

NETWORK SECURITY ASSESSMENT REPORT

EXECUTIVE SUMMARY

In the Network Security Assessment of our AWS cloud infrastructure, several key findings and recommendations have been highlighted. The assessment revealed opportunities to improve network segmentation for enhanced resource isolation, tighten access control policies, and ensure consistent usage of VPC Flow Logs for better security monitoring. Furthermore, the report suggests enhancing our DDoS protection mechanisms for automated network routing and real-time attack insights. Our AWS environment has shown resilience and scalability, but implementing these recommendations will further bolster our network security, ensuring a more secure and agile cloud infrastructure. We acknowledge the efforts of our IT and security teams and look forward to implementing these improvements.

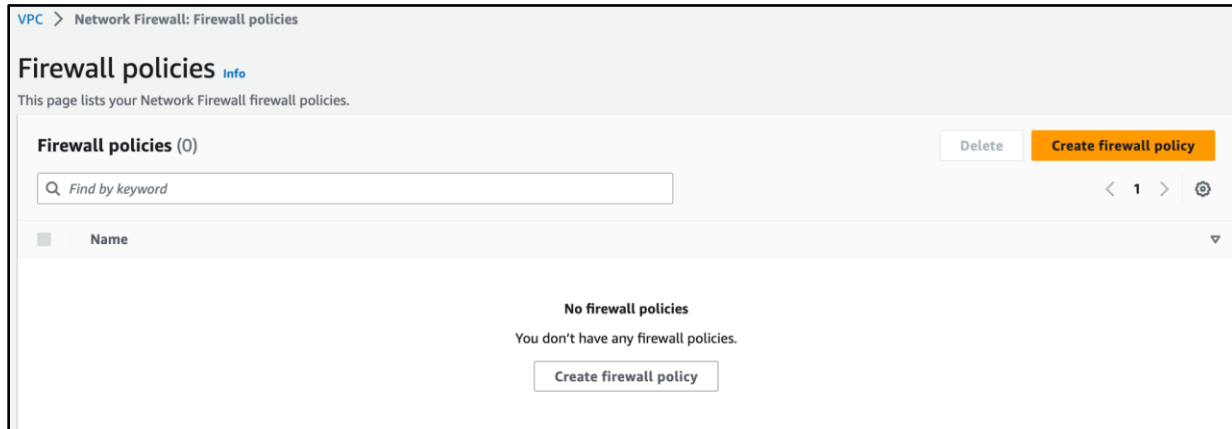
SUMMARY OF FINDINGS

AWS Resources	Security Gap	Severity
Security Groups	Security group PublicSG has SSH port 22 open to the internet. Instance security group has SSH port 22 open to the internet	High
Subnets	VPC does not have Network Firewall enabled. VPC Flow logs are disabled. VPC subnet assigns public ip by default	Medium
S3	S3 User has the inline policy bucket-access attached	Low
Security Groups	Security group PublicSG is not being used. Security group PrivateSG is not being used.	Low

VPC does not have Network Firewall enabled.

Description: VPC does not have Network Firewall enabled.

Severity: Medium



Potential Impact:

In a healthcare setting, turning off a network firewall can lead to a serious security lapse that could expose patient data to cyberattacks and illegal access. The organization is more susceptible to network attacks, data breaches, and non-compliance with healthcare data protection regulations when its firewall is not active. This puts patient data at risk and may have negative legal and reputational effects.

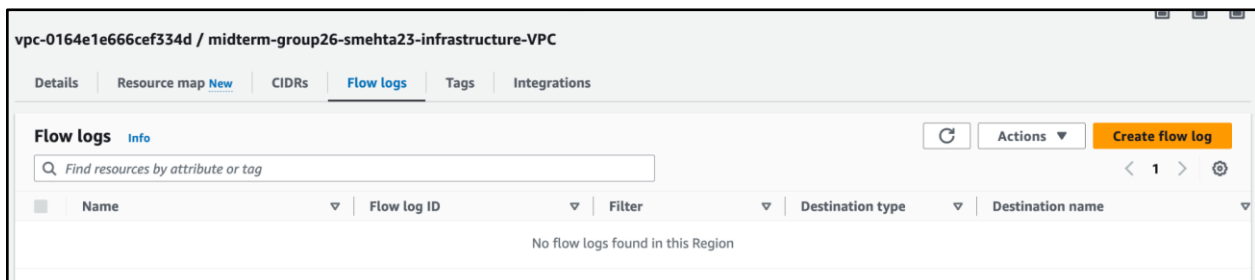
Remediation:

Ensure all VPCs have Network Firewall enabled.

VPC Flow logs are disabled.

Description: VPC Flow logs are disabled

Severity: Medium



Potential Impact:

Disabling VPC flow logs in a healthcare organization's cloud environment can hinder the ability to monitor and audit network traffic. This lack of visibility may make it challenging to detect and investigate security incidents, data breaches, and unauthorized access to patient data, potentially compromising data security and compliance.

Remediation:

It is recommended that VPC Flow Logs be enabled for packet Rejects for VPCs.

VPC subnet assigns public IP by default.

Description: VPC subnet assigns public IP by default

Severity: Medium

subnet-0aa5c260635b26222 / midterm-group26-smehta23-infrastructure-Public-A

Actions ▾

Details

Subnet ID subnet-0aa5c260635b26222	Subnet ARN arn:aws:ec2:us-east-1:344784239560:subnet/subnet-0aa5c260635b26222	State Available	IPv4 CIDR 10.1.10.0/24
Available IPv4 addresses 250	IPv6 CIDR -	Availability Zone us-east-1a	Availability Zone ID use1-az4
Network border group us-east-1	VPC vpc-0164e1e666cef334d midterm-group26-smehta23-infrastructure-VPC	Route table rtb-0890439c34ff8b114 Public	Network ACL acl-017159aad54ed4a1d
Default subnet No	Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool -	Outpost ID -	IPv4 CIDR reservations -	IPv6 CIDR reservations -
IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled
DNS64 Disabled	Owner 344784239560		

Potential Impact:

The risk of data exposure and breaches can be increased when VPC subnets assign public IP addresses by default, unintentionally exposing patient data to the public internet. Patients' privacy and data integrity may be compromised as a result, along with possible legal action, noncompliance with data protection laws, and privacy violations.

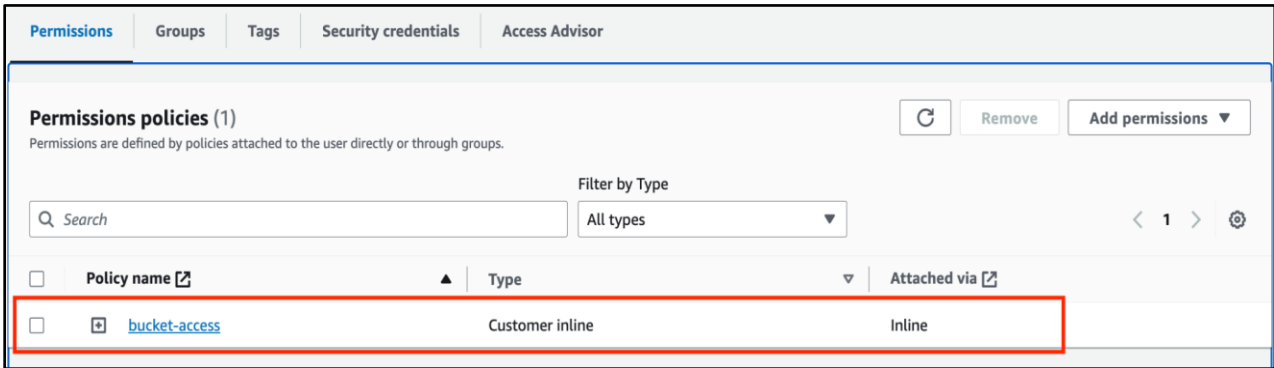
Remediation:

VPC subnets should not allow automatic public IP assignment.

S3 User has the inline policy bucket-access attached.

Description: S3 User has the inline policy bucket-access attached

Severity: Low



Potential Impact:

An S3 bucket with an inline policy attached that allows for excessive access can put patient data at serious risk of security breaches. These policies could unintentionally give unauthorized users extensive access to the data, which could lead to privacy violations and data breaches.

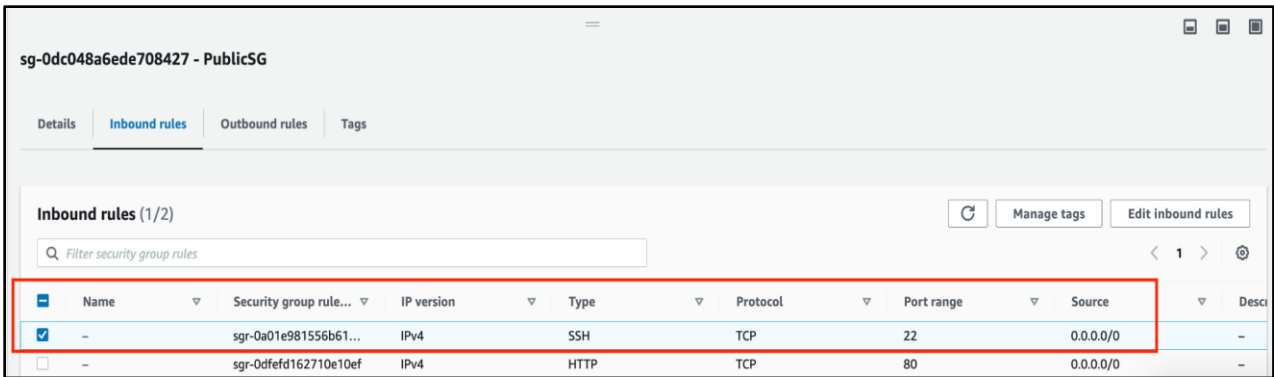
Remediation:

Remove any policy attached directly to the user. Use groups or roles instead.

Security group PublicSG has SSH port 22 open to the internet.

Description: Security group PublicSG has SSH port 22 open to the internet

Severity: High



Potential Impact:

Security risks to patient data may arise from leaving a security group (PublicSG) open to the internet and leaving port 22 (SSH) open. This setup could give unwanted users access to the system, which could result in data breaches, privacy violations, and compliance problems. These could have major repercussions for the healthcare provider's reputation and legal standing.

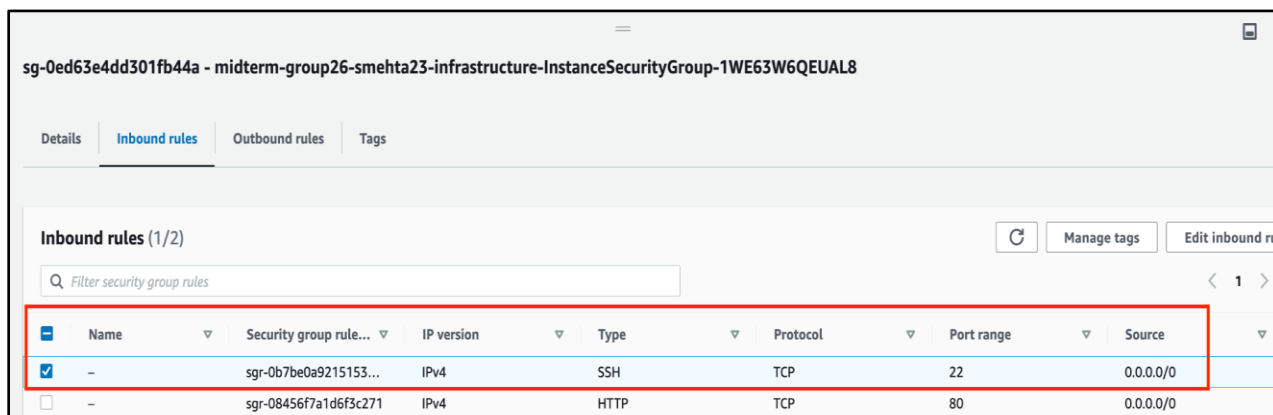
Remediation:

Use a Zero Trust approach. Narrow ingress traffic as much as possible. Consider north-south as well as east-west traffic.

Instance security group has SSH port 22 open to the internet.

Description: Instance security group has SSH port 22 open to the internet.

Severity: High



sg-0ed63e4dd301fb44a - midterm-group26-smehta23-infrastructure-InstanceSecurityGroup-1WE63W6QEUAL8

Details Inbound rules Outbound rules Tags

Inbound rules (1/2)

Filter security group rules

	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input checked="" type="checkbox"/>	-	sgr-0b7be0a9215153...	IPv4	SSH	TCP	22	0.0.0.0/0
<input type="checkbox"/>	-	sgr-08456f7a1d6f3c271	IPv4	HTTP	TCP	80	0.0.0.0/0

Potential Impact:

Security risks to patient data may arise from leaving a security group (Instance SG) open to the internet and leaving port 22 (SSH) open. This setup could give unwanted users access to the system, which could result in data breaches, privacy violations, and compliance problems. These could have major repercussions for the healthcare provider's reputation and legal standing.

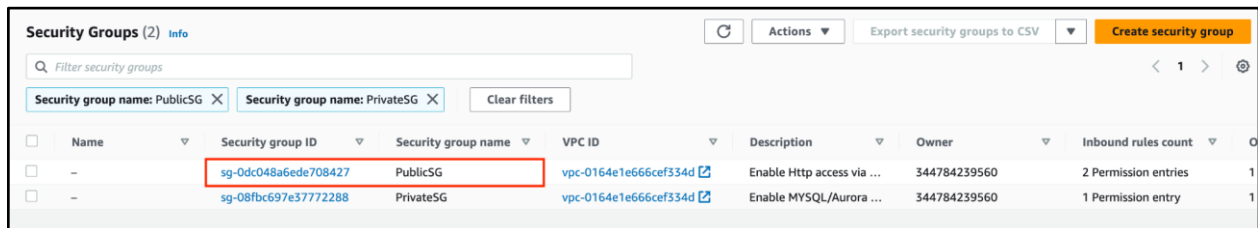
Remediation:

Use a Zero Trust approach. Narrow ingress traffic as much as possible. Consider north-south as well as east-west traffic.

Security group PublicSG is not being used.

Description: Security group PublicSG is not being used

Severity: Low

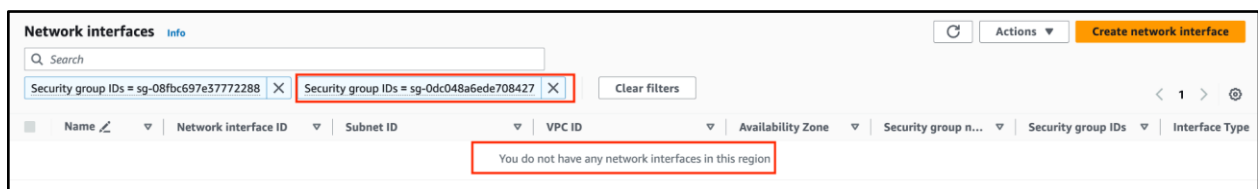


Security Groups (2) Info

Filter security groups

Security group name: PublicSG X Security group name: PrivateSG X Clear filters

	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	
<input type="checkbox"/>	-	sg-0dc048a6ede708427	PublicSG	vpc-0164e1e666cef334d	Enable Http access via ...	344784239560	2 Permission entries	1
<input type="checkbox"/>	-	sg-08fbc697e37772288	PrivateSG	vpc-0164e1e666cef334d	Enable MySQL/Aurora ...	344784239560	1 Permission entry	1



Network interfaces Info

Search

Security group IDs = sg-08fbc697e37772288 X Security group IDs = sg-0dc048a6ede708427 X Clear filters

	Name	Network interface ID	Subnet ID	VPC ID	Availability Zone	Security group n...	Security group IDs	Interface Type
You do not have any network interfaces in this region								

Potential Impact:

Unused public security groups have the potential to open security holes in cloud infrastructure, making it possible for unauthorized users to access resources holding patient data. The confidentiality and privacy of patient information, as well as the standing of the healthcare organization, may be at risk due to this underutilized security group's exposure to data, breaches, and problems with regulatory compliance.

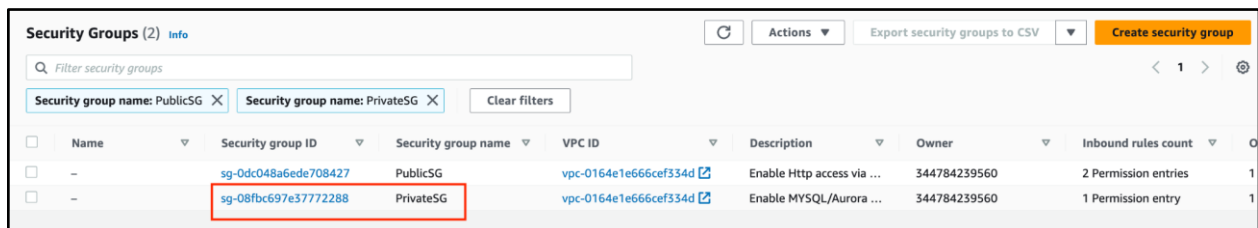
Remediation:

List all the security groups and then use the cli to check if they are attached to an instance.

Security group PrivateSG is not being used.

Description: Security group PrivateSG is not being used

Severity: Low

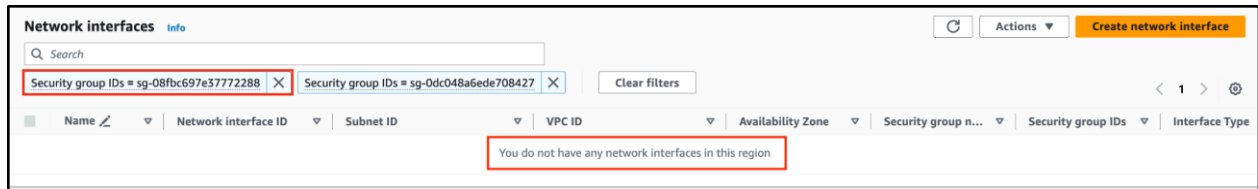


Security Groups (2) Info

Filter security groups

Security group name: PublicSG X Security group name: PrivateSG X Clear filters

	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	
<input type="checkbox"/>	-	sg-0dc048a6ede708427	PublicSG	vpc-0164e1e666cef334d	Enable Http access via ...	344784239560	2 Permission entries	1
<input type="checkbox"/>	-	sg-08fbc697e37772288	PrivateSG	vpc-0164e1e666cef334d	Enable MySQL/Aurora ...	344784239560	1 Permission entry	1



Potential Impact:

Ineffective use of a private security group can lead to needless access restrictions and difficulties in controlling access to resources that hold patient data. This underutilized security group might make it more difficult for authorized parties to access data, which could cause problems with compliance, disrupt operations, and make it more difficult to provide patient care.

Remediation:

List all the security groups and then use the cli to check if they are attached to an instance.

