Policy Snippets & Secure Architecture & Segmentation

ShopSphere Market

IT Team Security Operations Manual

Introduction: Understanding Your Role

Hello IT Team,
This manual defines your critical role in implementing and maintaining the hybrid cloud security architecture for **ShopSphere Market**. You are the backbone of our infrastructure, ensuring that technical assets remain efficient, resilient, and secure. Your mission is not only operational management but also close collaboration with the **Security Operations Center (SOC)** team to safeguard our hybrid environment.

1. Core Architecture & Responsibility Matrix

Our security model follows a **hybrid architecture**, integrating **Google Cloud Platform (GCP)** with our on-premise network.

Your responsibilities include:

- **Operational Management**: Administration, operation, and maintenance of servers, endpoints, and network systems.
- **Security Implementation**: Enforcing security policies, managing user accounts, and handling initial incident response in coordination with SOC.

2. Asset Inventory & Management

A **complete and accurate asset inventory** is the foundation of our security program.

- **Regular Updates**: Add or remove assets in real time.
- **Detailed Records**: Maintain accurate information for each asset (name, type, IP, location, responsible team).

3. Network & Security Rule Management

Firewalls

- **Default Deny Policy**: Reject all traffic unless explicitly allowed.
- **Rule Implementation**: Permit only essential communication (e.g., DMZ → Data Tier, On-premise → GCP).

VPN Tunnel

- **Maintenance**: Ensure VPN stability between on-premise and GCP.
- **Encryption**: Keep VPN protocols up-to-date.

Network Segmentation

- **Zone Isolation**: Payment Zone and SOC Room must remain fully isolated using VLANs/firewalls.
- **Access Control**: Block direct employee access to databases or payment systems.

4. Systems & Endpoint Management

SAP Business One

- **Patching**: Apply all updates and security patches.
- **User Management**: Enforce least privilege for SAP access.

Employee Endpoints

- **EDR**: Ensure **CrowdStrike EDR** is installed and active on all desktops and POS systems.
- **Regular Updates**: Keep OS and applications patched to prevent exploitation.

5. Collaboration with SOC

Collaboration with the SOC is vital for effective detection and response.

- **Log Management**: Forward all logs to the **SIEM in GCP**.

- **Incident Response**: When SOC detects compromise (e.g., via EDR), immediately isolate the device and follow remediation instructions.

6. Secure Architecture & Segmentation

Target Architecture

Our **hybrid cloud model** is divided into logical and isolated zones:

- **DMZ (GCP)**: Public-facing e-commerce platform, protected by Cloud Armor & Load Balancing.
- **Data Tier (GCP)**: MySQL 8.0 database, isolated from the internet, accessible only via DMZ.
- **Payment Zone (On-premise)**: Hosts Payment Processing Servers & Digital Payment Gateway; PCI DSS compliant.
- **Internal Operations Zone (On-premise)**: SAP Business One and ~100 employee endpoints protected by EDR.
- **Security & Monitoring Zone (On-premise + GCP)**: SOC Room and Security Subnet for centralized SIEM/EDR monitoring.

A **VPN tunnel** secures hybrid connectivity.

---

7. Network Traffic Rules

Source Zone	Destination Zone	Protocol	Port(s)	Purpose	Action
Internet	GCP DMZ (10.10.3.0/24)	HTTPS	443	Customer access	Allow
GCP DMZ	GCP Data Tier (10.10.4.0/24)	TCP	3306	Web → DB queries	Allow
On-premise App Zone	On-premise Payment Zone	TLS	8443	Secure payment flow	Allow
On-premise Payment Zone	Visa/Mastercard API	HTTPS	443	Payment processing	Allow

Source Zone	Destination Zone	Protocol	Port(s)	Purpose	Action
On-premise Network	GCP Security Subnet	HTTPS	443, 8080	Log forwarding	Allow
Any	Any	All	All	Default Deny	Deny

---

8. Firewall Policy Snippets (Terraform – GCP)

```
# Rule: Internet → DMZ (HTTPS)
resource "google_compute_firewall" "allow-internet-to-dmz" {
  name    = "allow-internet-to-dmz"
  network = "shopsphere-vpc"
  allow { protocol = "tcp" ports = ["443"] }
  source_ranges      = ["0.0.0.0/0"]
  destination_ranges = ["10.10.3.0/24"]
  description        = "Allow inbound HTTPS to DMZ."
}

# Rule: DMZ → Data Tier (MySQL)
resource "google_compute_firewall" "allow-dmz-to-data-tier" {
  name    = "allow-dmz-to-data-tier"
  network = "shopsphere-vpc"
  allow { protocol = "tcp" ports = ["3306"] }
  source_ranges      = ["10.10.3.0/24"]
  destination_ranges = ["10.10.4.0/24"]
  description        = "Allow queries from DMZ to DB."
}

# Rule: On-premise → SIEM/EDR (Log forwarding)
resource "google_compute_firewall" "allow-onprem-to-security" {
  name    = "allow-onprem-to-security"
  network = "shopsphere-vpc"
  allow { protocol = "tcp" ports = ["443", "8080"] }
  source_ranges      = ["192.168.0.0/16"]
  destination_ranges = ["10.10.5.0/24"]
  description        = "Allow logs via VPN to SIEM/EDR."
}
```

```
# Rule: Default Deny All
resource "google_compute_firewall" "default-deny-all" {
  name    = "deny-all-unlisted"
  network = "shopsphere-vpc"
  deny { protocol = "all" }
  source_ranges      = ["0.0.0.0/0"]
  destination_ranges = ["0.0.0.0/0"]
  priority           = 65535
  description        = "Block all unlisted traffic."
}
```

---

9. On-Premise Firewall Rules

- **Employee** → **Internet/Cloud**: Allowed.
- **Employee** → **SAP**: Allowed.
- **App Zone** → **Payment Zone**: Allowed (TLS 8443).
- **Default Deny**: Block all other traffic.

10. Rationale

Our design follows **Defense in Depth**, ensuring layered protection:

- **Segmentation**: Isolating payment & database systems reduces exposure.
- **Least Privilege**: Strict traffic rules align with **PCI DSS & ISO 27001**.
- **Endpoint Protection**: EDR prevents endpoint exploitation.
- **Centralized Security**: SIEM & EDR in GCP provide scalable monitoring and unified response.