VPC Firewall Rules List – ShopNimbus Security Project

Project ID: shopnimbus-security-group7
Prepared by: Gloria Akhadelor-Job
Date: October 12, 2025

1. Purpose

This document defines the implemented firewall rules for the ShopNimbus project. The rules enforce network segmentation, restrict unauthorized access, and ensure secure tier communication. Configurations follow NIST PR.DS, CIS, and PCI DSS network protection standards.

2. Firewall Rules Summary

Rule Name	Direction	Allowed	Source Range	Target Tag	Purpose
allow-https-web	INGRESS	tcp:443	0.0.0.0/0	web-tier	Allow HTTPS access to web server
allow-internal-app	INGRESS	tcp:8080	10.0.0.0/8	app-tier	Permit internal App Tier traffic
allow-internal-db	INGRESS	tcp:3306	10.0.0.0/8	db-tier	Allow DB access from App Tier
allow-logging	EGRESS	tcp:443	0.0.0.0/0	logging-tier	Enable outbound logging to Cloud services
deny-all-ingress	INGRESS	none	0.0.0.0/0	all	Default deny-all ingress rule
deny-all-egress	EGRESS	none	0.0.0.0/0	all	Restrict unauthorized outbound traffic

3. Implementation Commands

The following commands were used to configure firewall rules: gcloud compute firewall-rules create allow-https-web --direction=INGRESS --rules=tcp:443 --source-ranges=0.0.0.0/0 --target-tags=web-tier gcloud compute firewall-rules create allow-internal-app --direction=INGRESS --rules=tcp:8080 --source-ranges=10.0.0.0/8 --target-tags=app-tier gcloud compute firewall-rules create allow-internal-db --direction=INGRESS --rules=tcp:3306 --source-ranges=10.0.0.0/8 --target-tags=db-tier gcloud compute firewall-rules create allow-logging --direction=EGRESS --rules=tcp:443 --target-tags=logging-tier gcloud compute firewall-rules create deny-all-ingress --direction=INGRESS --action=DENY --rules=all --source-ranges=0.0.0.0/0 gcloud compute firewall-rules create deny-all-egress --direction=EGRESS --action=DENY --rules=all --destination-ranges=0.0.0.0/0

4. Verification

Verification Command: gcloud compute firewall-rules list --format='table(name, direction, allowed, sourceRanges, targetTags)'

5. Compliance Mapping

- CIS Control 4.1: Manage network traffic through firewalls. - NIST PR.PT-4: Secure communication channels. - PCI DSS 1.1.6: Maintain firewall configuration standards. - GDPR Art. 32: Ensure data protection through technical safeguards.

6. Review and Maintenance

Firewall rules are reviewed monthly to maintain compliance and security posture. Unauthorized changes are prohibited and monitored through Cloud Audit Logs.