



TECHDEFENCELABS

Your Trusted **Cyber Security** Partner

A CERT-In Empanelled Information Security Organisation

No:- 3(15)/2004-CERT-In



Document Authorization, Revision History, and Control

Document Preparation	
Document Title	Firewall Configuration Review Assessment Report
Evaluated Organization	LKP Securities Limited
Document ID	TDL-LSL-CR-01/26/0168
Report Version	v1.0
Assessment Approach	Configuration Review Assessment Audit Report
Type of Audit Report	First Audit Report
Primary Assessment Period	08 Jan 2026 to 09 Jan 2026
Re-Assessment Period	Follow Up Not Performed
Report Prepared by	Vivek Pawar
Reviewed by	Heet Kakadiya
Approved by	Rohit Soni
Released by	Pavan Saxena
Date of Release	15 Apr 2026

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	15 Apr 2026	First Audit Report

Document Distribution List			
Name	Organization	Designation	Email Id
Dhruv Chauhan	TechDefence Labs	Manager – Enterprise Business	dhruv.chauhan@techdefence.com
Umair Patel	LKP Securities Ltd	Asst. Manager – Information Security	umair.patel@lkpsec.com

Confidentiality and Disclaimer

This report is prepared exclusively for the management of the Evaluated organization and is intended solely for internal use. TechD Cybersecurity Limited disclaims any liability to third parties for the unauthorized use or distribution of this document or its contents. The findings, information, data, advice, and recommendations are based on the cooperation of the Evaluated organization and the data provided during the assessment period. Any limitations due to environmental constraints, access restrictions, or insufficient information may have impacted the thoroughness of our analysis and could result in unidentified vulnerabilities.

The report assesses the initial security controls implemented by the Evaluated organization, specifically focusing on the security of the defined domain and systems in-scope. TechD Cybersecurity Limited highlights areas for potential improvement; however, the responsibility for implementing and maintaining robust security measures lies with the management of the Evaluated organization. The information provided in this document reflects the state of the security environment at the time of preparation and is not an exhaustive evaluation.

Note: *For the purpose of this report, the term “Evaluated organization” refers to the client organization for which this assessment was conducted.*

©TechD Cybersecurity Limited, 2026
9th Floor, Abhishree Adroit,
Near Mansi Circle, Vastrapur,
Ahmedabad-380015.

Table of Contents

Document Authorization, Revision History, and Control	2
Document Preparation	2
Document Change History	2
Document Distribution List	2
Confidentiality and Disclaimer	3
1. Assessment Details	5
1.1 Engagement Scope	5
1.2 Scope Exclusions	6
1.3 Project Team	6
1.4 Tools used during the assessment	7
2. Configuration Audit Methodology and Standards	8
2.1 Phases of the Assessment	8
2.2 Standards and Methodologies	8
3. Executive Summary	9
3.1 Visual Representation of Assessment Results	9
4. Detailed Observations	10
4.1 Firewall 2700 Configuration Review	10
4.2 Firewall 4700 Configuration Review	15
Annexure A - Engagement Limitations	20
Annexure B - Retesting Statement	20
Annexure C - Disclaimer and Precautions for Patch Implementation	21
Annexure D - CERT-In Reporting and Remediation Compliance	21

1. Assessment Details

The Evaluated organization engaged TechD Cybersecurity Limited to assess the Configuration of its infrastructure. The evaluation focused on identifying infrastructure Configuration-level vulnerabilities, testing security of its Configuration. The assessment followed industry standards, including Center for Internet Security (CIS) Benchmarks.

1.1 Engagement Scope

The following Infrastructure IPs provided by the Evaluated organization were identified as in scope for this Configuration review assessment, as defined during the engagement.

In Scope of Assessment			
Type of Infrastructure	IP Address	No. of Devices	Internal/External
Firewall	203.115.117.226, 51.162.176.206	2	Internal

1.2 Scope Exclusions

1. The configuration review of any applications hosted on the scoped IP servers/devices fall outside the specified configuration review scope will not be considered.
2. Security testing and Vulnerability Assessment and Penetration Testing (VAPT) of the scoped IPs are outside the scope of the configuration review.
3. Any part of the IPs, management console, or configurations not provided by the evaluated organization will be considered out of scope.

1.3 Project Team

Below are the TechD Cybersecurity Limited Auditing team members who played a key role in this engagement:

Name	Designation	Email-ID	Qualifications/ Certifications	Listed in CERT-In Snapshot? (Yes/No)
Pavan Saxena	Team Lead - VAPT	pavan@techdefence.com	BCA OSCP, (ISC)2 - CC, AZ-900, CEHv12, eJPT-v2, CAP, CNSP, CAPen, KLCP, ISO-27001: Lead Auditor	Yes
Rushikesh Patil	Sr. Security Analyst	Rushikesh.patil@techdefence.com	CEH Master, ISO27001	No
Kunal Patil	Security Analyst	kunal.p@techdefence.com	BSc, CAP, CNSP	No

1.4 Tools used during the assessment

Sr. No	Name of Tool /Software used	Version of the tool /Software used	Open Source /Licensed
01	Nessus Professional	v 10.11.3	Licensed

2. Configuration Audit Methodology and Standards

2.1 Phases of the Assessment

- **Pre-engagement Phase:** Define the scope, timeline, and rules of engagement for the review. Identify relevant CIS benchmarks to be followed for the configuration assessment.
- **Configuration Analysis:** Compare system configurations against CIS benchmarks using automated tools and manual techniques. Identify deviations, vulnerabilities, and misconfigurations.
- **Manual Analysis:** Manually inspect critical configurations that automated tools may miss, focusing on areas like user access controls and service settings to uncover complex risks.
- **Reporting and Recommendations:** Document configuration weaknesses and their potential impact. Provide prioritized, actionable recommendations to align systems with CIS best practices.
- **Remediation and Rescan:** After remediation, rescan systems to ensure vulnerabilities are fixed. Verify compliance with CIS benchmarks and ensure no new risks have been introduced.

2.2 Standards and Methodologies

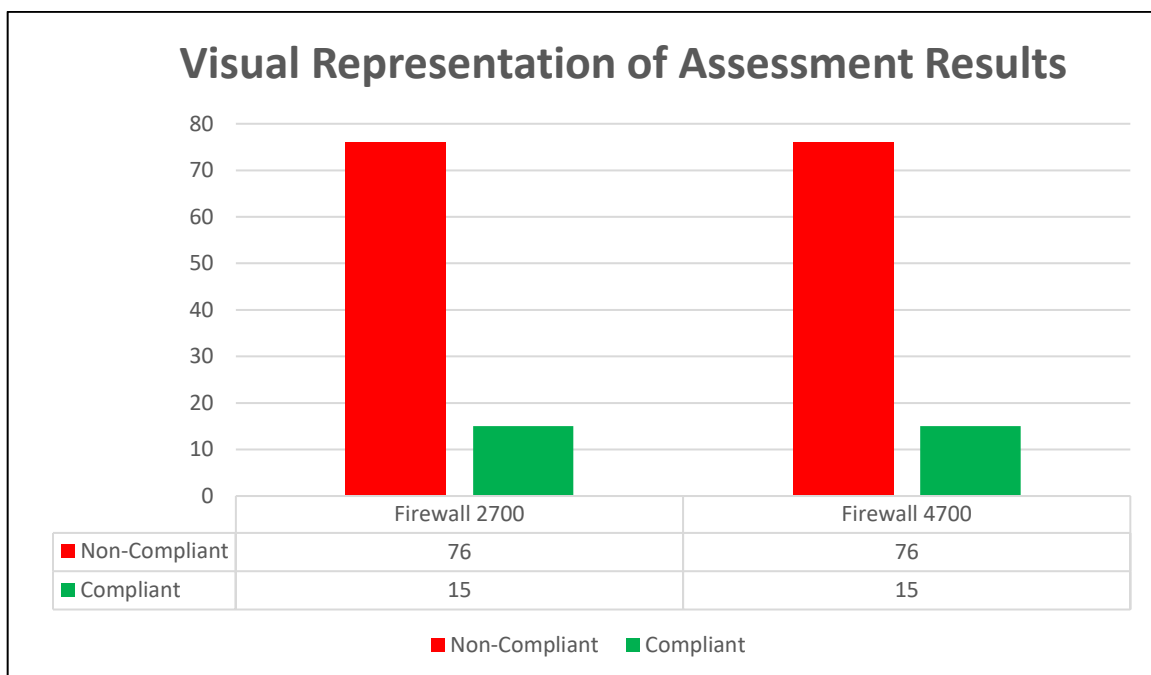
- **Center for Internet Security (CIS) Benchmarks:** The CIS Benchmarks are a set of globally recognized best practices designed to secure IT systems and data from cyber threats. Developed through a consensus-based process involving cybersecurity professionals, government agencies, and industry experts, these benchmarks provide comprehensive configuration guidelines. They cover a wide range of IT systems, including operating systems, server software, cloud computing environments, network devices, and mobile devices.

These benchmarks serve as a foundational standard for performing configuration reviews, ensuring that systems are securely configured and compliant with industry best practices. By following CIS Benchmarks, organizations can significantly enhance their security posture and reduce the risk of vulnerabilities in their systems.

3. Executive Summary

The following section provides an Executive Summary of the Configuration Review Audit, highlighting both compliant and non-compliant aspects identified during the audit. Detailed recommendations for each observation are outlined in Section 4 of this report.

3.1 Visual Representation of Assessment Results



4. Detailed Observations

4.1 Firewall 2700 Configuration Review

#	Audit Check Name	IP Address	Infrastructure Type	Status
1	SonicWALL - AAA - LDAP server is trusted	203.115.117.226	Firewall 2700	Non-Compliant
2	SonicWALL - AAA - RADIUS server is trusted	203.115.117.226	Firewall 2700	Non-Compliant
3	SonicWALL - Anti-Spyware - DMZ	203.115.117.226	Firewall 2700	Non-Compliant
4	SonicWALL - Anti-Spyware - LAN	203.115.117.226	Firewall 2700	Non-Compliant
5	SonicWALL - Anti-Spyware - WAN	203.115.117.226	Firewall 2700	Non-Compliant
6	SonicWALL - Anti-Spyware - WLAN	203.115.117.226	Firewall 2700	Non-Compliant
7	SonicWALL - AutoDownload Firmware - Enabled	203.115.117.226	Firewall 2700	Non-Compliant
8	SonicWALL - AutoUpdate - Enabled	203.115.117.226	Firewall 2700	Non-Compliant
9	SonicWALL - Client AV Enforcement On - DMZ	203.115.117.226	Firewall 2700	Non-Compliant
10	SonicWALL - Client AV Enforcement On - LAN	203.115.117.226	Firewall 2700	Non-Compliant
11	SonicWALL - Client AV Enforcement On - WLAN	203.115.117.226	Firewall 2700	Non-Compliant
12	SonicWALL - Content Filtering On - DMZ	203.115.117.226	Firewall 2700	Non-Compliant
13	SonicWALL - Content Filtering On - LAN	203.115.117.226	Firewall 2700	Non-Compliant
14	SonicWALL - Content Filtering On - WLAN	203.115.117.226	Firewall 2700	Non-Compliant
15	SonicWALL - Detection Prevention - ICMP packets	203.115.117.226	Firewall 2700	Non-Compliant
16	SonicWALL - Detection Prevention - IP TTL Decrement	203.115.117.226	Firewall 2700	Non-Compliant
17	SonicWALL - Flood Protection - Layer 2 - All Interfaces	203.115.117.226	Firewall 2700	Non-Compliant
18	SonicWALL - Flood Protection - Layer 2 - Threshold	203.115.117.226	Firewall 2700	Non-Compliant
19	SonicWALL - Flood Protection - Layer 2 - WAN machines	203.115.117.226	Firewall 2700	Non-Compliant
20	SonicWALL - Flood Protection - TCP - Enforce compliance	203.115.117.226	Firewall 2700	Non-Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
21	SonicWALL - Flood Protection - TCP - Max Seg Lifetime	203.115.117.226	Firewall 2700	Non-Compliant
22	SonicWALL - Flood Protection - TCP - Timeout <= 5 minutes	203.115.117.226	Firewall 2700	Non-Compliant
23	SonicWALL - GAV ON - DMZ	203.115.117.226	Firewall 2700	Non-Compliant
24	SonicWALL - GAV ON - LAN	203.115.117.226	Firewall 2700	Non-Compliant
25	SonicWALL - GAV ON - WAN	203.115.117.226	Firewall 2700	Non-Compliant
26	SonicWALL - GAV ON - WLAN	203.115.117.226	Firewall 2700	Non-Compliant
27	SonicWALL - GMS hostname/IP - Review	203.115.117.226	Firewall 2700	Non-Compliant
28	SonicWALL - IDP ON - DMZ	203.115.117.226	Firewall 2700	Non-Compliant
29	SonicWALL - IDP ON - LAN	203.115.117.226	Firewall 2700	Non-Compliant
30	SonicWALL - IDP ON - WAN	203.115.117.226	Firewall 2700	Non-Compliant
31	SonicWALL - IDP ON - WLAN	203.115.117.226	Firewall 2700	Non-Compliant
32	SonicWALL - Logging Level - Information	203.115.117.226	Firewall 2700	Non-Compliant
33	SonicWALL - Login Banner - Public Zone	203.115.117.226	Firewall 2700	Non-Compliant
34	SonicWALL - Login Banner - Trusted Zone	203.115.117.226	Firewall 2700	Non-Compliant
35	SonicWALL - Login Banner - VPN Zone	203.115.117.226	Firewall 2700	Non-Compliant
36	SonicWALL - Login Banner - WAN Zone	203.115.117.226	Firewall 2700	Non-Compliant
37	SonicWALL - Login Banner - Wireless Zone	203.115.117.226	Firewall 2700	Non-Compliant
38	SonicWALL - PW Policy - Lockout - Num Attempts <=3	203.115.117.226	Firewall 2700	Non-Compliant
39	SonicWALL - PW Policy - Lockout Duration - >= 5 minutes	203.115.117.226	Firewall 2700	Non-Compliant
40	SonicWALL - Password Policy - Affected User types	203.115.117.226	Firewall 2700	Non-Compliant
41	SonicWALL - Password Policy - Affected User types - full-admins	203.115.117.226	Firewall 2700	Non-Compliant
42	SonicWALL - Password Policy - Affected User types - limited-admins	203.115.117.226	Firewall 2700	Non-Compliant
43	SonicWALL - Password Policy - Change Period <=30 days	203.115.117.226	Firewall 2700	Non-Compliant
44	SonicWALL - Password Policy - Complexity Level	203.115.117.226	Firewall 2700	Non-Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
45	SonicWALL - Password Policy - Password Uniqueness >= 10	203.115.117.226	Firewall 2700	Non-Compliant
46	SonicWALL - Password Policy - minimum length >= 8	203.115.117.226	Firewall 2700	Non-Compliant
47	SonicWALL - Review the DNS Server Settings	203.115.117.226	Firewall 2700	Non-Compliant
48	SonicWALL - Review the NTP server configuration	203.115.117.226	Firewall 2700	Non-Compliant
49	SonicWALL - SSL Control - Block the conn. and log the event	203.115.117.226	Firewall 2700	Non-Compliant
50	SonicWALL - SSL Control - Certs - Untrusted CA	203.115.117.226	Firewall 2700	Non-Compliant
51	SonicWALL - SSL Control - Detect Expired Certificates	203.115.117.226	Firewall 2700	Non-Compliant
52	SonicWALL - SSL Control - Detect MD5 Digest	203.115.117.226	Firewall 2700	Non-Compliant
53	SonicWALL - SSL Control - Detect SSLv2	203.115.117.226	Firewall 2700	Non-Compliant
54	SonicWALL - SSL Control - Detect Self-signed certs	203.115.117.226	Firewall 2700	Non-Compliant
55	SonicWALL - SSL Control - Detect Weak Ciphers (<64 bits)	203.115.117.226	Firewall 2700	Non-Compliant
56	SonicWALL - SSL Control - Enable Blacklist	203.115.117.226	Firewall 2700	Non-Compliant
57	SonicWALL - SSL Control - Enable Whitelist	203.115.117.226	Firewall 2700	Non-Compliant
58	SonicWALL - SSL Control ON - DMZ	203.115.117.226	Firewall 2700	Non-Compliant
59	SonicWALL - SSL Control ON - LAN	203.115.117.226	Firewall 2700	Non-Compliant
60	SonicWALL - SSL Control ON - WAN	203.115.117.226	Firewall 2700	Non-Compliant
61	SonicWALL - SSL Control ON - WLAN	203.115.117.226	Firewall 2700	Non-Compliant
62	SonicWALL - Security Services - Gateway AV - CIFS/Netbios	203.115.117.226	Firewall 2700	Non-Compliant
63	SonicWALL - Security Services - Gateway AV - Enabled	203.115.117.226	Firewall 2700	Non-Compliant
64	SonicWALL - Security Services - Gateway AV - FTP Inbound	203.115.117.226	Firewall 2700	Non-Compliant
65	SonicWALL - Security Services - Gateway AV - FTP Outbound	203.115.117.226	Firewall 2700	Non-Compliant
66	SonicWALL - Security Services - Gateway AV - HTTP Inbound	203.115.117.226	Firewall 2700	Non-Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
67	SonicWALL - Security Services - Gateway AV - HTTP Outbound	203.115.117.226	Firewall 2700	Non-Compliant
68	SonicWALL - Security Services - Gateway AV - IMAP	203.115.117.226	Firewall 2700	Non-Compliant
69	SonicWALL - Security Services - Gateway AV - POP3	203.115.117.226	Firewall 2700	Non-Compliant
70	SonicWALL - Security Services - Gateway AV - SMTP Inbound	203.115.117.226	Firewall 2700	Non-Compliant
71	SonicWALL - Security Services - Gateway AV - SMTP Outbound	203.115.117.226	Firewall 2700	Non-Compliant
72	SonicWALL - Security Services - Gateway AV - TCP Stream Inbound	203.115.117.226	Firewall 2700	Non-Compliant
73	SonicWALL - Security Services - Gateway AV - TCP Stream Outbound	203.115.117.226	Firewall 2700	Non-Compliant
74	SonicWALL - Security Services - IDP - Enabled	203.115.117.226	Firewall 2700	Non-Compliant
75	SonicWALL - Syslog server - >=1 server configured	203.115.117.226	Firewall 2700	Non-Compliant
76	SonicWALL - User Inactivity Timeout - 5 minutes or less	203.115.117.226	Firewall 2700	Non-Compliant
77	SonicWALL - Detection Prevention - Randomize IP IDs	203.115.117.226	Firewall 2700	Compliant
78	SonicWALL - Detection Prevention - Stealth Mode	203.115.117.226	Firewall 2700	Compliant
79	SonicWALL - Disable insecure services - HTTP	203.115.117.226	Firewall 2700	Compliant
80	SonicWALL - Ensure default 'admin' username is not used	203.115.117.226	Firewall 2700	Compliant
81	SonicWALL - Flood Protection - Layer 3 - Protection Mode	203.115.117.226	Firewall 2700	Compliant
82	SonicWALL - Flood Protection - TCP - Handshake enforcement	203.115.117.226	Firewall 2700	Compliant
83	SonicWALL - Flood Protection - TCP - checksum enforcement	203.115.117.226	Firewall 2700	Compliant
84	SonicWALL - Log Alert Emails - Enabled	203.115.117.226	Firewall 2700	Compliant
85	SonicWALL - Password Policy - User Lockout - Enabled	203.115.117.226	Firewall 2700	Compliant
86	SonicWALL - SNMP Community Name - 'public' or 'private'	203.115.117.226	Firewall 2700	Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
87	SonicWALL - SSL Control - Enable SSL Control	203.115.117.226	Firewall 2700	Compliant
88	SonicWALL - Use non default admin access ports - 'SSH'	203.115.117.226	Firewall 2700	Compliant
89	SonicWALL - Use non default admin access ports - HTTP	203.115.117.226	Firewall 2700	Compliant
90	SonicWALL - Use non default admin access ports - HTTPS	203.115.117.226	Firewall 2700	Compliant
91	SonicWALL - Web Interface - Does not use self-signed cert	203.115.117.226	Firewall 2700	Compliant

4.2 Firewall 4700 Configuration Review

#	Audit Check Name	IP Address	Infrastructure Type	Status
1	SonicWALL - AAA - LDAP server is trusted	51.162.176.206	Firewall 2400	Non-Compliant
2	SonicWALL - AAA - RADIUS server is trusted	51.162.176.206	Firewall 4700	Non-Compliant
3	SonicWALL - Anti-Spyware - DMZ	51.162.176.206	Firewall 4700	Non-Compliant
4	SonicWALL - Anti-Spyware - LAN	51.162.176.206	Firewall 4700	Non-Compliant
5	SonicWALL - Anti-Spyware - WAN	51.162.176.206	Firewall 4700	Non-Compliant
6	SonicWALL - Anti-Spyware - WLAN	51.162.176.206	Firewall 4700	Non-Compliant
7	SonicWALL - AutoDownload Firmware - Enabled	51.162.176.206	Firewall 4700	Non-Compliant
8	SonicWALL - AutoUpdate - Enabled	51.162.176.206	Firewall 4700	Non-Compliant
9	SonicWALL - Client AV Enforcement On - DMZ	51.162.176.206	Firewall 4700	Non-Compliant
10	SonicWALL - Client AV Enforcement On - LAN	51.162.176.206	Firewall 4700	Non-Compliant
11	SonicWALL - Client AV Enforcement On - WLAN	51.162.176.206	Firewall 4700	Non-Compliant
12	SonicWALL - Content Filtering On - DMZ	51.162.176.206	Firewall 4700	Non-Compliant
13	SonicWALL - Content Filtering On - LAN	51.162.176.206	Firewall 4700	Non-Compliant
14	SonicWALL - Content Filtering On - WLAN	51.162.176.206	Firewall 4700	Non-Compliant
15	SonicWALL - Detection Prevention - ICMP packets	51.162.176.206	Firewall 4700	Non-Compliant
16	SonicWALL - Detection Prevention - IP TTL Decrement	51.162.176.206	Firewall 4700	Non-Compliant
17	SonicWALL - Flood Protection - Layer 2 - All Interfaces	51.162.176.206	Firewall 4700	Non-Compliant
18	SonicWALL - Flood Protection - Layer 2 - Threshold	51.162.176.206	Firewall 4700	Non-Compliant
19	SonicWALL - Flood Protection - Layer 2 - WAN machines	51.162.176.206	Firewall 4700	Non-Compliant
20	SonicWALL - Flood Protection - TCP - Enforce compliance	51.162.176.206	Firewall 4700	Non-Compliant
21	SonicWALL - Flood Protection - TCP - Max Seg Lifetime	51.162.176.206	Firewall 4700	Non-Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
22	SonicWALL - Flood Protection - TCP - Timeout <= 5 minutes	51.162.176.206	Firewall 4700	Non-Compliant
23	SonicWALL - GAV ON - DMZ	51.162.176.206	Firewall 4700	Non-Compliant
24	SonicWALL - GAV ON - LAN	51.162.176.206	Firewall 4700	Non-Compliant
25	SonicWALL - GAV ON - WAN	51.162.176.206	Firewall 4700	Non-Compliant
26	SonicWALL - GAV ON - WLAN	51.162.176.206	Firewall 4700	Non-Compliant
27	SonicWALL - GMS hostname/IP - Review	51.162.176.206	Firewall 4700	Non-Compliant
28	SonicWALL - IDP ON - DMZ	51.162.176.206	Firewall 4700	Non-Compliant
29	SonicWALL - IDP ON - LAN	51.162.176.206	Firewall 4700	Non-Compliant
30	SonicWALL - IDP ON - WAN	51.162.176.206	Firewall 4700	Non-Compliant
31	SonicWALL - IDP ON - WLAN	51.162.176.206	Firewall 4700	Non-Compliant
32	SonicWALL - Logging Level - Information	51.162.176.206	Firewall 4700	Non-Compliant
33	SonicWALL - Login Banner - Public Zone	51.162.176.206	Firewall 4700	Non-Compliant
34	SonicWALL - Login Banner - Trusted Zone	51.162.176.206	Firewall 4700	Non-Compliant
35	SonicWALL - Login Banner - VPN Zone	51.162.176.206	Firewall 4700	Non-Compliant
36	SonicWALL - Login Banner - WAN Zone	51.162.176.206	Firewall 4700	Non-Compliant
37	SonicWALL - Login Banner - Wireless Zone	51.162.176.206	Firewall 4700	Non-Compliant
38	SonicWALL - PW Policy - Lockout - Num Attempts <=3	51.162.176.206	Firewall 4700	Non-Compliant
39	SonicWALL - PW Policy - Lockout Duration - >= 5 minutes	51.162.176.206	Firewall 4700	Non-Compliant
40	SonicWALL - Password Policy - Affected User types	51.162.176.206	Firewall 4700	Non-Compliant
41	SonicWALL - Password Policy - Affected User types - full-admins	51.162.176.206	Firewall 4700	Non-Compliant
42	SonicWALL - Password Policy - Affected User types - limited-admins	51.162.176.206	Firewall 4700	Non-Compliant
43	SonicWALL - Password Policy - Change Period <=30 days	51.162.176.206	Firewall 4700	Non-Compliant
44	SonicWALL - Password Policy - Complexity Level	51.162.176.206	Firewall 4700	Non-Compliant
45	SonicWALL - Password Policy - Password Uniqueness >= 10	51.162.176.206	Firewall 4700	Non-Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
46	SonicWALL - Password Policy - minimum length >= 8	51.162.176.206	Firewall 4700	Non-Compliant
47	SonicWALL - Review the DNS Server Settings	51.162.176.206	Firewall 4700	Non-Compliant
48	SonicWALL - Review the NTP server configuration	51.162.176.206	Firewall 4700	Non-Compliant
49	SonicWALL - SSL Control - Block the conn. and log the event	51.162.176.206	Firewall 4700	Non-Compliant
50	SonicWALL - SSL Control - Certs - Untrusted CA	51.162.176.206	Firewall 4700	Non-Compliant
51	SonicWALL - SSL Control - Detect Expired Certificates	51.162.176.206	Firewall 4700	Non-Compliant
52	SonicWALL - SSL Control - Detect MD5 Digest	51.162.176.206	Firewall 4700	Non-Compliant
53	SonicWALL - SSL Control - Detect SSLv2	51.162.176.206	Firewall 4700	Non-Compliant
54	SonicWALL - SSL Control - Detect Self-signed certs	51.162.176.206	Firewall 4700	Non-Compliant
55	SonicWALL - SSL Control - Detect Weak Ciphers (<64 bits)	51.162.176.206	Firewall 4700	Non-Compliant
56	SonicWALL - SSL Control - Enable Blacklist	51.162.176.206	Firewall 4700	Non-Compliant
57	SonicWALL - SSL Control - Enable Whitelist	51.162.176.206	Firewall 4700	Non-Compliant
58	SonicWALL - SSL Control ON - DMZ	51.162.176.206	Firewall 4700	Non-Compliant
59	SonicWALL - SSL Control ON - LAN	51.162.176.206	Firewall 4700	Non-Compliant
60	SonicWALL - SSL Control ON - WAN	51.162.176.206	Firewall 4700	Non-Compliant
61	SonicWALL - SSL Control ON - WLAN	51.162.176.206	Firewall 4700	Non-Compliant
62	SonicWALL - Security Services - Gateway AV - CIFS/Netbios	51.162.176.206	Firewall 4700	Non-Compliant
63	SonicWALL - Security Services - Gateway AV - Enabled	51.162.176.206	Firewall 4700	Non-Compliant
64	SonicWALL - Security Services - Gateway AV - FTP Inbound	51.162.176.206	Firewall 4700	Non-Compliant
65	SonicWALL - Security Services - Gateway AV - FTP Outbound	51.162.176.206	Firewall 4700	Non-Compliant
66	SonicWALL - Security Services - Gateway AV - HTTP Inbound	51.162.176.206	Firewall 4700	Non-Compliant
67	SonicWALL - Security Services - Gateway AV - HTTP Outbound	51.162.176.206	Firewall 4700	Non-Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
68	SonicWALL - Security Services - Gateway AV - IMAP	51.162.176.206	Firewall 4700	Non-Compliant
69	SonicWALL - Security Services - Gateway AV - POP3	51.162.176.206	Firewall 4700	Non-Compliant
70	SonicWALL - Security Services - Gateway AV - SMTP Inbound	51.162.176.206	Firewall 4700	Non-Compliant
71	SonicWALL - Security Services - Gateway AV - SMTP Outbound	51.162.176.206	Firewall 4700	Non-Compliant
72	SonicWALL - Security Services - Gateway AV - TCP Stream Inbound	51.162.176.206	Firewall 4700	Non-Compliant
73	SonicWALL - Security Services - Gateway AV - TCP Stream Outbound	51.162.176.206	Firewall 4700	Non-Compliant
74	SonicWALL - Security Services - IDP - Enabled	51.162.176.206	Firewall 4700	Non-Compliant
75	SonicWALL - Syslog server - >=1 server configured	51.162.176.206	Firewall 4700	Non-Compliant
76	SonicWALL - User Inactivity Timeout - 5 minutes or less	51.162.176.206	Firewall 4700	Non-Compliant
77	SonicWALL - Detection Prevention - Randomize IP IDs	51.162.176.206	Firewall 4700	Compliant
78	SonicWALL - Detection Prevention - Stealth Mode	51.162.176.206	Firewall 4700	Compliant
79	SonicWALL - Disable insecure services - HTTP	51.162.176.206	Firewall 4700	Compliant
80	SonicWALL - Ensure default 'admin' username is not used	51.162.176.206	Firewall 4700	Compliant
81	SonicWALL - Flood Protection - Layer 3 - Protection Mode	51.162.176.206	Firewall 4700	Compliant
82	SonicWALL - Flood Protection - TCP - Handshake enforcement	51.162.176.206	Firewall 4700	Compliant
83	SonicWALL - Flood Protection - TCP - checksum enforcement	51.162.176.206	Firewall 4700	Compliant
84	SonicWALL - Log Alert Emails - Enabled	51.162.176.206	Firewall 4700	Compliant
85	SonicWALL - Password Policy - User Lockout - Enabled	51.162.176.206	Firewall 4700	Compliant
86	SonicWALL - SNMP Community Name - 'public' or 'private'	51.162.176.206	Firewall 4700	Compliant
87	SonicWALL - SSL Control - Enable SSL Control	51.162.176.206	Firewall 4700	Compliant

#	Audit Check Name	IP Address	Infrastructure Type	Status
88	SonicWALL - Use non default admin access ports - 'SSH'	51.162.176.206	Firewall 4700	Compliant
89	SonicWALL - Use non default admin access ports - HTTP	51.162.176.206	Firewall 4700	Compliant
90	SonicWALL - Use non default admin access ports - HTTPS	51.162.176.206	Firewall 4700	Compliant
91	SonicWALL - Web Interface - Does not use self-signed cert	51.162.176.206	Firewall 4700	Compliant

Annexure A - Engagement Limitations

The security assessment was conducted within the scope and timeline agreed upon during the engagement with the Evaluated organization. Due to time limitations and operational constraints, it may not have been possible to identify every potential vulnerability present within the environment.

Testing activities were limited to the systems, endpoints, and functionalities that were made accessible by the Evaluated organization during the defined assessment period. The findings presented in this report represent the security posture of the evaluated systems at the time of testing and should not be interpreted as a guarantee that no additional vulnerabilities exist.

Annexure B - Retesting Statement

Upon completion of remediation activities by the Evaluated organization, a re-assessment may be conducted to verify whether the identified vulnerabilities have been successfully mitigated. The purpose of the re-assessment is limited to validating the remediation of the specific findings documented in this report.

The Evaluated organization is expected to address the identified vulnerabilities within a period of ninety (90) days from the date of report issuance, in accordance with the agreed remediation service level timelines. Re-assessment requests submitted within this period will be accommodated as part of the engagement to verify the implemented fixes.

Requests for re-assessment submitted after the ninety (90) day remediation window may be subject to a separate engagement or additional scope, as the validity and relevance of the original findings may change over time due to updates in the application environment.

Annexure C - Disclaimer and Precautions for Patch Implementation

Before implementing any remediation, actions based on this report, the following precautions should be observed:

- **Backup & Recovery:** Ensure complete backups of systems, applications, and data are taken prior to changes, along with a defined rollback plan to restore services in case of failure.
- **Controlled Testing:** Validate all fixes in a UAT or staging environment before deploying to production to avoid service disruption.
- **Third-Party References:** External links provided for remediation guidance are for reference only; their accuracy and availability are not guaranteed.
- **Assessment Limitations:** Findings are based on testing performed within the defined scope, timeline, and accessible environment. Certain vulnerabilities, especially those requiring intrusive testing, may not have been identified.
- **Point-in-Time Evaluation:** This report reflects the security posture at the time of assessment. New vulnerabilities may emerge due to system changes or evolving threats.
- **Ongoing Security Responsibility:** Security is a continuous process. The responsibility for implementing fixes and maintaining security controls rests with the Evaluated organization.

Annexure D - CERT-In Reporting and Remediation Compliance

As a CERT-IN empanelled organization, we have received communication stating that all CERT-IN empanelled organizations are required to submit audit-related data (including Cyber Audits, IS Audits, Regulatory audits, and VAPT audits) to CERT-IN starting from the fiscal year 2024. We will be sharing this VAPT Audit Reports or related details with CERT-IN. According to CERT-IN regulations, a period of 90 days is provided for the remediation/patching process from the release date of the audit reports. Therefore, we kindly request you to address all mentioned vulnerabilities within the 90-day timeframe and to inform us for the follow-up audit.