**SafeSquid Product Security**

**Vulnerability Assessment Report**

**FOR HDFC AMC**

**Assessment Date:**

February 12, 2026

**Target System Version:**

SafeSquid 2025.1001.1232.3

**Hardening Index: 65/100**

# Executive Summary

This Product Security Vulnerability Assessment Report provides a comprehensive evaluation of the SafeSquid Secure Web Gateway (SWG) deployment. The assessment was conducted on February 12, 2026, utilizing industry-standard security scanning methodologies including network vulnerability scanning, system hardening analysis, and OVAL compliance evaluation.

## Key Findings

* **Zero Critical Vulnerabilities Detected:** OVAL compliance testing identified 0 vulnerable packages out of 41,255 total tests
* **Strong Proxy Architecture:** HTTP proxy functionality operational with content filtering and security policy enforcement
* **Comprehensive DNS Services:** BIND 9.20.18 running with DNS name resolution services on ports 53/TCP and 53/UDP
* **System Hardening Index: 65/100:** Moderate hardening posture with 47 recommendations for enhanced security
* **SSH Service Exposed:** OpenSSH 10.0p2 accessible on port 22 with suggestions for hardening

## Risk Assessment Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Level** | **Count** | **Status** | **Action** |
| **Critical** | **0** | Pass | None required |
| **High** | **0** | Pass | None required |
| **Medium** | **2** | Review | Address |
| **Low/Info** | **47** | Informational | Recommended |

# Detailed Findings

## 1. Network Vulnerability Assessment

**Methodology:** Comprehensive Nmap scanning including port enumeration, service detection, and OS fingerprinting

## Open Services Inventory

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Protocol** | **Service** | **Version** |
| 22 | TCP | SSH | OpenSSH 10.0p2 |
| 53 | TCP/UDP | DNS | ISC BIND 9.20.18 |
| 8080 | TCP | HTTP Proxy | SafeSquid 2025.1001 |

## HTTP Proxy Security Findings

**Status:** Operational

**Key Observations:**

* Proxy responds correctly with HTTP 301 redirects
* Content-Security-Policy headers properly configured
* SafeSquid custom headers present indicating active filtering
* Client identification and user-agent detection functional
* Cache management headers properly configured

## 2. OVAL Compliance Assessment

**Test Framework:** Open Vulnerability Assessment Language (OVAL)

**Total Tests Executed:** 41,255

**Vulnerable/Non-Compliant: 0**

**Compliant/Patched: 41,255 (100%)**

**Errors/Unknown:** 0

## 3. System Hardening Analysis

**Assessment Tool:** Lynis v3.1.4

**Hardening Index:** 65 / 100 (Moderate)

**Total Tests Performed:** 253

**Findings: 2 Warnings, 47 Suggestions**

# Medium-Risk Findings

## Finding 1: Firewall Rules Not Active

**Severity:** MEDIUM

**Description:** The iptables module is loaded but no firewall rules are currently active.

**Impact:** Reduces defense-in-depth protection and may allow unintended network traffic.

**Recommendation:** Deploy appropriate iptables ruleset or alternative host-based firewall.

**Action:** Configure iptables to restrict SSH and DNS access to trusted networks.

## Finding 2: Security Repository Not Configured

**Severity:** MEDIUM

**Description:** No Debian security repository configured in APT sources.

**Impact:** Security patches may not be available, increasing vulnerability exposure window.

**Recommendation:** Add Debian security repository to receive timely security updates.

**Action:** Add security repository to /etc/apt/sources.list and run apt-get update.

# Informational Findings (47 Items)

The following represents prioritized hardening recommendations from the Lynis assessment:

## High Priority Recommendations

* **SSH Hardening:** Disable TCP forwarding, X11 forwarding, and agent forwarding. Reduce MaxAuthTries and MaxSessions.
* **GRUB Password:** Set password protection on GRUB boot loader

## Medium Priority Recommendations

* Enable auditd for process accounting and audit logging
* Separate /home and /var partitions to limit disk exhaustion impact
* Install PAM password strength enforcement modules
* Disable USB and firewire drivers when not required
* Restrict compiler access to root user only

APPROVE for production deployment with remediation of findings within 7 days.