# ShopNimbus Firewall Rules List — Project shopnimbus-security-group7

## 1. Purpose

This document provides a detailed summary of the firewall configurations implemented in the ShopNimbus Google Cloud Platform (GCP) project (shopnimbus-security-group7). The firewall rules enforce network segmentation and access control between the Web, Application, and Database tiers, ensuring that communication occurs only through authorized channels. These configurations are critical to the project’s security architecture and form the basis for detection and monitoring activities under Week 4: Detection, Response, and Recovery.

## 2. Verification Command

The following gcloud command is used to verify existing firewall configurations:

* gcloud compute firewall-rules list --format="table(name, direction, sourceRanges, allowed, targetTags)"

## 3. Firewall Rules Configuration

The table below outlines the current firewall rules configured within the project.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rule Name | Direction | Source Range | Allowed Protocols / Ports | Target Tags | Description |
| web-allow-http | INGRESS | 0.0.0.0/0 | tcp:80 | web-sa | Allows HTTP traffic to the Web Tier from any external source. |
| web-allow-https | INGRESS | 0.0.0.0/0 | tcp:443 | web-sa | Allows HTTPS traffic for secure web connections. |
| app-allow-internal | INGRESS | 10.0.1.0/24 | tcp:8080 | app-sa | Allows only internal Web → App communication within the VPC. |
| db-allow-internal | INGRESS | 10.0.2.0/24 | tcp:3306 | db-sa | Restricts database access to internal App Tier connections only. |
| db-deny-external | INGRESS | 0.0.0.0/0 | ALL | db-sa | Blocks all external connections to the Database Tier for data protection. |
| allow-icmp-internal | INGRESS | 10.0.0.0/16 | icmp | all-tiers | Allows internal ICMP (ping) traffic for diagnostics within VPC. |
| egress-allow-internet | EGRESS | 0.0.0.0/0 | tcp:443 | web-sa,app-sa | Allows outbound HTTPS traffic for updates and API communication. |

## 4. Monitoring and Detection Integration

Firewall activity and configuration changes are continuously monitored using Cloud Logging and the Security Command Center (SCC). SCC’s findings are exported to BigQuery via the log sink 'scc\_findings\_sink', stored in the dataset 'scc\_logs'. Alerts are configured to detect unauthorized firewall modifications or anomalous ingress attempts. Command reference for verification:

* gcloud logging read "protoPayload.methodName=compute.firewalls.insert OR protoPayload.methodName=compute.firewalls.patch" --limit 10 --format="table(timestamp, protoPayload.authenticationInfo.principalEmail, protoPayload.methodName)"

## 5. Compliance and Security Notes

All firewall rules adhere to the principle of least privilege, allowing only the necessary traffic required for service operation. Ingress rules are tightly scoped to internal IP ranges wherever possible. Public access is restricted to HTTP/HTTPS on the Web Tier only. These rules support NIST SP 800-53 controls (AC-4, SC-7) and align with GCP’s best practices for network security segmentation.

## 6. Conclusion

The firewall configuration for project shopnimbus-security-group7 successfully enforces network segmentation across the Web, Application, and Database tiers. The integration with Cloud Logging and SCC enables continuous visibility into configuration changes and potential network threats. These measures collectively support a robust detection and response framework for the ShopNimbus environment.