Department of Telecommunications
TELECOM ENGINEERING CENTER
Khurshid Lal Bhavan, Janpath, New Delhi-110001

Title:	Provisional Test Procedure For Type Approval for FIREWALL SYSTEM	
GR No:	**GR No. TEC/GR/IT/FWS-001/04/MARCH 2014**	**मार्च-14**

Clause No		**Clause**	**Type of test**	**Compliance**
			Physical Check / Declaration / Documentation / Report from Accredited Test Lab / Functional verification / Information / Lab Test (Test Reference)	**Complied / Not Complied / Submitted / Not Submitted / Not Applicable (Indicate Annexure No for Test Results)**
1		**Introduction**		
1.1		Scope This document specifies the Generic Requirements of firewall system which is intended to be deployed by various service providers to secure their Information Technology/Telecommunication infrastructure	Information	
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)/telecomm	Information	

		network.		
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	Information	
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	Information	
1.5		The interpretation of the clauses of the RFC's shall be as per RFC 2119	Information	
2		**Description**	Information	
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	Declaration	
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	Declaration	
2.3		The Operating System used in firewall shall not hamper the functionality of the firewall	Declaration	
2.4		The firewall shall be appliance based with dedicated hardware designed for networking and security services	Declaration	
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):	Declaration	

	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	Declaration	
	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	Declaration	
	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	Declaration	
3		**Functional Requirements**	Information	
3.1		The firewall system shall consist of following functional components	Information	
3.1.1		Hardware and architecture	Declaration	
3.1.2		Filtering	Declaration	
3.1.3		Integrity	Declaration	
3.1.4		Privacy	Declaration	
3.1.5		Update	Declaration	
3.1.6		Management and reporting - Database, Report, User interface, access control, logging, reliability, availability, performance and scalability, software requirement, security administration and management	Declaration	
3.2		Filtering	Information	
3.2.1		Traffic Filtering Features	Information	
	i.	The Firewall shall support HTTP, HTTPS and FTP filtering	Functional Verification	
	ii.	The Firewall shall support Java and Active-x filtering	Functional Verification	
	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)	Functional Verification	
	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	Functional Verification	

		malicious content contained in certain MIME types		
	v.	The Firewall shall support Static packet filtering	Functional Verification	
	vi.	The Firewall shall support Dynamic packet filtering	Functional Verification	
	vii.	The Firewall shall support Stateful firewall	Functional Verification	
	viii.	The Firewall shall support Group Filtering based on L3/L7 parameters such as IP, Directory Number Identification Service (DNIS), subnet etc. is provided	Functional Verification	
	ix.	The Firewall shall have the capability to drop any unwanted traffic directed towards the router	Functional Verification	
	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	Declaration	
	xi.	The Firewall shall support MAC Address Filtering based on source and destination address	Functional Verification	
	xii.	The Firewall shall support Discard Unknown to drop packets that are sourced from Unknown MAC address	Functional Verification	
	xiii.	The Firewall shall support Bridge protocol data unit (BPDU) filtering	Functional Verification	
	xiv.	The Firewall shall support Unicast MAC filtering	Functional Verification	
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	Information	
	a.	Broadcast Traffic	Functional Verification	
	b.	Source MAC Address	Functional Verification	
	c.	Destination MAC Address	Functional Verification	
	d.	Source MAC/IP Address	Functional Verification	
	e.	Destination IP Address	Functional Verification	
	f.	IP Port Number	Functional Verification	

	g.	Filters to block IGMP groups should be supported, Filter list should allow individual blocking of Multicast Groups	Functional Verification	
	h.	TCP flags	Functional Verification	
	i.	IGMP type	Functional Verification	
	j.	ICMP type	Functional Verification	
	k.	Ether type	Functional Verification	
	l.	Blocking of user-to-user flows	Functional Verification	
	m.	Source and destination IP address range (subnet)	Functional Verification	
	n.	Protocol type	Functional Verification	
3.2.3		The firewall shall Support filtering for at least following Standard Based Internet Services	Information	
	1	Block AH traffic as per RFC 1825 & RFC 1828	Declaration	
	2	Permit or Block BGP as per RFC 4271 & MBGP (Multiprotocol Extensions for BGP-4) as per RFC 4760	Functional Verification	
	3	DHCPv4 per RFC 3396 & DHCPv6 AS PER RFC 3315	Functional Verification	
	4	DNS	Functional Verification	
	5	Permit or Deny ESP as per RFC 1827 & RFC 1829	Declaration	
	6	FTP as per RFC 959 ,RFC 2228 & RFC 2428 for IPv6	Declaration	
	7	Active FTP	Functional Verification	
	8	Passive FTP	Functional Verification	
	9	GOPHER as per RFC 1436	Declaration	
	10	Permit or Deny GRE as per RFC 2784	Declaration	
	11	H323	Declaration	
	12	HTTP1.0 and HTTP 1.1as per RFC 1945 & RFC 2616	Declaration	
	13	ICMP_ANY as per RFC 792 for IPv4 and RFC 4443 for IPv6	Functional Verification	
	14	IKEv2 as per RFC 4306	Functional Verification	
	15	IMAP	Declaration	
	16	Internet-Locator-Service	Declaration	
	17	L2TP as per RFC 2661	Functional	

			Verification	
	18	NFSv4 as per RFC 3530	Declaration	
	19	NNTP as per RFC 3977	Declaration	
	20	NTPv4 as per RFC 5905	Functional Verification	
	21	OSPF as per RFC 2328; OSPFv6 as per RFC 5340	Functional Verification	
	22	PING as per RFC 792	Functional Verification	
	23	POP3as per RFC 1081	Functional Verification	
	24	PPTP as per RFC 2637	Functional Verification	
	25	RIP2 as per RFC 2453 & RIPng for IPv6 as per 2080	Functional Verification	
	26	SIP as per 3261	Functional Verification	
	27	SMTP as per RFC 2821	Functional Verification	
	28	SNMPv2 & v3	Functional Verification	
	29	SSH	Functional Verification	
	30	SYSLOG	Functional Verification	
	31	TCP as per RFC 793,RFC 1122, RFC 3168, RFC 6093, RFC 6528	Functional Verification	
	32	TELNET	Functional Verification	
	33	TFTP	Functional Verification	
	34	UDP	Functional Verification	
	35	IGMP (Multicast Protocols) as per RFC 2113, RFC 2236 &PIM-SM as per RFC 2362, RFC 2588	Functional Verification	
	36	IRC	Declaration	
3.2.4		The firewall shall Support filtering for at least following proprietary Internet Services:[IDP]	Information	
	a)	LDAP as per RFC 4510	Functional Verification	
	b)	HTTPS	Functional Verification	
	c)	RADIUS	Functional Verification	
	d)	DIAMETER	Functional Verification	
3.2.5		The firewall shall support e-mail related filtering as follows:[IDP]	Information	

	a.	RDBMS	Declaration	
	b.	DB2	Declaration	
	c.	SQL	Functional Verification	
3.2.6		The firewall shall support for filtering multimedia applications such as VoIP, H.323, SIP, RTP, RTCP etc	Functional Verification	
3.2.7		The firewall shall support for filtering HTTP traffic based on URLs based on content string matches	Functional Verification	
3.2.8		The firewall System shall be based on stateful connection-oriented fire walling and support Static and Dynamic packet filtering	Declaration	
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	Functional Verification	
3.2.10		Web cache redirection: The Firewall shall support transparent redirection of HTTP traffic as per RFC 3040	Declaration	
3.3		**Security Services**	Information	
3.3.1		The firewall System shall provide the following security features	Information	
	a.	Prevent denial-of-service attacks	Functional Verification	
	b.	Java Applet Filtering to stop dangerous Java applications on a per-client or per-IP address basis	Functional Verification	
	c.	Support for unicast Reverse Path forwarding to prevent IP spoofing attacks	Functional Verification	
	d.	Prevent TCP SYN attacks	Functional Verification	
	e.	Prevent IP fragmentation attacks	Functional Verification	
	f.	Support for ICMP filtering with configurable threshold	Functional Verification	
	g.	UDP flood detection with configurable threshold using IPS	Functional Verification	
	h.	Detect Ping of Death	Functional Verification	
	i.	Detect Land attack	Functional Verification	
	j	Detect Win Nuke attack using IPS	Functional Verification	
	k.	Filter IP source route option	Functional Verification	

3.3.2		**TCP Security Services**	Information	
	i.	The Firewall shall support TCP stream reassembly and analysis	Functional Verification	
	ii.	The Firewall shall support TCP traffic normalization	Functional Verification	
	iii.	The Firewall shall support Flag and option checking	Functional Verification	
	iv.	The Firewall shall support TCP packet checksum verification	Functional Verification	
	v.	The Firewall shall support privacy, identity control feature and also provides transport layer security features	Functional Verification	
3.3.3		**Traffic Blocking**	Information	
	i.	i. The Firewall shall support protecting the port-80 misuse to block application such as Instant Messaging like Yahoo messenger	Functional Verification	
	ii.	The Firewall shall support Blocking of popular peer-to-peer protocols	Functional Verification	
3.3.4		**DDOS Attacks**	Information	
	i.	The Firewall shall protect from Distributed Denial of Service (DdoS) attacks	Functional Verification	
3.4		**Virtual Private Network**	Information	
	i.	The Firewall shall have Inbuilt support for IPSEC VPNs and SSL VPN functionality. It shall also support split tunneling VPN and client-based IPSec VPN tunnels	Lab Test-Refer Test 16 of compendium	
	ii.	IKE (internet Key Exchange) protocol keep alive shall be supported that allows the devices to detect a dead remote peer for IPSEC redundancy	Lab Test-Refer Test 16 of compendium	
	iii.	The platform shall use purpose-built hardware that is optimized for packet filtering and encryption	Declaration	
	iv.	The Firewall shall support DES, 3DES, AES encryptions algorithm	Functional Verification	
	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	Functional Verification	
	vi.	The VPN shall support external certificate authorities	Declaration	
	vii.	It shall support local certificate authority & shall support create/renew/Delete self signed certificate	Declaration	

	viii.	It shall be possible to apply bandwidth management policies on all traffic passing through the IPSec/L2TP/PPTP/SSL VPN tunnels	Declaration	
3.5		**Integrity: -** The firewall subsystem shall have the ability to detect data manipulation by any means using IPSec	Declaration	
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	Declaration	
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	Functional Verification	
3.5.3		The firewall System shall not affect the performance of the components (including servers) which it is protecting	Declaration	
3.5.4		Overload protection mechanism shall be available. System shall revert back to normal mode of operation when load is reduced	Declaration	
3.5.5		On power up the firewall shall use built-in system monitoring & diagnostics before going online to detect failure of hardware	Functional Verification	
3.5.6		Communication among the firewall system's components shall be secure	Declaration	
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	Declaration	
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	Information	
3.6.1		The firewall system shall have Inbuilt support for IPSEC VPNs and VPN functionality. The firewall shall also support split tunneling VPN	Functional Verification	
3.6.2		Extensive debugging capabilities to assist in hardware problem resolution shall be supported	Declaration	

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	Functional Verification	
3.6.4		The platform shall use hardware that is optimized for packet filtering and encryption	Declaration	
3.6.5		The platform shall support firewalling for VLAN (IEEE 802.1q).	Functional Verification	
3.6.6		The firewall system shall be capable of clustering multiple firewalls together into a redundant and highly available stateful configuration	Declaration	
3.6.7		The firewall system shall provide for a single default gateway IP address for all firewalls in a cluster	Declaration	
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	Functional Verification	
3.6.9		There shall be a means of connecting directly to the firewall system through a console connection	Functional Verification	
3.6.10		The firewall system shall have a facility to block any unencrypted means of access to the firewall except physical connection	Functional Verification	
3.6.11		The firewall system shall support application layer inspection of sessions	Functional Verification	
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	Functional Verification	
	a.	The firewall state engine shall support the passing of OSPF, BGP traffic and multicast packets in transparent mode	Functional Verification	
	b.	The firewall system shall support application layer inspection of sessions	Functional Verification	
	c.	The firewall system shall provide a means to define and modify existing services and state engine	Functional Verification	
3.7		**Updates**	Information	
3.7.1		The firewall System shall support TFTP/FTP for easy software upgrades over the network in a secure way	Functional Verification	
3.7.2		Firewall System shall support SNMP v3 as per RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414 and RFC 3826	Lab test -Refer Test 19 of the compendium	
3.8		**Logging**	Information	

3.8.1		Firewall System shall support Logging /Monitoring via Syslog. The firewall logging features shall include the following	Information	
	a.	The firewall logs shall contain information about the firewall policy rule that triggered the log using Firewall eMS/Manager	Functional Verification	
	b.	The firewall shall be capable of capturing detailed packet data to a log	Functional Verification	
	c.	The firewall logging shall not impact firewall performance	Declaration	
	d.	The firewall shall provide a means for synchronizing time between firewalls, the log server and the administration station using NTP	Functional Verification	
	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	Functional Verification	
	3.8.2	The firewall shall be able to send logs to different firewall log servers	Functional Verification	
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	Declaration	
3.8.4		The firewall shall be able to filter log data by user for AAA authenticated users	Functional Verification	
3.8.5		The firewall shall be able to consolidate log data for efficient reports using Firewall eMS/Manager	Functional Verification	
3.8.6		The firewall shall be able to consolidate log data for	Information	
	a.	Network services	Functional Verification	
	b.	Network resources	Functional Verification	
	c.	User/groups	Functional Verification	
	d.	Connection duration	Functional Verification	
	e.	Number of bytes transferred	Functional Verification	
	f	Blocked connections	Functional Verification	
	g	Source/Des. IP addresses	Functional Verification	
	h	Failed authentication attempts	Functional Verification	

	i	Date/Time	Functional Verification	
	j	Firewall identity	Functional Verification	
	k	Intrusion attempts	Functional Verification	
	l	Alert/error conditions	Functional Verification	
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	Functional Verification	
3.8.8		The log consolidator shall be able to use firewall objects/users for use in the consolidation policy using Firewall eMS/Manager	Declaration	
3.8.9		The firewall shall send log information to an external log server via an encrypted connection using FTP or syslog	Functional Verification	
3.9		**Reporting** It shall be Optional for the purchaser to have an integrated or separate reporting system	Information	
3.9.1		The firewall shall provide in-depth details on network traffic and activities.	Declaration	
3.9.2		Reporting software components shall support distributed environment/ installation	Declaration	
3.9.3		User level access restrictions shall be possible for accessing managing the components and generating reports	Functional Verification	
3.9.4		Remote management and generation of reports shall be possible	Functional Verification	
3.9.5		The firewall shall generate reports consisting of audit in easy to understand formats	Functional Verification	
3.9.6		The firewall shall support well-predefined and custom reports	Functional Verification	
3.9.7		The reports shall be available in different formats, e.g. CSV, PDFetc. Tendering authority shall provide the detail of report formats	Functional Verification	
3.9.8		The reports shall be automatically sent to e-mail, etc	Functional Verification	
3.9.9		The firewall shall provide a means for specifying thresholds and conditions for which it would send an alert	Functional Verification	

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	Declaration	
3.11.		**IPv6 Protocol Requirements**	Information	
3.11.1		The firewall shall support IPv6 as per RFC 2460, RFC 4861, RFC 4862and RFC 4443 routing in coexistence with IPv4 routing	Lab Test-Refer Test 16 of compendium	
3.11.2		IP Routing Protocols	Information	
	i.	RIPng for IPv6 as per RFC 2080	Lab Test-Refer Test 16 of compendium	
	ii.	OSPFv3 for IPv6 as per RFC 2740	Lab Test-Refer Test 16 of compendium	
	iii.	IPv6 Static Routing	Lab Test-Refer Test 16 of compendium	
	iv.	IPv6 Route Redistribution	Lab Test-Refer Test 16 of compendium	
3.11.3		**General IPv6 support**	Information	
	i.	IPv6 Address types: Unicast (Unique Local IPv6 address as per RFC 4193), Anicast and Multicast	Declaration	
	ii.	ICMPv6 as per RFC 2463	Functional Verification	
	iii.	IPv6 Neighbor Discovery as per RFC 2461	Lab Test-Refer Test 16 of compendium	
	iv.	IPv6 stateless auto configuration as per RFC 4862	Lab Test-Refer Test 16 of compendium	
	v.	IPv6 MTU path discovery as per RFC 1981	Lab Test-Refer Test 16 of compendium	
	vi.	IPv6 ping	Functional Verification	
	vii.	ICMPv6 redirect	Functional Verification	
	viii.	ICMPv6 rate limiting	Functional Verification	
	ix.	IPv6 neighbor discovery duplicate address detection	Declaration	

	x.	IPv6 default router preference as per RFC 2711	Lab Test-Refer Test 16 of compendium	
	xi.	IPv6 access control	Functional Verification	
	xii.	Syslog over IPv6	Functional Verification	
	xiii.	IP SLAs for IPv6	Declaration	
	xiv.	IPv6 Specification as per RFC 2460	Lab Test-Refer Test 16 of compendium	
	xv.	IPv6 Scoped Address Architecture as per RFC 4007	Declaration	
	xvi	ICMPv6 for IPv6 Specification as per RFC 4443	Lab Test-Refer Test 16 of compendium	
3.11.4		**IPv6 QoS**	Information	
	i.	Packet classification as per RFC 2474	Declaration	
	ii.	Traffic shaping	Declaration	
	iii.	Traffic policing	Declaration	
	iv.	MQC packet marking/re-marking as per RFC 2475	Declaration	
	v.	IPv6 QoS queuing	Lab Test-Refer Test 16 of compendium	
	vi.	Weighted random early detection (WRED)- based drop	Declaration	
	vii.	Assured Forwarding PHB Group shall be as per RFC 2597	Declaration	
	viii.	LAN switch shall support An Expedited Forwarding PHB as per RFC 2598	Declaration	
3.11.5		**IPv6 Services**	Information	
	i.	Standard access control lists for IPv6	Functional Verification	
	ii.	Secure Shell (SSH) support over IPv6	Functional Verification	
	iii.	IPv6 MIB support	Declaration	
	iv.	SNMP over IPv6	Functional Verification	
	v.	IPv6 IPSec VPN	Functional Verification	
	vi.	Stateless DHCPv6	Functional Verification	
	vii.	DHCPv6 prefix delegation	Functional Verification	
	viii.	DHCP for IPv6 relay agent	Functional Verification	
	ix.	DHCPv6 prefix delegation via AAA	Functional Verification	

	x.	DHCPv6 Server Stateless Auto Configuration	Functional Verification	
	xi.	DHCPv6 Client Information Refresh Option.	Functional Verification	
	xii.	DHCPv6 relay agent notification for prefix delegation	Functional Verification	
	xiii.	DHCPv6 relay- reload persistent interface ID option	Functional Verification	
	xiv.	DHCP - DHCPv6 Individual Address Assignment	Functional Verification	
	xv.	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) as per RFC 3315	Lab Test-Refer Test 16 of compendium	
	xvi.	DNS Extensions to Support IP Version 6 as per RFC 3596	Lab Test-Refer Test 16 of compendium	
	xvii.	DHCP IPv6 Prefix Delegation RFC 3633	Lab Test-Refer Test 16 of compendium	
	xviii.	DNS Configuration options for DHCPv6 as per RFC 3646	Lab Test-Refer Test 16 of compendium	
	xix.	Stateless DHCP Service for IPv6 as per RFC 3736	Lab Test-Refer Test 16 of compendium	
	xx.	IP Forwarding Table MIB as per RFC 4292	Lab Test-Refer Test 16 of compendium	
	xxi.	Management Information Base for the Internet Protocol as per RFC 4293	Lab Test-Refer Test 16 of compendium	
	xxii.	Dynamic Host Configuration Protocol version 6 (DHCPv6) options s as per RFC 3319	Lab Test-Refer Test 16 of compendium	
3.11.6		IPv6 Multicast	information	
	i.	IPv6 Multicast Listener Discovery (MLD) protocol versions 1 and 2	Functional Verification	
	ii.	IPv6 PIM sparse mode (PIM-SM)	Functional Verification	
	iii.	IPv6 PIM Source Specific Multicast (PIM-SSM)	Functional Verification	
	iv.	IPv6 multicast scope boundaries	Declaration	
	v.	IPv6 multicast MLD access group	Declaration	
	vi.	IPv6 multicast PIM accept register	Declaration	
	vii.	IPv6 multicast PIM embedded RP support	Declaration	
	viii.	IPv6 multicast RPF flooding of bootstrap router (BSR) packets	Declaration	
	ix.	IPv6 multicast routable address hello	Declaration	

		option		
	x.	IPv6 multicast SSM mapping for MLDv1 SSM	Declaration	
	xi.	IPv6 multicast IPv6 BSR—ability to configure RP mapping	Declaration	
	xii.	IPv6 multicast MLD group limits	Declaration	
	xiii.	IPv6 Multicast Address Assignments as per RFC 2375	Declaration	
	xiv.	IPv6 Multicast Listener Discovery (MLD) protocol, versions 1 and 2 as per RFC 2710	Lab Test-Refer Test 16 of compendium	
	xv.	MLDv2 for IPv6 as per RFC 3810 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address as per RFC 3956	Lab Test-Refer Test 16 of compendium	
4		**Interconnectivity & Interoperability**	Information	
4.1.		Firewall shall inter-work with existing Servers, Routers, LAN switches, etc as deployed in SP's IT/telecommunication infrastructure	Declaration	
4.1.1		It shall be a fully integrated multi-platform wide security solution	Declaration	
4.1.2		The firewall shall support 802.1Q Trunking.	Lab Test-Refer Test 16 of compendium	
4.1.3		The firewall System shall support the following minimum performance levels	Information	
	a)	Wire rate throughput at all interfaces;	Declaration	
	b)	Stateful failover shall be supported to eliminate session loss;	Declaration	
	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);	Declaration	
	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);	Declaration	
	e)	The Firewall System Chassis shall be rack mountable in a 19" rack	Physical Verification	

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. Tendering authority shall provide the actual interface requirement. The firewall system can be offered for type approval under one or more categories as per the clause.	Declaration	
		10/100 Interface	Lab Test-Refer Test 1,10 of the compendium	
		1G Electrical Interface	Lab test -Refer Test 1,10 of the compendium	
		1G Optical Interface	Lab test - Refer Test 2,11,12,13 of the compendium	
		10GE interface	Lab test - Refer Test 2,11,12,13 of the compendium	
4.3.		**User interface**	Information	
4.3.1		Firewall System shall support management via web user interface (HTTP and HTTPS), Command Line interface (Console), Secure Command Shell (SSH).	Functional Verification	
4.3.2		It shall be possible to monitor firewalls from the central site	Declaration	
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	Functional Verification	
	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	Functional Verification	

	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	Functional Verification	
	c.	The firewall EMS shall provide a means for exporting the firewall rules set and configuration to a text file	Functional Verification	
	d.	The firewall shall support external user database authentication for firewall admin user	Functional Verification	
	e.	Any changes or commands issued by an authenticated user shall be logged to an external database using AAA	Functional Verification	
	f.	Remote network access to the firewall shall only be possible through the outside interface	Functional Verification	
	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	Functional Verification	
	h.	There shall be a means of connecting directly to the firewall through an encrypted connection to perform troubleshooting and packet captures	Functional Verification	
	i.	There shall be a means of connecting directly to the firewall through a console connection	Functional Verification	
	j.	The EMS shall allow for a hierarchical architecture for rules set administration and viewing of firewall configurations	Functional Verification	
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	Declaration	

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.	Declaration	
5		**Quality of Service**	Information	
5.1.		**Qualitative Requirements (QR)**: The Firewall System shall meet the following qualitative requirements	Information	
5.1.1		The supplier / manufacturer shall manufacture with international quality standards ISO 9002 for which the manufacturer shall be duly accredited. The quality plan describing the quality assurance system followed by the manufacturer shall be required to be submitted	Declaration	
5.1.2		The equipment locally manufactured in India shall be as per guidelines vide Documents No. QM 118, QM 205, QM 206, QM 210 and QM 301	Declaration	
5.1.3		The equipment shall meet the environmental requirements as per category A of QM-333/Issue-1/Sept 1990	Declaration	
5.1.4		All components used shall be as per approval procedures prescribed by BSNL in document QA QM – 324	Declaration	
5.1.5		Marking and identification of the equipment, sub assemblies, PCBs etc. shall be as per guidelines given in Para 5.1.7 Quality Assurance Telecom Document QM 351/Issue 2 /Jan.'95	Declaration	
5.1.6		The MTBF (Mean Time Between Failure) and MTTR (Mean Time To Restore) predicted and the manufacturer shall furnish observed values along with calculations	Declaration	
6		EMI/EMC Requirements	Test Report of Accredited Lab	
7		Safety Requirements	Information	

7.1		The operating personnel shall be protected against shock hazards as per **IS 8437 (1993)** – Guide on the effects of current passing through the human body (equivalent to IEC publications 60479-1 (1984). The manufacturer / supplier shall submit a certificate in respect of compliance to these requirements.	Declaration	
7.2		The equipment shall conform to IS 13252 (2003)- “Safety of information technology equipment including electrical business equipment” [equivalent to IEC publication 60950 {2001}] and IS 10437 {1986} “Safety requirements of radio transmitting equipments” [equivalent to IEC publication 60215]. The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements”	Declaration	
8		Security Requirements	Information	
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	Declaration	
8.2		**Management and reporting**	Information	
8.2.1		**Access Control** – The firewall subsystem shall control information and access through predetermined security policy.	Declaration	
	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.	Declaration	
	b)	The firewall subsystem shall allow data communication only by authenticated network resources.	Declaration	
	c)	The firewall shall not support any unencrypted means of access to the firewall other than physical console access	Functional Verification	

	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.	Functional Verification	
	e)	The firewall System shall support Telnet client functionality. It shall be possible to deactivate Telnet 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 telnet session shall be configurable.	Functional Verification	
8.3		The firewall System shall support Remote login as per the latest guidelines issued by DoT.	Declaration	
8.4		The Firewall shall meet the security certification requirements mandated by DoT from time to time.	Declaration	
9		**Other Mandatory Requirements :** The Firewall shall meet the following mandatory requirements	Information	
9.1		**Engineering Requirements:** The Firewall System shall meet the following engineering requirements	Information	
9.1.1		The equipment shall adopt state of the art technology.	Functional verification	
9.1.2		The manufacturer shall furnish the actual dimensions and weight of the equipment.	Declaration	
9.1.3		All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations	Declaration	
9.1.4		All LAN cabling shall be of Gigabit Ethernet ready	Declaration	
9.1.5		The equipment shall have adequate cooling arrangements	Declaration	
9.2		**Operational Requirement (OR)**: The Firewall System shall meet the following Maintenance & operational requirements	Information	
9.2.1		The equipment shall be designed for continuous operation	Declaration	
9.2.2		The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sea level	Declaration	
9.2.3		The design of the equipment shall not allow plugging of a module in the wrong slot or upside down	Declaration	
9.2.4		The removal or addition of any cards shall not disrupt traffic on other cards	Declaration	

9.2.5		In the event of a full system failure, a crash dump shall be supported for analysis and problem resolution	Functional verification	
9.2.6		A power down condition shall not cause loss of connection configuration data storage in high availability mode	Functional verification	
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	Declaration	
9.3		Other Requirements	Information	
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	Functional verification	
9.3.2		Wherever, the standardized documents like ITU-T, QA and TEC documents are referred, the latest issue and number with the amendments shall be applicable	Information	
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	Information	
	a.	The equipment shall be able to function over the range specified in the respective chapters, without any degradation in performance	Declaration	
	b.	The equipment shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity.	Declaration	
	c.	The derived DC voltages shall have protection against short circuit and overload	Declaration	
9.3.4		The equipment shall have	Information	
	a.	Proper earthing arrangement	Declaration	
	b.	Protection against short circuit / open circuit	Declaration	
	c.	Protection against accidental operations for all switches / controls provided in the front panel	Declaration	
	d.	Protection against entry of dust, insects and lizards	Declaration	
10		**Desirable Requirements / Tendering Information**	Information	

10.1		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.	Information	
10.2		**Optional Firewall Services:**	Information	
10.2.1		**HTTP security services:**	Information	
	a.	The Firewall shall support RFC compliance	Declaration	
	b.	The Firewall shall support protocol anomaly detection	Functional Verification	
	c.	The Firewall shall support protocol state tracking	Functional Verification	
	d.	The Firewall shall support MIME type validation	Functional Verification	
	e.	The Firewall shall support Uniform Resource Identifier (URI) length enforcement	Functional Verification	
10.2.2		FTP security services:	Information	
	a.	The Firewall shall support Protocol anomaly detection	Functional Verification	
	b.	The Firewall shall support Protocol state tracking	Functional Verification	
	c.	The Firewall shall support NAT and PAT for FTP security services	Functional Verification	
	d.	The Firewall shall support Dynamic Port opening & closing	Functional Verification	
	e.	The Firewall shall have the capability to enforce what operations users and groups can perform within FTP sessions	Functional Verification	
10.3		The firewall shall support IEEE 802.3ad link aggregation control protocol (LACP)	Functional Verification	
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	Information	
10.4.1		Functional requirement of IDP is divided into following:	Information	
	a.	Architecture	Information	
	b.	Incident Monitoring and Detection	Information	
	c.	Incident Response	Information	
	d.	Configuration	Information	
	e.	Management	Information	
	f.	Security	Information	
	g.	Performance	Information	

	h.	Updates and Technical Support	Information	
10.4.2		**Architecture**	Information	
	i.	IDP shall detect and actively prevent attacks in real-time and shall be placed in INLINE mode	Functional Verification	
	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	Functional Verification	
	iii.	The installation of the IDP shall not require changes to the network infrastructure or affect the MTBF of the network in any way	Functional Verification	
	iv.	IDP shall allow working in failover mode	Functional Verification	
	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	Functional Verification	
	vi.	Attack Isolation at multi-gigabit speeds, ensures the availability of mission critical traffic even while under attack	Functional Verification	
	vii.	IDP devices shall block only the attack session without effecting service to legitimate clients	Functional Verification	
	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	Functional Verification	
	ix.	IDP system shall have Centralized configuration, management & Reporting station with provision for secure communication & authentication between IDP & management station	Functional Verification	
	x.	IDP performance shall not reduce by enabling Layer 7 attacks filters	Functional Verification	
	xi.	The IDP shall be able to get synchronized to a network time source through Network Time Protocol or simple Network Time Protocol	Functional Verification	
	xii.	The IDP shall be scalable and re-configurable, and its licensing shall be such so as not to affect network expansion	Functional Verification	

	xiii.	IDP system if installed in bridge mode shall be transparent and invisible to network (Applicable only if Bridge mode deployment available)	Functional Verification	
10.4.3		The IDP shall Support filtering for at least following proprietary Internet Services:	Information	
	1	NetMeeting	Functional Verification	
	2	PC-Anywhere	Declaration	
	3	SIP-Messenger	Functional Verification	
	4	SAMBA	Declaration	
	5	SKYPE, HANGOUT, GOOGLE-TALK etc	Functional Verification	
10.4.4		The IDP shall support e-mail related filtering as follows:	Information	
	a)	Lotus Notes based on SMTP	Declaration	
	b)	Microsoft Exchange based on SMTP	Functional Verification	
10.4.5		Incident Monitoring and Detection	Information	
	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	Functional Verification	
	ii.	Protocol analysis (for protocol like FTP, HTTP, SMTP, POP3, IMAP, TELNET etc.) and pattern matching shall be supported by IDP.	Functional Verification	
	iii.	IDP shall support pattern-based signatures having a strong sense of context, so that false alarms/incident detections are minimized	Functional Verification	
	iv.	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	Functional Verification	
	v.	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	Functional Verification	
	vi.	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	Functional Verification	

	vii	IDP shall able to detect & block known P2P based instant messanging application like skype & known chat application like WLM, Rediffbol etc	Functional Verification	
	viii.	IDP shall able to detect VoIP (like SIP) data and shall be able to block the same	Functional Verification	
	ix.	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	Functional Verification	
	x.	IDP shall be able to detect and shall be able to stop any Suspicious Activity	Functional Verification	
	xi.	Creation of User-specified signatures shall be possible based upon contents i.e. string matching etc	Functional Verification	
	xii.	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).	Functional Verification	
	xiii.	IDP shall support signatures tuning to match the operational requirements of the customer network so that false policies are minimized	Functional Verification	
	xiv.	IDP shall support help system that describes the incidents in adequate detail, providing sufficient information about	Information	
	a.	The incident	Functional Verification	
	b.	The potential damage	Functional Verification	
	c.	Possible false positives	Functional Verification	
	d.	The systems affected	Functional Verification	
	e.	How to respond immediately upon detection of the incident	Functional Verification	
	f.	How to remove the vulnerability associated with the incident	Functional Verification	
	xv.	IDP shall be configured to focus on the incidents that pose the greatest risk to the network	Functional Verification	
	xvi.	IDP shall detect the malicious activity event in fragmented and de-fragmented packets	Functional Verification	
	xvii.	IDP shall provide Stateful Operation	Functional Verification	
	a.	TCP Reassembly	Functional Verification	

	b.	IP De-fragmentation	Functional Verification	
	c.	Bi-directional Inspection	Functional Verification	
	e.	Access Lists	Functional Verification	
	xviii.	IDP shall provide Signature Detection for at least 3500 (more than 1500 vulnerability based) Vendors Signature Database and 5,000 User Defined Signatures	Functional Verification	
	xix.	IDP shall have Anomaly Detection Mechanism for Protocol Anomalies and Sampling Based Traffic Anomalies to prevent against Day Zero or Unknown Attacks	Functional Verification	
	xx.	The IDP shall provide the capability to annotate incidents recorded in the database	Functional Verification	
	xxi.	IDP shall provide Intrusion Detection & Prevention for at least following Applications	Information	
	a.	Web Protection: IIS and Apache vulnerabilities, protection for web applications such as CGI, Cold Fusion, FrontPage, SQL Injection and cross-site scripting	Functional Verification	
	b.	Mail Server Protection: including protection from mail based worms and exploits of mail protocols (POP3, IMAP and SMTP) vulnerabilities	Functional Verification	
	c.	Remote access protection: Telnet vulnerabilities and FTP server protection	Functional Verification	
	d.	SNMP Vulnerability	Functional Verification	
	e.	Worms & Viruses	Functional Verification	
	f.	SQL server protection: prevention of the exploitation of vulnerabilities found in SQL implementation from miscellaneous vendors	Functional Verification	
	g.	DNS protection: prevents the exploitation of vulnerabilities found in DNS implementation of various vendors	Functional Verification	
	h.	Backdoor & Trojans: prevents the backdoor outbound and inbound communications, and prevent the network from being controlled remotely	Functional Verification	

	i.	Brute Force Protection - prevents the password guessing attacks (brute force) in miscellaneous services	Functional Verification	
	j.	Protection against Mass mailing worm and viruses	Functional Verification	
	xxii.	IDP shall provide full Application Security Intelligence including	Information	
	a.	IP spoofing protection	Functional Verification	
	b.	DoS and DDOS protection	Functional Verification	
	c.	Protocol Anomaly protection	Functional Verification	
	d.	Traffic Anomaly Protection	Functional Verification	
	e.	TCP Reassembly, normalization and de-fragmentation	Functional Verification	
	f.	Syn flood protection	Functional Verification	
	g.	Backdoor /Bi-directional inspection for attack traffic	Functional Verification	
	h.	Stateful signature inspection	Functional Verification	
	xxiii.	IDP Shall Protect against various DOS & DDOS attacks as follows	Information	
	a.	One Packet Attack Protection	Functional Verification	
	b.	Protection against TCP, UDP & ICMP Flood	Functional Verification	
	c.	SYN Flood	Functional Verification	
	d.	Layer 2 attacks such as DHCP Flooding prevention	Functional Verification	
10.4.6		**Incident Response**	Information	
	i.	IDP shall be able to show alarms on the management console, upon detection of an incident	Functional Verification	
	ii.	IDP shall be able to send an SNMP trap to the network upon detection of an incident	Functional Verification	
	iii.	IDP shall be able to log a summary of an incident to persistent data storage	Functional Verification	
	iv.	IDP shall be able to terminate a TCP/UDP session upon detection of malicious activity. IDP shall be capable to kill intrusion attempts	Functional Verification	
	v.	Shall detect attack due to URL decoding vulnerabilities	Functional Verification	
	vi.	IDP shall be capable of	Functional	

			Verification	
	a.	Block attacks in real time	Functional Verification	
	b.	Drop Attack Packets	Functional Verification	
	c.	Reset/ drop Connections	Functional Verification	
	d.	Packet Logging	Functional Verification	
	e.	IDP shall be capable of Attack Isolation	Functional Verification	
	f.	Access Control of traffic per application ports and networks allows a predefined set of applications only and denies all other types of traffic	Functional Verification	
	g.	Attack isolation and protection against unknown flooding attacks	Functional Verification	
10.4.7		**Configuration**	Information	
	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	Functional Verification	
	ii.	IDP shall provide creation of multiple IDP policy for different zone instead of blanket policy at interface level	Functional Verification	
	iii.	IDP shall support help system providing a detailed description of the attack signature that is selected	Functional Verification	
	iv.	The interface shall allow attack signatures to be activated or deactivated via check-box selection. (optional)	Functional Verification	
	v.	The administrator, from the management console, shall be able to specify the response to each pre-defined event	Functional Verification	
	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	Functional Verification	
	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.	Functional Verification	

	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	Functional Verification	
	ix.	IDP shall be capable of attack policy customization	Functional Verification	
	x.	IDP shall have provision to analyze and identify the ingress point of attack	Functional Verification	
10.4.8		**IDP user interface**	Information	
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	Information	
	a.	HTTPS	Functional Verification	
	b.	SSH	Functional Verification	
10.4.8.3		**IDP user interface shall provide Graphical User Interface (GUI) as follows**	information	
	i.	IDP shall be able to graphically depict both suspicious activity and normal network activity	Functional Verification	
	ii.	The graphical interface shall be easy to use for by operators and shall require no special technical knowledge	Functional Verification	
	iii.	The graphical interface shall use an iconic display to alert operators to important occurrences	Functional Verification	
	iv.	The graphical interface shall be able to display summary information sorted by source address (initiator), destination address (target), or event type	Functional Verification	
	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	Functional Verification	
	vi.	The graphical interface shall be able to consolidate multiple event occurrences into a single alarm		
10.4.8.4		**Data Management**	Information	
	i.	IDP shall have comprehensive database with more than 3500 attack(of them atleast 1500 vulnerabilities based) signatures	Functional Verification	

	ii.	IDP shall support data management capabilities provide critical information required for risk assessment and decision-making	Functional Verification	
	iii.	IDP shall be capable of prioritization of security event data for quick and easy threat assessment	Functional Verification	
10.4.8.5		**IDP Reports**	Information	
	i.	IDP shall have built-in customized report generation capability e.g. excel, text, HTML, etc., as per SP's requirement which shall be specified at the time of tendering	Functional Verification	
	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	Functional Verification	
	iii.	It shall be possible to generate multiple forms of reporting suitable for all technical levels	Functional Verification	
	iv.	IDP shall support reports that may be exported to different formats, such as excel, HTML or a Word document etc.	Functional Verification	
	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	Functional Verification	
	vi.	IDP shall provide drill down reports based on Real Time attack statistics for following	Information	
	a.	Security event risk level	Functional Verification	
	b.	Date/time	Functional Verification	
	c.	Subnets (Networks/ IP Address)	Functional Verification	
	d.	Event name	Functional Verification	
	e.	Source IP	Functional Verification	
	f.	Destination IP	Functional Verification	
	g.	User Identity	Functional Verification	
	h.	Response taken	Functional Verification	
	i.	Severity	Functional Verification	

	j.	Top attack types	Functional Verification	
	k.	Attack groups	Functional Verification	
	l.	Top-10 Source of Attacks	Functional Verification	
	m.	Top-10 Destination of attacks	Functional Verification	
	vii.	Management station shall be able to show Graph with number of attacks coming from different networks	Functional Verification	
	viii.	Provision to automatically generate & email reports daily, weekly or monthly to predefined email addresses.(optional)	Functional Verification	
	ix.	Provide reports in different formats like excel sheet, Word, HTML etc	Functional Verification	
	x.	IDP shall provide alerts/ notify by following	Information	
	a.	SNMP trap	Functional Verification	
	b.	Logging	Functional Verification	
	c.	Syslog	Functional Verification	
10.4.9		**Security - IDP**	Information	
	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	Functional Verification	
	ii.	The IDP shall monitor its internal application modules and notify the management station when a module goes off line unexpectedly	Functional Verification	
	iii.	The IDP and management console shall be protected against intentional or accidental abuse, unauthorized access and loss of communication	Functional Verification	
	iv.	The management console shall have the feature of idle time disconnection.(optional)	Functional Verification	
10.4.10		**Performance IDP**	Information	
	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	Functional Verification	

	ii.	IDP shall handle traffic bursts gracefully, switching to sampling mode until the traffic levels return to a consistent level.(optional)	Functional Verification	
10.4.11		**IDP Updates**		
	i.	The IDP software and its attack signature database shall be updated at least once in a month	Functional Verification	
	ii.	Update attack signatures, rule bases and service releases via the Internet or with Version Upgrades	Functional Verification	
	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	Functional Verification	
	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	Functional Verification	
	v.	IDP Shall support 24/7 Security Update Service	Functional Verification	
	vi.	IDP Shall support Real Time signature update	Functional Verification	
	vii.	IDP shall support for customized signatures	Functional Verification	
	viii.	IDP Shall support Automatic signature synchronization from database server on Internet	Functional Verification	
	iv.	The IDP shall provide for regular updates to the signature database	Functional Verification	
10.5		**Anti-Virus**		
10.5.1		The Firewall shall be deployed as Gateway Scanning engine	Functional Verification	
10.5.2		The Firewall shall be able to scan traffic without acting as a mail server in case of mail protocols	Functional Verification	
10.5.3		The FIREWALL shall be able to operate in transparent mode.(Applicable if bridge mode is supported)	Functional Verification	
10.5.4		The Firewall shall protect HTTP, SMTP, FTP, POP3 and IMAP protocols	Functional Verification	
10.5.5		The Firewall shall support both stream based Anti Virus scanning and file based Anti Virus scanning	Functional Verification	
10.5.6		The Firewall shall have Signature and Behavioral antivirus engine	Functional Verification	

10.5.7		The Firewall shall perform both inbound and outbound inspection	Functional Verification	
10.5.8		The Firewall shall have 2.5+ million virus signatures for comprehensive coverage	Functional Verification	
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	Functional Verification	
10.5.10		The Firewall shall stop zero day variants	Functional Verification	
10.5.11		The Firewall shall support Spam and Virus filtering and shall have its own Spam/Virus list that shall be updated automatically	Functional Verification	
10.5.12		The Firewall shall be multi-threaded	Functional Verification	
10.5.13		The Firewall shall be able to scan all traffic or specific extensions as defined by the administrator	Functional Verification	
10.5.14		The Firewall shall support an Allow and Deny list of valid IP/Domains to allow/deny relaying for	Functional Verification	
10.5.15		The Firewall shall be able to block attachment by file name and extension	Functional Verification	
10.5.16		The Firewall shall support Recursive Analysis on messages and Compressed files	Functional Verification	
10.5.17		The Firewall shall have separate inbound and outbound virus and content. Scanning policies	Declaration	
10.5.18		The Firewall shall support real mode for HTTP virus scanning	Functional Verification	
10.5.19		The Firewall shall provide option to bypass scanning for specific HTTP traffic	Functional Verification	
10.5.20		The Firewall shall scan http traffic based on username, source/destination IP address or URL based regular expression	Functional Verification	
10.6		**Documentation**	information	
10.6.1		**Documentation:** This section 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:	Information	
	a)	System description documents	Information	
	b)	Installation, Operation and Maintenance	Information	

		documents		
	c)	Training documents	Information	
	d)	Repair manual	Information	
10.6.2		**System description documents:** The following system description documents shall be supplied along with the system.	Information	
	a)	Over-all system specification and description of hardware and software.	Document Verifications	
	b)	Equipment layout drawings.	Document Verifications	
	c)	Cabling and wiring diagrams.	Document Verifications	
	d)	Detailed specification and description of all Input / Output devices	Document Verifications	
	e)	Adjustment procedures, if there are any field adjustable units.	Document Verifications	
	f)	Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification.	Document Verifications	
10.6.3		**System operation documents:** The following system operation documents shall be available.	Information	
	a)	Installation manuals and testing procedures.	Document Verifications	
	b)	Precautions for installation, operations and maintenance	Document Verifications	
	c)	Operating and Maintenance manual of the system.	Document Verifications	
	d)	Safety measures to be observed in handling the equipment	Document Verifications	
	e)	Man-machine language (command set) manual.	Document Verifications	
	f)	Fault location and trouble shooting instructions including fault dictionary.	Document Verifications	
	g)	Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement.	Document Verifications	
	h)	Emergency action procedures and alarm dictionary.	Document Verifications	
10.6.4		**Training Documents**	Information	
	a)	Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available.	Document Verifications	

	b)	Any visional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be provided immediately following the issue of such updates.	Document Verifications	
	c)	The structure and scope of each document shall be clearly described.	Document Verifications	
	d)	The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.	Document Verifications	
	e)	All diagrams, illustrations and tables shall be consistent with the relevant text.	Document Verifications	
10.7		**Installation**	Information	
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.	Declaration	
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.	Declaration	
10.7.3		All installation materials, consumables and spare parts to be supplied.	Declaration	
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.	Declaration	
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.	Declaration	
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.	Declaration	
10.7.7		Special tools required for wiring shall be provided along with the equipment	Physical Verification	

10.8		**Tendering authority shall specify**	Information	
	i.	Firewall category/ies and corresponding Interface requirement	Information	
	ii.	Requirement of HTTP and FTP security Services as per clause 10.2	Information	
	iii.	Requirement of Integrated Reporting system as per clause 3.9	Information	
	iv.	Link Aggregation requirement as per clause 10.3	Information	
	v.	Requirement of Intrusion detection and Pretension system integrated with the Firewall [Single Box] as per clause 10.4	Information	
	vi.	Requirement of Integrated antivirus as per clause 10.5	Information	
	vii	Requirement of IDP Reports as integrated with the system as per clause 10.4.8.5	Information	
	viii.	Documentation Requirements as per clause 10.6	Information	
	ix.	Installation requirements as per clause 10.7	Information	
10.9		**Minimum Equipments Required for Type Approval**	Information	
	i.	One Firewall of the offered category and interfaces as per the clause 4.2	Information	
	ii.	It is optional for offering the optional features as clause 10.8.	Information	
	iii.	Type approval Certificate shall indicate	Information	
	a.	Category of Firewall	Information	
	b	Optional features offered for testing as per clause 10.8	Information	