Cohort 2
Group 1

Team

Emmanuel Macaulay
Cloud Security Engineer
FE/23/43836097

Hadiza Oladipupo
GRC Analyst
FE/23/63922892

Yinka Akintola
CISO
FE/23/99525446

Adu Olamilekan
Network Administrator
FE/23/81232810

Sholanke Abayomi
SOC Analyst
FE/24/6766294920

Adedamola Babafemi
Penetration Tester
FE/23/31535673

Ayanbode Olanrewaju
Cyber Security Engineer
FE/23/49305691

Cloud Security: Threat Hunting with AWS Network Firewall

Motivation

Why this project?

- In today's digital landscape, cloud computing has become the backbone of modern business operations. As organizations increasingly migrate their infrastructure and data to cloud-based platforms, the importance of cloud security cannot be overstated.

- Current Landscape: Cyber threats are on the rise, especially in cloud infrastructures.

Project Goal

- Enhance security using an AWS Network Firewall to detect and prevent unauthorized access (unecrypted communication) over our network.

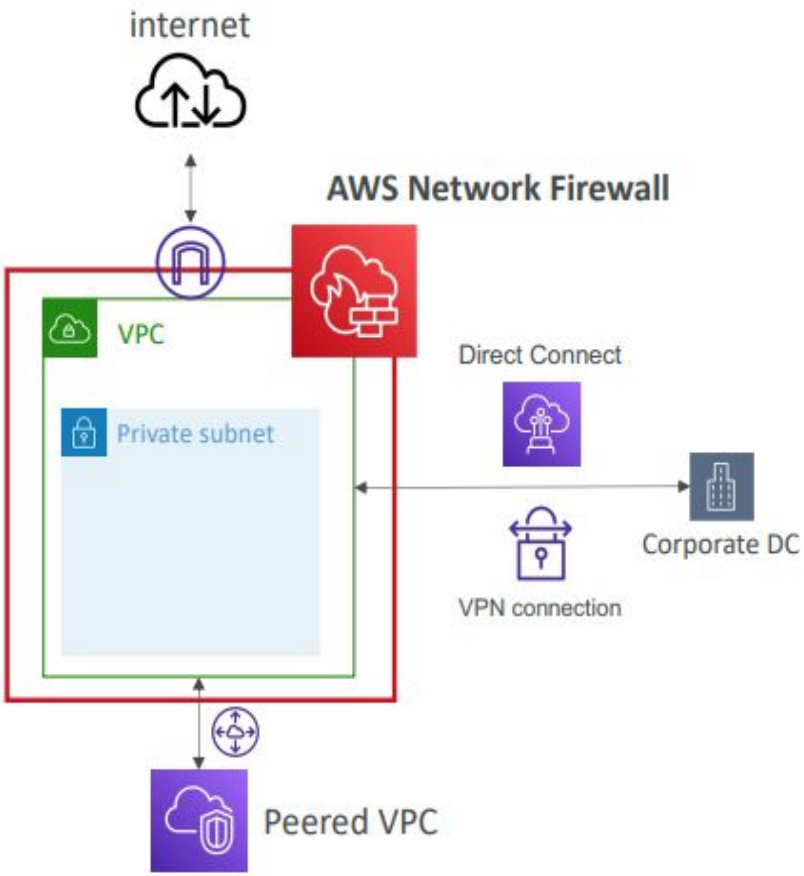
What Is AWS Network Firewall?

AWS Network Firewall

- Protect your entire Amazon VPC

- From Layer 3 to Layer 7 protection
- Any direction, you can inspect
  - VPC to VPC traffic
  - Outbound to internet
  - Inbound from internet
  - To / from Direct Connect & Site-to-Site VPN

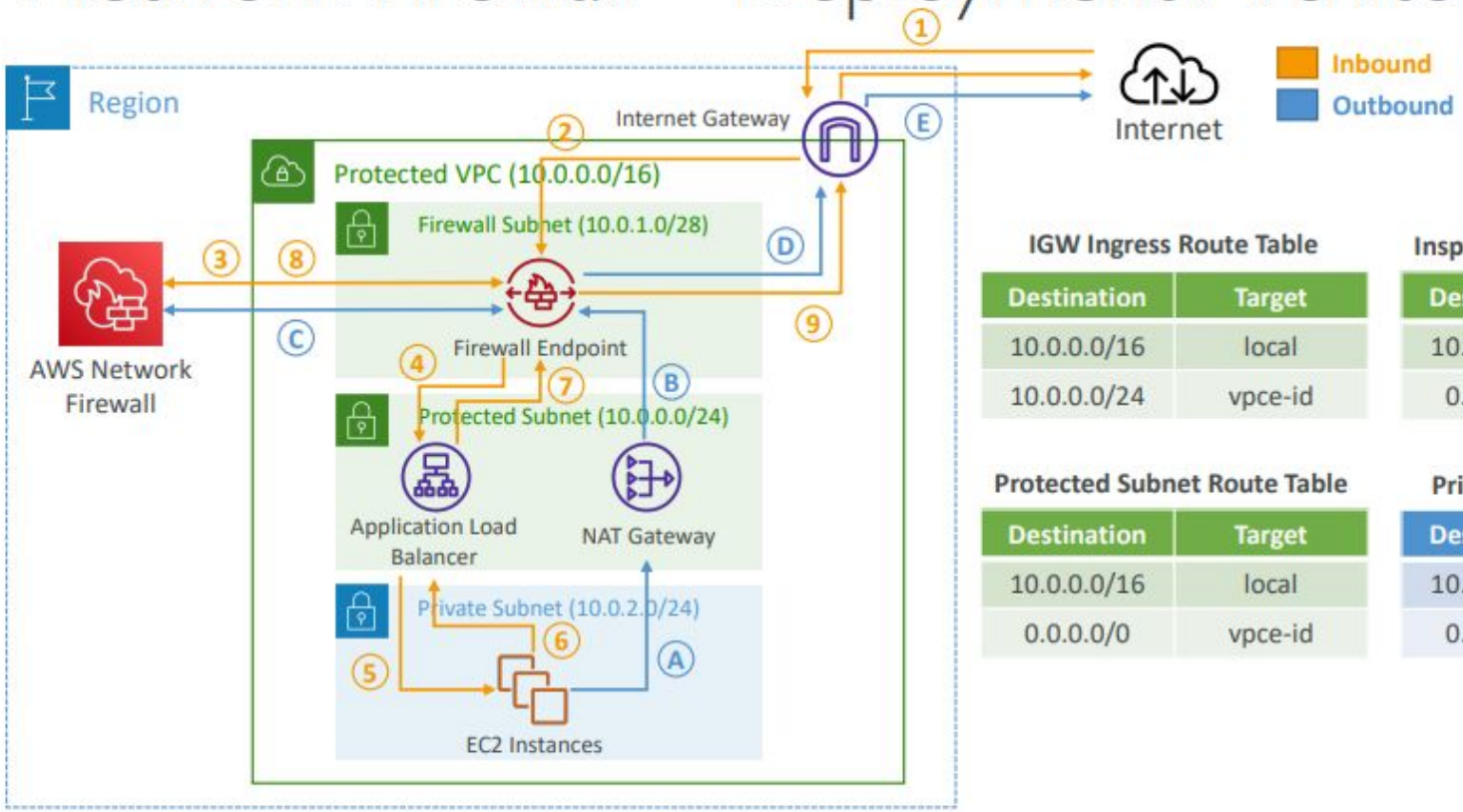
- Internally, the AWS Network Firewall uses the AWS Gateway Load Balancer
- Rules can be centrally managed cross-account by AWS Firewall Manager to apply to many VPCs



Network Firewall – Fine Grained Controls

- Supports 1000s of rules
  - IP & port - example: 10,000s of IPs filtering
  - Protocol – example: block the SMB protocol for outbound communications
  - Stateful domain list rule groups: only allow outbound traffic to *.mycorp.com or third-party software repo
  - General pattern matching using regex
- **Traffic filtering: Allow, drop, or alert for the traffic that matches the rules**
- **Active flow inspection** to protect against network threats with intrusion-prevention capabilities (like Gateway Load Balancer, but all managed by AWS)
- Send logs of rule matches to Amazon S3, CloudWatch Logs, Kinesis Data Firehose

Network Firewall – Deployment Architectures



IGW Ingress Route Table

Destination	Target
10.0.0.0/16	local
10.0.0.0/24	vpce-id

Inspection Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Protected Subnet Route Table

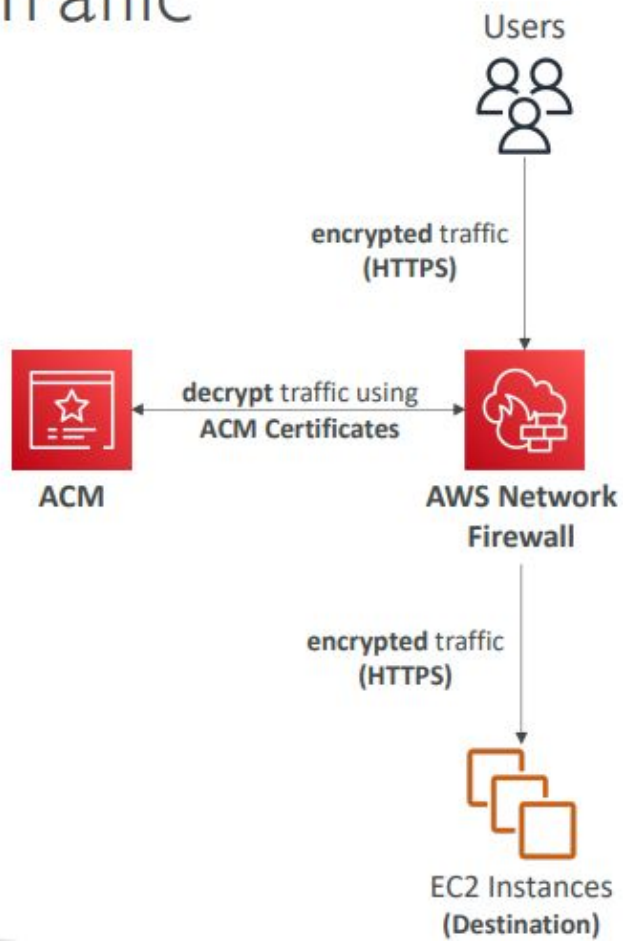
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	vpce-id

Private Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	natgw-id

Network Firewall – Encrypted Traffic

- AWS Network Firewall supports **Deep Packet Inspection (DPI) for encrypted traffic Transport Layer Security (TLS)**
- It decrypts the TLS traffic, inspects and blocks any malicious content, then re-encrypts the traffic for the destination
- Integrates with **AWS Certificate Manager (ACM)**



Challenges We're Trying to Solve

Key Challenge:

- **Unauthorized Network Access:** Detecting and preventing unauthorized access to the network, potentially leading to data breaches or system compromise.
- **Infiltration Attempts:** Identifying and blocking infiltration attempts by hackers, which can result in sensitive data exposure or disruption of business operations.
- **Non-TLS Traffic Over TLS Ports:** Detecting and mitigating non-TLS (unencrypted) traffic traversing over TLS ports (e.g., port 443), which can indicate malicious activity.

Issues in Focus

- Tracking unauthorized traffic.
- Quick response to infiltration attempts.
- Protecting cloud infrastructure from diverse threats.

What We Did

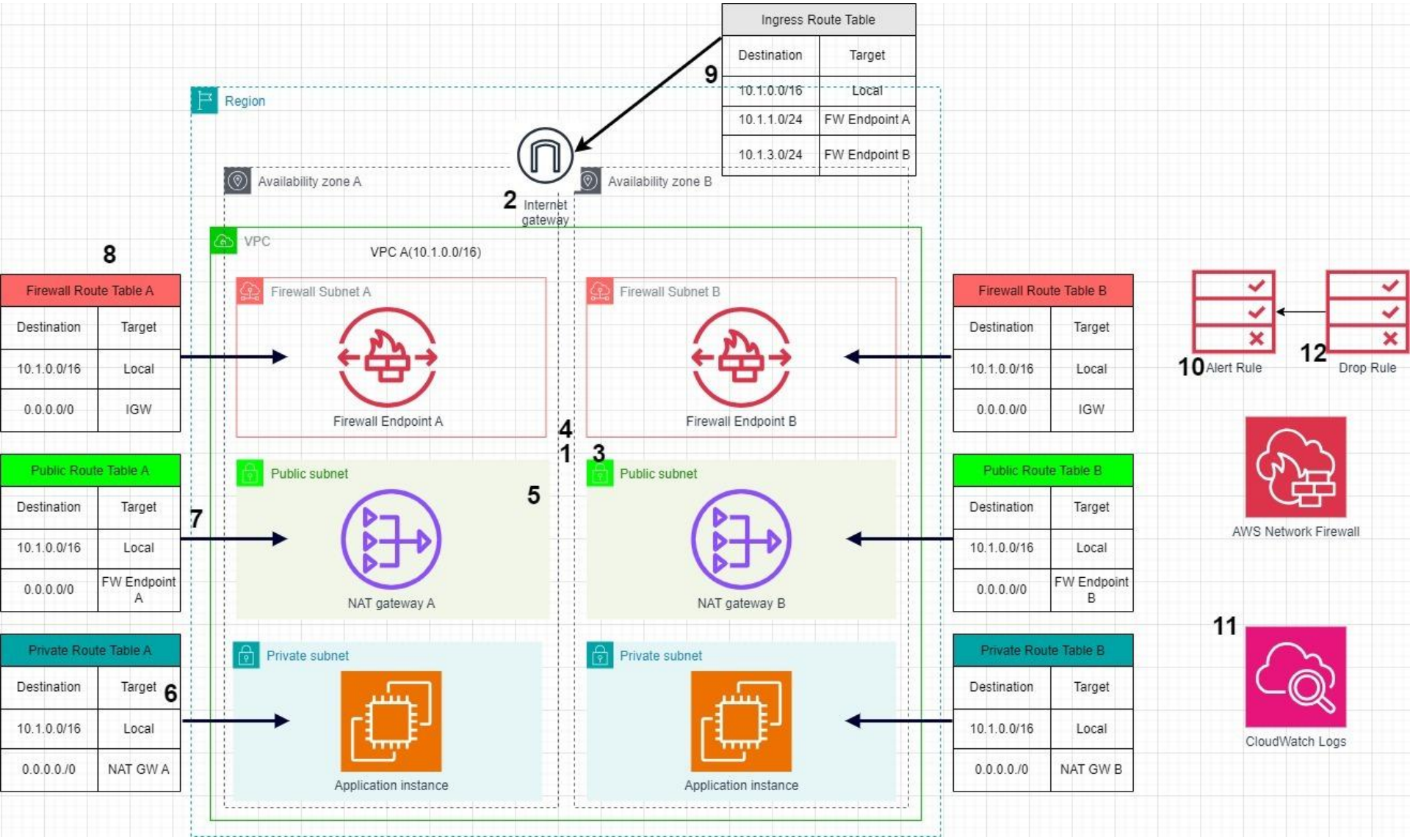
Solution Overview

- Configured AWS Network Firewall for threat detection.
- Set up rule groups to monitor non-TLS traffic on TLS ports.

Steps Taken

- Created firewall rule group to detect suspicious traffic.
- Integrated AWS CloudWatch Logs for firewall monitoring.

Architectural Diagram



Steps taken in Configuring the Firewall

...

aws | Services | Search [Option+S] | N. Virgini

NAT gateways

Peering connections

▼ Security

1. Scroll

Network ACLs

Security groups

▼ DNS firewall

Rule groups

Domain lists

▼ Network Firewall

Firewalls

2. Click

Firewall policies

Network Firewall rule groups

TLS inspection configurations

Network Firewall resource groups

▼ Virtual private network (VPN)

Customer gateways

Virtual private gateways

Site-to-Site VPN

VPC > Network Firewall: Firewalls

Firewalls

This page lists your firewalls in AWS Network Firewall.

Firewalls (1)

Delete | Create firewall

Find by keyword

1

Name	Status	Configuration sync state
InspectionFirewall	Ready	In sync

3. Click

Select a firewall

aws Services Search [Option+S] N. Virgini [redacted]

NAT gateways
Peering connections

- Security
  - Network ACLs
  - Security groups
- DNS firewall
  - Rule groups
  - Domain lists
- Network Firewall
  - Firewalls
  - Firewall policies
  - Network Firewall rule groups
  - TLS inspection configurations
  - Network Firewall resource groups
- Virtual private network (VPN)
  - Customer gateways
  - Virtual private gateways
  - Site-to-Site VPN

Firewall details | Firewall policy settings | Monitoring

1. Scroll

Firewall details

Edit

Name	Description
InspectionFirewall	-

VPC

Edit

Associated VPC
vpc-0c48c4cc7613fec14

2. Review

Firewall subnets
subnet-04aa77f8be1532f15 (IPv4)
subnet-0a5ad1f2b057ec63f (IPv4)

Firewall endpoints

1

3. Review

Availability Zone	Firewall subnet	Endpoint ID	Firewall endpoint status
us-east-1a	subnet-04aa77f8be1532f15	vpce-089b0e2dd63a5172b	Ready
us-east-1b	subnet-0a5ad1f2b057ec63f	vpce-0ddf8030b4d0b5dab	Ready

aws | Services | Search [Option+S] | N. Virgini

Security groups

▼ DNS firewall

Rule groups

Domain lists

1. Scroll

▼ Network Firewall

Firewalls

Firewall policies

Network Firewall rule groups

2. Click

TLS conf

Network Firewall resource groups

▼ Virtual private network (VPN)

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

▼ AWS Verified Access

Verified Access instances

VPC > Network Firewall: 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

The following table lists all of your rule groups.

Add rule groups to policy

Your rule groups (2)

Delete | Create rule group

3. Click

Find resources by name or value

Name	Type
DomainAllow-RuleGroup	Stateful
IcmpAlert-RuleGroup	Stateful

Select a rule group

aws Services Search [Option+S] N. Virgini

Step 1
Choose rule group type

Step 2
Describe rule group

Step 3
Configure rules

Step 4 - *optional*
Configure advanced settings

Step 5 - *optional*
Add tags

Step 6
Review and create

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

1. Review

- (●) **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

2. Choose

Suricata compatible rule string

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**.

3. Choose

4. Click

Cancel Next

aws | Services | Search [Option+S] | N. Virgini | User-[redacted]

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

Step 1
Choose rule group type

Step 2
Describe rule group

Step 3
Configure rules

Step 4 - *optional*
Configure advanced settings

Step 5 - *optional*
Add tags

Step 6
Review and create

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.

Suricata-RuleGroup ← 1. Type

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.

10 ← 2. Type

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

3. Click

Cancel | Previous | Next

aws Services Search [Option+S] N. Virgini

IP set references - *optional* Info

An IP set reference is a variable used in your rules that refers to a resource associated with a list of IPs or CIDRs.

Variable name	Resource ID	CIDRs	
IP_set_reference	Choose an IP set	0	Remove
Enter one variable name.	Choose an ID to associate with the variable name.	The number of CIDRs used by this resource.	

1. Scroll

Add IP set reference

You can add as many as 4 more IP set references.

CIDR usage

The total number of CIDRs used by the IP set references accross the firewall.

0/1,000,000

Suricata compatible rule string Info

Suricata is an open source network IPS that includes a standard rule-based language for traffic inspection.

Suricata compatible rule string

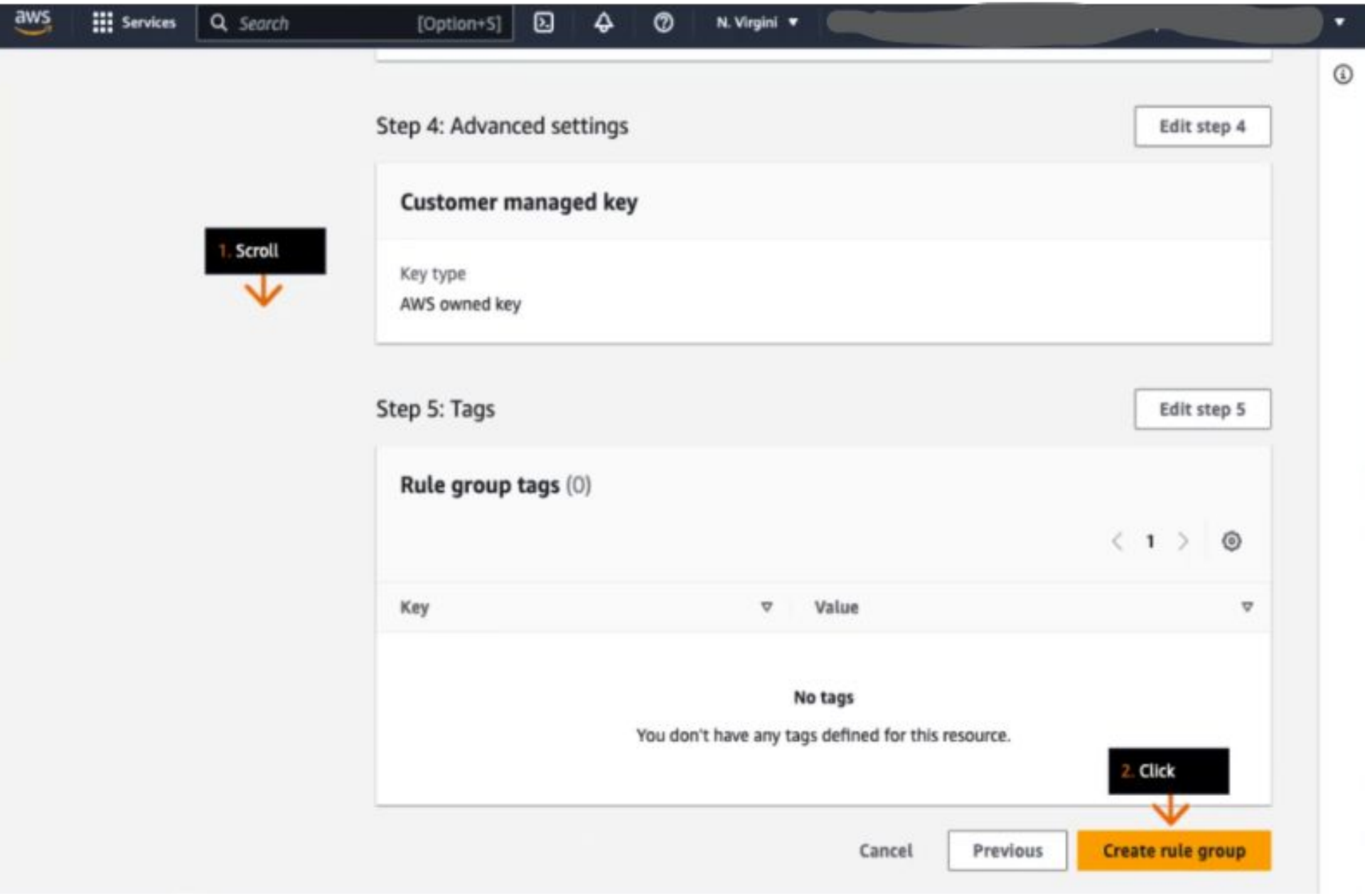
2. Type

```
alert tcp any any <> any 443 (msg:"SURICATA Port 443 but not TLS";
flow:to_server,established; app-layer-protocol:!tls; sid:2271003; rev:1;)
```

Copy rules

3. Click

Cancel Previous Next


aws
Services
Search
[Option+S]
N. Virgini
Step 4: Advanced settings
Edit step 4
Customer managed key
1. Scroll
Key type
AWS owned key
Step 5: Tags
Edit step 5
Rule group tags (0)
1
Key
Value
No tags
You don't have any tags defined for this resource.
2. Click
Cancel
Previous
Create rule group

aws Services Search [Option+S] N. Virgini

Network ACLs

Security groups

DNS firewall

Rule groups

Domain lists

Network Firewall

Firewalls

Firewall policies

2. Click

Network Firewall rule groups

TLS inspection configurations

Network Firewall resource groups

Virtual private network (VPN)

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

You've successfully created rule group Suricata-RuleGroup.

1. Review

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.

Add rule groups to policy

Your rule groups (3)

Delete | Create rule group

Find resources by name or value

1

Name	Type
DomainAllow-RuleGroup	Stateful
IcmpAlert-RuleGroup	Stateful
Suricata-RuleGroup	Stateful

Select a rule group

aws Services Search [Option+S] N. Virgini

Network ACLs

Security groups

DNS firewall

Rule groups

Domain lists

Network Firewall

Firewalls

Firewall policies

Network Firewall rule groups

TLS inspection configurations

Network Firewall resource groups

Virtual private network (VPN)

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

VPC > Network Firewall: Firewall policies

Firewall policies Info

This page lists your Network Firewall firewall policies.

Firewall policies (1)

Delete | Create firewall policy

Find by keyword

1

Name
InspectionFirewall-Policy

1. Click

Select a firewall policy

aws Services Search [Option+S] N. Virgini

Network ACLs
Security groups

DNS firewall
Rule groups
Domain lists

Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups

Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints

Priority | Name | Capacity

Stateful rule evaluation order and default actions

Edit

The way that your stateful rules are order

1. Scroll

Rule order	Default actions
Action order	-

2. Click

Stateful rule groups (2)

Actions

- Create stateful rule group
- Add unmanaged stateful rule groups
- Add managed stateful rule groups
- Disassociate from policy
- Rule group details

3. Choose

Name	Capacity	Is ma	
DomainAllow-RuleGroup	100	No	
IcmpAlert-RuleGroup	100	No	Not available

Capacity units consumed by stateless rule groups
The total capacity units consumed by stateless rule groups can't exceed 30,000.
0/30000

Capacity units consumed by stateful rule groups
The total capacity units consumed by stateful rule groups can't exceed 30,000.
200/30000

aws Services Search [Option+S] N. Virgini

VPC > Network Firewall: Firewall policies > InspectionFirewall-Policy > Add my own stateful rule groups

Add unmanaged stateful rule groups Info

Select and add the stateful rule groups that you want in your firewall policy.

A firewall policy can be associated with multiple firewalls. Modifying a firewall policy affects all firewalls that reference it.
To use rule groups that are managed for you, see AWS Partner Network (APN) integrations.

Stateful rule group (1)

Create rule group

Find resources by name or value

1

	Name
☑	Suricata-RuleGroup

1. Choose

Cancel

Add stateful rule group

2. Click

aws Services Search [Option+S] N. Virgini [redacted]

NAT gateways
Peering connections

▼ Security
Network ACLs
Security groups

▼ DNS firewall
Rule groups
Domain lists

▼ Network Firewall
Firewalls ← 3. Click
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups

▼ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN

Stateful rule evaluation order and default actions

Edit

The way that your stateful rules are ordered for evaluation.

1. Scroll

Rule order	Default actions
Action order	-

Stateful rule groups (3)

2. Review

Actions ▼

1

Name	Capacity	Is managed?	Run in alert mode?
DomainAllow-RuleGroup	100	No	Not available
IcmpAlert-RuleGroup	100	No	Not available
Suricata-RuleGroup	10	No	Not available

Capacity units consumed by stateless rule groups
The total capacity units consumed by stateless rule groups can't exceed 30,000.
0/30000

Capacity units consumed by stateful rule groups
The total capacity units consumed by stateful rule groups can't exceed 30,000.
210/30000

aws Services Search [Option+S] N. Virgini [redacted]

NAT gateways
Peering connections

▼ Security
Network ACLs
Security groups

▼ DNS firewall
Rule groups
Domain lists

▼ Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups

▼ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN

VPC > Network Firewall: Firewalls

Firewalls Info

This page lists your firewalls in AWS Network Firewall.

Firewalls (1)

Delete | Create firewall

Find by keyword

1

	Name	Status	Configuration sync state
○	InspectionFirewall	Ready	In sync

1. Click

Select a firewall

aws Services Search [Option+S] N. Virgini [redacted]

NAT gateways
Peering connections

Security
Network ACLs
Security groups

DNS firewall
Rule groups
Domain lists

Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups

Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN

VPC > Network Firewall: Firewalls > InspectionFirewall

InspectionFirewall Info

Delete

Overview Info

Firewall status	Associated firewall policy	Associated VPC
Ready	Inspection[illegible]	vpc-0c48c4cc7613fec14

1. Click

Firewall details | Firewall policy settings | Monitoring

Firewall details

Edit

Name	Description
InspectionFirewall	-

VPC

Edit

Associated VPC	Firewall subnets
vpc-0c48c4cc7613fec14	subnet-04aa77f8be1532f15 (IPv4) subnet-0a5ad1f2b057ec63f (IPv4)

aws Services Search [Option+S] N. Virgini [redacted]

NAT gateways
Peering connections

▼ Security
Network ACLs
Security groups

▼ DNS firewall
Rule groups
Domain lists

▼ Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups

▼ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN

Change protections

Edit

Delete protection
Disabled

1. Scroll

Subnet change protection
Disabled

Logging

Edit

Network Firewall generates logs for stateful rule groups. You can configure different destinations for different log types.

Log type	Log destination for alerts	Log destination for flows
Flow, Alert	CloudWatch log group - /InspectionFW/TH/Alert	CloudWatch log group - /InspectionFW/TH/Flow

2. Review

Customer managed key

Edit

Key type
AWS owned key

Firewall tags (1)

Edit

1

aws Services cloudwatch N. Virginia

NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall reso groups
Virtual private netwo (VPN)
Customer gateways
Virtual private gatewa
Site-to-Site VPN

1. Type

Services (3)
Features (15)
Resources New
Documentation (11,571)
Knowledge Articles (20)
Marketplace (1,042)
Blogs (531)
Events (4)
Tutorials (1)

Search results for 'cloudwatch'

Try searching with longer queries for more relevant results

Services

CloudWatch 2. Click
Monitor Resources and Applications

Amazon EventBridge
Serverless service for building event-driven applications.

Athena
Serverless interactive analytics service

Features

See all 15 results

Servers
AWS Transfer Family feature

CloudWatch Synthetics
CloudWatch feature

aws Services Search [Option+S] N. Virginia [redacted]

CloudWatch

Favorites and recents

Dashboards

Alarms 0 0 0

Logs

Log groups ← 1. Click

Logs Insights

Live tail New

Metrics

X-Ray traces

Events

Application monitoring

Insights

Settings New

Getting Started

CloudWatch > Log groups

Log groups (3)

By default, we only load up to 10000 log groups.

Actions | View in Logs Insights | Start tailing | Create log group

Filter log groups or try prefix search | Exact match | 1

Log group	Data ...	Sensi...	Retenti...
/InspectionFW/TH/Alert ← 2. Click	-	-	Never expire
/InspectionFW/TH/Flow	-	-	Never expire
/TH/Lambda/RetrieveVpceId-us-east-1	-	-	1 day

Test Simulation

from within our network going outside -then its going to log it in cloudwatch:
echo "Non-TLS test traffic" | nc -w 3 142.250.190.78 443

Test with curl to Send HTTPS Requests
The curl command will send legitimate HTTPS requests to a known website. : curl -v https://www.example.com

check for HTTP/2 200 OK

Test with openssl to Verify TLS Handshake:
openssl s_client -connect www.google.com:443

What to Check:
Look for Verify return code: 0 (ok)

Expert Recommendations

Recommendations for Improving Cloud Security:

- Regular updates to firewall rules.
- Establish incident response protocols for suspicious activity.
- Use advanced monitoring tools like AWS CloudWatch for real-time alerts.

Thank You!