7. Security Groups & Network ACL Configuration

This section describes how traffic is explicitly allowed or denied at every layer of the architecture—from the Site-to-Site VPN entry point through the application and database tiers, and finally outbound internet access.

The design intentionally uses **Security Groups as the primary security control** and keeps **Network ACLs minimal** to avoid unnecessary stateless complexity. This aligns with AWS best practices and improves operational clarity.

7.1 Network Entry Point – VPN and VPC Routing

Virtual Private Gateway (VGW)

The Virtual Private Gateway is attached to the VPC and acts as the termination point for the Site-to-Site VPN connection from the on-premise network.

Key characteristics:

- VPN tunnel terminates at the VGW
- VGW itself does **not** enforce security group rules
- Traffic control begins at **VPC route tables** and **Security Groups**

Private Route Table Configuration

```
resource "aws_route" "onprem_vpn_route" {
  route_table_id         = aws_route_table.private_rt.id
  destination_cidr_block = var.on_prem_cidr
  gateway_id             = aws_vpn_gateway.vgw.id
}
```

Effect

- Any traffic destined for `192.168.10.0/24` is routed back through the VPN
- Enables bidirectional communication between AWS and on-prem

- Applies uniformly to all private subnets (application and database)

7.2 On-Premise → AWS Application Flow (Inbound)

Step 1: On-Premise to VGW

- On-premise firewall encrypts traffic destined for the AWS VPC CIDR (`10.0.0.0/16`)
- Traffic traverses the IPsec tunnel over the public internet
- VGW terminates the tunnel and decrypts the packet

Step 2: VGW to Private Subnets

- The VPC router inspects the destination IP (e.g., `10.0.11.25`)
- Traffic is delivered directly to the appropriate private subnet
- No inbound route table decision is required beyond CIDR matching

---

7.3 Application Load Balancer Security Group (Controlled Entry)

ALB Placement

- Deployed in **private subnets**
- Configured as an **internal load balancer** (`internal = true`)
- Not accessible from the public internet

The ALB is reachable only from:

- The on-premise network via the Site-to-Site VPN
- Authorized AWS resources within the VPC

ALB Security Group Rules

Inbound

- TCP 80 / 443
- Source:
  - On-premise CIDR (`192.168.10.0/24`) via VPN
  - (Optional) Internal VPC CIDR if required

Outbound

- Forward traffic to application EC2 instances

Security Rationale

- ALB acts as the single, controlled ingress point
- No direct access to EC2 instances or RDS from on-prem or the internet
- Enforces clear separation between client access and application execution

---

7.4 Application EC2 Security Group (Strict East-West Control)

Application EC2 Placement

- Deployed in private subnets
- No public IP addresses
- Not directly reachable from the internet

Application EC2 Security Group Rules

Inbound

- Application port (HTTP / 8080)

- Source: **ALB Security Group only**

Outbound

- TCP 3306 → RDS Security Group
- `0.0.0.0/0` → NAT Gateway (for OS updates and external dependencies)

Key Protection Principle

Even if the ALB is exposed internally, EC2 instances are never exposed directly.
All on-prem traffic must follow the enforced path:

VPN → ALB → EC2

Direct access to EC2 instances is not permitted.

7.5 RDS Security Group (Database Isolation)

RDS Placement

- Private subnets only
- `publicly_accessible = false`

RDS Security Group Rules

Inbound

- TCP 3306
- Source: **Application EC2 Security Group only**

Outbound

- None explicitly required (stateful return traffic is allowed)

Isolation Guarantees

The database **cannot** be accessed:

- From the public internet
- Directly from the on-premise network
- From the ALB

Only the application layer is permitted to communicate with the database.

7.6 AWS → On-Premise Return Traffic

When AWS resources respond to on-premise requests:

1. EC2 or RDS sends response traffic to `192.168.10.x`
2. The VPC router consults the private route table

Route match:

```
192.168.10.0/24 → VGW
```

3.
4. Traffic exits AWS via the VPN tunnel
5. On-premise firewall decrypts and forwards traffic to the application server

Because Security Groups are **stateful**, return traffic is automatically permitted without additional rules.

7.7 Outbound Internet Access (Private Subnets)

Private Route Table (Internet Access)

- Destination: `0.0.0.0/0`
- Target: NAT Gateway

Traffic Flow

1. Private EC2 instance initiates an outbound request

Traffic flows:

```
EC2 → VPC Router → NAT Gateway → Internet Gateway
```

2.
3. NAT Gateway replaces the private IP with an Elastic IP

4. Return traffic is mapped back to the originating EC2 instance

Security Properties

- No route exists from the Internet Gateway to private subnets
- NAT Gateway allows **responses only**
- Inbound internet-initiated connections are impossible

7.8 Network ACLs (Deliberately Minimal)

Design Choice

- Default Network ACLs are retained
- No custom stateless rules are introduced

Rationale

Security Groups already provide:

- Least-privilege access control
- Stateful inspection
- Clear intent and easier auditing

Custom NACLs would:

- Increase operational complexity

- Require symmetric inbound and outbound rules
- Increase the risk of accidental service disruption

For this architecture, Security Groups provide sufficient and clearer control.