Network Security Policy Document

Purpose

This document defines the network security policies implemented using Linux iptables to protect a microservices-based application infrastructure.

The primary objectives are:

- Enforce service-to-service isolation
- Apply least privilege networking
- Protect public-facing components from abuse and denial-of-service
- Restrict outbound (egress) traffic
- Enable logging and auditability of denied traffic

Security Rules and Explanations

Rule 1: Database Access Restriction

```
iptables -A FORWARD ! -s 10.0.0.40/32 -d 10.0.0.60/32 -p tcp --dport 5432 -j DROP
```

Description:

Blocks all access to the PostgreSQL database except from the Order Service.

Explanation:

- `! -s 10.0.0.40/32` → Matches any source except Order Service
- `-d 10.0.0.60/32` → Targets the database
- `--dport 5432` → PostgreSQL port

Security Benefit

- Enforces least privilege
- Prevents unauthorized data access and lateral movement

Rule 2: Redis Access Restriction

```
iptables -A FORWARD ! -s 10.0.0.30/32 -d 10.0.0.50/32 -p tcp --dport 6379 -j DROP
```

Description

Restricts Redis access to the Product Service only.

Security Benefit

- Prevents cache poisoning

- Protects in-memory data from unauthorized services

Rule 3: API Gateway Rate Limiting

```
iptables -A FORWARD -d 10.0.0.20/32 -p tcp --dport 3000 \
  -m limit --limit 100/minute --limit-burst 20 -j ACCEPT

iptables -A FORWARD -d 10.0.0.20/32 -p tcp --dport 3000 -j DROP
```

Description

Limits incoming connections to the API Gateway.

Explanation

- Allows up to 100 requests per minute
- Permits an initial burst of 20 connections
- Drops traffic exceeding the limit

Security Benefit

- Mitigates Denial-of-Service (DoS) attacks
- Protects backend services from overload

Rule 4: Outbound Traffic Restrictions (Egress Control)

```
iptables -A FORWARD -s 10.0.0.0/16 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/16 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/16 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -s 10.0.0.0/16 -p udp --dport 53 -j ACCEPT
```

Description

Allows only essential outbound traffic from application services.

Allowed Traffic

- HTTP (80)
- HTTPS (443)
- DNS (53 TCP/UDP)

Security Benefit

- Prevents data exfiltration
- Reduces risk of malware or unauthorized external connections

Rule 5: Logging Dropped Packets

```
iptables -A FORWARD -j LOG --log-prefix "DROPPED: " --log-level 4
```

Description

Logs all packets dropped by firewall rules.

Security Benefit

- Enables monitoring and auditing
- Assists in troubleshooting and incident response