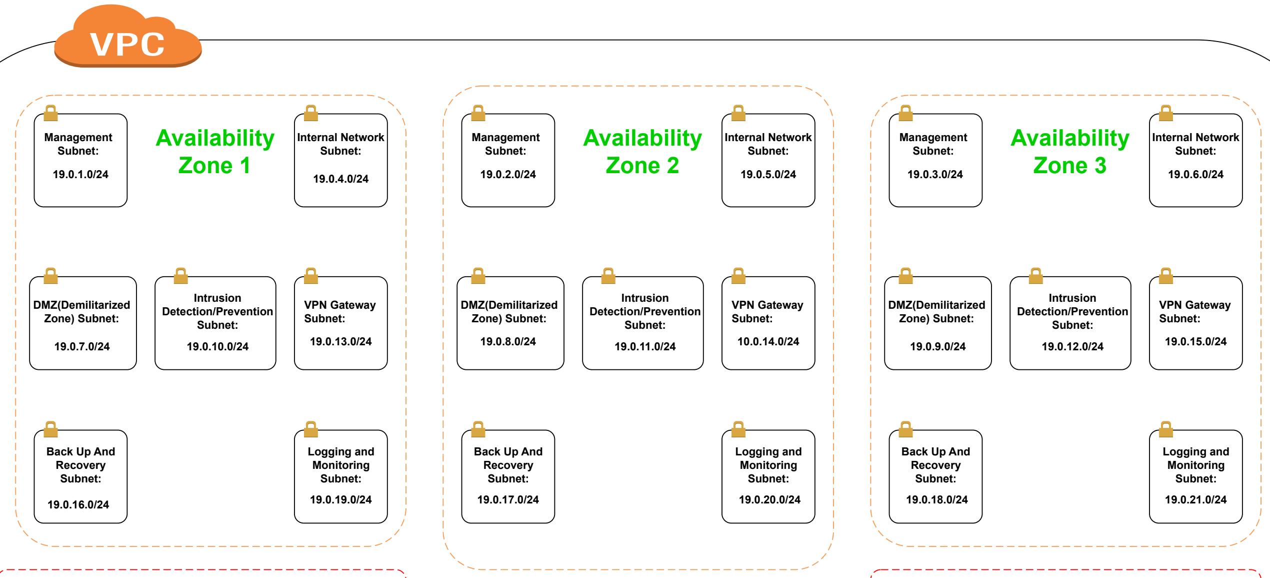

Availability Zone 1

Management Subnet: 19.0.1.0/24

Internal Network Subnet: 19.0.4.0/24

DMZ(Demilitarized Zone) Subnet: 19.0.7.0/24

Intrusion Detection/Prevention Subnet: 19.0.10.0/24

VPN Gateway Subnet: 19.0.13.0/24

Back Up And Recovery Subnet: 19.0.16.0/24

Logging and Monitoring Subnet: 19.0.19.0/24

Availability Zone 2

Management Subnet: 19.0.2.0/24

Internal Network Subnet: 19.0.5.0/24

DMZ(Demilitarized Zone) Subnet: 19.0.8.0/24

Intrusion Detection/Prevention Subnet: 19.0.11.0/24

VPN Gateway Subnet: 10.0.14.0/24

Back Up And Recovery Subnet: 19.0.17.0/24

Logging and Monitoring Subnet: 19.0.20.0/24

Availability Zone 3

Management Subnet: 19.0.3.0/24

Internal Network Subnet: 19.0.6.0/24

DMZ(Demilitarized Zone) Subnet: 19.0.9.0/24

Intrusion Detection/Prevention Subnet: 19.0.12.0/24

VPN Gateway Subnet: 19.0.15.0/24

Back Up And Recovery Subnet: 19.0.18.0/24

Logging and Monitoring Subnet: 19.0.21.0/24

Security Group Name: Management Subnet SG

- **Inbound Rules: Allow SSH (port 22) access from specific IP ranges of SOC team members for management purposes.**
- **Outbound Rules: Allow necessary outbound traffic for management tasks (e.g., DNS, NTP).**

Internal Network Subnets
- Security Group Name: InternalSG
- Inbound Rules: Allow traffic only from specific subnets or security groups within the VPC that need access to internal resources (e.g., web servers, application servers, databases).
- Outbound Rules: Allow necessary outbound traffic for internal communication (e.g., database queries, API calls).

3. DMZ (Demilitarized Zone) Subnet:
- Security Group Name: DMZSG
- Inbound Rules: Allow only essential ports for public-facing services (e.g., HTTP, HTTPS, SMTP) from external sources (e.g., 0.0.0.0/0).
- Outbound Rules: Restrict outbound traffic to minimize exposure and limit communication to necessary destinations (e.g., DNS, NTP).

7. Logging and Monitoring Subnet:
- Security Group Name: LoggingSG
- Inbound Rules: Allow traffic only from authorized sources (e.g., internal management systems, IDS/IPS) for log collection and analysis.
- Outbound Rules: Allow necessary outbound traffic for communication with log aggregation and SIEM (Security Information and Event Management) systems.

4. Intrusion Detection/Prevention Subnet:
- Security Group Name: IDPSG
- Inbound Rules: Allow traffic only from trusted sources (e.g., management subnet, specific IP ranges of security operations personnel) for monitoring and analysis purposes.
- Outbound Rules: Allow necessary outbound traffic for communication with central logging and monitoring systems (e.g., syslog, SNMP).

5. VPN Gateway Subnet:
- Security Group Name: VPNSG
- Inbound Rules: Allow VPN traffic (e.g., IPsec, SSL) from authorized IP ranges or devices.
- Outbound Rules: Allow necessary outbound traffic for VPN connectivity and related services.

6. Backup and Recovery Subnet:
- Security Group Name: BackupSG
- Inbound Rules: Allow traffic only from authorized sources (e.g., management subnet, backup servers) for data replication and backup operations.
- Outbound Rules: Allow necessary outbound traffic for backup and recovery tasks (e.g., storage replication, database backups).

NACL's

1. Management Subnet:
- NACL: Create a custom NACL named "ManagementNACL" and associate it with the management subnet (e.g., 10.0.1.0/24).
- Define ingress and egress rules in the ManagementNACL to allow necessary management traffic (e.g., SSH, RDP) from authorized IP ranges and deny all other traffic.

NACL's

2. Internal Network Subnets:
- NACL: Create a custom NACL named "InternalNACL" and associate it with each internal network subnet (e.g., web servers, application servers, databases).
- Define ingress and egress rules in the InternalNACL to allow communication between internal resources based on their requirements while restricting unauthorized access.

NACL's

3. DMZ (Demilitarized Zone) Subnet:
- NACL: Create a custom NACL named "DMZNACL" and associate it with the DMZ subnet (e.g., 10.0.13.0/24).
- Define ingress rules in the DMZNACL to allow specific ports for public-facing services (e.g., HTTP, HTTPS) and restrict access to sensitive resources.

NACL's

6. Backup and Recovery Subnet:
- NACL: Create a custom NACL named "BackupNACL" and associate it with the backup and recovery subnet (e.g., 10.0.22.0/24).
- Define ingress and egress rules in the BackupNACL to allow communication between backup resources and restrict access to backup data.

NACL's

7. Logging and Monitoring Subnet:
- NACL: Create a custom NACL named "LoggingNACL" and associate it with the logging and monitoring subnet (e.g., 10.0.25.0/24).
- Define ingress and egress rules in the LoggingNACL to allow traffic necessary for log collection and analysis while restricting unauthorized access.

NACL's

3. DMZ (Demilitarized Zone) Subnet:
- NACL: Create a custom NACL named "DMZNACL" and associate it with the DMZ subnet (e.g., 10.0.13.0/24).
- Define ingress rules in the DMZNACL to allow specific ports for public-facing services (e.g., HTTP, HTTPS) and restrict access to sensitive resources.

NACL's

4. Intrusion Detection/Prevention Subnet:
- NACL: Create a custom NACL named "IDPNACL" and associate it with the intrusion detection/prevention subnet (e.g., 10.0.16.0/24).
- Define ingress and egress rules in the IDPNACL to allow traffic necessary for monitoring and analysis while blocking unauthorized access to security appliances.

NACL's

5. VPN Gateway Subnet:
- NACL: Create a custom NACL named "VPNNACL" and associate it with the VPN gateway subnet (e.g., 10.0.19.0/24).
- Define ingress and egress rules in the VPNNACL to allow VPN traffic from authorized sources while blocking other traffic to maintain security.

Internet Gateway

1. **Create an Internet Gateway (IGW):**
- Go to the VPC Dashboard in the AWS Management Console.
- Select "Internet Gateways" from the left-hand menu.
- Click "Create internet gateway" and name it, e.g., "SOC-IGW."
- Once created, attach the IGW to your VPC.

2. **Route Table Configuration:**
- Go to the "Route Tables" section in the VPC Dashboard.
- Select the route table associated with your VPC.
- Add a route to the IGW for internet-bound traffic (destination: 0.0.0.0/0, target: your IGW).

3. **Subnet Association:**
- Ensure that the subnets requiring internet access are associated with the route table containing the route to the IGW.

4. **Security Group Configuration:**
- Review the security group configurations to ensure that appropriate rules are in place for inbound and outbound internet-bound traffic.
- Allow necessary inbound traffic from the internet to specific resources (e.g., web servers) while restricting access to sensitive services.
- Permit outbound traffic from internal resources to the internet based on your project requirements.

5. **NACL Configuration:**
- Review and update the NACL configurations to allow internet-bound traffic while maintaining network security.
- Ensure that the NACL rules permit outbound traffic from the subnets to the internet and allow return traffic for established connections.
- Deny or restrict unauthorized inbound traffic from the internet to protect internal resources.

6. **Testing and Monitoring:**
- Test internet connectivity from resources within the subnets associated with the IGW.
- Monitor network traffic and security logs to detect any unexpected or malicious activity.

1. **Associate Subnets with the Route Table:**
- Ensure that the subnets requiring internet access are associated with the route table that has a route pointing to the Internet Gateway (IGW). This allows resources in those subnets to access the internet.

2. **Update NACLs:**
- Review and update the NACL configurations to allow necessary inbound and outbound internet traffic while maintaining security.
- Ensure that outbound traffic from the subnets to the internet is permitted, and inbound traffic is restricted based on your project's security requirements.

3. **Update Security Groups:**
- Review and update the security group configurations to allow inbound and outbound internet-bound traffic based on your project's security policies.
- Permit necessary inbound traffic from the internet to specific resources while restricting access to sensitive services.
- Allow outbound traffic from internal resources to the internet as needed.

4. **Test Connectivity:**
- Test internet connectivity from resources within the subnets associated with the IGW to ensure that they can access the internet as expected.
- Validate that security measures, such as NACLs and security groups, are effectively controlling internet traffic and maintaining network security.

1. **Management Subnet:**
- Ensure that the management subnet (e.g., 10.0.1.0/24) is associated with a custom route table named "ManagementRouteTable."
- In the ManagementRouteTable, add a default route (0.0.0.0/0) with the target set to the Internet Gateway (IGW). This allows management resources to access the internet for updates, patches, and other necessary tasks.

2. **Internal Network Subnets:**
- Associate each internal network subnet (e.g., web servers, application servers, databases) with a custom route table named "InternalRouteTable."
- In the InternalRouteTable, add routes for internal communication between subnets, pointing to the local VPC CIDR block.
- If necessary, add specific routes for outbound internet-bound traffic to the IGW.

3. **DMZ (Demilitarized Zone) Subnet:**
- Associate the DMZ subnet (e.g., 10.0.13.0/24) with a custom route table named "DMZRouteTable."
- In the DMZRouteTable, add routes for public-facing services, pointing to the local VPC CIDR block or specific internal resources, and add a default route to the IGW for outbound internet access.

7. **Logging and Monitoring Subnet**:
- Associate the logging and monitoring subnet (e.g., 10.0.25.0/24) with a custom route table named "LoggingRouteTable."
- Configure routes in the LoggingRouteTable for communication with log aggregation systems, SIEM solutions, and other monitoring resources.

4. **Intrusion Detection/Prevention Subnet:**
- Associate the intrusion detection/prevention subnet (e.g., 10.0.16.0/24) with a custom route table named "IDPRouteTable."
- In the IDPRouteTable, configure routes for communication with management systems, logging servers, and other necessary resources within the VPC.

5. **VPN Gateway Subnet:**
- Associate the VPN gateway subnet (e.g., 10.0.19.0/24) with a custom route table named "VPNRouteTable."
- Configure routes in the VPNRouteTable for VPN connectivity, pointing to the VPN gateway, and ensure that necessary internal resources are accessible via VPN.

6. **Backup and Recovery Subnet:**
- Associate the backup and recovery subnet (e.g., 10.0.22.0/24) with a custom route table named "BackupRouteTable."
- Add routes in the BackupRouteTable for communication with backup servers, storage repositories, and replication targets.