

Amazon Firewall

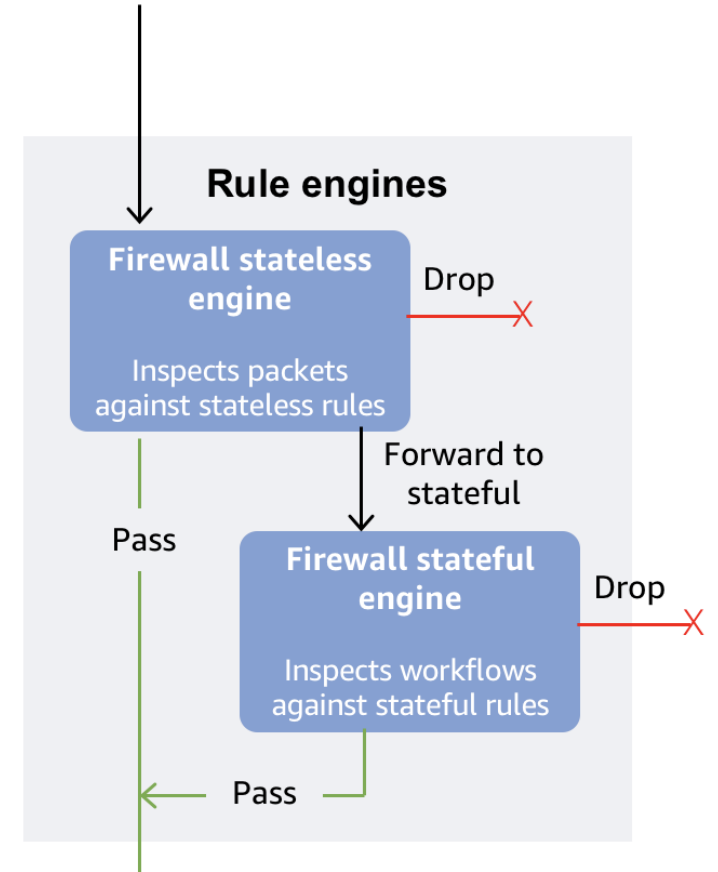
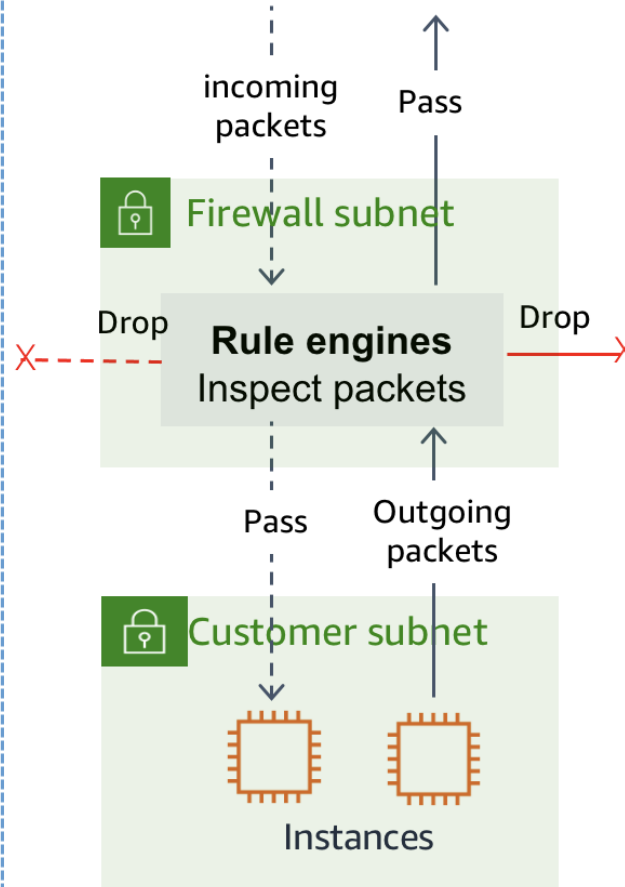
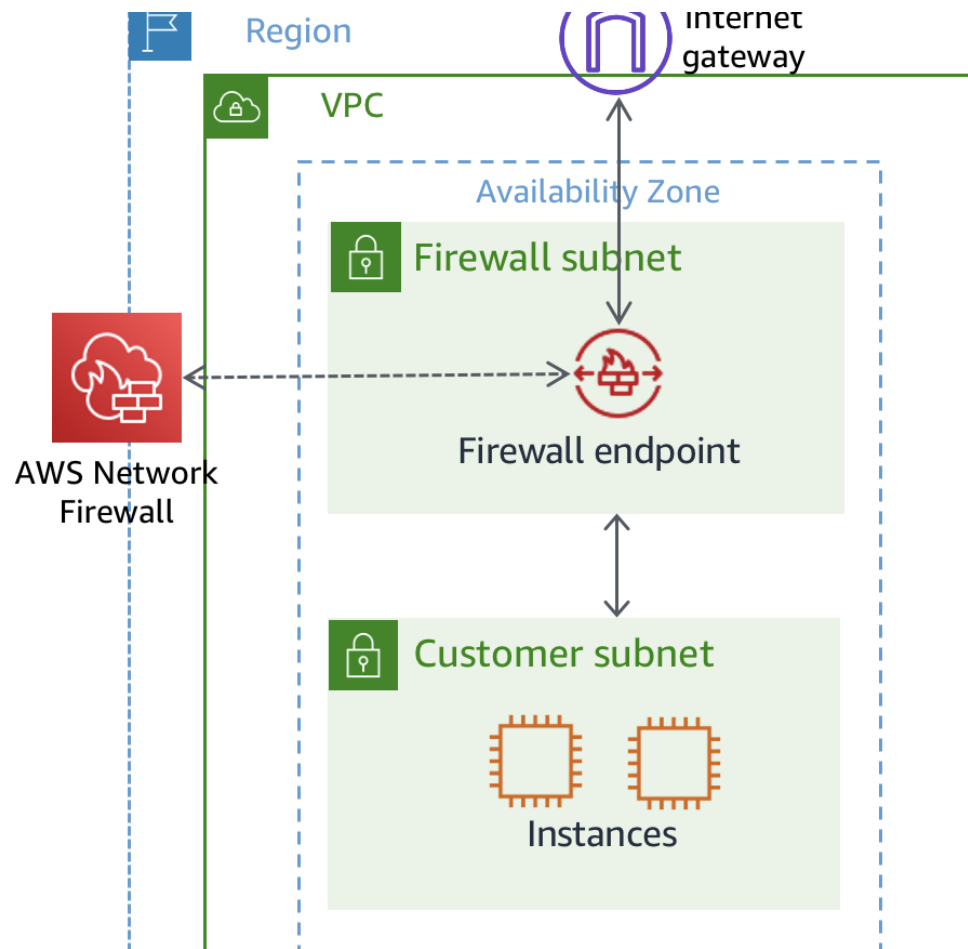
CloudSiksha

AWS Firewall

- A managed service that makes it easy to deploy essential network protections for the VPCs
- Define firewall rules that allow for fine-grained control over network traffic
 - **Ex: Blocking outbound Server Message Block (SMB) requests to prevent the spread of malicious activity**
- Deployed in a VPC AZ as an endpoint
 - **Change routing rules to pass traffic through the endpoint**
- Currently not widely available
 - **North Virginia, Oregon and Ireland**

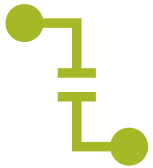






Firewall Operation

AWS Network Firewall terms



Firewall

A firewall connects the VPC that needs to be protected to the protection behavior that's defined in a firewall policy



Firewall Policy

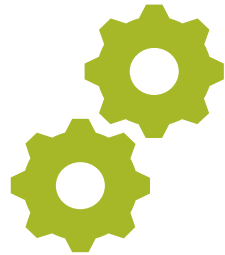
Defines the behavior of the firewall in a collection of stateless and stateful rule groups and other settings



Rule Groups

A rule group is a collection of stateless or stateful rules that define how to inspect and handle network traffic

Rule Groups



Stateless and Stateful Rule Group

Stateless rules analyze each packet without traffic workflow context

Stateful rules analyze packets within a traffic workflow context



Stateful rule group

5-tuple format, specifying source IP, source port, destination IP, destination port, and protocol, and specify the action to take for matching traffic

Domain list, specifying a list of domain names and the action to take for traffic that tries to access one of the domains

Suricata compatible IPS rules, providing advanced firewall rules using Suricata rule syntax

Thanks



CloudSiksha