वर्गीय आवश्यकताओं के लिए मानक

टीईसी 49090:2023

(सं: टीईसी/जीआर/आईटी/एफडब्लूएस/01/04-मार्च2014 को अधिक्रमित करता है)

STANDARD FOR GENERIC REQUIREMENTS

TEC 49090:2023

(Supersedes No. TEC/GR/IT/FWS/01/04-March 2014)

फायरवाल प्रणाली

Firewall System

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 Firewall System, appliance based as well as virtual, which is intended to be deployed by various service providers to secure their Information Technology / Telecommunication infrastructure.

CONTENTS

History Sheet 5
References 6

Chapters

1 Introduction 11
2 Description 12
3 Functional/Operational Requirements..... 14
4 Interconnectivity & Interoperability Requirements..... 23
5 Quality Requirements 25
6 EMI/EMC Requirements..... 26
7 Safety Requirements..... 31
8 Security Requirements..... 32
9 Other Mandatory Requirements 33
10 Desirable Requirements / Tendering Information 35
Glossary 46

HISTORY SHEET

Sl.No.	Standard / document *No.*	*Title*	*Remarks*
1.	GR No.GR/FWS-01/01.SEP2002	GR for the FIREWALL SYSTEM	First Edition
2.	GR No.GR/FWS-01/02.JUL 2006	GR for the FIREWALL SYSTEM	Second Edition
3.	TEC/GR/IT/FWS-001/03/Jan. 2011	GR for the FIREWALL SYSTEM	Revision of 2nd edition and reformatted as per CSSP 01 May 2008
4.	TEC/GR/I/FWS-001/04 MAR 2014	GR for the FIREWALL SYSTEM	Third Edition: incorporation of the IPv6 requirements and other changes
5.	TEC 49090:2023	Standard for Generic Requirements for a Firewall System	Fourth Edition: inclusion of Virtual / Cloud based Firewall

References

QM 118, QM205, QM206, QM210, QM 301, QM 324, QM 333, QM 351	Quality Manual issued by the QA Circle
TEC/EMI/TEL-001/01/FEB-09	EMI/EMC Standards
TEC/SD/NMS-02/01	Standard on NMS
ITU-T Rec H 323	ITU-T Recommendations on Packet-based multimedia communications systems
RFC 792	INTERNET CONTROL MESSAGE PROTOCOL
RFC 793	TRANSMISSION CONTROL PROTOCOL
RFC 959	FILE TRANSFER PROTOCOL (FTP)
RFC 1081	Post Office Protocol - Version 3
RFC 1122	Requirements for Internet Hosts -- Communication Layers
RFC 1436	The Internet Gopher Protocol
RFC 1825	Security Architecture for the Internet Protocol
RFC 1827	IP Encapsulating Security Payload (ESP)
RFC 1828	IP Authentication using Keyed MD5
RFC 1829	The ESP DES-CBC Transform
RFC 1918	Address Allocation for Private Internets
RFC 8201	Path MTU Discovery for IP version 6
RFC 2080	RIPng for IPv6
RFC 2113	IP Router Alert Option
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
RFC 2228	FTP Security Extensions
RFC 2236	IGMPv2
RFC 2328	OSPF Version 2
RFC 4601	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
RFC 2375	IPv6 Multicast Address Assignments
RFC 2428	FTP Extensions for IPv6 and NATs
RFC 2453	RIP Version 2
RFC 8200	Internet Protocol, Version 6 (IPv6) Specification
RFC 4861	Neighbor Discovery for IP Version 6 (IPv6)

RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	Architecture for Differentiated Services
RFC 2588	IP Multicast and Firewalls
RFC 2597	Assured Forwarding PHB Group
RFC 3246	An Expedited Forwarding PHB
RFC 2637	Point-to-Point Tunneling Protocol (PPTP)
RFC 2661	Layer Two Tunneling Protocol "L2TP"
RFC 2710	Multicast Listener Discovery (MLD) for IPv6
RFC 2711	IPv6 Router Alert Option
RFC 5340	OSPF for IPv6
RFC 2784	Generic Routing Encapsulation (GRE)
RFC 5321	Simple Mail Transfer Protocol
RFC 3040	Internet Web Replication and Caching Taxonomy
RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP
RFC 3261	SIP: Session Initiation Protocol
RFC 8415	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3319	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
RFC 3396	Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 7530	Network File System (NFS) version 4 Protocol
RFC 3596	DNS Extensions to Support IP Version 6
RFC 8415	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC 3646	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

RFC 8415	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC 3956	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
RFC 3977	Network News Transfer Protocol (NNTP)
RFC 4007	IPv6 Scoped Address Architecture
RFC 4193	Unique Local IPv6 Unicast Addresses
RFC 4271	A Border Gateway Protocol 4 (BGP-4)
RFC 4292	IP Forwarding Table MIB
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 5996	Internet Key Exchange (IKEv2) Protocol
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 4510	Lightweight Directory Access Protocol (LDAP)
RFC 4760	Multiprotocol Extensions for BGP-4
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)
RFC 4862	IPv6 Stateless Address Auto configuration
RFC 5340	OSPF for IPv6
RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification
RFC 6093	On the Implementation of the TCP Urgent Mechanism
RFC 6528	Defending against Sequence Number Attacks
IEEE 802.1q	IEEE Standards for Local and metropolitan area networks Virtual Bridged Local Area Networks
ISO 9000:2008	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
CISPR 11	Limits and methods of measurement of radio disturbance characteristics of industrial, scientific & medical (ISM) radiofrequency equipment
CISPR 32	Limits and methods of measurement of radio disturbance characteristics of ITE
EN 55011	Industrial, scientific and medical (ISM) radio-frequency equipment - Electromagnetic disturbance characteristics - Limits and methods of measurement

EN 55032	Information Technology Equipment - Radio disturbance characteristics - Limits and methods of measurement
IEC/EN 61000-4-2	Testing and measurement techniques – Electrostatic discharge immunity test
IEC/EN 61000-4-3	Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
IEC/EN 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test
IEC/EN 61000-4-5	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test
IEC/EN 61000-4-6	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields
IEC/EN 61000-4-11	Electromagnetic compatibility (EMC) Part 4-11: Testing and measurement techniques Voltage dips, short interruptions and voltage variations immunity tests
IEC 60479-1	Effects of current on human beings and livestock - Part 1: General aspects
IEC 13252	Information Technology Equipment -- Safety, Part 1: General Requirements
IS 10437	Safety requirements for radio transmitting equipment

CHAPTER 1

INTRODUCTION

1.1. Scope

This document specifies the Generic Requirements of firewall system, hardware based as well as virtual, which is intended to be deployed by various service providers to secure their Information Technology/Telecommunication infrastructure.

1.2. Introduction

Firewall System is one of the protection mechanisms available for providing network security. This is the first line of defense, which allows filtering out the unauthorized traffic from entering into Service Provider's (SP) network. The Firewall also does not allow exiting of unauthorized traffic from the SP's network. The Firewall System shall provide the single, integrated security policy which can be distributed across multiple firewall gateways and managed remotely from the central place for service provider. This document contains the detailed functional and technical requirements of a firewall system with pure firewall functionality ranging from low end to high end, which may be deployed by Service Provider to provide security for the installed IT infrastructure (equipment and servers, etc)/telecom network. The Virtual/Cloud based Firewall will run on servers which may be complemented with some additional NICs as needed.

1.3. For all ITU – T recommendations and TEC standards referred in this document, the latest release/issue with all associated amendments, addendum and corrigendum shall be applicable.

1.4. The RFC documents of the IETF are subject to periodic revision. Hence where ever RFC's are mentioned in this document, the offered product shall meet either the referred RFC or its previous version or its previous draft or its updated version. Wherever a feature of the RFC is mentioned, product shall comply with the part of the RFC specifying the feature.

1.5. The interpretation of the clauses of the RFC's shall be as per RFC 2119.

CHAPTER 2

DESCRIPTION

2.1 The firewall System architecture shall be able to define a single, integrated security policy distributed across multiple firewalls and managed remotely from the central place. The architecture shall be able to give central integration, configuration and management for the firewall as well as other third party security applications.

2.2 The firewall System shall be able to get configured as an application gateway, circuit level gateway and as a set of filtering mechanism. The firewall shall be flexible to implement the appropriate network security architecture.

2.3 The Operating System used in firewall shall not hamper the functionality of the firewall.

2.4 The firewall shall be appliance based with dedicated hardware designed or virtual firewall for networking and security services.

2.5 The sub network shall have no limitation on numbers of components (servers, etc.) and IP address. It shall also be possible to include servers of discrete IP address. As shown in figure 1 the firewall System architecture shall be able to divide the network into atleast the following three separate zones (sub networks):

a) **Secure Zone** - This shall be highly protected zone. Only authorized and authenticated personnel shall be permitted beyond this zone. Mission critical applications like NMS and Billing servers shall be in this zone.

b) **Demilitarized zone** (Perimeter Network) – This shall be semi-protected zone. Only users that have been checked and authenticated shall gain access to this zone. Application servers like WWW, Proxy, DNS, Radius, E-mail, etc., shall be in this zone.

c) **Open Zone** – These are open zones containing Remote Access Servers, Routers. The firewall system shall support creation of more zones and be site configurable to be included in any of the zone.

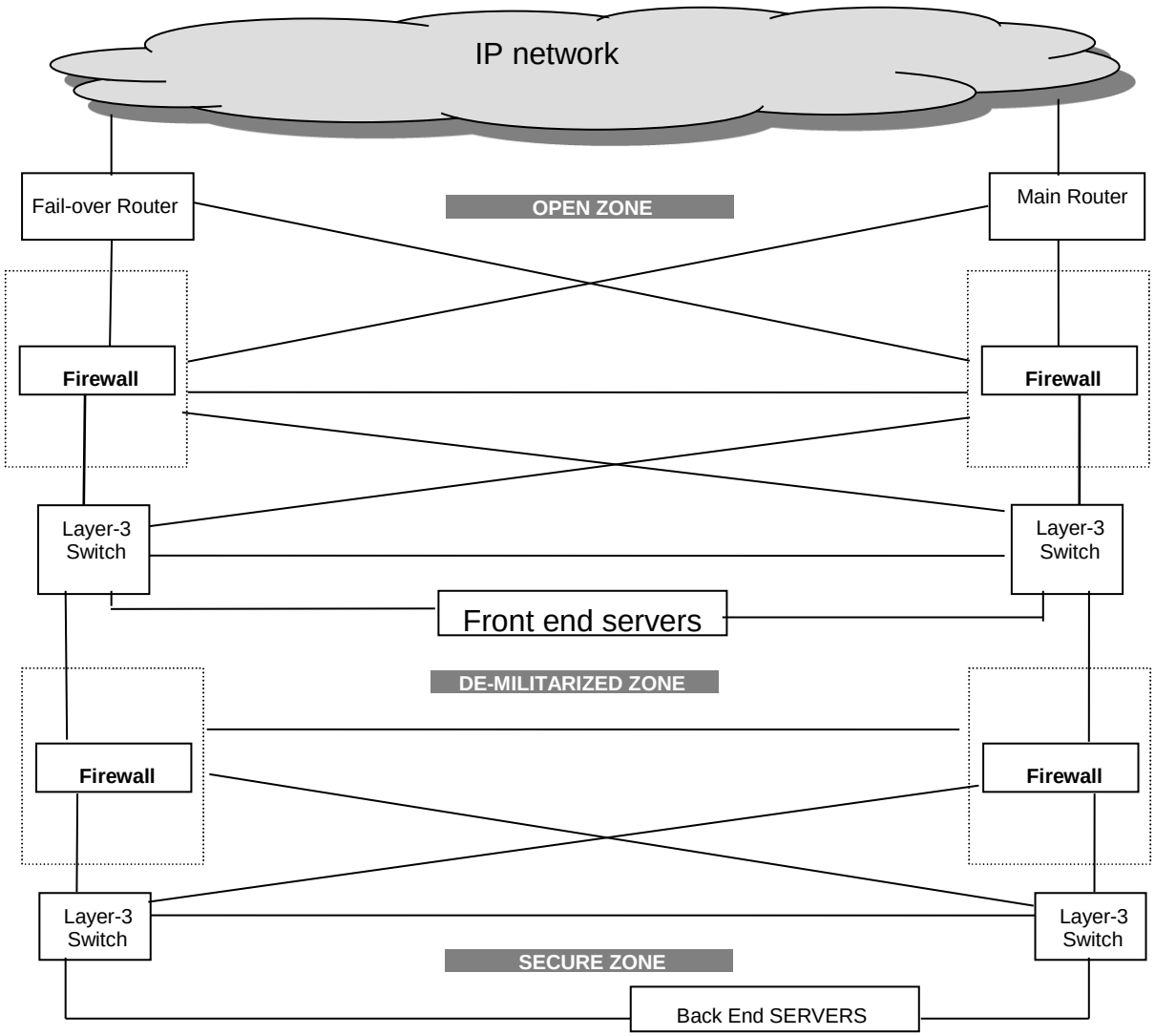

Figure 1: Architecture & Deployment of Firewall System

CHAPTER 3

FUNCTIONAL REQUIREMENTS

3.1. The firewall system shall consist of following functional components.

3.1.1. Hardware/virtual firewall and architecture

3.1.2. Filtering

3.1.3. Integrity

3.1.4. Privacy

3.1.5. Update

3.1.6. Management and reporting - Database, Report, User interface, access control, logging, reliability, availability, performance and scalability, software requirement, security administration and management.

3.2. Filtering

3.2.1. Traffic Filtering Features

i. The Firewall shall support HTTP, HTTPS and FTP filtering.

ii. The Firewall shall support Java and Active-x filtering.

iii. The Firewall shall allow users to modify the engine filtering logic such that it detects incidents related to a subset of the network traffic (e.g., specific IP address)

iv. The Firewall shall support Filtering based on select MIME types, such as JPEG extensions, which allows administrators to accurately deny worm and virus activity that could be associated with malicious content contained in certain MIME types.

v. The Firewall shall support Static packet filtering

vi. The Firewall shall support Dynamic packet filtering

vii. The Firewall shall support Stateful firewall

viii. The Firewall shall support Group Filtering based on L3/L7 parameters such as IP, Directory Number Identification Service (DNIS), subnet etc. is provided.

ix. The Firewall shall have the capability to drop any unwanted traffic. .

x. The Firewall shall support extensive packet filtering and firewalling at wire speed without degradation in interface and router performance. The Firewall shall have the ability to assign traffic filters based on any parameter like IP address/TCP/UDP port etc.

xi. The Firewall shall support MAC Address Filtering based on source and destination address.

xii. The Firewall shall support Discard Unknown to drop packets that are sourced from Unknown MAC address.

xiii. The Firewall shall support Bridge protocol data unit (BPDU) filtering when configured in L2 mode.

xiv. The Firewall shall support Unicast MAC filtering.

3.2.2. The Firewall shall have the capability to filter L2 traffic configurable on per Port/ PVC/ Service basis at least for the following parameters::

a. Broadcast Traffic
b. Source MAC Address
c. Destination MAC Address
d. Source MAC/IP Address
e. Destination IP Address
f. IP Port Number
g. Filters to block IGMP groups should be supported, Filter list should allow individual blocking of Multicast Groups
h. TCP flags
i. IGMP type
j. ICMP type
k. Ether type
l. Blocking of user-to-user flows
m. Source and destination IP address range (subnet)
n. Protocol type

3.2.3. The firewall shall Support filtering for at least following Standard based Internet Services:

1. Block AH traffic as per RFC 1825 & RFC 1828
2. Permit or Block BGP as per RFC 4271 & MBGP (Multiprotocol Extensions for BGP-4) as per 4760
3. DHCPv4 per RFC 3396 & DHCPv6 AS PER RFC 8415
4. DNS
5. Permit or Deny ESP as per RFC 1827 & RFC 1829
6. FTP as per RFC 959 ,RFC 2228 & RFC 2428 for IPv6
7. Active FTP
8. Passive FTP
9. GOPHER as per RFC 1436
10. Permit or Deny GRE as per RFC 2784
11. H323
12. HTTP1.0 and HTTP 1.1as per RFC 1945 & RFC 2616
13. ICMP_ANY as per RFC 792 for IPv4 and RFC 4443 for IPv6
14. IKEv2 as per RFC 5996
15. IMAP
16. Internet-Locator-Service
17. L2TP as per RFC 2661
18. NFSv4 as per RFC 7530
19. NNTP as per RFC 3977
20. NTPv4 as per RFC 5905
21. OSPF as per RFC 2328; OSPFv6 as per RFC 5340
22. PING as per RFC 792.
23. POP3as per RFC 1081
24. PPTP as per RFC 2637.
25. RIP2 as per RFC 2453 & RIPng for IPv6 as per 2080
26. SIP as per 3261
27. SMTP as per RFC 5321
28. SNMPv2 & v3
29. SSH
30. SYSLOG

31. TCP as per RFC 793,RFC 1122, RFC 3168, RFC 6093, RFC 6528.
32. TELNET
33. TFTP
34. UDP
35. IGMP (Multicast Protocols) as per RFC 2113, RFC 2236 &PIM-SM as per RFC 4601, RFC 2588
36. IRC

3.2.4. The firewall shall support filtering for following authentication Protocols

a) LDAP as per RFC 4510
b) HTTPS
c) RADIUS
d) DIAMETER
e) TACACS

3.2.5. The firewall shall support Layer-7 filtering including but not limited to the following database applications:

a) RDBMS
b) DB2
c) SQL

3.2.6. The firewall shall support for filtering multimedia applications such as VoIP, H.323, SIP, RTP, RTCP etc.

3.2.7. The firewall shall support for filtering HTTP traffic based on URLs based on content string matches for enterprise deployment.

3.2.8. The firewall System shall be based on stateful connection-oriented fire walling and support Static and Dynamic packet filtering.

3.2.9. The firewall System shall comply with RFC 1918 compatible with support for Static & Dynamic Network Address Translation and Port Address Translation with capability to generate and maintain the address translation rules.

3.2.10. Web cache redirection: The Firewall shall support transparent redirection of HTTP traffic as per RFC 3040.

3.3. Security Services:

3.3.1. The firewall System shall provide the following security features:

a) Prevent denial-of-service attacks.
b) Java Applet Filtering to stop dangerous Java applications on a per-client or per-IP address basis.
c) Support for unicast Reverse Path forwarding to prevent IP spoofing attacks.
d) Prevent TCP SYN attacks.
e) Prevent IP fragmentation attacks.
f) Support for ICMP filtering with configurable threshold.
g) UDP flood detection with configurable threshold using IPS.
h) Detect Ping of Death.
i) Detect Land attack.
j) Detect Win Nuke attack using IPS.
k) Filter IP source route option.

3.3.2. TCP Security Services

i. The Firewall shall support TCP stream reassembly and analysis

ii. The Firewall shall support TCP traffic normalization

iii. The Firewall shall support Flag and option checking

iv. The Firewall shall support TCP packet checksum verification

v. The Firewall shall support privacy, identity control feature and also provides transport layer security features.

3.3.3. Traffic Blocking:

i. The Firewall shall support protecting the port-80 misuse to block application such as Instant Messaging like Yahoo messenger.

ii. The Firewall shall support Blocking of popular peer-to-peer protocols.

3.3.4. DDOS Attacks

i. The Firewall shall protect from Distributed Denial of Service (DdoS) attacks.

3.4. Virtual Private Network

i. The Firewall shall have Inbuilt support for IPSEC VPNs functionality. It shall also support split tunneling VPN and client-based IPSec VPN tunnels.

ii. IKE (internet Key Exchange) protocol keep alive shall be supported that allows the devices to detect a dead remote peer for IPSEC redundancy.

iii. The hardware based platform shall use purpose-built hardware that is optimized for packet filtering and encryption. This requirement is not mandatory for virtual firewalls.

iv. The Firewall shall support DES, 3DES, AES encryptions algorithm.

v. The Firewall shall support VPN failover for redundancy where more than one connections are in group & if one connection goes down it automatically switch over to another.

vi. The VPN shall support external certificate authorities.

vii. It shall support local certificate authority & shall support create/renew/Delete self signed certificate.

viii. It shall be possible to apply bandwidth management policies on all traffic passing through the IPSec/L2TP/PPTP/SSL VPN tunnels

3.5. Integrity: - The firewall subsystem shall have the ability to detect data manipulation by any means using IPSec.

3.5.1. The firewall System modules running on different machines shall be able to share information and mutually update information and shall be able to work in synchronization with each other. Firewall shall be able to take over from another firewall when that has gone down. It shall provide a stateful transition during failover to prevent session losses.

3.5.2. The firewall System shall support online software reconfiguration to ensure that changes made to a firewall configuration take place with immediate effect.

3.5.3. The firewall System shall not affect the performance of the components (including servers) which it is protecting.

3.5.4. Overload protection mechanism shall be available. System shall revert back to normal mode of operation when load is reduced.

3.5.5. On power up the firewall shall use built-in system monitoring & diagnostics before going online to detect failure of hardware.

3.5.6. Communication among the firewall system's components shall be secure

3.5.7. The firewall shall be capable of communicating with Intrusion Detection System or in-built IPS over standard APIs or OPSec. APIs for the same shall be provided.

3.6. **Privacy**: - The firewall subsystem shall prevent unauthorized access of the network to see the contents of the message being sent. The firewall System shall also support the following features:

3.6.1. The firewall system shall have Inbuilt support for IPSEC VPNs and VPN functionality.

3.6.2. Extensive debugging capabilities to assist in hardware problem resolution shall be supported for appliance based firewall.

3.6.3. IKE (Internet Key Exchange) protocol keep alive shall be supported that allows the devices to detect a dead remote peer for IPSEC redundancy.

3.6.4. The platform shall use hardware that is optimized for packet filtering and encryption for appliance based firewall

3.6.5. The platform shall support firewalling for VLAN (IEEE 802.1q).

3.6.6. The firewall system shall be capable of clustering multiple firewalls together into a redundant and highly available stateful configuration.

3.6.7. The firewall system shall provide for a single default gateway IP address for all firewalls in a cluster.

3.6.8. There shall be a means of connecting directly to the firewall system through an encrypted VPN connection to perform troubleshooting and packet captures.

3.6.9. There shall be a means of connecting directly to the firewall system through a console connection.

3.6.10. The firewall system shall have a facility to block any unencrypted means of access to the firewall.

3.6.11. The firewall system shall support application layer inspection of sessions.

3.6.12. The firewall shall provide state engine support for all common protocols like HTTP, TFTP, SMTP etc. This engine shall support the following features:

a) The firewall state engine shall support the passing of OSPF, BGP traffic and multicast packets in transparent mode.

b) The firewall system shall support application layer inspection of sessions.

c) The firewall system shall provide a means to define and modify existing services and state engine.

3.7. Updates

3.7.1. The firewall System shall support TFTP/FTP for easy software upgrades over the network in a secure way.

3.7.2. Firewall System shall support SNMP v3 as per RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414 and RFC 3826.

The firewall system shall also support SFTP/SCP.

3.8. Logging

3.8.1. Firewall System shall support Logging /Monitoring via Syslog. The firewall logging features shall include the following:

a) The firewall logs shall contain information about the firewall policy rule that triggered the log using Firewall eMS/Manager.

b) The firewall shall be capable of capturing detailed packet data to a log.

c) The firewall logging shall not impact firewall performance.

d) The firewall shall provide a means for synchronizing time between firewalls, the log server and the administration station using NTP.

e) The firewall system shall provide statistics about the health of the firewall and the amount of traffic traversing the firewall using Firewall eMS/Manager.

3.8.2. The firewall shall be able to send logs to different firewall log servers.

3.8.3. The consolidated log data shall be made available through a central/secure log database for easy management & retrieval using a reporting database using Firewall eMS/Manager.

3.8.4. The firewall shall be able to filter log data by user for AAA authenticated users.

3.8.5. The firewall shall be able to consolidate log data for efficient reports using Firewall eMS/Manager

3.8.6. The firewall shall be able to consolidate log data for

a) Network services,

b) Network resources

c) User/groups

d) Connection duration

e) Number of bytes transferred

f) Blocked connections

g) Source/Des. IP addresses

h) Failed authentication attempts

i) Date/Time

j) Firewall identity

k) Intrusion attempts

l) Alert/error conditions

3.8.7. The user shall be able to specify/create modify/delete rules/policies to collect log data and consolidate based on what he requires using Firewall eMS/Manager.

3.8.8. The log consolidator shall be able to use firewall objects/users for use in the consolidation policy using Firewall eMS/Manager.

3.8.9. The firewall shall send log information to an external log server using FTP or syslog.

3.9. Reporting

It shall be Optional for the purchaser to have an integrated or separate reporting system

3.9.1. The firewall shall provide in-depth details on network traffic and activities.

3.9.2. Reporting software components shall support distributed environment/ installation.

3.9.3. User level access restrictions shall be possible for accessing managing the components and generating reports

3.9.4. Remote management and generation of reports shall be possible

3.9.5. The firewall shall generate reports consisting of audit in easy to understand formats

3.9.6. The firewall shall support well-predefined and custom reports

3.9.7. The reports shall be available in different formats, e.g. CSV, PDFetc. Tendering authority shall provide the detail of report formats .

3.9.8. The reports shall be automatically sent to e-mail, etc.

3.9.9. The firewall shall provide a means for specifying thresholds and conditions for which it would send an alert

3.10. Database

The firewall subsystem shall allow maintenance of detailed records and audit trail information. The firewall System shall be able to provide complete real time control of the network configuration including accounting, live connections monitoring, alerting, notification to the syslog server.

3.11. IPv6 Protocol Requirements:

3.11.1. The firewall shall support IPv6 as per RFC 8200, RFC 4861, RFC 4862and RFC 4443 routing in coexistence with IPv4 routing.

3.11.2. **IP Routing Protocols:** The Firewall shall meet the following IP Routing Protocols relating to IPv6

i. RIPng for IPv6 as per RFC 2080

ii. OSPFv3 for IPv6 as per RFC 5340

iii. IPv6 Static Routing

iv. IPv6 Route Redistribution

3.11.3. General IPv6 support: The Firewall shall meet the following general IPv6 support Requirements**-**

i. IPv6 Address types: Unicast (Unique Local IPv6 address as per RFC 4193), Anicast and Multicast.

ii. ICMPv6 as per RFC 4443

iii. IPv6 Neighbor Discovery as per RFC 4861

iv. IPv6 stateless auto configuration as per RFC 4862

v. IPv6 MTU path discovery as per RFC 8201

vi. IPv6 ping
vii. ICMPv6 redirect
viii. ICMPv6 rate limiting
ix. IPv6 neighbor discovery duplicate address detection
x. IPv6 default router preference as per RFC 2711
xi. IPv6 access control
xii. Syslog over IPv6
xiii. IP SLAs for IPv6
xiv. IPv6 Specification as per RFC 8200
xv. IPv6 Scoped Address Architecture as per RFC 4007
xvi. ICMPv6 for IPv6 Specification as per RFC 4443

3.11.4. IPv6 QoS: The Firewall shall meet the following IPv6 QoS Requirements

i. Packet classification as per RFC 2474
ii. Traffic shaping
iii. Traffic policing
iv. Packet marking/re-marking as per RFC 2475
v. IPv6 QoS queuing
vi. Weighted random early detection (WRED)- based drop
vii. Assured Forwarding PHB Group shall be as per RFC 2597

3.11.5. IPv6 Services: The Firewall shall meet the following IPv6 Service Requirements

i. Standard access control lists for IPv6
ii. Secure Shell (SSH) support over IPv6
iii. IPv6 MIB support
iv. SNMP over IPv6
v. IPv6 IPSec VPN
vi. Stateless DHCPv6
vii. DHCPv6 prefix delegation
viii. DHCP for IPv6 relay agent
ix. DHCPv6 prefix delegation via AAA
x. DHCPv6 Server Stateless Auto Configuration
xi. DHCPv6 Client Information Refresh Option.
xii. DHCPv6 relay agent notification for prefix delegation
xiii. DHCPv6 relay- reload persistent interface ID option
xiv. DHCP - DHCPv6 Individual Address Assignment
xv. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) as per RFC 8415

xvi. DNS Extensions to Support IP Version 6 as per RFC 3596

xvii. DHCP IPv6 Prefix Delegation RFC 8415

xviii. DNS Configuration options for DHCPv6 as per RFC 3646

xix. Stateless DHCP Service for IPv6 as per RFC 8415

xx. IP Forwarding Table MIB as per RFC 4292

xxi. Management Information Base for the Internet Protocol as per RFC 4293

xxii. Dynamic Host Configuration Protocol version 6 (DHCPv6) options as per RFC 3319.

3.11.6. IPv6 Multicast: The Firewall shall meet the following IPv6 Multicast Requirements

i. IPv6 Multicast Listener Discovery (MLD) protocol versions 1 and 2

ii. IPv6 PIM sparse mode (PIM-SM)

iii. IPv6 PIM Source Specific Multicast (PIM-SSM)

iv. IPv6 multicast scope boundaries

v. IPv6 multicast MLD access group

vi. IPv6 multicast PIM accept register

vii. IPv6 multicast PIM embedded RP support

viii. IPv6 multicast RPF flooding of bootstrap router (BSR) packets

ix. IPv6 multicast routable address hello option

x. IPv6 multicast SSM mapping for MLDv1 SSM

xi. IPv6 multicast IPv6 BSR—ability to configure RP mapping

xii. IPv6 multicast MLD group limits

xiii. IPv6 Multicast Address Assignments as per RFC 2375

xiv. IPv6 Multicast Listener Discovery (MLD) protocol, versions 1 and 2 as per RFC 2710

xv. MLDv2 for IPv6 as per RFC 3810 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address as per RFC 3956

CHAPTER 4

INTERCONNECTIVITY & INTEROPERABILITY

4.1. Firewall shall inter-work with existing Servers, Routers, LAN switches, etc as deployed in SP's IT/telecommunication infrastructure.

4.1.1. It shall be a fully integrated multi-platform wide security solution.

4.1.2. The firewall shall support 802.1Q Trunking.

4.1.3. The firewall System shall support the following minimum performance levels

a) wire rate throughput at all interfaces;

b) Stateful failover shall be supported to eliminate session loss;

c) firewall shall support redundant fans, Disk, Control subsystem and CPU or firewall shall be deployed in high availability configuration in No single point of failure configuration (NSPOF);

d) **Redundant and Hot swappable Power supplies.** Firewall shall be DC (-48 V nominal capable to operate in the range of -40 to -56 V) or AC Powered (220 V + 10% -15%) nominal at 50 ± 2 Hz. The power feeding arrangements to the Power supply units shall also be provided in redundant configuration. (Optional for category A);

e) The Firewall System Chassis shall be rack mountable in a 19" rack

4.2. The resources in the firewall, such as CPU memory, etc. shall be capable of handling the minimum performance as per categorization below with all the features enabled as specified in this document without deterioration in performance.

Category	Throughput with all filtering policies applied.	Interface (minimum requirement)	Concurrent Session	Session / sec	VLAN support
A	100 Mbps	10/100 x 2	100K	2K	15
B	1 Gbps	1 GE x 2	250,000	15K	200
C	3 Gbps	1 GE x 6	500,000	40K	1K
D	10 Gbps	10 GE x 4	1.5M	150K	1K
E	20 Gbps	10 GE x 4	3M	200K	1K
F	40 Gbps	10GE x 4	6M	400K	1K
G	100 Gbps	10GE x 8	20M	1M	1K

Tendering authority shall provide the actual interface requirement.

The firewall system can be offered for type approval under one or more categories as above.

4.3. User interface

4.3.1. Firewall System shall support management via web user interface (HTTP and HTTPS), Command Line interface (Console), Secure Command Shell (SSH).

4.3.2. It shall be possible to monitor firewalls from the central site.

4.3.3. The Firewall System shall be manageable through an (element management system (EMS). The EMS application for the firewall system shall be UNIX or any other industry standard OS based and provide management for a minimum of 10 firewall devices from a single EMS system. EMS of Firewall shall provide FCAPS (Fault Configuration, Accounting, Provisioning and Security) as per TEC standard: SD/NMS-02. In addition it shall provide following:

a) SSH support: The firewall shall support up to five SSH clients to simultaneously access the firewall console. SSH availability shall be with a triple Data Encryption Standard (3DES) activation key

b) The firewall shall provide a Graphical User Interface (GUI) and a Command Line Interface (CLI) for making changes to the firewall rules set. Access to vie firewall via the GUI and CLI through an encrypted channel.

c) The firewall EMS shall provide a means for exporting the firewall rules set and configuration to a text file.

d) The firewall shall support external user database authentication for firewall admin user.

e) Any changes or commands issued by an authenticated user shall be logged to an external database using AAA.

f) Remote network access to the firewall shall only be possible through the outside interface

g) The firewall EMS shall be capable of pushing firewall security policies and configurations to individual or multiple firewalls through a secure, encrypted connection to the firewall administration interfaces

h) There shall be a means of connecting directly to the firewall through an encrypted connection to perform troubleshooting and packet captures.

i) There shall be a means of connecting directly to the firewall through a console connection

j) The EMS shall allow for a hierarchical architecture for rules set administration and viewing of firewall configurations.

4.4. Reliability, Availability, Performance and Scalability of Firewall system and EMS: It shall provide the Reliability, Availability, Performance and Scalability requirements as per clause 6.2 of TEC standard on NMS: SD/NMS-02/01 as applicable to firewall system, with over 99.999% availability.

4.5. Software Requirement of Firewall system and EMS: The solution architecture shall be flexible to meet design requirements and shall be delivered in several hardware arrangements, or be customised to fit specific requirements. It shall provide the software requirements as per clause 4.1 of TEC standard on NMS: SD/NMS-02/01 as applicable to firewall system.

CHAPTER 5

QUALITY OF SERVICE
(Not applicable for virtual/cloud based Firewall)

5.1 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.

5.2 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.

5.3 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

EMI/EMC REQUIREMENTS
(Not applicable for virtual/cloud based Firewall)

6.1 Product under this GR would belong to Class B.

6.2 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

SAFETY REQUIREMENTS
(Not applicable for virtual/cloud based Firewall)

7.1 Safety Requirements:

7.1.1 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

SECURITY REQUIREMENTS

8.1. Security Administration and Management of Firewall system and EMS

The firewall system shall have Security Administration and management function for administering security policy and managing security related information. These features shall be provided by NMS/EMS, if not indicated otherwise. It shall as per clause 3.5.3 of TEC standard on NMS: SD/NMS-02/01.

8.2. Management and reporting

8.2.1. **Access Control** – The firewall subsystem shall control information and access through predetermined security policy.

a) The firewall System functionality shall be carried out with the help of a completely independent operating system, which shall be written/ hardened with Information security as the objective.

b) The firewall subsystem shall allow data communication only by authenticated network resources.

c) The firewall shall not support any unencrypted means of access to the firewall other than physical console access

d) The firewall System shall be able to support authentication challenging users and Support State of art encryption and authentication standards like IPSec, RADIUS, DIAMETER etc.

e) The firewall System shall support remote client functionality. It shall be possible to deactivate remote session. It shall support egress and ingress filtering so that only authorized IP address is able to enter into the firewall system. Number of permitted remote session shall be configurable.

8.3. The firewall System shall support Remote login as per the latest guidelines issued by DoT.

8.4. The Firewall shall meet the security certification requirements mandated by DoT from time to time.

CHAPTER 9

OTHER MANDATORY REQUIREMENTS
(Not applicable for virtual/cloud based Firewall)

The Firewall shall meet the following mandatory requirements.

9.1. **Engineering Requirements:** The Firewall System shall meet the following engineering requirements:

9.1.1. The equipment shall adopt state of the art technology.

9.1.2. The manufacturer shall furnish the actual dimensions and weight of the equipment.

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

9.1.4. All LAN cabling shall be of Gigabit Ethernet ready.

9.1.5. The equipment shall have adequate cooling arrangements.

9.2. **Operational Requirement (OR):** The Firewall System shall meet the following Maintenance & operational requirements:

9.2.1. The equipment shall be designed for continuous operation.

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

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

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

9.2.5. In the event of a full system failure, a crash dump shall be supported for analysis and problem resolution.

9.2.6. A power down condition shall not cause loss of connection configuration data storage in high availability mode.

9.2.7. Live Insertion and hot swap of modules shall be possible for chassis based firewalls to ensure maximum network availability and easy maintainability.

9.3. **Other Requirements:**

9.3.1. 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.

9.3.2. 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.

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

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

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

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

9.3.4. 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.

CHAPTER 10

DESIRABLE REQUIREMENTS / TENDERING INFORMATION

10.1 General:

This chapter describes the desirable requirements for the Firewall and will depend upon the requirement of the purchaser. Hence the tendering authority may choose out of the clauses mentioned below as per requirement.

10.2 Optional Firewall Services:

10.2.1 HTTP security services:

a. The Firewall shall support RFC compliance

b. The Firewall shall support protocol anomaly detection

c. The Firewall shall support protocol state tracking

d. The Firewall shall support MIME type validation

e. The Firewall shall support Uniform Resource Identifier (URI) length enforcement.

10.2.2 FTP security services:

a. The Firewall shall support Protocol anomaly detection

b. The Firewall shall support Protocol state tracking

c. The Firewall shall support NAT and PAT for FTP security services

d. The Firewall shall support Dynamic Port opening & closing

e. The Firewall shall have the capability to enforce what operations users and groups can perform within FTP sessions.

10.3 The firewall shall support IEEE 802.3ad link aggregation control protocol (LACP).

10.4 Intrusion Detection & Prevention (IDP) Requirements

If the tendering authority wishes to purchase the IDP solution integrated with the firewall, the following clauses shall apply. The same shall be specified by the tendering authority.

10.4.1 Functional requirement of IDP is divided into following:

a. Architecture.

b. Incident Monitoring and Detection.

c. Incident Response.

d. Configuration.

e. Management

f. Security.

g. Performance.

h. Updates and Technical Support.

10.4.2 Architecture :

i. IDP shall detect and actively prevent attacks in real-time and shall be placed in INLINE mode.

ii. The latency introduced by the IDP shall be minimum and shall not become a congestion point or become a central point of failure to the network being monitored.

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

iv. IDP shall allow working in failover mode.

v. IDP 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.

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

vii. IDP devices shall block only the attack session without effecting service to legitimate clients.

viii. 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.

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

x. IDP performance shall not reduce by enabling Layer 7 attacks filters.

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

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

xiii. IDP system if installed in bridge mode shall be transparent and invisible to network (Applicable only if Bridge mode deployment available)

10.4.3 The IDP shall Support filtering for at least following proprietary Internet Services:

1. NetMeeting
2. PC-Anywhere
3. SIP-Messenger
4. SAMBA
5. SKYPE, HANGOUT, GOOGLE-TALK etc

10.4.4 The IDP shall support e-mail related filtering as follows:

a) Lotus Notes based on SMTP
b) Microsoft Exchange based on SMTP

10.4.5 Incident Monitoring and Detection -:

i. IDP 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 etc.) and pattern matching shall be supported by IDP. iii. IDP shall support pattern-based signatures having a strong sense of context, so that false alarms/incident detections are minimized.

iii. IDP 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.

iv. IDP 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.

v. IDP shall support blocking of anonymous open HTTP Proxy running on 80 port or any other port & also shall support client based open proxy like Ultra surf.

vi. IDP shall able to detect & block known P2P based instant messanging application like skype & known chat application like WLM, Rediffbol etc.

vii. IDP shall able to detect VoIP (like SIP) data and shall be able to block the same.

viii. IDP 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. IDP 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. IDP 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).

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

xiii. IDP 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.

xiv. IDP shall be configured to focus on the incidents that pose the greatest risk to the network.

xv. IDP shall detect the malicious activity event in fragmented and de-fragmented packets.

xvi. IDP shall provide Stateful Operation

a. TCP Reassembly

b. IP De-fragmentation

c. Bi-directional Inspection

d. Forensic Data Collection

e. Access Lists

xvii. IDP shall provide Signature Detection for at least 3500 (more than 1500 vulnerability based) Vendors Signature Database and 5,000 User Defined Signatures

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

xix. The IDP shall provide the capability to annotate incidents recorded in the database.

xx. IDP 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. Protection against Mass mailing worm and viruses

k. SSL Encrypted Attack Protection(optional)

xxi. IDP 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

xxii. IDP 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

10.4.6 Incident Response -:

i. IDP shall be able to show alarms on the management console, upon detection of an incident.

ii. IDP shall be able to send an SNMP trap to the network upon detection of an incident.

iii. IDP shall be able to log a summary of an incident to persistent data storage.

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

v. Shall detect attack due to URL decoding vulnerabilities.

vi. IDP shall be capable of:

a) Block attacks in real time

b) Drop Attack Packets

c) Reset/ drop Connections

d) Packet Logging

e) IDP shall be capable of Attack Isolation:

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

g) Attack isolation and protection against unknown flooding attacks.

10.4.7 Configuration -:

i. IDP 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.

ii. IDP shall provide creation of multiple IDP policy for different zone instead of blanket policy at interface level.

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

iv. The interface shall allow attack signatures to be activated or deactivated via check-box selection. (optional)

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

vi. IDP 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.

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

viii. 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.

ix. IDP shall be capable of attack policy customization.

x. IDP shall have provision to analyze and identify the ingress point of attack.

10.4.8 IDP user interface -:

10.4.8.1 Provide customizable features such as Detection Rules, Reports, Alerts, and Responses via the IDP user interface.

10.4.8.2 IDP user interface shall support following for access:

a) HTTPS

b) SSH

10.4.8.3 IDP user interface shall provide Graphical User Interface (GUI) as follows:

i. IDP 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 IDP in response to the event.

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

10.4.8.4 Data Management -:

i. IDP shall have comprehensive database with more than 3500 attack(of them atleast 1500 vulnerabilities based) signatures.

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

iii. IDP shall be capable of prioritization of security event data for quick and easy threat assessment.

10.4.8.5 IDP Reports:-

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

v. 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.

vi. IDP 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. User Identity

h. Response taken.

i. Severity.

j. Top attack types

k. Attack groups

l. Top-10 Source of Attacks

m. Top-10 Destination of attacks

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

viii. Provision to automatically generate & email reports daily, weekly or monthly to predefined email addresses.(optional)

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

x. IDP shall provide alerts/ notify by following:

a. SNMP trap

b. Logging

c. Syslog

10.4.9 Security - IDP:

i. The IDP 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.

ii. The IDP shall monitor its internal application modules and notify the

management station when a module goes off line unexpectedly.

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

iv. The management console shall have the feature of idle time disconnection.(optional)

10.4.10 Performance IDP -:

i. IDP shall process network traffic at a rate that does not add delay, or becomes a congestion point while attack signatures active. iii. IDP shall support performance that scales well with the number of attack signatures and filters active.

ii. IDP shall handle traffic bursts gracefully, switching to sampling mode until the traffic levels return to a consistent level.(optional)

10.4.11 IDP Updates -:

i. The IDP 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 IDP remotely and securely with new signature (Pattern of DoS Attack, pattern for hacking attempts using a particular hacking software etc.) updates or full IDP software update.

v. IDP Shall support 24/7 Security Update Service

vi. IDP Shall support Real Time signature update

vii. IDP shall support for customized signatures.

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

ix. The IDP shall provide for regular updates to the signature database

10.5 Anti-Virus

10.5.1 The Firewall shall be deployed as Gateway Scanning engine.

10.5.2 The Firewall shall be able to scan traffic without acting as a mail server in case of mail protocols

10.5.3 The FIREWALL shall be able to operate in transparent mode.(Applicable if bridge mode is supported)

10.5.4 The Firewall shall protect HTTP, SMTP, FTP, POP3 and IMAP protocols

10.5.5 The Firewall shall support both stream based Anti Virus scanning and file based Anti Virus scanning

10.5.6 The Firewall shall have Signature and Behavioral antivirus engine.

10.5.7 The Firewall shall perform both inbound and outbound inspection

10.5.8 The Firewall shall have 2.5+ million virus signatures for comprehensive coverage

10.5.9 The Firewall shall perform email attachment inspection including compressed files in multiple layers (eg where a compressed attachment has another compressed file), email messages and FTP downloads/uploads, or embedded scripts

10.5.10 The Firewall shall stop zero day variants

10.5.11 The Firewall shall support Virus filtering and shall have its own Virus list that shall be updated automatically.

10.5.12 The Firewall shall be multi-threaded

10.5.13 The Firewall shall be able to scan all traffic or specific extensions as defined by the administrator.

10.5.14 The Firewall shall support an Allow and Deny list of valid IP to allow/deny relaying for.

10.5.15 The Firewall shall be able to block attachment by file name and extension.

10.5.16 The Firewall shall support Recursive Analysis on messages and Compressed files

10.5.17 The Firewall shall have separate inbound and outbound virus and content. Scanning policies

10.5.18 The Firewall shall support real mode for HTTP virus scanning.

10.5.19 The Firewall shall provide option to bypass scanning for specific HTTP traffic.

10.5.20 The Firewall shall scan http traffic based on username, source/destination IP address or URL based regular expression.

10.6 Documentation

10.6.1 Documentation:

This clause 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

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

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

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

10.6.3 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 (command set) manual.

f) Fault location and trouble shooting 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.

10.6.4 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.

10.7 Installation

10.7.1 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.

10.7.2 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.

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

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

10.7.5 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.

10.7.6 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.

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

10.8 Tendering authority shall specify

(i) Firewall category and corresponding Interface requirement.

(ii) Requirement of HTTP and FTP security Services as per clause 10.2

(iii) Requirement of Integrated Reporting system as per clause 3.9

(iv) Link Aggregation requirement as per clause 10.3

(v) Requirement of Intrusion detection and Pretension system integrated with the Firewall [Single Box] as per clause 10.4

(vi) Requirement of Integrated antivirus as per clause 10.5

(vii) Requirement of IDP Reports as integrated with the system as per clause 10.4.8.5

(viii) Documentation Requirements as per clause 10.6

(ix) Installation requirements as per clause 10.7

10.9 Minimum Equipments Required for Type Approval

(i) One Firewall of the offered category and interfaces as per the clause 4.2

(ii) It is optional for offering the optional features as clause 10.8.

(iii) Type approval Certificate shall indicate

a) Category of Firewall

b) Optional features offered for testing as per clause 10.8

Glossary

3DES	Triple DES
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BSNL	Bharat Sanchar Nigam Limited
CA	Certification Authority
CPU	Central Processing Unit
DES	Data Encryption Standard
DHCP	Direct Host control Protocol
DNS	Domain Name Server
EIA	Electronic Industries Association
EMC	Electromagnetic Compatibility
EMS	Element management system
FTP	File Transfer Protocol
HDCP	High bandwidth Digital Content Protection
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
ICMP	Internet Control Message Protocol
ICSA	International Computer Security Association
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSec	IP Security Protocols
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
LAN	Local area network
LDAP	Lightweight directory management Protocol
MIB	Management Information Base
MIME	multipurpose Internet mail extensions
MTBF	Mean Time between Failure
MTNL	Mahanagar Telephone Nigam Limited
MTTR	Mean time to repair
NAT	Network Address Translator

NMS	Network Management System
OS	Operating system
OSPF	Open shortest path first
PC	Personal Computer
POP	Post Office Protocol
PSTN	Public switched Telephone Network
RADIUS	Remote access dial in user service
RFC	Request for Comments
RPC	Remote procedure call
RTCP	Real time control protocol
S/MIME	Secure MIME
SIP	Session Initiated Protocol
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
SQL	Sequential query language
SSH	Site Security Handbook
TACACS	Terminal Access Controller Access Control System
TCP	Transmission control protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industries Association
UDP	User Datagram Protocol
URL	Universal resource locator
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WWW	World Wide Web