सत्यमेव जयते

वर्गीय आवश्यकताओं के लिए मानक
टीईसी ४९१४०:२०२५

(सं: टीईसी/जीआर/आईटी/आईपीएस-००१/०३/सितंबर-१८ को अधिक्रमित करता है)

STANDARD FOR GENERIC REQUIREMENTS
TEC 49140:2025

(Supersedes No. TEC/GR/IT/IPS-001/03/Sep-18)

इंट्रूशन प्रेवेनशन सिस्टम

Intrusion Prevention System

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नईदिल्ली–110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release 03: Feb, 2025

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

Table of Contents

History Sheet

Sl. No.	Number/Name	Description
1	GRNo.GR/IPS-01/01 NOV.2006	First edition of GR for the IPS
2**.**	TEC/GR/I/IPS-001/02 MAR 2012	Second edition of GR for the IPS
3.	TEC 49140:2025	Standard for Generic Requirements for Intrusion Prevention System (IPS)

References:

TEC GR/Standards: on EMC and NMS available on TEC website (https://tec.gov/in/standards-specifications)

S.No.	Standard No.	Standard Name
1.	QM 118, QM205, QM 206, QM 210, QM 301, QM-324	QA/ QM Standards
	QM-333, /Issues-1/Sept.1990	
	QM 351/Issue 2 / Jan' 95	
2.	802.Q	ITU Standards
	IEEE 802.1q	
3.	IEC 61000-4-2	Other Standards
	IEC 61000-4-4	
	IEC 61000-4-3	
	IEC 61000-4-5	
	IEC 61000-4-6	
4.	Class A of CISPR 32 (2015)	
	9001:2000	
5.	IS 8473 91993) (equipment & IEC publication 47-9-1 (1984))	
6.	IS 13252 (1992) (equipment & IEC publication 95(1986) & 215 (1987))	
7.	RFC 1981	

CHAPTER-1

INTRODUCTION

1.1 This document lays down the Generic Requirement (GR) of Intrusion Prevention system (IPS) used to protect the IT infrastructure of service provider (SP).

1.2 The need of network security starts with the truth that every network is insecure. There are various levels of protection of IP network such as perimeter protection, application protection, e-business protection, key server protection, policy compliance, preventing legal liability etc. Traditionally, firewall is the tool for first level or perimeter protection as it acts upon policy of accepting or denying the traffic.

1.3 The intrusion detection system (IDS) performs second level of security by monitoring all the data flowing from and into the IP network. The IDS silently reads all the data traversing the network and takes action on the basis of configured policies. This includes the reconfiguration of firewall to drop the packet/ session with attack signature, TCP reset to drop the session, etc. TEC has already laid down the generic requirement of firewall (latest TEC GR available on https://tec.gov.in/standards-specifications) and IDS (latest TEC GR available on https://tec.gov.in/standards-specifications). However for critical applications, the time taken in process identifying the attack and blocking the same through firewall, TCP reset, etc. may cause severe losses. Further it may not be possible to stop attack all the time by an off line device and also many evasion techniques exist which may even not let IDS to detect the attack offline. Hence the need of in line and stealth monitoring with capability to accept or deny the traffic emerge. The device doing these functions is called Intrusion Prevention system (IPS).

1.4 IPS MONITORS AND EVALUATES NETWORK TRAFFIC AND PROTECTS NETWORK FROM:

i. External attacks

ii. Internal attacks

iii. Network misuse

IPS is deployed at key points within network. It is usually deployed at access points of network where it works with or without firewall(s) to protect the network from unauthorized access attempts, attacks and misuse. IPSs are mostly deployed in fail-over mode and a typical deployment is shown in figure –1.

CHAPTER-2

Description of System and Architecture

2.1 Architecture - IPS shall provide the following:

i. IPS shall detect and actively prevent attacks in real-time and shall be placed in INLINE mode. It shall be possible to deploy IPS in following modes:

a) Stealth
b) Inline
c) Sniffer

ii. IPS shall be server or appliance based. Multiple such servers may be provided in load balancing mode to cater to the load as specified by SP. Load balancers shall be as per TEC latest GR **available on https://tec.gov.in/standards-specifications**).

iii. IPS shall not add delay or become a congestion point or become a central point of failure to the network being monitored.

iv. The installation of the IPS shall not require changes to the network infrastructure or affect the MTBF of the network in any way.

v. IPS shall allow working in failover mode.

vi. IPS shall provide multi segment protection with provision to have different security policies for different IP addresses/ subnets, port, VLANs & also provision for different action per segment/policy.

vii. Attack Isolation at multi-gigabit speeds, ensures the availability of mission critical even while under attack.

viii. Integrated bandwidth management and traffic shaping enables full control and optimization of application performance and SLAs.

ix. IPS devices shall block only the attack session without effecting service to legitimate clients.

x. For each attack the system shall send a complete capture of the filtered packet along with the attack event report to management station that can be used as proof of attack.

xi. IPS system shall have Centralized configuration, management & Reporting station with provision for secure communication & authentication between IPS & management station.

xii. IPS system shall be able to protect Multi Segment in the network through sensors.

xiii. It shall be able to manage and control multiple IPS sensors installed on different host/network segment).

xiv. IPS shall support architecture that allows for the capability of remotely and securely updating installed sensor base automatically.

xv. Management station shall provide extensive Attack Reporting & Forensic. IPS shall support architecture that allows the attack recognition and response modules (sensors) to be integrated into other network devices, such as firewalls and switches through standard protocol like SNMP.

xvi. IPS performance shall not reduce by enabling Layer 7 attacks filters.

xvii. Provision to install IPS system in different architecture (In-line, Sensors + manager, etc.)

xviii. IPS system shall be transparent and invisible to network

xix. IPS shall have bypass mechanism so that device can become wire on any failure. IPS shall not require external switch for bypass functionality.

xx. The IPS shall be able to get synchronized to a network time source through Network Time Protocol or simple Network Time Protocol.

xxi. Operate in Stealth Mode and be managed via out-of-band communications with IPS Console.

xxii. The IPS shall be scalable and re-configurable, and its licensing shall be such so as not to affect network expansion.

xxiii. Shall have Protocol aware ability regardless of connection port information and shall support protocols using variable port numbers.

xxiv. Provide for redundancy of management console connection

xxv. Provide Real Time, Unobtrusive Network monitoring in Promiscuous Mode

xxvi. IPS shall have Redundant, hot swappable, load sharing power supply (for category B and C only). It shall be able to operate at DC voltage of – 40 to – 57 volts.

xxvii. IPS shall protect all nodes in different LAN segments of network. It shall support the following performance figures as per the following categories:

Category	Minimum number of interfaces to be supported	Sustained throughput under attack	Concurrent TCP/UDP sessions	New sessions per second tpo be supported	Minimum number of networks segments to be protected
A	1Gbps x 2 and 100 Mbps x2	500	200,000	40,000 / second	2
B	1 Gbps x 10	2 Gbps	500,000	100,000 / second	5
C	10 Gbps x 2	5 Gbps	700,000	20,00,000 / second	10

In addition to these interfaces one 100 Mbps FE interface shall be provided for management in all categories. The above figures are indicative only. Actual interface (type and no.) shall be provided by tendering authority. For inline mode of operation, the no. of interfaces shall be double the no. of segments to be protected.

CHAPTER-3

Functional Requirement of IPS

3.1 Functional Requirement of IPS:

Functional requirement of IPS is divided into following:

a) Incident Monitoring and Detection

b) Incident Response

c) Configuration

d) Management

3.2 Incident Monitoring and Detection - IPS shall provide the following :

i. IPS shall be able to monitor the network traffic on all the LAN segment for signs of attack, unauthorized access attempts and misuse and shall be able to detect them.

ii. Protocol analysis (for protocol like FTP, HTTP, SMTP, POP3, IMAP, TELNET, P2P, IM etc.) and pattern matching shall be supported by IPS. In addition, IPS shall be able to trace and log sessions.

iii. IPS shall support pattern-based signatures having a strong sense of context, so that false alarms/incident detections are minimized.

iv. IPS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.

v. IPS shall detect incidents based on patterns in network traffic that indicate malicious intent (pattern-based signatures) and shall be able to take action on the basis of configured policies.

vi. IPS shall be able to detect incidents based on a number of occurrences over a specified period of time (frequency or threshold-based signatures) and shall be able to take action on the basis of configured policies.

vii. IPS shall be able to detect and shall be able to stop Denial of Service attacks like Smurf attack, Teardrop attack, UDP Flooding, Land attack, WinNuke attack, TFN2K, SYN attack, Stream – like DoS attack, IP/MAC spoofing etc.

viii. IPS shall be able to detect and shall be able to stop Pre-Attack Probes like various types of TCP/UDP scanners, Vertical Scanning Detection, etc.

ix. IPS shall be able to detect and shall be able to stop any Suspicious Activity.

x. Creation of User-specified signatures shall be possible based upon contents i.e. string matching etc.

xi. IPS shall be able to detect active content on the network like Java, ActiveX, etc. and shall be able to take action on the basis of configured policies.

xii. IPS shall be able to modify the application filtering logic such that it detects incidents related to a subset of the network traffic (specific IP addresses, for example).

xiii. IPS shall support signatures tuning to match the operational requirements of the customer network so that false policies are minimized.

xiv. IPS shall support help system that describes the incidents in adequate detail, providing sufficient information about:

a. The incident.

b. The potential damage.

c. Possible false positives.

d. The systems affected.

e. How to respond immediately upon detection of the incident.

f. How to remove the vulnerability associated with the incident.

xv. IPS shall be configured to focus on the incidents that pose the greatest risk to the network.

xvi. IPS shall detect the malicious activity event in fragmented and de-fragmented packets.

xvii. IPS shall provide Stateful Operation

a. TCP Reassembly

b. IP De-fragmentation

c. Bi-directional Inspection

d. Forensic Data Collection

e. Access Lists

xviii. IPS shall provide Signature Detection for at least 3500 Vendors Signature Database and 40,000 User Defined Signatures

xix. IPS shall have Anomaly Detection Mechanism for Protocol Anomalies and Sampling Based Traffic Anomalies to prevent against Day Zero or Unknown Attacks

xx. The Solution shall be capable of Correlating between Vulnerability and Intrusion Events in real-time

xxi. The IPS shall provide the capability to annotate incidents recorded in the database.

xxii. IPS shall provide Intrusion Detection & Prevention for at least following Applications:

a. Web Protection: IIS and Apache vulnerabilities, protection for web applications such as CGI, Cold Fusion, FrontPage, SQL Injection and cross-site scripting

b. Mail Server Protection: including protection from mail based worms and exploits of mail protocols (POP3, IMAP and SMTP) vulnerabilities.

c. Remote access protection: Telnet vulnerabilities and FTP server protection.

d. SNMP Vulnerability

e. Worms & Viruses

f. SQL server protection: prevention of the exploitation of vulnerabilities found in SQL implementation from miscellaneous vendors.

g. DNS protection: prevents the exploitation of vulnerabilities found in DNS implementation of various vendors.

h. Backdoor & Trojans: prevents the backdoor outbound and inbound communications, and prevent the network from being controlled remotely.

i. Brute Force Protection - prevents the password guessing attacks (brute force) in miscellaneous services.

j. SSL Encrypted Attack Protection

k. Protection against Mass mailing worm and viruses

xxiii. IPS shall provide full Application Security Intelligence including:

a. IP spoofing protection

b. DoS and DDOS protection

c. Protocol Anomaly protection

d. Traffic Anomaly Protection

e. TCP Reassembly, normalization and de-fragmentation

f. Syn flood protection

g. Backdoor /Bi-directional inspection for attack traffic.

h. Stateful signature inspection

xxiv. IPS Shall Protect against various DOS & DDOS attacks as follows:

a. One Packet Attack Protection

b. Protection against TCP, UDP & ICMP Flood

c. SYN Flood

d. Layer 2 attacks such as DHCP Flooding prevention

xxv. IPS shall have provision to protect evasion techniques as prevention against SSL encapsulated attack using internal or external Add-On hardware with provision to add this feature/HW at later stage.

3.3 Incident Response - IPS shall provide the following:

i. IPS shall be able to send alarms to the management console, or to multiple management consoles, upon detection of an incident.

ii. IPS shall be able to send an SNMP trap to the network or system's management console upon detection of an incident.

iii. IPS shall support native integration with popular Network Management Systems through SNMPv3 and latest updates.

iv. IPS shall be able to notify an administrator via e-mail of an incident or attack or misuse on pre-defined email ids.

v. IPS shall be able to log a summary of an incident to persistent data storage.

vi. The IPS shall be able to record relevant data from a packet based on the attack signature and write it to persistent data storage for future analysis or evidence.

vii. The IPS is able to copy the relevant data of an attack to the management console while automatically stopping the attack so that it may be viewed as it is happening.

viii. IPS shall be able to terminate a TCP/UDP session upon detection of malicious activity. IPS shall be capable to kill intrusion attempts.

ix. Shall detect attack due to URL decoding vulnerabilities.

x. IPS shall also be able to respond to an incident by executing one or more user-specified programs. These can be batch files, command line scripts, executables, etc.

xi. IPS shall be capable of attack response customization.

xii. IPS shall be able to filter unwanted events, protocol etc.

xiii. IPS shall provide security event section replay.

xiv. IPS active response shall also include the execution of user defined programs.

xv. IPS shall be capable of:

   a. Block attacks in real time

   b. Drop Attack Packets

   c. Reset/ drop Connections

   d. Packet Logging

xvi. IPS shall provide following passive TCP reset responses:

   a. Close client

   b. Close server

   c. Close connection

xvii. IPS shall be capable of Attack Isolation:

a. Access Control of traffic per application ports and networks allows a predefined set of applications only and denies all other types of traffic.

b. Attack isolation and protection against unknown flooding attacks.

c. Dynamic Bandwidth Borrowing – optional.

d. Guarantee Bandwidth for critical Application- optional.

e. Traffic shaping, including bandwidth per traffic flow, which allows limiting bandwidth per client or session within a global Band Width Mgt. policy – optional.

f. Limit Bandwidth per Application- optional.

g. PPP limit per session- optional.

h. Layer 2- 7 Traffic classification & BW shaping with provision for BW sharing between policies- optional.

3.4 Configuration - IPS shall provide the following:

i. Remote IPS (IPS not connected with management console on the same LAN) and sensors shall support applications that shall be configured from the management console using a point-and click-interface.

ii. IPS shall support configuration templates that describe an application configuration (i.e., active pre-defined signatures, and responses etc.). These templates shall be customizable, applied to many applications at the same time, saved for future use, and exchanged among management domains.

iii. IPS shall support help system providing a detailed description of the attack signature that is selected.

iv. The priority level (evaluation criteria of rules shall be specifiable) for each pre-defined signature shall be configurable from the management console.

v. The interface shall allow attack signatures to be activated or deactivated via check-box selection.

vi. The administrator, from the management console, shall be able to specify the response to each pre-defined event.

vii. The administrator from the management console shall be able to specify multiple responses to each attack or misuse.

viii. IPS shall be able to tune the pre-defined signatures in such a way that the false alarms/incident detections are minimized. Shall provide capability to filter out false positives once they have been identified as such.

ix. IPS shall be capable to tune event propagation.

x. IPS shall be able to be configured such that attack signature and traffic analysis focus only on specified hosts, specified protocols, or specified services.

xi. It shall be possible to specify New Services (as defined by TCP/IP port number) by the administrator. New attack signatures shall then be based upon that new, user-defined Service.

xii. IPS shall be capable of attack policy customization.

xiii. IPS shall have provision to analyse and identify the ingress point of attack.

3.5 Management Console - IPS shall provide the following:

IPS shall support Management Console to receive inputs, information and alarms from all the sensors/ IPS on different LAN segment connected to the console. The console shall be able to manage the sensors and sensors configurations, remotely upgrade the sensors, collect data from the sensors, and generate reports on network activity.

i. It shall be possible to monitor events from any IPS, from a single, authorized management console and any IPS shall be able to report attack and misuse of data to multiple management consoles simultaneously.

ii. The management console shall provide depository of software packages for downloading/updating of the IPS software centrally.

iii. The management console shall have in-built facilities for remote installation of IPS Modules and Components.

iv. The management console of the Solution shall be well integrated to all IPS/sensors and shall be a single vendor solution.

v. Shall allow for the separation and delegation of security administrative tasks to different, specified individuals through role-based administration

vi. It shall support SNMP v3 .

vii. Provide customizable features such as Detection Rules, Reports, Encryption Options, Alerts, and Responses via the IPS Management interface

viii. The console shall also provide the following dynamic sensors management capabilities:

a. Start/stop monitoring.

b. Start/stop managing.

c. Acquire/release/revoke master control.

d. Start/resume/shutdown/pause operations.

e. Apply or uninstall updates to IPS software/attack signatures.

f. Add/remove/change encryption providers/keys.

g. Apply active responses in Real Time.

h. Apply policies.

ix. Management console shall support following for access :

a. HTTP, HTTPS

b. SSH

c. Telnet

3.6 IPS Management console shall provide Graphical User Interface (GUI) as follows:

i. IPS shall be able to graphically depict both suspicious activity and normal network activity.

ii. The graphical interface shall be easy to use for by operators and shall require no special technical knowledge.

iii. The graphical interface shall use an iconic display to alert operators to important occurrences.

iv. The graphical interface shall be able to display summary information sorted by source address (initiator), destination address (target), or event type.

v. The graphical interface shall support a "drill down" mechanism so that the operator may obtain additional information about an event. This information includes action(s) that were taken by IPS in response to the event.

vi. The graphical interface shall be able to consolidate multiple event occurrences into a single alarm.

3.7 Management - IPS shall provide the following:

i. IPS shall have comprehensive database with more than 1500 attack signatures.

ii. It shall be possible to adopt data from many IPS applications on a single management console. This includes event summary data as well as the binary content of logged sessions.

iii. Data on the management console shall be stored in an RDBMS database.

iv. It shall be possible to export the ODBC database to another database or to a delineated text file.

v. The database structure shall be completely open.

vi. IPS shall support data management capabilities provide critical information required for risk assessment and decision-making.

vii. IPS shall be capable of prioritization of security event data for quick and easy threat assessment.

viii. The IPS shall be complete in all respects including database signature files and shall be integrated and out of the box without any inter-dependency on any other 3rd party software for its functioning

3.8 Report management - IPS shall provide the following:

i. IPS shall have built-in customized report generation capability e.g. excel, text, HTML, etc., as per SP's requirement which shall be specified at the time of tendering.

ii. It shall be possible to generate templates for the pre-defined reports, so that custom reports can be generated using the standards reports as a starting point.

iii. It shall be possible to generate multiple forms of reporting suitable for all technical levels.

iv. IPS shall support reports that shall be configurable and customizable using third party tools if required.

v. IPS shall support reports that may be exported to different formats, such as excel, HTML or a Word document etc.

vi. Provision for structured reporting to reduce security events messages floods when the device is under attack. Instead of sending an event per each security event, the device shall send an event within a pre-defined reporting period.

vii. IPS shall provide drill down reports based on Real Time attack statistics for following:

a. Security event risk level.

b. Date/time.

c. Subnets (Networks/ IP Address)

d. Event name.

e. Source IP.

f. Destination IP.

g. Response taken.

h. Sensor identity.

i. Severity.

j. Top attack types

k. Attack groups

l. Top-10 Source of Attacks

m. Top-10 Destination of attacks

n. IPS login details

o. Identity based reporting for period of activity (similar to source/ destination/ username)

It shall be possible to have above statistics for complete IPS or Port Group or individual port on IPS.

viii. User shall be able to customize Reports

ix. Management station shall be able to show Graph with number of attacks coming from different networks

x. Provision to automatically generate & email reports daily, weekly or monthly to predefined email addresses.

xi. Provide reports in different formats like excel sheet, Word, HTML etc.

xii. IPS shall provide alerts/ notify by following:

   a. SNMP trap
   b. Logging
   c. Syslog
   d. E-mail
   e. Script
   f. Message on IPS user interface

CHAPTER-4

Quality Requirements

4.1 **Qualitative Requirement (QR):** The IPS shall meet the following qualitative requirements:

4.1.1 The manufacturer shall furnish the MTBF value. Minimum value of MTBF shall be specified by the purchaser. The calculations shall be based on the guidelines given in either QA document No. QM-115 {January 1997} "Reliability Methods and Predictions" or any other international standards.

4.1.2 The equipment shall be manufactured in accordance with international quality management system ISO 9001:2015 or any other equivalent ISO certificate for which the manufacturer should be duly accredited. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted.

4.1.3 The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue-March, 2010} (TEC 14016:2010) "Standard for Environmental testing of Telecommunication Equipment" or any other equivalent international standard, for operation, transportation and storage. The applicable environmental category A or B to be decided by the purchaser based on the use case.

CHAPTER-5

EMC/EMI Requirements

5.1 Electromagnetic Compatibility (EMC):

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished:-

a) Conducted and radiated emission (applicable to telecom equipment):

Name of EMC Standard: “CISPR 32 (2015) with amendments - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits:-

i) To comply with Class B of CISPR 32 (2015) with amendments for indoor deployments and Class A of CISPR 32 (2015) with amendments with amendments for outdoor deployments.

b) Immunity to Electrostatic discharge:

Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits:-

i) Contact discharge level 2 {± 4 kV} or higher voltage;

ii) Air discharge level 3 {± 8 kV} or higher voltage;

c) Immunity to radiated RF:

Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test".

Limits:-

For Telecom Equipment and Telecom Terminal Equipment without Voice interface (s)

Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):

Name of EMC Standard: IEC 61000-4-4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test".

Limits:-

Test Level 2 i.e.

a) 1 kV for AC/DC power lines;

b) 0. 5 kV for signal / control / data / telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test".

Limits:-

i) For mains power input ports : (a) 2 kV peak open circuit voltage for line to ground coupling (b) 1 kV peak open circuit voltage for line to line coupling

ii) For telecom ports : (a) 2kV peak open circuit voltage for line to ground (b) 2KV peak open circuit voltage for line to line coupling.

f) Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2013) with amendments) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields”.

Limits:-

Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: IEC 61000-4-11 (2004) “Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests”.

Limits:-

i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500 ms)

ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and

iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

iv) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10s.

h) Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):

Name of EMC Standard: IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests.

Limits:-

i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B.

ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C.

iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B.

iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C.

v. Voltage variations corresponding to 80% and 120%of supply for 100 ms to10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B.

Note: - For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16 (TEC 11016:2016) and the referenced base standards i.e. IEC and CISPR standards and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (h) and TEC Standard TEC/SD/DD/EMC-221/05/OCT-16 (TEC 11016:2016). The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 11	EN 55011
CISPR 32	EN55032
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11
IEC 61000-4-29	EN 61000-4-29

CHAPTER-6

Safety Requirements

6.1 Safety Requirements:

The equipment shall conform to relevant safety requirements as per IS/IEC 62368-1:2018 or Latest as prescribed under Table no. 1 of the TEC document ‘SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT”: TEC10009: 2024. The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements.

i.

CHAPTER-7

Security Requirements

7.1 Security - IPS shall provide the following:

i. IPS shall support separate communications channels for control data and for event data.

ii. These communications channels shall use TCP/ UDP, connection oriented, and use ports that can be specified by the network administrator, allowing for simple passage through firewalls.

iii. Communication among IPS components shall be authenticated/ encrypted with standards such as AES 256, 1536 bit RSA etc.

iv. The IPS shall support stealth mode, so that the IPS existence on the monitored network shall not be known to any device except the sensors installed on the network devices.

v. The IPS shall be able to protect itself against attacks and shall not use any service/functionality/feature on the host that might make it vulnerable to attack.

vi. The IPS shall monitor its internal application modules and notify the management station when a module goes off line unexpectedly.

vii. IPS shall be capable of using out-of-band communications for its communications channels.

viii. The IPS and management console shall be protected against intentional or accidental abuse, unauthorized access and loss of communication.

ix. The IPS and management console security features shall include operator authentication, command, menu restriction and operator privileges. The management console shall support four level passwords.

x. Management console must enable the System administrator to define the level of access to the network capabilities or features for each assigned password. The management console shall block the access to the operator in case of unauthorized commands being tried for five times. The management console shall also not allow the entry into the management console in case wrong password is provided more than three times during the login.

xi. The supervisor shall be able to monitor and log all operator activities in the management console(s).

xii. The dynamic password facility shall be provided in which the Operator may change his password at any time.

xiii. The management console shall have the feature of idle time disconnection.

xiv. The man-machine communication programs shall have the facility of restricting the use of certain commands or procedures to certain passwords and terminals

xv. IPS shall be certified for the features described in this document by any one of the following:

a. Tolly
b. ICSA
c. FIPS
d. OPSEC
e. NIST
f. NSS

7.2 Performance - IPS shall provide the following:

i. IPS shall support applications that can monitor network traffic and take action autonomously, without a console running.

ii. IPS shall process network traffic at a rate that does not add delay, or becomes a congestion point while attack signatures active. For 1 Gbps of throughput, the delay shall not be more than 500 µs.

iii. IPS shall support performance that scales well with the number of attack signatures and filters active. Increasing the number of predefined or custom signatures shall not impact the performance of the system.

iv. IPS shall handle traffic bursts gracefully, switching to sampling mode until the traffic levels return to a consistent level.

7.3 Updates - IPS shall provide the following:

i. The IPS software and its attack signature database shall be updated at least once in a month.

ii. Update attack signatures, rule bases and service releases via the Internet or with Version Upgrades

iii. It shall be possible to download and update new attack signatures and major software releases from the Web in addition to local update from the management console.

iv. It shall be possible to update IPS remotely and securely with new signature (Pattern of DoS Attack, pattern for hacking attempts using a particular hacking software etc.) updates or full IPS software update.

v. IPS Shall support 24/7 Security Update Service

vi. IPS Shall support Real Time signature update

vii. IPS shall support for customized signatures.

viii. IPS Shall support Automatic signature synchronization from database server on Internet.

ix. The IPS shall provide for regular updates to the signature database and also update the changes on the sensors that are spread across the network from one central place.

CHAPTER -8

Other Mandatory Requirements

8.1 **Engineering Requirements**: The IPS shall meet the following engineering requirements:

a) The equipment shall be fully solid state and adopt state of the art technology.

b) The equipment shall be compact, composite construction and lightweight. The manufacturer shall furnish the actual dimensions and weight of the equipment.

c) All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations.

d) All LAN cabling shall be of Gigabit Ethernet ready.

e) The equipment shall have adequate cooling arrangements.

f) Each sub-assembly shall be clearly marked with schematic reference to show its function, so that it is identifiable from the layout diagram in the handbook.

g) Each terminal block and individual tags shall be numbered suitably with clear identification code and shall correspond to the associated wiring drawings.

h) All controls, switches, indicators etc. shall be clearly marked to show their circuit diagrams and functions.

i) It shall be possible to block only user selected malicious traffic as required.

j) System should be able to detect attacks within encrypted network traffic VPN connections, HTTP over SSL (HTTPS) and SSH sessions.

8.2 **Operational Requirement (OR):** The IPS shall meet the following Maintenance & operational requirements:

i. The equipment shall be designed for continuous operation.

ii. The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sea level.

iii. Suitable visual indications shall be provided to indicate healthy and unhealthy conditions.

iv. The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.

v. The removal or addition of any cards shall not disrupt traffic on other cards.

vi. All mission critical modules shall be identified and provided in full redundant configuration for high reliability.

vii. A single point failure on the equipment shall not result in network or network management system downtime.

viii. Special tools required for wiring shall be provided along with the equipment.

ix. In the event of a bug found in the software, the manufacturer shall provide patches and firmware replacement if involved, free of cost. Compatibility of the existing hardware shall be maintained with future software/firmware.

x. In the event of a full system failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.

xi. Multi vendor, Multi application environment shall be supported by IPS.

xii. A power down condition shall not cause loss of connection configuration data storage.

xiii. Live Insertion and hot swap of modules shall be possible to ensure maximum network availability and easy maintainability.

xiv. The Hardware and software components shall not pose any problems in the normal functioning of all network elements wherever interfacing with service provider network for voice, data and transmission systems, as the case may be.

8.3 The system hardware and software shall not pose any problem, due to changes in date and time caused by events such as changeover of millennium / century, leap year etc., in the normal functioning of the system.

8.4 Wherever, the standardized documents like ITU-T, IETF, QA and TEC documents are referred, the latest issue and number with the amendments shall be applicable.

8.5 Power Supply: The equipment power supply requirements are given for each of the category. In addition, it shall meet the following requirements:

(i) The equipment shall be able to function over the range specified in the respective chapters, without any degradation in performance.

(ii) The equipment shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity.

(iii) The derived DC voltages shall have protection against short circuit and overload.

8.6 **System description documents**: The following system description documents shall be supplied along with the system.

i) Over-all system specification and description of hardware and software.

ii) Equipment layout drawings.

iii) Cabling and wiring diagrams.

iv) Schematic drawings of all circuits in the system with timing diagrams wherever necessary.

v) Detailed specification and description of all Input / Output devices

vi) Adjustment procedures, if there are any field adjustable units.

vii) Spare parts catalogue - including information on individual component values, tolerances, etc. enabling procurement from alternative sources.

viii) Detailed description of software describing the principles, functions, and interactions with hardware, structure of the program and data.

ix) Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data.

x) Program and data listings.

xi) Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification.

8.7 **System operation documents**: The following system operation documents shall be available.

i) Installation manuals and testing procedures.

ii) Precautions for installation, operations and maintenance

iii) Operating and Maintenance manual of the system.

iv) Safety measures to be observed in handling the equipment

v) Man-machine language manual.

vi) Fault location and trouble shooting instructions including fault dictionary.

vii) Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement.

viii) Emergency action procedures and alarm dictionary.

8.8 Training Documents

i) Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available.

ii) Any provisional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be provided immediately following the issue of such updates.

iii) The structure and scope of each document shall be clearly described.

iv) All diagrams, illustrations and tables shall be consistent with the relevant text.

v) The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.

8.9 Repair Manual

i) List of replaceable parts used

ii) Detailed ordering information for all the replaceable parts

iii) Procedure for trouble shooting and sub-assembly replacement

iv) Test fixtures and accessories for repair

v) Systematic trouble shooting charts (fault tree) for all the probable faults with their remedial actions.

CHAPTER -9

Desirable Requirements

9.1 Installation

i) All necessary interfaces, connectors, connecting cables and accessories required for satisfactory installation and convenient operations shall be supplied. Type of connectors, adopters to be used shall be in conformity with the interfaces defined in this GR.

ii) It shall be ensured that all testers, tools and support required for carrying out the stage by stage testing of the equipment before final commissioning of the network shall be supplied along with the equipment.

iii) All installation materials, consumables and spare parts to be supplied.

iv) All literature and instructions required for installation of the equipment, testing and bringing it to service shall be made available in English language.

v) For the installations to be carried out by the supplier, the time frames shall be furnished by the supplier including the important milestones of the installation process well before commencing the installations.

vi) The equipment shall have:

a) Proper earthing arrangement,

b) Protection against short circuit / open circuit

c) Protection against accidental operations for all switches / controls provided in the front panel.

d) Protection against entry of dust, insects and lizards.

9.2 Software Maintenance:

i. All the software updates shall be provided on continuous basis.

ii. The software for the support of all protocols and interfaces mentioned in this GR shall be ensured in the devices.

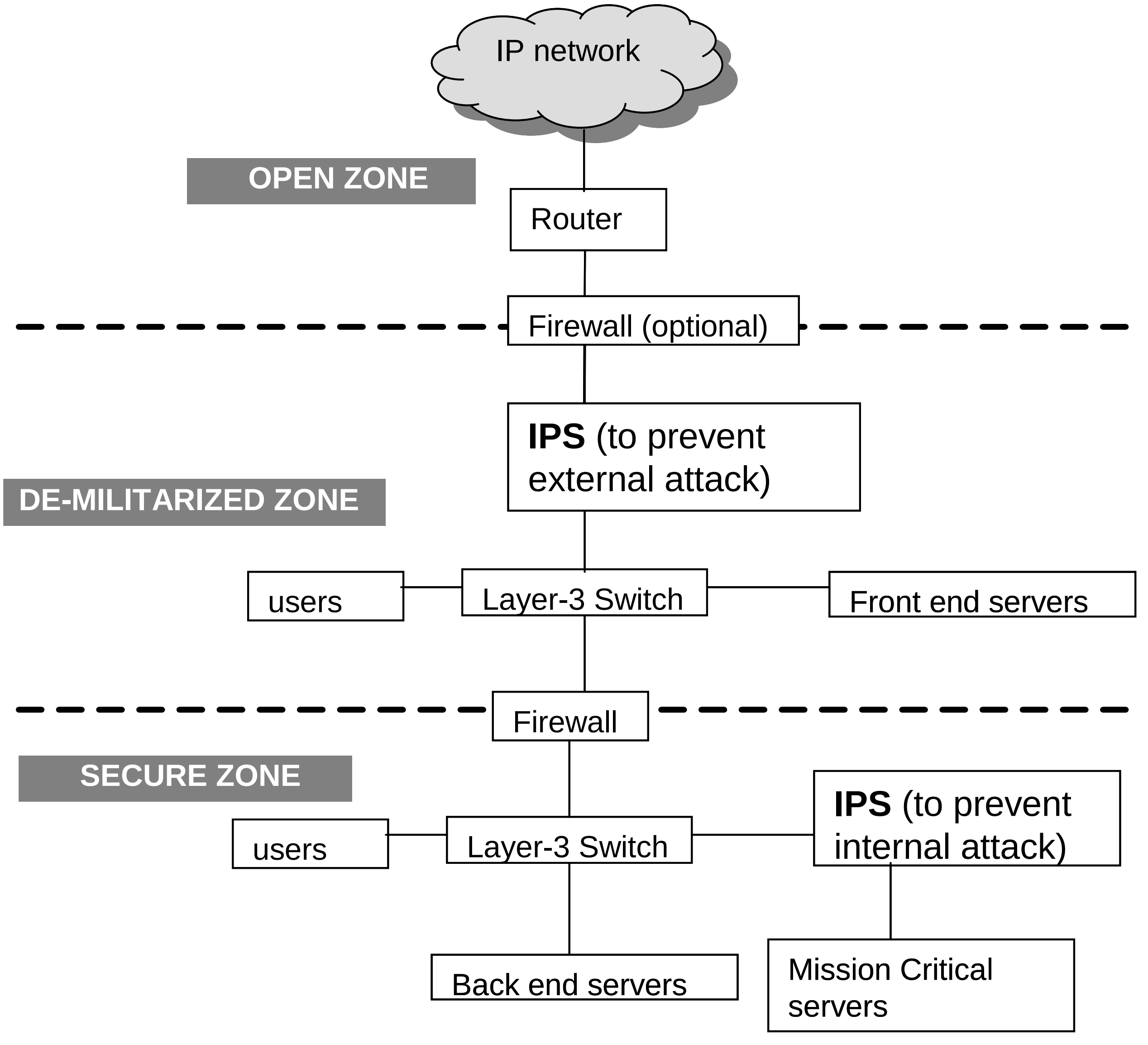

Figure 1: Intrusion Prevention system (IPS) deployment

Glossary

BSNL	:	Bharat Sanchar Nigam Limited
CA	:	Certification Authority
CPU	:	Central Processing Unit
DES	:	Data Encryption Standard
3DES	:	triple DES
DNS	:	Domain Name Server
EIA	:	Electronic Industries Association
EMC	:	Electromagnetic Compatibility
EMS	:	Enterprise management system
FTP	:	File Transfer Protocol
HDCP	:	High bandwidth Digital Content Protection
HTTP	:	Hypertext Transfer Protocol
ICSA	:	International Computer Security Association
ICMP	:	Internet Control Message Protocol
IEEE Engineers	:	Institute of Electrical and Electronics
IKE	:	Internet Key Exchange protocol
IETF	:	Internet Engineering Task Force
IMAP	:	Internet Message Access Protocol
IP	:	Internet Protocol
IPv6	:	Internet Protocol version 6
IPSec	:	IP Security Protocols
ITU	:	International Telecommunication Union
ITU-T	:	Telecommunication Standardization Sector of ITU
LAN	:	Local area network
MIB	:	Management Information Base
MTNL	:	Mahanagar Telephone Nigam Limited
MTBF	:	Mean Time between Failure
MTTR	:	Mean Time To Restore
NAT	:	Network Address Translator
NMS	:	Network Management System
OS	:	Operating system
PC	:	Personal Computer

POP	:	Post Office Protocol
PSTN	:	Public switched Telephone Network
RADIUS	:	Remote Authentication Dial-In User Service
RFC	:	Request for Comments
SIP	:	Session Initiated Protocol
SMTP	:	Simple Mail Transfer Protocol
SNMP	:	Simple network management protocol
SSH	:	Site Security Handbook
TCP	:	Transmission control protocol
TCP/IP protocol	:	Transmission control protocol/Internet
TIA	:	Telecommunications Industries Association
TFTP	:	Trivial File Transfer Protocol
UDP	:	User Datagram Protocol
VLAN	:	Virtual Local Area Network
VPN	:	Virtual Private Network
WWW	:	World Wide Web