Day-8

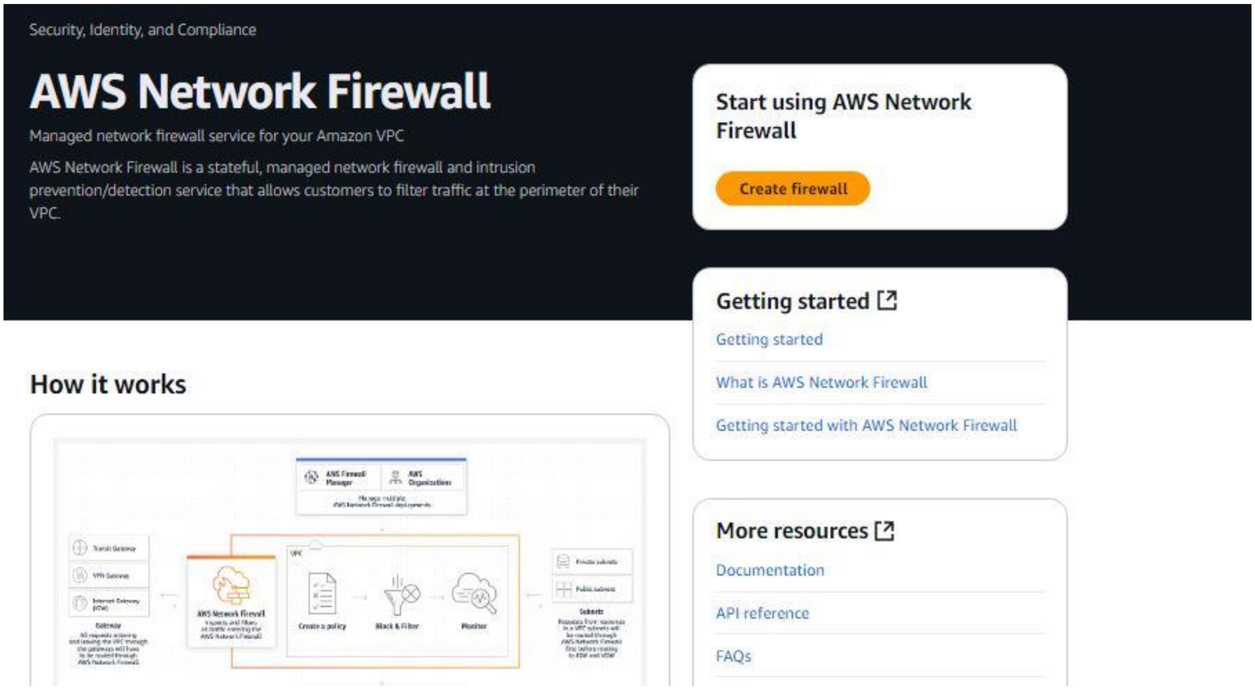
……………………………………….

Today I got brief information of AWS Network Firewall and its purpose, how to apply policies, and how it the First wall of defense from unauthorized accessed to your VPC. Also did a task on how to calculate the pricing for enabling Network Firewall with different criteria's. All of the information's are given as follows:

AWS Network Firewall:

AWS Network Firewall is a managed firewall service that helps you protect your Amazon Virtual Private Cloud (VPC) from unauthorized access and malicious traffic. It provides network traffic filtering and security capabilities for your VPC perimeter, allowing you to create custom rules to inspect and control the traffic in your VPC.
It offers advanced security with deep packet inspection and stateful traffic filtering to detect and block malicious traffic. It is highly scalable, automatically adjusting to varying network traffic levels. The service also integrates seamlessly with AWS services like CloudWatch for monitoring and AWS WAF for enhanced web protection, providing a robust, multi-layered security solution.

Firewall Dashboard:



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.

Start using AWS Network Firewall

Create firewall

Getting started

Getting started

What is AWS Network Firewall

Getting started with AWS Network Firewall

More resources

Documentation

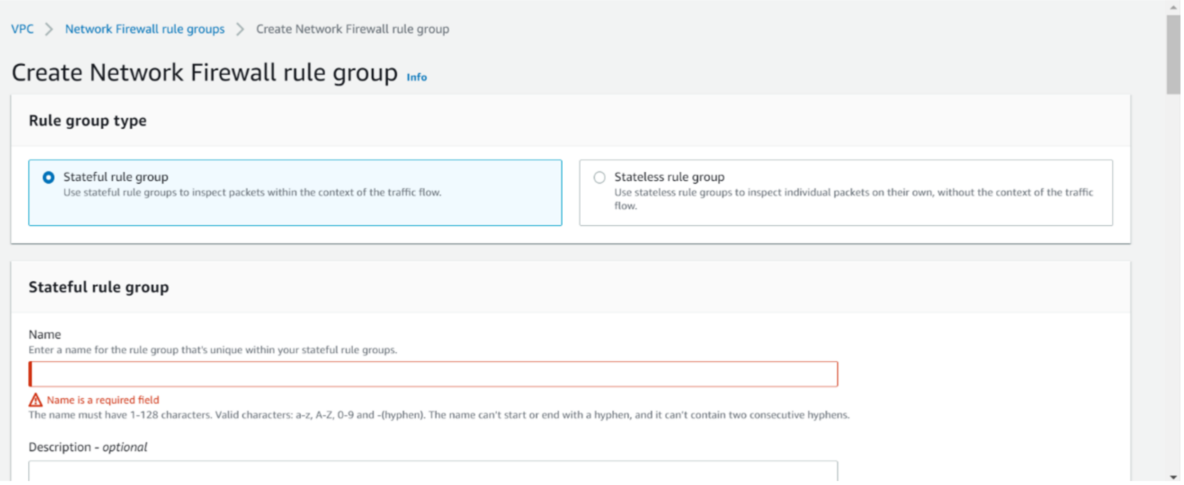
API reference

FAQs

How it works

AWS Firewall Manager
AWS Organizations
Manage multiple AWS Network Firewall deployments
Transit Gateway
VPN Gateway
Internet Gateway (IGW)
Gateway
All requests entering and leaving the VPC through the gateways will have to be routed through AWS Network Firewall
AWS Network Firewall
Inspects and filters all traffic entering the AWS Network Firewall
VPC
Create a policy
Block & Filter
Monitor
Private subnets
Public subnets
Subnets
Requests from resources in a VPC subnets will be routed through AWS Network Firewall first before routing to IGW and VGW

Create a Rule Group:



VPC > Network Firewall rule groups > Create Network Firewall rule group

Create Network Firewall rule group Info

Rule group type

● Stateful rule group
Use stateful rule groups to inspect packets within the context of the traffic flow.

○ Stateless rule group
Use stateless rule groups to inspect individual packets on their own, without the context of the traffic flow.

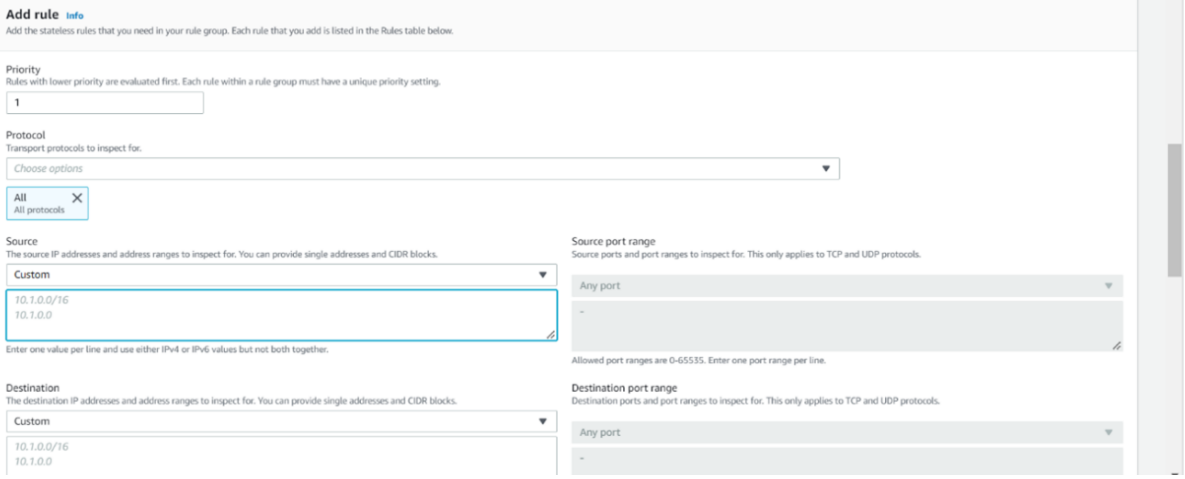
Stateful rule group

Name
Enter a name for the rule group that's unique within your stateful rule groups.

⚠ Name is a required field
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*

Add Rule:



Add rule Info
Add the stateless rules that you need in your rule group. Each rule that you add is listed in the Rules table below.

Priority
Rules with lower priority are evaluated first. Each rule within a rule group must have a unique priority setting.
1

Protocol
Transport protocols to inspect for.
Choose options ▼
All ✕
All protocols

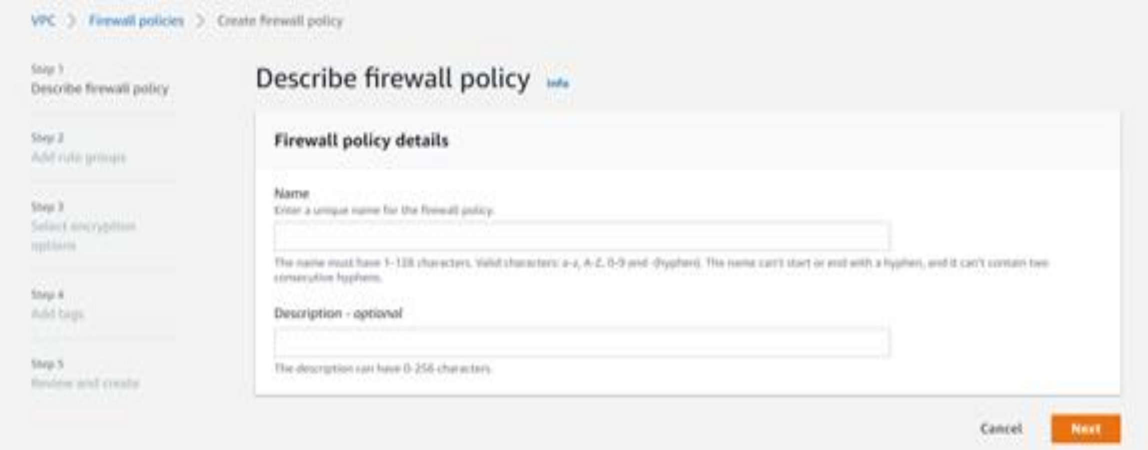
Source
The source IP addresses and address ranges to inspect for. You can provide single addresses and CIDR blocks.
Custom ▼
10.1.0.0/16
10.1.0.0
Enter one value per line and use either IPv4 or IPv6 values but not both together.

Source port range
Source ports and port ranges to inspect for. This only applies to TCP and UDP protocols.
Any port ▼
-
Allowed port ranges are 0-65535. Enter one port range per line.

Destination
The destination IP addresses and address ranges to inspect for. You can provide single addresses and CIDR blocks.
Custom ▼
10.1.0.0/16
10.1.0.0

Destination port range
Destination ports and port ranges to inspect for. This only applies to TCP and UDP protocols.
Any port ▼
-

Create a Rule Group:



VPC > Firewall policies > Create firewall policy

Step 1
Describe firewall policy

Step 2
Add rule groups

Step 3
Select encryption options

Step 4
Add tags

Step 5
Review and create

Describe firewall policy Info

Firewall policy details

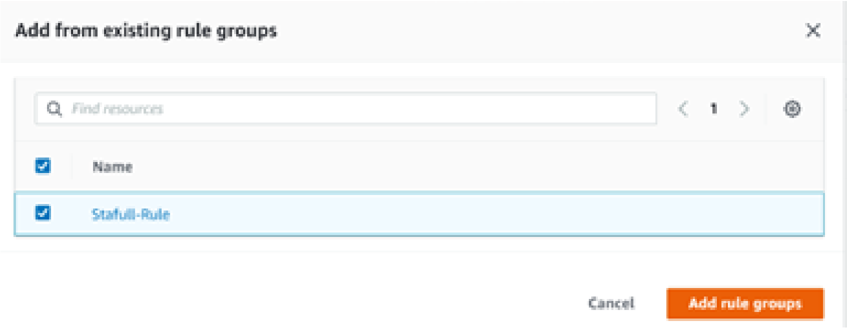
Name
Enter a unique name for the firewall policy.

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*

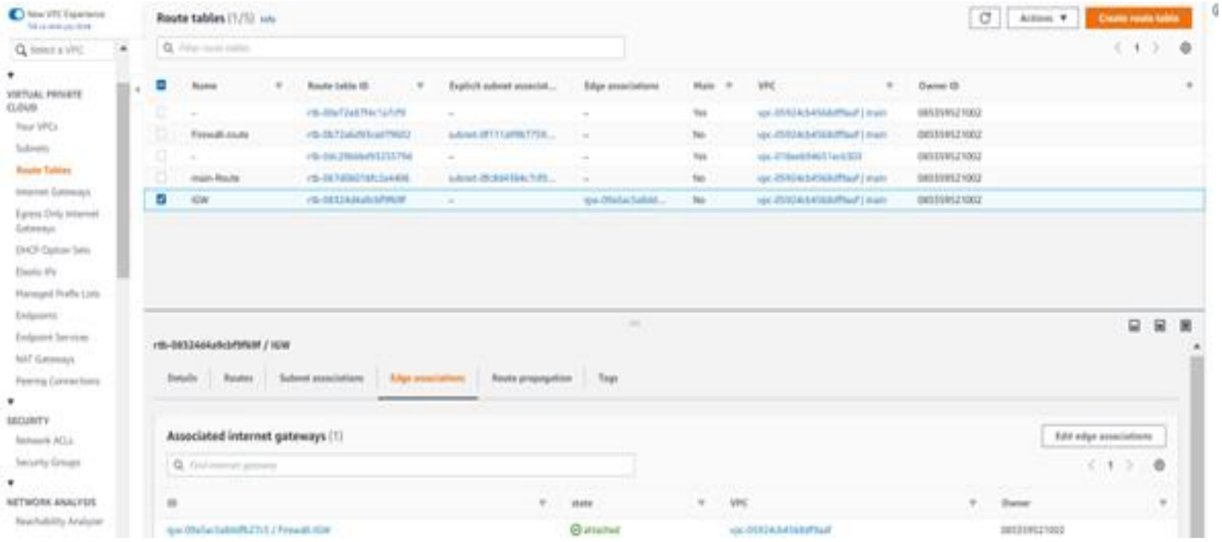
The description can have 0-256 characters.

Attach rule group to Firewall Policy:



☑	Name
☑	Stafull-Rule

Configure Rote table to Firewall:



Route tables (1/5) Info

☑	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
□	–	[illegible]	–	–	Yes	[illegible] | main	[illegible]
□	Firewall-route	[illegible]	subnet-[illegible]...	–	No	[illegible] | main	[illegible]
□	–	[illegible]	–	–	Yes	[illegible]	[illegible]
□	main-Route	[illegible]	subnet-[illegible]...	–	No	[illegible] | main	[illegible]
☑	IGW	[illegible]	–	igw-[illegible]...	No	[illegible] | main	[illegible]

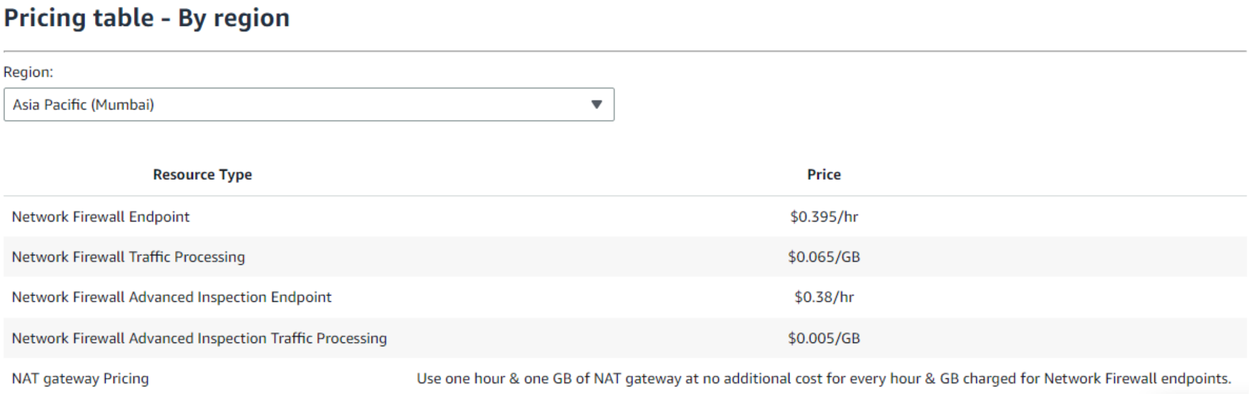
[illegible] / IGW

Associated internet gateways (1)

ID	state	VPC	Owner
igw-[illegible] / Firewall-IGW	attached	vpc-[illegible]	[illegible]

And this is how one can create an configure a Network Firewall. You can create multiple rule groups for assigning specific rules to specific VPC as per the need. This makes managing the cloud easy and keeps it more secure.

The pricing to use the firewall with the specifications and needs with outbound are publically available on: Here . Example of Asia Pacific (Mumbai)



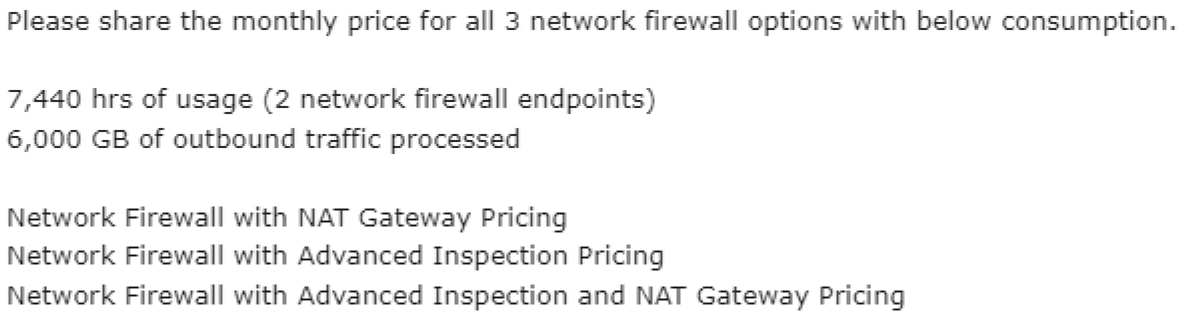
Pricing table - By region

Region:

Asia Pacific (Mumbai) ▼

Resource Type	Price
Network Firewall Endpoint	$0.395/hr
Network Firewall Traffic Processing	$0.065/GB
Network Firewall Advanced Inspection Endpoint	$0.38/hr
Network Firewall Advanced Inspection Traffic Processing	$0.005/GB
NAT gateway Pricing	Use one hour & one GB of NAT gateway at no additional cost for every hour & GB charged for Network Firewall endpoints.

The task given to me was as follows:

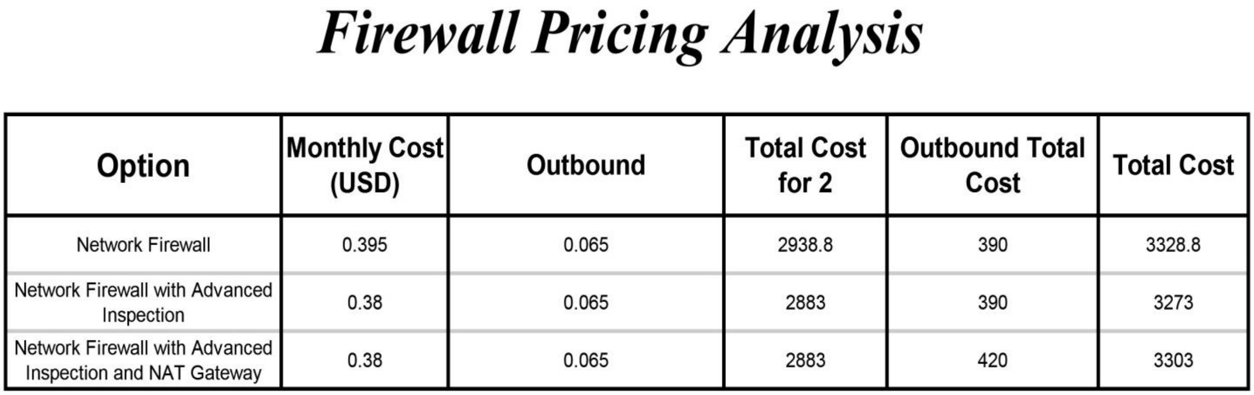


Please share the monthly price for all 3 network firewall options with below consumption.

7,440 hrs of usage (2 network firewall endpoints)
6,000 GB of outbound traffic processed

Network Firewall with NAT Gateway Pricing
Network Firewall with Advanced Inspection Pricing
Network Firewall with Advanced Inspection and NAT Gateway Pricing

Solution:



Firewall Pricing Analysis

Option	Monthly Cost (USD)	Outbound	Total Cost for 2	Outbound Total Cost	Total Cost
Network Firewall	0.395	0.065	2938.8	390	3328.8
Network Firewall with Advanced Inspection	0.38	0.065	2883	390	3273
Network Firewall with Advanced Inspection and NAT Gateway	0.38	0.065	2883	420	3303