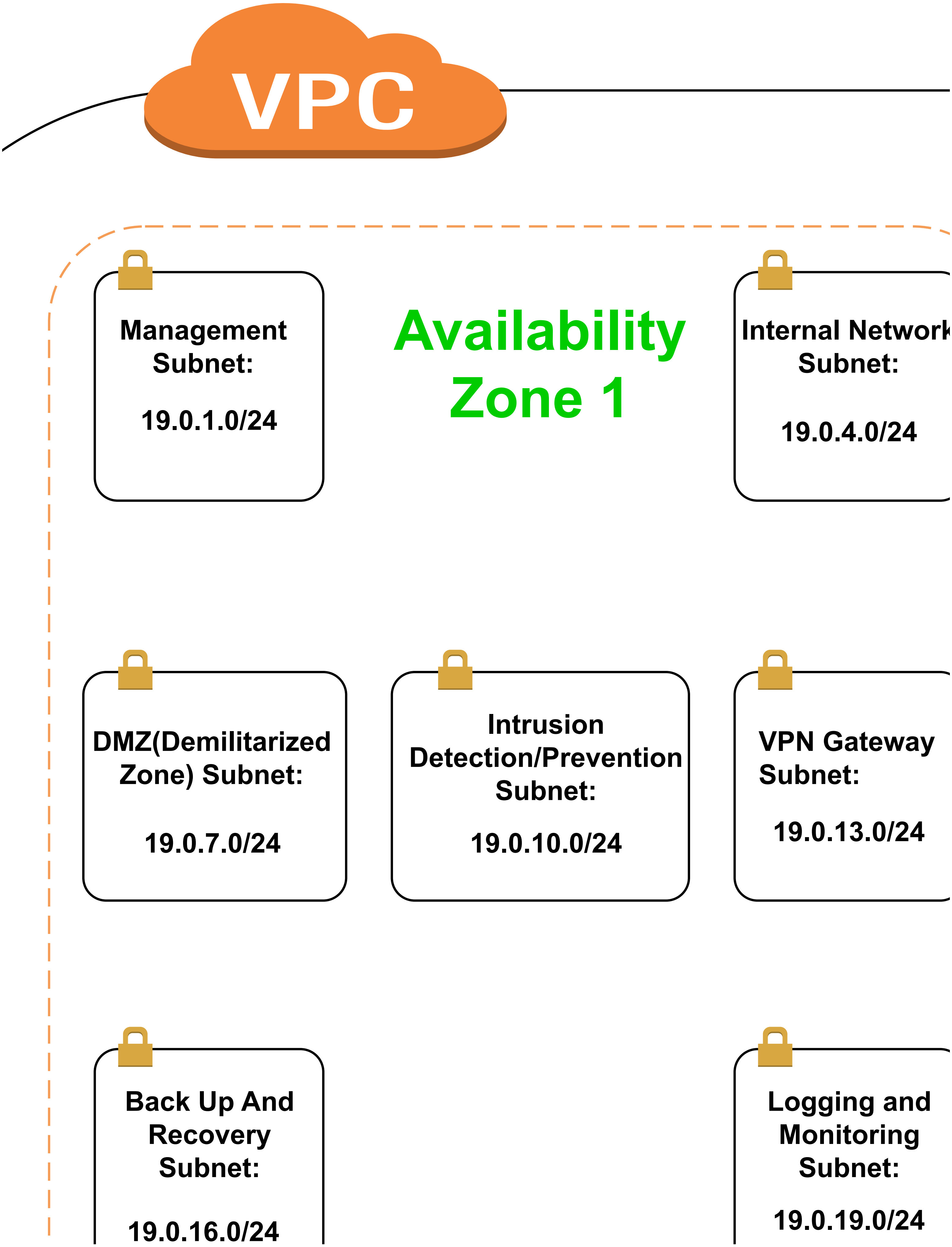


VPC

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:

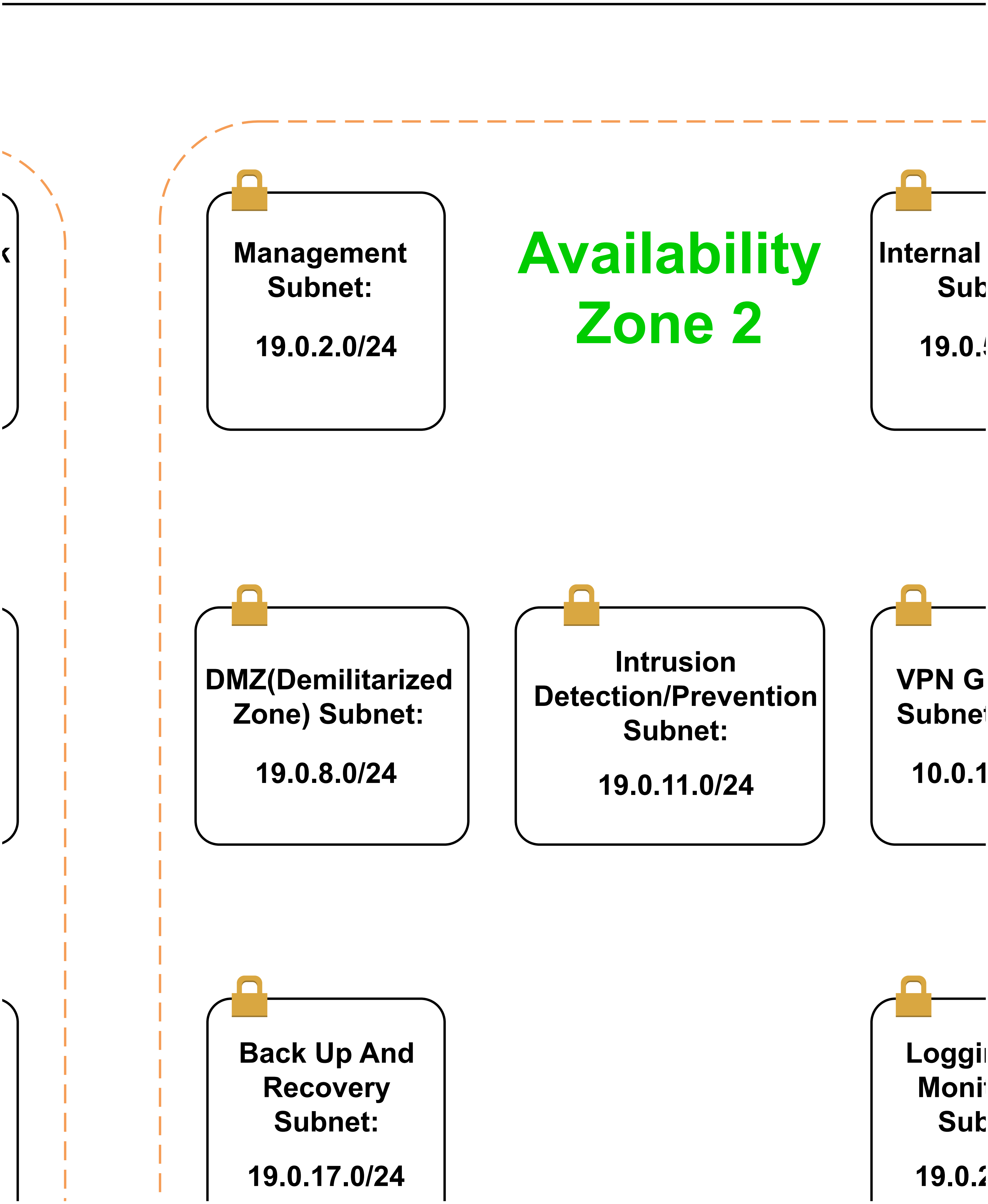
19.0.13.0/24

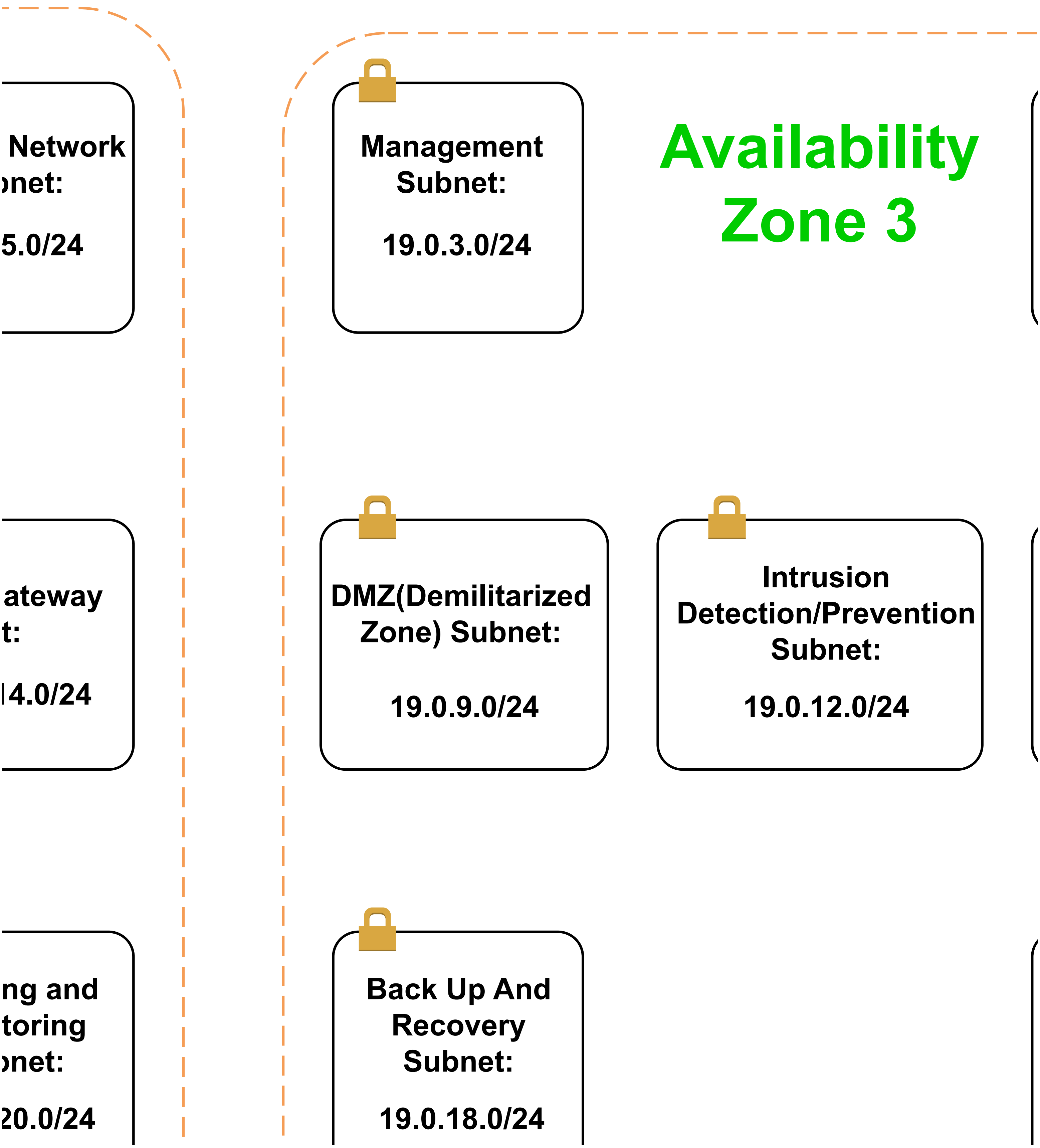
Back Up And Recovery Subnet:

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 Sub
19.0.
DMZ(Demilitarized Zone) Subnet:
19.0.8.0/24
Intrusion Detection/Prevention Subnet:
19.0.11.0/24
VPN G Subnet
10.0.1
Back Up And Recovery Subnet:
19.0.17.0/24
Loggi Moni Sub
19.0.2



Network
net:

5.0/24

ateway
t:

4.0/24

ng and
toring
net:

20.0/24

Management
Subnet:

19.0.3.0/24

Availability Zone 3

DMZ(Demilitarized
Zone) Subnet:

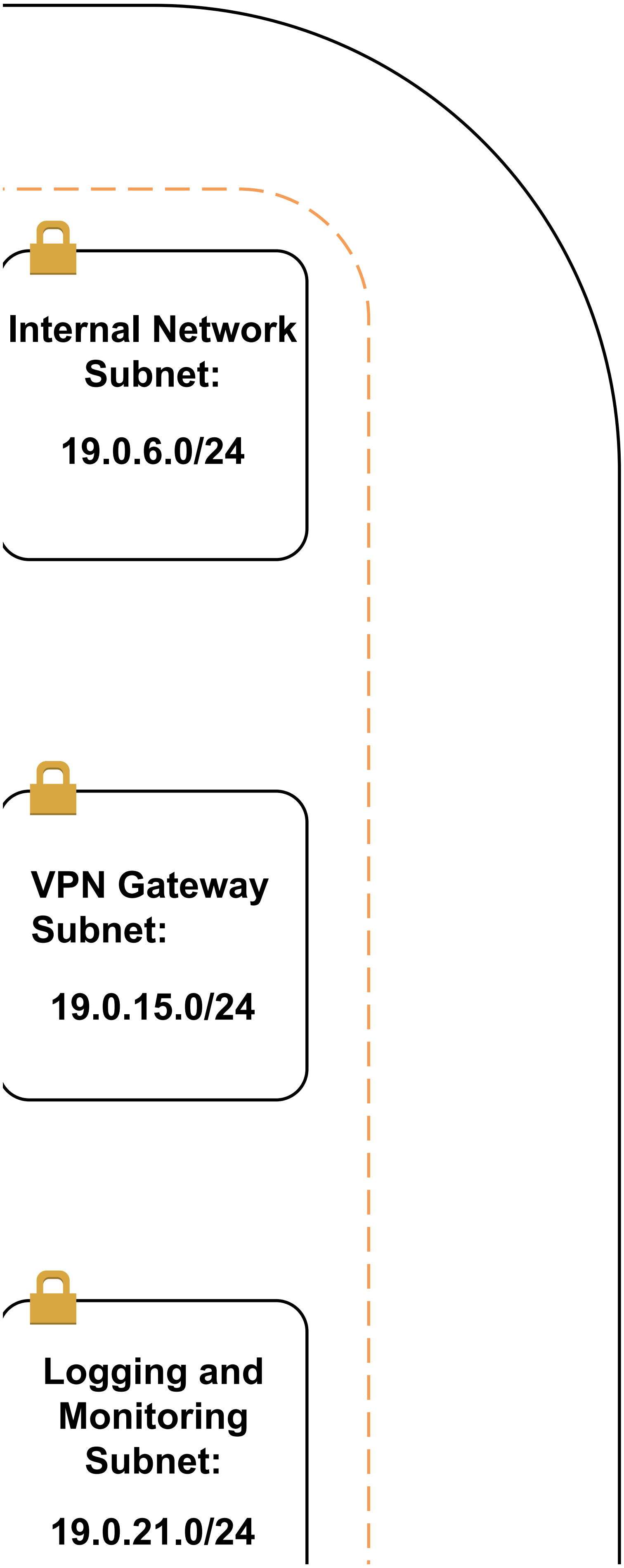
19.0.9.0/24

Intrusion
Detection/Prevention
Subnet:

19.0.12.0/24

Back Up And
Recovery
Subnet:

19.0.18.0/24



Internal Network Subnet:

19.0.6.0/24

VPN Gateway Subnet:

19.0.15.0/24

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).

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.

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

NACL's

ernal

with log
stems.

4. Intrusion Detection/Prevention Subnet:
- Security Group Name: IDPSG
- Inbound Rules: Allow traffic only from trusted sources (e.g., m
specific IP ranges of security operations personnel) for monitoring a
- Outbound Rules: Allow necessary outbound traffic for commu
logging and monitoring systems (e.g., syslog, SN

5. VPN Gateway Subnet:
- Security Group Name: VPNSG
- Inbound Rules: Allow VPN traffic (e.g., IPsec, SSL) from auth
devices.
- Outbound Rules: Allow necessary outbound traffic for VPN co
services.

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

NACL's

3. DMZ (Demilitarized Zone) Subnet:
- NACL: Create a custom NACL named "DMZNACL" and associate it with the D
- Define ingress rules in the DMZNACL to allow specific ports for public-facing servic
access to sensitive resources.

nanagement subnet,
and analysis purposes.
ınication with central
IMP).

ıorized IP ranges or

nnectivity and related

g., management subnet,
ɔperations.
ı and recovery tasks (e.g.,
.

MZ subnet (e.g., 10.0.13.0/24).
ːes (e.g., HTTP, HTTPS) and restrict

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 the 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 restric access to sensitive resources.

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 th route to the IGW.

4. **Security Group Configuration:**
- Review the security group configurations to ensure that appropriate rules are in place for inbound a 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

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

ir

NACL's

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

ct

ne

and

s.

subnet (e.g.,

s and restrict

subnet (e.g.,

nalysis while

NACL's

4. Intrusion Detection/Prevention Subnet:
- NACL: Create a custom NACL named "IDPNACL" and associate it with the intrusio
10.0.16.0/24).
- Define ingress and egress rules in the IDPNACL to allow traffic necessary for mon
unauthorized access to security appliances.

NACL's

5. VPN Gateway Subnet:
- NACL: Create a custom NACL named "VPNNACL" and associate it with the VPN g
- Define ingress and egress rules in the VPNNACL to allow VPN traffic from author
traffic to maintain security.

1. **Associate Subnets with the Route Tab
- Ensure that the subnets requiring internet access are assoc
that has a route pointing to the Internet Gateway (IGW). This a
subnets to access the internet.

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

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

4. **Test Connectivity:**
- Test internet connectivity from resources within the subnets

n detection/prevention subnet (e.g.,

nitoring and analysis while blocking

jateway subnet (e.g., 10.0.19.0/24).
rized sources while blocking other

ole:
ciated with the route table
llows resources in those**

**ary inbound and outbound
ty.
: is permitted, and inbound
requirements.**

**ow inbound and outbound
urity policies.
resources while restricting**

internet as needed.

associated with the IGW to

5. **NACL Configuration**:
- Review and update the NACL configurations to allow internet-bound traffic while maintaining netwo security.
- Ensure that the NACL rules permit outbound traffic from the subnets to the internet and allow retur 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. **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 VP 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 specifi internal resources, and add a default route to the IGW for outbound internet access.

ork

rn

/).

C

c

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

- Test internet connectivity from resources within the subnets
ensure that they can access the internet as ex
- Validate that security measures, such as NACLs and securi
controlling internet traffic and maintaining netwo

4. **Intrusion Detection/Prevention Subnet**:
- Associate the intrusion detection/prevention subnet (e.g., 10.0.16.0/24) wit
"IDPRouteTable."
- In the IDPRouteTable, configure routes for communication with managemer
other necessary resources within the VPC.

e named

.M solutions, and

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

6. **Backup and Recovery Subnet**:
- Associate the backup and recovery subnet (e.g., 10.0.22.0/24) with a c
"BackupRouteTable."
- Add routes in the BackupRouteTable for communication with backup serv
replication targets.

associated with the IGW to
xpected.
ity groups, are effectively
ork security.

th a custom route table named

nt systems, logging servers, and

table named "VPNRouteTable."
ne VPN gateway, and ensure that
/PN.

custom route table named

vers, storage repositories, and