Government of India
Department of Telecommunications
Telecommunication Engineering Centre
Gate No. 5, Khurshid Lal Bhawan, Janpath, New Delhi-110001.
(IT Division)

File No. 4-1/2022-IT/TEC/MTCTE issues-Part(3) Dated: 05.06.2025

Subject: **Formulation of new Standard for Essential Requirements(ER) of "Load Balancer Equipment" - Inviting comments.**

In exercise of the powers conferred by rule 5(1) of the Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules 2025, a draft new Standard for Essential Requirements (ER) of "Load Balancer Equipment" is enclosed herewith (**Annexure-I**) for stakeholder consultation. It is requested to go through the aforesaid enclosed draft Standard and offer your inputs/comments.

2. The comments may please be furnished in the template sheet enclosed herewith as Annexure-II through email to **adic1.tec@gov.in** & **diri.tec@nic.in** at the earliest and latest within **sixty days** please.

Enclosures:
(i) Draft Standard for Essential Requirements (ER) of "Load Balancer Equipment" (**Annexure-I**)
(ii) Template/Format sheet for providing comments (**Annexure-II**)

(Jasvir Singh Panesar)
Director (IT), TEC
Email: diri.tec@nic.in

To,

All Manufacturer & Stakeholders

Copy to:
1. Sr DDG TEC
2. AD(IT), TEC - with request for uploading on TEC website/Portal
3. AD(IMP&TEP), TEC - with request for uploading on TBT Enquiry Point

Annexure-I

Draft ER -- Load Balancer Equipment

Scope: This ER covers all types of Load Balancers such as Hardware Load Balancers, Software load balancers, Cloud Load balancers, Application delivery controllers, Network Load balancers.

Definition: Any network or application-layer device that performs load balancing functions, such as distributing incoming traffic across multiple servers/resources to optimize performance, ensure high availability, and prevent server overload, can be tested as per Load Balancer parameters.

1. Variant 1: Load Balancer Equipment

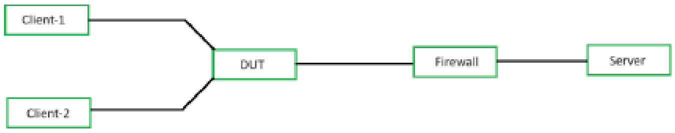
1.1 Parameters Linked with Product Variant:

S.No.	Parameter Name	Standard Name (Name of Standard RFC/ Functional Test)
1.1.1	Conducted And Radiated Emission - Class A	TEC EMI EMC Standard CISPR 32 EN550 32. Annex-B
1.1.2	Immunity to AC Voltage Dips and Short Interruptions	TEC EMI EMC Standard EN/IEC:61000-4-11. Annex-B
1.1.3	Immunity to DC Voltage Dips and Short Interruptions	EN/IEC:61000-4-29. Annex-B
1.1.4	Immunity to Electrostatic Discharge	TEC EMI EMC Standard EN/IEC:61000-4-2. Annex-B
1.1.5	Immunity to Fast Transients (Burst)	TEC EMI EMC Standard EN/IEC:61000-4-4. Annex-B
1.1.6	Immunity to Radiated RF	TEC EMI EMC Standard EN/IEC:61000-4-3. Annex-B
1.1.7	Immunity to RF Field Induced Conducted Disturbance	TEC EMI EMC Standard EN/IEC:61000-4-6. Annex-B
1.1.8	Immunity to Surges	TEC EMI EMC Standard EN/IEC:61000-4-5. Annex-B
1.1.9	IT Equipment Safety	IS 13252-1 or IEC:60950-1 or IEC 62368-1. Annex-A1
1.1.10	Manageability SNMP V2 or V3	RFC 3416 or RFC 3410. Functional Test No 38 or 39
1.1.11	IPv4 Parameters Set-D	RFC 791, Annex-P11
1.1.12	IPv6 Parameters	RFC 8200,4861, 4862, 8201, 4443 Annex-P11

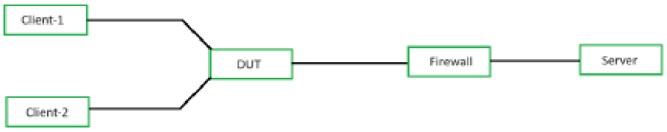
1.1.13	L3 DDoS Protection	Functional Test No. 51 Annex-P11
1.1.14	L4 DDoS Protection	Functional Test No. 52 Annex-P11
1.1.15	L7 DDoS protection	Functional Test No. 53 Annex-P11
1.1.16	Server Health Check	Functional Test – T1
1.1.17	Dynamic Traffic Distribution	Functional Test – T2
1.1.18	Persistent Session Management	Functional Test – T3
1.1.19	SSL/TLS Offloading	Functional Test – T4

Interfaces: Inputs may be given for various types interfaces applicable to this Equipment.

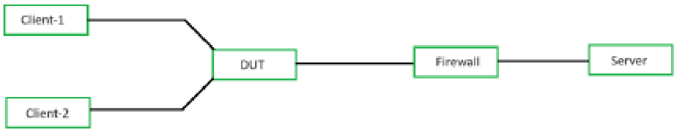
Test No.-51

Parameter Name	L3 DDoS protection	**Requirement**	The IP Security equipment should be able to detect and prevent L3 DDoS attacks
Objective	To verify if the IP Security equipment has the capability to detect and prevent against Layer 3 DDoS attack.		
Topology			
Pre-Test Conditions			
1. Configure the DUT to be inline with the firewall. 2. Configure the client on external side of DUT and server on internal side of DUT. 3. Configure the security profile for identifying and protecting against L3 DDoS attack. 4. Apply the profile to IP Security policy.			
Test Procedure		**Expected Results**	
1. Perform normal ping from Client-1 and perform ICMP flood from Client-2. 2. Verify if the DUT can identify the flood traffic and block it. 3. Perform ICMP flood attack from Client-2 with random source IP addresses. 4. Verify if the DUT can identify the flood traffic and block it. 5. Verify the CPU usage and memory utilization on server.		1. The DUT must identify the L3 DDoS attack and block the flood traffic. 2. Server memory and CPU utilization must stay under threshold.	

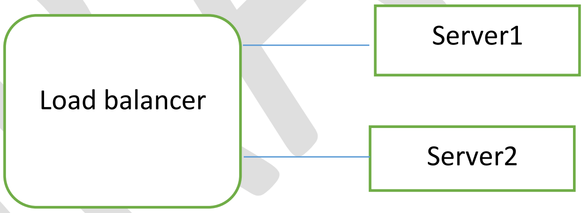
Test No.-52

Parameter Name	L4 DDoS protection	**Requirement**	The IP Security equipment should be able to detect and prevent L4 DDoS attacks
Objective	To verify if the IP Security equipment has the capability to detect and prevent against Layer 4 DDoS attack.		
Topology			
Pre-Test Conditions			
1. Configure the DUT to be inline with the firewall. 2. Configure the client on external side of DUT and server on internal side of DUT. 3. Configure the security profile for identifying and protecting against L4 DDoS attack. 4. Apply the profile to IP Security policy.			
Test Procedure		**Expected Results**	
1. Send a normal TCP-SYN from Client-1 and perform TCP SYN and UDP flood from Client-2. 2. Verify if the DUT can identify the flood traffic and block it. 3. Perform TCP SYN and UDP flood attack from Client-2 with random source IP addresses. 4. Verify if the DUT can identify the flood traffic and block it. 5. Verify the CPU usage and memory utilization on server.		1. The DUT must identify the L4 DDoS attack and block the flood traffic. 2. Server memory and CPU utilization must stay under threshold.	

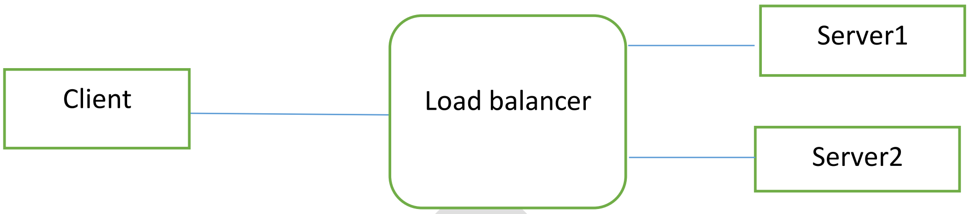
Test No.-53

Parameter Name	L7 DDoS protection	**Requirement**	The IP Security equipment should be able to detect and prevent L7 DDoS attacks
Objective	To verify if the IP Security equipment has the capability to detect and prevent against Layer 7 DDoS attack.		
Topology			
Pre-Test Conditions			
1. Configure the DUT to be inline with the firewall. 2. Configure the client on external side of DUT and server on internal side of DUT. 3. Configure the security profile for identifying and protecting against L7 DDoS attack. 4. Apply the profile to IP Security policy.			
Test Procedure		**Expected Results**	
1. Send a normal HTTP request from Client-1 and perform HTTP/HTTPS flood from Client-2. 2. Verify if the DUT can identify the flood traffic and block it. 3. Perform HTTP/HTTPS flood attack from Client-2 with random source IP addresses. 4. Verify if the DUT can identify the flood traffic and block it.		1. The DUT must identify the L7 DDoS attack and block the flood traffic. 2. Server memory and CPU utilization must stay under threshold.	

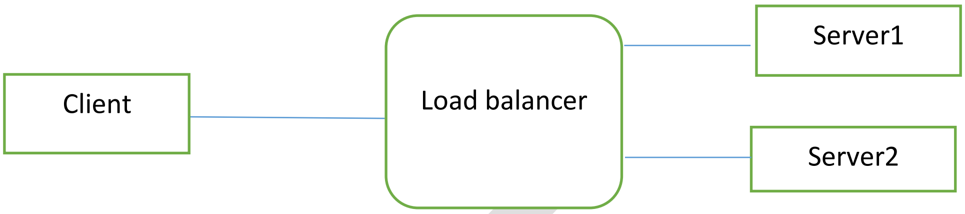
Functional Test – T1

Parameter Name	Server Health Check	**Requirement**	The load balancer shall periodically perform health checks on backend servers and remove unhealthy servers from the server pool.
Objective	To verify if the load balancer is able to perform periodic health checks on backend servers and remove unhealthy servers from the server pool		
Topology			
Pre-Test Conditions			
1. Load balancer is configured with necessary health check parameters 2. Server1 and Server2 are configured to respond HTTP status 200 (OK) to Load balance health check requests.			
Test Procedure		**Expected Results**	
1. Ensure the backend servers are added to the server pool in load balancer. 2. Ensure Load balancer is configured with necessary health check parameters. 3. Configure Server2 to respond with HTTP status 500 (Internal server error) to load balancer health check request. 4. Verify if the Load balancer detects unhealthy server and removes it from the server pool. 5. Resolve the unhealthy server (Server2) by configuring to respond with HTTP status 200 (OK) for Load balancer health check request. 6. Verify if the Load balancer detects that server is recovered and adds back to the server pool.		1. The Load balancer shall detect Server2 failure and remove it from the server pool. 2. The Load balancer shall detect Server2 restoration and add it back to the server pool. 3. The Load balancer shall generate logs for Server2 failure and restoration events.	

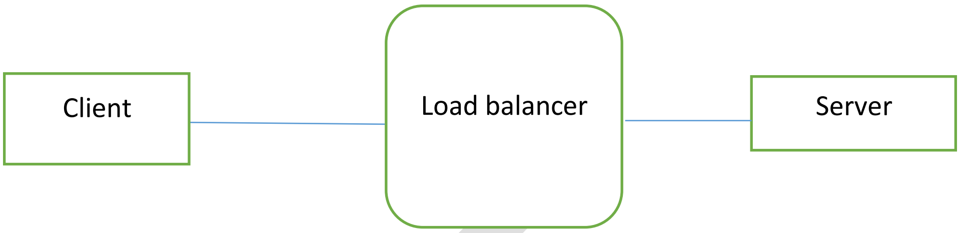
Functional Test – T2

Parameter Name	Dynamic Traffic Distribution	**Requirement**	The load balancer shall distribute incoming client requests dynamically across all backend servers based on the configured load balancing algorithm.
Objective	To validate that the load balancer distributes incoming client requests across all backend servers dynamically based on the configured load balancing algorithm.		
Topology			
Pre-Test Conditions			
1. Load balancer is properly configured with backend pool members (Server1 and Server2). 2. Servers are operational and accessible from the load balancer. 3. Load-balancing algorithm is set to the desired mode (e.g., round-robin, least connections). 4. Monitoring tools are available to track traffic distribution.			
Test Procedure		**Expected Results**	
1. From the client machine, send multiple HTTP/HTTPS requests to the load balancer's virtual IP. 2. Capture the packets at Server1 and Server2 to confirm that both servers are receiving traffic per the load-balancing algorithm. 3. Introduce a heavy load on Server1 and verify that the load balancer sends more traffic to Server2. 4. Remove the heavy load and verify if traffic distribution restores between both Server1 and Server2.		1. The Load balancer shall be able to distribute traffic dynamically between Server1 and Server2 as per configured algorithm and server availability.	

Functional Test – T3

<table>
<tr><td><b>Parameter Name</b></td><td>Persistent Session Management</td><td><b>Requirement</b></td><td>The load balancer shall ensure that a user session is consistently routed to the same backend server for the duration of the active session.</td></tr>
<tr><td><b>Objective</b></td><td colspan="3">To verify that the load balancer supports persistent session management and correctly redirects subsequent requests from the same client to the same backend server.</td></tr>
<tr><td><b>Topology</b></td><td colspan="3"> </td></tr>
<tr><td colspan="4"><b>Pre-Test Conditions</b></td></tr>
<tr><td colspan="4">1. The Load balancer is configured to use persistent session management using parameters like source IP/cookie.
2. Server1 and Server2 are hosting the same web application.
3. Client shall be able to reach both the servers through Load balancer.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2"><b>Expected Results</b></td></tr>
<tr><td colspan="2">1. Initiate a new session from the Client to the web application via the load balancer and record the session ID.
2. Send multiple subsequent requests to the web application from the same session.
3. Monitor which backend server receives the requests.
4. Simulate session changes by changing the IP address or clearing the session ID.
5. Verify if the traffic is routed to a different backend server.</td><td colspan="2">1. The Load balancer shall have mechanisms to manage persistent sessions.
2. All requests from the same session shall be consistently routed to the same backend server by the Load balancer.
3. The Load balancer shall route the traffic to a different backend server when the session changes.</td></tr>
</table>

Functional Test – T4

<table>
<tr><td><b>Parameter Name</b></td><td>SSL/TLS Offloading</td><td><b>Requirement</b></td><td>Load balancer shall be able to perform SSL/TLS offloading by decrypting the SSL/TLS encrypted traffic</td></tr>
<tr><td><b>Objective</b></td><td colspan="3">Verify if the Load balancer is able to perform SSL/TLS offloading by decrypting the SSL/TLS encrypted traffic</td></tr>
<tr><td><b>Topology</b></td><td colspan="3">
</td></tr>
<tr><td colspan="4"><b>Pre-Test Conditions</b></td></tr>
<tr><td colspan="4">1. Load balancer is configured with SSL/TLS offloading policy.
2. Web application is running on the Server.
3. Client is able to reach Server through Load balancer.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2"><b>Expected Results</b></td></tr>
<tr><td colspan="2">1. Configure a virtual IP on the Load balancer to handle SSL/TLS traffic.
2. Configure the incoming port as 443 (HTTPS) and outgoing port as 80 (HTTP) in the Load balancer.
3. Configure the backend server details which hosts the web application in the Load balancer.
4. Send HTTPS traffic from the client to virtual IP for accessing files in the backend server.</td><td colspan="2">1. Device shall receive the HTTPS traffic, decrypt and send the HTTP request to backend server.
2. Device shall receive the HTTP response, re-encrypt and send HTTPS response to client.
3. Device shall perform SSL/TLS handshake with the client.</td></tr>
</table>

ANNEXURE-II

Comments on draft for new Standard for Essential Requirements (ER) of "**Load Balancer Equipment**"

Name of Manufacturer/Stakeholder:

Organization:

Contact details:

TABLE-A: Inputs/ Comments on the technical test parameters for the Load Balancer Equipment

Clause No./ Sr. No.	**Technical Parameter Name Description**	**Comments**	**Justification/ Remarks**

TABLE-B: Inputs/ Comments for the Suggested Applicable Interfaces for the Load Balancer Equipment

Sr. No.	**Interface Name**