does not give an instance internet access.

Stateful and Stateless Filtering

Security groups are stateful, allow-only filters; network ACLs are stateless, ordered allow/deny filters. **Network ACLs must permit return traffic**, including ephemeral ports; security groups automatically permit responses to allowed traffic.

DNS

DNS maps names to endpoints. Use **Resolver inbound endpoints for queries entering VPCs** and outbound endpoints with forwarding rules for queries leaving toward other DNS servers. Private hosted zones provide answers to associated VPCs.

Core services



Amazon VPC

Use **NAT gateways for outbound IPv4** from private subnets and egress-only internet gateways for outbound-only IPv6. Gateway endpoints reach Amazon S3 without NAT; peering is nontransitive.



Amazon Route 53

Use **failover routing for active-passive DNS**, weighted routing for traffic proportions, and latency routing for the lowest-latency Region. DNS caching delays clients receiving changed answers.



Amazon CloudFront

Use **cache keys to separate response variants** and TTLs to control freshness. Invalidate stale objects for urgent updates; versioned filenames bypass old cached objects without invalidation.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate