Comments on Revision of Test Guide Titled "Unified Threat Management (UTM)"

(Draft Test Guide Standard No. TEC 49121:2025)

Name of

Manufacturer/Stakeholder:

Organization:

Contact details:

Clause No.	Clause	Comments	Other Remarks, if any

Note: The comments on the revision of Test Guide titled "Unified Threat management (UTM)" may be provided in the above format vide Email to adic1.tec@gov.in and diri.tec@nic.in

अनंतिम टेस्ट गाइड
टीईसी ४९१२१:२०२५

(सं: टीईसी/टीजी/आईटी/यूटीएम- ३१०/०२ मार्च-२०१८)

PROVISIONAL TEST GUIDE

TEC 49121:2025

(Earlier No. TEC/TG/IT/UTM-310/02 Mar-2018)

for

संयुक्त थ्रट प्रबंधन

Unified Threat Management (UTM)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलालभवन, जनपथ, नई दिल्ली–११०००१, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release 03: June, 2025

FOREWORD

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

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

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

ABSTRACT

This Test Guide of testing pertains specifies the TSTP conversion to Test Guide of Unified Threat Management which is intended to be deployed by various service providers to secure their IT/Telecommunication infrastructure.

CONTENTS

दूरसंचार अभियांत्रिकी केंद्र / Telecommunication Engineering Centre
(दूरसंचार विभाग) / (Department of Telecommunications)
खुर्शीद लाल भवन, जनपथ, नई दिल्ली-११०००१ / Khurshid Lal Bhawan, Janpath, New Delhi-110001.

File No. 7-3/2024-IT/TEC/GR-R3 Date: 21-05-2025

Information Sheet

S.No.	Item	Comments/Remarks by Division
1	Standard Document No. (Erstwhile GR/IR/SR)	*TEC 49120:2025*
2	Name of Product/Equipment/Service	*Unified Threat Management (UTM)*
3	Approval (Type/Interface/CoA/Others)	*Type Approval*
4	Group/Division	*Information Technology (IT)*
5	Test Guide (Erstwhile TSTP) Status (Available-AV, Not Available-N/AV, Not Required-NR)	*AV*
6	If Available Test Guide No.	*TEC 49121:2025*
7	Man - Hours	*450 Hrs*
8	Category (I to X)	*Cat IV*
9	If Standard document supersedes an old Standard (Change in Issue) i. Old document No. ii. Old document ceases to exist on iii. Incremental test schedule /procedure iv. Incremental Man – Hours v. Incremental Category (mention if different from sl.no.7)	*Yes* *TEC/GR/IT/UTM-010/02/Mar-18* *01.03.2025* *N/A* *N/A* *N/A*
10	Amendment/Errata/Addendum issued if any with date i. Incremental Testing ii. Incremental Man Hours iii.	*N/A*

	Incremental Category	
11	Decentralization Status (Yes/No)	*Centralized*
12	Availability of document in soft copy (Yes/No) Soft Copy Status for i. Standard Document	*Yes (available on TEC website tec.gov.in/standards-specifications)*
	i. Test Guide(erstwhile TSTP)	*Yes (available on TEC website tec.gov.in/standards-specifications)*
	iii. Field Trial Observation Schedule	*Not Available*
	iv. Incremental Testing	*N/A*
	v. Amendment/Errata/Addendum (Soft copy to be sent to RC Division)	*N/A*
13	. Field Trial Required (Yes/No), if yes then a) Field Trial observation schedule status (AV, N/AV, NR) b) Field Trial Period	*No*
14	Whether trader is eligible for approval certification sought (Yes/No)	*Yes*
15	Special Remarks, if any	

Signature----------

Name & Designation----------

Copy to:

1. DDG (RC), TEC
2. ADG (Doc.), TEC for circulation to all RTECs

A. HISTORY SHEET

Sl. No.	TSTP No.	Equipment/Interface	Issue
1.	Original GR No.: TEC/I/UTM/2009-10/01/430/JAN 2011 GR for UNIFIED THREAT MANAGEMENT.	First edition of GR for the UNIFIE D THREAT MANA GEMENT	Original GR No.: TEC/I/UTM/2009-1001/430/JAN 2011 GR for UNIFIED TREAT MANAGEMENT.
2.	Revision (First): TEC/TG/IT/UTM-310/02/MAR-18	Second edition with technological updates. The following major changes done. a. Bridge mode is made mandatory, b. IPV6 is made mandatory, c. New EMS standard reference is given, Additional category (Cat E) with 10G interfaces and 2,000,000 concurrent session	Revision (First): TEC/GR/IT/UTM-01/02/MAR-18
3.	TEC 49121:2025	Conversion of TSTP to Test Guide	Revision: TEC 49121:2025

B. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of Unified Threat Management ***for*** telecommunications network (UTM) as per TEC Standard No. 49120:2025.

C. General information:

Sl.no	General Information	Details *(to be filled by testing team)*	
1	Name and Address of the Applicant		
2	Date of Registration		
3	Name and No. of GR/IR/Applicant' s Spec. against which the approval sought		
4	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
5	Any other relevant Information:-		

D. Testing team: *(to be filled by testing team)*

S.No.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the Test Instruments:

	Name of testing instrument	**Make /Model** *(to be filled by testing*	**Validity of calibration** *(to be filled by testing team)*
1			
2			
3			
4			
5			
6			
7			
8			

F. Equipment Configuration Offered: *(to be filled by testing team)*

a. <Equipment/product name> Configuration:

	Item	Details	

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

b. <Other equipment name> Configuration:

	Item	Details	

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

G. Equipment/System Manuals: *(to be filled by testing team)*

Availability of Maintenance manuals, Installation manual, Repair manual & User Manual etc. (Y/N)

H. Clause-wise Test Type and Test No.:

Functional Test – Any test or inspection performed to showcase the functionality mentioned in the clause. Functional Test may be performed to test the feature / functionality mentioned in the clause. For some clauses specific methodology is mentioned and for other clauses testing can be done as per original manufacturer suggested procedures for proving the functionality / feature mentioned. For all the functional tests, Figure-1 of section I may be referred to.

Physical Verification – Any test where functionality / feature is proven by physically inspecting the equipment / device / GUI.

Documentation – Original equipment manufacturer's publically available documentation verifying or proving the feature / functionality / parameter mentioned in the clause.

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)**
1.1		Scope: This document specifies the Generic Requirements of Unified Threat Management which is intended to be deployed by various service providers to secure their IT/Telecommunication infrastructure.	Information	

1.2		UTM (Unified Threat Management) is a security appliance that unifies and integrates multiple security features onto a single hardware platform. The Appliance requires network firewall capabilities, network intrusion detection and prevention, gateway antivirus and anti-spam, and content filtering features etc. This document contains the detailed functional and technical requirements of a UTM, which shall be deployed by Service Provider to provide security for the installed IT infrastructure (equipment and servers, etc)/telecom network.	Information	
2.1		The UTM Appliance shall have following features on a single hardware platform:	Information	
	1	Firewall with stateful packet inspection	Declaration	
	2	Intrusion Detection & Prevention	Declaration	
	3	Content Identification & Filtering	Declaration	
	4	Gateway Level Anti-virus	Declaration	
	5	Gateway level Anti-spam	Declaration	
	6	IPSec & SSL VPN	Declaration	
	7	Bandwidth Management	Declaration	
	8	Multi-Link Manager (Optional)	Declaration	
	9	Internet Access Management (Optional)	Declaration	

	10	Reporting.	Declaration	
2.2		Firewall System is one of the protection mechanisms available for providing network security. It filters out the unauthorized traffic from entering into SP' s network. The Firewall also does not allow exiting of unauthorized traffic from the SP' s network. The Intrusion Detection is part of security system designed to monitor all the data flowing from and into the IP network which could be an intranet or a Service Providers network. The IDS silently reads all the data traversing the network and takes action on the basis of configured policies.	Information	
2.3		The Intrusion Prevention System (IPS) does in line and stealth monitoring with capability to accept or deny the traffic emerge.	Information	
2.4		Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Anti-spam refers to any software, hardware or process that is used to combat the proliferation of spam or to keep spam from entering a system.	Information	
3.1		**UTM Firewall**		

3.1.1		The UTM Firewall shall support any valid Certification Authority (CA) server. Purchaser to specify.	Declaration	
3.1.2		The UTM Firewall architecture shall be able to define a single, integrated security policy distributed across multiple UTMs and managed remotely from the central place. The architecture shall be able to give central integration, configuration and management for the UTM.	Declaration	
3.1.3		The UTM Firewall shall be able to get configured as an application gateway and as a set of filtering mechanism. The UTM shall be flexible to implement the appropriate network security architecture.	Declaration	
3.1.4		The UTM Firewall shall be appliance based with dedicated hardware designed for networking and security services	Declaration	
3.1.5		The UTM Firewall shall not use any of the **Commercial, off-the-shelf** (**COTS**)Operating system.	Declaration	
3.1.6		The UTM Firewall shall be able to be deployed in a bridge mode (Fig. 1 b) with minimum disruption in the current network topology.	Declaration	
3.1.7		As shown in figure 1a the UTM System architecture, deployed in Gateway mode, shall be able to divide the network into at least 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.	Functional verification	
	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.	Functional verification	
	c	**Open Zone –** These are open zones containing Remote Access Servers, Routers**.** The UTM Firewall shall support creation of more zones and shall be site configurable to be included in any of the zone. 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.	Functional verification	
3.1.8		The UTM Firewall shall be able to filter packets based on the following criterion:	Information	
	a	Source and destination IP address	Functional verification	
	b	Source and destination IP address range (subnet)	Functional verification	

	c	User Identity	Functional verification	
	d	Protocol type	Functional verification	
	e	Port number (Source Port, Destination port)	Functional verification	
	f	Custom defined	Functional verification	
	g	Fragments	Functional verification	
	h	Acknowledgement bits (Optional)	Functional verification	
	i	Transmission Control Protocol (TCP) sequence number (Optional)	Functional verification	
	j	TCP flags (Optional) The UTM shall Support filtering for at least following Internet Services (List is illustrative;): Purchaser to specify Standard Services:	Functional verification	
	1	AH	Declaration	
	2	DHCP	Declaration	
	3	DNS	Declaration	
	4	ESP	Declaration	
	5	FINGER	Declaration	

	6	FTP	Declaration	
	7	Active FTP	Declaration	
	8	Passive FTP	Declaration	
	9	GOGHER	Declaration	
	10	GRE	Declaration	
	11	H323	Declaration	
	12	HTTP	Declaration	
	13	ICMP_ANY	Declaration	
	14	IKE	Declaration	
	15	IMAP	Declaration	
	16	INFO_ADDRESS	Declaration	
	17	INFO_REQUEST	Declaration	
	18	Internal-Locator-Service	Declaration	
	19	NFS	Declaration	
	20	NNTP	Declaration	
	21	NTP	Declaration	
	22	OSPF	Declaration	
	23	PING	Declaration	
	24	POP3	Declaration	
	25	PPTP	Declaration	
	26	RIP	Declaration	

	27	SIP	Declaration	
	28	SMTP	Declaration	
	29	SNMP	Declaration	
	30	SSH	Declaration	
	31	SYSLOG	Declaration	
	32	TCP	Declaration	
	33	TELNET	Declaration	
	34	TFTP	Declaration	
	35	TIMESTAMP	Declaration	
	36	UDP	Declaration	
	37	UUCP	Declaration	
	38	IRC	Declaration	
	39	RLOGIN	Declaration	
	40	L2TP (optional)	Declaration	
	41	IGMP (optional)	Declaration	
	42	BGP (optional)	Declaration	
		Proprietary Services:		
	1	NetMeeting	Functional verification	
	2	PC-Anywhere	Functional verification	

	3	QUAKE	Functional verification	
	4	RAUDIO	Declaration	
	5	SIP-Messenger	Functional verification	
	6	TALK	Functional verification	
	7	VDOLIVE	Declaration	
	8	WALS	Declaration	
	9	WINFRAME	Declaration	
	10	X-WINDOWS	Declaration	
	11	SAMPA	Declaration	
	12	SKYPE	Functional verification	
3.1.9		The UTM Firewall shall support following filtering database applications:	Information	
	a	DB2 (IBM Product)	Functional verification	
	b	SQL and variants like MY-SQL	Functional verification	
	C	POSTGRES,	Functional verification	
	d	Oracle	Functional verification	

3.1.10		The firewall shall support e-mail related filtering as follows:	Information	
	a	MIME	Functional verification	
	b	Lotus Notes	Functional verification	
	c	Microsoft Exchange	Functional verification	
	d	S/MIME SSL Protected appliance cannot be inspected. S MIME encryption is done by Client and decryption also on Client.	Functional verification	
	e	The firewall shall support active directory for following authentication Protocols		
	1	LDAP	Functional verification	
	2	HTTPS	Functional verification	
	3	RADIUS	Functional verification	
	4	TACACS+	Functional verification	
3.1.11		The UTM Firewall shall support for filtering multimedia applications such as VoIP, H.323, SIP, RTP, RTCP etc.	Functional verification	

3.1.12		The UTM Firewall shall be based on stateful connection-oriented fire walling and support Static and Dynamic packet filtering.	Functional verification	
3.1.13		The UTM Firewall 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.	Declaration	
3.1.14		The UTM Firewall shall provide the following security features:		
	a	Prevent denial-of-service attacks.	Functional verification	
	b.	Prevent Unauthorized access to information	Functional verification	
	c.	Prevent modification of information	Functional verification	
	d	Java Applet Filtering to stop dangerous Java applications on a per-client or per-IP address basis.	Functional verification	
	e.	Support for unicast Reverse Path forwarding to prevent IP spoofing attacks.	Functional verification	
	f.	Prevent TCP SYN attacks	Functional verification	
	g.	Prevent IP fragmentation attacks.	Functional verification	

	h.	Support for ICMP filtering with configurable threshold.	Functional verification	
	i	UDP flood detection with configurable threshold.	Functional verification	
	j.	Detect Ping of Death.	Functional verification	
	k.	Detect Land attack.	Functional verification	
	l.	Detect Win Nuke attack.	Functional verification	
	m.	Filter IP source route option.	Functional verification	
3.1.15		The UTM System shall support IPv4 and IPv6 with the provision of coexistence for both versions.	Functional verification	
3.1.16		The UTM Firewall must support clustering for High Availability and stateful transition during the failover to prevent session losses.	Functional verification	
3.1.17		The UTM Firewall shall support online software reconfiguration to ensure that changes made to a UTM configuration take place with immediate effect.	Functional verification	
3.1.18		The UTM Firewall shall not affect the performance of the components (including hosted servers) which it is protecting.	Declaration	

3.1.19		On power up the UTM Firewall shall use built-in system monitoring & diagnostics before going online to detect failure of hardware.	Declaration	
3.1.20		Communication among the UTM system' s components shall be secure.	Declaration	
3.1.21		The UTM Firewall must support user identity as matching criteria along with Source/Destination IP/Subnet/group, destination Port in UTM rule.	Functional verification	
3.1.22		The UTM Firewall shall have provision to apply multiple threat policies like Anti-Virus, Anti-Spam, Intrusion Prevention, Content	Functional verification	
		filtering, Bandwidth Management & also a routing decision on firewall rules on inter zone traffic.		
3.1.23		The UTM Firewall shall support user defined multi zone security architecture.	Functional verification	
3.1.24		The UTM Firewall shall support 802.1q VLAN tagging support.	Functional verification	
3.1.25		There shall be a means of connecting directly to the UTM Firewall through an encrypted connection to perform troubleshooting and packet captures.	Functional verification	
3.1.26		There shall be a means of connecting directly to the UTM Firewall through a console connection.	Functional verification	

3.1.27		The UTM Firewall shall have the option to disable any unencrypted means of access to the UTM.	Functional verification	
3.1.28		The UTM Firewall shall support GUI or command line interface for Static/Dynamic routing	Functional verification	
3.1.29		The UTM Firewall must provide Mac Address (Physical Address) based UTM rule to provide OSI Layer 2 to Layer 7 security.	Functional verification	
3.1.30		The UTM Firewall shall support HTTPS for easy software upgrades over the network in a secure way.	Functional verification	
3.1.31		The UTM Firewall shall support SNMP v2c or / SNMP v3. It shall also support the	Declaration	
		SNMP get & set, SNMP trap, MIB II, UTM MIB, Syslog MIB etc. UTM system shall support public MIBs; in case private MIBs are used, same shall be provided to the SPs.		
3.1.32		The UTM Firewall shall support on appliance Logging and also via Syslog. The UTM logging features shall include the following:		
	a	The UTM Firewall logs shall contain information about the UTM policy rule that triggered the log.	Functional verification	
	b	The UTM Firewall shall be capable of capturing detailed packet data to a log.	Functional verification	
	c	The UTM Firewall logging shall not impact UTM performance.	Functional verification	

	d	The UTM Firewall and log server shall be capable to synchronise with an NTP server.	Functional verification	
3.1.33		The UTM Firewall shall be able to send logs to different syslog servers.	Functional verification	
3.1.34		The UTM Firewall consolidated log data shall be made available through a central/secure log database for easy management & retrieval using a reporting database.	Declaration	
3.1.35		The UTM Firewall shall be able to filter log data by user	Functional verification	
3.1.36		The UTM Firewall shall be able to consolidate log data for efficient reports	Declaration	
3.1.37		The UTM Firewall shall be able to consolidate log data for		
	a.	Network services,	Functional verification	
	b.	Network resources	Functional verification	
	c.	User/groups	Functional verification	
	d.	Domains/departments	Functional verification	
	e.	Connection duration	Functional verification	

	f.	Number of bytes transferred	Functional verification	
	g.	Bandwidth usage	Functional verification	
	h.	Blocked connections	Functional verification	
	i.	Source/Des. IP addresses	Functional verification	
	j.	URLs	Functional verification	
	k.	Failed authentication attempts	Functional verification	
	l.	Date/Time	Functional verification	
	m.	UTM identity	Functional verification	
	n.	Intrusion attempts	Functional verification	
	o.	Alert/error conditions	Functional verification	
	p.	Peak activity based on users, services, time, etc	Functional verification	

	q.	The user shall be able to specify/create modify/delete rules/policies to collect log data and consolidate based on what he requires.	Functional verification	
	r.	The log consolidator shall be able to use UTM objects/users for use in the consolidation policy.	Functional verification	
	s.	The UTM Firewall shall send log information to an external log server via an encrypted connection using FTP or syslog.	Functional verification	
3.1.38		The UTM Firewall shall provide integrated on appliance reporting for in-depth details on network traffic and activities. (Optional)	Declaration	
3.1.39		The UTM Firewall shall support multiple syslog servers for remote logging.	Functional verification	
3.1.40		The UTM Firewall shall support Auditing facility to track all activity carried out Security appliance.	Declaration	
3.1.41		The UTM Firewall shall have configurable options to send reports on designated email address.	Functional verification	
3.1.42		Extensive debugging capabilities to assist in hardware problem resolution shall be supported.	Declaration	

3.2		Intrusion Detection & Prevention (IDP) System. Functional requirement of IDP is divided into following:		
	a.	Architecture.	Declaration	
	b.	Incident Monitoring and Detection.	Declaration	
	c.	Incident Response.	Declaration	
	d.	Configuration.	Declaration	
	e.	Management	Declaration	
	f.	Security.	Declaration	
	g.	Performance.	Declaration	
	h.	Updates and Technical Support.	Declaration	
3.2.1		**Architecture:**		
	i.	IDP shall detect and actively prevent attacks in real-time and shall be placed in INLINE mode.	Functional verification	
	ii	IDP shall not add delay or become a congestion point or become a central point of failure to the network being monitored.	Declaration	
	iii	The installation of the IDP shall not require changes to the network infrastructure or affect the MTBF of the network in any way.	Declaration	
	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	Functional verification	
		Time Protocol or simple Network Time Protocol. NTP v3 (RFC 1305)/NTP v4 (RFC 5905) shall be supported.		

	xii	The IDP shall be scalable and re-configurable, and its licensing shall be such so as not to affect network expansion.	Declaration	
	xiii	DP system if installed in bridge mode shall be transparent and invisible to network	Functional verification	
	xiv	IDP if installed in bridge mode shall generate appropriate alarms on any failure. (Purchaser to specify).	Functional verification	
3.2.2		**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.	Functional verification	
	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.	Functional verification	
	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.	Functional verification	
	iv	IDP shall be able to detect and shall be able to stop Denial of Service attacks like Smurf	Functional verification	

		attack, Teardrop attack, UDP Flooding, Land attack, WinNuke attack, TFN2K, SYN attack, Stream – like DoS attack, IP/MAC spoofing etc. IP Anomaly engine should be part of the offering – Bad L4 Checksum, Land Attacks, Bad TCP Lengths, TCP Null Flags, Bad URL Length, UDP Port loopback, Bad TCP Urgent flags, TCP XMAS attacks, Bad TCP or UDP checksum, Bad IP header Lengths, Incorrect iP TTL, IP IP Payload, Oversize Payload, Bad IP Checksum etc.- Optional		
	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.	Functional verification	
	vi	IDP shall able to detect & block known P2P based instant messaging application like skype & known chat application like WLM, Rediffbol etc.	Functional verification	
	vii	IDP shall able to detect VoIP (like SIP) data and shall be able to block the same.	Functional verification	
	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	Functional verification	
	ix	IDP shall be able to detect and shall be able to stop any Suspicious Activity.	Functional verification	
	x	Creation of User-specified signatures shall be possible based upon contents i.e. string	Declaration	

		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).	Declaration	
	xii	IDP shall support signatures tuning to match the operational requirements of the customer network so that false policies are minimized.	Declaration	
	xiii	IDP shall support help system that describes the incidents in adequate detail, providing sufficient information about:	Declaration	
	a.	The incident.	Declaration	
	b.	The potential damage.	Declaration	
	c.	Possible false positives.	Declaration	
	d.	The systems affected.	Declaration	
	e.	How to respond immediately upon detection of the incident.	Declaration	
	f.	How to remove the vulnerability associated with the incident?	Declaration	
xiv		IDP shall be configured to focus on the incidents that pose the greatest risk to the network.	Declaration	
xv		IDP shall detect the malicious activity event in fragmented and de-fragmented packets.	Functional Verification	
xvi		IDP shall provide Stateful Operation	Functional Verification	

	a.	TCP Reassembly	Functional Verification	
	b.	IP De-fragmentation	Functional Verification	
	c.	Bi-directional Inspection	Functional Verification	
	d.	Forensic Data Collection	Functional Verification	
	e.	Access Lists	Functional Verification	
xvii		IDP shall provide Signature Detection for at least 3500 (more than 1500 vulnerability based) Vendors Signature Database and 5,000 User Defined Signatures refer to NVD catalogue and CVE catalogue. – standard data base to be referred.	Declaration	
xviii		IDP shall have Anomaly Detection Mechanism for Protocol Anomalies and Sampling Based Traffic Anomalies to prevent against Day Zero or Unknown Attacks	Declaration	
xix		The IDP shall provide the capability to annotate incidents recorded in the database.	Declaration	
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	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	
	k.	SSL Encrypted Attack Protection(optional)	Functional Verification	
xxi		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	
xxii		IDP Shall Protect against various DOS & DDOS attacks as follows:		

	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	
3.2.3		**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	
3.2.4		**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.	Declaration	
	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.	Declaration	
	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.	Declaration	
	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.	Declaration	
	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.	Declaration	
	ix	IDP shall be capable of attack policy customization.	Declaration	
	x	IDP shall have provision to analyze and identify the ingress point of attack.	Functional Verification	

3.2.5		**IDP user interface -:**		
3.2.5.1		Provide customizable features such as Detection Rules, Reports, Alerts, and Responses via the IDP user interface.	Declaration	
3.2.5.2		IDP user interface shall support following for access:		
	a.	HTTPS	Functional Verification	
	b.	SSH	Functional Verification	
3.2.5.3		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.	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.	Functional Verification	
3.2.5.4		**Data Management -:**		
	i	IDP shall have comprehensive database with more than 3500 attack (of them atleast 1500 vulnerabilities based) signatures. Standard databases to be referred.	Declaration	
	ii	IDP shall support data management capabilities provide critical information required for risk assessment and decision-making.	Declaration	
	iii	IDP shall be capable of prioritization of security event data for quick and easy threat assessment.	Declaration	
3.2.5.5		**IDP Reports -:**		
	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.	Declaration	

	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.	Declaration	
	ii	It shall be possible to generate multiple forms of reporting suitable for all technical levels.	Declaration	
	iv	IDP shall support reports that may be exported to different formats, such as excel, HTML or a Word document etc.	Declaration	
	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.	Declaration	
	vi	IDP shall provide drill down reports based on Real Time attack statistics for following:	Declaration	
	a.	Security event risk level.	Declaration	
	b.	Date/time.	Declaration	
	c.	Subnets (Networks/ IP Address)	Declaration	
	d.	Event name.	Declaration	
	e.	Source IP.	Declaration	
	f.	Destination IP.	Declaration	
	g.	User Identity	Declaration	
	h.	Response taken.	Declaration	

	i.	Severity.	Declaration	
	j.	Top attack types	Declaration	
	k.	Attack groups	Declaration	
	l.	Top-10 Source of Attacks	Declaration	
	m.	Top-10 Destination of attacks	Declaration	
	vii	Management station shall be able to show Graph with number of attacks coming from different networks	Functional Verification	
	vii i	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:	Functional Verification	
	a.	SNMP trap	Functional Verification	
	b.	Logging	Functional Verification	
	c.	Syslog	Functional Verification	
3.2.6		**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.	Declaration	
	ii	The IDP shall monitor its internal application modules and notify the management station when a module goes off line unexpectedly.	Declaration	
	iii	The IDP and management console shall be protected against intentional or accidental abuse, unauthorized access and loss of communication.	Declaration	
	iv	The management console shall have the	Declaration	
		feature of idle time disconnection. (optional)		
3.2.7		**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.	Declaration	
	ii.	IDP shall handle traffic bursts gracefully, switching to sampling mode until the traffic levels return to a consistent level. (optional)	Declaration	
3.2.8		**IDP Updates -:**		

	i	The IDP software and its attack signature database shall be updated at least once in a month.	Declaration	
	ii	Update attack signatures, rule bases and service releases via the Internet or with Version Upgrades	Declaration	
	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.	Declaration	
	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.	Declaration	
	v	IDP Shall support 24/7 Security Update Service	Declaration	
	vi	IDP Shall support Real Time signature update	Declaration	
	vii	IDP shall support for customized signatures.	Declaration	
	viii	IDP Shall support Automatic signature synchronization from database server on Internet.	Declaration	
	ix	The IDP shall provide for regular updates to the signature database	Declaration	

3.3		**Content Filtering & Application Filtering** The UTM shall have an integrated solution with local database instead of querying to database hosted somewhere on the internet.	Declaration	
3.3.1		It shall filter websites by category, eg. Adult, Sports, Gambling etc	Functional verification	
3.3.2		It shall automatically update URL category database from the vendor' s website.	Declaration	
3.3.3		It shall allow the administrator to define different web filtering policies by IP address, user and groups.	Functional verification	
3.3.4		It shall be able to allow manual configuring blocking of custom URLs as per Goat' s directives.	Functional verification	
3.3.5		It shall have at least 25 Million URLs categorized in the URL filtering database. Cloud backed URL lists should be supported. option	Declaration	
3.3.6		It shall have minimum of 40+ URL categories.	Declaration	
3.3.7		It shall have user configurable include/exclude lists	Functional verification	
3.3.8		It shall support spyware blocking	Functional verification	
3.3.9		It shall support blocking of SPAM URLs.	Functional verification	

3.3.10		It shall have the ability to update URL blocking database from centralized console	Functional verification	
3.3.11		Network Administrators shall have the added ability to manually add test URLs to the UTM' s filter list	Functional verification	
3.3.12		It shall be able to block HTTPS based on Host name/Fully Qualified Domain Name with the help of certificates.	Functional verification	
3.3.13		It shall be able to block HTTP uploads	Functional verification	
3.3.14		It shall be able to block URLs based on regular expression	Functional verification	
3.3.15		It shall be able to identify and block request coming through proxy servers on the base of username and IP address.	Functional verification	
3.3.16		It shall comply to internet access policy (as framed by Government/authority) pertaining to Children.	Declaration	
3,3.17		It must provide web category based bandwidth management and prioritization	Functional verification	
3.3.18		It shall provide option to customize access denied message for each category. (optional	Functional verification	
3.3.19		It shall be able to block all known chat application like Yahoo, MSN AOL, Google, Rediff, Jabber.	Declaration	

3.3.20		It shall block access through HTTP or HTTPS based anonymous proxies available on the internet.	Declaration	
3.3.21		It shall be able to identify traffic based on Productive, Neutral, unhealthy & non-working websites as specified by admin.(optional)	Declaration	
3.3.22		It shall able to identify & block URL translation request.	Functional verification	
3.3.23		It shall support granular application control.	Functional verification	
3.3.24		It shall support minimum 10+ application category like File transfer, P2P, Proxy, Streaming media, VoIP, etc. 250 supported. 50+ to be made	Declaration	
3.3.25		It shall support more then 300+ applications like skype, Ultra surf, MSN file transfer, Gmail on HTTPS, external SOCKS etc	Declaration	
3.3.26		It shall allow administrator to create time base access for the particular application.	Functional verification	
3.3.27		It shall control application irrespective of IP, Port, etc.	Functional verification	
3.4		**Anti-Virus/Anti-Spam**		
3.4.1		The UTM shall be deployed as Gateway Scanning engine.	Functional verification	

3.4.2		The UTM shall be able to scan traffic without acting as a mail server in case of mail protocols	Functional verification	
3.4.3		The UTM shall be able to operate in transparent mode.	Functional verification	
3.4.4		The UTM shall protect HTTP, SMTP, FTP, POP3 and IMAP protocols	Functional verification	
3.4.5		The UTM shall support both stream based Anti-Virus scanning and file based Anti-Virus scanning	Functional verification	
3.4.6		The UTM shall have Signature and Behavioral antivirus engine.	Functional verification	
3.4.7		The UTM shall perform both inbound and outbound inspection	Functional verification	
3.4.8		The UTM shall have 2.5+ million virus signatures for comprehensive coverage	Declaration	
3.4.9		The UTM 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	Declaration	
3.4.10		The UTM shall stop zero day variants	Declaration	
3.4.11		The UTM shall provide mass mailing virus/spam detection and mail attachment virus detection.	Functional verification	

3.4.12		The UTM shall support Spam and Virus filtering and shall have its own Spam/Virus list that shall be updated automatically.	Declaration	
3.4.13		The UTM shall have URL database to filter SPAMs having URLs	Functional verification	
3.4.14		The UTM shall be multi-threaded	Declaration	
3.4.15		The UTM shall be capable of implementing protocol based Anti-spam rules	Functional verification	
3.4.16		The UTM shall have support for Server based anti-spam, the Anti-virus system shall be able to scan all traffic or specific extensions as defined by the administrator.	Functional verification	
3.4.17		The configuration tools shall provide the ability to be used individually or collectively for access controls, mailbox filtering, address verification, a real-time black hole list, relay blocking, and authentication services.	Declaration	
3.4.18		The UTM shall support an Allow and Deny list of valid IP/Domains to allow/deny relaying for.	Functional verification	
3.4.19		The UTM shall support POP/IMAP4 and SMTP authentication	Functional verification	
3.4.20		The UTM shall be able to scan by message subject, header, body, and attachment objects.	Declaration	

3.4.21		The UTM shall be able to block attachment by file name and extension.	Functional verification	
3.4.22		The UTM shall provide Malformed Mail format detection	Functional verification	
3.4.23		The UTM shall support Recursive Analysis on messages and Compressed files	Declaration	
3.4.24		The UTM shall have separate inbound and outbound virus and content. Scanning policies	Functional verification	
3.4.25		The UTM shall provide detailed logging for the virus found message, which shall include Date, Time, Sender, Receipt, Subject, and File name which contained the virus, Action take for the file, which contained the virus.	Functional verification	
3.4.26		The UTM shall provide on appliance quarantined facility and also personalized user based quarantine area	Functional verification	
3.4.27		The UTM shall support mail archive option to send copy of incoming and outgoing	Declaration	
		mails to administrator on defined email address. (optional)		
3.4.28		The UTM shall have multiple configurable policies for email id/address group for quarantine setting, different action instead of blanket policy.	Functional verification	
3.4.29		The UTM shall support real time spam detection instead of using signature database	Functional verification	

3.4.30		The UTM shall save bandwidth by blocking spam messages at gateway level itself without downloading the message using advanced IP Reputation Filtering feature.	Functional verification	
3.4.31		The UTM shall support IP/Email address white list/Black list facility.	Functional verification	
3.4.32		The UTM shall support option to enable/disable antispam scanning for SMTP authenticated traffic.	Functional verification	
3.4.33		The UTM shall support real time spam detection & also supports proactive virus detection technology which detects and blocks the new outbreaks immediately and accurately.	Declaration	
3.4.34		The UTM shall provide historical reports based on username, IP address, Sender, Recipient & spam category.	Functional verification	
3.4.35		The UTM must provide Anti-Spam Message Digest feature per user. (optional)	Declaration	
3.4.36		The UTM shall provide historical reports based on username, IP address, Sender, Recipient & Virus Names.	Functional verification	
3.4.37		The UTM shall support real mode for HTTP virus scanning.	Functional verification	
3.4.38		The UTM shall support batch mode for HTTP virus scanning. (optional)	Declaration	

3.4.39		The UTM shall provide option to bypass scanning for specific HTTP traffic	Functional verification	
3.4.40		The UTM shall scan http traffic based on username, source/destination IP address or URL based regular expression.	Functional verification	
3.4.41		The UTM shall support multiple anti-virus policy for sender/recipient email address or address group for notification setting, quarantine setting & file extension setting instead of single blanket policy. (optional)	Functional verification	
3.5		**Virtual Private Network**		
3.5.1		The UTM shall have Inbuilt support for IPSEC VPNs and SSL VPN functionality.	Functional verification	
3.5.2		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	
3.5.3		The platform shall use purpose-built hardware that is optimized for packet filtering and encryption	Declaration	
3.5.4		The UTM shall support DES, 3DES, AES encryptions algorithm.	Functional verification	
3.5.5		The UTM 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	Declaration	

3.5.6		The VPN shall support external certificate authorities.	Declaration	
3.5.7		It shall support local certificate authority & shall support create/renew/Delete self-signed certificate.	Declaration	
3.5.8		All traffic passing through IPSec/L2TP/PPTP/SSL VPN tunnel shall be scanned for threats by passing through the Anti-Virus, Anti-Spam and Intrusion Prevention modules.	Functional verification	
3.5.9		It shall be possible to apply bandwidth management policies on all traffic passing through the IPSec/L2TP/PPTP/SSL VPN tunnels	Functional verification	
3.5.10		It shall provide on appliance SSL-VPN solution with Web Access (Clientless), Full Tunnel and Split Tunnel control. Solution shall provide per user / group SSL-VPN access; the licensing terms will be decided by tendering authority.	Functional verification	
3.5.11		It shall support export facility of Client-to-site configuration for hassle free VPN configuration in remote Laptop/Desktop.	Functional verification	
3.5.12		It shall support commonly available IPsec VPN clients.	Declaration	
3.6		**Reporting**		

3.6.1		UTM must provide integrated on appliance reporting for in-depth details on network traffic and activities.	Declaration	
3.6.2		UTM shall provide minimum 45 different templates to view the reports.	Declaration	
3.6.3		It shall provide logging of Antivirus, Antispam, Content Filtering, Traffic Discovery, IPS, UTM Activity logs.	Functional verification	
3.6.4		It shall provide detailed reports for all files uploaded via HTTP or HTTPS protocol. The report shall include username/IP address/URL/File name/Date and Time.	Functional verification	
3.6.5		It shall provide data transfer reports on the base of application, username, IP Address.	Functional verification	
3.6.6		It shall provide connection wise reports for user, source IP, destination IP, source port, destination port or protocol.	Functional verification	
3.6.7		It shall have facility to send reports on mail address or on FTP server.	Declaration	
3.6.8		It shall provide appropriate regulatory compliance reports. It shall support Auditing facility to track all activity carried out Security appliance.	Declaration	
3.6.9		It shall support multiple syslog servers for remote logging.	Functional verification	
3.6.10		It shall have configurable option to send reports on designated email address.	Functional verification	

3.6.11		It shall provide reports for all blocked attempts done by users/IP Address.	Functional verification	
3.6.12		User level access restrictions shall be possible for accessing and managing the components and generating reports	Functional verification	
3.6.13		Remote management and generation of reports shall be possible	Functional verification	
3.6.14		It shall generate reports consisting of audit, trend and cost information in easy to understand formats	Functional verification	
3.6.15		It shall support well-predefined and custom reports	Declaration	
3.6.16		It shall be available in different formats, e.g. excel, text, HTML, etc. Tendering authority shall provide the detail of report formats.	Functional verification	
3.6.17		It shall support generation of real time and historical performance data report on schedule which could be hourly/daily/weekly/monthly/annually or as decide by the user	Functional verification	
3.6.18		It shall not be limited to only web surfing reports but it shall also provide protocol, IP, user, event, virus, attack wise reports.	Functional verification	
3.6.19		It shall provide option to archive the reports & the same is possible to restore in reporting solution for graphical view later on	Declaration	
3.6.20		It shall give reports for Protocol wise non-working or unhealthy websites report.	Declaration	

3.6.21		It shall give complete information about all inbound & outbound connections established through UTM with data transfer.	Functional verification	
4.		Interconnectivity & Interoperability		
4.1		Hardware shall inter-work with existing Servers, Routers, LAN switches, etc as deployed in SP' s IT/telecommunication infrastructure.	Declaration	
4.2		It shall be a fully integrated multi-platform wide security solution.	Declaration	
4.3		The UTM system shall support unrestricted users i.e. licenses shall not be based on the number of users using the UTM.	Declaration	
4.4		The UTM system shall facilitate / support Firewalls/IPS/IDS/Antivirus/Antispam from different vendors to work in Active-Active (using internal or OPSEC certified external load balancer), multi-applications and shall support third-party products on OPSEC alliance. Tendering authority shall provide the detail of existing firewall systems	Declaration	
4.5		The UTM shall support 802.1Q Trunking.	Functional verification	
4.6		The UTM shall support link-aggregation based on IEEE 802.3ad standard.	Functional verification	

4.7		The UTM firewall System shall support the following minimum performance levels	Declaration	
	a.	wire rate throughput at all interfaces.	Functional verification	
	b.	stateful failover shall be supported to eliminate session loss.	Functional verification	
4.8		UTM 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).	Functional verification	
4.9		**Power Supply:** UTM shall have redundant and Hot swappable power supplies. UTM 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).	Functional verification	
4.10		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.	Declaration	
4.11		Tendering authority shall provide the actual interface requirement.	Declaration	

4.12		The firewall system can be offered for type approval under one or more categories as above.	Declaration	
4.13		**User interface**	Information	
4.13.1		Firewall System shall support management via web user interface (HTTP and HTTPS), Command Line interface (Console), Secure Command Shell (SSH).	Functional verification	
4.13.2		It shall be possible to monitor firewalls from the central site.	Functional verification	
4.13.3		The UTM shall be manageable through an (element management system (EMS). The EMS application for the UTM system shall be UNIX or any other industry standard OS based and provide management for a minimum of 10 UTM devices from a single EMS system. EMS of UTM shall provide FCAPS (Fault Configuration, Accounting, Provisioning and Security) as per TEC standard: on eMS available on TEC website (https://tec.gov.in/standards-specifications). In addition, it shall provide following:	Declaration	
	a.	SSH support: The UTM 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 UTM 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 UTM EMS shall provide a means for exporting the UTM rules set and configuration to a text file.	Functional verification	
	d.	The UTM 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.	Functional verification	
	f.	Remote network access to the UTM shall only be possible through the administration interface	Functional verification	
	g.	The UTM EMS shall be capable of pushing UTM security policies and configurations to individual or multiple UTM through a secure, encrypted connection to the UTM administration interfaces	Functional verification	
	h.	There shall be a means of connecting directly to the UTM through an encrypted connection to perform troubleshooting and packet captures.	Functional verification	

	i.	There shall be a means of connecting directly to the UTM through a console connection	Functional verification	
	j.	The EMS shall allow for a hierarchical architecture for rules set administration and viewing of UTM configurations	Declaration	
4.14		**Reliability, Availability, Performance and Scalability of Firewall system and EMS:** It shall provide the Reliability, Availability, Performance and Scalability requirements as per relevant clauses of latest TEC standard on EMS as applicable to UTM system, with over 99.9% availability:	Declaration	
4.15		**Software Requirement of UTM:** 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 relevant clauses of latest TEC standard on EMS as applicable to UTM system.	Declaration	
4.16		**Man Machine Communication of UTM:** It shall provide the Man Machine Communication requirements as per clause 9.1 of TEC standard for GR : TEC 49110:2025 available on TEC website (https://tec.gov.in/standards-specifications) as applicable to UTM system. The UTM shall be capable to store O&M data	Declaration	

		for a minimum duration of one month with		
		facility for back up on offline storage such as tape drive, CD/DVD/ MOD, etc.		
4.17		The Firewall System Chassis shall be rack mountable in a 19" rack.	Functional verification	
4.18		Desktop model or rack mount model may be decided by the purchaser.	Functional verification	
5.0		**Qualitative Requirements (QR):** The UTM System shall meet the following qualitative requirements:		
5.1		The manufacturer shall furnish the MTBF value. Minimum value of MTBF shall be specified by the purchaser. The calculations shall be based on the guidelines given in either QA document No. QM-115 {January 1997} "Reliability Methods and Predictions" or any other international standards.	Declaration	

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.	Declaration	
5.3		The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue- March, 2010} (TEC 14016:2010) "Standard for Environmental testing of Telecommunication Equipment" or any other equivalent international standard, for operation, transportation and storage. The applicable environmental category A or B to be decided by the purchaser based on the use case.	Declaration	
6.0		**EMI/EMC Requirements**		
6.1		The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein.		
	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".	Report from Accredited Test Lab	

		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;	Report from Accredited Test Lab	
	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 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	Report from Accredited Test Lab	

		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;	Report from Accredited Test Lab	

	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. 2 kV peak open circuit voltage for line to ground **b.** 2 kV peak open circuit voltage for line to line coupling.	Report from Accredited Test Lab	
	f.	**Immunity to conducted disturbance induced by Radio frequency fields:** **Name of EMC Standard:** IEC 61000-4-6 (2013) "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.	Report from Accredited Test Lab	

	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 500ms) ii. a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) 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.	Report from Accredited Test Lab	

	h.	**Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any): Name of EMC Standard:** IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests. **Limits:-** i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B. ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C. iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B. iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C. v. Voltage variations corresponding to 80% and 120%of supply for 100 ms to10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B. Note: - For checking compliance with the		

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

			IEC/CISPR	**Euro Norm**			
			CISPR 11	EN55011			
			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 IEC 61000-4-29	EN 61000-4-11 EN 61000-4-29			

7.0		**Safety Requirements**		
		The equipment shall conform to relevant safety requirements as per IS/IEC 62368-1:2018 or Latest as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT": TEC10009: 2024. The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements.		
8.0		**Security Requirements**	Information	
8.1		**Security Administration and Management of UTM system** The UTM 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	Functional verification	
		as per clause 3.6 of TEC standard on EMS: TEC 52006:2016		

8.2	b.	**Management and Reporting** **Access Control** – The firewall subsystem shall control information and access through predetermined security policy. a) The UTM 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 UTM subsystem shall allow data communication only by authenticated network resources. c) The UTM shall not support any unencrypted means of access to the firewall d) The UTM System shall be able to support transparent authentication and Support State of art encryption and authentication standards like IPSec and RADIUS/ DIAMETER. e) The UTM System shall support Telnet client and server 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 **UTM** System shall support Remote login via PSTN / Internet / etc. with multilevel (at least 5 level) of password.		
9.1		**Engineering Requirements**: The UTM System shall meet the following engineering requirements:	Information	
9.1.1		The equipment shall be fully solid state and adopt state of the art technology.	Declaration	
9.1.2		The equipment shall be compact, composite construction and lightweight. 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	
9.1.6		Each sub-assembly shall be clearly marked with schematic reference to show its function, so that it is identifiable from the layout diagram in the handbook.	Declaration	

9.1.7		Each terminal block and individual tags shall be numbered suitably with clear identification code and shall correspo to the associated wiring drawings.	Declaration	
9.1.8		All controls, switches, indicators etc. shall be clearly marked to show their circuit diagrams and functions.	Declaration	
9.1.9		**Operational Requirement (OR):** The UTM System shall meet the following Maintenance & operational requirements:	Information	
9.1.10		The equipment shall be designed for continuous operation	Declaration	
9.1.11		The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sea level.	Declaration	
9.1.12		Suitable visual indications shall be provided to indicate healthy and unhealthy conditions	Declaration	
9.1.13		The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.	Declaration	
9.1.14		The removal or addition of any cards shall not disrupt traffic on other cards.	Declaration	

9.1.15		All mission critical modules shall be identifie and provided in full redundant configuration for high reliability.	Declaration	
9.1.16		A single point failure on the equipment	Declaration	
		shall not result in network or network management system downtime.		
9.1.17		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	
9.1.18		Special tools required for wiring shall be provided along with the equipment.	Declaration	
9.1.19		In the event of a full system failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.	Declaration	
9.1.20		Multi-vendor, Multi application environment shall be supported by firewall system.	Declaration	
9.1.21		A power down condition shall not cause loss of connection configuration data storage.	Declaration	

9.1.22		Live Insertion and hot swap of modules shall be possible to ensure maximum network availability and easy maintainability.	Declaration	
9.1.23		The Hardware and software components shall not pose any problems in the normal functioning of all network	Declaration	
		elements wherever interfacing with service provider network for voice, data and transmission systems, as the case may be.		
9.2		**Other Requirements:**	Information	
9.2.1		The system hardware and software shall not pose any problem, due to changes in date and time caused by events such changeover of millennium / century, leap year etc., in the normal functioning of the system.	Declaration	
9.2.2		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.	Declaration	

9.2.3		Power Supply: The equipment power supply requirements are given for each of the category. In addition, it shall meet the following requirements:	Declaration	
9.2.4		The equipment shall be able to function over the range specified in the respective chapters, without any degradation in performance.	Declaration	
9.2.5		The equipment shall be protected in case of voltage variation beyond the range specified and also against input	Declaration	
		reverse polarity.		
9.2.6		The derived DC voltages shall have protection against short circuit and overload.	Declaration	
9.3		**Documentation and Installation**		
9.3.1		This chapter describes the general requirements for documentation to be provided. All technical documents shall be in English language both in CD-ROM and in hard copy. The documents shall comprise of:		
	a.	System description documents	Declaration	
	b.	Installation, Operation and Maintenance documents	Declaration	
	c.	Training documents	Declaration	

	d.	Repair manual	Declaration	
9.3.2		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.	Declaration	
	b.	Equipment layout drawings.	Declaration	
	c.	Cabling and wiring diagrams.	Declaration	
	d.	Schematic drawings of all circuits in the system with timing diagrams wherever necessary.	Declaration	
	e.	Detailed specification and description of all Input / Output devices	Declaration	
	f.	Adjustment procedures, if there are any field adjustable units.	Declaration	
	g.	Spare parts catalogue - including information on individual component values, tolerances, etc. enabling procurement from alternative sources.	Declaration	
	h.	Detailed description of software describing the principles, functions, and interactions with hardware, structure of the program and data.	Declaration	

	i.	Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data.	Declaration	
	j.	Program and data listings.	Declaration	
	k.	Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification.	Declaration	
9.3.3		System operation documents**:** The following system operation documents shall be available.	Declaration	
	a.	Installation manuals and testing procedures.	Declaration	
	b.	Precautions for installation, operations and maintenance	Declaration	
	c.	Operating and Maintenance manual of the system.	Declaration	
	d.	Safety measures to be observed in handling the equipment	Declaration	
	e.	Man-machine language manual.	Declaration	
	f.	Fault location and troubleshooting instructions including fault dictionary.	Declaration	
	g.	Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement.	Declaration	

	h.	Emergency action procedures and alarm dictionary.	Declaration	
9.4		**Training Documents**		
9.4.1		Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available.	Declaration	
9.4.2		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.	Declaration	
9.4.3		The structure and scope of each document shall be clearly described.	Declaration	
9.4.4		The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification necessary information.	Declaration	
9.4.5		All diagrams, illustrations and tables shall be consistent with the relevant text.	Declaration	
9.5		**Installation**		

9.5.1		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	
9.5.2		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	
9.5.3		All installation materials, consumables and spare parts to be supplied	Declaration	
9.5.4		All literature and instructions required for installation of the equipment, testing and bringing it to service shall be	Declaration	
		made available in English language.		

9.5.5		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	
9.5.6		The equipment shall have:		
	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	
10.1		**Bandwidth Management.**		
10.1.1		UTM shall have integrated bandwidth management.	Declaration	
10.1.2		UTM shall able to set guaranteed and burstable bandwidth per User/IP/Application on individual or shared basis.	Declaration	
10.1.3		It shall provide option to define different bandwidth for different schedules in a single policy & bandwidth shall change as per schedule in run time.	Declaration	

10.1.4		It shall able to set guaranteed and burstable bandwidth per User/IP/Application on individual or shared basis.	Declaration	
10.1.5		It shall provide option to set different level of priority for critical application.	Declaration	
10.1.6		It shall provide option to define different bandwidth for different schedule in a single policy & bandwidth shall change as per schedule on the fly	Declaration	
10.1.7		It must provide web category based bandwidth management and prioritization.	Declaration	
10.2		**Multi-Link Manager**		
10.2.1		UTM shall support load balancing & failover for more than 2 ISP.	Declaration	
10.2.2		UTM shall support explicit routing based on Source, Destination, Username, and Application.	Declaration	
10.2.3		It shall support weighted round robin algorithm for Load balancing.	Declaration	
10.2.4		It shall provide option to create failover condition on ICMP, TCP or UDP protocol to detect failed ISP connection.	Declaration	
10.2.5		It shall send alert email to admin on change of gateway status.	Declaration	
10.2.6		It shall have Active/Active (Round Robin) and Active/Passive gateway load balancing and failover support.	Declaration	
10.3		**Internet Access Management**		

10.3.1		It shall support integration with Windows NTLM, Active Directory, LDAP, Radius or Local Database for user authentication.	Declaration	
10.3.2		It shall support Automatic Single Sign (ASSO) for transparent user authentication.	Declaration	
10.3.3		It shall support Dynamic DNS configuration.	Declaration	
10.3.4		It shall provide on appliance bandwidth utilization graph on daily, weekly, monthly or yearly for total or individual ISP link.	Declaration	
10.3.5		It shall provide real time data transfer/bandwidth utilization done by individual user/IP address/application.	Declaration	
10.3.6		It shall support Parent Proxy with IP/FQDN support.	Declaration	
10.3.7		It shall support NTP.	Declaration	
10.3.8		It shall support user/IP/mac binding functionality to map username with IP address & MAC address	Declaration	
10.3.9		It shall have multi lingual support for Web admin console.	Declaration	
10.3.10		It shall support Version roll back functionality.	Declaration	
10.3.11		It shall support session time out & idle time out facility to forcefully logout the users.	Declaration	
10.3.12		It shall support ACL based user creation for administration purpose.	Declaration	

10.3.13		It shall support LAN bypass facility in case appliance is configured in transparent mode.	Declaration	
10.3.14		It shall support inbuilt PPPOE client and shall be capable to automatically update all required configuration whenever PPPOE get changed.	Declaration	
10.3.15		It shall allow creating policy to assign total number of hours for Internet surfing per user.	Declaration	
10.3.16		It shall support creation of Data Quota policy on daily/weekly/monthly/yearly basis for individual user or group basis.	Declaration	
10.3.17		It shall support creation of cyclic data quota policy on Daily/weekly/Monthly/yearly basis for individual user or on group.	Declaration	
10.3.18		It shall support creation of internet access time policy for individual users or on group basis.	Declaration	
10.3.19		It shall provide an on appliance user portal that allows user to view his/her own activity details like Data transfer, total internet usage details, web usage details and Quarantined mails.	Declaration	

I. TEST SETUP & PROCEDURES:

1. Test No.	
2. Test Details	*Name and Other relevant details*
3. Test Instruments Required	1. <Name> 2.
4. Test Setup	
5. Test Procedure	*Testing Steps may be written here….* 1) ..... 2) ..... 3) .....
6. Test Limits	(if any)
7. Expected Results	1. **.....**<values>.....**.....** 2. **.....**<values>...**.....** 3. Other tests (test name)

Further Test Setup & Procedures may be added as per requirement

J. SUMMARY OF TEST RESULTS

TEC Standard No._____

TEC Test Guide No._____

Equipment name & Model No.

_____

Clause No.	***Compliance*** *(Complied /Not Complied / Submitted/Not Submitted / Not Applicable)*	***Remarks /*** ***Test Report Annexure No.***

[Add as per requirement]

Date:

Place:

Signature & Name of TEC testing Officer /

**** Signature of Applicant / Authorized Signatory***