200

No. EI-D/GA/1-74/2011

ERNET India

(An Autonomous Scientific Society under Department of Information technology, GoI)
Jeevan Prakash Building, 10th Floor,
25, K.G Marg,
New Delhi-110 001

Dated:- 29.1.2013

Subject:- Invitation of Bids for supply, installation, commissioning & integration of Firewalls , IPSs, UTMs, Antivirus – Antispam Gateways & EMS

Kindly refer to the advertisement appeared in Times of India dated 25.08.2012, tender document dated 27.08.2012 and subsequent communication dated 07.09.2012 uploaded on ERNET Website regarding the subject matter. Regarding the subject tender ERNET received queries from various bidders. Based on the queries received, amendment in the tender document is made as per Annexure attached. The revised bid submission date is 18.2.2013 at 3.00 PM.

2. All the prospective bidders are requested to kindly submit their bids in conformity with the tender document and amendment in the tender document referred in para 1 above. The bidders are requested to submit their bids by 18.2.2013 in ERNET India by 3.00 P.M The bids will be opened on the same day at 3.30 P.M

29/1/13

(Dinesh Kumar Dixit)
Registrar & CPO

To,
All the prospective bidders

Annexure-II

Amendments to the tender document no. EI-D/GA/1-74/2011, Dated: 07-09-2012

S. No	Tender Section-Clause	Specification in the tender	Amendment/Clarification
A	**Annexure-II- 3-EMS**		
1	M: Service Help Desk)-Clause no 2	The solution should have built-in remote diagnostics capabilities enabling service desk personnel to remotely take over control of the end user's machine for troubleshooting, updating a file, changing a user's configuration, and looking at settings. It should provide the facility to record these sessions for auditing and recordings should be available for review at a later date.	This clause stands deleted
2	Architecture-"c"	Each of the Large PoPs, and Medium PoPs will have a dedicated, independent management console. These remote consoles should be consolidated at the central site which will be based at ERNET Hq. New Delhi to reflect overall status of the network and systems using bridging technology- i.e., Large and Medium PoPs will have their own consoles for alerts, traps and management, with selective escalation and status updates being forwarded to the central console at New Delhi.	The network & all devices/resources will be monitored & managed across all PoPs of ERNET from the central site. Desktop, if needed at any remote site will be provisioned by ERNET.
3	Number-3 (at starting of tender document) & EMS Architecture-"d"	3. ERNET India intends to enter... Enterprise Management System is to be installed at ERNET POP at Delhi for... d) The processing load should be distributed across the processors and network links that can handle it, allowing for large number of objects to be monitored. There should also be middle layers in the architecture to spread the processing load further and improve scalability.	EMS servers need to be deployed at central PoP in Delhi.
4	Architecture- j	EMS solution should be supplied including all hardware, accessories, licences, softwares, etc. The servers required to run EMS should be part of solution and should be Linux based.	This clause should be read as "EMS solution should be supplied including all hardware, accessories, licenses, softwares, etc. The servers required to run EMS should be part of solution and should be Linux/Windows OS based. The bidders should quote any additional component, not mentioned in the BOM, which is mandatory to make the system fully operational."
5	M: Service Help Desk, Clause no 5	The solution should be bundled with a tool that will allow administrators to customize the GUI using a point-and-click interface to add and change forms, objects, and fields in forms	This clause to be read as "The solution should be bundled with a tool that will allow administrators to customize the GUI to add and change forms, objects, and fields in forms."
6	D: Server Monitoring-Clause no 7	It should provide an easy to use mechanism to modify/create your own custom scenarios/conditions without any programming knowledge	This clause should be read as "It should provide an easy to use tool/mechanism to modify/create your own custom scenarios/conditions without any programming knowledge"

7	D: Server Monitoring- Clause no 12	It should support all standard platforms for server monitoring including both Physical and Virtual Windows, Unix (HP, Solaris, AIX), Linux, AS/400 and Database like DB2, Oracle, MS-SQL, and Sybase.	"AS/400" in this clause stands deleted
8	B:(Traffic Analysis….. Generation)- Clause no 14	The Fault Management Module should support real-time data/statistics on all the network elements under maintenance-mode in a single console.	This clause should be read as "The Fault Management Module should support real-time data/statistics on all the network elements in a single console."
9	K:(Workflow Automation)		This clause stands deleted.
10	L:(Batch Job and Workload Automation) Clause no 3	Solution should provide user ability to map the key business impacting jobs into a service and enables the Service Monitoring to integrate into Service Desk and Service Impact Management for any failure or delays.	This clause stands deleted.
11	L:(Batch Job and Workload Automation) Clause no 4	Solution should have the ability to forecast the schedule for a future date and simulate the flow of jobs in terms to the estimated start and end times of jobs and business services with option to add what-if scenarios for better simulation.	This clause stands deleted.
12	L:(Batch Job and Workload Automation)		This clause stands deleted.
13	b: Mail Application Management- (i)	The system should have agents to manage SMTP mail server on Solaris, Linux , Windows and Messaging system Sun java Communications suite 6, Messaging Server 7.0, Communication Express 6.3, etc.	This clause should be read as "The system should have agents to manage SMTP mail server/systems of all leading brands. Currently, ERNET is using Sun Java Messaging system. ERNET is in process to procure new Messaging System. The bidder should provide agents to manage the same as well when ERNET request for the same."
14	c: Web Application Management- (i)	The system should have agents to manage Netscape Web server on Solaris, Linux and Windows. It should also be able to manage other popular Web server like Microsoft IIS, Lotus Domino, Apache etc.	This clause should be read as "The system should have support to manage all leading Web server on Unix, Linux and Windows. It should also be able to manage popular Web server like Microsoft IIS, Lotus Domino, Apache etc. It should have agents to manage the following: The EXISTING Infrastructure in ERNET for Web services are : ERNET is using the hosting environment consisting of RHEL5 & RHEL6 with Apache, Mysql etc. Apart from this the windows platforms are Windows 2003, 2008, 2012. ERNET is also using clustering and virtualisation environment with base machines being RHEL topped with Xen and Base machine Windows 2008 / 2012 with Clustering and Hyper-V. Guest OS are again RHEL5/6 and Windows Server 2003/2008/2012. Harware are a combination of individual as well as Blade server and storage."
15	G:(Database Monitoring)	Additional Queries	Database monitoring is required as a part of EMS solution as detailed in the tender. Please refer Annexure-I (items at s.no. 3) for various licensing requirements.
B	**Annexure-II-5. UTM**		

1	Point 4	Firewall & Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0, FIPS 140-2 certified	This clause should be read as "Firewall & Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0, FIPS 140-2/VPNC/equivalent certified"
2	Point 8	Complete firewall management solution including real-time monitoring, event logs collection, & policy enforcement should be from a single device only (mgt server/appliance).	This should be read as "Complete firewall management solution including real-time monitoring, event logs collection, & policy enforcement should be provided. NAS of 40TB usable should be provided alongwith the solution for events log collection, monitoring etc."
3	Point 10	Firewall should support the multicast protocols as a multicast host, by participating in DVMRP, IGMP and PIM-DM / PIM-SM	This clause should be read as "Firewall should support the multicast protocols as a multicast host, by participating in IGMP and PIM-DM / PIM-SM"
4	Point 12	All UTM features like Antivirus, Web filtering, Messaging Security & Intrusion Prevention should be available as software modules & should be independent, modular & centrally managed	This clause to be read as "UTM should provide Firewall and IPS features. Both should be available as separate independent modules and should be modular. The UTM device should be able to provide BOTs detection and provide protection against Botnets."
5	Point 15	Appliance should have Identity Awareness Capabilities	This clause stands deleted
6	Point 17	Firewall should have a provision to support Network DLP for SMTP,HTTP and FTP protocols	This clause should be read as "Firewall should be capable of providing protection against Botnets to avoid any data loss"
7	Point 19	The Rule Change Management process should have Tracking and Audit trails with Graphical comparison of Rule change with Session management and Change approval	The feature/functionality is important & needed. The same may be provided through equivalent mechanism.
8	Point 25	Firewall Throughput (Large Packets) should be minimum 4Gbps which is scalable to 8 Gbps or higher on the same box without addition of any other hardware	This clause should be read as "Firewall Throughput (Large Packets) should be minimum 6Gbps or higher on the same box without addition of any other hardware."
9	Point 26	Integrated IPS should be more than 3.5 Gbps	This clause should be read as "Integrated IPS should be minimum 3Gbps."
10	Point 33	Firewall Real-Time Monitoring, Management & Log Collection (with storage) should be a SINGLE Appliance / Server	This clause should be read as "Firewall Real-Time Monitoring, Management & Log Collection (with storage) should be a single/separate Appliance / Server"
11	Point 34	should support the system authentication with TACACS+, RADIUS	This clause should be read as "should support the system authentication with TACACS+/RADIUS"
12	Point 40	Firewall should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods	This clause should be read as "Firewall should support the authentication protocols RADIUS/TACACS, LDAP, and PKI methods
13	Point 48	IPS should have the functionality of Software Fail Open	This clause should be read as "IPS should have the functionality of Software/hardware Fail Open"
14	Point 49	IPS Software Fail Open functionality can be defined in terms Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required	This feature/functionality is important and required which may be provided through equivalent mechanism.
15	Point 58	Should have more than 80+ Categories based on Application types, Security Risk level etc	This clause should be read as "Should have more than 40+ Categories based on Application types, Security Risk level etc"
16	Point 59	Should support User and Group based policies	This feature/functionality is important and required which may be provided through either internal or external device/mechanism.

17	Point 60	Should provide Seamless and Agent-less integration with Active Directory	No change. Active Directrory integration is important and required feature. Additional mechanisms such as RADIUS etc are also allowed.
18	Point 62	SSL VPN portal for Secure web based connectivity for web applications, web based resources, shared files emails	This clause should be read as "SSL VPN portal for Secure web based connectivity for web applications, web based resources, shared files emails through internal/external solution"
19	Point 63	End Point Scanning on Demand for endpoint compliance and malware scanner, key loggers, trojans and Self remediation for out of compliance users	This clause stands deleted
20	Point 64	Secure Virtual Workspace for virtual environment, insulated from the host and encrypts and deletes browser and applications cache, files, etc when session ends	This clause should be read as "Secure Virtual Workspace for virtual environment, insulated from the host and encrypts and deletes browser and applications cache, files, etc when session ends through internal/external solution"
21	Point 65	Real-Time Monitoring, Management & Log Collection (with storage) should not be distributed to more than ONE server/appliance.	This clause should be read as "Real-Time Monitoring, Management & Log Collection (with storage)"
22	Point 73	Management should provide detailed Event analysis for Firewall, IPS, Application Control, DLP with reporting of all the components.	This clause should be read as "Management should provide detailed Event analysis for Firewall, IPS, with reporting of all the components."
23	Point 74	The solution should be IPv6 complaint and should have dual stack UTM & Firewall supporting all the features in IPv4 & IPv6.	No change. UTM should be IPv6 ready from day one.
C	**Annexure-II-4.Antivirus Antispam Gateway**		
1	General Requirements-Point-7	The solution should support SMTP and POP3 protocol	This clause should be read as "The solution should support SMTP protocol, however, support for POP3 protocol is desirable."
2	Anti-Virus Protection-point-30	The solution proposed should contain a network level Anti-Virus solution for the SMTP and POP3 traffic	This clause should be read as "The solution proposed should contain a network level Anti-Virus solution for the SMTP traffic, however, that for POP3 traffic is desirable."
3	Anti-Virus Protection-point-48	The solution should be able to protect registered documents for data leakage. Once registered the documents should be protected from leaking through SMTP traffic.	This clause should be read as "The solution should support to protect registered documents for data leakage. Once registered the documents should be protected from leaking through SMTP traffic."
4	System Administration-Point-74	Should generate reports showing the details of viruses found along with the username, time of access, URL accessed.	This clause should be read as "Should generate reports showing the details of viruses found along with the username, time of access, URL/Domains accessed.
5	Email Management		Currently, ERNET is using Sun Java Messaging system. ERNET is in process to procure new Messaging System. The bidder should provide agents to manage the same as well when ERNET request for the same."
D	**Annexure-II-1. Firewall**		

1	Point no-1	The Firewall should be an appliance based firewall	This clause should be read as "The Firewall should be an appliance based firewall based on open and scalable architecture."
2	Point no-5	Firewall should provide real world performance of 10 Gbps. Real world profile should include but not limited to HTTP, FTP , SMTP and IMAPv4	Add clause: Performance throughput asked is for real world traffic and not just only on UDP. The Bidder should submit Test Reports ascertaining real world perfomance as asked for.
3	Point no-10	Firewall should support atleast 100000 policies	This clause should be read as "Firewall should support atleast 30000 policies."
4	Point no-11	Firewall should be chassis based and should have at least 6 nos. of gigabit ports and 4 nos. of 10Gig ports with dedicated separate HA interface/port and management port.	This clause should be read as "Firewall should be appliance based dedicated device and should have at least 6 nos. of gigabit ports and 4 nos. of 10Gig ports with dedicated separate HA interface/port and management port. The appliance should support/have interfaces scalability of 40% of the asked capacity.
5	Point no-21	Firewall should support dynamic downloading and enforcement of ACLs on a per-user basis once the user is authenticated with the appliance.	This clause should be read as "Firewall should support dynamic downloading and enforcement of ACLs on a per-user basis once the user is authenticated with the appliance(Internally/externally)."
6	Point no-22	Firewall should provide application inspection services for applications like HTTP, FTP, SNMP, DNS, SMTP, NFS, LDAP etc.	This clause should be read as "Firewall should provide application inspection services for applications like HTTP, FTP, SNMP, DNS, SMTP, NFS, LDAP, SIP, TFTP, etc."
7	Point no-24	Firewall should be able to block popular peer-to-peer applications and should have botnet filtering capabilities.	Add clause as "Botnet Filtering capabilities should also include blocking communication between the infected Bots and the Command & Control Centers."
			Add clause as "Botnet Filtering capabilities are must. It should have it's own reputation/ dynamic database to provide dynamic filter database about Botnets providing protection against spyware, adware, malware, data tracking, adult content that are used for distribution of above etc"
8	Point no-26	Firewall should support HTTP security services such as - RFC compliance, protocol anomaly detection, protocol state tracking, Uniform Resource Identifier (URI) length enforcement	This clause should be read as "Firewall should support HTTP security services such as checking for RFC 2616 Conformance, use of RFC defined methods only, protocol anomaly detection, protocol state tracking, Uniform Resource Identifier (URI) length enforcement"
9	Point no-27	Firewall should support H.323 security services such as – H.323 v3 & v4 with Direct Call Signaling, NAT & PAT support for H.323 services.	This feature/functionality is important and required which may be provided through either internal or external device/mechanism.
10	Point no-28	Firewall should support SIP security services such as – ability to secure both UDP and TCP based SIP environments, NAT & PAT based address translation support for SIP phones.	This feature/functionality is important and required which may be provided through either internal or external device/mechanism.
11	Point no-29	Firewall should support inspection of H.323 and SIP voice traffic	This feature/functionality is important and required which may be provided through either internal or external device/mechanism.

12	Point no-34	Firewall should support IPSEC and SSL VPN functionality simultaneously.	This clause should be read as "Firewall should support IPSEC and SSL VPN functionality simultaneously (internally/ externally) for unlimited users.
13	Point no-37	Firewall should support Suite B Cryptography	This clause should be read as "Firewall should support Suite B cryptography including ECDSA, ECDH & SHA-2."
14	Point no-41	Firewall should support IPSec IKEv2 or latest (site to site and VPN remote access)	This clause should be read as "Firewall should support IPSec IKEv2 or latest (site to site and VPN remote access) with advanced algorithms such as SHA-256, SHA-384, SHA-512, etc."
15	Point no-42	Firewall should support SSL Clientless access	This clause should be read as "Firewall should support SSL Clientless access(Internally/ externally)"
16	Point no-43	Firewall should support SSL access via a Client	This clause should be read as "Firewall should support SSL access via a Client(Internally/externally)"
17	Point no-44	Firewall should support SSL and IPsec encryption performed by dedicated hardware processors	This clause should be read as "Firewall should support SSL and IPsec encryption performed by dedicated hardware processors(Internally/ externally)." Having dedicated hardware acceleration engines is a standard guideline specially for resource intensive tasks such as encryption hence dedicated hardware is required for the same.
18	Point no-45	Firewall should support Active/Passive High Availability	The entire solution should be implemented in HA mode including the HA port
19	Point no-70	Online Certificate Status Protocol (OCSP)	The clause should be read as " Online Certificate Status Protocol (OCSP) (Internally/externally)
20	Point no-74	RSA Keon	This clause stands deleted
21	Point no-75	iPlanet (Netscape)	This clause stands deleted
22	Point no-76	Baltimore	This clause stands deleted
	Point no-75	iPlanet (Netscape)	This clause stands deleted
23		Request for addition	Add clause as "Firewall should be able to integrate with Active Directory without any additional hardware/software at the firewall end."
24		Request for Consideration	Add clause as "Firewall should support virtual firewall capability with minimum 200 virtual firewalls"
E	**Annexure-II-2. IPS**		
1	Point -2.	IPS appliance should have minimum 8 Gbps performance capacity and should have capability to process minimum 8 Gbps Layer-7 throughputs	This clause should be read as "IPS appliance should have minimum 8 Gbps performance capacity and should have capability to process minimum 8 Gbps Layer-7 throughputs with scalability of 40% of the asked performance capacity in the future"
2	Point-4.	IPS system should have High Availability mechanism of pass-thru to allow traffic flow uninterrupted during the power failure or Hardware issues for minimum of 4 Gigabit copper segments.	No change. The IPS has been asked in High Availability mode(1+1) working active-active configuration. Please refer Annexure-I(Schedule of requirement)
3	Point-5.	IPS should not offer latency more than 100 micro seconds.	This clause should be read as "IPS should not offer latency more than 150 micro seconds. Documentary proof in the form of test report should be submitted."

4	Point-12.	IPS system should have multicore CPU architecture for scalability, deep packet inspection and performance.	This clause should be read as "IPS system should have multicore CPU/ASIC/NPU architecture for scalability, deep packet inspection and performance."
5	Point-18.	Should have enhanced visibility into IPv6 traffic	This clause should be read as "Should have enhanced visibility into IPv6 traffic. IPS should be IPv6 ready from day one."
6	Point-19.	IPS system should provide a provision to export real time signature information of ongoing DOS/DDOS attacks and malware propagation.	This clause should be read as "IPS system should provide a provision to export real time signature information of ongoing DOS/DDOS attacks, malware propagation, protection against HTTP page flood attacks and DNS critical infrastructure against flood attack that misuse DNS server resources."
7	Point-20.	IPS system should have following Attack detection & mitigation capability for following:	
	n)	IPS system should provide protection against following zero day server cracking techniques	
	(ii)	Web sites application vulnerability scanning and hacking protection.	This feature/functionality is important and may be provided through equivalent mechanism.
	r)	Server cracking protection	This feature/functionality is important and may be provided through equivalent mechanism.
	t)	Horizontal and vertical scanning protection	This feature/functionality is important and may be provided through equivalent mechanism.
8	Point-23.	IPS System should support protection against encrypted SSL based attacks using an SSL accelerator either inbuilt or externally deployed in sniffing mode.	This clause should be read as "IPS System should support protection against encrypted SSL based attacks using an SSL accelerator either inbuilt or externally deployed in sniffing/inline mode."
9	Point-24.	For SSL traffic IPS should have minimum 1Gbps encrypted throughput and 5000 SSL CPS	This clause should be read as "For SSL traffic IPS should support minimum 1Gbps encrypted throughput and 5000 SSL CPS through SSL accelerator either inbuilt or externally deployed."
10	Point-27.	IPS System should have comprehensive Bandwidth Management capability for end to end QoS	
	i)	Rate shaping capability for provisioning Guaranteed and burst bandwidth	These clauses should be read as "IPS should have bandwidth rate limiting capability for QoS for provisioning bandwidth on various parameters for rate limiting purpose."
	ii)	Rate shaping policies per segment, per source/destination subnet, source/destination port, VLANID, Application header and Content based	
	iii)	TOS bits marking and reading	
	iv)	Application level QoS and traffic shaping.	
	v)	IPS system should have dynamic black list to suspend mallicious source IP's for predefined duration.	
11	Point-29.	Security Maintenance	
	iv)	IPS Should support Provision to add static own attack signatures up-to 2500.	Minimum capacity has been defined. Bidders may offer higher as well.
12	Point-32.	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 should send an event within a pre-defined reporting period.	The feature/functionality is important & needed. The same may be provided through equivalent mechanism.

13	Point-36.	IPS solution should be common criteria EAL-4 certified.	This clause should be read as “IPS solution should be common criteria EAL 2 certified or higher"
14		Additional suggestions	Add clause as: "IPS should support provide advanced botnet protection using heuristic detection methods."
F	**General Conditions**		
1	5. Eligibility Criteria- a) v	The bidder should have been in the business of ICT, data network and their security implementation / integration related activities for at least the past 5 years. The Network Security equipment Installation, Integration and Project Management services should not be sub-contracted and should be executed only by the employees of the Bidder Company who are on its payrolls. The Bidder shall submit the declaration duly signed and stamped by Bidder’s authorized signatory regarding these along with the bid. The bidder should have OEM certified engineers at each service site.	No change. This clause is self-explanatory. An undertaking to this effect duly signed & stamped should be submitted by the Bidder's authorised signatory
2	5. Eligibility Criteria- a) ix	The bidder should have an office in the Delhi state/ NCR with support centers manned with their own qualified engineers across India with a Toll Free number.	No change. An undertaking duly signed & stamped by Bidder's authorised signatory with confirmation of details as required should be given.
3	5. Eligibility Criteria- a) xii	The bidders should give clause-by-clause compliance for the technical specification of the equipments as in the tender document in their technical bids. Also give compliance of all the terms & conditions as mentioned in the Tender document.	No Change. The bidder should submit unconditional compliance as requested in this clause of the tender
4	5. Eligibility Criteria- a) xiii	All the equipment & devices should be properly configured. There should not be any deliberated vulnerability left in the equipment. In case, any deliberate vulnerability is observed in the equipment later on, the bidder/OEM of the equipment/systems should be liable to penalty as per DoT Amendment of ISP license agreement for security related concern no. 820-01/2006-LR (Vol.II) Pt. dated 03.06.2011. An undertaking to this effect should be given by the bidder/OEM.	No Change. The bidder should submit unconditional compliance as requetsed in this clause of the tender
5	5. Eligibility Criteria- b) ii	OEMs whose products have been offered in the bid shall have Technical Assistance Centre(TAC) in India and shall have Toll Free Number for TAC to support the equipment at each location. OEM(s) should have direct presence with their own office in India manned with their own engineers for minimum of last 5 years. Relevant documentary proof should be submitted	No change. The bidder should submit any relevant documentary proofs which confirm this clause for its compliance
6	5. Eligibility Criteria- b) iii	The OEM should have good global reference for their products in Education & Research network. Documentary proof should be submitted.	No change. Appropriate documents confirming the criteria should be provided.

7	5. Eligibility Criteria- b) iv	The OEM should have minimum turnover of Rs. 100.00 Crores each year during the last three financial years. Attested & audited copies of the company's annual reports for the years 2009-10, 2010-11 and 2011-12 have to be attached along with the bid, duly certified by the Charted Accountant.	This clause should be read as "The OEM should have minimum turnover of Rs. 100.00 Crores(or equivalent in US Dollars) each year during the last three financial years. Attested & audited copies of the company's annual reports for the years 2009-10, 2010-11 and 2011-12 have to be attached along with the bid, duly certified by the Charted Accountant. Relevant documents confirming above required turnover in US Dollars should be submitted"
8	Annexure-I item at s.no. 1 of Schedule of requirement	Firewall: Appliance based stateful firewall with all hardware, accessories, licenses, softwares, etc. to provide perimeter layer of protection to the Network Infrastructure and resources. Should have two appliances configured in High Availability mode (1+1) working in active-active configuration with each appliance has 4 x 10 Gigabit Ethernet ports, 6x1Gigabit Ethernet ports and Redundant Power Supply	No change. The description of the item in the Table(Annexure-I) is clear & self-explanatory which clearly confirms that each of five locations should have two appliances configured in High Availability mode (1+1) working in active-active configuration.
9	Annexure-I item at s.no. 5 of Schedule of requirement	UTM: Appliance based Unified Threat Management System with firewall, and IPS systems with all hardware, accessories, licenses, softwares, etc. Should have two appliances configured in High Availability mode (1+1) working in active-active configuration with each appliance has 8 x 1Gigabit Ethernet ports and Redundant Power Supply	No change. The description of the item in the Table(Annexure-I) is clear & self-explanatory which clearly confirms that each of five locations should have two appliances configured in High Availability mode (1+1) working in active-active configuration.
10	Annexure-I item at s.no. 6 of Schedule of requirement	Comprehensive Annual Maintenance (AMC)/ support of Two Years after Warranty period of Three Years	Please refer General conditions clause 24 of the tender which is self-explanatory.
11	Annexure -I, item at 3-a,b,c & d	EMS	Additional licenses are required for future requirement. Annexure-I-3(a) & 3(c) are required immediately and 3(b) & 3(d) are required in future as per the requirement.
12	General Condition-clause 24	Warranty & SLA Uptime	Please add in clause 24.1 as "The maximum deduction will be upto total amount of bank guarantee submitted by the bidder during warranty and that during AMC period will be upto total amount of AMC for that year"
13	General Conditions-clause 33	Scope of Work-iv: One Resident Engineer ……to decide L1 bidder.	This clause should be read as "One Resident Engineer with Educational Qualification of B.E, / B. Tech in Engineering/ Technologies in Electronics / Communication / Computers with minimum 3 years experience in the offered products to be posted at each of 5 large PoPs during warranty & AMC period. Cost of resident engineer at all the 5 locations per annum basis for five years should be provided in the price schedule and will be calculated to decide L1 bidder. Onsite Resident Engineer should be provided for 8 hour shift for 6 days a week and on call during holidays."

14		Additional Request	Add clause 34 in General Conditions of tender as "Force Majeure:ERNET may grant an extension of time limit set for the completion of the work in case the timely completion of the work is delayed by force majeure beyond the contractor's control, subject to what is stated in the following sub paragraphs and to the procedures detailed there in being followed. Force majeure is defined an event of effect that cannot reasonably be anticipated such as acts of God (like earthquakes, floods, storms etc.), acts of states, the direct and indirect consequences of wars (declared or un-declared), hostilities, national emergencies, civil commotions and strikes (only those which exceed a duration of ten continuous days) at successful bidder's factory. The successful Bidder's right to an extension of the time limit for completion of the work in above mentioned cases, is subject to the following procedures: a) That within 10 days after the occurrence of a case of force majeure but before the expiry of the stipulated date of completion, the bidder informs the ERNET in writing that the bidder considers himself entitled to an extension of the time limit. b) That the successful bidder produces evidence of the date of occurrence and the duration of the force majeure in an adequate manner by means of documents drawn up by responsible authorities. c) That the successful bidder proves that the said conditions have actually been interfered with the carrying out of the contract. d) That the successful bidder proves that the delay occurred is not due to his own action or lack of action 34.1 Apart from the extension of the time limit, force majeure does not entitle the successful bidder to any relaxation or to any compensation of damage or loss suffered.
15		Additional Request	Add in tender Clause 5-iii (Eligibility Criteria) as "The Bidder should provide documented proof for back to back support from OEM."
16		Additional Request	The tender document as uploaded on 7-9-2012 on ERNET website was in PDF format.

17		Additional Request	Add clause 35 in General Conditions of tender as "TERMINATION 35.1 The Purchaser, may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the supplier, terminate the contract in whole or in part, a) if the supplier fails to execute the contract within the time period (s) specified in the contract, or any extension thereof granted by the Purchaser. b) if the supplier fails to perform any other obligation (s) under the contract; c) if the supplier, in either of the above circumstances, does not remedy his failure within a period of 3 days (or such longer period as the Purchaser may authorize in writing) after receipt of the default notice from the Purchaser. d) On a notice period of 7 days.
			35.2 In the event the Purchaser terminates the contract in whole or in part pursuant to above sub-clause, the Purchaser may procure, upon such terms and in such manner as it deems appropriate, goods/services similar to those undelivered and the supplier shall be liable to the Purchaser for any excess cost for such similar goods/services. However, the supplier shall continue the performance of the contract to the extent not terminated. 35.3 The Purchaser may at any time terminate the Contract by giving written notice to the supplier, without compensation to the supplier if it becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination will not prejudice or effect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.
18		Additional Request	Add clause 36 in General Conditions of tender as "Arbitration This Contract shall be governed by laws of India. Disputes arising out of this contract shall be first referred to the senior executives of each party for an amicable solution. If the dispute is not resolved within a period of thirty (30) days, the same shall be referred to arbitration in accordance with Arbitration and Conciliation Act, 1996 (including all amendments thereto). Each party shall appoint one arbitrator each and the two appointed arbitrators shall appoint the third arbitrator. The decision of the arbitrators shall be final and binding on both parties. The venue of arbitration shall be New Delhi, India. Subject to the above, this contract shall be subject to the jurisdiction of the courts of New Delhi, India."

19	Addition		Add clause 37 in General Conditions of the tender as " ERNET India will entered into a Rate Contract with selected bidder to cater it's users'/customers' and own requirements which will be valid for a period of Twenty-Four (24) Months in the first instance from the date of award of contract. It may be extended for a further period of Six (6) Months (at ERNET's Option and mutual agreement with bidder and depending upon the need for continuity of the hardware technology/architecture). The selected bidder will supply, install & commission different equipment & services at the rates finalized through this tender during the period(including extended period) of rate contract. The Unit rates finalised through this tender will be used to place the purchase orders based on requirement during the validity of the rate contract."
20	5. Eligibility Criteria- a)		Add clause at 5. Eligibility Criteria- a)-(xiv) of the tender as "The bidder should ensure that all the equipment and softwares quoted should be IPv4 and IPv6 ready from day one"
21	Addition		Add clause 38 in General Conditions of the tender as " The bidder shall organise technical training about the equipment after installation and commissioning has been completed . Training will be provided on no additional cost for a batch of 15-20 people for 5 days in New Delhi. All the training material will be provided by the Implementation Agency/bidder."
22	Annexure -I, item at 7	Resident Engineer	The Qty(Quantity) should be read as 5

Note: Subject to the above amendments, all other terms & conditions and specifications of the tender documents remain unchanged.