

Amazon Network Firewall

AWS Network Firewall is a managed service that provides network protections for your Amazon Virtual Private Cloud (VPC). It allows you to deploy essential network security features to protect your workloads and applications running in the cloud. Here's an overview of what AWS Network Firewall offers:

Key Features:

1. Stateless and Stateful Rule Engine:

- **Stateless Rules:** These rules are simpler and apply to individual packets without considering previous packets in the flow. They are ideal for tasks like packet filtering based on IP address, protocol, and port.
- **Stateful Rules:** These rules track the state of network connections and can filter traffic based on entire sessions, not just individual packets. This allows for more complex security policies, such as intrusion prevention.

2. Domain Name Filtering:

- You can block or allow traffic based on domain names, which is useful for preventing access to malicious websites.

3. Centralized Management:

- You can manage and deploy network security policies across multiple VPCs and accounts within your AWS environment.

4. Deep Packet Inspection:

- AWS Network Firewall supports deep packet inspection (DPI) to detect and block specific types of content or application protocols, providing advanced threat detection capabilities.

5. Integration with AWS Services:

- It integrates seamlessly with other AWS services like AWS CloudWatch, AWS CloudTrail, and AWS VPC Traffic Mirroring for logging, monitoring, and threat detection.

6. Scalability and Availability:

- As a managed service, AWS Network Firewall scales automatically based on traffic and ensures high availability without the need for manual intervention.

Use Cases:

- **Intrusion Detection and Prevention:** Monitor and block malicious traffic in real time.
- **Web Filtering:** Control access to websites and prevent data exfiltration.
- **Network Segmentation:** Secure your VPC by segmenting different parts of your network based on security needs.

- **Compliance:** Helps meet regulatory requirements by enforcing specific security policies and monitoring network traffic.

How It Works:

AWS Network Firewall is deployed within your VPC, and it inspects and filters traffic between subnets within the VPC or between the VPC and the internet or other networks. You define rules and policies that specify the allowed and denied traffic, and the firewall enforces these rules.

Benefits:

- **Ease of Use:** As a fully managed service, it eliminates the need to manage and maintain firewall infrastructure.
- **Customizable:** You can tailor the rules to meet specific security needs.
- **Cost-Effective:** You pay only for the traffic processed by the firewall and the resources consumed, with no upfront costs.

AWS Network Firewall is ideal for organizations looking to enhance the security of their cloud infrastructure with a scalable, managed solution that integrates well with other AWS services.

This guide walks you through setting up and managing a basic AWS Network Firewall within a Virtual Private Cloud (VPC). You start by creating a VPC, subnets, and an Internet Gateway, then configure route tables to control traffic flow. After launching an EC2 instance in your VPC, you install necessary services and ensure internet connectivity.

The key steps involve setting up firewall rule groups (both stateful and stateless) that define which domains and protocols are allowed or blocked. You then create a firewall policy and apply it to your firewall. The firewall is configured to allow or block specific traffic, such as permitting access to certain websites (like Google and Microsoft) while blocking others (e.g., YouTube).

Finally, you verify the firewall's effectiveness by testing website access from your EC2 instance and adjusting the rules as needed. The process concludes with the cleanup of all resources.

End Goal: The goal is to set up a secure VPC environment where internet access is tightly controlled by an AWS Network Firewall, allowing or blocking traffic based on specified rules.

To begin with the Lab:

1. In your AWS Console navigate to VPC and click on Create VPC. Here you have to choose VPC only, give it a name then give your IPv4 CIDR block as you can see below, and click on Create VPC.

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

VPC only

VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

demo-firewall-VPC

IPv4 CIDR block [Info](#)

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Tenancy [Info](#)

Default



2. Then we are going to create our Subnet. So, go to subnets and click on Create Subnet.
3. First, choose your VPC then scroll down give your subnet a name, and give the IPv4 subnet CIDR block.

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-0f9d5a647c360d3d1 (demo-firewall-VPC)



Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.



IPv4 subnet CIDR block

256 IPs



- Now we are going to create another subnet for the firewall. Choose your VPC and then give your subnet a name chooses the AZ and give the CIDR block as shown below.

VPC

VPC ID

Create subnets in this VPC.



Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.



IPv4 subnet CIDR block

16 IPs



5. After creating your subnet, you need to create an Internet Gateway. So, go and click on create. Just give it a name and click on create IGW.

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional

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

Key

Value - optional



Remove

[Add new tag](#)

You can add 49 more tags.

Cancel

[Create internet gateway](#)

6. Now attach it with your VPC.

The following internet gateway was created: igw-0b7939efdc9e94a17 - demo-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

[Attach to a VPC](#)

VPC > Internet gateways > igw-0b7939efdc9e94a17 / demo-IGW

Actions ▾

Details		Info	
Internet gateway ID igw-0b7939efdc9e94a17	State Detached	VPC ID -	Owner 878893308172

Tags

Search tags

Key	Value
Name	demo-IGW

Manage tags

< 1 > ⚙

VPC > Internet gateways > Attach to VPC (igw-0b7939efdc9e94a17)

Attach to VPC (igw-0b7939efdc9e94a17) [Info](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

X

▶ AWS Command Line Interface command

Cancel

Attach internet gateway

7. Now we are going to create a public route table and associate our subnet with it. So, give it a name and choose your VPC, click on create.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

Tags

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

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="demo-public-route-table"/>

Add new tag

You can add 49 more tags.

Cancel **Create route table**

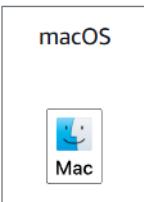
- Now you need to associate your subnet with the route table. After that create a route for internet gateway and choose the destination as 0.0.0.0/0.

Routes	Subnet associations	Edge associations	Route propagation	Tags
Explicit subnet associations (1)				
<input type="text" value="Find subnet association"/> Edit subnet associations				
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	
demo-public-subnet	subnet-0b590a7e287fe620f	10.0.0.0/16	-	
Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (2)				
<input type="text" value="Filter routes"/> Both Edit routes				
Destination	Target	Status	Propagated	
0.0.0.0/0	igw-0b7939efdc9e94a17	Active	No	
10.0.0.0/16	local	Active	No	

- Now we are done with our VPC, so navigate to EC2 and create an EC2 instance.
- Choose Windows Machine, your instance type, and the key pair.

Recents

Quick Start



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

ami-09927fda4a30717cd (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Microsoft Windows 2022 Datacenter edition. [English]

Architecture

AMI ID

64-bit (x86)

ami-09927fda4a30717cd

Verified provider

11. Just remember to choose your VPC and the subnet. Create your instance.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0f9d5a647c360d3d1 (demo-firewall-VPC)
10.0.0.0/16



Subnet [Info](#)

subnet-0b590a7e287fe620f demo-public-subnet
VPC: vpc-0f9d5a647c360d3d1 Owner: 878893308172
Availability Zone: ap-southeast-1a Zone type: Availability Zone
IP addresses available: 65531 CIDR: 10.0.0.0/16

Create new subnet

Auto-assign public IP [Info](#)

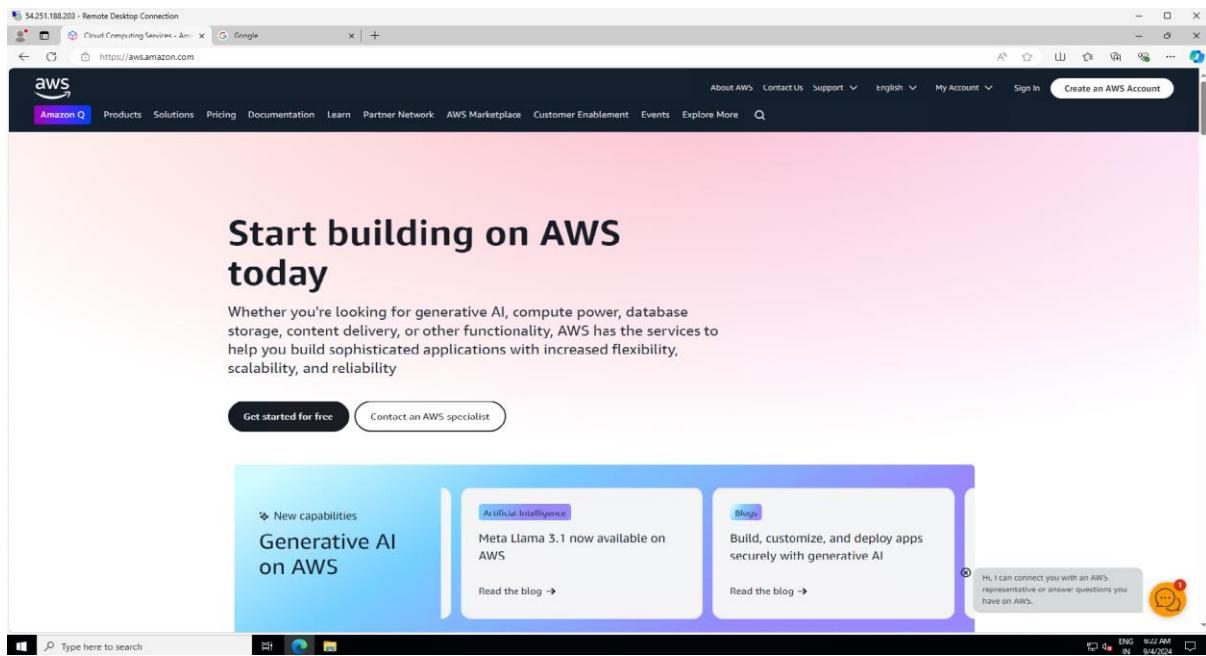
Enable

Additional charges apply when outside of free tier allowance

12. Once your instance is created login to it then open the internet browser in your VM.

13. Below you can see that on our machine we can reach the internet.

14. Also, install the IIS service on your instance.



15. Now we are going to set up the Network Firewall. So, come back to your VPC, and from the left pane scroll down to Network Firewall, then open network firewall rule groups. Click on Create rule groups.
16. In step 1, choose Stateful rule groups and in the format choose domain list. In rule evaluation order choose Action order. Click on next.

Choose rule group type Info

Network Firewall rule groups are either stateless or stateful. Stateless rule groups evaluate packets in isolation, while stateful rule groups evaluate them in the context of their traffic flow.

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.

Rule group format

Domain list ▾

Rule evaluation order | Info
The way that your stateful rules are ordered for evaluation.

Strict order - recommended
Rules are processed in the order that you define, starting with the first rule.

Action order
Rules with a pass action are processed first, followed by drop, reject, and alert actions. This option was previously named **Default order**.

Cancel **Next**

17. After that give it a name and capacity as you see below. Click on next.

Describe rule group Info

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

Rule group details

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

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.

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.

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

[Cancel](#) [Previous](#) [Next](#)

18. Now in step 3, give the domain names that you want to allow. Keep CIDR ranges to default, protocols to default and in action choose Allow.

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
www.aws.amazon.com
www.microsoft.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.

HTTP
 HTTPS

Action [Info](#)
Action to take when a request matches the domain names in this group.

Allow
 Deny

[Cancel](#) [Previous](#) **Next**

19. For step 4, skip it and move to the review page then create your firewall rule groups.

Configure advanced settings - *optional* [Info](#)

Configure a customer managed AWS Key Management Service (KMS) key to encrypt and decrypt your resources.

Customer managed key [Info](#)

You can use a customer managed key in AWS Key Management Service (KMS) to encrypt your data at rest. If you don't configure a customer managed key, Network Firewall encrypts your data using an AWS managed key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)

[Cancel](#) [Previous](#) **Next**

20. Below you can see that our Stateful rule group has been created now we are going to create a stateless rule group. Click on create rule group.

Rule groups Info

A rule group is a reusable set of firewall rules for inspecting and filtering network traffic. You can use stateless or stateful rule groups to configure the traffic inspection criteria for your firewall policies. You can create your own rule groups or you can use rule groups that are managed by AWS Marketplace Sellers.

Your rule groups | AWS managed rule groups

The following table lists all of your rule groups.

Your rule groups (1)		Delete	Create rule group
<input type="text"/> Find resources by name or value		< 1 >	②
<input type="checkbox"/>	Name	Type	▼
<input type="checkbox"/>	Stateful-rule	Stateful	▼

Add rule groups to policy

21. Here in step 1 you need to choose the Stateless rule group and click on next.

Choose rule group type Info

Network Firewall rule groups are either stateless or stateful. Stateless rule groups evaluate packets in isolation, while stateful rule groups evaluate them in the context of their traffic flow.

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**

22. Then give it a name and capacity as you can see below.

Describe rule group [Info](#)

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

Rule group details

Name

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

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.

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.

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

[Cancel](#)[Previous](#)[Next](#)

23. Now on step 3, first set its priority and choose ICMP and RDP protocol then scroll down. In the source and destination choose as shown below in the snapshot. Lastly, in the rule actions choose forward to stateful rule groups. Then click on add.

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.

Protocol

Transport protocols to inspect for.



ICMP X

Protocol: 1

RDP X

Protocol: 27

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.

Destination

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

Custom

10.0.0.0/16

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 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.

Rule action

Choose how you want the firewall to handle packets that match the rule criteria.

Pass

Discontinue all inspection of the packet and permit it to go to its intended destination.

Drop

Discontinue all inspection of the packet and block it from going to its intended destination.

Forward to stateful rule groups

Discontinue stateless inspection of the packet and forward it to the stateful rule engine for inspection.

Publish metrics - optional | [Info](#)

Publish a custom Amazon CloudWatch metric to monitor the usage of your stateless rule groups.

-

Add rule

24. Then in the rules you will see your rule and click on next. Move to the review page and create your stateless rule group.

 You've successfully added the rule to this rule group. You can add more rules if you'd like. If you add or update any rules in this rule group, we recommend that you **Analyze** your rules for behavior such as asymmetric routing. [Info](#) 

Rules (1) [Info](#)

[Delete](#) [Analyze](#)

< 1 > 

<input type="checkbox"/>	Priority	Protocol	Source	Destination	Source po...	Destinati...	A
<input type="checkbox"/>	10	ICMP, RDP	0.0.0.0/0	10.0.0.0/16			F

[Cancel](#) [Previous](#) [Next](#)

25. Below you can see that we have created both of our rule groups.

Rule groups [Info](#)

A rule group is a reusable set of firewall rules for inspecting and filtering network traffic. You can use stateless or stateful rule groups to configure the traffic inspection criteria for your firewall policies. You can create your own rule groups or you can use rule groups that are managed by AWS Marketplace Sellers.

[Your rule groups](#) [AWS managed rule groups](#)

[Add rule groups to policy](#)

The following table lists all of your rule groups.

Your rule groups (2)		Delete	Create rule group
<input type="checkbox"/> Find resources by name or value		< 1 >	
<input type="checkbox"/> Name	Type		
<input type="checkbox"/> Stateful-rule	Stateful		
<input type="checkbox"/> Stateless-rule	Stateless		

26. Now we need to create a firewall policy. So, in step 1 give it a name and click on next.

Describe firewall policy [Info](#)

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

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.

Stream exception policy [Info](#)

Choose how Network Firewall handles traffic when a network connection breaks midstream.

Drop

Drop all subsequent traffic going to the firewall.

Continue

Continue processing rules without context from previous traffic.

Reject

Fails closed, sends a TCP reset packet to the sender, and drops all subsequent traffic going to the firewall.

[Cancel](#)

[Next](#)

27. Then in step 2, keep default settings for stateless default actions.

Stateless default actions

Stateless default actions determine how Network Firewall should handle packets that don't match any stateless rule group contained in this policy. You must set stateless default action regardless of whether you define stateless rule groups for the policy.

Fragmented packets [Info](#)

Choose how to treat fragmented packets.

Use the same actions for all packets

Use different actions for full packets and fragmented packets

Rule action

Choose how to handle a packet that matches the rule's match criteria.

Pass

Discontinue all inspection of the packet and permit it to go to its intended destination.

Drop

Discontinue all inspection of the packet and block it from going to its intended destination.

Forward to stateful rule groups

Discontinue stateless inspection of the packet and forward it to the stateful rule engine for inspection.

Publish metrics - optional [Info](#)

Publish a custom Amazon CloudWatch metric to monitor the usage of your stateless rule groups.

Enable

28. After that you need to add your stateless rule groups and choose Action order in stateful rule evaluation order. In the end, choose your stateful rule group. Move to review page and create your firewall policy.

Stateless rule group (1)		
	Priority	Name
<input type="checkbox"/>	1	Stateless-rule

Stateful rule evaluation order and default actions
The way that your stateful rules are ordered for evaluation.

Rule evaluation order | [Info](#)

Strict order - *recommended*
Rules are processed in the order that you define, starting with the first rule.

Action order
Rules with a pass action are processed first, followed by drop, reject, and alert actions. This option was previously named **Default order**.

Stateful rule group (1)		
	Name	Capacity
<input type="checkbox"/>	Stateful-rule	1000

29. Now we are going to create our Firewall. So, go to Firewalls and click on Create. Give a name to your firewall and click on next.

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.

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.

[Cancel](#)[Next](#)

30. Then in the step 2 choose your AZ, your firewall subnet and the IP address type, click on next.

Configure VPC and subnets Info

The firewall protects the subnets within an Amazon Virtual Private Cloud (VPC) by filtering traffic going between the subnets and locations outside of your VPC. After you create the firewall and its associated firewall policy, configure your VPC to route traffic through the endpoints created by the firewall.

VPC

For each Availability Zone where you want protection, provide Network Firewall with a public subnet that's dedicated to the firewall endpoint. Only use the firewall subnets that you specify here for the firewall. Don't use them for any other purpose.

VPC

Choose the VPC where you want to create this firewall.



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

[Remove subnet](#)[Add new subnet](#)[Cancel](#)[Previous](#)[Next](#)

31. For step 3, disable the protection. Click on next.

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

Customer managed key Info

You can use a customer managed key in AWS Key Management Service (KMS) to encrypt your data at rest. If you don't configure a customer managed key, Network Firewall encrypts your data using an AWS managed key.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)

Cancel

Previous

Next

32. Then choose your existing firewall policy. Move to the review page and create your firewall. It will take some time to create your firewall.

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

Choose firewall policy

Choose the firewall policy to associate with this firewall.

firewall-policy

Cancel

Previous

Next

33. Below you can see that our firewall is now ready.

demo-firewall

Overview

Firewall status: Ready

Associated firewall policy: [firewall-policy](#)

Associated VPC: [vpc-0f9d5a647c360d3d1](#)

Firewall details

Name: demo-firewall

Description: -

VPC

Associated VPC: [vpc-0f9d5a647c360d3d1](#)

Firewall subnets: [subnet-0d7ac7872cf7ac2af](#) (IPv4)

34. Go to your EC2 instance and in the security group you need to add an ICMP port for source CIDR 10.0.0.0/16.

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-0b4b1ce297342ea...	IPv4	All ICMP - IPv4	ICMP	All	10.0.0.0/16
-	sgr-04b7228a53cdf130b	IPv4	RDP	TCP	3389	0.0.0.0/0

35. Now move to the route table and create route tables to change the routing. So, we are going to create two route tables, one for the firewall and another for the internet gateway.

36. Below you can see that we have created both of our route tables.

Route tables (4) [Info](#)

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC	Owner ID
-	rtb-058408fba977b712e	-	-	Yes	vpc-0f9d5a647c360d3d1 dem...	878893308172
demo-public-route-table	rtb-01648a0008c5bd862	subnet-0ab615bf7f0d9d...	-	No	vpc-0f9d5a647c360d3d1 dem...	878893308172
IGW-RT	rtb-08cd579eb8e8a2aac	-	-	No	vpc-0f9d5a647c360d3d1 dem...	878893308172
firewall-RT	rtb-037b7be9fd95fce88	-	-	No	vpc-0f9d5a647c360d3d1 dem...	878893308172

37. So, in your Internet gateway route table go to edge association and associate it with your Internet gateway. Then go to route, click on edit, and in the target choose gateway load balancer, click on save.

VPC > Route tables > rtb-08cd579eb8e8a2aac

rtb-08cd579eb8e8a2aac / IGW-RT

Details Info			
Route table ID rtb-08cd579eb8e8a2aac	Main No	Explicit subnet associations -	Edge associations igw-0b7939efdc9e94a17 / demo-IGW
VPC vpc-0f9d5a647c360d3d1 demo-firewall-VPC	Owner ID 878893308172		

Routes | Subnet associations | **Edge associations** | Route propagation | Tags

Associated internet gateways (1)

ID	State	VPC	Owner
igw-0b7939efdc9e94a17 / demo-IGW	Attached	vpc-0f9d5a647c360d3d1	878893308172

Edit edge associations

VPC > Route tables > rtb-08cd579eb8e8a2aac > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	Gateway Load Balancer Endpoint vpc-08d8e9656cb707468	Active	No

Add route

Cancel | Preview | **Save changes**

38. Now go to the firewall route table, in the subnet association, associate your firewall subnet with your firewall route table.
39. After that go to the routes and create a route for internet gateway from destination 0.0.0.0/0.

rtb-037b7be9fd95fce88 / firewall-RT

Details Info			
Route table ID rtb-037b7be9fd95fce88	Main No	Explicit subnet associations subnet-0d7ac7872cf7ac2af / demo-firewall-subnet	Edge associations -
VPC vpc-0f9d5a647c360d3d1 demo-firewall-VPC	Owner ID 878893308172		

Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
demo-firewall-subnet	subnet-0d7ac7872cf7ac2af	10.0.4.0/28	-

Edit subnet associations

rtb-037b7be9fd95fce88 / firewall-RT

Details Info			
Route table ID rtb-037b7be9fd95fce88	Main No	Explicit subnet associations subnet-0d7ac7872cf7ac2af / demo-firewall-subnet	Edge associations -
VPC vpc-0f9d5a647c360d3d1 demo-firewall-VPC	Owner ID 878893308172		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0b7939efdc9e94a17	Active	No
10.0.0.0/16	local	Active	No

Both | Edit routes

40. Finally, go to your public route table, in the route we'd added the route for the internet gateway, but now we will change it to the gateway load balancer. As you can see below.

rtb-01648a0008c5bd862 / demo-public-route-table

Details Info

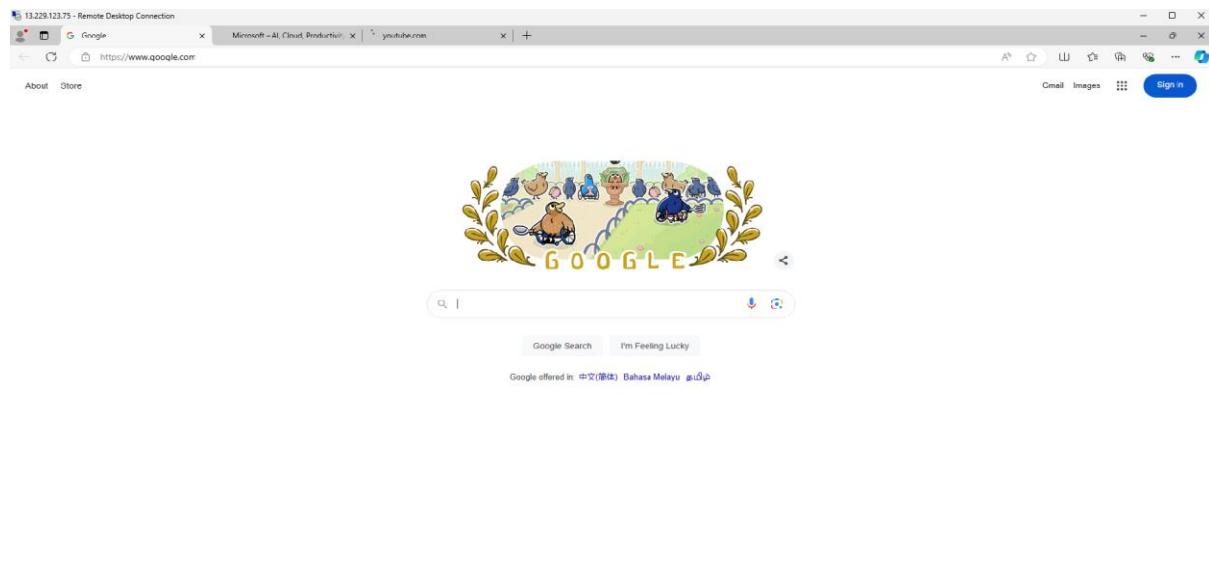
Route table ID rtb-01648a0008c5bd862	Main No	Explicit subnet associations subnet-0ab615bf7fd9d658 / demo-public-subnet	Edge associations -
VPC vpc-0f9d5a647c360d3d1 demo-firewall-VPC	Owner ID 878893308172		

Routes | Subnet associations | Edge associations | Route propagation | Tags

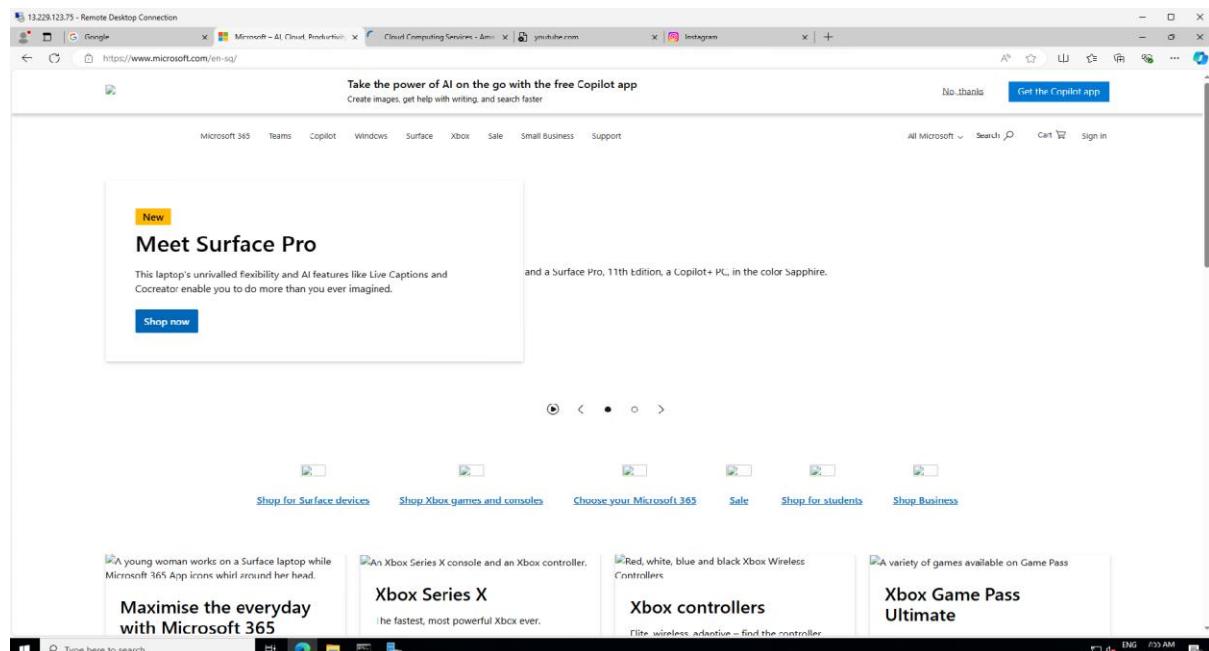
Routes (2)

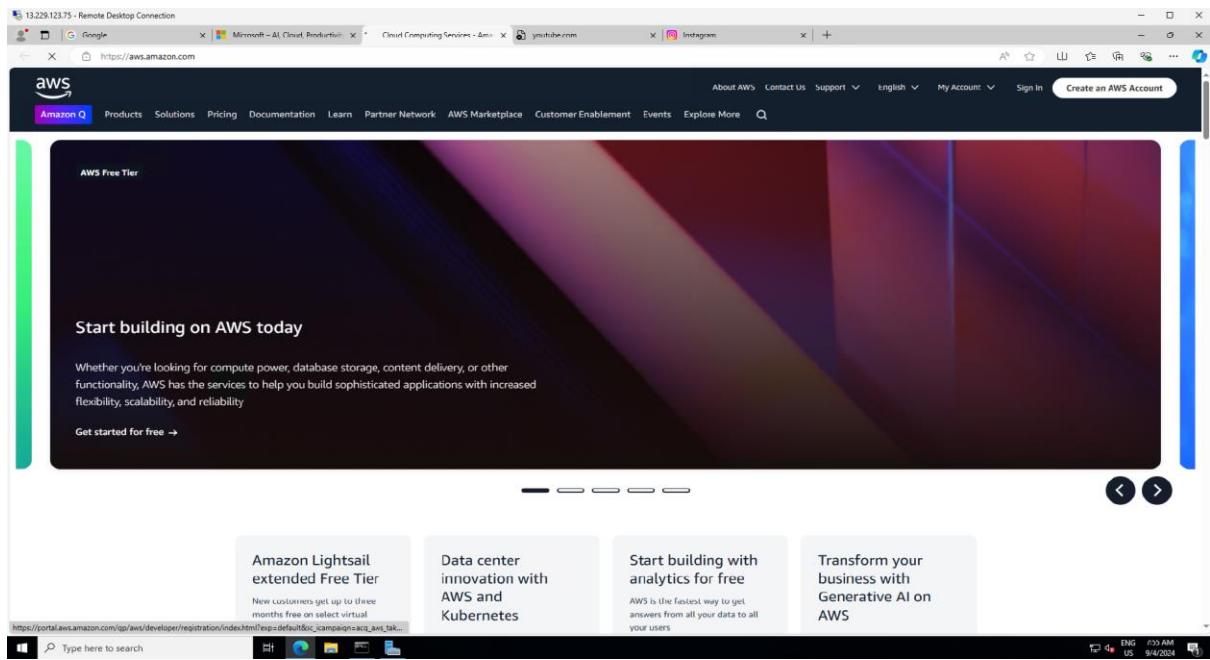
Filter routes			
Destination	Target	Status	Propagated
0.0.0.0/0	vpce-08d8e9656cb707468	Active	No
10.0.0.0/16	local	Active	No

41. After all this connect with your instance again and open your browser in it. Then try to reach google.com you will see that you can reach it.

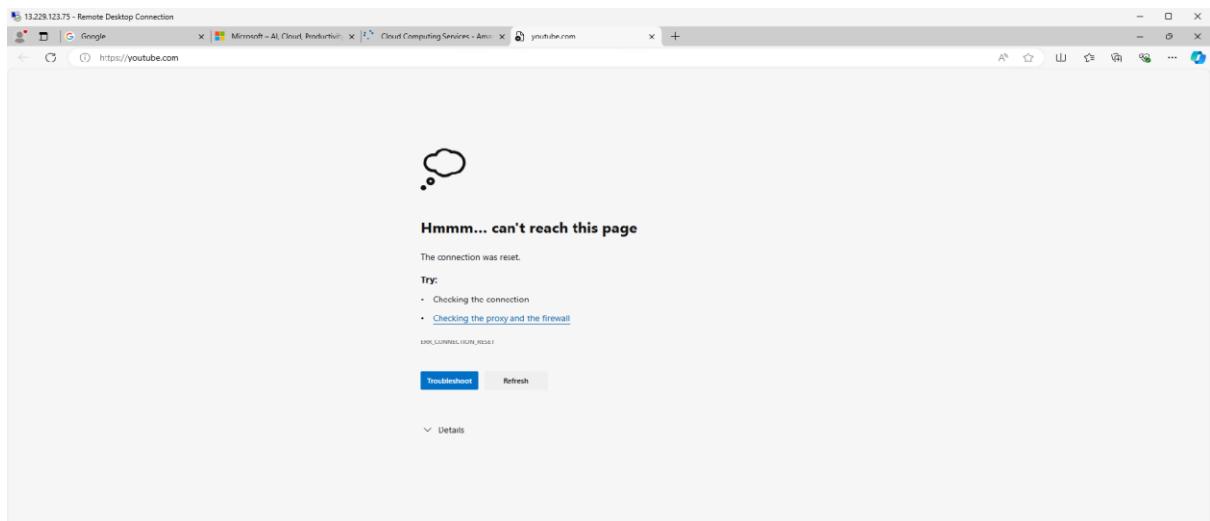


42. It goes the same for Microsoft.com and aws.amazon.com.





43. But if you try to reach any other website other then these three. For example, youtube.com, you will get an error message for this.



44. Now comeback to your VPC and navigate to firewall rule groups and open your stateful rule group. In the domains section click on edit.

A screenshot of the AWS VPC Firewall Rule Groups interface. The left sidebar shows "Domains (3)". The main table lists three domains: "www.google.com", "www.aws.amazon.com", and "www.microsoft.com". Each row has a checkbox labeled "Name" and a "Delete" button. At the top right, there are "Delete" and "Edit" buttons, and a navigation bar with arrows and a refresh icon.

45. In the domain list add youtube.com and click on save. Then go back to your instance and refresh the page for YouTube.

Edit domains for Stateful-rule

X

Domain names

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

```
www.google.com  
www.aws.amazon.com  
www.microsoft.com  
www.youtube.com|
```

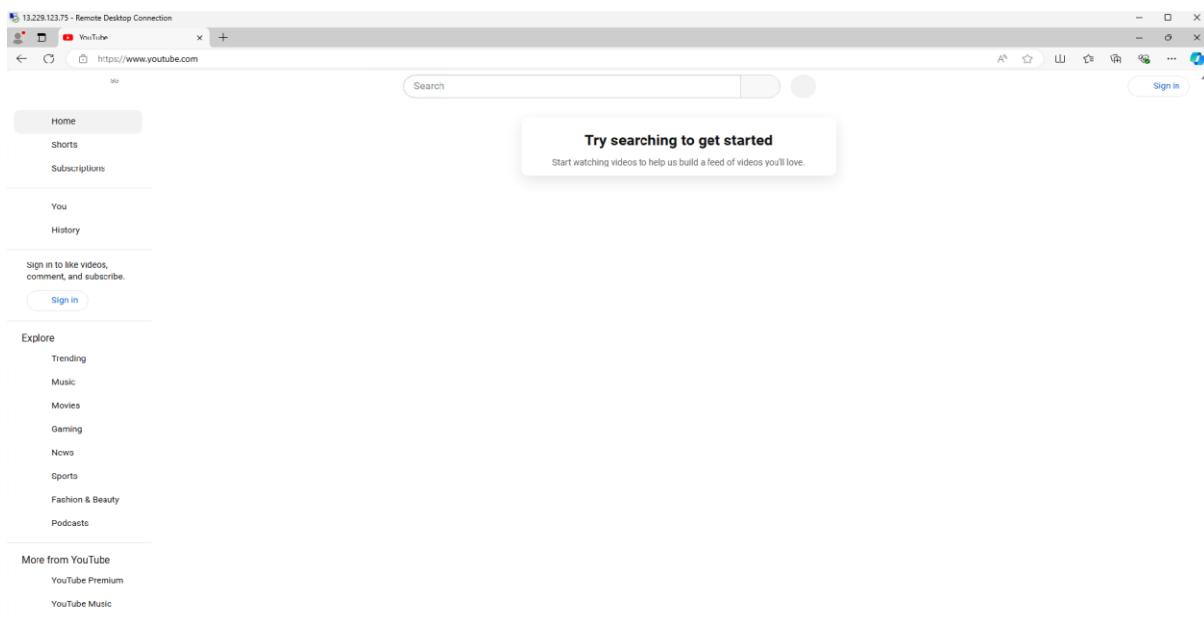
Enter one domain name per line.



Cancel

Save

46. You will see that you can reach the youtube.com now.



47. Once you are done delete all your resources.

**First, you need to delete the gate load balancer routes from the route table.
Then delete your firewall, firewall policy, and firewall rule groups.
Terminate your instance. Delete your VPC (Optional)**