AWS Certified Advanced Networking - Specialty Cheat Sheet

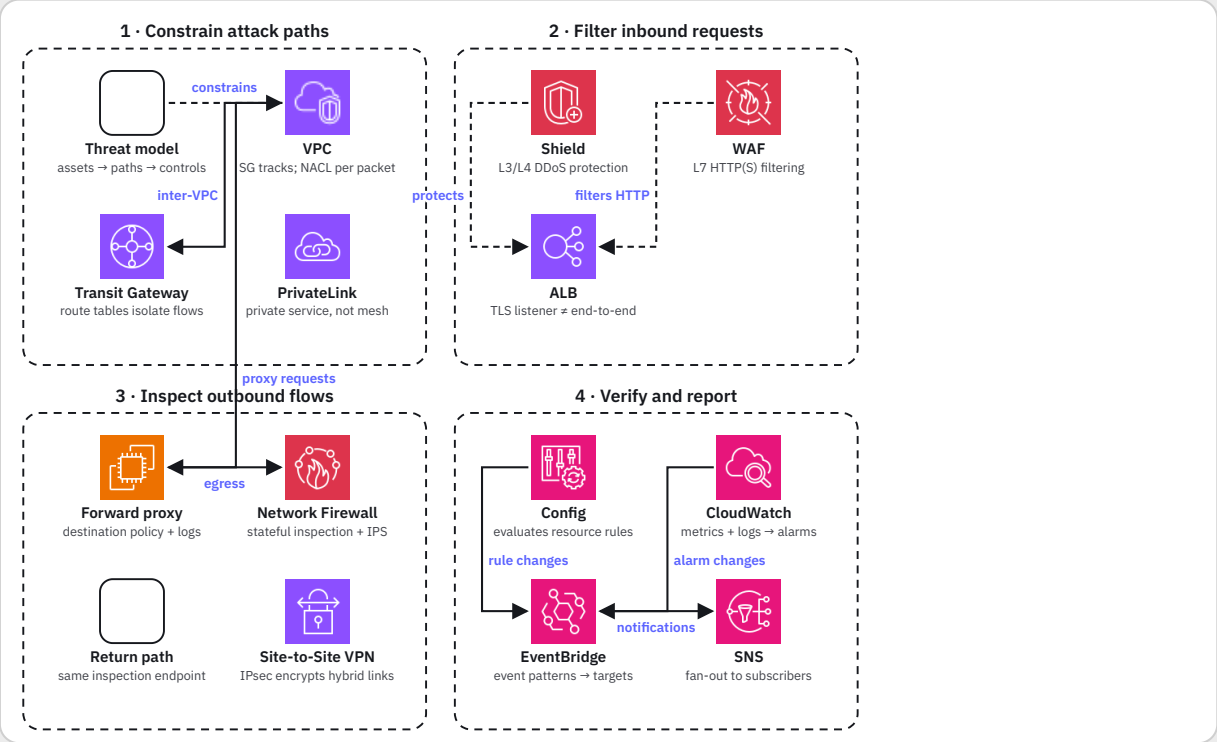
ANS-C01 · Domain 4 of 4

BlowStack

DOMAIN 4 · NETWORK SECURITY, COMPLIANCE, AND GOVERNANCE · 24% OF THE EXAM · TASK STATEMENT 4.1

Implement and maintain network features to meet security and compliance needs and requirements

Model, filter, inspect, verify



1 Constrain attack paths

Trust boundaries determine controls: public APIs need application defenses; pods need workload isolation. Three-tier segmentation and least-privilege rules limit lateral movement; separate subnets alone do not.

2 Filter inbound requests

DDoS vs exploits: Shield Standard is automatic; AWS WAF rules require configuration. ALB TLS termination does not encrypt the target hop; HTTPS targets protect that hop. WAF does not repair vulnerable code.

3 Inspect outbound flows

Symmetric routing keeps stateful inspection working. Routes must steer both directions through the firewall and deny proxy bypass. Transit Gateway appliance mode preserves flow AZ affinity for centralized inspection.

4 Verify and report

Acceptance testing proves behavior, not just configuration. Inject AZ/path failures, measure recovery against RTO, and verify inspection survives. AWS Config compliance alone does not prove failover or application recovery.

Exam traps

- **Detection is not prevention**: Amazon GuardDuty produces threat findings; it does not block packets. AWS WAF filters HTTP requests; AWS Network Firewall inspects routed network traffic.
- **Return traffic differs**: security groups track flows; network ACLs need explicit return rules, including ephemeral ports. Endpoint policies restrict service access; they do not create routes.
- **Central policy is not routing**: AWS Firewall Manager manages supported protections across AWS Organizations accounts; it does not automatically steer traffic through inspection endpoints.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

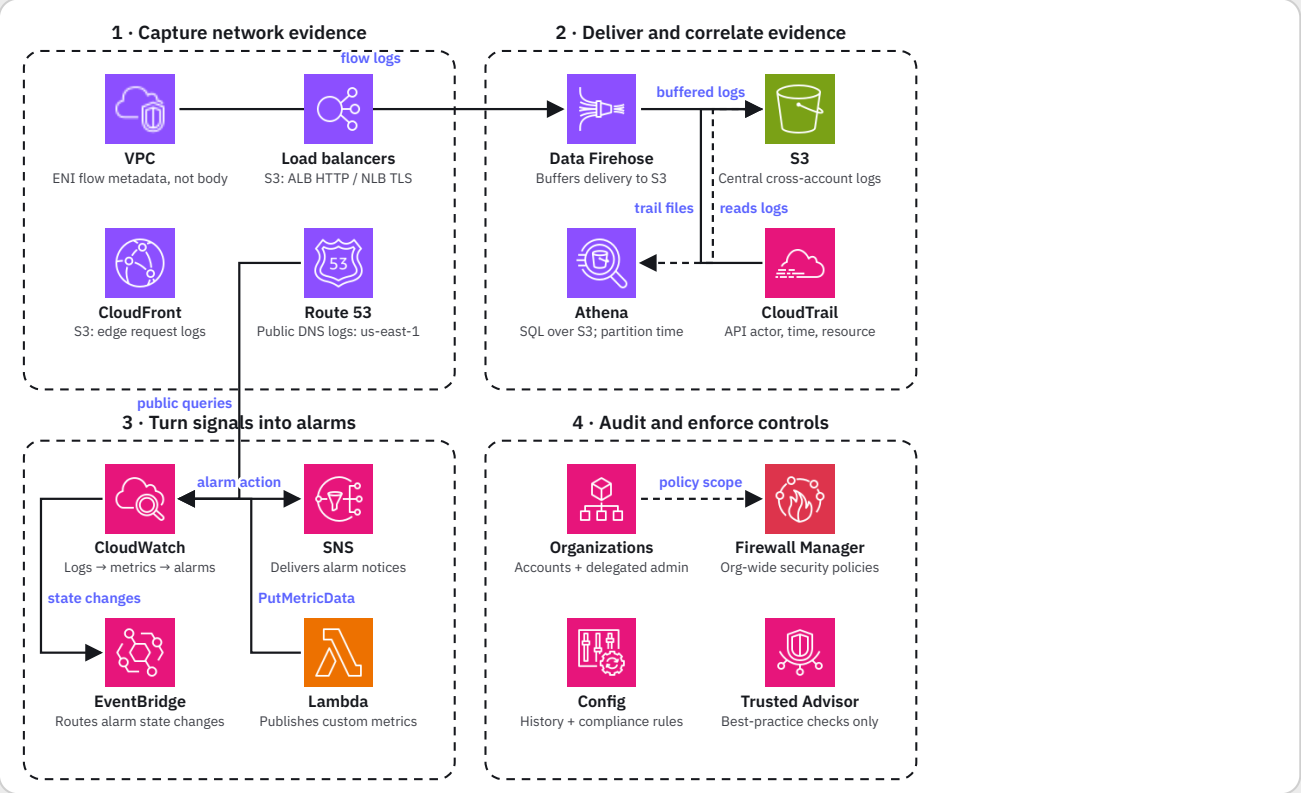
ANS-C01 · Domain 4 of 4

BlowStack

DOMAIN 4 · NETWORK SECURITY, COMPLIANCE, AND GOVERNANCE · TASK STATEMENT 4.2

Validate and audit security by using network monitoring and logging services

Capture, correlate, alert, audit



1 Capture network evidence

Flow Logs include 5-tuple, packets/bytes, start/end, action and log-status; custom formats add tcp-flags, flow-direction and pkt-srcaddr/pkt-dstaddr. Flow and load balancer logging require explicit enablement.

2 Deliver and correlate evidence

Correlate API changes with flow/access logs by event time, account and resource; normalize schemas and allow delivery delays. Cross-account delivery needs IAM grants and destination policies; SSE-KMS also needs key permissions.

3 Turn signals into alarms

Metric alarms evaluate metrics, not raw logs: use metric filters or Lambda. Anomaly Detection learns a baseline; limit dimensions to control metric cardinality. EventBridge routes state changes, not metric thresholds.

4 Audit and enforce controls

Firewall Manager centrally applies supported security policies across Organizations accounts; enable Config recording as required. Config detects drift; remediation needs an action. Policy as Code makes checks repeatable.

Exam traps

- For **packet payloads**, use VPC Traffic Mirroring from supported ENIs to an ENI/NLB target using VXLAN UDP 4789. Flow Logs contain aggregated metadata, not packet captures.
- **REJECT** does not identify the blocking rule. Security groups are stateful; network ACLs are stateless and need return-path rules, including ephemeral ports.
- Route 53 **public query logs** use CloudWatch Logs in us-east-1. Resolver query logs support CloudWatch Logs, S3 or Firehose; VPC Flow Logs also support those three destinations.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

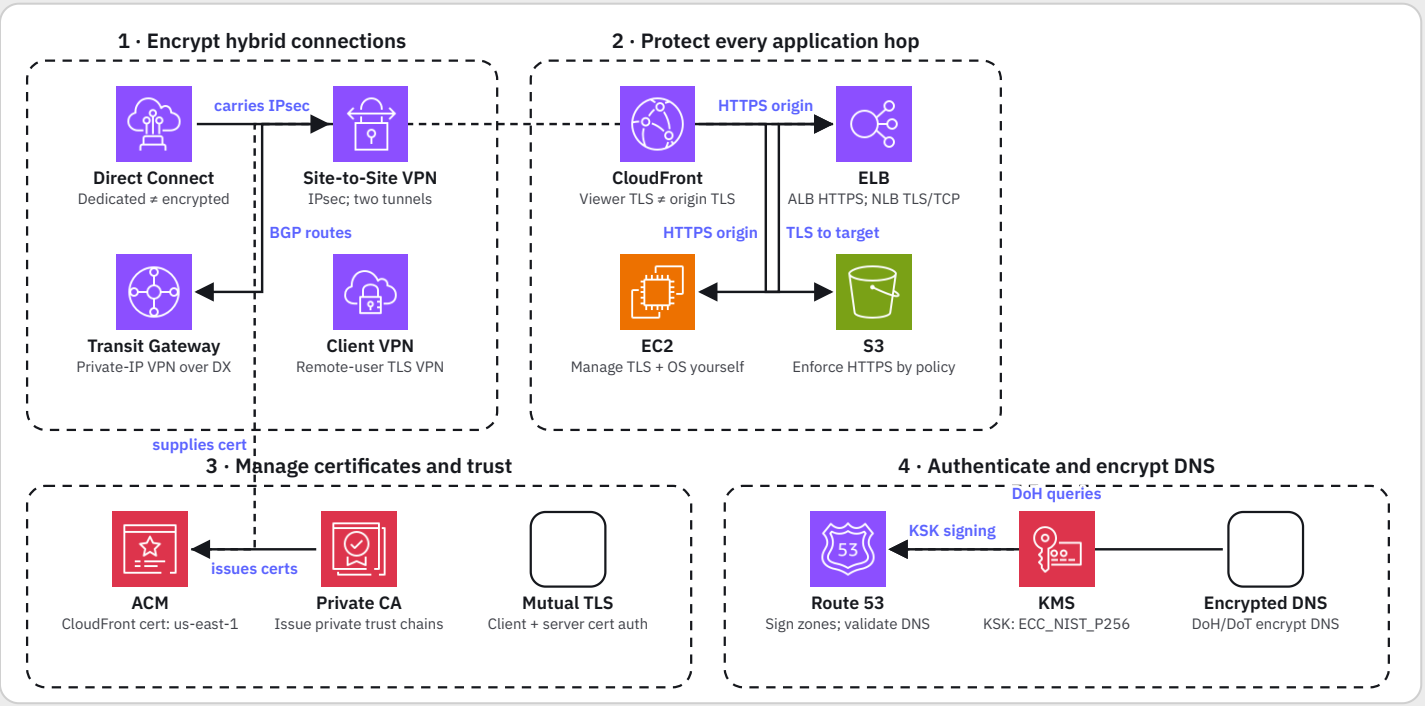
ANS-C01 · Domain 4 of 4

BlowStack

DOMAIN 4 · NETWORK SECURITY, COMPLIANCE, AND GOVERNANCE · TASK STATEMENT 4.3

Implement and maintain confidentiality of data and communications of the network

Encrypt, authenticate, validate, renew



1 Encrypt hybrid connections

Use **IPsec over Direct Connect** for confidentiality: public VPN uses a public VIF; private-IP VPN requires a transit VIF, Direct Connect gateway, and Transit Gateway. BGP exchanges routes; Client VPN uses TLS.

2 Protect every application hop

Enforce **TLS on every hop**: configure CloudFront origin HTTPS and encrypted ELB target connections separately. S3 can deny aws:SecureTransport=false; EC2 TLS, patches, and keys remain customer-managed.

3 Manage certificates and trust

Use **private PKI** for internal identities and mTLS; ALB verify mode validates client certificates against a trust store. ACM renews eligible in-use certificates; exported certificates require redeployment.

4 Authenticate and encrypt DNS

Use **DNSSEC** for signed answers: Route 53 public-zone signing needs a customer-managed KMS key in us-east-1; Resolver validation is separate. DoH/DoT encrypt resolver traffic, not the full DNS resolution path.

Exam traps

- **Direct Connect is not encrypted by default**. MACsec protects supported dedicated links; IPsec protects VPN traffic. BGP exchanges routes but supplies no payload encryption.
- **TLS termination is not end-to-end TLS**. ALB HTTPS targets encrypt without validating target certificates. NLB TCP passthrough preserves client TLS for target-side termination and mTLS.
- **DNSSEC does not encrypt DNS**: signatures provide authenticity and integrity. DoH/DoT provide transport confidentiality; they do not replace DNSSEC or establish authoritative-zone authenticity.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

ANS-C01 · Domain 4 of 4

BlowStack

DOMAIN 4 · NETWORK SECURITY, COMPLIANCE, AND GOVERNANCE · WHAT TO REMEMBER

Concepts and services of Network Security, Compliance, and Governance

Concepts to know

Stateful and Stateless Filtering

Stateful filters track connections; stateless filters evaluate each packet. Security groups automatically permit response traffic; network ACLs require **explicit rules in both directions**, including applicable ephemeral ports.

Encryption in Transit

Encryption protects data on network paths. Choose TLS for application connections or IPsec for network tunnels; **private connectivity does not imply encryption**, and TLS termination leaves subsequent hops needing separate protection.

Network Segmentation

Segmentation separates workloads by trust level and restricts traffic between them. Choose route isolation plus filtering to limit lateral movement; **separate subnets alone are not a security boundary**.

Core services



Amazon VPC

Use **security groups for stateful resource filtering** and network ACLs for stateless subnet filtering. Flow logs show traffic metadata and ACCEPT/REJECT decisions, not packet payloads.



AWS Network Firewall

Use **routed network inspection** for ingress, egress, or inter-VPC traffic. Stateful inspection requires symmetric paths through the same firewall endpoint; deployment alone does not steer traffic.



Amazon CloudWatch

Use **metric filters and alarms** to turn matching log events into threshold-based notifications. AWS CloudTrail records API activity; Amazon CloudWatch evaluates operational metrics and alarms.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty