Day 15

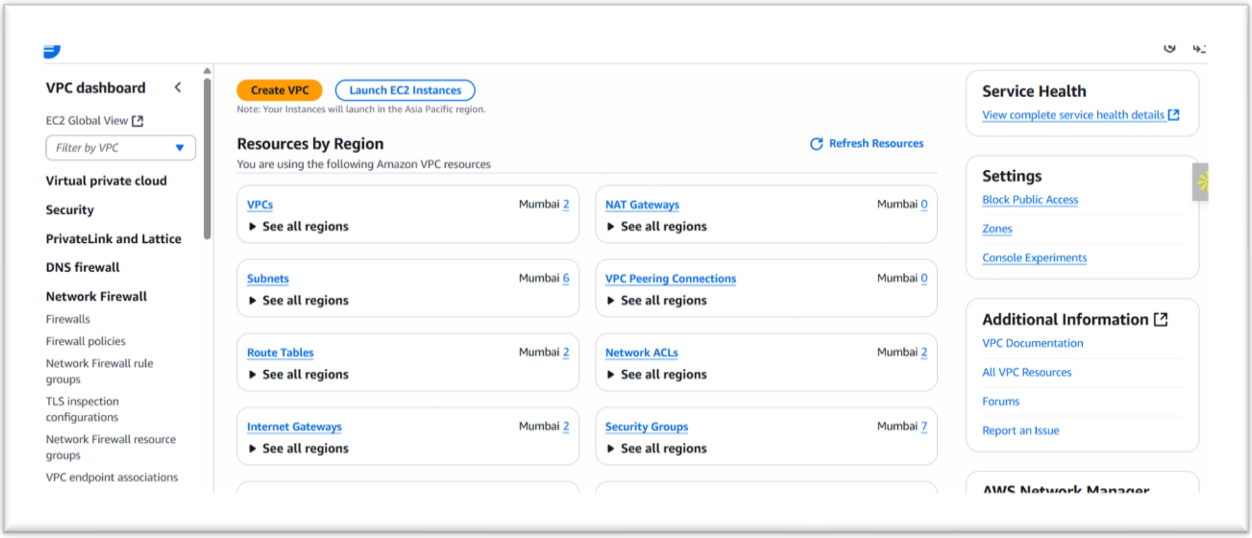
“CLOUD SECURITY”

Securing a VPC using AWS Network Firewall:

1. Advanced Threat Protection: AWS Network Firewall is a managed, stateful firewall that provides intrusion detection and prevention (IDS/IPS), web filtering, and customizable rule enforcement to block unauthorized domains, IPs, and malicious traffic using Suricata.
2. Scalable and Highly Available: It automatically scales with network traffic and supports centralized logging via CloudWatch, S3, or Kinesis for real-time visibility and analysis of firewall activity.
3. Policy-Driven Management: It uses core components — firewalls, firewall policies, and rule groups — allowing administrators to define fine-grained inspection rules and centrally manage security controls across subnets and AZs.

Where can we find this Network Firewall option?

It is under the VPC dashboard, under the subsection named “Network Firewall”.



Note: Your Instances will launch in the Asia Pacific region.

Resources by Region

You are using the following Amazon VPC resources

VPCs — Mumbai 2 — ▶ See all regions

NAT Gateways — Mumbai 0 — ▶ See all regions

Subnets — Mumbai 6 — ▶ See all regions

VPC Peering Connections — Mumbai 0 — ▶ See all regions

Route Tables — Mumbai 2 — ▶ See all regions

Network ACLs — Mumbai 2 — ▶ See all regions

Internet Gateways — Mumbai 2 — ▶ See all regions

Security Groups — Mumbai 7 — ▶ See all regions

Some basic information about this:

What is a firewall?

A firewall is a security system that monitors, filters, and controls incoming and outgoing network traffic based on defined security rules.

Why do we need a firewall?

We need firewalls to:

- Block malicious traffic
- Inspect traffic at deeper layers (e.g., application or packet-level)
- Detect intrusions or attacks (e.g., port scanning, malware communication)
- Enforce fine-grained security policies

Why is it needed if we already have VPC, NACL, and CloudWatch?

- VPC offers isolated networking but not deep packet inspection.
- NACL provides stateless filtering (IP/port-based) at the subnet level.
- Security Groups are stateful, but limited to allow rules.
- CloudWatch is for monitoring and alerting, not filtering.
- Firewall adds deep inspection, intrusion detection/prevention, domain-based filtering, and scalable threat defense — beyond basic access control.

What makes AWS Network Firewall different?

- Uses Suricata for stateful inspection and signature-based threat detection
- Supports domain-based blocking, custom rule sets, and protocol-level filtering
- Integrated with CloudWatch, S3, Kinesis, and Firewall Manager
- Automatically scales with traffic and supports centralized control

What does AWS Network Firewall inspect?

- Source/Destination IPs
- Ports
- Protocols (e.g., TCP, UDP, ICMP)
- Domains (e.g., block bad.com)
- Packet content (deep inspection)

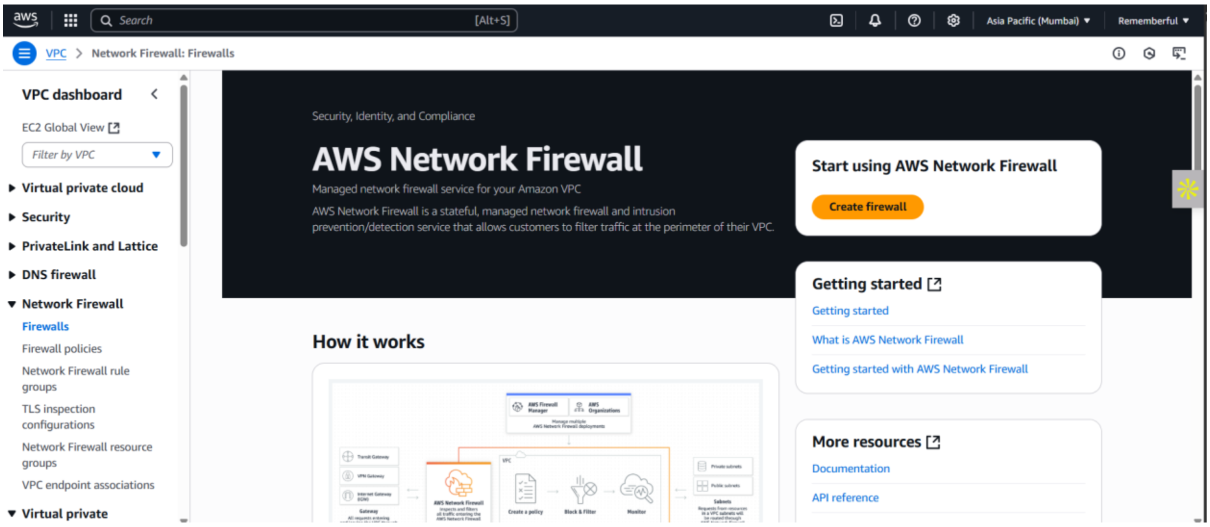
Who should use AWS Network Firewall?

- Enterprises needing **intrusion detection**
- Organizations needing **centralized firewall policies**
- Workloads under **compliance** (e.g., PCI-DSS)
- Security-first deployments requiring **custom traffic rules**

Creating the Network Firewall:

Steps:

Open the “Firewall” tab: following screen will appear.



Security, Identity, and Compliance

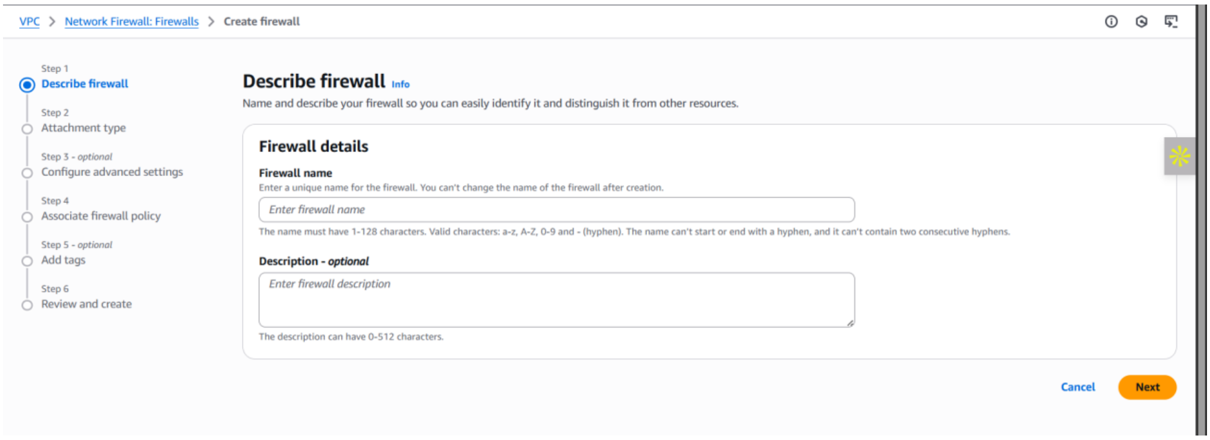
AWS Network Firewall

Managed network firewall service for your Amazon VPC

AWS Network Firewall is a stateful, managed network firewall and intrusion prevention/detection service that allows customers to filter traffic at the perimeter of their VPC.

How it works

Click on the “create firewall” orange coloured button: following screen will appear.



VPC > Network Firewall: Firewalls > Create firewall

Step 1
○ Describe firewall
Step 2
○ Attachment type
Step 3 - *optional*
○ Configure advanced settings
Step 4
○ Associate firewall policy
Step 5 - *optional*
○ Add tags
Step 6
○ Review and create

Describe firewall Info

Name and describe your firewall so you can easily identify it and distinguish it from other resources.

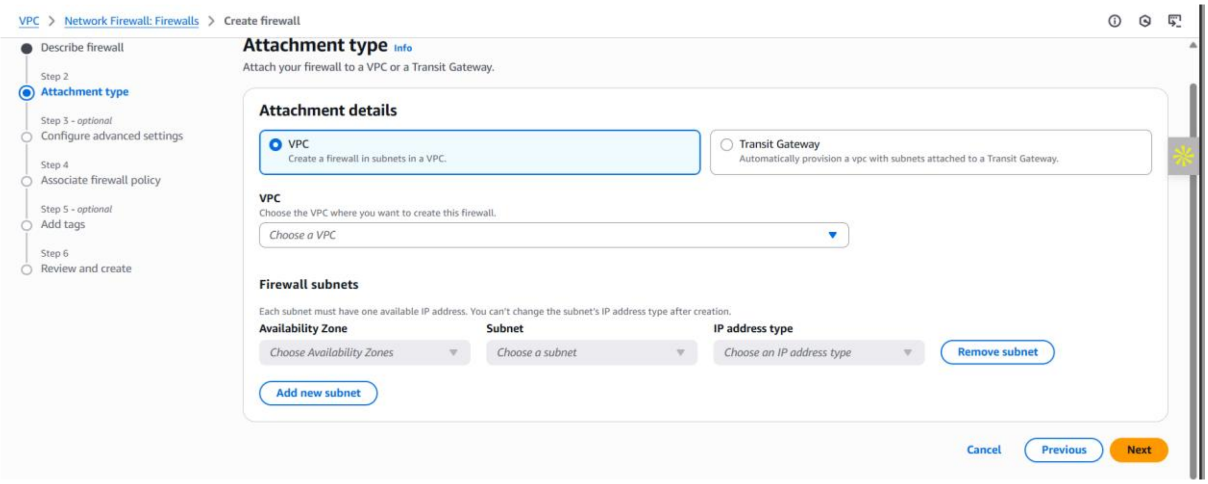
Firewall details

Firewall name
Enter a unique name for the firewall. You can't change the name of the firewall after creation.
Enter firewall name
The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9 and - (hyphen). The name can't start or end with a hyphen, and it can't contain two consecutive hyphens.

Description - *optional*
Enter firewall description
The description can have 0-512 characters.

Cancel   Next

Fill the first appeared “Describe Firewall” section, and move to the “Next”: following screen with the following options will appear.



VPC > Network Firewall: Firewalls > Create firewall

● Describe firewall
Step 2
○ Attachment type
Step 3 - *optional*
○ Configure advanced settings
Step 4
○ Associate firewall policy
Step 5 - *optional*
○ Add tags
Step 6
○ Review and create

Attachment type Info

Attach your firewall to a VPC or a Transit Gateway.

Attachment details

● VPC
Create a firewall in subnets in a VPC.

○ Transit Gateway
Automatically provision a vpc with subnets attached to a Transit Gateway.

VPC
Choose the VPC where you want to create this firewall.
Choose a VPC ▼

Firewall subnets

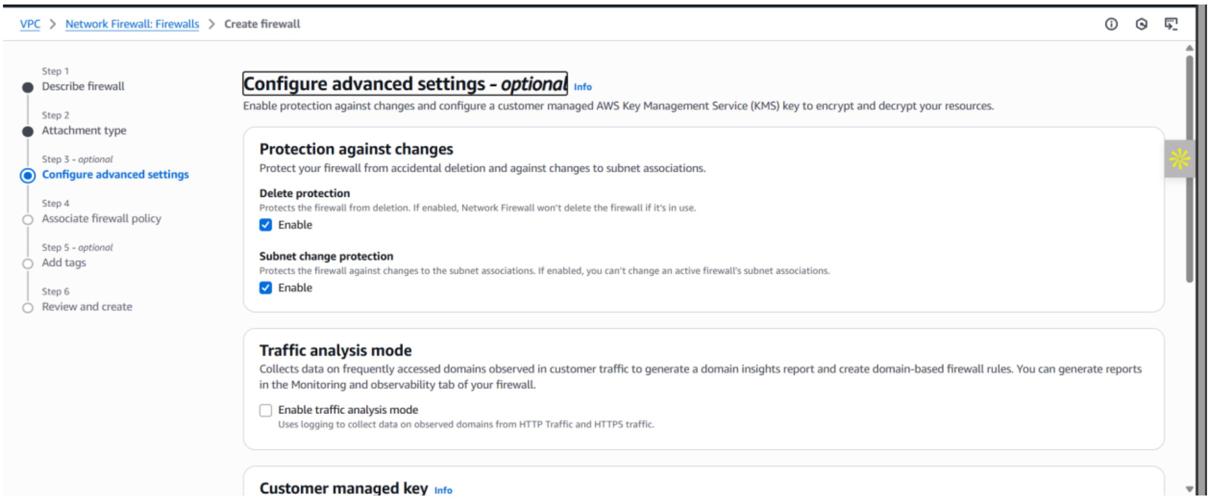
Each subnet must have one available IP address. You can't change the subnet's IP address type after creation.

Availability Zone	Subnet	IP address type	
Choose Availability Zones ▼	*Choose a subnet* ▼	*Choose an IP address type* ▼	Remove subnet

Add new subnet

Cancel   Previous   Next

Fill it, and click on the “Next” button: following screen will appear. Fill and move to the next.



VPC > Network Firewall: Firewalls > Create firewall

Step 1
● Describe firewall
Step 2
● Attachment type
Step 3 - *optional*
○ Configure advanced settings
Step 4
○ Associate firewall policy
Step 5 - *optional*
○ Add tags
Step 6
○ Review and create

Configure advanced settings - *optional* Info

Enable protection against changes and configure a customer managed AWS Key Management Service (KMS) key to encrypt and decrypt your resources.

Protection against changes

Protect your firewall from accidental deletion and against changes to subnet associations.

Delete protection
Protects the firewall from deletion. If enabled, Network Firewall won't delete the firewall if it's in use.
☑ Enable

Subnet change protection
Protects the firewall against changes to the subnet associations. If enabled, you can't change an active firewall's subnet associations.
☑ Enable

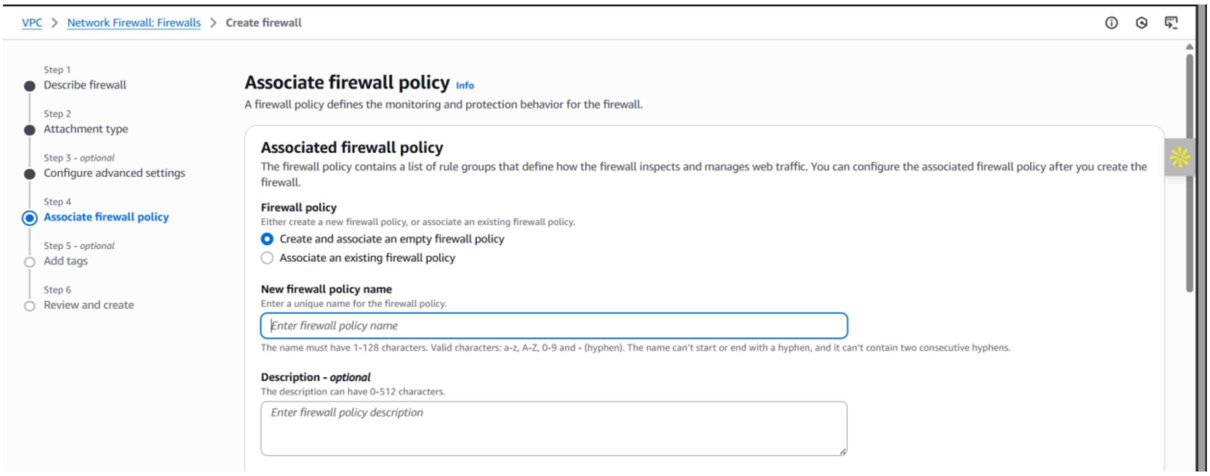
Traffic analysis mode

Collects data on frequently accessed domains observed in customer traffic to generate a domain insights report and create domain-based firewall rules. You can generate reports in the Monitoring and observability tab of your firewall.

☐ Enable traffic analysis mode
Uses logging to collect data on observed domains from HTTP Traffic and HTTPS traffic.

Customer managed key Info

At next, we have to encounter the firewall policy:



VPC > Network Firewall: Firewalls > Create firewall

Step 1
Describe firewall

Step 2
Attachment type

Step 3 - *optional*
Configure advanced settings

Step 4
Associate firewall policy

Step 5 - *optional*
Add tags

Step 6
Review and create

Associate firewall policy Info

A firewall policy defines the monitoring and protection behavior for the firewall.

Associated firewall policy

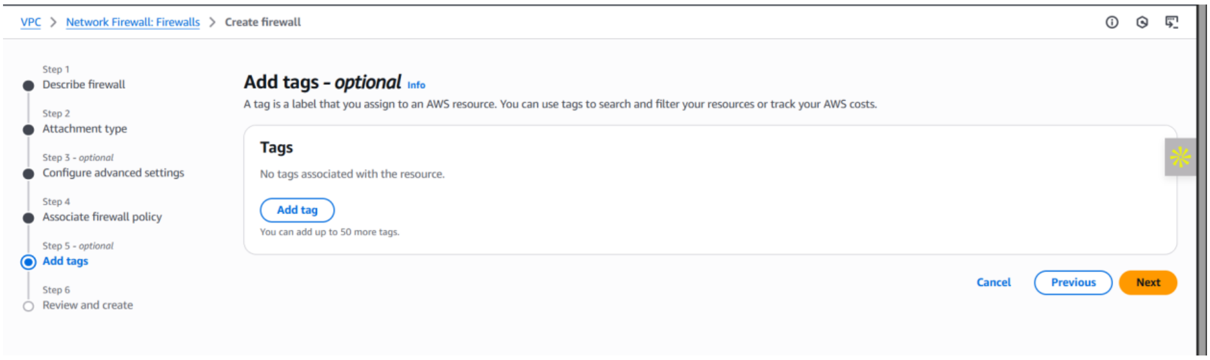
The firewall policy contains a list of rule groups that define how the firewall inspects and manages web traffic. You can configure the associated firewall policy after you create the firewall.

Firewall policy
Either create a new firewall policy, or associate an existing firewall policy.
● Create and associate an empty firewall policy
○ Associate an existing firewall policy

New firewall policy name
Enter a unique name for the firewall policy.
Enter firewall policy name
The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9 and - (hyphen). The name can't start or end with a hyphen, and it can't contain two consecutive hyphens.

Description - *optional*
The description can have 0-512 characters.
Enter firewall policy description

Fill it, and move to the next: add tags if you need.



VPC > Network Firewall: Firewalls > Create firewall

Step 1
Describe firewall

Step 2
Attachment type

Step 3 - *optional*
Configure advanced settings

Step 4
Associate firewall policy

Step 5 - *optional*
Add tags

Step 6
Review and create

Add tags - *optional* Info

A tag is a label that you assign to an AWS resource. You can use tags to search and filter your resources or track your AWS costs.

Tags

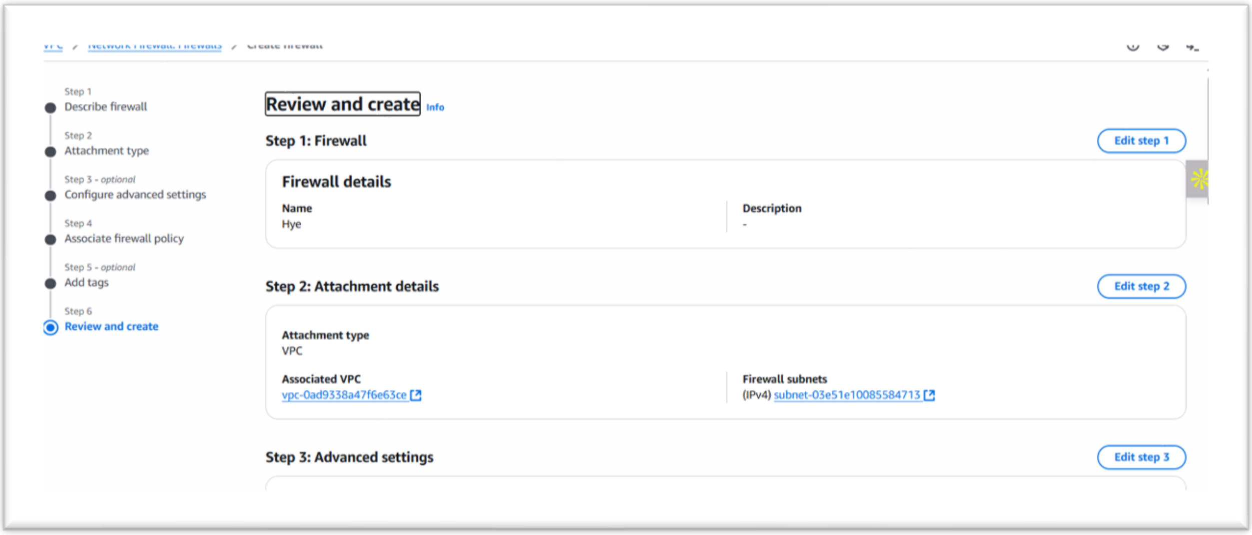
No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel Previous Next

Review and create the firewall in the last step, 'step 6':



Step 1
Describe firewall

Step 2
Attachment type

Step 3 - *optional*
Configure advanced settings

Step 4
Associate firewall policy

Step 5 - *optional*
Add tags

Step 6
Review and create

Review and create Info

Step 1: Firewall Edit step 1

Firewall details

Name
Hye

Description
-

Step 2: Attachment details Edit step 2

Attachment type
VPC

Associated VPC
vpc-0ad9338a47f6e63ce

Firewall subnets
(IPv4) subnet-03e51e10085584713

Step 3: Advanced settings Edit step 3

Best Practices for a Secure Firewall in AWS:

1. Use a Least Privilege Rule Model

- Only allow necessary traffic.
- Deny all other traffic by default.
- Follow the zero-trust principle: no traffic is trusted unless explicitly permitted.

2. Separate Stateless and Stateful Rule Groups

- Use stateless rules to handle high-volume, simple filters (e.g., IP blocks).
- Use stateful rules for deep inspection (e.g., domain blocking, protocol rules, DPI).

3. Update Rule Groups Regularly

- Regularly update signature/rule sets to reflect latest threat intelligence.
- Monitor AWS Managed Rule Groups if integrated with Firewall Manager.

4. Use Domain Filtering

- Block access to malicious domains using DNS domain filtering in stateful rules.
- Enforce allow-listed domains for outbound connections, especially for sensitive workloads.

5. Enable Logging and Monitoring

- Send logs to CloudWatch, S3, or Kinesis Firehose.
- Enable alerting for suspicious patterns like port scans or repeated denials.
- Use CloudTrail to track configuration changes.

6. Test Rules Before Production Deployment

- Use test environments to verify firewall rule behavior.
- Simulate traffic flows to confirm intended behavior (allowed/blocked).

7. Align with Compliance Requirements

- Define rules according to your industry's security frameworks (e.g., PCI DSS, HIPAA).
- Document and audit firewall configurations periodically.

8. Use Firewall Policies Efficiently

- Create centralized policies and reuse them across multiple firewalls in different VPCs.
- Use tag-based access control to manage large deployments.

9. Protect Critical Subnets First

- Place the firewall in public-facing VPC subnets, especially where Internet or VPN/NAT Gateway is involved.
- Use dedicated subnets for firewall endpoints.

10. Integrate with AWS Firewall Manager

- If managing multiple accounts, use AWS Firewall Manager for centralized rule enforcement and compliance across all VPCs.

--The End--