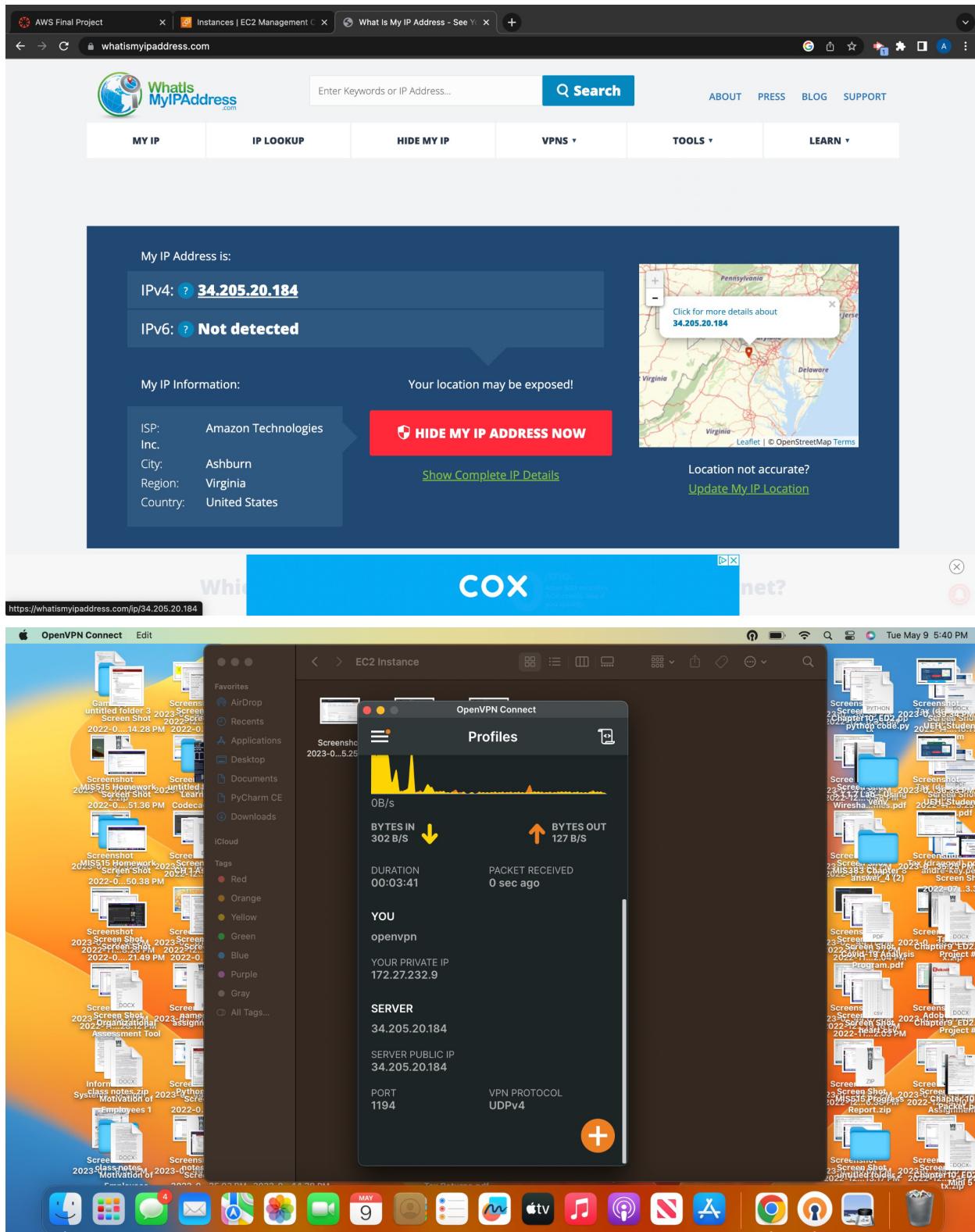


Launching an EC2 instance for OpenVPN - IP before and after connecting to VPN

The screenshot shows the AWS EC2 Management console with the URL us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances. The left sidebar shows navigation options like EC2 Dashboard, Global View, Events, Limits, Instances (selected), Images, AMIs, AMI Catalog, and Elastic Block Store. The main area displays the 'Instances (1/1) Info' page for a single instance named 'my_instance' (i-0b0b5f8c493886260). The instance is listed as 'Running' with an 't2.micro' type, 2/2 checks passed, and located in the 'us-east-1c' availability zone. Below this, the 'Instance: i-0b0b5f8c493886260 (my_instance)' details page is shown, with tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. The 'Details' tab is selected, showing information such as Instance ID (i-0b0b5f8c493886260), Public IPv4 address (34.205.20.184), Private IPv4 addresses (172.31.95.170), and various network and instance type details.

The screenshot shows the whatismyipaddress.com website. The top navigation bar includes links for ABOUT, PRESS, BLOG, and SUPPORT. The main content area displays the user's IP information: My IP (68.1.223.113), IP Lookup, Hide My IP, Tools, and Learn. A prominent green banner from monday.com says 'Work smarter. Accomplish more.' Below this, a map shows the location of the IP address (68.1.223.113) in San Diego, California. The page also provides My IP Information (ISP: Cox Communications LLC, City: San Diego, Region: California, Country: United States) and a button to 'HIDE MY IP ADDRESS NOW'. There are also links to 'Show Complete IP Details' and 'Update My IP Location'.



Setting up monitoring for traffic on the instance - CloudWatch Alarms and Simple Notification Service (SNS).

Screenshot of a Gmail inbox showing an alarm notification from AWS Notifications.

ALARM: "my_primary_alarm" in US East (N. Virginia)

AWS Notifications <no-reply@sns.amazonaws.com> to me 6:33 PM (3 minutes ago)

You are receiving this email because your Amazon CloudWatch Alarm "my_primary_alarm" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [0909337.0 (10/05/23 01:28:00)] was greater than or equal to the threshold (150.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 10 May, 2023 01:33:25 UTC".

View this alarm in the AWS Management Console: https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/my_primary_alarm

Alarm Details:

- Name: my_primary_alarm
- Description: This is my alarm to trigger an email
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [0909337.0 (10/05/23 01:28:00)] was greater than or equal to the threshold (150.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Wednesday 10 May, 2023 01:33:25 UTC
- AWS Account: 844137130423
- Alarm Arn: arn:aws:cloudwatch:us-east-1:844137130423:alarm:my_primary_alarm

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 150.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:

- MetricNamespace: AWS/EC2
- MetricName: NetworkOut
- Dimensions: [InstanceId = i-0b0b5f8c493886260]
- Period: 300 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing

State Change Actions:

- OK: - ALARM: [arn:aws:sns:us-east-1:844137130423:429 sns_andre]
- INSUFFICIENT_DATA:

Screenshot of the AWS CloudWatch Metrics console showing the "my_primary_alarm" metric.

CloudWatch > Alarms > my_primary_alarm

Graph

NetworkOut

NetworkOut ≥ 150 for 1 datapoints within 5 minutes

Bytes

98.5M
49.3M
150

22:30 23:00 23:30 00:00 00:30 01:00 01:30

Click timeline to see the state change at the selected time.

Legend:

- Red circle: In alarm
- Green square: OK
- Grey square: Insufficient data
- Blue square: Disabled actions

Details | Tags | Actions | History | Parent alarms

AWS Final Project

CloudWatch Management Console

Instances | EC2 Management

Creating Visualizations using CloudWatch Metrics

ALARM: "my_primary_alarm"

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:~(alarmStateFilter=~'ALARM')

aws Services cloud WAN

i-0b0b5f8c493886260 1/17 N. Virginia andreyousif

CloudWatch

Favorites and recent

Dashboards

Alarms ▲ 1 ○ 0 ○ 0

In alarm

All alarms

Billing

Logs

Metrics

X-Ray traces

Events

Application monitoring

Insights

Settings

Getting Started

CloudWatch > Alarms

Alarms (1)

Hide Auto Scaling alarms

Clear selection

Create composite alarm

Actions

Create alarm

Search

In alarm Any type Any actions ...

Name	State	Last state update	Conditions	Actions
my_primary_alarm	In alarm	2023-05-09 18:33:25	NetworkOut >= 150 for 1 datapoints within 5 minutes	Actions enabled

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS CloudWatch Management Console interface. The main focus is the 'Alarms' section under the 'CloudWatch' navigation bar. There is one alarm listed: 'my_primary_alarm', which is currently in an 'In alarm' state. The condition for this alarm is 'NetworkOut >= 150 for 1 datapoints within 5 minutes'. The left sidebar provides navigation links for various CloudWatch services such as Logs, Metrics, and X-Ray traces. The top navigation bar includes tabs for AWS Final Project, CloudWatch Management Console, Instances | EC2 Management, Creating Visualizations using CloudWatch Metrics, and ALARM: "my_primary_alarm". The browser address bar shows the URL for the CloudWatch home page.

Configuring S3 storage to hold backups

The screenshot shows the AWS S3 console interface. On the left, a sidebar titled 'Amazon S3' lists various options like 'Access Points', 'Storage Lens', and 'Feature spotlight'. The main area displays the 'andre429bucket' page. At the top, there are tabs for 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Below the tabs, a table lists the single object in the bucket:

Name	Type	Last modified	Size	Storage class
Image2.jpg	jpg	May 8, 2023, 20:30:19 (UTC-07:00)	375.4 KB	Standard

The screenshot shows the 'Create lifecycle rule' configuration page. The 'Lifecycle rule configuration' section includes fields for the rule name ('my_rule') and scope ('Apply to all objects in the bucket'). A note states: 'If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". Learn more'.

The 'Lifecycle rule actions' section contains several options, with the first one checked: 'Move current versions of objects between storage classes'. Other options include 'Move noncurrent versions of objects between storage classes', 'Expire current versions of objects', 'Permanently delete noncurrent versions of objects', and 'Delete expired object delete markers or incomplete multipart uploads'.

The screenshot shows the AWS S3 Management Console interface for creating a lifecycle rule. At the top, there are several tabs and a search bar. Below the search bar, there's a section for filtering actions based on object tags or object size.

Transition current versions of objects between storage classes

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. [Learn more](#)

Choose storage class transitions

Glacier Instant Retrieval ▾ Days after object creation: 7 Remove Add transition

Review transition and expiration actions

Current version actions	Noncurrent versions actions
Day 0 • Objects uploaded	Day 0 No actions defined.
↓	
Day 7 • Objects move to Glacier Instant Retrieval	

Cancel Create rule

The screenshot shows the AWS S3 Management Console displaying a success message: "The lifecycle configuration was updated. Lifecycle rule 'my_rule' was successfully added. It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed."

Lifecycle configuration [Info](#)

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules (1)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Actions	Create lifecycle rule																	
<input type="button" value="View details"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Actions ▾"/>	<input type="button" value="Create lifecycle rule"/>														
<input type="text" value="Find lifecycle rules by name"/>																		
<table border="1"> <thead> <tr> <th>Lifecycle rule name</th> <th>Status</th> <th>Scope</th> <th>Current version actions</th> <th>Noncurrent versions actions</th> <th>Expired object delete markers</th> <th>Incomplete multipart uploads</th> </tr> </thead> <tbody> <tr> <td>my_rule</td> <td>Enabled</td> <td>Entire bucket</td> <td>Transition to Glacier Instant Retrieval</td> <td>-</td> <td>-</td> <td>-</td> </tr> </tbody> </table>					Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads	my_rule	Enabled	Entire bucket	Transition to Glacier Instant Retrieval	-	-	-
Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads												
my_rule	Enabled	Entire bucket	Transition to Glacier Instant Retrieval	-	-	-												

Configuring a backup tool to auto backup the instance- AWS Backup Service

Screenshot of the AWS Backup - Backup vaults page:

AWS Backup > Backup vaults

Backup vaults (2) Info

Backup vaults are containers where your backups are stored. You can have one default vault or multiple vaults where backups can be stored.

Create backup vault

Backup vault name	Vault lock status	Recovery points	KMS encryption key ID
Default	-	1	430a03fd-af4c-4d02-a96b-741b136595bd
my_backup_plan_vault	-	0	430a03fd-af4c-4d02-a96b-741b136595bd

AWS Backup

- My account
 - Dashboard
 - Backup vaults**
 - Backup Vault Lock
 - Backup plans
 - Protected resources
 - Jobs
 - Legal holds
 - Settings
- External resources
 - Gateways
 - Hypervisors
 - Virtual machines
- My organization
 - Cross-account monitoring
 - Backup policies
- Backup Audit Manager
 - Frameworks
 - Reports

CloudWatch | CloudShell | Feedback | Language | © 2023, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Screenshot of the AWS Backup - Backup plans page:

AWS Backup > Backup plans

Summary

Backup plan name	Version ID	Last modified	Last runtime
my_backup_plan	YTQwMGViM2EtOTM3Ny00MDc4LW1YjYtMmNkYTkyOWMzMzGJ	May 8, 2023, 20:22:29 (UTC-07:00)	May 8, 2023, 22:00:14 (UTC-07:00)

Backup rules (3)

Backup rules specify the backup schedule, backup window, and lifecycle rules.

Name	Backup vault	Destination Backup vault
DailyBackups	Default	-
MonthlyBackups	Default	-
WeeklyBackups	my_backup_plan_vault	-

Resource assignments (2)

Resource assignments specify which resources will be backed up by this Backup plan.

Name	IAM role ARN	Creation time
mis_resource	arn:aws:iam::844137130423:role/service-role/AWSBackupDefaultServiceRole	May 8, 2023, 20:26:22 (UTC-07:00)
primary_backup_plan	arn:aws:iam::844137130423:role/service-role/AWSBackupDefaultServiceRole	May 8, 2023, 20:38:09 (UTC-07:00)

AWS Backup

- My account
 - Dashboard
 - Backup vaults
 - Backup Vault Lock
 - Backup plans
 - Protected resources
 - Jobs
 - Legal holds
 - Settings
- External resources
 - Gateways
 - Hypervisors
 - Virtual machines
- My organization
 - Cross-account monitoring
 - Backup policies
- Backup Audit Manager
 - Frameworks
 - Reports

CloudWatch | CloudShell | Feedback | Language | © 2023, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Creating IAM users with the permissions/policies

AWS Final Project | CloudWatch Management Con... | Inbox (2,324) - ayousif1832@... | Real Madrid 1-1 Manchester C... | IAM Management Console | +

us-east-1.console.aws.amazon.com/iamv2/home#/users/details/ec2access_andre?section=permissions

aws Services Search [Option+S] Global andreyousif

Identity and Access Management (IAM)

1 policy removed

IAM > Users > ec2access_andre

ec2access_andre

Delete

Summary

ARN arn:aws:iam::844137130423:user/ec2access_andre	Console access ⚠ Enabled without MFA	Access key 1 Not enabled
Created May 09, 2023, 18:15 (UTC-07:00)	Last console sign-in Never	Access key 2 Not enabled

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Directly

Find policies < 1 > ⌂

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Language

AWS Final Project | CloudWatch Management Con... | Inbox (2,325) - ayousif1832@... | Real Madrid 1-1 Manchester C... | IAM Management Console | +

us-east-1.console.aws.amazon.com/iamv2/home#/users/details/S3access_andre?section=permissions

aws Services Search [Option+S] Global andreyousif

Identity and Access Management (IAM)

1 policy removed

IAM > Users > S3access_andre

S3access_andre

Delete

Summary

ARN arn:aws:iam::844137130423:user/S3access_andre	Console access ⚠ Enabled without MFA	Access key 1 Not enabled
Created May 09, 2023, 18:17 (UTC-07:00)	Last console sign-in Never	Access key 2 Not enabled

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (3)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonInspector2FullAccess	AWS managed	Directly
AmazonS3FullAccess	AWS managed	Directly
AWSBackupServiceRolePolicyForS...	AWS managed	Directly

Find policies < 1 > ⌂

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Language

Screenshot of the AWS IAM Management Console showing the 'Users' page. The left sidebar shows 'Identity and Access Management (IAM)'. The main area displays two users: 'ec2access_andre' and 'S3access_andre'. Both users have 'None' for Groups, Last activity, MFA, Password age, and Active key age.

User name	Groups	Last activity	MFA	Password age	Active key age
ec2access_andre	None	Never	None	3 minutes ago	-
S3access_andre	None	Never	None	1 minute ago	-

Configuring a vulnerability scanner - Inspector - REPORT

Screenshot of the Amazon Inspector console showing the 'Findings' page. A modal window titled 'Introducing the new Amazon Inspector' provides information about the service's capabilities. The main table lists three findings:

Severity	Date	Finding	Target	Template
Medium	Yesterday at...	On instance i-0b0b5f8c493886260, TCP port 22 which is associated with 'SSH' is reac...	Assessment-Targe...	Assessment-
Low	Yesterday at...	On instance i-0b0b5f8c493886260, TCP port 443 which is associated with 'HTTPS' is ...	Assessment-Targe...	Assessment-
Informational	Yesterday at...	Aggregate network exposure: On instance i-0b0b5f8c493886260, ports are reachable f...	Assessment-Targe...	Assessment-

Creating and Deploying an EC2 Instance with OpenVPN

As part of this project, I have implemented an AWS-based cloud system that utilizes EC2 instances with OpenVPN Server, CloudWatch, backup services, IAM, and Inspector. Throughout the process, I have taken into consideration the principles of cloud and information security, recognizing their importance and the benefits they bring to the system and its users.

I began by launching an EC2 instance for OpenVPN Server and configuring it by SSH into the instance. I then set up monitoring for traffic on the instance by enabling detailed monitoring and configuring CloudWatch Alarms to monitor network traffic on the instance. I configured S3 storage to hold backups, and set up a vulnerability scanner by creating an assessment template and launching an assessment run.

One of the key components of my system is the use of EC2 instances with OpenVPN Server. This allows for secure remote access to the system while also ensuring that all data transmissions are encrypted. To further enhance the security of my system, I have implemented Identity and Access Management (IAM) to control access to AWS resources, limiting access to only authorized users and groups.

As part of my AWS-based cloud system, I have also created an S3 bucket and implemented lifecycle rules to move backups to Glacier. First, I created an S3 bucket to store my backups and other data. I ensured that the bucket was configured with appropriate permissions and access controls to limit access to authorized users and groups only. I also enabled versioning

to ensure that previous versions of files could be recovered if necessary. Next, I implemented lifecycle rules to manage the lifecycle of my backups.

To ensure the reliability and availability of my system, I have implemented backup services, including AWS Backup, to protect against data loss and to ensure that my data is always recoverable in the event of a disaster. Additionally, I have implemented CloudWatch to monitor my application's network traffic.

Furthermore, I have implemented Inspector to perform regular security assessments and vulnerability scans, ensuring that my system is secure and up-to-date with the latest security patches and updates. Throughout the design and implementation of my system, I have prioritized information security by adhering to key principles such as confidentiality, integrity, and availability.

In conclusion, the implementation of an AWS-based cloud system utilizing EC2 instances with OpenVPNServer, CloudWatch, backup services, IAM, and Inspector has proven to be an effective solution for any organization. By adhering to the principles of cloud and information security, I have created a secure and reliable system that meets the needs of users while also protecting their data and privacy.

Securing the System

When it comes to further securing a system, there are several measures that can be taken beyond the basic security controls already in place. Regularly updating and patching the system is an important topic in system hardening. Regularly applying security updates and patches to the system is very important because it can help to address known vulnerabilities and prevent attackers from exploiting them. Also, disabling services and protocols that are not needed can reduce the attack surface of the system and minimize the risk of a successful attack.

In addition, network security measures such as firewalls, intrusion detection and prevention systems, and virtual private networks can help to protect the system from network-based attacks. Also, using secure protocols such as HTTPS, SSH, and TLS can help to protect data in transit and prevent attacks. Encrypting sensitive data at rest can also provide an additional layer of protection.

Furthermore, implementing access controls such as user accounts and permissions, can help to limit access to sensitive information and prevent unauthorized access. Monitoring system logs can help to detect suspicious activity and potential security breaches. Log files should be stored securely and regularly reviewed for any unusual activity.

Finally, conducting regular security audits can help to identify any vulnerabilities or weaknesses in the system and provide recommendations for improving security. Also, implementing Multi-Factor Authentication (MFA) adds an extra layer of security to the authentication process, making it more difficult for attackers to gain unauthorized access.

3 Months Support Plan

I provided a three month support plan to continue running this VPN Server in AWS and described how I would support it while keeping security in mind. The plan includes regular patching and updating of the system, and monitoring logs for malicious or unauthorized access. I also identified the roles and responsibilities of the System Administrator and Security Analyst in carrying out these tasks. By following this plan, I can ensure the system's availability and protect it from security threats.

I would recommend applying security patches and updates as soon as they become available. Depending on the severity of the vulnerability, I would either update the system immediately or schedule a maintenance window. I would check for updates weekly and apply them during a maintenance window.

Monitoring logs for any suspicious activity, such as unauthorized access attempts or unusual traffic patterns. Reviewing logs weekly to identify any security incidents and take necessary actions to mitigate them. Implementing Multi-Factor Authentication (MFA) for all users to restrict access to the VPN and setting up ACL.

As of roles and responsibilities, the following roles would be responsible for the above tasks. A System Administrator would be responsible for applying patches and updates, maintaining the system, and configuring security features. A Security Analyst would be responsible for monitoring logs, analyzing security incidents, and providing recommendations for improving the system's security.

In conclusion, these three months support plan outlines the approach to supporting the VPN system in AWS while keeping security in mind. By implementing regular patching, monitoring logs, and improving security features, it can ensure the system's availability and protect it from security threats.

Incident Response Plan

In the event of a security breach or compromise of my EC2 instance and VPN, my incident response plan will involve the following steps. The first step would be to isolate the affected system from the network to prevent further damage and to preserve evidence for forensic analysis. Once the system has been contained, I will conduct an analysis of the incident to determine the scope and nature of the attack, the information that may have been compromised, and the potential impact on my application. I will take immediate steps to mitigate the damage caused by the attack, such as changing access codes and passwords, scanning for malware, and implementing additional security controls. Depending on the severity of the attack, I may need to rebuild the affected application from scratch. If backups are available, I will restore the application from the most recent backup that has been verified as clean. I will also conduct a thorough review of my backup procedures to ensure that they are secure and up-to-date. I will investigate the source of the attack to determine whether it was the result of an external threat or an internal security breach. I will use all available resources to identify the attacker, including network logs, system logs, and any other relevant data.

In conclusion, my incident response plan is designed to help me quickly and effectively respond to security incidents and minimize the impact on my application. I will continually review and update my plan to ensure that it remains effective against new and evolving threats.