OPEN TENDER

Procurement of Unified Threat Management (UTM) Appliance for Indian Institute of Science

TINA/IISc/01/2016

Telecom and Internet Access Committee
Indian Institute of Science
Bangalore 560012

January 2016

INTRODUCTION :

Telecom and Internet Access Committee (TINA) at Indian Institute of Science (IISc) provides the Telecom, Internet and Network services to the Institute Community. The core network infrastructure is currently located in the Supercomputer Education and Research Centre (SERC) and provides services to the Institute faculty, staff and students round the clock. The campus having around 50 departments is connected to the core infrastructure by a fiber optic backbone with active devices delivering Gigabit performance. The Institute is a part of the National Knowledge Network (NKN) of the Government of India and currently has one Gigabit Internet Bandwidth. In addition to this, the Institute also has Internet Bandwidth of 20 Mbps from Tata Communications.

The connectivity diagram of the campus backbone and the details of the core infrastructure located at SERC are given in Annexure 1 (at the end of the document).

The technical specifications for the proposed requirement is given in annexure 2 (at the end of the document).

SCOPE OF WORK :

The Institute invites proposals in a two cover format from bidders who have the competence and capability to supply Unified Threat Management (UTM) Appliance to meet all the stated requirements, which are detailed out in subsequent sections. The offer from the bidders is expected to be a total turn-key solution which includes supply, transportation to the site, transit insurance, installation and commissioning, integration with the existing environment and three years of comprehensive warranty after the same is accepted by the Institute.

Detailed Technical Scope of Work and the technical specifications are mentioned in the subsequent sections.

The proposed system will be housed in the Ground floor of the existing SERC building and the requirements of power and cooling, will be the responsibility of the Purchaser. The solution proposed by the bidders is expected to be a total turn-key solution meeting all the stipulated requirements including Supply, installation, commissioning and integration of the UTM appliance with the core infrastructure along with warranty services for a period of three years after acceptance.

The bidders have to ensure that the resources (personnel) allocated for each one of the above tasks are competent and capable to meet all the technical requirements in order to ensure that the broad objective of delivery of services as per expectations is fully met.

BIDDER'S ELIGIBILITY CRITERIA

1. The Appliance proposed (Unified Threat Management/Next Generation Firewall) should have been implemented by the bidder (system integrator or the OEM) in at least two customer sites in India in the last two years (Jan 2013 to Dec 2015). If the bidder happens to be a system integrator either the bidder or the OEM should meet the above condition. The bid should include the authorization letters from the OEM stating that the bidder has implemented the solution as a total turn-key solution.
2. The technical bid should clearly demarcate the responsibilities between the bidder and the OEM. Complete details of the same have to be submitted with the bid.
3. The (primary) bidder is expected to be a profit-making company with an annual turn-over of at least Rs.10 Crores in each of the last 3 financial years.

4. The bidder (along with their OEM) should be in a position to demonstrate their competence and capability, as a team, to deliver all the services expected during the contract period.
5. The technology proposed by the bidder for this requirement should have been evaluated by Gartner in 2014-2015 and should appear either in the leader's or the challenger's quadrant.
6. The proposed appliance should have at least one of the following certifications EAL4+ / ICSA / NSS-Lab.

Compliance to conditions 1 to 6 above are mandatory and are not relaxable.

EARNEST MONEY DEPOSIT (EMD) and BID SECURITY

The bidders have to submit along with the technical bid a demand draft from a public sector bank or scheduled bank in India for an amount of Rs.5 lakhs as bid security. Failure to comply with this requirement will result in rejection of the bid.

After the evaluation of the tender and placement of the purchase order on the successful bidder, the EMD amount will be returned to the unsuccessful bidders within 45 days.

EMD amount will be returned to the successful bidder after the Institute places a firm purchase order for the procurement of the appliance and the successful bidder submits the performance bank guarantee. Details of PBG is given in subsequent section.

EVALUATION METHODOLOGY

1. The bids received from the bidders will be evaluated by the Technical Committee constituted by the Institute.

2. The evaluation process to identify the successful bidder based on a technical evaluation details of which are mentioned subsequently in this document.
3. Evaluation of technical bids.
   3.1. In the first stage only the technical bids are evaluated. The mandatory conditions stipulated elsewhere in the document must be adhered to and failure of the same will result in disqualification of the bid.
   3.2. The technical criteria set out for evaluation of the technical offer is given below.
   3.3. It is to be noted that bidders who score the minimum marks shown in the Table 1 in each category, and **a total of 70 marks**, will be considered as technically meeting the requirements and will be considered for further evaluation.

Table 1: Bidder's Evaluation Criteria

Sl. No.	Description	Max. Score	Min. Score
1	Bidder's Eligibility Criteria (of Bidder or OEM)	30	20
2	Solution superiority & Compliance	30	20
3	Technical Presentation	25	15
4	Implementation Methodology	15	10
	Total	100	65

3.4. The technical scores for the each of the above will be given based on the detailed explanation given below:

3.4.1. **Bidder's Eligibility Criteria:**

1. **Supporting Documents:** For item (1): A copy of the P.O.; for item (2), a letter from the customer site stating clearly the duration of contract, scope, and

satisfactory delivery of services; for item (3): annual audited balance sheet for 3 years; for item (4): letter from OEM; for item (5): Gartner evaluation report; for item (6): certificates from the respective labs.

2. **Scoring Scheme:** Meeting Items (1) to (6) in Bidder's Eligibility criteria will entail 20 marks. Additionally, a maximum of 10 marks will be given for Item 4, which will be based on the implementations taken up by the bidder over and above the stated requirement.

3.4.2 Solution Superiority

1. **Supporting Documents:** Bidder has to clearly indicate the superiority of the proposed solution (hardware, software, integration, etc.)
2. **Scoring Scheme:** Solutions meeting the technical requirements of the tender will be given 65 marks. Additional marks will be given based on the superiority of the proposed solution as evaluated by the technical committee.

3.5. It is to be noted that only those bidders who score an aggregate of 70 or higher will be considered as technically qualified. Further, a bidder must score the minimum score indicated against each category in Table 1, in order to be qualified. The decision of the technical committee is final and binding on all the bidders.

<u>EVALUATON OF COMMERCIAL BIDS</u>

1. Commercial bids shall be opened for the technically qualified bidders after the technical evaluation. The Institute will communicate the date and time of opening of the commercial bids to the qualified bidders.
2. Commercial bids will be opened on the said date and time, irrespective of the presence of the bidder / authorized representative.

3. Commercial bids which are not in compliance with the terms and conditions set out [Refer to "***Commercial Terms and Conditions***"] in the tender will be rejected.
4. The bidder who is meeting all the terms and conditions of the tender and is technically short listed and offers the price which is the lowest will be declared as the successful bidder.

ACCEPTANCE CRITERIA :

The successful bidder has to implement the solution at the site and complete the necessary integration of the appliance with the core network infrastructure deployed at SERC and demonstrate the performance of the equipment to the technical committee.

The technical committee and the technical team of the successful bidder will arrive at a mutually acceptable acceptance test plan (ATP) which will form the basis of the acceptance.

The warranty services will start only after the appliance is accepted by the Institute.

SERVICE LEVEL AGREEMENT

1. The bidder has to ensure that the solution proposed, as a total turnkey solution to meet the stated requirements, delivers an uptime guarantee of 99.5% measured on a monthly basis, with mean time to restore in the event of a failure not exceeding 4 hours.

2. In the event of a failure of any of the sub-systems or components of the proposed solution, the bidder has to ensure that the defects are rectified before the end of the next working day.
3. Failure to meet the above requirement will result in extension of the warranty services by 3 days for delay of each day during the warranty period.

4. Therefore, the bidder along with the OEM, has to put systems and processes in place to address the above during the period of the contract.

WARRANTY:

1. Warranty services for the system supplied by the successful bidder should be valid for a period of 3 years from the date of acceptance of the equipment. Warranty service charges (in Indian rupees) have to be explicitly mentioned as a separate line item in the Commercial Bid.
2. During the warranty period, the bidder shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all the systems supplied.
3. During the warranty period, the bidder shall attend to all the hardware problems on site and shall replace the defective parts at no extra cost to the purchaser.
4. During the warranty period, the bidder shall attend to all failures relating to software installation, configuration, management and performance. Periodic maintenance w.r.t. software upgrades, updates, and patches, as well as preventive maintenance, are the responsibilities of the bidder.
5. The bidder should also clearly indicate post-warranty comprehensive AMC cost, covering all hardware and software aspects, as a percentage of the equipment cost, for a period of 2 years, on an annual basis, in the Commercial bid.

GUIDELINES TO BIDDERS

A **two-cover system** is proposed for the submission of tenders, consisting of

Technical Bid: The technical bid should contain

I. Executive Summary of the proposal
II. Overall Compliance Statement
III. Terms and conditions of the offer.
IV. Supporting technical material, including brochures.
V. Audited annual balance sheet of the company for the last 3 years
VI. Supporting documents for bidder's eligibility criteria
VII. Agreeing to the terms and conditions of the tender; A copy of the tender document, duly signed on each page with seal, must be enclosed;
VIII. A copy of the masked Commercial bid of the bill-of-materials to be included in the technical bid.

Covers containing the technical and commercial bids must be individually sealed, and superscripted respectively as "TINA/IISc/01/2016 – Technical Bid" and ""TINA/IISc/01/2016 – Commercial Bid". The two covers must be put in a larger envelope, sealed, superscribed as "Tender for procurement of UTM Appliance – TINA/IISc/01/2016". Non-conformance of any of the above can result in disqualification.

The envelope should be addressed to:

The Chairperson, TINA
Department of Electronic Systems Engineering
Indian Institute of Science
Bangalore 560012

Additional Guidelines:

1. The total solution as per the agreed bill of materials has to be supplied within 6 weeks from the date of LoI from IISc and the installation is to be completed within 2-3 weeks after supply of the equipment.
2. IISc is eligible for customs and excise duty exemption under notification 10/97-ce. Hence please quote the ED component, if

any, separately so as to avail exemption on issue of certificate by us. Bidders planning to quote any imported solution have to give the offer in the respective currency.

3. The offer has to clearly state the components of pricing separately. For example, the supply part, F & I, I & C, Warranty services and any other charges have to be quoted as separate line items.
4. A copy of the masked Commercial bid has to be given in the technical offer and the process followed by the Institute is a two cover bid system.
5. No request for any further extension of the above deadline shall be entertained. Delayed and/or incomplete tenders are liable to be rejected.
6. All the covers should bear the name and address of the bidder.
7. The Technical Bid and the Commercial Bid should be duly signed by the authorized representative of the bidder.
8. The Technical Bid and the Commercial Bid should be bound separately as complete volumes.
9. The prices should not be mentioned in the Technical Bid.
10. A tender, not complying with any of the above conditions is liable to be rejected. Incomplete proposals are liable to be rejected.
11. The Director, IISc, Bangalore-12 reserves the right to modify the technical specifications or the required quantity at any time. In such case, the bidders will be notified.
12. The Director, IISc reserves the right to accept or reject any proposal, in full or in part, without assigning any reason.
13. The bidders are requested to go through the Terms and Conditions detailed in this document, before filling out the tender. Agreeing to the terms and conditions of the tender document (by signing all pages of the copy of a tender document) is a mandatory requirement.
14. A prebid-clarification meeting is scheduled as per the timeline given below. Queries relating to the tender documents must be submitted in writing (email: tina_utm@dese.iisc.ernet.in) on or before the specified timeline. Queries received after this deadline will not be entertained.

COMMERCIAL TERMS & CONDITIONS

1. The commercial bid should contain among other things, payment terms, warranty, installation and commissioning charges. These charges will be paid only after successful supply, installation and acceptance. IISc will enter into a contract with the successful bidder which will detail all contractual obligations during the warranty period. Bidders have to quote for AMC charges for 2 years after the 3 year warranty period.
2. In case of rupee offer, the component of tax, E.D. and any other statutory levies should be shown separately and not included in the total amount, to enable us to avail exemption.
3. In case of imports, the commercial bid should contain among other things, the name and address of the Indian agent, if any, and the agency commission payable to the agent. Agency commission part will be deducted from FOB value, and will be paid to the agent by us separately in equivalent Indian rupees. Please quote the prices for shipment on 'FOB' terms.
4. In respect of an imported solution, IISc will arrange for customs clearance, at Bangalore airport, which will be final destination airport. Hence, costs related to customs/clearance need not be included in the offer.
5. In CIF offers of imported solutions, insurance should be on "Warehouse to Warehouse" basis and should not terminate at Bangalore airport.
6. IISc is not exempted from any other VAT or other taxes. Hence this component may be shown as separate line item wherever applicable.
7. Proposals should contain the name and contact details, viz., phone, fax and email of the designated person to whom all future communication will be addressed.
8. Prices should be quoted in detail, for all the subsystems given in the Technical Specifications part of the tender. Further, price validity should be for six months and IISc may place a repeat order for another appliance.

9. IISc will place the purchase order only on the successful bidder.
10. It is to be noted that the primary bidder will be the system integrator for the total requirement and will be responsible to ensure that the OEMs understand all the requirements and are in a position to execute their respective responsibilities for the successful implementation of the contract.

PAYMENT TERMS

1. The conditions regarding payment terms are as follows:
2. The total project cost will consists of two parts:
   a) Equipment supply part (Supply)
   b) Installation, commissioning, warranty and maintenance services part (referred to as "services" in short)
3. The total cost of the system (Supply part) will be paid through SIGHT DRAFT/Letter of Credit (documents through Bank).
4. Installation charges, if any, payable only in Indian Rupees, will be paid after acceptance of the system.
5. Warranty charges will be paid (in Indian Rupees) in equal quarterly installments. The payment will be made at the end of each quarter after satisfactory completion of services. Hence, warranty charges for the 2nd year and the 3rd year have to be quoted as a percentage of the equipment cost and as separate line items. In case the warranty for the 2nd year and the 3rd year are bundled for the appliance, then IISc reserves the right to hold 10% of the appliance cost as a performance security.
6. The Performance Bank Guarantee (PBG) is 5% of the value of the product in INR and the successful bidder has to submit necessary documentation to ensure that it will be effective before opening LC.

Schedule of Events:

The tender document will be made available on the IISc website from the date of release of the tender.

Table 2: Schedule of Events

Release of Tender	January 25, 2016
Submission of queries (for Prebid clarification):	January 31, 2016, 3.00 pm
Prebid Clarification Meeting at SERC, IISc	February 2, 2016, 3.00 pm
Submission of Tender Response	Feb. 16, 2016, 11.00 am
Technical presentations	February 17-19, 2016
Shortlisting	February 25, 2016, 4.00 pm
Opening of price bids	February 26. 2016, 3.00 pm

No request for extension of any deadline will be entertained.

ANNEXURE 1

TECHNICAL SPECIFICATIONS

This section provides required technical specifications of the product

I. System Level Specifications

1. Proposed solution should be hardware based appliance. It should have inbuilt Flash/HDD Storage.

2. Proposed solution should comply with FCC and CE norms

3. The proposed solution should match the following criteria
   a) Must have a 64-bit hardware platform
   b) Proposed appliance should contain 15 or more ports of 1 G SFP+ and 8 or more ports of 10 G SFP+ Fiber pluggable modules, and 8 or more copper GbE ports
   c) 200,000 new connections per second
   d) 12,000,000 concurrent sessions
   e) 10,000 Minimum concurrent users
   f) 50 Mpps or above Firewall throughput (packets per second of 64

bytes packets)

g) 10 Gbps or above IPS throughput

h) 4 Gbps or above Fully Protected throughput, i.e., with Anti-virus, IPS, Firewall, VPN, Web application firewall services enabled

i) 4 Gbps or above Anti-Virus throughput

j) 1.4 Gbps or above SSL VPN throughput

k) 4000 or above concurrent VPN connections

l) 10000 concurrent web sessions through web cache

4. All features should have equivalent support for IPV4 & IPV6, unless explicitly specified.

5. The proposed solution should support unrestricted user/node license or minimum of 50,000 nodes.

6. The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS and Application Control. Option to enable / disable any service should be available. The appliance should support WCCP (Web Cache Communication Protocol).

7. The proposed solution must support User and Role based policy configuration for security and Internet bandwidth management.

8. The proposed solution should provide on-appliance reports / dedicated reporting server based not only on IP addresses but also usernames.

9. Firewall appliance should have a feature of holding at least two OS images simultaneously to support resilience & easy rollbacks during version upgrades.

10. The appliance should generate audit trail and have secure interface to transfer it to the remote system.

II. Administration, Authentication and General Configuration

1. The proposed solution should support administration via secure communication over HTTPS, SSH version 2 or above and from Console Terminal.

2. Solution must support multiple administrators working in parallel. All the policies and objects on which Administrator 1 is working should be locked for all other administrators. However, administrators can work on policy rules and objects that are not locked. Changes done by Administrator-1 should not be visible to other administrators till the time Administrator-1 publishes the changes.

3. Solution must allow administrator to choose to log in in read-only or read-write mode.

4. The proposed solution should be able to export and import configuration backup including user objects.

5. The proposed solution must be deployable in Route (Layer 3) and Transparent Mode (Layer 2), individually and simultaneously.

6. The proposed solution should support policy-based routing.

7. The proposed solution should support integration with Windows Active Directory, LDAP, RADIUS or Local Database for user authentication.

8. The proposed solution must support SSL/TLS connections to LDAP/Active Directory servers.

9. The proposed solution must support Automatic Transparent Single Sign On (SSO) for user authentication. SSO must be proxy-independent and should support user authentication for network applications like *http, https, ssh, git, skype etc.*

10. The proposed solution should provide bandwidth utilization graphs on daily, weekly, monthly and yearly basis for each one of the ISP links terminating on the UTM appliance.

11. The proposed solution should provide real time data transfer/ bandwidth utilization details with respect to individual users / IP addresses/ applications.

12. The proposed solution should support NTP.

13. The proposed solution should support user/IP address/MAC address binding that can map username to corresponding IP and MAC addresses for security reasons.

14. The proposed solution should support version roll back functionality.

15. The proposed solution should be able to force-logout users upon session time-out, quota exceeded (over-download) and idle time-out.

16. The proposed solution should support group-based user creation for administration purposes.

17. The proposed solution should support SNMP v1, v2c and v3.

18. The proposed solution must be firmware-based rather than software-mounted. It should be able to hold two firmware images on the appliance simultaneously, to facilitate instant rollback.

19. The proposed solution must provide flexible, granular role-based, application based and flow based bandwidth management, GUI for administration for configuring hosts, networks, services, access rules, bandwidth allocation, VPN, NAT, etc.

20. The proposed solution must provide support for multiple authentication servers for each module (e.g. firewall, VPN etc).

21. The proposed solution must support multiple Thin Client (Microsoft TSE, Citrix) authentication mechanisms and must be able to differentiate between requests originating from the same IP address.

22. The proposed solution must support:

    a) DHCP/DHCPv6 Server,

    b) DHCP/DHCPv6 Relay Agent,

    c) DNS/DNSv6 Proxy,

    d) Bandwidth reservation for critical applications like DNS,

    e) Customizable login and security settings.

23. The proposed solution must provide customizable administrator

password complexity setting.

24. The proposed solution should support event-triggered alerts/alarms, based on preset thresholds.

Firewall

1. The proposed solution should have EAL4+ / ICSA / West Coast Labs Checkmark certification.
2. The proposed solution should be a standalone appliance with secured OS.
3. The proposed solution should support stateful inspection with sessions identified by usernames, and in the presence of dynamic NAT and PAT.
4. The proposed solution should use User Identity as a matching criterion along with Source/Destination IP/Subnet/group/port in firewall rules.
5. The proposed solution should facilitate the application of UTM policies related to AV/AS, IPS, content filtering, bandwidth policy and policy-based routing decisions on the firewall rule itself.
6. The proposed solution should support a user-defined multi-zone security architecture.
7. The proposed solution should have predefined applications based on port/signature and also should support creation of custom applications based on port/protocol number.
8. The proposed solution should support inbound NAT load balancing with different load balancing methods like First Alive, Round Robin, Random, Sticky IP and failover, with server health check by TCP or ICMP probe.
9. The proposed solution should support 802.1q VLAN tagging.
10. The proposed solution should support dynamic routing like RIP1, RIP2, OSPF.

11. The proposed solution must support IPv6 as per www.ipv6ready.org guidelines.

12. The proposed solution must support IPv6 Dual Stack Implementation.

13. The proposed solution must support tunnelling like 6in4, 6to4, 4in6, 6rd.

14. The proposed solution must support all IPv6 configuration on GUI.

15. The proposed solution must support DNSv6.

16. The proposed solution must support DoS protection against IPv6 attacks.

17. The proposed solution must support spoof prevention on IPv6.

18. The proposed solution must support the 802.3ad standard for Link Aggregation.

19. The proposed solution must support Application-based Bandwidth Management, which allows the administrator to create application-based bandwidth policies.

20. The solution should be able to address all aspects of the Advanced Persistent Threat (APT) lifecycle, including: Blocking known malware sources, blocking known malware, identifying and blocking unknown or zero-day malware attacks, protecting against client-side vulnerabilities, blocking command and control back-door traffic, blocking server-side vulnerabilities, and advanced application and user control.

21. The proposed solution must support sandbox based inspection and protection of unknown viruses and malware.

Gateway Anti-virus and Anti-Spam

1. The proposed solution should have an integrated Anti-Virus capability.
2. The proposed solution should have an EAL4+ / ICSA / West Coast Labs Checkmark certification.
3. The proposed solution must work as an SMTP proxy rather than an MTA or relay server.
4. The proposed solution should support scanning for SMTP, SMTPS, POP3, IMAP, FTP, HTTP, HTTPS, websockets and FTP over HTTP protocols.
5. The proposed solution should be able to detect the latest phishing URLs in email content and warn the end-user.
6. The basic virus signature database of the proposed solution should comprise all wild list signatures and variants, as well as those for malware, like phishing and spyware.
7. The basic virus signature database of the proposed solution should comprise of all the viruses "in the wild" and variants. Further, it should also contain database of all known malware/spyware used for phishing and accessing/stealing information without the end user's knowledge.
8. The proposed solution should be able to block dynamic/executable files based on file extensions.
9. The proposed solution should support multiple customizable anti-virus policies based on user groups and applications.
10. The proposed solution should update the signature database at a frequency of less than one hour and it should also support manual updates.
11. For POP3 and IMAP traffic, the proposed solution should strip the virus infected attachment and then notify the recipient and the administrator.

12.	The proposed solution should scan http traffic based on username, source/destination IP address and URL based regular expressions.
13.	The proposed solution should provide the option to bypass scanning for specific HTTP traffic.
14.	The proposed solution should support real mode and batch mode for HTTP virus scanning.
15.	The proposed solution should be able to scan files irrespective of the filename extension.
16.	The proposed solution should be able to provide reports based on username, IP address, sender, recipient, virus names and time window etc from archived data.

Web Filtering Framework

1.	The solution should protect users from downloading virus / malware-embedded files by stopping viruses/malware at the gateway itself. It should provide real-time security scanning.
2.	The proposed solution should stop incoming malicious files with updated signatures & prevent access to malware-infected websites and unblock the sites when the threats have been removed.
3.	The proposed solution should be able to categorize URLs into at least 75 predefined categories, and the categories should be customizable. The solution should have the capabilities to block, permit, allow & log protocols HTTP, HTTPS, FTP, Websocket and others. It should also list the protocols that it supports.
4.	The proposed solution should have the ability to identify and block proxy avoidance techniques, for example, Tor network, open Internet VPN sites.
5.	The proposed solution should provide cloud-based web categorization for real time filtering and zero day attacks.
6.	The proposed solution must be able to work as a standalone transparent proxy.

7. The proposed solution must have the following features built in:

a) Should be able to block HTTPS based URLs

b) Should be able to block URLs based on regular expressions

c) Should support exclusion list based on regular expressions

d) Should be able to block any HTTP / HTTPS upload traffic

e) Should be able to block Google cached websites based on category.

f) Should be able to block websites hosted on Content Distribution Network companies such as Akamai.

g) Should be able to identify and block requests coming from a host behind a proxy server on the basis of username and IP address.

h) Should be able to identify and block URL translation requests.

8. The proposed solution should support application control blocking features as follows

a) Should be able to block known chat applications like Yahoo, MSN, AOL, Google, Rediff, Jabber, WhatsApp, Viber etc.

b) Should support YouTube Education Filter

c) Should support blocking of File transfer on known Chat applications and FTP protocol.

9. The proposed solution must block HTTP or HTTPS based anonymous proxy requests.

10. The proposed solution should allow customization of Access Denied message for each category.

11. The proposed solution should be CIPA compliant and should have predefined CIPA based Internet access policy.

12. The proposed solution should be able to classify traffic as Productive and Non-productive, as specified by administrator.

13. The proposed solution should have specific categories that broadly

	classify websites. For instance, websites that reduce employee productivity, bandwidth choking sites or malicious websites.
14.	The proposed solution should be able to generate reports based on username, IP address, URL, groups, categories and category type.
15.	The proposed solution should support creation of Internet access policies based on time etc. for individual users or user group.
16.	The proposed solution must provide logging and extensive controls on Instant Messaging (IM) traffic for Yahoo and MSN messengers such as log of chat sessions for all or specific set of users.

VPN

1.	The proposed solution should have an EAL4+ / ICSA / West Coast Labs Checkmark certification.
2.	The proposed solution should support IPsec (Net-to- Net, Host-to-Host, Client-to-site), L2TP, PPTP and SSL VPN connections.
3.	The proposed solution should support DES, 3DES, AES encryption algorithms.
4.	The proposed solution should support pre-shared keys as well as digital certificate based authentication.
5.	The proposed solution should support multiphase IPSec VPN negotiations.
6.	The proposed solution should support external certificate authorities.
7.	The proposed solution should support export facility for Client-to-site configuration which ensures hassle-free VPN configuration in remote Laptops/Desktops.
8.	The proposed solution should support commonly available IPsec VPN clients.
9.	The proposed solution should support local certificate authority & should support creation/renewal/deletion of self-signed certificates.

10. The proposed solution should support VPN failover for redundancy purposes wherein more than one connection is grouped together. If one connection goes down, it automatically switches over to another working connection, ensuring zero downtime.

11. The proposed solution should support threat free IPsec/L2TP/PPTP VPN tunneling.

12. The proposed solution must support VPN client from Apple iOS, Windows mobile and Android.

13. The proposed solution must provide on-appliance SSL VPN solution with Web Access (Clientless), Web Application Access (most commonly used protocols), Full Tunnel and Split Tunnel control. The solution should provide per user / group SSL VPN access (which involves free licenses for unlimited users).

Logging and Reporting

1. The proposed solution must support authentication to comply with Internet Privacy laws.

2. The proposed solution must have on-appliance / dedicated server reporting solution.

3. The proposed solution should interwork with any reporting solution.

4. The proposed solution should allow exporting of reports in PDF, HTML and CSV formats.

5. The proposed solution should support secure logging of Antivirus, Antispam, Content Filtering, Traffic discovery, IPS, Firewall activity on syslog compatible server.

6. The proposed solution should provide detailed reports for all files uploaded via the HTTP or HTTPS protocol. The report should include username/IP address/URL/File name/Date and Time.

7. The proposed solution should provide data transfer reports on the

	basis of application, username and IP address.
8.	The proposed solution should provide connection-wise reports for user, source IP, destination IP, source port, destination port or protocol.
9.	The proposed solution should facilitate sending of reports on email addresses.
10.	The proposed solution should provide audit reports in compliance with SOX, HIPAA, PCI, FISMA and GLBA.
11.	The proposed solution should support auditing facilities to track all activity carried out on the appliance.
12.	The proposed solution should support multiple syslog servers for remote logging.
13.	The proposed solution should forward logging information of all modules to syslog servers.
14.	The proposed solution should have customizable email alerts/automated report scheduling.
15.	The proposed solution should provide reports for all blocked attempts by users/IP addresses.
16.	The proposed solution must be capable of analyzing logs and reports derived from proprietary devices including UTMs, Proxy Firewalls and Syslog-compatible devices.
17.	The proposed solution must be capable of providing Multiple Dashboard Report, along with the facility to customize the dashboards.
18.	The proposed solution should be capable of forensic analysis to help organizations reconstruct the sequence of events that occurred at the time of a security breach.

19. The proposed solution should provide zone-based reporting.

20. The proposed solution should provide complete BYOD visibility.

21. The proposed solution should support customizable logging levels (verbose to minimal).

22. The proposed solution should allow rebranding or customization of reports.

Application Control Solution

1. The proposed solution must provide inbuilt Application Filtering and control solutions.

2. The proposed solution must identify (Allow/Block/Log) the applications regardless of port, protocols and encryption, including SSL/TLS.

3. The proposed solution's application database must get updated automatically without any manual intervention.

4. The proposed solution must give identity based reports (username along with IP).

5. The proposed solution must be capable of blocking the following type of applications:

6. Applications that allow file transfer

   a) Online Games

   b) Instant Messengers (Including Non-English Versions).

   c) Peer-to-Peer (P2P) applications (Including Non-English Versions)

   d) Browser Based Web Proxy (Regardless of IP address or Port Number)

   e) Web 2.0 based applications (Facebook, CRM etc.)

   f) Applications that provide Remote Control

	g) All type of streaming media (Both Web and Software Based) h) VOIP Applications
7.	The proposed solution must be capable of identifying hidden applications running over standard ports (80, 443, 22 etc.)
8.	Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance.
9.	Application Intelligence should have controls for Instant Messenger, Peer-to-Peer, Malware Traffic etc.
10.	The solution should allow for third party signature.

DELIVERABLES

During the deployment phase of the project IISc, Bangalore requires the following deliverables:

1. **DEPLOYMENT PLAN**

   written documentation of the deployment approach and recommendations for seamless integration of the UTM device in live network with minimum downtime.

2. **DETAILED TECHNICAL REPORT**

   IISc network specific document developed for the use of IISc, Bangalore technical staff which discusses: the methodology employed, positive security aspects identified, detailed technical vulnerability findings, an assignment of a risk rating for each vulnerability, supporting detailed exhibits for vulnerabilities when appropriate, and detailed technical remediation steps.

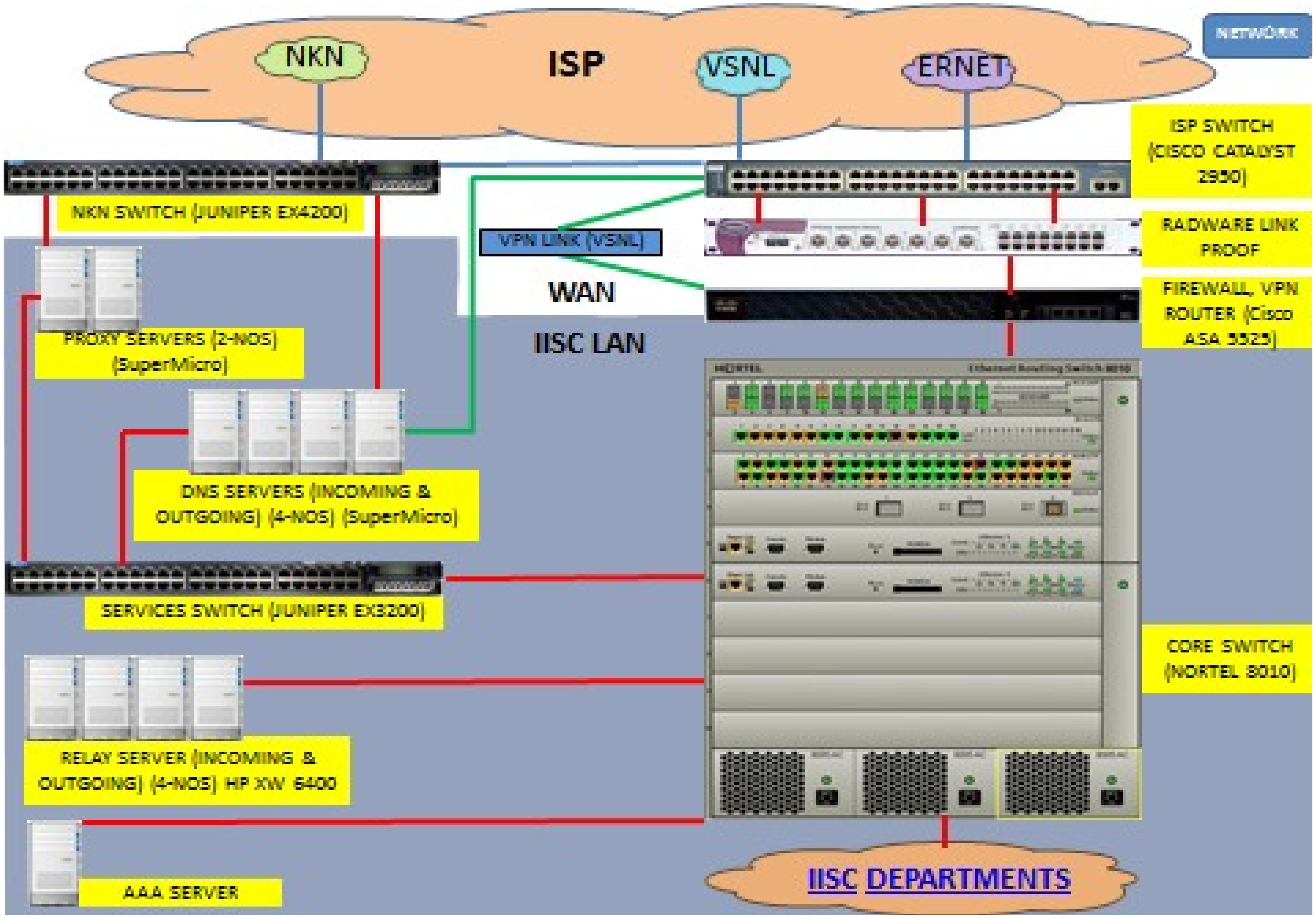
3. **TRAINING**

   Appropriate number of training sessions for IISc Technical staff for effective operations and management of the appliance.

4. **PRESENTATION & EXECUTIVE SUMMARY REPORT**

   A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.

ANNEXURE – 2


NETWORK
NKN
ISP
VSNL
ERNET
ISP SWITCH (CISCO CATALYST 2950)
NKN SWITCH (JUNIPER EX4200)
VPN LINK (VSNL)
RADWARE LINK PROOF
WAN
FIREWALL, VPN ROUTER (Cisco ASA 5525)
IISC LAN
PROXY SERVERS (2-NOS) (SuperMicro)
DNS SERVERS (INCOMING & OUTGOING) (4-NOS) (SuperMicro)
SERVICES SWITCH (JUNIPER EX3200)
CORE SWITCH (NORTEL 8010)
RELAY SERVER (INCOMIING & OUTGOING) (4-NOS) HP XW 6400
AAA SERVER
IISC DEPARTMENTS