Public & Private Subnets

Status	Not Started

1. Introduction

In cloud networking (particularly AWS, Azure, GCP), Virtual Private Clouds (VPCs) use subnet segmentation to separate resources based on their internet accessibility requirements. This architecture follows security best practices and the principle of least privilege.

2. Core Definitions

Public Subnet

Technical Definition: A subnet whose associated route table contains a route to an Internet Gateway (IGW) or equivalent internet-facing gateway component. Resources in this subnet can have direct bi-directional communication with the internet.

Key Characteristics:

- Route table destination: `0.0.0.0/0` → Target: `igw-xxxxxx`
- Resources may have public IPv4 addresses, Elastic IPs, or IPv6 addresses
- Typically placed in a DMZ (Demilitarized Zone) architecture
- Network Access Control Lists (NACLs) and security groups control traffic

Private Subnet

Technical Definition: A subnet whose route table does NOT contain a route to an Internet Gateway. Instead, it routes internet-bound traffic through a Network Address Translation (NAT) gateway or proxy.

Key Characteristics:

- Route table destination: `0.0.0.0/0` → Target: `nat-gateway-xxxxxx` (for outbound only)
- No direct inbound internet connections
- Uses RFC 1918 private IP ranges:
  - `10.0.0.0/8`
  - `172.16.0.0/12`
  - `192.168.0.0/16`

3. Detailed Technical Comparison

Aspect	Public Subnet	Private Subnet
Internet Access	Direct inbound/outbound	Outbound via NAT only
IP Addressing	Public + Private IPs	Private IPs only
Route Table	Routes to IGW	No route to IGW
Security Layers	NACL + Security Groups + WAF	NACL + Security Groups
Typical Use Cases	Load Balancers, Bastion Hosts, Web Servers	Application Servers, Databases, Cache
Cost Components	Data transfer costs higher	Lower data transfer costs
Network ACL Default	Less restrictive (varies)	More restrictive

4. Technical Architecture Components

Internet Gateway (IGW)

- Horizontally scaled, redundant VPC component
- Enables communication between VPC and internet
- Provides NAT for instances with public IPv4 addresses
- Supports IPv4 and IPv6 traffic

NAT Gateway/Instance

- **NAT Gateway**: Managed AWS service in public subnet
- **NAT Instance**: EC2 instance performing NAT functions
- Allows private subnet resources to initiate outbound connections
- Blocks unsolicited inbound connections

Route Tables

json

```
// Public Subnet Route Table
{
  "Destination": "0.0.0.0/0",
  "Target": "igw-12345",
  "Status": "Active"
}

// Private Subnet Route Table
{
  "Destination": "0.0.0.0/0",
  "Target": "nat-67890",
  "Status": "Active"
}
```

5. Security Considerations

Public Subnet Security

1. **Network ACLs**: Stateless filtering at subnet boundary
2. **Security Groups**: Stateful filtering at instance level
3. **Web Application Firewall**: For HTTP/HTTPS traffic
4. **DDoS Protection**: Cloud-native DDoS mitigation

Private Subnet Security

1. **Isolation**: No direct internet exposure

2. **VPC Endpoints**: Access AWS services without internet
3. **VPC Flow Logs**: Monitor network traffic
4. **Encryption**: Data in transit via TLS/SSL

6. Practical Implementation

CIDR Planning Example

text

```
VPC CIDR: 10.0.0.0/16

Public Subnets:
- 10.0.1.0/24 (AZ A)
- 10.0.2.0/24 (AZ B)

Private Subnets:
- 10.0.3.0/24 (AZ A) - App Tier
- 10.0.4.0/24 (AZ B) - App Tier
- 10.0.5.0/24 (AZ A) - Data Tier
- 10.0.6.0/24 (AZ B) - Data Tier
```

7. Reference Architectures

Two-Tier Web Application

text

```
Internet → [Public Subnet]
          ↓
[Application Load Balancer] (Public)
          ↓
[Private Subnet - App Tier]
          ↓
[Private Subnet - Database Tier]
```

Three-Tier Architecture

text

```
[Public Subnet]
├── Internet Gateway
├── NAT Gateway
└── Bastion Host

[Private Subnet - Web Tier]
├── Auto Scaling Group
└── Web Servers

[Private Subnet - App Tier]
├── Application Servers
└── Internal Load Balancer

[Private Subnet - Data Tier]
├── Database Cluster
└── Elasticache
```