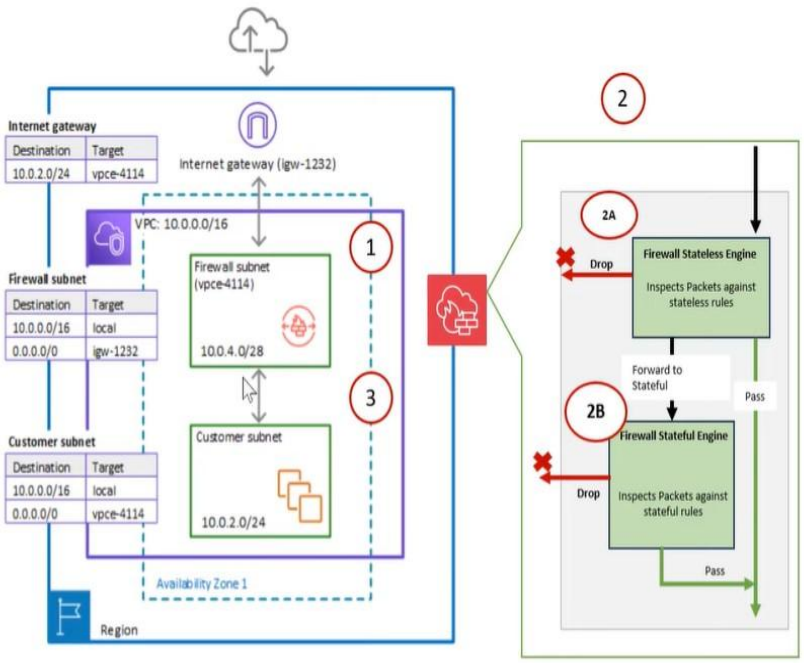
AWS NETWORK FIREWALL DEMO LAB

Demo Steps

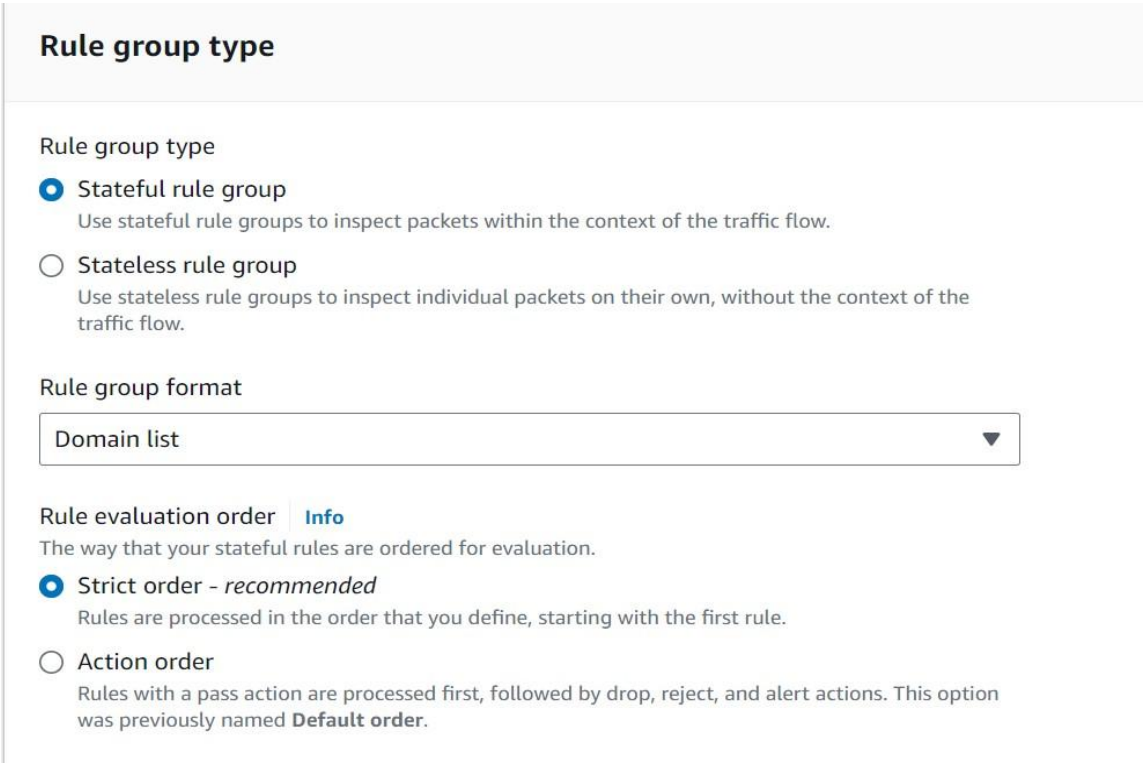
- Create a VPC, Name Firewall Lab VPC – CIDR 10.0.0.0/16
- Create one Workload Subnet (Public) – 10.0.2.0/24
- Create a Security group to allow RDP, HTTP/s, ICMP traffic to the instance.
- Create and attach an Internet GW to VPC
- Create a route table for Workload Subnet to send internet traffic to Internet GW
- Launch an EC2 web Server Instance and check domains accessibility.
- Now Create Firewall Subnet – CIDR 10.0.4.0/28
- Create Stateful Rule Group (domain list) – to block traffic to few sites.
- Create Stateless Rule Group for ICMP and RDP Traffic
- Change the routing for traffic to move through the firewall subnet
- Test the functionality of AWS Network Firewall.

AWS Network Firewall: Traffic Flow



STEP 1:- Created a VPC with firewall and public subnet.
Created 2 Route table attach each with subnet.
Created Internet Gateway and attach to the VPC.
Launch an EC2 Instance in the Public Subnet.

STEP 2 :- Created Rule Group in Network Firewall Section.



Rule group details

Name

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

Rule1

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*

This description appears when you view this rule group's details. It can help you quickly identify what your rule group is used for.

Enter rule group description

The description can have 0-256 characters.

Capacity Info

The number of rules you expect to have in this rule group during its lifetime. You can't change capacity after rule group creation, so leave room to grow.

1000

The capacity must be greater than or equal to 1 and less than 30,000.

Configure rules Info

An AWS Network Firewall rule group is a reusable set of criteria for inspecting and handling network traffic.

Domain list rule Info

Allow or deny traffic based on the domain name list.

Domain names

List the domain names you want to inspect and either allow or deny.

www.google.com

Enter one domain name per line.

CIDR ranges

The source traffic CIDR ranges to inspect.

- (•) Default
  Use the CIDR range of the VPC where Network Firewall is deployed.
- ( ) Custom
  Set your own list of CIDR ranges.

Protocols

The protocols to inspect.

- [x] HTTP
- [x] HTTPs

Action Info

Action to take when a request matches the domain names in this group.

- ( ) Allow
- (•) Deny

Rule group type

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.

Cancel Next

Rule group details

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

rule2

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*
This description appears when you view this rule group's details. It can help you quickly identify what your rule group is used for.

Enter rule group description

The description can have 0-256 characters.

Capacity Info
The number of rules you expect to have in this rule group during its lifetime. You can't change capacity after rule group creation, so leave room to grow.

1000

The capacity must be greater than or equal to 1 and less than 30,000.

Cancel Previous Next

Stateless 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.

100

Protocol

Transport protocols to inspect for.

Choose options

RDP
Protocol: 27

ICMP
Protocol: 1

Source

The source IP addresses and address ranges to inspect for. You can provide single addresses and CIDR blocks.

Any IPv4 address

0.0.0.0/0

Enter one value per line and use either IPv4 or IPv6 values but not both together.

Source port range

The source ports and port ranges to inspect for. This only applies to TCP and UDP protocols.

Any port

10:1000

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
2001:db8:2de::e13

Enter one value per line and use either IPv4 or IPv6 values but not both together.

Destination port range

The destination ports and port ranges to inspect for. This only applies to TCP and UDP protocols.

Any port

10:1000

Allowed port ranges are 0-65535. Enter one port range per line.

The following table lists all of your rule groups.

Your rule groups (2)

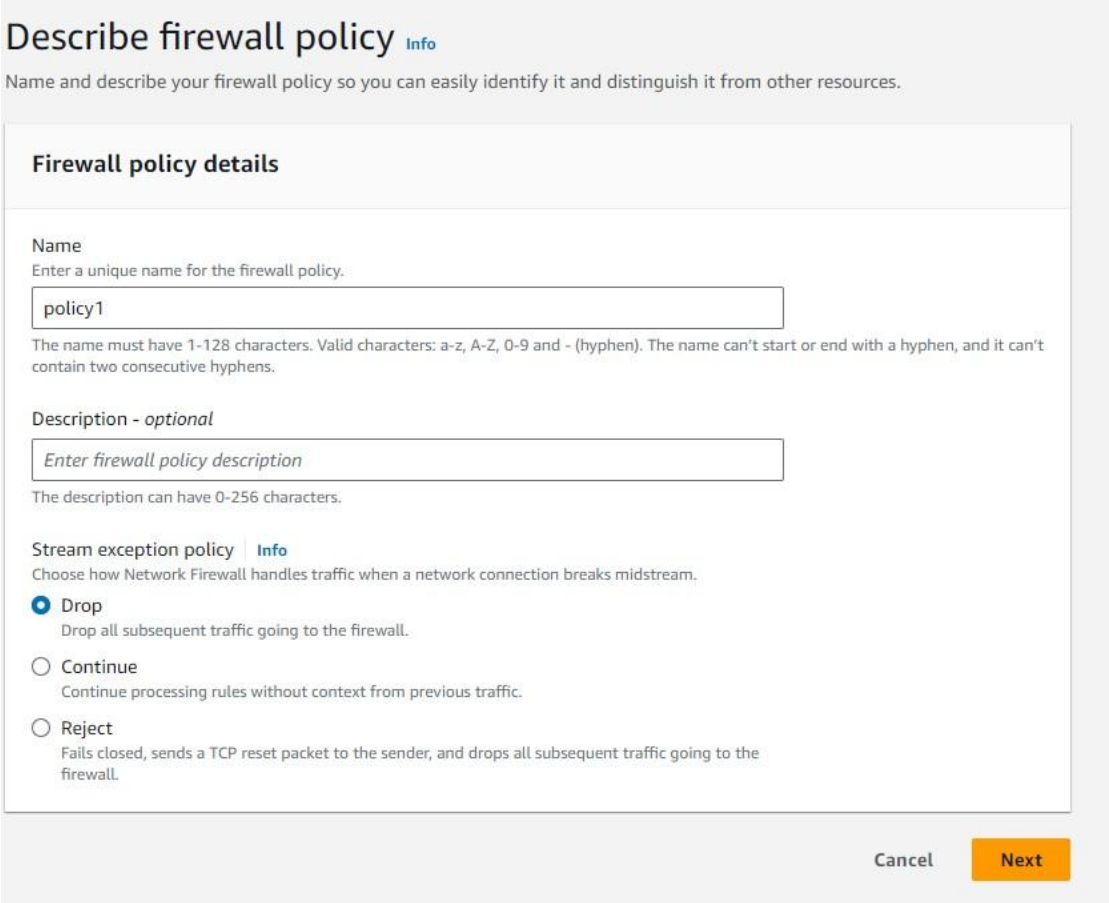
Delete | Create rule group

Find resources by name or value

1

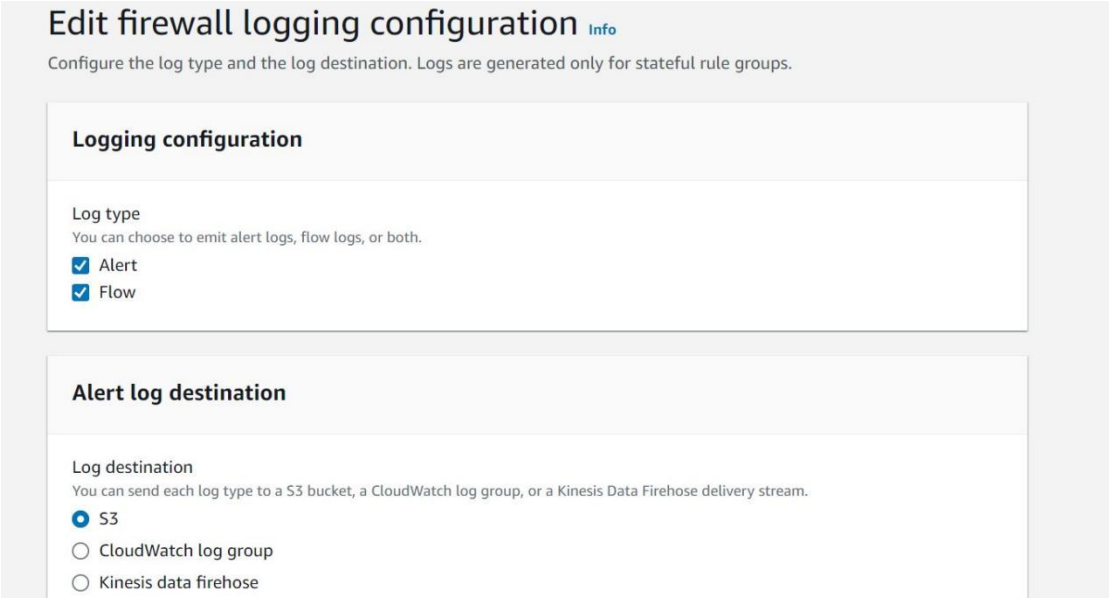
Name	Type
Stateful	Stateful
Stateless	Stateless

STEP 3 :- Created Firewall Policy in the Network Firewall Section.



STEP 4 :- Created Network Firewall and attached the Policy to it.

STEP 5 :- Enable logging in the Netowork Firewall and Save it in S3 Bucket



STEP 6 :- Check on the Instance for the website's, which we blocked is accessible or not.