FM-KED-003 — Network Connectivity Loss on Virtual Machine

Severity: S1 — Critical
Recovery Class: B — Standard Recovery
Covered by Monthly Support: Yes (diagnostics only)

Description

A virtual machine becomes partially or fully unreachable due to loss of network connectivity. This may affect administrative access, application availability, or external integrations.

The root cause may lie in operating system configuration, firewall rules, cloud security settings, or infrastructure provider issues.

Typical Symptoms

- SSH access unavailable or unstable
- Applications unreachable from external networks
- Inability to access external services or the public internet
- Timeouts in inter-service communication

Diagnostic Checklist

Proceed in order. Each step narrows the responsibility boundary.

---

1. Verify SSH Connectivity

```
ssh user@vm_ip
```

If SSH is unreachable:

- Verify correct IP and credentials

- Check whether the VM responds to ICMP (ping), if allowed

---

2. Verify Internet Access from the VM

```
ping -c 3 8.8.8.8
curl https://example.com
```

Distinguish between:

- No outbound connectivity
- DNS resolution issues

---

3. Check OS-Level Firewall Rules

```
sudo iptables -L -n
sudo ufw status
```

Verify that required inbound and outbound traffic is allowed.

---

4. Check Cloud Security Groups and Network Rules

- Review inbound and outbound rules in the cloud provider console
- Confirm correct ports, protocols, and source ranges
- Verify network routing and subnet configuration

---

5. Escalation to Infrastructure Provider

If all checks above are inconclusive:

- Collect timestamps, VM identifiers, and observed symptoms
- Open a support ticket with the cloud provider
- Attach diagnostic evidence and test results

This step marks the transition beyond Finmars operational control.

Preventive Notes

- Restrict firewall changes to controlled processes
- Audit security group changes regularly
- Maintain documented network topology and access rules

Responsibility Boundary

Finmars SCSA provides best-effort diagnostics and configuration verification.
Network outages caused by infrastructure providers, underlying hardware, or provider-managed networks are outside Finmars SCSA responsibility.

Revision #1
Created 2026-01-07 14:27:34 UTC by Sergei Zhitenev
Updated 2026-01-07 14:28:18 UTC by Sergei Zhitenev