Firewalls in AWS Cloud Computing: Detailed Overview

AWS provides a range of firewall and traffic control mechanisms to help secure cloud infrastructure. Each operates at a different layer and is suitable for different use cases. Here's a detailed explanation of all the key firewalls in AWS.

1. Security Groups (SGs)

- Scope: Instance-level (e.g., EC2, RDS, Lambda in VPC)
- Type: Virtual firewall for controlling traffic to AWS resources
- Direction: Inbound and outbound
- Rules: Allow rules only (no deny)
- Stateful: Yes (return traffic is automatically allowed)
- Use Case: Basic firewall to control access to EC2 instances or other resources
- Example: Allow inbound SSH (port 22) from your IP address; allow HTTP (port 80) to the world.

2. Network Access Control Lists (NACLs)

- Scope: Subnet-level
- Type: Stateless firewall for controlling traffic in and out of subnets
- Direction: Inbound and outbound
- Rules: Both allow and deny rules supported
- Stateful: No (responses to allowed requests must also be explicitly allowed)
- Use Case: Block specific IP addresses or provide an extra layer of security alongside security groups
- Example: Deny inbound traffic from a specific IP address range (e.g., 203.0.113.0/24)

3. AWS Network Firewall

- Scope: VPC-level

- Type: Managed, stateful, network-level firewall
- Features:
  - Domain name filtering
  - IP/Port filtering
  - Stateful traffic inspection
  - Integration with Suricata rule engine
- Stateful: Yes
- Use Case: Centralized firewall management across multiple VPCs, enterprise-grade security
- Example: Block access to known malicious domains; allow only specific protocols to flow between subnets

4. AWS WAF (Web Application Firewall)

- Scope: Application-level (Layer 7)
- Applies To:
  - Amazon CloudFront
  - API Gateway
  - Application Load Balancer (ALB)
  - AWS AppSync
- Traffic Type: HTTP/HTTPS only
- Features:
  - Protects against SQL injection, XSS, and other common attacks
  - IP rate limiting
  - Bot control
  - Custom rules based on user-agent, headers, etc.
- Use Case: Protect public-facing web applications

- Example: Block requests with malicious SQL patterns in query strings

5. VPC Traffic Mirroring and VPC Flow Logs

- Note: Not firewalls themselves, but valuable for monitoring and troubleshooting
- VPC Traffic Mirroring:
  - Capture network traffic at the ENI level for inspection
  - Use with third-party IDS/IPS systems
- VPC Flow Logs:
  - Log IP traffic going to and from network interfaces
  - Use for auditing, analysis, and intrusion detection

6. Third-Party Firewalls (Available via AWS Marketplace)

- Vendors: Fortinet, Palo Alto Networks, Check Point, Cisco, etc.
- Use Case: Organizations needing features beyond native AWS firewalls (e.g., advanced threat protection, centralized security management)
- Deployment: As EC2 instances or via AWS Gateway Load Balancer

Summary Comparison Table:

Firewall Type	Level	Stateful	Allow/Deny	Typical Use Case
Security Group	Instance	Yes	Allow only	Basic instance protection
NACL	Subnet	No	Both	Subnet-level access control
AWS Network Firewall	VPC	Yes	Both	Enterprise-grade centralized firewall
AWS WAF	Application	Yes	Both	Protect web apps from Layer 7 attacks

Firewalls in AWS Cloud Computing: Detailed Overview

Third-Party Firewalls	Varies	Depends	Depends	Advanced/Custom firewall capabilities