 # Part II
Classic AWS Architecture Design
(30 marks total)
Part II.1. - Base design questions (20/30 marks)

To provide illustration in `.drawio` or exported `.png`:
- (5/30 marks) Suggest a CIDR division table for each subnets in each Network tiers
- (5/30 marks) To illustrate the VPC, Subnets design according to your CIDR division above
- (5/30 marks) To correctly place these components:
  - EC2 in AutoScalingGroups
  - RDS database and EFS network file system with 1-AZ failover setup (feel free to choose main and failover AZ)
  - ALB and NATGW
  - AWS Network Firewall endpoints
  - IGW (AWS Internet Gateway)
- (5/30 marks) To correctly design:
  - The Route Tables as well as
  - Inbound and Outbound rules for the different Security Groups
End.

Objective:
Research and improve on the base Virtual Private Cloud (VPC) example.
Design the new cloud infrastructure, produce specification documentation and architecture diagrams.

 # Resilient Architecture Specification Document:
This record needs to be progressively completed throughout concept and development phases. It documents the existing conditions, design considerations, parameters and details, actions, technical decisions, design verifications and safety considerations. Key values underpinning resilient architecture:
- Cost-efficient
- Available
- Fault-tolerant
- Scalable

The following items are in scope for the new design. The technology stack has a dependency on this work and will leverage the Amazon Web Services (AWS) capability to deliver service or secure existing services.

New VPC Design Requirements:

- There are **3 Availability Zones (AZ)** for the VPC with each subnet tier spanning across all 3 AZs.
- There are **5 VPC subnet tiers**:
1) **Public subnets AWS Network `Firewall Tier`**.
2) **Public subnets 'Protected Tier'** by AWS Network Firewall, contains AWS **Application Load Balancer (ALB)** and **Network Address Translation Gate Way (NATGW).**
3) **Private subnets `Multi-Purpose Tier`** contains **Elastic Compute Cloud (EC2)** workloads, **`microservices`** managed by the **'AutoScalingGroup'**, and load balanced by the ALB.
4) **Private subnets `Secure Tier`** contains AWS ** Relational Database Service (RDS), Elastic File System (EFS)** and **AWS Managed databases.**
5) **Private subnets `Management Tier`** contains **EC2 jump hosts** for the **'AWS Manager - Session Manager'**, **RDS access from the `Secure Tier` only;** No other "hops" allowed.
- All **traffic into** the VPC is inspected by the **AWS Network Firewall service**.
- All **traffic out** to the public internet is inspected by **AWS Network Firewall service**

Opportunities/ Recommendations:
- ****Set up 3 Elastic IP address**** for the NAT gateway in the architecture example given.
- Network EC2 in a private subnet and public subnet with **NAT Gateway routing to private subnet**
- Produce updated network policy documentation and design specification documentation regularly throughout implementation phase and after go-live.
- Use **Security Group Source** with SG-Id;
- Use **VPC Endpoint** for S3;
- Use **IAM database authentication tokens** generated using AWS access keys.
- Use ****Transit Gateway**** to connect VPCs to simplify network architecture.
- Use ****AWS PrivateLink**** to access AWS services over private network connections instead of the public internet.
- Use ****AWS Direct Connect**** to establish a dedicated network connection from on-premise to AWS.
- Use ****AWS Global Accelerator**** to improve the availability and performance of applications by routing traffic over the AWS global network.
- Use **Highest value for maximum connections** AWS RDS micro instance.
Table - showing RDS connections forecast:

```
MODEL      max_connections innodb_buffer_pool_size
---------  --------------- ----------------------
t1.micro   34                326107136 (  311M)
m1-small   125              1179648000 ( 1125M,  1.097G)
m1-large   623              5882511360 ( 5610M,  5.479G)
m1-xlarge  1263            11922309120 (11370M, 11.103G)
```

```
m2-xlarge  1441            13605273600 (12975M, 12.671G)
m2-2xlarge 2900            27367833600 (26100M, 25.488G)
m2-4xlarge 5816            54892953600 (52350M, 51.123G)
```

New VPC Classless Inter-Domain Routing (CDIR) Strategy:

- Use CDIR method for allocating IP addresses and for IP routing.
- **Master CIDR 10.0.0.0/16**
- Plan for scaling.
- Leverage AWS **Network Address Use (NAU)** tables for all network architecture; **Find Sum of NAU Units**
- Use NAU current/future state to plan/design Subnet Groups/ CDIR Blocks
- **1 VPC, 3 AZ, 5 Tiers**
- **NAU 158**
- **10.0.0.0/20-10.0.0.0/24**
- Don't use the first four IP addresses and the last IP address in each subnet CIDR block. These cannot be assigned to a resource, such as an EC2 instance. For example, in subnet CIDR block 10.0.0.0/24, the following five IP addresses are reserved:
  - 10.0.0.0: Network address.
  - 10.0.0.1: Reserved by AWS for the VPC router.
  - 10.0.0.2: Reserved by AWS.
  - 10.0.0.3: Reserved by AWS for future use.
  - 10.0.0.255: Network broadcast address and can’t be used in a VPC.
- Don’t use 172.17.0.0/16 CIDR range as it conflicts with services like AWS Cloud9 or Amazon SageMaker.

AWS Network Address Use Table:

Resource	**NAU units**
Each IPv4 and IPv6 address assigned to a network interface for an EC2 instance in the VPC	1
Additional network interfaces attached to an EC2 instance	1
Prefix assigned to a network interface	1

Resource	NAU units
Network Load Balancer per AZ	6
VPC endpoint per AZ	6
Transit gateway attachment	6
Lambda function	6
NAT gateway	6
EFS attached to an EC2 instance	6

![Network Address Usage Calculation (NAU)](<Screenshot 2024-01-06 at 4.17.40 AM.png>)

How NAU is calculated

If you understand how NAU is calculated, it can help you plan for the scaling of your VPCs.

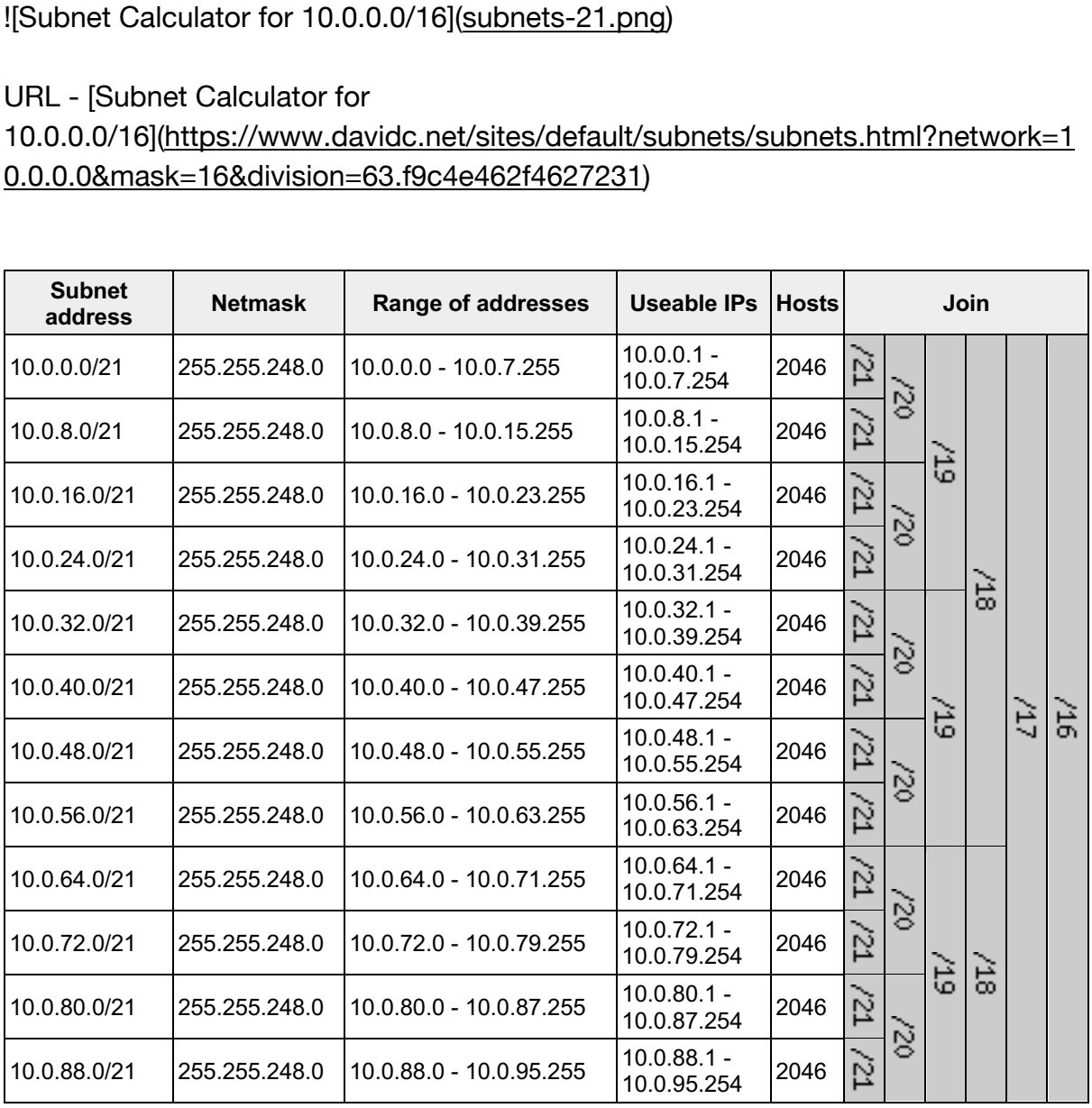
The following table explains which resources make up the NAU count in a VPC and how many NAU units each resource uses. Some AWS resources are represented as single NAU units and some resources are represented as multiple NAU units. You can use the table to learn how NAU is calculated.

Resource	NAU units
Each IPv4 and IPv6 address assigned to a network interface for an EC2 instance in the VPC	1
Additional network interfaces attached to an EC2 instance	1
Prefix assigned to a network interface	1
Network Load Balancer per AZ	6
VPC endpoint per AZ	6
Transit gateway attachment	6
Lambda function	6
NAT gateway	6
EFS attached to an EC2 instance	6

New VPC NAU Calculation:
15 – IPv4 subnets x15
03 – Additional Services x3

05 – Service improvements x3
18 – Application Load Balancer x3
90 – AZ 3 x 5 tier VPC X 6 per endpoint
06 – Possible Transit gateway
06 - Lambda S3
06 - NAT Gateway
06 - EFS per twin EC2 instance
03 - Network Firewall endpoint requires a dedicated subnet
****Total 158 NAU Units****

New VPC CDIR/Subnet Groups:
CDIR Master: 10.0.0.0/16



URL - [Subnet Calculator for 10.0.0.0/16](https://www.davidc.net/sites/default/subnets/subnets.html?network=10.0.0.0&mask=16&division=63.f9c4e462f4627231)

Subnet address	Netmask	Range of addresses	Useable IPs	Hosts
10.0.0.0/21	255.255.248.0	10.0.0.0 - 10.0.7.255	10.0.0.1 - 10.0.7.254	2046
10.0.8.0/21	255.255.248.0	10.0.8.0 - 10.0.15.255	10.0.8.1 - 10.0.15.254	2046
10.0.16.0/21	255.255.248.0	10.0.16.0 - 10.0.23.255	10.0.16.1 - 10.0.23.254	2046
10.0.24.0/21	255.255.248.0	10.0.24.0 - 10.0.31.255	10.0.24.1 - 10.0.31.254	2046
10.0.32.0/21	255.255.248.0	10.0.32.0 - 10.0.39.255	10.0.32.1 - 10.0.39.254	2046
10.0.40.0/21	255.255.248.0	10.0.40.0 - 10.0.47.255	10.0.40.1 - 10.0.47.254	2046
10.0.48.0/21	255.255.248.0	10.0.48.0 - 10.0.55.255	10.0.48.1 - 10.0.55.254	2046
10.0.56.0/21	255.255.248.0	10.0.56.0 - 10.0.63.255	10.0.56.1 - 10.0.63.254	2046
10.0.64.0/21	255.255.248.0	10.0.64.0 - 10.0.71.255	10.0.64.1 - 10.0.71.254	2046
10.0.72.0/21	255.255.248.0	10.0.72.0 - 10.0.79.255	10.0.72.1 - 10.0.79.254	2046
10.0.80.0/21	255.255.248.0	10.0.80.0 - 10.0.87.255	10.0.80.1 - 10.0.87.254	2046
10.0.88.0/21	255.255.248.0	10.0.88.0 - 10.0.95.255	10.0.88.1 - 10.0.95.254	2046

Subnet address	Netmask	Range of addresses	Useable IPs	Hosts	Join					
10.0.96.0/21	255.255.248.0	10.0.96.0 - 10.0.103.255	10.0.96.1 - 10.0.103.254	2046	/21	/20	/19	/18	/17	
10.0.104.0/21	255.255.248.0	10.0.104.0 - 10.0.111.255	10.0.104.1 - 10.0.111.254	2046	/21					
10.0.112.0/21	255.255.248.0	10.0.112.0 - 10.0.119.255	10.0.112.1 - 10.0.119.254	2046	/21	/20				
10.0.120.0/21	255.255.248.0	10.0.120.0 - 10.0.127.255	10.0.120.1 - 10.0.127.254	2046	/21					
10.0.128.0/21	255.255.248.0	10.0.128.0 - 10.0.135.255	10.0.128.1 - 10.0.135.254	2046	/21	/20	/19			
10.0.136.0/21	255.255.248.0	10.0.136.0 - 10.0.143.255	10.0.136.1 - 10.0.143.254	2046	/21					
10.0.144.0/21	255.255.248.0	10.0.144.0 - 10.0.151.255	10.0.144.1 - 10.0.151.254	2046	/21	/20				
10.0.152.0/21	255.255.248.0	10.0.152.0 - 10.0.159.255	10.0.152.1 - 10.0.159.254	2046	/21					
10.0.160.0/21	255.255.248.0	10.0.160.0 - 10.0.167.255	10.0.160.1 - 10.0.167.254	2046	/21	/20	/19			
10.0.168.0/21	255.255.248.0	10.0.168.0 - 10.0.175.255	10.0.168.1 - 10.0.175.254	2046	/21					
10.0.176.0/21	255.255.248.0	10.0.176.0 - 10.0.183.255	10.0.176.1 - 10.0.183.254	2046	/21	/20				
10.0.184.0/21	255.255.248.0	10.0.184.0 - 10.0.191.255	10.0.184.1 - 10.0.191.254	2046	/21					
10.0.192.0/21	255.255.248.0	10.0.192.0 - 10.0.199.255	10.0.192.1 - 10.0.199.254	2046	/21	/20	/19			
10.0.200.0/21	255.255.248.0	10.0.200.0 - 10.0.207.255	10.0.200.1 - 10.0.207.254	2046	/21					
10.0.208.0/21	255.255.248.0	10.0.208.0 - 10.0.215.255	10.0.208.1 - 10.0.215.254	2046	/21	/20				
10.0.216.0/21	255.255.248.0	10.0.216.0 - 10.0.223.255	10.0.216.1 - 10.0.223.254	2046	/21					
10.0.224.0/21	255.255.248.0	10.0.224.0 - 10.0.231.255	10.0.224.1 - 10.0.231.254	2046	/21	/20	/19			
10.0.232.0/21	255.255.248.0	10.0.232.0 - 10.0.239.255	10.0.232.1 - 10.0.239.254	2046	/21					
10.0.240.0/21	255.255.248.0	10.0.240.0 - 10.0.247.255	10.0.240.1 - 10.0.247.254	2046	/21	/20				
10.0.248.0/21	255.255.248.0	10.0.248.0 - 10.0.255.255	10.0.248.1 - 10.0.255.254	2046	/21					

Secure Application Specifications

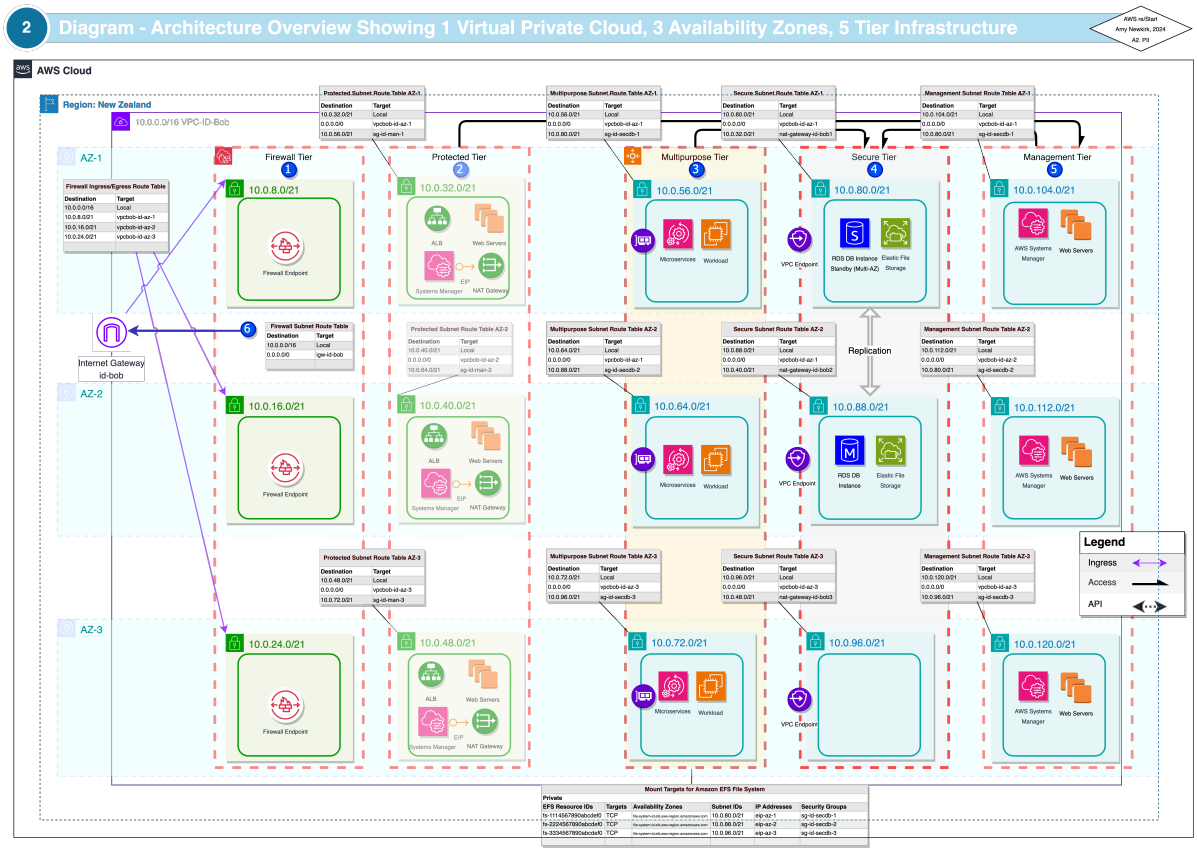
The following diagram provides an overview of the resources included in the preliminary design. The VPC has public subnets and private subnets in three Availability Zones. Each public subnet contains a NAT gateway and an application load balancer. The workload servers run in the private subnets, are launched and terminated by using an Auto Scaling group, and receive traffic from the load

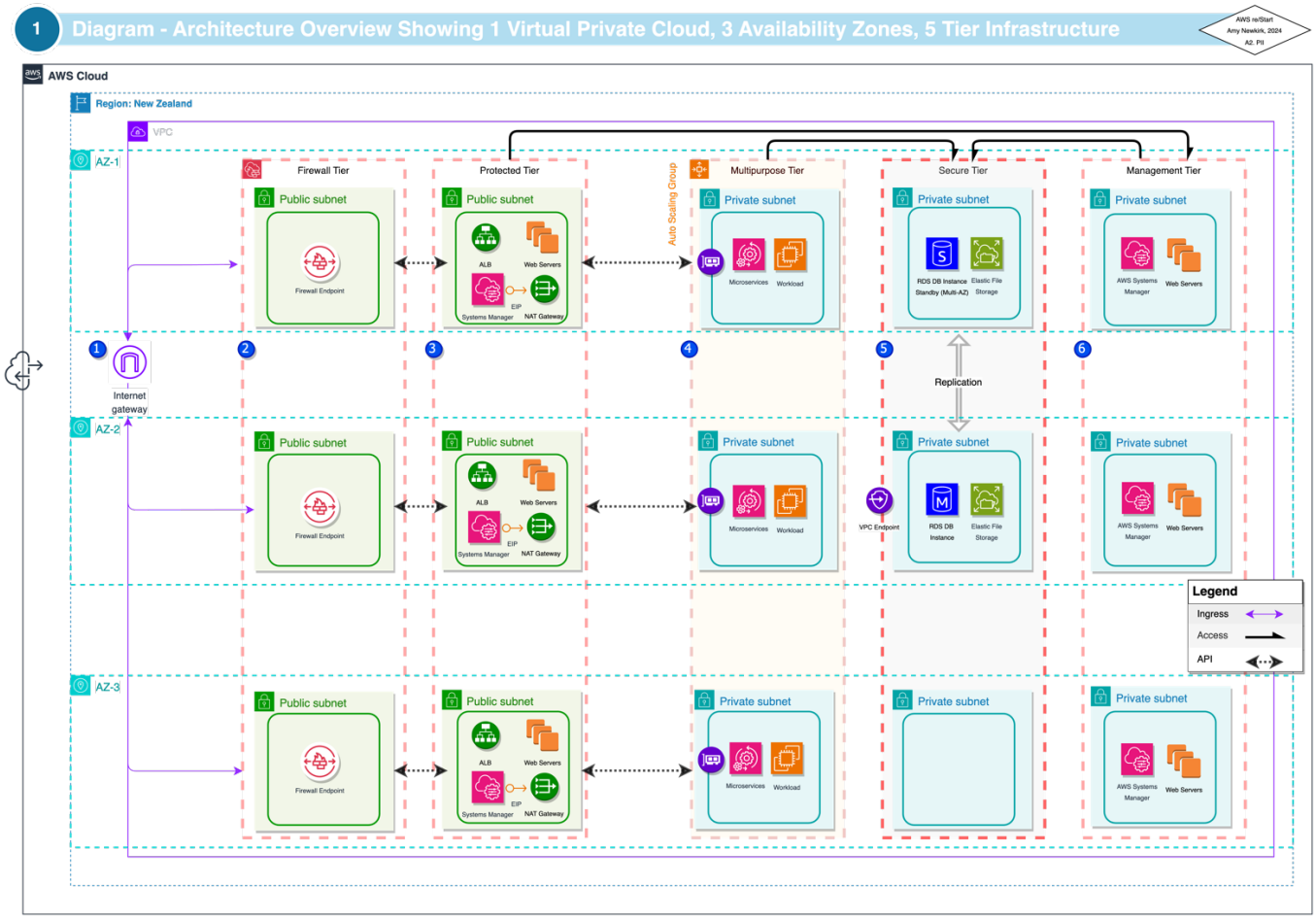
balancer. The secure database servers can connect to the internet using the NAT gateway in the same availability zone, they can also connect to Amazon S3 by using a gateway VPC. The RDS database and EFS network file system have a 1 AZ failover.

The following diagram provides an overview of the resources included in the new VPC design. The VPC has public subnets and private subnets in two Availability Zones. The web servers run in the public subnets and receive traffic from clients through an Application Load Balancer (ALB).

- The VPC has public subnets and private subnets in three Availability Zones.
- The **web servers run in the public subnets** and receive traffic from clients through an Application Load Balancer (ALB).
- The database servers can connect to Amazon S3 by using a gateway VPC endpoint.
- The servers can connect to the internet by using the NAT gateway.
- The servers can connect to Amazon S3 by using a gateway VPC endpoint.

Diagram 1 - Showing Overview





![High Level Overview](Part II.0 Diagram Amy Newkirk v6.0drawio.xml-1 - Num Overview.png)

Security

This section of the design details the routing tables, security group for the load balancer, security groups for the web servers, and security group for the database servers.

Routing Tables

Traffic is routed back to the firewall endpoint.

Ingress/Egress Route Table For Internet Gateway

IGW has ingress route table associated to it. The route table has entry for each protected subnet directing traffic to firewall endpoint in the corresponding AZ. This ensures that traffic is symmetrically returned to the right firewall endpoint to maintain stateful traffic inspection.

AWS Network Firewall doesn't perform NAT, ingress and egress to the internet depends on public IPs or EIPs associated to individual elastic network interfaces (ENIs) in the protected subnets.

Security Groups

The following rules were used to create security groups associated with “AWS re/Start, Assignment2 network infrastructure. The security group must allow traffic from the load balancer over the listener port and protocol. It must also allow health check traffic.

The security group for the web servers allows traffic from the ALB. The database servers run in the private subnets and receive traffic from the web servers. The security group for the database servers allows traffic from the web servers. The database servers can connect to Amazon S3 by using a gateway VPC endpoints

- The ****subnet security group for the web servers**** allows traffic from the load balancer.
- The ****database security group**** for the database servers allows traffic from the private subnet web servers.

Load Balancers			
Inbound			
Source	**Protocol**	**Port range**	**Comments**
ID of the load balancer security group	*listener protocol*	*listener port*	Allows inbound traffic from the load balancer on the listener port
ID of the load balancer security group	*health check protocol*	*health check port*	Allows inbound health check traffic from the load balancer

Load balancer

The security group for your Application Load Balancer or Network Load Balancer must allow inbound traffic from clients on the load balancer listener port. To accept traffic from anywhere on the internet, specify 0.0.0.0/0 as the source. The load balancer security group must also allow outbound traffic from the load balancer to the target instances on the instance listener port and the health check port.

Web servers

The following security group rules allow the web servers to receive HTTP and HTTPS traffic from the load balancer. You can optionally allow the web servers to receive SSH or RDP traffic from your network. The web servers can send SQL or MySQL traffic to your database servers.

Security Web servers

Inbound			
Source	**Protocol**	**Port range**	**Description**
ID of the security group for the load balancer	TCP	80	Allows inbound HTTP access from the load balancer
ID of the security group for the load balancer	TCP	443	Allows inbound HTTPS access from the load balancer
Public IPv4 address range of your network	TCP	22	(Optional) Allows inbound SSH access from IPv4 IP addresses in your network
IPv6 address range of your network	TCP	22	(Optional) Allows inbound SSH access from IPv6 IP addresses in your network
Public IPv4 address range of your network	TCP	3389	(Optional) Allows inbound RDP access from IPv4 IP addresses in your network
IPv6 address range of your network	TCP	3389	(Optional) Allows inbound RDP access from IPv6 IP addresses in your network

Security Web servers			
Outbound			
Destination	**Protocol**	**Port range**	**Description**
ID of the security group for instances running Microsoft SQL Server	TCP	1433	Allows outbound Microsoft SQL Server access to the database servers
ID of the security group for instances running MySQL	TCP	3306	Allows outbound MySQL access to the database servers

Database servers

The following security group rules allow the database servers to receive read and write requests from the web servers.

Opportunity - Secure Layer (Database) Rule

Security Database servers			
Inbound			
Source	**Protocol**	**Port range**	**Comments**
ID of the web server security group	TCP	1433	Allows inbound Microsoft SQL Server access from the web servers

ID of the web server security group	TCP	3306	Allows inbound MySQL Server access from the web servers

Security Database servers			
Outbound			
Destination	**Protocol**	**Port range**	**Comments**
0.0.0.0/0	TCP	80	Allows outbound HTTP access to the internet over IPv4
0.0.0.0/0	TCP	443	Allows outbound HTTPS access to the internet over IPv4

Security Policy

Opportunity Scaling policy - Create a target tracking scaling policy

End.