AWS Certified Security - Specialty Cheat Sheet

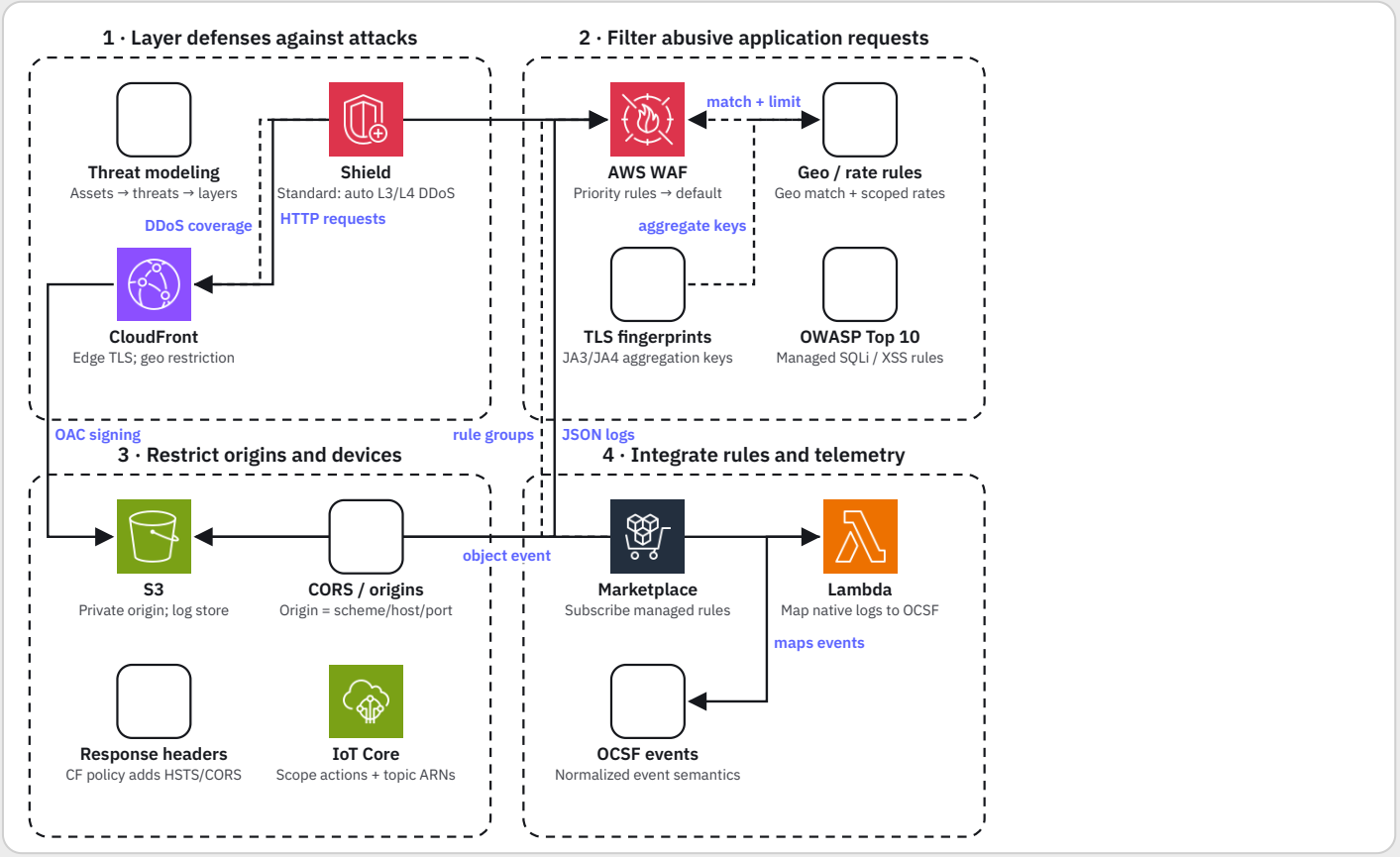
SCS-C03 · Domain 3 of 6

BlowStack

DOMAIN 3 · INFRASTRUCTURE SECURITY · 18% OF THE EXAM · TASK STATEMENT 3.1

Design, implement, and troubleshoot security controls for network edge services

Layer, filter, restrict, normalize



1 Layer defenses against attacks

Defense in depth matches controls to threats: Shield handles L3/L4 DDoS; AWS WAF filters L7 requests. **Shield Advanced** adds paid enhanced protection, response-team access, and eligible DDoS cost protection.

2 Filter abusive application requests

Rate-based rules aggregate by IP or custom keys; scope-down statements select requests to count. Count tests without blocking. WAF geo rules allow selective handling; CloudFront geo restriction covers the distribution.

3 Restrict origins and devices

Prevent origin bypass with S3 Block Public Access, CloudFront OAC, and a distribution-scoped bucket policy. S3 CORS permits selected browser origins, methods, and headers; IoT policies separately enforce least privilege.

4 Integrate rules and telemetry

OCSF is a normalization schema, not native AWS WAF logging. Marketplace subscriptions supply rule groups that must be added to a web ACL. S3 event notifications can invoke AWS Lambda to transform delivered logs.

Exam traps

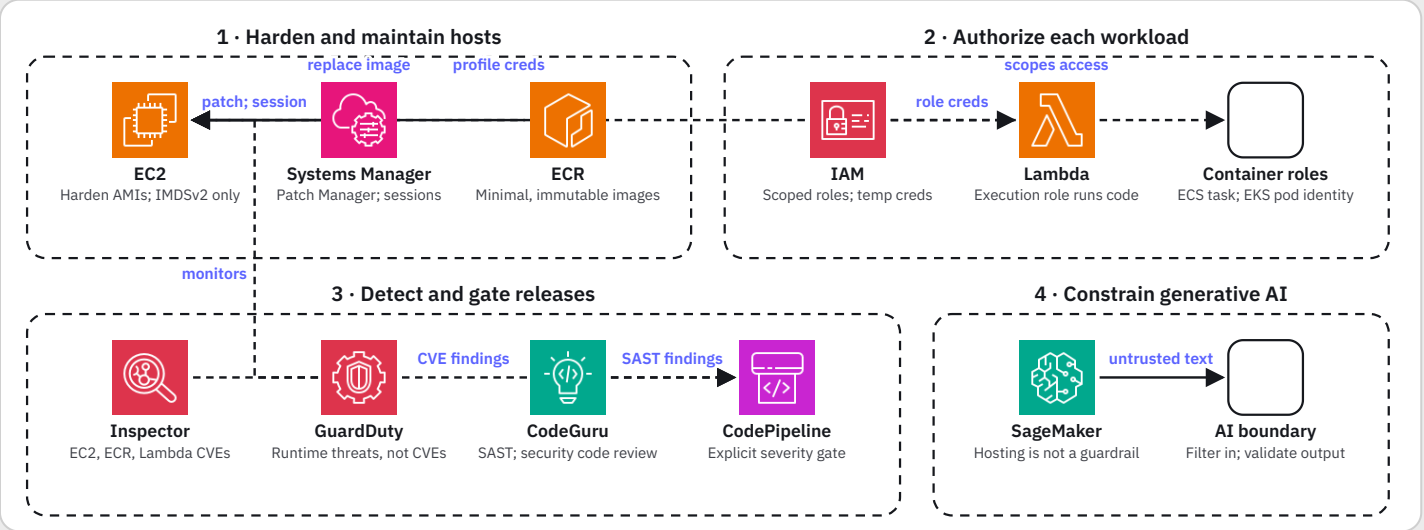
- **CORS is not authorization**: it relaxes browser same-origin checks; it does not block direct HTTP clients or grant access to private S3 objects.
- **WAF is not an OWASP cure**: managed rules reduce exploit traffic, but broken authorization and insecure application design still require application controls.
- **Shield Advanced is not automatic enrollment**: supported resources require protection configuration; automatic application-layer DDoS mitigation must also be enabled where supported.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 3 · INFRASTRUCTURE SECURITY · TASK STATEMENT 3.2

Design, implement, and troubleshoot security controls for compute workloads

Harden, authorize, detect, constrain



1 Harden and maintain hosts

Use **immutable images** for repeatable hardening; test and replace workloads. Patch Manager schedules baseline-driven updates. Session Manager requires SSM Agent, IAM permissions, and HTTPS reachability.

2 Authorize each workload

Use **workload roles**, not keys: EC2 instance profile, Lambda execution role, ECS task role, EKS Pod Identity or IRSA. The ECS task execution role pulls images and sends logs; the task role authorizes application calls.

3 Detect and gate releases

Use **security quality gates** to block releases: integrate SAST and vulnerability findings, define severity thresholds, and fail the stage explicitly. Findings alone do not block deployment; GuardDuty detects runtime behavior.

4 Constrain generative AI

Treat **model output** as untrusted: validate before execution or display, enforce DLP on inputs and outputs, and authorize tool actions outside the model. Retrieved content can carry prompt injection; prompt filters alone are insufficient.

Exam traps

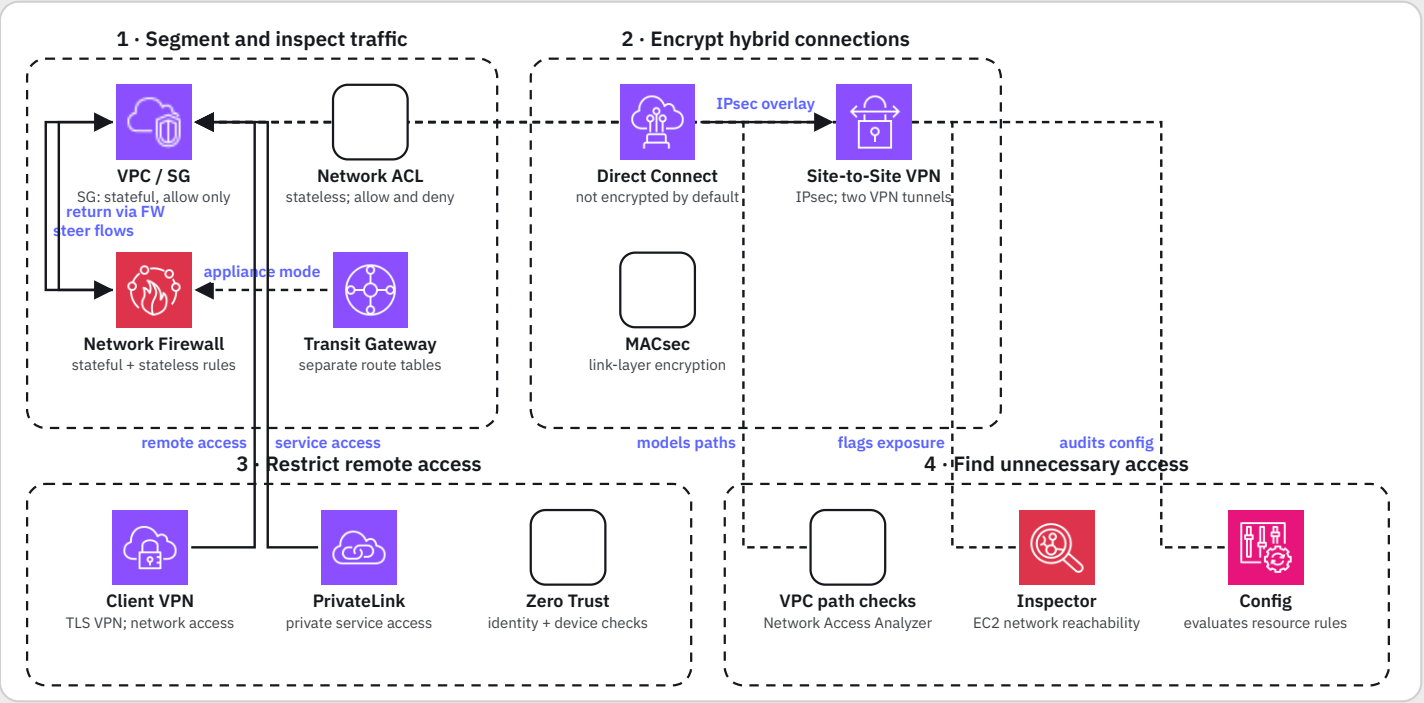
- **Inspector finds; it does not patch.** Patch Manager patches managed EC2 operating systems; customers rebuild vulnerable images and dependencies and update Lambda code or container images.
- **Session Manager needs no inbound SSH**, but requires agent, IAM, and HTTPS connectivity. EC2 Instance Connect supplies short-lived SSH keys; SSH still needs a network path.
- **GuardDuty is not a CVE scanner.** Runtime Monitoring covers supported EC2/ECS/EKS workloads; Lambda Protection analyzes network activity, not Lambda process-level runtime events.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 3 · INFRASTRUCTURE SECURITY · TASK STATEMENT 3.3

Design and troubleshoot network security controls

Segment, inspect, encrypt, restrict, verify



1 Segment and inspect traffic

Use **symmetric routing** for stateful inspection; TGW appliance mode preserves the appliance path. Steer north/south and east/west flows through inspection; separate route tables enforce segmentation.

2 Encrypt hybrid connections

Choose **IPsec** for encrypted hybrid transport over the internet or Direct Connect. MACsec protects supported dedicated connections at the link layer, not the full application path.

3 Restrict remote access

Choose **AWS Verified Access** for identity/device-based application access without a VPN. AWS Client VPN requires routes and authorization; AWS PrivateLink exposes a service, not a routed network.

4 Find unnecessary access

Use **Network Access Analyzer** to find unintended paths from configuration, not packet probes. Inspector reports EC2 exposure; Config evaluates compliance. Remediation must be configured to remove unnecessary access.

Exam traps

- **Return traffic** is automatic for permitted security-group flows, not network ACLs. Stateless ACLs need both directions allowed, including the applicable ephemeral ports.
- A stateless Network Firewall pass action does not invoke stateful inspection. Use **forward to stateful rules** when packets must reach the stateful engine.
- A subnet is not **isolated** merely because workloads lack public IPs. NAT, transit routes, and permissive controls can still allow unwanted outbound or east/west traffic.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 3 · INFRASTRUCTURE SECURITY · WHAT TO REMEMBER

Concepts and services of Infrastructure Security

Concepts to know

Stateful and Stateless Filtering

Security groups track connections; network ACLs evaluate packets independently. Choose **explicit return-path rules** for network ACLs, including ephemeral ports; preserve symmetric routing through stateful inspection.

Least privilege

Grant only required actions, resources, and connectivity. Choose **workload-specific roles with temporary credentials** over embedded keys; distinguish application permissions from permissions used to deploy or operate the workload.

Network Segmentation

Segmentation limits exposure and lateral movement through enforced traffic boundaries. Choose **routes plus filtering** to control east/west and north/south traffic; separate subnets alone do not enforce isolation.

Core services



AWS WAF

Filters HTTP(S) requests. Choose **rate-based rules** for request floods and managed rules for common web exploits; scope rules carefully and test in Count mode before blocking.



Amazon VPC

Choose **security groups** for stateful resource-level access and network ACLs for stateless subnet-level allow/deny rules. Troubleshoot routes and both filtering layers when traffic fails.



AWS Systems Manager

Choose **Session Manager** for administrative access without inbound SSH/RDP ports or bastions; choose Patch Manager to automate OS patching. Managed nodes require IAM permissions and service connectivity.

Get practice exams and lessons for AWS Certified Security - Specialty