सत्यमेव जयते

वर्गीय आवश्यकताओं के लिए मानक

टीईसी 49130:2023

(सं: टीईसी/जीआर/आईटी/आईडीएस-001/04/सितम्बर-18 को अधिक्रमित करता है)

STANDARD FOR GENERIC REQUIREMENTS
TEC 49130:2023

(Supersedes No.TEC/GR/IT/IDS-001/04/SEP-18)

आई पी नेटवर्क सुरक्षा के लिए इंटरुजन डिटेक्शन सिस्टम

Intrusion Detection System for IP Network Security

ISO 9001:2015

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

Release: May, 2023

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.

ABSTRACT

This Standard for Generic Requirements for Intrusion Detection System for IP network security is used to protect the IT infrastructure of any organisation.

CONTENTS

Chapters

HISTORY SHEET

S. No.	***GR No.***	***Title***	***Remarks***
1.	GR No. GR/IDS-01/01 FEB 2003	Generic Requirement for Intrusion Detection System	First edition of GR for Intrusion Detection System for IP Network Security
2.	GR No. GR/IDS-01/02 OCT 2007	Generic Requirement for Intrusion Detection System	Second edition with technological updates
3.	GR No. TEC/GR/I/IDS-001/ 03. MAR 2011	Generic Requirement for Intrusion Detection System for IP Network System	Third edition with technological updates
4.	TEC/GR/IT/IDS-001/04/SEP-18	Generic Requirement for Intrusion Detection System for IP Network System	Fourth edition with technological updates
5.	TEC 49130:2023	Standard for Generic Requirements for Intrusion Detection System for IP Network Security	5th edition with inclusion of Virtual / Cloud based IDS

REFERENCES

Sl. No.	*Document No.*	*Title/Document Name*
1.	TEC/SD/DD/EMC-221/05.OCT 2016	EMI/EMC Standards
2.	TEC/GR/IT/LSW-002/03/MAR-2015	Load Balancer
3.	QM 118, QM205, QM 206, QM 210, QM 301, QM-324, QM 351	Quality Manual issued by the QA Circle
4.	QM-333	Standards on Environmental Testing for Telecom Equipment
5.	IEC/EN 61000-4-2	Testing and measurement techniques – Electrostatic discharge immunity test
6.	IEC/EN 61000-4-3	Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
7.	IEC/EN 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test
8.	IEC/EN 61000-4-5	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test
9.	IEC/EN 61000-4-6	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields
10.	IEC/EN 61000-4-11	Electromagnetic compatibility (EMC) - Part 4-11: Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests".
11.	EN 55011	Industrial, scientific and medical (ISM) radio-frequency equipment - Electromagnetic disturbance characteristics - Limits and methods of measurement
12.	EN 55022	Information Technology Equipment - Radio disturbance characteristics - Limits and methods of measurement
13.	ISO 9002 or 9001:2000	Series of standards, developed and published by the International Organization for Standardization (ISO), that define, establish, and

		maintain an effective quality assurance system for manufacturing and service industries
14.	IS 8473 (latest) (equipment & IEC publication 479-1)	Information technology -- Protocol for providing the connectionless-mode network service -- Part 2: Provision of the underlying service by an ISO/IEC 8802 subnetwork
15.	IS 13252 (equipment & IEC publication 95 & 215)	Information Technology Equipment -- Safety, Part 1: General Requirements
16.	Class A of CISPR 11	Limits and methods of measurement of radio disturbance characteristics of industrial, scientific & medical (ISM) radiofrequency equipment
17.	Class A of CISPR 22/ 32	Limits and methods of measurement of radio disturbance characteristics of ITE
18.	RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
19.	RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
20.	RFC 3413	Simple Network Management Protocol (SNMP) Applications
21.	RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

CHAPTER 1

1. INTRODUCTION

1.1 This document lays down the Generic Requirement (GR) of Intrusion Detection system (IDS) used to protect the IT infrastructure of any organisation. As per security policy, Intrusion Detection System shall be deployed at key points within Service Provider IP based network. IDS shall be hardware based or virtual/cloud based.

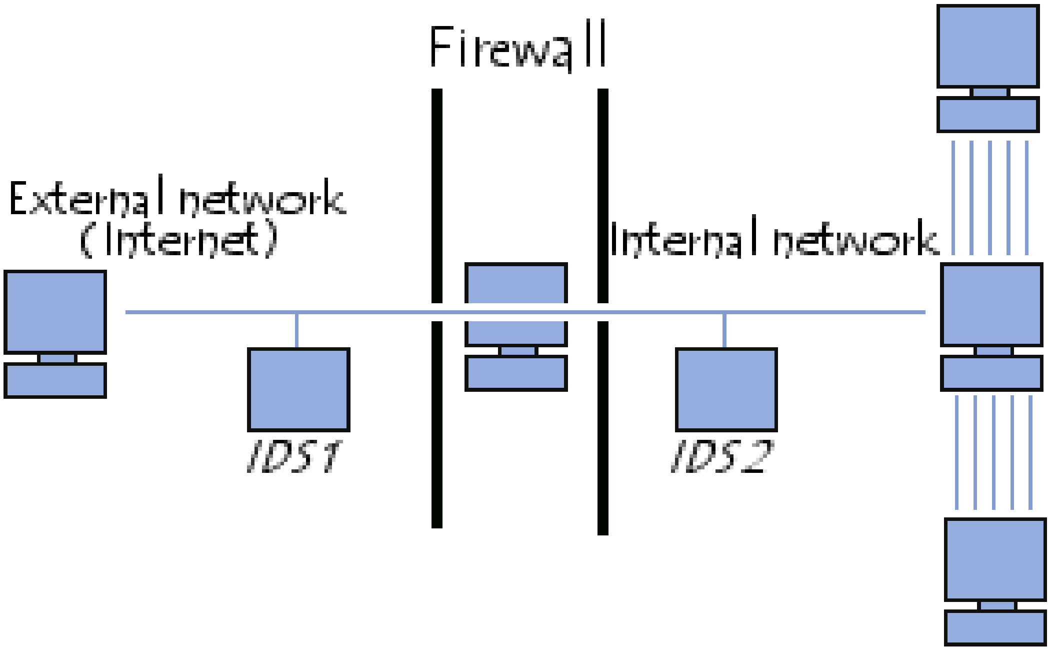

Fig1: Typical Deployment of IDS in a Network

1.2 Network-based Intrusion Detection System monitors and evaluates network traffic for two types of problems:

a. Attacks, either from outside or inside the network
b. Network misuse as per security policy.

1.3 Network-based Intrusion Detection is deployed at key points within network. It is usually deployed at access points of network where it works with firewall(s) to protect the network from unauthorized access attempts, attacks and misuse. Strategic deployment of IDS shall also include installing sensors (software which detect any attempt based on configured policy) in crucial LAN and WAN segments because application part of IDS (Engines) resides on one or a few dedicated hosts (machines on LAN with separate IP address) and is used to monitor all network segments. IDS host(s) is (are) mostly deployed in fail-over mode.

CHAPTER – 2

2. **Description**

2.1 The need for 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. Firewall is the tool for first level or perimeter protection as it acts upon policy of accepting or denying the traffic. The second level of security checks the allowed traffic, which is flowing through the network. There are certain types of attacks and network or system misuse that can be most easily discovered by monitoring the network traffic.

2.2 The IDS is a part of second level of security system designed to monitor all the data flowing from and into the IP network which could be an intranet or any network. The IDS is typically used along with the LAN Switch, which is configured to mirror all the data from all the ports to the port where IDS is connected. The IDS silently reads all the data traversing the network and takes action on the basis of configured policies. Intrusion Detection System monitors and evaluates network traffic and protects network from:

a. External attacks
b. Internal attacks
c. Network misuse

CHAPTER – 3

3. Functional Requirements:

3.1 Intrusion Detection system (IDS) shall support the following features:

a. Architecture(for hardware based IDS)
b. Management Consoles.
c. Graphical User Interface.
d. Incident Monitoring and Detection.
e. Incident Response.
f. Configuration.
g. Data Management.
h. Report management.
i. Security.
j. Performance.
k. Updates and Technical Support.

3.2 Architecture

i. IDS shall protect all nodes in different LAN segments of network. It shall support the performance figures as per the following categories, based on the number & type of the interfaces and the throughput capacity. The purchaser may opt for any of these categories depending on their requirement:

Category	Minimum no of interfaces to be supported	IDS/IPS Throughput	Firewall Concurrent TCP /UDP sessions	Minimum number of networks segments to be protected
A	4 x 1GE	500 Mbps	200,000	1/10
B	2 x 10GE and 8 x 1GE	2 Gbps	500,000	2/20
C	4 x 10GE and 2 x 1GE	10 Gbps	700,000	5/100
D	2 x 100GE and 2 x 10GE	50 Gbps	700,000	5/100
E	4 x 100GE and 2 x 10GE	100 Gbps	700,000	5/100

In addition to these interfaces 2 * 1000 Mbps GE interface shall be provided for management in all categories.

ii. IDS shall be based on a hardened standard operating system and should be made available with latest version.

iii. IDS shall fully support 10/100/1000 Base-T and optical Gigabit Ethernet Interfaces for hardware based IDS. The exact requirement shall be specified by the purchaser.

iv. The IDS should be supported as an integrated hardware or module within the Firewall Appliance for seamless integration (Optional).

v. Ordinarily, IDS shall not neither add delay nor become a congestion point. Purchaser may specify the acceptable delay.

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

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

viii. It shall be able to manage and control multiple IDS sensors installed on different host/network segment via a central manager.

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

x. IDS shall support Active-Active or Active-Standby configuration deployments. IDS shall not become a single point of failure to the network.

xi. IDS shall support architecture that adapts well to higher network speeds and switched network topologies.

xii. IDS shall support attack recognition and response modules to be integrated into other network devices, such as firewalls, switches etc.

xiii. It shall have the capability of defining virtualized IDS/IPS sensors based on physical interface and VLAN group.

xiv. IDS shall support the capability of remotely and securely updating installed sensor base automatically.

xv. IDS shall be server or appliance based. For server/appliances based IDS, multiple such servers may be provided along with external load balancer to balance the load as specified by the Purchaser. The Load balancers shall be as per TEC GR (TEC/GR/IT/LSW-002/03/MAR-2015).

xvi. IDS 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.

xvii. 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.

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

xix. IDS system shall be able to protect all Segments in the network that are behind the IPS/IDS.

xx. Should support online signature updates 24 hours a day to help ensure protection against the latest threats.

xxi. It shall be able to manage and control multiple IDS systems installed on different host/network segment.

xxii. Shall support Global Correlation which provides real-time updates on the global threat environment beyond system perimeter by adding reputation analysis, reducing the window of threat exposure, and providing continuous feedback.

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

xxiv. Management station shall provide extensive Attack Reporting & Forensic data. IDS 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 V2c or SNMP V3.

xxv. The IDS shall be able to get synchronized to a network time source through Network Time Protocol V4 or simple Network Time Protocol.

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

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

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

xxix. The hardware based IDS shall have Redundant, hot swappable, load sharing Power Supply. It shall be able to operate at a nominal power supply of -48 volts DC, with a variation over the range -44V to -57V. For equipment requiring AC mains, nominal AC voltage for single phase be 230V with a variation of -15% to 10% at 50+- 2 Hz without any degradation in the performance. Purchaser shall specify the exact power requirements.

3.3 Management Consoles

3.3.1 IDS shall support Management Console to receive inputs, information and alarms from all the sensors (Network and Host based) 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. The console shall also provide the following sensors management capabilities:

i. Start/stop monitoring.
ii. Start/stop managing.
iii. Acquire/release/revoke master control.
iv. Start/resume/shutdown/pause operations.
v. Apply or uninstall updates to IDS software/attack signatures.
vi. Apply active responses.
vii. Apply policies.

3.3.2 Further it shall be possible to monitor events from any IDS, from a single, authorized management console and any IDS shall be able to report attack and misuse of data to multiple management consoles simultaneously. Management console shall support following for access:

a. HTTP, HTTPS

b. SSH

c. Telnet

d. SSL

3.4 Graphical User Interface

i. IDS 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 IDS in response to the event.

vi. IDS shall consolidate related event occurrences into a single alarm. The graphical interface shall be able to display the same.

3.5 Incident Monitoring and Detection

i. IDS shall 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. The IDS/IPS should support syslog/SDEE for logging events.

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

iv. IDS 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. Should support IPv4, IPv6, and hybrid IPv6 and IPv4 networks.

vi. Tunnelling Protocol Detection Support for GRE, IP-in-IP, MPLS.

vii. IDS 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.

viii. IDS 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.

ix. Application inspection control of HTTP, port 80 misuse/application tunnelling, FTP, mime type detection/filtering. DHCP, DNS, FTP, file sharing (peer-to-peer, Finger, HTTP, HTTPS, IMAP, Ident, LPR, NNTP, NTP, POP, R-Services, RPC, MSRPC, SMTP, SNMP, SOCKS, SQL, SSH, Telnet TFTP, H.323, H.225, WINS, MSSQL, IRC, LDAP, SMB, TNS, and anomaly-based day-zero scanning worm protection.

x. IDS shall be able to detect 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.

xi. IDS shall be able to detect Pre-Attack Probes like various types of TCP/UDP scanners.

xii. IDS shall be able to detect Suspicious Activity.

xiii. Creation of User-specified signatures, including the signatures created through the use of biometric devices, and their matching (e.g. string matching) shall be possible.

xiv. IDS 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.

xv. IDS 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).

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

xvii. IDS 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.

g. Common Vulnerability and Exposure (Optional for purchaser)

xviii. IDS shall be configured to focus on the incidents that pose the greatest risk to the network.

xix. IDS shall detect the malicious activity event in fragmented and defragmented packets.

xx. IDS shall provide Stateful / real-time inspection of

a. TCP Reassembly

b. IP De-fragmentation

c. Bi-directional Inspection

d. Forensic Data Collection

e. Access Lists

xxi. IDS shall provide Signature Detection for at least 3500 Vendors Signature Database The support for user defined signatures shall be as per purchaser requirement.

xxii. IDS shall have An**o**maly Detection Mechanism for Protocol Anomalies and Sampling Based Traffic Anomalies to prevent against Day Zero or Unknown Attacks.

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

xxiv. The IDS shall provide the capability to annotate incidents recorded in the database. IDS 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/TLS Encrypted Attack Protection such as TCP SYN Floods, SSL Negotiation Floods, HTTPS Floods.

k) Protection against Mass mailing worm and viruses

xxv. IDS 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

xxvi. IDS Shall Detect/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

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

xxviii. IPS should be able to rate limit traffic based on source/destination IP address and source/destination port numbers. Should also be able to determine host operating system by inspecting characteristics of the packets exchanged in the network.

3.6 Incident Response

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

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

iii. IDS shall support native integration with popular Network Management Systems through SNMP V3 so that NMS is able to take corrective action automatically.

iv. IDS shall be able to notify an administrator via e-mail of an incident or attack or misuse.

v. IDS shall be able to log a summary of an incident to local data storage.

vi. IDS shall be able to terminate a TCP session by issuing TCP Reset packets to each end of the connection.

vii. IDS shall be able to prevent TCP, UDP, and any other access to a network by automatically reconfiguring a firewall or router to prevent certain traffic from crossing the firewall boundary for a user-specified period of time.

viii. IDS shall 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. (Optional for purchaser)

ix. IDS shall support integration with firewall to alter the firewall rule dynamically in order to pre-empt any intrusive activity. Such alteration shall be logged and the administrator shall be alerted in real time.

x. IDS shall be capable of attack response customization.

xi. IDS shall be capable to kill intrusion attempts.

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

xiii. IDS shall provide security event section replay. (Optional for Purchaser)

xiv. IDS shall provide TCP reset alarm

xv. IDS active response shall at least include the following:

a) Firewall reconfiguration via open protocols like OPSEC.

b) Execution of user defined programs. (Optional for Purchaser)

3.7 Configuration

i. Remote IDS (IDS 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. IDS 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. IDS shall support help system providing a detailed description of the attack signature that is selected.

iv. The priority level (evaluation criteria of rules should 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 The administrator, from the management console, shall be able to specify the response to each pre-defined event.

vi. The administrator from the management console shall be able to specify response to each attack or misuse.

vii. IDS shall be able to tune the pre-defined signatures in such a way that the false alarms/incident detections are minimized.

viii. IDS shall be capable to tune event propagation.

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

x. 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.

xi. IDS shall be capable of attack policy customization.

3.8 Data Management

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

ii. Data on the management console shall be stored in a database such as ODBC, MySQL etc.

iii. It shall be possible to export the one database to another database or to a delineated text file.

iv. IDS shall have comprehensive database with more than 3500 attack signatures.

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

vi. IDS shall be capable of prioritization of security event data for quick and easy threat assessment.

3.9 Report management

i. IDS shall have built-in report generation capability as per requirement which shall be specified at the time of tendering by the tendering authority.

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

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

vi. IDS shall provide reports based on:

  a) Security event risk level.
  b) Date/time.
  c) Event name.
  d) Source IP.
  e) Destination IP.
  f) Response taken.
  g) Sensor identity.
  h) Severity.
  i) Top attack types
  j) Attack groups
  k) Top-10 Source of Attacks
  l) Top-10 Destination of attacks
  m) IDS login details

vii. User shall be able to customize Reports

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

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

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

xi. IDS shall provide alerts/ notify by the following:

a) SNMP trap

b) Logging

c) Syslog/ SDEE

d) E-mail

e) Script

3.10 Performance

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

ii. IDS 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.

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

3.11 Updates and technical support

i. The IDS software and its attack signature database shall be updated at least monthly.

ii. 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.

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

iv. IDS Shall support 24/7 Security Update Service

v. IDS Shall support Real Time signature update

vi. IDS shall support for customized signatures.

vii. IDS shall support Automatic or manual signature synchronization from database server on Internet as per the administrator requirement. (As per purchaser’s option)

viii. The IDS 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 – 4

4. Engineering and Operational Requirements:

(Not applicable for virtual/cloud based IDS)

4.1 The Intrusion Detection system (IDS) 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 manufacturers 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) 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.

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

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

g) All LAN cabling shall be of Gigabit Ethernet ready standards.

h) The equipment shall have natural cooling arrangement which shall not involve any forced cooling such as by using fans etc. either inside or outside the equipment. However, in case this is unavoidable and the fans are to be used, these shall be DC operated and shall not impact on the MTBF of the equipment. The DC operated fans shall be available in redundant configuration.

4.2 The Intrusion Detection system (IDS) shall meet the following Maintenance & operational requirements:

a) The equipment shall be designed for continuous operation.

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

c) Suitable visual indications shall be provided to indicate the healthy and unhealthy conditions.

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

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

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

g) A single point failure on the equipment shall not result in network or Network Management System downtime.

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

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

j) 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.

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

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

CHAPTER - 5

5. Qualitative Requirements (QR):

(Not applicable for virtual/cloud based IDS)

a) The manufacturer shall furnish the MTBF value. Minimum value of MTBF shall be 500,000 hours. 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.

b) 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.

c) The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue- March, 2010} "Standard for Environmental testing of Telecommunication Equipments" or any other equivalent international standard, for operation, transportation and storage. The applicable tests shall be for environmental category "D" including vibration and corrosion (salt mist).

CHAPTER - 6

6. EMI/EMC Requirements

(Not applicable for virtual/cloud based IDS)

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report from accredited test lab shall be furnished from a test agency.

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 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. 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 - 7

7. Safety Requirements:

(Not applicable for virtual/cloud based IDS)

7.1 The equipment shall conform to:

i. IS 13252 part 1: 2010 “Information Technology Equipment –Safety- Part 1: General Requirements” [equivalent to IEC 60950-1 {2005} “Information Technology Equipment –Safety- Part 1: General Requirements”]

OR

IEC 62368-1: 2018 “Audio/video, information and communication technology equipment - Part 1: Safety requirements”

CHAPTER - 8

8. Security

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

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

iii. The data carried in these communications channels shall be authenticated and encrypted using the public key encryption and private key encryption.

iv. The IDS shall support stealth mode, so that it does not betray its presence on the network. In other words, the IDS existence on the monitored network shall not be known to any device except the sensors installed on the network devices.

v. The IDS 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 IDS shall support console to monitor its connections to the applications and shall be able to detect when an application goes off line unexpectedly.

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

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

ix. The IDS and management console security features shall include operator authentication, command, menu restriction and operator privileges. The management console shall support three or more 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 three 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. Should support the following detection techniques -

- Protocol anomaly detection
- Statistical anomaly detection
- Application anomaly detection
- Statistical analysis
- Evasion protection
- Vulnerability-based signature detection (>97%)
- Exploit-based signature detection (<3%)
- Session normalization and evasion detection
- On-box event correlation

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

a) Tolly

b) ICSA

c) FIDS

d) OPSEC

e) NIST

f) NSS

CHAPTER - 9

9. Information for the procurer of the product

9.1 Documentation:

9.1.1 This chapter describes the general requirements for documentation to be provided. All technical documents shall be in English language both in CD-ROM and in hard copy. The documents shall comprise of:

a) System description documents.

b) Installation, Operation and Maintenance documents.

c) Training documents.

d) Repair manual.

9.2 System description documents:

The following system description documents shall be supplied along with the system.

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

b) Equipment layout drawings.

c) Cabling and wiring diagrams.

d) Schematic drawings of all circuits in the system with timing diagram wherever necessary.

e) Detailed specification and description of all Input / Output devices.

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

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

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

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

j) Program and data listings.

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

9.3 System operation documents:

The following system operation documents shall be available.

a) Installation manuals and testing procedures.

b) Precautions for installation, operations and maintenance.

c) Operating and Maintenance manual of the system.

d) Safety measures to be observed in handling the equipment.

e) Man-machine language manual.

f) Fault location and troubleshooting instructions including fault dictionary.

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

h) Emergency action procedures and alarm dictionary.

9.4 Training Documents

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

b) 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.

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

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

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

9.5 Repair Manual

a) List of replaceable parts used.

b) Detailed ordering information for all the replaceable parts.

c) Procedure for trouble shooting and sub-assembly replacement.

d) Test fixtures and accessories for repair.

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

9.6 Installation

a) 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.

b) 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.

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

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

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

f) The equipment shall have:

g) Proper earthing arrangement.

h) Protection against short circuit / open circuit.

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

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

CHAPTER - 10

10. Tendering Information

10.1 Guidelines for the Tendering Authority

10.1.1 For optional features, the requirement if any may be stipulated by tendering/purchasing authority

ABBREVIATIONS

For the purpose of this document the following abbreviations apply:

BSNL	Bharat Sanchar Nigam Limited
CGM	Chief General Manager
CISC	Complex Instruction Set Computer
CISPR	The International Special Committee on Radio Interference
DC	Direct Current
DoS	Denial of Service
EMC	Electro Magnetic Compatibility
FTP	File Transfer Protocol
HTML	Hyper Text Media Language
HTTP	Hyper Text Transfer Protocol
GRE	Generic Routing Encapsulation
IDS	Intrusion Detection System
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
IMAP	Interactive Mail Access Protocol
ITU-T	Telecommunication Standardization sector of International Telecommunication Union
LAN	Local Area Network
MAC	Media Access Control
MTBF	Mean Time Between Failure
MTNL	Mahanagar Telephone Nigam Limited
MTTR	Mean Time To Restore
NMS	Network Management System
ODBC	Open Data Base Connectivity
OPSEC	Open Platform for Security
POP	Post Office Protocol
QA	Quality Assurance
QM	Quality Manual
RF	Radio Frequency
RISC	Reduced Instruction Set Computer
SDEE	Security Device Event Exchange

SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEC	Telecommunication Engineering Centre
UDP	User Datagram Protocol
WAN	Wide Area Network