Instances that can receive and send traffic and a private subnet that can’t receive traffic directly from the Internet --- but can send traffic to the internet (through NAT gateway)

ACL for public subnet

Inbound

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rule | Source IP | Protocol | Port | Allow/Deny | Info |
| 100 | 0.0.0.0/0 |  | 80 | ALLOW | Allows inbound HTTP traffic |
| 101 | 0.0.0.0/0 |  | 443 | ALLOW | Allows inbound HTTPS traffic |
| 102 | Your IP address |  | 22 | ALLOW | Allows inbound SSH traffic |
| 103 | 0.0.0.0/0 |  | 1024-65535 | ALLOW | Allows inbound traffic that respond to requests sent from subnet (e.g. updates) |
| 104 | 0.0.0.0/0 |  |  |  |  |
|  | | | | | |

Outbound

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Destination IP | Port | Allow/Deny | Info |
| 100 | 0.0.0.0/0 | 80 | ALLOW | Allows outbound HTTP traffic from subnet to internet |
| 101 | 0.0.0.0/0 | 443 | ALLOW | Allows outbound HTTPS traffic from subnet to internet |
| 102 | 10.18.1.0/24 | 22 | ALLOW | Allows outbound SSH access to instances in private subnet |
| 103 | 10.18.1.0/24 | 27017 | ALLOW | Allows outbound MongoDB access to instances in private subnet |

ACL Rules for Private Subnet

Inbound

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Source IP | Port | Allow/Deny | Info |
| 100 | 10.0.0.0/24 | 27017 | ALLOW | Allow web servers in public subnet to read and write to MongoDB in private subnet |
| 101 | 10.0.0.0/24 | 22 |  | Allow inbound SSH traffic in public subnet |
| 102 | 10.0.0.0/24 | 1024-65535 |  | Allow inbound return traffic from the NAT device in public subnet from requests from the private subnet. |
| \* | 0.0.0.0.0/0 | all | DENY | Deny all inbound traffic not handled by existing rule |
| 104 |  |  |  |  |

Outbound

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Destination IP | Port | Allow/Deny | Comments |
| 101 | 0.0.0.0/0 | 80 | ALLOW | Allow outbound HTTP traffic from subnet to internet |
| 102 | 0.0.0.0/0 | 443 | ALLOW | Allow outbound HTTPS traffic from subnet to interent |
| 103 | 10.18.0.0/24 |  | ALLOW | Allow outbound responses to public subnet (responses to wen server in public subnet for database communication) |
| \* | All | All | DENY | Deny all other outbound traffic |

**Network Access Control List**

Optional layer of security for VPC, that acts as a firewall for controlling traffic in and out of one or more subnets. ACL operates at the **subnet level** and evaluates traffic entering and existing a subnet.

**Security groups**

Acts as a virtual firewall for your instance to control inbound and outbound traffic. Acts at the **instance level** (not the subnet level). Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups.

**Differences:**

Security Groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the **instance level.** While ACLs act as a firewall for associated subnets, controlling both inbound and outbound traffic at the **subnet level**.

**Bastion host:**

A special purpose hardened computer on a network that is specifically designed and configured to withstand attacks. The computer usually hosts a single application and all other services are removed or limited to reduce threat to the computer. The rest of your servers are blocked from direct access.

It can filter incoming traffic and prevent malicious traffic entering the network (acts like a gateway). Examples: mail, domain name system, web and file transfer protocol (FTP) servers.