भारतीय उष्णदेशीय मौसम विज्ञान संस्थान

पाषाण, पुणे – 411 008

INDIAN INSTITUTE OF TROPICAL METEOROLOGY
PASHAN, PUNE – 411 008

निविदा सं. सी-050-26/निविदा/02/2011

<u>निविदा सूचना/TENDER NOTICE</u>

निदेशक, भारतीय उष्णदेशीय मौसम विज्ञान संस्थान, डॉ. होमी भाभा रोड, पाषाण, पुणे – 411 008 (भारत) नेटवर्क सुरक्षा प्रणाली की आपूर्ति एवं संस्थापन हेतु ख्यातिप्राप्त आईटी/सुरक्षा सामग्री विक्रेता से पृथक मुहरबंद लिफाफे में मुहरबंद निविदाएं (भा -I तकनीकी बोली, भा -II वाणिज्यिक बोली) आमंत्रित करते हैं :

Director Indian Institute of Tropical Meteorology, Dr. Homi Bhabha Raod, Pashan, Pune – 411 008 (India) invites sealed tenders (Part-I-Technical bid, Part-II- Commercial Bid) in separate sealed covers from Reputed IT / Security vendors for supply and Installation of Network Security System.

विस्तृत निविदा दस्तावेज एवं तकनीकी विशिष्टताएं संस्थान के अभिकलित्र एवं आँकड़ा प्रभा के कार्यालय से प्राप्त किए जा सकते हैं।

Detailed Tender Documents and Technical Specifications can be obtained from the office of Computer and Data Division of this Institute.

बोली पूर्व बठक की तिथि एवं समय	: 19 सितंबर 2011 1100 बजे
Pre-bid meeting date and time	: 19th September 2011 at 1100 hrs.
भाउमौविसं,पुणे में निविदा प्राप्त होने की अंतिम तिथि	: 29 सितंबर 2011 1200 बजे तक
Last date of receipt of Tender at IITM, Pune	: 29th September 2011 upto 1200 hrs.
निविदा खोलने की तिथि (केवल तकनीकी बोलियाँ)	: 29 सितंबर 2011 को 1600 बजे
Opening of Tenders (Technical bids only)	: 29th September 2011 at 1600 Hrs.

संस्थान को किसी निविदा या सभी निविदाओं को बिना कारण बताए निरस्त करने का अधिकार ह। विस्तृत विवरण हेतु कृपया हमारी वेबसाईट **www.tropmet.res.in** देखें।

The Institute reserves the right to reject any or all tenders without assigning any reason thereof. For further details please visit our web site : **www.tropmet.res.in**

अभिकलित्र अभियंता/Computer Engineer

कृते निदेशक/For Director

jeelani@tropmet.res.in

भारतीय उष्णदेशीय मौसम विज्ञान संस्थान

INDIAN INSTITUTE OF TROPICAL METEOROLOGY,

(पृथ्वी विज्ञान मंत्रालय का स्वायत्त संस्थान, भारत सरकार के अधीन)

(An Autonomous Institute of the Ministry of Earth Sciences, Govt. of India)

सं. / No. C-050-26 **दिनांक / Date 26.08.2011**

To

M/s .

Sub : Network Security System

Dear Sirs,

Sealed Quotations are invited in two bid format from reputed and experienced vendors for Turnkey solution of **''Network Security System.''**

You are therefore requested to submit the filled quotation in two bid format complying all the terms and conditions as mentioned in Annexure – I and II so as to reach this Institute on or before **29th September 2011 at 1200 Hrs.**

Thanking you,

Yours Sincerely,

(S.U. Athale)
STO-II
Computer & Data Division
For Director

Encl : 1 Terms & Conditions
2 Specifications

तार : ट्रॉपमेट, पुणे Grams : TROPMET, PUNE
फैक्स : Fax : (020) 25893825 दूरभाष : Telephone - 25893600 / 25893675 - 81
डॉ. होमी भाभा मार्ग, पाषाण / Dr. Homi Bhabha Road, Pashan, पुणे / Pune - 411 008 (भारत / India)

ANNEXURE-I

INDIAN INSTITUTE OF TROPICAL METEOROLOGY, PUNE – 411 008
TERMS & CONDITIONS

ENQUIRY NO: C-050/26/2011 Tender Notice No: C-050/26/02/2011

1) The Tenderers are requested to give detailed sealed tender in their own forms in two Bids i.e.
Part – I Technical Bid.
Part - II Commercial Bid, both the bids addressed to the Director, Indian Institute of Tropical Meteorology, Dr. Homi Bhabha Road, NCL Post, Pashan, Pune – 411 008, INDIA.

2) This tender is not transferable.

3) Complete tender document is available on Institute's website http://www.tropmet.res.in. If a request is made to IITM for Tender Documents a sum of **Rs.1000/- (Rs. One Thousand only) (Non-refundable)** has to be paid in the form of Demand Draft drawn in favour of "The Director, Indian Institute of Tropical Meteorology, Pune" **preferably from Nationalized Bank**. No Tender fee is required if downloaded from website.

4) Tenders addressed to the Director, Indian Institute of Tropical Meteorology, Pune 411008 are to be submitted for each item in duplicate in double cover, under two bids system. Superscribed with Tender No. for purchase of **"Network Security System – 01 Set** due on **29th September 2011.**

5) You have to submit two separate bids in two separate envelopes and you may keep both the bid envelopes in an envelope for sending to us.

One envelope will contain only the TECHNICAL SPECIFICATIONS of the indented equipment and compliance report (line by line) along with EMD.

Another envelope will contain only the financial bid in which price and any other information, which has financial implications, will only be given.

The main envelope, which will contain both the bids, should be super scribed with our **tender enquiry No. C-050.26/Tender/02/2011 due on 29th September 2011.**

6) Please indicate page nos. on your quotation ex. If the quotation is containing 25 Pages, please indicate as 1/25, 2/25, 3/25 ----------25/25.

7) Cost of the items should be mentioned clearly in the Commercial Offer (Part-II) only and should be quoted in Indian Rupees.

8) Last date for the receipt of completed tender is up to 12:00 hrs. on **29th September 2011 & technical bids** will be opened on the same day at 1600 hrs in the presence of the representatives of the vendors present.

9) The prebid meeting is scheduled on 1**9th September at 1100 hrs.** for discussions.

10) The tender must be valid for a period of at least **90** days from the date of opening.

11) The purpose of certain specific conditions is to get or procure best Equipment / service etc. for IITM. The opinion of Technical Committee shall be guiding factor for Technical short listing.

12) **Vendor shall finally warrant that all the stores, equipment and components supplied under the SUPPLY ORDER shall be new and of the first Quality according to the specifications and shall be free from all the defects (even concealed fault, deficiency in the design material and workmanship**).

13) Tender must clearly indicate the features offered unit price, VAT tax, transport, transit-insurance, installation charges..etc. . **The vendor should mention the price of the equipment and the duties/taxes to be paid such as customs duty/excise duty/VAT/Octroi etc. separately.**

14) **The complete equipment including operational manuals should be supplied within stipulated period mentioned in the LOI/supply order and the vendor should install the equipment within fifteen days after the delivery of the equipment**.

15) As this Institute is exempted from payment of Custom Duty, Excise Duty and Octroi, exemption certificates will be issued on request.

16) The equipments must carry on-site warranty for **Three Years** from the date of taking over of the equipments after the acceptance tests. Warranty period will stand extended for a period of total downtime of the equipments.

17) The vendor has to furnish a Bank Guarantee to the extent of 10% of the order value from a nationalized bank in the prescribed format valid for the entire period of warranty including extension if any.

18) No advance can be paid.

19) The **payment terms** shall be as follows:

i) 70% payment against delivery.

ii) 20% payment after satisfactory installation, and successful completion of acceptance tests and training.

iii) 10% payment after execution of Bank Guarantee from a Nationalized Bank and successful completion of acceptance test. The Bank Guarantee will remain valid until the expiry of warranty period including the extensions if any.

20) The prices quoted should be firm and irrevocable and not subject to any change whatsoever, even due to increase in cost of raw material components and fluctuation in the foreign exchange rates and excise duty.

21) Vendor should arrange complete training on the entire solution atleast three members from this Institute free of charge on his own cost.

22) Indicate the names of the Indian reputed Organizations where you have supplied the similar equipment and may attach the satisfactory performance report of the Similar work from user Organization.

23) a) If you have supplied identical or similar equipment to other Institutes under Ministry of Earth Sciences and Ministry of Science & Technology, the details of such supplies for the preceding three years should be given together with the prices eventually or finally paid.

b) Based on the above information IITM will have its option to obtain details of the equipment, their performance, after sales services etc. for evaluation of the tender, directly from the concerned Labs. /Scientists etc.

24) The Institute is autonomous scientific research organization under the Ministry of Earth Sciences and is a recognized center for studies leading to M.Sc., M.Tech and Ph.D. of the University of Pune and various other Universities. As such, all possible concessions / discounts / rebates applicable for educational Institutions may be given.

25) Any upgrade of OS and associated other software during the warranty period should be supplied free of charge.

26) The vendor should have appropriate facilities and trained personnel for supply, installation and warranty-maintenance of the equipment to be supplied. Detailed information in this regard may be furnished.

27) Kindly attach a copy of your latest DGS&D, New Delhi registration Certificate under the compulsory Scheme of Ministry of Finance regarding the registration of Indian Agent of foreign supplier wherever it is applicable.

28) The Tenderer is required to furnish the Permanent Account Number (PAN) Allotted by the Income Tax Department. If registered with the National Small Industries Corporation, the registration number, purpose of registration and the validity period of registration' etc. should also be provided in Technical Bid for Indian Agents.

29) Vendor should clearly mention in the Technical Bid from the following:

- **Make and model of item quoted.**
- Delivery period.
- Company profile with a list of those institutes/users should be attached where vendor has supplied the equipments in question in past.
- A letter of AUTHORISED REPRESENTATIVE from the Principal should invariably be attached with quotation
- A copy of latest Income Tax clearance Certificate from Income Tax Department (INDIA)

30) Octroi payment if any, the same may please be shown separately.

31) The Tenderers are requested to quote for Educational Institutional Price for equipment, since we are eligible for the same.

32) Acceptance tests to be prescribed later will be carried out after installation and the items will be taken over only after successful completion of the acceptance tests.

33) The equipments are required to be installed at **IITM**, **Pune.**

34) The equipment will be networked by the vendor in the existing **LAN** of the Institute.

35) The item should be supplied with manuals and the manuals including technical Literature / Electronic drawings / circuit diagrams should be complete in all respects to operate the system without any problem.

36) The Tenderer has to state in detail the Electrical Power/UPS requirements, floor Space, head room, foundation needed and also to state whether Air-conditioned environment is needed to house the system and to run the tests. i.e. pre-installation facilities required for installation may please be intimated in the technical bid. *

37) Goods should not be dispatched until the Vendor receives a firm order.

38) The Date and Time of opening for Part-II (Commercial Bid) will be intimated only to pre-qualified and technically acceptable Tenderers for the item at a later date.

39) **Earnest Money Deposit:**

a) **The Earnest Money Deposit of Rs. 1,00,000/- (Rs. One lakh only) must be paid / sent along with your technical bid in the form of a Demand Draft, Banker cheque or Bank Guarantee (from a Nationalized Bank only) drawn in favour of The Director, Indian Institute of Tropical Meteorology, Pune payable at Pune, otherwise your technical & financial bids will not be considered at all**. The Earnest Money of successful bidder will be returned only after installation, satisfactory demonstration and on acceptance of the equipment by the user Scientist / HOD as per the terms of our purchase order. If the successful bidder fails to fulfill the contractual obligations before the due date, he will forfeit the EMD.

The Earnest Money of the unsuccessful bidder whose technical bid has not been found suitable will be returned within **One Month** after receipt of Technical Committee recommendations.

b) Those who are registered with Central Purchase Organization (e.g. DGS&D), National Small Industries Corporation or the concerned Ministry / Department need not to furnish EMD along with their bids.

c) Though EMD has to be submitted by Demand Draft, Banker's Cheque or Bank Guarantee, we prefer to have Bank Guarantee for easy return to the bidders once a decision is taken by IITM. (Specimen of Bank Guarantee is enclosed at Annexure 'A').

d) **Tenders not accompanied with Demand Draft I Bank Guarantee towards "Earnest Money Deposit" will summarily be rejected**.

40) Part and incomplete tenders are liable to be rejected.

41) Conditional Offers will not be considered.

42) The tenders must be clearly written or typed without any cancellations / corrections or overwriting.

43) **Fax** / **E-mail** / **Telegraphic** / **Telex tenders will not be considered.**

44) IITM will not be responsible:
    a) For delayed / late quotations submitted / sent by Post / Courier etc.
    b) For submission / delivery of quotations at wrong places other than the Office of Director, IITM, Pune – 411 008.

45) If the vendor fails to Supply and Install the system as per specifications mentioned in the order within the due date, the Supplier is liable to pay liquidated damages of one percent value of the Purchase Order awarded, per every week delay subject to a maximum of 10% for every week beyond the due date and such money will be deducted from any money due or which may become due to the vendor.

46) **Venders should submit a bar chart along with technical bid for supply of equipment and for completion of work, failing which technical bid shall not be considered. The entire project is expected to be completed within (5 weeks for equipment supply + 15 days for completion) 7-8 weeks from date of Issue of LOI.**

47) In case of any dispute regarding part-shipment, non-compliance of any feature etc., the Director, Indian Institute of Tropical Meteorology, Pune will be the final authority to decide the appropriate action and it will be binding on the vendor.

48) The quantity is likely to be increased in future.

49) The vendor needs to submit manufacturer's authorization form with tender enquiry number listed.

50) The Vendor Should give an SLA for (24X7) support valid for three years with 2 hours response time and same day resolution.

51) The vendor needs to have a full fledged office, PoC or testing centre to showcase and test the functionality of the ordered equipments in Pune.

52) The commercial evaluation criteria shall be based on total cost of ownership for a period of five years.

53) Vendors should quoted for additional two years license and warranty as an optional quote.

54) The vendor should have a full fledge office in Pune with a complete Technical team and the principle should have a TAC opening in India (24x7).

55) The vendor should have supplied and deployed similar kind of Installation in govt. Institutes Like IITM (research and educational). Completion certificate for the same should be enclosed.

56) The vendor should conduct survey on any of the working days and working hours, if needed, so as to ensure the completion of entire project since it will be awarded on turnkey basis.

57) Last Date and Time for receipt of Tenders: **Upto 1200 hrs. on 29th September 2011.**

58) Date and Time of opening of Tenders : **At 1600 hrs. on 29th September 2011.** (Part - I Technical Bid only).

59) Director reserves the right to reject any or all tenders without assigning any reason.

BID Security Form

Where as 1 (hereinafter called ‘‘The Bidder’’) has submitted its bid dated (date of submission of bid) for the supply of _____ (Name and /or description of the goods.) (Here in after called ‘‘the Bid’’).

KNOW ALL PEOPLE by these presents that WE _____ (name of bank) of (name of the country), having our registered office at (address of bank)(hereinafter called "the Bank"), are bound unto (name of Purchaser) Hereinafter called ‘‘ The purchaser’’) in the sum of _____ for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents. Sealed with .the Common Seal of the said Bank this ____ day of 20 ___ The CONDITIONS of this obligation are.

1. If the Bidder withdraws it's bid during the period of bid validity specified by the Bidder on the Bid Form; or
2. If the Bidder, having been notified of the acceptance of it's bid by the Purchaser during the period of bid validity:
   a) fails or refuses to execute the; Contract Form if required; or
   b) fails or refuses to furnish the performance security, in accordance with the Instruction to Bidders.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, Without· the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it , owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee shall remain in force up to one year after the period of the bid validity, and any demand in respect thereof should reach the Bank not later than the above date.

(Signature of the Bank)
Name of Bidder.

ANNEXTURE- II

TECHNICAL SPECIFICATIONS DOCUMENT

STANDARD ABBREVIATIONS:

1. *AV - Anti Virus*
2. *IPS - Intrusion Prevention Systems*
3. *SPI - Stateful Packet Inspection*
4. *VPN - Virtual Private Network*
5. *ICSA - International Computer Security Association*
6. *EAL - Evaluation Assurance Level*
7. *HA - High Availability*
8. *RoHS - Restriction of Hazardous Substances*
9. *NAT - Network Address Translation*
10. *IEEE - Institute of Electrical and Electronics Engineers*
11. *RIP - Routing Information Protocol*
12. *OSPF - Open Shortest Path First*
13. *BGP - Border Gateway Protocol*
14. *ISIS - Intermediate System To Intermediate System*
15. *ECMP - Equal Cost Multipath Protocol*
16. *RFC - Request for Comments*
17. *PIM - Protocol Independent Multicast*
18. *AES - Advanced Encryption Standard*
19. *SHA - Secure Hash Algorithm*
20. *L2TP - Layer 2 Tunneling Protocol*
21. *SSL - Secure Sockets Layer*
22. *IPSec - Internet Protocol Security*
23. *PPTP - Point-to-Point Tunneling Protocol*
24. *DES - Data Encryption Standard*
25. *AES - Advanced Encryption Standard*
26. *NNTP - Network News Transfer Protocol*
27. *MIME - Multipurpose Internet Mail Extensions*
28. *TTL - Time to live*
29. *DSCP - Differentiated Services Code Point*
30. *DNSBL- DNS-based Blackhole List*

1. **General Requirements:**

   a. The general purpose requirement is for a comprehensive security solution of high firewall throughput (~ 40 Gbps) with high VPN throughput (~ 10 Gpbs) for Securing and Sharing High Performance Computing and other institutes resources with two factor Authentication solution and other security features as mentioned below. The solution is required to be deployed in virtualized context environments and High Availability, in order to consolidate the existing multiple security infrastructures along with complete redundancy as per the Institutes Network & Security design requirements.

   b. The solution/s should be based on design of processors for acceleration of Antivirus, stateful packet header inspection, VPN encryption/decryption, protocol anomaly offloading, and quality of service enforcement and other essential security features as mentioned below. It should also provide acceleration for processing of all packet sizes which include time sensitive applications such as VoIP, real-time protocols, and multimedia applications.

   c. The Solution/s should be based on unlimited IP addresses license.

   d. The family of Product/s of the solution and the principle company should be certified by/for the following as per the applicable feature of the requirement.

      i. ICSA or equivalent industry leading third party certified
      ii. IPv6 certified
      iii. EAL4 or equivalent industry leading third party certified
      iv. RoHS complied
      v. NSS-Labs Approved or equivalent.
      vi. Internationally accepted marked/certified like UL/CUL, CE, ISI, VCCI..etc
      vii. ISO-9001 or CEI-CMM level Certified

2. **Base device Hardware Requirements:**

   a. The Product/s of the solution for the base firewall should give the following and similar secondary hardware/s to be considered for the HA environment.

      i. Minimum Two 10/100/1000 copper Ethernet Management Interfaces (Mgmt and heartbeat).
      ii. Minimum 2 Hardware accelerated 10 GbE SFP+ along with 10G SFP+ SR fiber optic transceivers and should be scalable up to minimum 8 10GbE ports.
      iii. Minimum 16 Fully loaded Hardware Accelerated 1-GbE SFP Interfaces with 1000base-TX.
      iv. Minimum 100 GB SSD Local storage capacity.
      v. A console port and minimum 2 USB ports..etc.
      vi. Redundant power supply Hot swappable (100-240V AC).
      vii. Should have operating conditions of 0-40 deg C and 20-90% non condensing Humid environment or better.

3. **System Operations and Management Requirements:**

   a. The System Software/OS is expected to be :

      i. Proprietary in order to prevent inheriting common OS vulnerabilities
      ii. Resided on flash disk for more reliability over hard disk
      iii. Should allow dual/OS selectable booting for last safe boot feature.
      iv. Should be Upgradeable via CLI, Web UI, TFTP..etc

   b. The configurations on the device shall:

i. Be easily backup or restored via GUI and CLI to/from local PC, remote management or USB disk
ii. Provide CLI command configuration file that is readable by Windows Notepad/Wordpad
iii. Have option for encrypting while taking backup.

c. The system should provide management access through:
i. GUI using HTTP or HTTPs access where administration service port can be configured, example via tcp port 8080..etc
ii. CLI console using console port, SSHv2, telnet which service ports can be configured.
iii. Access of CLI console through GUI is preferred.

d. The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACAS+ with option of 2 factor authentication

e. The system should support to created detailed profile/role base login accounts for administration and limited access accounts.

f. The system should be able to limit remote management access from specific trusted network/s or host/s with corresponding login account.

4. <u>Solution Requirement Details:-</u>

a. The solution should support virtualization for consolidation with minimum 10 virtual systems included and should be scalable to 100 plus.

b. The following features should be available in the virtualized context environment:

i. Firewall
ii. IPSEC & SSLVPN
iii. IPS settings
iv. Antivirus settings
v. Antispam settings
vi. URL Filtering Settings
vii. Application Control Settings
viii. User & Group settings
ix. Log & reporting settings
x. Support for Two factor Authentication config.

c. The system should be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes should be available concurrently using Virtual Contexts.

d. When running the unit/s in transparent/bridge mode, the system should be capable of configuring firewall policies to translate source or destinations addresses of packets as they pass through the unit.

e. The physical interfaces should be capable of link aggregation/trunking (IEEE 802.3ad standard). And should also allow for high availability (HA) by automatically redirecting traffic from a failed link in a particular trunk to the remaining working links.

f. The physical interfaces can be configured as VLAN trucks and should support more than 5000 vlans

g. The system should be able to support routing protocols including
i. RIPv1 & v2 (&ng)
ii. OSPF
iii. BGP-4
iv. ISIS
v. PIMv2

h. The system should provide minimum 10000 static routes and 200 policy routes or more

k. The system shall be able to provide outbound ISP side/Wan link load balancing capabilities using ECMP with optional methods of:

   i. Source IP based (source IP based)
   ii. Weight-based
   iii. Usage-based

l. The system shall be able to provide Wan link redundancy using ping probes

m. The System should inherit all the standard RFC's.

n. Token based Two Factor, centralized Logging and other requirements as mentioned below.

5. **Firewall Requirements**:-

a. Should give minimum 40 Gbps +- 10% throughput with the base unit or more.

b. Should be able to handle minimum 40 Lakh +- 10 % concurrent sessions or more.

c. Should be able to handle 1 Lakh new session per second or more.

d. Should be able to create 1 Lakh IPv4/IPv6 firewall policies or more.

e. Policy Features:

   i. Support for IPv4 and IPv6 GUI firewall policy.
   ii. Each policy should have address object(s) (IP, IP range, Subnet, FQDN and Geographical networks), service object(s), schedule Object(s), tags, comments..etc.
   iii. Filtration of policies based on selected objects.
   iv. URL redirect on a policy

f. Traffic shaping Features:

   i. Ability to enable and disable traffic shaping as per firewall policy.
   ii. Ability to set guarantee and max bandwidth per firewall policy.
   iii. Ability to pass Differentiated Service tagging and to tag packet for DiffSer.

g. Other Stateful Firewall Inspection Features:

   i. Policy based Network Address Translation (dynamic and static NAT)
   Minimum 10K Static NAT; one to one address mapping and static NAT groups
   ii. Minimum 2 ^ 11 IP pools for dynamic NAT
   iii. Port Forwarding
   iv. Authentication disclaimer.

6. VPN requirements

a. Should be ICSA IPSEC & SSL VPN or equivalent industry leading third party certified.

b. Should provide more than 10 Gbps +- 10% of VPN throughput for AES-256+SHA1 or better.

c. Should support the following:

   i. IPSEC VPN
   ii. PPTP VPN
   iii. L2TP VPN
   iv. SSL VPN

d. Should have hardware VPN acceleration for IPSEC (DES, 3DES, AES) encryption/decryption and SSL encryption/decryption.

e. IPSEC VPN features/capabilities:-

i. Multi-zone VPN supports.
ii. IPSec, ESP security.
iii. Support for Aggressive and Dynamic mode
iv. Hardware accelerated encryption using IPSEC, DES, 3DES, AES
v. Support for perfect forward secrecy group 1 and group 2 configuration
vi. MD5 or SHA1 authentication and data integrity.
vii. Automatic IKE (Internet Key Exchange) and Manual key exchange.
viii. Support for NAT traversal
ix. Support for Extended Authentication
x. Support for Hub and Spoke architecture
xi. Support for Redundant gateway architecture
xii. DDNS support

f. system should support IPSEC and PPTP VPN pass through so that computers or subnets on internal network can connect to a VPN gateway on the Internet

g. The system should support 2 forms of site-to-site VPN configurations

i. Route based IPSec tunnel
ii. policy based IPSec tunnel

i. The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode.

j. The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.

k. SSL VPN operation:

The SSL VPN should be able to operate in two modes
i. Web application based
ii. client server architecture based

l. SSL VPN features:

i. Should detect the browser type to download the appropriate client type - Java or ActiveX.
ii. Should be able to operate on all standard Operating systems with standard browsers.
iii. Should be able to perform host checking before SSL tunneling.
iv. Should be able to create bookmarks for SSL-VPN users.
v. Should be complied with the Two Factor Authentication System described below.

7. User/Two factor Authentication Requirements (Separate or Integrated device)

a. The Solution should be able to support various form of user Authentication methods simultaneously , including the facilitation for:

i. Minimum 5000 Local Database entries or more
ii. Minimum 10 LDAP server entries or more
iii. Minimum 10 RADIUS server entries or more
iv. Minimum 10 TACACS+ server entries or more
v. Single Signon ability.

b. Token requirements

   i. User Tokens should be available in the form of light portable hardware (eg. Keychains)
   ii. System should also be able to send OTP's in the form of email and or SMS.
   iii. Minimum 50 user hardware tokens should be included in the solution and should be scalable to 1000 user Tokens for two factor authentication.

c. The system should be able to create up to minimum 100 user groups which are lists of user identities. An identity can be:

   i. a local user account (user name and password) stored on the unit
   ii. a local user account with a password stored on a RADIUS, LDAP, or TACACS+ server
   iii. a RADIUS, LDAP, or TACACS+ server (all identities on the server can authenticate)
   iv. a user/user group defined on a Microsoft Active Directory server

d. When user authentication is enabled on a firewall policy, the authentication challenge is issued for any of the four selectable protocols:

   i. HTTP (can also be set to redirect to HTTPS)
   ii. HTTPS
   iii. FTP
   iv. Telnet

e. The solution should be on complete HA environment.

8. IPS Requirements (Separate or Integrated device)

a. The solution should be Internet Computer Security Association (ICSA) or equivalent industry leading third party certified.

b. The IPS through put should be minimum 5 Gbps for UDP traffic and minimum 1 Gbps for tcp traffic or better.

c. The IPS detection should have both technologies:
   i. Signature based detection using real time updated database
   ii. Anomaly based detection based on statistics and thresholds

d. Should be able to configure Denial of Service policies.

e. The system shall be able to create customized IPS signatures

f. The IPS Signature database should have more than 3,000 signatures and should be updated manually & automatically.

g. When a signature is matched, the following actions should be taken automatically:

   i. Logging the Detailed attack
   ii. Alert by email
   iii. SNMP traps
   iv. Packet logging
   v. Action on the session.

h. Should allow implementation of gradual IPS signature

i. The device shall allow administrators gradual IPS anomaly implementation by:
   i. Based on source and destination IPs
   ii. Based on thresholds values and actions

j. The solution /system is preferred in a HA environment.

9. Antivirus and Antispam Requirements (can be Integrated or Separate device)

9.1 **Antivirus**

a. The Antivirus system should be Internet Computer Security Association (ICSA) AV, Westcoast or equivalent industry leading third party certified.

b. The solution/system should be able to provide more than 1 Gbps of AV throughput.

c. The system should be able to block, allow or monitor using AV signatures and file blocking based as per firewall policy with configurable selection of the following services :

   i. HTTP, HTTPS
   ii. SMTP, SMTPS
   iii. POP3, POP3S
   iv. IMAP, IMAPS
   v. FTP, FTPS
   vi. Instant Messenger
   vii. NNTP

d. AV Signatures should be updated by pull, push or manual methods.

e. The system should be able to detect Grayware composing spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs apart from viruses that are designed to harm the performance of system in the network.

f. The system should be able to enable/disable heuristics engine, and block suspected file attachments.

g. The AV solution shall be able to quarantine blocked and infected files to either local hard disk or to an external defined location.

h. The system should be able to block or allow oversize file based on configurable thresholds values for each protocol types.

9.2 **Antispam**

i. The system should have the ability to provide antispam capabilities over SMTP, POP3 & IMAP.

j. The antispam solution should have the ability to use the following techniques:

   i. Inhouse IP address black list, URL black list and checksum database
   ii. IP address BWL
   iii. DNSBL & open relay lists check
   iv. MIME headers check
   v. Check on banned words in subject or body

k. The system should be able inspect SSL encrypted traffic for https, imaps, pop3s, smtps etc. and should also be able to perform AV scanning, Antispam , dataloss prevention etc.

10. URL/ Web Content Filter Requirements

a. The system should provide web content filtering features such as:

   i. Blocking web plug-ins such as ActiveX, Java Applet, and Cookies.
   ii. URL block
   iii. Keyword based block
   iv. Block Exempt List

b. The System should be able to query a realtime database with more than 5 crores rated websites under different categories.

c. The system should have the intelligence to display/block unblocked and blocked content in a mixed web page.

d. The system shall allow creating local website categories.

e. The system should be able to override database ratings with local ratings

f. The device should be able to send log messages when filter criteria is matched.

g. The system should be able to replace the web page when filter criteria is matched.

h. The system should be able inspect SSL encrypted traffic for https for URL filtering.

11. Web Caching, DLP, Proxy & Optimization

a. The system should have ability to store the web documents temporarily (cache) to reduce bandwidth usage, server load, and perceived lag.

b. The Cashing should support reverse, forward, explicit and transparent proxy caching of HTTP 1.0 and HTTP 1.1 web sites and configurations be based on RFC 2616 with IP/range of Source and destination, port etc.

c. The system should be able to be configured as explicit proxy with Proxy FQDN, Maximum HTTP request length, Maximum HTTP message length, adding headers to Forwarded Requests, Proxy Port, Interfaces that listen to proxy request..etc

d. The Data Loss prevention System should be able to identify, monitor and protect loss of data. Should be able to support multiple web, mail & IM, data transfer protocols and take appropriate actions (eg. Block, excempt, ban, ban sender, quarantine IP or interface, archive..etc) with options for configuration of various detection settings.

e. The System should be able to define optimization techniques for optimizing bandwidth, protocol optimization, byte caching technique, remote client WAN optimization, for traffic based on (Source & destination) IP/range, protocol, port no and monitoring of the same.

12. Application Control Requirements

a. The system/solution should have the ability to detect, log and take action against more than 1000 application signatures

b. The application signatures should be manual or automatically updated

c. The system should be able to define application control list based on selectable application group and/or list and its corresponding actions.

d. The system shall be able to set the Session TTL, apply traffic shaping and DSCP marking of the selected application/group.

e. The system should be able to manage and control VoIP usage.

f. The system should maintain statistics on selected IM and P2P applications, and VoIP protocols.

13. High Availability Requirements for as mentioned above

a. The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s. Any failure of Primary Hardware should be replaced same day with in 5 hours.

b. The solution should log the event, send snmp traps, send alert email when a fail-over occurs.

c. High Availability feature should be deployable either NAT/Route, Transparent or hybrid mode

d. The HA environment should have:

   i. Should be linearly scalable for higher redundancies and performance.
   ii. Active-Active redundancy
   iii. Active –Passive redundancy
   iv. Load sharing feature by using standard load balancing algorithms.
   v. Mutliple heart beats.
   vi. Support of interface link monitoring failover
   vii. Support for external ping probe failover
   viii. Option for defining master/primary and secondary.
   ix. Automated firmware upgrades.

14. Log & Report Requirements (Separate device required)

a. The solution should be capable of logging both internally and externally with the following components & options:

   i. dedicated centralized logging mechanism with minimum 1 TB raw storage
   ii. Minimum 4 10/100/1000 Ethernet interfaces
   iii. Buffer memory
   iv. syslog server options
   v. optional Hard Disk

b. Reports should be generated instantly or via schedules by the reporting device/s.

c. The Log and report solution should be able to:

   i. Provide web based real time attack log viewer /dash board.
   ii. Search and Filter the log.
   iii. Identify Correlated attack logs and top attacks information on at different periods of time.
   iv. Collect packet logs from the IPS device and display them real time.

d. The Solution should be not be license based (IP/device/usage/period) and should support and receive logs for minimum 100 reporting devices.

TECHNICAL COMPLAINCE STATEMENT

The Technical compliance statement is to be submitted completely filled in the below format w.r.t above details duly stamped and signed by the vendor along with technical bid.

SL No.	Complied/Deferred	Details if Deferred	Remarks
1.a			
1.b			
1.c			
1.d			
2.a			
3.a			
3.b			
3.c			
-			
-			
-			
-			
-			
-			
14.a			
14.b			
14.c			

NAME OF THE VENDOR

STAMP AND SIGNATURE

VENDOR PERFORMANCE STATEMENT FOR SIMILAR DEPLOYMENTS IN THE LAST THREE YEARS

Name of the Firm: _____

Pls note that vendors need to enclose supporting documents for the below details including satisfaction report.

Order placed by (full address of the purchaser)	Order No and date	Description and Qty of ordered equipment	Date of completion as per contract	Actual date of completion	Reasons for delay if applicable	Contact details for reference

NAME OF THE VENDOR

STAMP AND SIGNATURE

BILL OF QUANTITIES

Vendors should submit the BOQ in the following for format. Commercials are to be left blank in the technical bid, but other details like make & model No, description of stores and services, quantities..etc are to be duly filled and submitted along with technical bid.

Commercial rates are to be quoted in INR and are to be submitted only with commercial bid. All the applicable taxes till IITM's door delivery are to be considered while quoting tax details, tax exemption/concession benefits shall be transferred to IITM while execution/suuply/installation.

Sl No	**Details of Make & Model No /Description of Stores/ Services ..etc**	**Quantity (No of items, Set, etc)**	**Unit Rate in INR (cost per item)**	**Taxes (Tax details)**	**Total in INR (Unit rate x Quantity + taxes)**
1.					
2.					
3.					
-					
-					
-					
	Total Cost of the entire Solution for three years onsite comprehensive warranty, support and licenses				
	Additional Cost for Fourth year with warranty, support and licenses				
	Additional Cost for Fifth year with warranty, support and licenses				
	Total Cost of Ownership for five years				