[INTERNAL - RESTRICTED DISTRIBUTION]

Network Infrastructure Audit

Internal Assessment - January 2026

Document ID:	AUDIT-2026-0003
Classification:	INTERNAL - Restricted
Conducted by:	V. Korolev (Infrastructure Auditor)
Reviewed by:	d4rkm4tter (Infrastructure Lead)
Period:	January 5-18, 2026

1. Executive Summary

This audit was conducted per quarterly schedule to assess the security posture of all production network infrastructure. The assessment covered firewall configurations, exposed services, access control policies, and network segmentation effectiveness. A total of 23 hosts were scanned across 4 network segments.

Overall risk rating: MODERATE. While critical infrastructure is properly segmented, several auxiliary services were found with insufficient access controls. Three hosts require immediate remediation. The Venom automated scanning framework identified 47 potential issues, of which 14 were confirmed as actionable findings after manual verification by V. Korolev.

2. Methodology

The audit followed the standard DP-AUDIT-7 methodology: passive reconnaissance, active port scanning (TCP full + top 1000 UDP), service enumeration, vulnerability assessment, and manual verification of critical findings. Tools used included nmap, masscan, and the internal Venom scanner (v3.2). All scanning was conducted from the designated audit VLAN to avoid triggering production IDS alerts.

Network segments assessed: PROD-1 (web-facing), PROD-2 (application layer), DATA-1 (databases and storage), MGMT (management and monitoring). Each segment was evaluated independently and cross-segment communication was verified against the approved firewall ruleset. V. Korolev performed additional manual testing on all CRITICAL and HIGH findings.

3. Critical Findings

ID	Host	Port	Service	Finding	Risk
F-01	node-01	7363	OpenSSH 8.9	Password auth enabled	MEDIUM
F-02	node-02	3306	MariaDB 10.6	Bound to 0.0.0.0	HIGH
F-03	cache-01	6379	Redis 7.0	No authentication	CRITICAL
F-04	web-02	8443	Nginx 1.22	Expired TLS cert	MEDIUM
F-05	mgmt-01	9090	Prometheus	No auth, public metrics	MEDIUM
F-06	backup-01	2222	OpenSSH 9.1	Outdated host keys	LOW
F-07	web-01	80	Apache 2.4	Directory listing enabled	MEDIUM

F-08	app-01	8080	Tomcat 9.0	Default manager creds	HIGH

4. Detailed Analysis

F-01: SSH Password Authentication

Node-01 has password authentication enabled in sshd_config despite policy SEC-041 requiring key-only authentication on all production hosts. The host accepts connections on non-standard port 7363, which provides minimal security through obscurity but does not compensate for the password authentication risk. Brute force protection via fail2ban is active but configured with generous thresholds (10 attempts / 10 min). V. Korolev successfully demonstrated a dictionary attack within the fail2ban window using a targeted wordlist.

F-02: MariaDB External Exposure

The MariaDB instance on node-02 is bound to all interfaces (0.0.0.0) rather than localhost only. While the firewall currently blocks external access to port 3306, any misconfiguration of firewall rules would immediately expose the database to the internet. The root account does not have a host restriction configured, meaning any source IP could authenticate if the firewall fails.

F-03: Redis Without Authentication (CRITICAL)

The Redis instance on cache-01 has no authentication configured and is accessible from PROD-1 and PROD-2 segments. An attacker with access to either segment could read and write to the cache, potentially manipulating session data or injecting malicious content. The Venom scanner confirmed arbitrary key read/write from any host in PROD-1. Additionally, Redis CONFIG commands are not restricted, allowing potential RCE via config file manipulation.

F-04: Expired TLS Certificate

Web-02's TLS certificate expired on 2025-12-31 and has not been renewed. Browsers display a security warning to end users. The expired certificate also means that HSTS preloading, if configured, may cause complete access failures on strict clients. Certificate management should be automated via certbot or similar ACME client.

F-07: Apache Directory Listing

Web-01 has Options +Indexes enabled in the Apache configuration, allowing directory browsing of the /uploads/ and /assets/ directories. This exposes internal file structures and potentially sensitive documents to anyone who navigates to these paths. While no credentials were found in exposed files, internal documentation and configuration templates were accessible.

F-08: Tomcat Default Credentials

The Tomcat manager interface on app-01 is accessible with default credentials (tomcat/tomcat). This allows an attacker to deploy arbitrary WAR files, effectively achieving remote code execution on the application server. This is rated HIGH rather than CRITICAL only because the Tomcat port is not directly exposed externally - access requires prior compromise of a PROD-1 host.

5. Network Segmentation Verification

Cross-segment communication was tested against the approved firewall policy. The Venom scanner attempted connections between all segment pairs on common service ports.

Source	Destination	Port	Expected	Actual	Status
PROD-1	DATA-1	3306	DENY	DENY	PASS
PROD-1	PROD-2	8080	ALLOW	ALLOW	PASS
PROD-2	DATA-1	3306	ALLOW	ALLOW	PASS
PROD-1	MGMT	9090	DENY	ALLOW	FAIL
PROD-2	MGMT	22	DENY	DENY	PASS
DATA-1	PROD-1	ANY	DENY	DENY	PASS
MGMT	PROD-1	22	ALLOW	ALLOW	PASS
PROD-1	MGMT	3000	DENY	ALLOW	FAIL
PROD-2	DATA-1	6379	ALLOW	ALLOW	PASS
DATA-1	MGMT	ANY	DENY	DENY	PASS

Two firewall rules are overly permissive, allowing PROD-1 to reach management services (Prometheus on 9090 and Grafana on 3000). These rules should be removed and management access restricted to the MGMT segment and VPN clients only.

6. Recommendations

Immediate (72 hours): Enable Redis authentication and bind to localhost. Bind MariaDB to localhost. Remove PROD-1 to MGMT firewall rules. Renew expired TLS certificate. Change Tomcat default credentials and restrict manager access to localhost only. Disable directory listing on web-01.

Short-term (30 days): Migrate all SSH to key-only authentication. Implement Project Doorman automated compliance checks across all segments. Deploy the Venom scanner on a weekly schedule with automated alerting. Review and tighten fail2ban thresholds. Implement automated certificate renewal via ACME.

Long-term (90 days): Implement network micro-segmentation for database tier. Deploy mutual TLS for all inter-service communication. Evaluate zero-trust architecture for management access. Establish automated configuration drift detection.

7. Appendix: Scan Results Summary

The following table summarizes all ports found open during the full TCP scan across all segments. Services marked with (*) were not in the approved service catalog and require review.

Host	Open Ports	Unexpected Services
node-01	22, 7363	7363 (non-standard SSH)*
node-02	22, 3306	3306 (external bind)*
cache-01	22, 6379	None
web-01	22, 80, 443	80 (directory listing)*
web-02	22, 80, 443, 8443	8443 (expired cert)*
app-01	22, 8080, 8443	8080 (default creds)*
mgmt-01	22, 3000, 9090	None (but overly accessible)
backup-01	2222	2222 (outdated keys)*
db-01	22, 5432	None
monitor-01	22, 8086, 3000	None

8. Compliance Status

Policy	Requirement	Status	Notes
SEC-041	Key-only SSH	PARTIAL	2 hosts non-compliant
SEC-055	TLS on all web services	FAIL	1 expired certificate
SEC-062	No default credentials	FAIL	Tomcat manager
SEC-070	Database localhost binding	FAIL	MariaDB on 0.0.0.0
SEC-075	Service authentication	FAIL	Redis unauthenticated
NET-010	Segment isolation	PARTIAL	2 overly permissive rules
NET-020	No directory browsing	FAIL	web-01 /uploads/

Overall compliance score: 62% (target: 95%). The infrastructure team has been given a 30-day remediation window with weekly progress reviews. V. Korolev will conduct a follow-up audit in March 2026 to verify remediation of all findings.