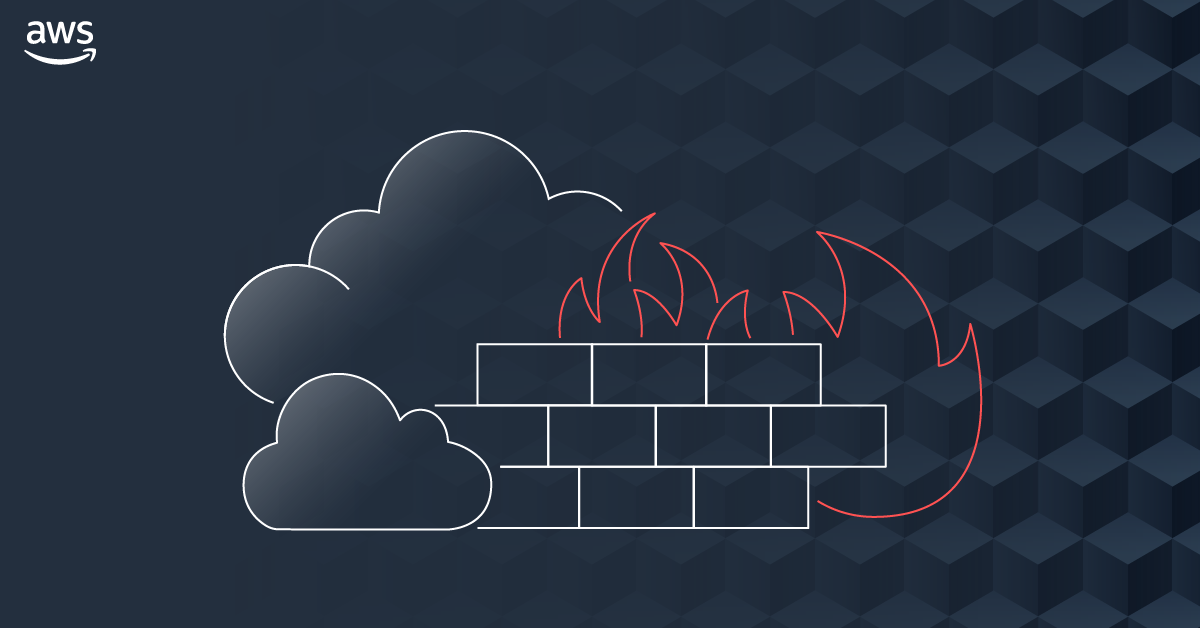
AWS Network Firewall

Image source aws.COM

## **Introduction:**

AWS Network Firewall is the recently launched, fully managed, highly available and scalable managed network by AWS basically providing security for the VPC's workloads.

* AWS network firewall is an intrusion prevention system (IPS) provides active traffic flow inspection by which it helps us to detect intrusion for VPC.
* It is a managed service which makes us easy to deploy essential network protection for the VPC's workloads. So, we don’t have to worry about the deploying and managing any infrastructure.
* AWS Network Firewall works together with AWS Firewall Manager so you can build policies based on AWS Network Firewall rules and then centrally apply those policies across your VPCs and accounts.

### **Perquisites:**

* AWS Account
* VPC
* 3 subnets
  + One for Network firewall
  + One for Main subnet
  + One for IGW

**components to be covered:**

* Network Firewall Rule Group
* Firewall policies
* Firewalls

**Resources Of AWS providing security services:**

Before going into deep inside the AWS network firewall, Let’s see what are the

capabilities we have in terms of security for the VPC.

* Security groups
* instance level.
* The traffic coming to the instance and going out of the instances will be evaluated by the rules.
* Network control list
* Subnet level security.
* We can add stateful rules where we can evaluate the traffic going in and out from the subnets
* AWS WAF
* I gives the security for the web application that’s running on the API’s, cloud front, load balancers.
* AWS shield
* Gives security against the ddos attacks.

SO, there is no easier way to scale network security across all your resources in your workloads regardless which AWS service you use.

* So far, how the traffic is routing to the subnet is:
  + Whenever traffic is coming through, it routed to the subnet directly through the Internet Gateway.
  + Any traffic going out of the subnet, will directly goes to IGW and route to the internet.

There was no middle-man or service to inspect the traffic between the Internet gateway and subnet.

There was no capability to not sending the traffic to the specific URL Or abort the flow of traffic coming from the specific URL.

* To solve this problem AWS launched a new security service called Network firewall, which provides network security to the user across all your resource workloads regardless which AWS service you use.

AWS Network firewall is highly available and scalable managed network by AWS basically providing security for the VPC's workloads.

* Network Firewall provides capability on URL filtering.

**How Traffic Flow inspection is Achieved**:

The way Traffic Flow inspection is Achieved here is:

* It will create a new subnet in our VPC in our availability zone in a particular region.
* It will create a VPC endpoint in the subnet called firewall subnet.
  + whenever any traffic coming to the subnet or going out of the subnet, the traffic is passed through the network Firewall subnet where network firewall is present.
  + It will inspect the Traffic using the defined policies and rules defined and pass the Traffic in and out.
  + By this way it provides the VPC level security.

In this blog, we are going to deploy the Network fire wall according to the architecture below.

**Deployment Architecture:**

Diagram

Description automatically generated

**Brief overview of steps involved:**

* + Before Beginning of the Firewall creation, make sure there should be
    - One VPC.
    - Two subnets, one for Main resource allocation and one for Network Firewall respectively.
    - 3 Route tables, one for Internet gateway, one for Main subnet, one for Network Firewall

Please follow the values of Ip addresses given in the Architecture diagram to avoid the confusion.

* Creating one Network firewall Rule Groups.
* Creating Firewall policy.
* Attaching the Rule groups and firewall policies.
* Creating one instance in the main instance, and check whether the traffic coming through the blocked URL we defined in the policies.

### **Step by Step Guide**

A screenshot of a computer

Description automatically generatedStep 1: Go to AWS console and go to VPC page. Select the Network Firewall Rule policy.

Step 2: Select Create Network Rule policy

A screenshot of a computer

Description automatically generated

Here, you can see there are two Rule Groups.

* stateless rules
* The traffic is evaluated whenever the traffic coming into the subnet. It won’t be evaluated when traffic coming out from the subnet.
* stateful rules
* The traffic will be evaluated on both directions.

A screenshot of a computer

Description automatically generated

You can see there are three types of rules in the stateful rule group.

We have three options.

1: 5-tupple

2: Domain list

3: Suricata computable IPS rules.

Graphical user interface

Description automatically generated

In 5-tupple option we can see below options

1: protocol:

* Transport protocol. Choose the protocol that you want to inspect. For all protocols, you can use IP, because all traffic on AWS and on the internet is IP.

2: source Ip

* Source Ip and Range. Traffic should come from the source address which provided in the list.

3: Source port:

* Source ports and port ranges. If specified, a packet must have a source port that's included in this list to match.

4: Destination:

* Destination IP addresses and ranges. If specified, a packet must have a destination address that's included in this list to match.

5: Destination Port:

* Destination ports and port ranges. If specified, a packet must have a destination port that's included in this list to match.

Traffic Direction

1: Any

* packets whose origination matches the rule's destination settings, and whose destination matches the rule's source settings

2: Forward

* Any traffic whose origination matches with the rule’s source setting and destination matches with the destination port mentioned in the rule setting will be forwarded.

ACTION

1: pass (the traffic will be allowed)

2: drop (the traffic will be denied)

3: Alert (alert will be initiated in log groups or in cloud watch)