INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY (IRDA)
Hyderabad

TENDER NOTICE.

IRDA invites sealed bids from reputed IT vendors for supply and installation of a Unified Threat Management Device. For details please visit **http://www.irdaindia.org/tenders.htm**. Last date for receipt of bids is 9th November 2009 by 3.00 PM

INVITATION OF BIDS

FOR

SUPPLY AND INSTALLATION OF a Unified Threat Management Device

INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY
3RD FLOOR, PARISRAMA BHAVAN,
BASHEER BAGH HYDERABAD 500 004
ANDHRA PRADESH

www.irdaindia.org

PH: (040) 23381183

FAX: (040) 6682 3334

IRDA (herein after referred as ‘Authority’) invites sealed bids from reputed IT vendors for the supply and installation of Unified Threat Management Device.

1. The application form for tender is given in **Annexure – ‘A**’. Interested parties can submit the duly filled in application form along with all relevant supporting documents.

2. At any time before the submission of bids, the Authority may, for any reason, whether at its own initiative or in response to a clarification requested by the vendors carry out amendment(s) to this Tenders document. The amendment will be made available in our website (www.irdaindia.org) and will be binding on them. The Authority may at its discretion extend the deadline for the submission of bids

3. The Technical specifications of the equipments to be supplied are in **Annexure – ‘B’**

4. The vendors shall submit the bids as per the format given in **Annexure – ‘C’. Those bids which are not in the format specified would be rejected.** The last date for receipt of Technical bid is 9th November 2009

5. The Authority reserves the right to accept or reject any application without assigning any reason there for.

6. Bids that are incomplete in any respect or those that are not consistent with the requirements as specified in this document or those that do not adhere to formats, wherever specified may be considered non-responsive and may be liable for rejection and no further correspondence will be entertained with such bidders .

7. Canvassing in any form would disqualify the applicant.

8. The selected Bidder should deliver and install the equipments **within 2-3 weeks from the receipt** of the Purchase Order.

Joint Director (IT)

SECTION – I

TERMS OF REFERENCE

A. ABOUT IRDA

Insurance Regulatory and Development Authority (IRDA) is a regulatory body to protect the interests of policy holders of insurance policies and to regulate, promote and ensure orderly growth of the Insurance Industry and for matters connected therewith or incidental thereto. Please visit the website www.irdaindia.org ;

B. SCOPE OF WORK

The selected vendors will have to execute supply and install the equipments within the stipulated time frame.

C. PREQUALIFICATION OF APPLICANT

1. The vendor **must be a reputed Firm/Company** incorporated in India with a standing of 5 years existence**.**

2. The vendor must be a **Original manufacturer of the equipments / Authorized Service Provider** / for the supply of equipments stated in annexure – A

3. The vendor should have its own service setup for servicing the supplied equipment.

D. TERMS & CONDITIONS:

1. All bids and supporting documentation shall be submitted in English.

2. IRDA will not take into consideration, any variation in the $ price.

3. All costs and charges, related to the bid, shall be expressed in Indian Rupees only.

4. Price quoted should be inclusive of all applicable Taxes.

5. The Bidder is liable to be rejected if the specifications of the equipments are not in line with the specifications stated at '**Annexure – B'**

6. Delivery Period

(i) Equipments should be delivered within 2-3 weeks of receipt of purchase order.

(ii) IRDA would be the deciding authority as to the definition of 'acceptable configuration'.

(iii) The delivery period, for all the items, shall include time taken for all procurement and other procedures such as Government clearances, customs, octroi, transport etc.

7. **Warranty**

I. **Vendor shall have to provide a comprehensive, on-site, post installation warranty 36 months from the date of acceptance of the system.** Vendor shall have to upgrade the system software during warranty period at its own cost and expenses, wherever applicable.

II. Warranty should cover all the system components including the software and other packages supplied by the vendor.

8. **Installation and Commissioning**

i. Vendor shall take the responsibility of installing and, commissioning the system.

ii. Vendor shall have to configure the equipments as per the requirements of the Authority.

iii. IRDA reserves the right to shift system to new locations within Hyderabad. Vendor shall assist IRDA during the process.

iv. All the above activities to be undertaken by the vendor at its own cost and expenses.

9. Acceptance

The warranty period shall commence from the date of acceptance of the system or device.

10. Maintenance

i. Complaints reported should be attended within 3-4 hours of lodging the complaint.

ii. Maximum time to repair a reported breakdown should be **twenty four (24)** clock hours. Time for this purpose shall be measured as interval between the time of reporting the problem and the time when the problem is fully solved making the faulty components/functions fully operational.

iii. Equipment standby system shall be provided till such time the problem is fully solved. Vendor shall assist in transferring the data to and from the standby system, wherever applicable.

iv. Vendor shall arrange an equivalent system during such breakdowns, if IRDA so desires.

v. Vendor shall have to support the systems and any software supplied by him.

vi. Vendor shall not be responsible for damage to the systems due to external circumstances such as earthquakes, floods, fires, riots, electrical faults, as well as damages caused by rodents.

11. Uptime Guarantee

Vendor shall have to guarantee a minimum average uptime of 98% calculated on a quarterly basis. Uptime percentage shall be calculated as (100 - Downtime Percentage). Downtime percentage shall be calculated as Unavailable Time divided by Total Available Time, calculated on a quarterly basis. Total Available Time is two shifts a day for six days a week. Unavailable Time is the time involved while any part of the core configuration or system software component is inoperative or operates inconsistently or erratically.

12. Support Strategy

I. Vendor shall provide effective maintenance support to IRDA

II. **The vendor shall inform in writing the contact person, address, phone nos. and fax nos. of their service centre**.

III. In case of any upgrade of the system during the proposed warranty period, the warranty shall also cover the upgraded system for the said contract period by the vendor.

13. Payment Terms

IRDA shall make payment in Indian Rupees Only.

The risk of currency fluctuation shall have to be borne by the vendor.

Payment terms shall be as follows:

- 90% against supply and installation of systems
- 10% against submission of bank guarantee valid for a period of 3 years

- Challan in duplicate shall accompany the delivery.

- Invoices shall be submitted in duplicate.

Delivery challan and invoice shall always quote purchase order number of IRDA.

All quotations, negotiations, formats, technical literature, correspondence, faxes etc. shall be considered as an integral part of the purchase order.

14. Penalty

Vendor shall have to pay liquidated damages to IRDA @ one percent (1%) per week on the unexecuted value of the order inclusive of all taxes, duties levies etc., or part thereof, for late delivery beyond the delivery period as mentioned in Clause 7. There shall be an upper ceiling of ten percent of the gross amount for the penalty to be deducted for any orders. The penalty applicable on the entire order amount shall be deducted from the payment amount due after acceptance of the systems. The performance bank guarantee shall be Ten percent of the order value irrespective of the penalties levied.

If delay exceeds one week from due date of delivery, IRDA reserves the right to cancel the entire order or part thereof. In case the vendor is unable to complete the delivery of any items ordered, IRDA shall procure the same through other sources and recover the consequent costs and damages from the vendor.

Necessary taxes like TDS (Tax Deducted at Source) if any, shall be deducted from the payments to be made by IRDA.

15. **Training**

Vendor shall provide basic training free of charge for IRDA end users, whenever required to do so by IRDA.

16. **Documentation**

Vendor shall have to supply all necessary documentation for the use of systems installed at IRDA. The documentation should be in English.

17. Language for Communication

This document and all responses shall be in English Only.

18. Transportation and Insurance

All the costs mentioned in the bids should include cost, insurance and freight (c.i.f.) till point of entry/border points. However, the vendor has the option to use transportation and insurance cover from any eligible source. Insurance cover should be provided till the items are accepted by IRDA. Insurance shall be payable in Indian rupees to facilitate replacement of damaged or lost goods. The vendor should also assure that the goods shall be replaced with no cost to IRDA in case insurance cover is not provided.

19. Force Majeure

Should either party be prevented from performing any of its obligations under this tender by reason of any cause beyond its reasonable control due to war, earthquake, floods or any natural disaster etc., the time for performance shall be extended until the operation or such cause has ceased, provided the party affected gives prompt notice to the other of any such factors or inability to perform, resumes performance as soon as such factors disappear or are circumvented. If under this clause either party is excused performance of any obligation for a continuous period of ninety (90) days, then the other party may at any time hereafter while such performance continues to be excused, terminate this agreement without liability, by notice in writing to the other.

20. Jurisdiction

The jurisdiction for the purpose of settlement of any dispute of differences whatsoever in respect of or relating to or arising out of or in any way touching this tender or the terms and conditions thereof or the construction and/or interpretation thereof shall be that of the appropriate court in Hyderabad. The jurisdiction of any other court in any place other than Hyderabad is specifically excluded.

21. Indemnity

The vendor shall, during the subsistence of the agreement, indemnify and keep indemnified harmless the IRDA from and against all the claims, losses and damages caused by the negligence of vendor’s personnel to any person or property arising out of the use or possession of the equipment or location by vendor or its personnel, as also arising out of any defect in title to the goods.

22. Confidentiality

The vendor shall keep confidential any information obtained under the contract and shall not divulge the same to any third party. In case of non-compliance of the confidentiality agreement, the contract is liable to be repudiated by IRDA. IRDA shall further have the right to regulate vendor staff.

The vendor shall not divulge to any person handling other divisions, subsidiaries or groups of Vendor, and its service support agency any information obtained by it in the course of its execution of its work and all the information gathered by the vendor shall be treated as professional communication and confidential. Any violation of this clause, shall be liable to cancellation of the contract and invoking the bank guarantee without notice to the vendor.

23. Publicity

The vendor shall not advertise or publicly announce that he is undertaking work for IRDA.

****

SECTION – II

INSTRUCTIONS TO BIDDERS

- The instructions mentioned should be read carefully by bidders before submitting the bid.

- Authority may ask for clarifications or further information to evaluate the Bid.

- If any information sought in this document is missing or not clearly specified by the vendor, it will be assumed that the vendor is not in a position to supply the information.

- The Authority may issue clarifications / amendments / modifications / errata and / or revised version of scope of work / other terms & conditions mentioned in the document and such amendments as will be made available in our website.

- An undertaking (self certificate) is to be submitted that the Organisation hasn't been blacklisted by any central/state Government department/organization.

- Each bid should have a proper index clearly mentioning the contents in the bid.

- Each bid should contain the Technical Bid and Financial Bid separately. The Technical Bid should clearly specify the Product Name and should be as per the specification given in the Tender. The Financial Bid should be inclusive of all the Taxes.

- Please note that all the pages should be numbered and all the pages of the bid document should be signed with date; and seal of the organization should be put near the signature of the authorized signatory on all the pages

- Bid document complete in all respects shall be submitted in a sealed envelope and superscripted as "***Tender for supply and installation of UTM Device*** " and addressed to :

  The Executive Director (Administration & IT)
  Insurance Regulatory and Development Authority
  3rd floor, Parisram Bhavan,

Basher Bagh, Hyderabad – 500 028

- The sealed quotations are to be dropped in the Tender Box kept at the reception of the Authority for the purpose.
- The last date of receipt of bid document is 9th November 2009 by 3.00 PM. No Bid document shall be entertained after the due date and time, under any circumstances.
- The covering letter to be submitted by the Bidder along with bid should be as per format given in this document.
- The decision regarding short listing / selection of vendor shall be with the Authority and shall be final.

- -

SECTION - III

CHECK LIST FOR SUBMISSION OF BID DOCUMENT

Applicants should ensure that the following documents are submitted while submitting the completed bidding document:-

i. Letter of submission of bid.

ii. Details as per application format (Annexure-A).

iii. Confirmation on Technical specifications (Annexure – B)

iv. Commercial Bids as per formats (Annexure – C)

v. Copy of the Registration certificate.

vi. List of financial / insurance sector/PSUs/ government clients and their contact details.

vii. Proof for Authorized Service Provider / Partner.

viii. Copy of the PAN/TAN number.

ix. An undertaking **(self certificate)** that the vendor hasn’t been blacklisted by any central/state Government department/organization.

Letter for submission of Bid

Date:

Place:

The Executive Director (Administration & IT)
Insurance Regulatory and Development Authority
3rd floor, Parisram Bhavan
Basher Bagh
Hyderabad – 500 028

Sub: Supply and installation of a Unified Threat Management Device– regarding.

Dear Sir,

The bid is being submitted by *(name of the Bidding Company)* for the ***supply and installation of UTM Device*** is in accordance with the requirements stipulated in the tender Document.

2. We have examined in detail and have understood, and abide by all the terms and conditions stipulated in the tender Document issued by the IRDA. Our application is consistent with all the requirements as stated in the tender Document.

3. The information submitted in our bid document is complete, and is strictly as per the requirements as stipulated in the tender Document, and is correct to the best of our knowledge and understanding. We shall be solely responsible for any errors or omissions or misrepresentations in our Bid.

Signature with Name & Seal
Place
Date:

ANNEXURE-A

APPLICATION FORM:

|

S.No	Particulars	
1	Name of the Organization Address : email : Telephone No. & Fax: Website:	
2	Name of the contact person: Telephone: Email ID :	
3	Type of the Organization (Public Sector /Limited/Private limited/Partnership, Proprietary) :	
4	Chief of the Organization : email Id : Telephone: Mobile:	
5	Registration details: (enclose certificates): • Company Registration (ROC Code)	
6	PAN/TAN No (enclose certificate):	
7	Activities of the Company: (List the activities)	
8	Names of five financial / Insurance sector/PSUs/ government clients to whom such equipments were supplied and installed in the preceding three years:	
9	Turnover of the Company for the last 3 years:	Year: Turnover 2005-06 2006-07 2007-08
10	Total No. of Employees:	

	• Technical Staff	

12. Any other information the applicant wants to furnish. :

Declaration

I hereby declare that the above information is true to the best of my knowledge.

Signature with Name & Seal
Place
Date:

ANNEXURE-B

INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY

5th Floor, Parisram Bhavan, Basher Bagh, Hyderabad – 500 004

SUPPLY AND INSTALLATION OF UNIFIED THREAT MANAGEMENT (UTM) Appliance

Technical Specifications

	Unified Threat Management Appliance	Confirm (Y/N)	Deviation if any
	Product Name		
	Specifications		
	General Specification		
1.1	Product or OEM should be ISO 9001-2000 Certified		
1.2	OEM should have presence at Hyderabad for sales & support		
1.3	Proposed appliance should support inbuilt HDD for storage of Logs & reports.		
1.4	Proposed solution should comply FCC and CE norms		
1.5	The proposed solution should match following criteria.		
	a. 6 number of 10/100/1000 Ethernet Ports		
	b. 20000 number of new connection / second		
	c. 600,000 number of concurrent connection		
	d. 2000 Mbps Firewall throughput		
	e. 200 Mpbs 3DES/AES VPN throughput		
	f. 900Mbps IPS throughput		
	g. 600 Mpbs AVAS throughput		
	h.UTM Throughput should be 450 Mbps		
1.6	The proposed solution should have unrestricted user/node license.		
1.7	The proposed solution must work as standalone HTTP proxy server with integrated Firewall, Anti Virus, Anti Spam, Content filtering, IPS.		
1.8	The proposed solution must support User based policy configuration for security & internet management.		
1.9	The proposed solution should have 3 years onsite warranty.		
	The proposed solution should provide on appliance reports based on user not only on the base of IP address.		
	Administration, Authentication & General Configuration		
2.1	The proposed solution should support administration via secured communication over HTTPS, SSH and from Console.		
2.2	The proposed solution should be able to export and import configuration backup including user objects		
2.3	The proposed solution should support Route (Layer 3)/transparent mode (Layer 2).		
2.4	The proposed solution should support integration with Windows NTLM, Active Directory, LDAP, Radius or Local Database for user authentication.		

2.5	The proposed solution should support Automatic Single Sign on (ASSO) for user authentication		
2.6	The proposed solution should support Dynamic DNS configuration.		
2.7	The proposed solution should provide bandwidth utilization graph on daily, weekly, monthly or yearly for total or individual ISP link.		
2.8	The proposed solution should provide real time data transfer/bandwidth utilization done by individual user/ip/application.		
2.9	The proposed solution should support Parent Proxy with IP/FQDN support.		
2.10	The proposed solution should support NTP.		
2.11	The proposed solution should support user/ip/mac binding functionality to map username with IP address & MAC address for security reason.		
2.12	The proposed solution should have multi lingual support for Web admin console.		
2.13	The proposed solution should support Version roll back functionality.		
2.14	The proposed solution should support session time out & Idle time out facility to forcefully logout the users.		
2.15	The proposed solution should support ACL based user creation for administration purpose.		
2.16	The proposed solution should support LAN bypass facility in case appliance is configured in Transparent mode.		
2.17	The proposed solution should support inbuilt PPPOE client and should be capable to automatically update all required configuration whenever PPPOE get changed.		
2.18	The proposed solution should support SNMP v1, v2c & v3.		
	Multiple ISP load balancing and Failover		
3.1	The proposed solution should support load balancing & failover for more than 2 ISP.		
3.2	The proposed solution should support explicit routing based on Source, Destination, Username, Application.		
3.3	The proposed solution should support weighted round robin algorithm for Load balancing.		
3.4	The proposed solution should provide option to create failover condition on ICMP, TCP or UDP protocol to detect failed ISP connection.		
3.5	The proposed solution should send alert email to admin on change of gateway status.		
3.6	The proposed solution should have Active/Active (Round Robin) and Active/Passive gateway load balancing and failover support.		
	High Availabiliy		
4.1	The proposed solution should support High Availability Active/Passive or Active/Active		
4.2	The proposed solution should support automatic & manual synchronization between appliances in cluster.		
4.3	The proposed solution should send notification to admin on change of appliance status in High Availability.		
4.4	The HA traffic between two peers must be encrypted.		

4.5	The proposed solution should support Link, device & Session failure.		
	Firewall		
5.1	The proposed solution should be standalone appliance with hardened OS.		
5.2	The proposed solution should be ICSA & Webcoast checkmark certified firewall.		
5.3	The proposed solution should support stateful inspection with user based one-to-one & dynamic NAT, PAT.		
5.4	The proposed solution must support user identity as matching criteria along with Source/Destination IP/Subnet/group, destination Port in firewall rule.		
5.5	The proposed solution should facilitate to apply unified threat policy like AV/AS, IPS, Content filtering, Bandwidth policy & policy based routing decision on firewall rule for ease of use, also unified threat controls must be applied on inter zone traffic.		
5.6	The proposed solution should support user defined multi zone security architecture.		
5.7	The proposed solution should have predefined application based on port/Signature & also support creation of custom application based on port/protocol number.		
5.8	The proposed solution should support ibound NAT load balancing.		
5.9	The proposed solution should support 802.1q VLAN tagging support.		
5.10	The proposed solution should support dynamic routing like RIP1, RIP2, ISPF, BGP4.		
5.11	The proposed solution should support Cisco compliance command line interface for Static/Dynamic routing.		
5.12	The proposed system should provide alert message on Dash Board whenever default password is not changed, non secure access is allowed & module subscription is expiring.		
5.13	The proposed system must provide Mac Address (Physical Address) based firewall rule to provide OSI Layer 2 to Layer 7 security		
	IPS		
6.1	The proposed solution should be webcoast checkmark certified.		
6.2	The proposed solution should have signature based and protocol anomaly based Intrusion prevention system.		
6.3	The proposed solution should have 3000+ signature database.		
6.4	The proposed solution must support creation of custom IPS signature.		
6.5	The proposed solution must support creation of multiple IPS policy for different zone instead of blanket policy at interface level.		
6.6	The proposed solution must support configuration option to disable/enable category/signature to reduce the packet latency.		
6.7	The proposed solution should give username along with IP in IPS alerts and reports.		
6.8	The proposed solution should automatically takes update from update server.		

6.9	The proposed solution must support blocking of anonymous open HTTP Proxy running on 80 port or any other port & also should support client based open proxy like Ultra surf. .		
6.10	The proposed solution should able to detect & block known P2P based instant messaging application like skype & known chat application like WLM, Rediffbol etc.		
6.11	The proposed solution should generate the alerts for attacks		
6.12	The proposed solution should generate historical reports based on top alerts, top attackers, severity wise, top victims, protocol wise.		
	Gateway Anti Virus		
7.1	The proposed solution should have an integrated Anti Virus solution.		
7.2	The proposed solution should have webcoast checkmark certification for Anti virus/Anti Spyware.		
7.3	The proposed solution must work as SMTP proxy not as MTA or relay server.		
7.4	The proposed solution should support scanning for SMTP, POP3, IMAP, FTP, HTTP, FTP over HTTP protocols.		
7.5	The basic virus signature database of proposed solution should comprise complete wild list signatures and variants as well as malware like Phising, spyware.		
7.6	The proposed solution should have facility to add signature/disclaimer in mails.		
7.7	The proposed solution must support on appliance quarantined facility and also personlized user based quarantine area.		
7.8	The proposed solution should support blocking of dynamic/executable files based on file extension.		
7.9	For SMTP traffic, the proposed solution should support following actions for infected, suspicious or protected attachments mails.		
	a. Drop mail		
	b. Deliver the mail without attachment		
	c. Deliver original mail		
	d. Notify to administrator		
7.10	The proposed solution should support multiple anti virus policy for sender/recipient email address or address group for notification setting, quarantine setting & file extension setting instead of single blanket policy		
7.11	The proposed solution should update the signature database at a frequency of less than one hour & it should also support manual update.		
7.12	For POP3 & IMAP traffic, the proposed system should strip the virus infected attachment & send notification to recipient & Admin.		
7.13	The proposed solution should scan http traffic based on username, source/destination IP address or URL based regular expression.		
7.14	The proposed solution should provide option to bypass scanning for specific HTTP traffic.		
7.15	The proposed solution should support real mode & batch mode for HTTP virus scanning.		

7.16	The proposed solution should provide historical reports based on username, IP address, Sender, Recipient & Virus Names.		
7.17	The proposed solution should have virus detection rate above 98%. Submit the required document.		
	Gateway Anti Spam		
8.1	The proposed solution should have an integrated Anti Spam solution.		
8.2	The proposed solution should have webcoast checkmark certification for Anti Spam.		
8.3	The proposed solution should have configurable policy options to select what traffic to scan for spam.		
8.4	The proposed solution should support spam scanning for SMTP, POP3, IMAP.		
8.5	The proposed solution should support RBL database for spam detection.		
8.6	The proposed solution must support mail archive option to keep copy of incoming & outgoing mails to administrator defined email address.		
8.7	The proposed solution should have multiple configurable policy for email id/address group for quarantine setting, different actions instead of blanket policy.		
8.8	The proposed solution must support on appliance quarantined facility and also personlized user based quarantine area with email release option		
8.9	The proposed solution should support real time spam detection & also supports proactive virus detection technology which detects and blocks the new outbreaks immediately and accurately.		
8.10	For Smtp traffic, the proposed solution support following actions		
	a. Tagging		
	b. Drop		
	c. Reject		
	d. Change recipient		
	e. Deliver the mail to recipient		
8.11	The proposed solution should support IP/Email address white list/Black list facility.		
8.12	The proposed solution should support option to enable/disable antispam scanning for SMTP authenticated traffic.		
8.13	The proposed solution should support spam detection using Recurrent pattern detection technology (RPD) to identify spam out breaks.		
8.14	The proposed solution should support language independent spam detection functionality.		
8.15	The proposed solution should block image based spam mails i.e. email message with text embedded in a image file.		
8.16	The proposed solution should provide historical reports based on username, IP address, Sender, Recipient & spam category.		
8.17	The proposed solution must provide Anti-Spam Message Digest feature per user.		
	Proxy Solution Web content filtering		

9.1	The proposed solution should be webcoast checkmark certified.		
9.2	The proposed solution should be integrated solution with local database instead of querying to database hosted somewhere on the internet.		
9.3	The proposed solution must work as Standalone HTTP proxy.		
9.4	The proposed solution must have 82+ web category with 40 Million URL database.		
9.5	The proposed solution must have following features inbuilt		
	a. Should able to block HTTPS based URLs with the help of Certificates.		
	b. Should able to block URL based on regular expression		
	c. Should support exclusion list based on regular expression		
	d. Must have support to block any HTTP Upload traffic.		
	e. Should able to block Google cached websites on based of category.		
	f. Should able to block websites hosted on Akamai.		
	g. Should able to identify & block requests coming from behind proxy server on the base of username & IP address.		
	h. Should able to identify & block URL translation request.		
9.6	The proposed solution should support application control blocking features as follows		
9.7	a. Should able to block known Chat application like Yahoo, MSN, AOL, Google, Rediff, Jabber etc		
9.8	b. Should support blocking of File transfer on known Chat application and FTP protocol.		
9.9	The proposed solution must block HTTP or HTTPS based anonymous proxy request available on the internet.		
9.10	The proposed solution should provide option to customize Access denied message for each category.		
9.11	The proposed solution should be CIPA compliant and should have predefined CIPA based internet access policy.		
9.12	The proposed solution should be able to identify traffic based on Productive, Neutral, unhealthy & non working websites as specified by admin.		
9.13	The proposed solution should have specific categories that would reduce employee productivity, bandwidth choking sites and malicious websites.		
9.14	The proposed solution should able to generate reports based on username, IP address, URL, groups, categories & category type.		
9.15	The proposed solution should support search criteria in reports to find the relevant data.		
9.16	The proposed solution should support creation of cyclic policy on Daily/Weekly/Monthly/Yearly basis for internet access on individual users/group of users.		
9.17	The proposed solution should support creation of internet access time policy for individual users or on group basis.		
9.18	The proposed solution should support creation of Data transfer policy on daily/weekly/monthly/yearly basis for individual user or group basis.		

9.19	The proposed solution should support creation of cyclic data transfer policy on Daily/weekly/Monthly/yearly basis for individual user or on group.		
9.20	The proposed solution should have integrated bandwidth management.		
9.21	The proposed solution should able to set guaranteed and burstable bandwidth per User/IP/Application on individual or shared basis.		
9.22	The proposed solution should provide option to set different level of priority for critical application.		
9.23	The proposed solution should provide option to define different bandwidth for different schedule in a single policy & bandwidth should change as per schedule on the fly.		
9.24	The proposed solution must provide web category based bandwidth management and prioritization.		
	VPN		
10.1	The proposed solution should be webcoast checkmark certified.		
10.2	The proposed solution should be VPNC Basic interop & AES interop certified.		
10.3	The proposed solution should support Ipsec (Net-to-Net, Host-to-Host, Client-to-site), L2tp & PPTP VPN connection.		
10.4	The proposed solution should support DES, 3DES, AES, Twofish, Blowfish, Serpent encryption algorithm.		
10.5	The proposed solution should support Pre shared keys & Digital certificate based authentication.		
	The proposed solution should support Main mode & Aggressive mode for phase 1 negotiation.		
10.6	The proposed solution should support external certificate authorities.		
10.7	The proposed solution should support export facility of Client-to-site configuration for hassle free VPN configuration in remote Laptop/Desktop.		
10.8	The proposed solution should support commonly available Ipsec VPN clients.		
10.9	The proposed solution should support local certificate authority & should support create/renew/Delete self signed certificate.		
10.10	The proposed solution should support VPN failover for redundancy purpose where more than one connections are in group & if one connection goes down it automatically switch over to another connection for zero downtime.		
10.11	The proposed solution should have preloaded third party certificate authority including VeriSign/Entrust.net/Microsoft and provide facility to upload any other certificate authority.		
10.12	The proposed solution should support Threat free Ipsec/L2TP/PPTP VPN tunnel.		
10.13	The proposed solution must provide on appliance SSL-VPN solution with Web Access (Clientless), Full Tunnel and Split Tunnel control. Solution should provide per user / group SSL-VPN access		
10.14	SSL-VPN solution should be certified by VPNC for SSL Portal / FireFox Compatibility / Java Script / Basic and Advanced Network Extensions.		

	Logging & Reporting		
11.1	The proposed solution should have integrated on appliance reporting.		
11.2	The proposed solution should support minimum 45 different templates to view the reports		
11.3	The proposed solution should provide reports in HTML, CSV & graphical format.		
11.4	The proposed solution should support logging of Antivirus, Antispam, content filtering, Traffic discovery, IDP, Firewall activity on syslog server.		
11.5	The proposed solution should provides detailed reports for all files uploaded via HTTP or HTTPS protocol. The report should include username/IP address/URL/File name/Date and Time.		
11.6	The proposed solution should provide data transfer reports on the based of application, username, Ipaddress.		
11.7	The proposed solution should provide connection wise reports for user, source IP, destination IP, source port, destination port or protocol.		
11.8	The proposed solution should have facility to send reports on mail address or on FTP server.		
11.9	The proposed system solution provides approximate 45 regulatory compliance reports for SOX, HIPPA, PCI, FISMA and GLBA compliance.		
11.10	The proposed solution should support Auditing facility to track all activity carried out Security appliance.		
11.11	The proposed solution should support multiple syslog server for remote logging.		
11.12	The proposed solution should forward logging information of all modules to syslog servers.		
11.13	The proposed solution should have configurable option to send reports on designated email address.		
11.14	The proposed solution should be able to provide detailed reports about all mails passing through the firewall.		
11.15	The proposed solution should provide reports for all blocked attempts done by users/Ipaddress.		

ANNEXURE-C

FORMAT FOR SUBMISSION OF QUOTATION

Supply and installation of Unified Threat Management Device

Name of the Firm:

Address:

Bill of Quantities

Sl.No.	Description	Qty. (Nos.)	Unit Rate (Rs.)	Amount (Rs.)
1	Supply and Commissioning of Unified Threat Management Device (as per the specifications stated above) Name of the Product: Product Code (If any) (With one year Comprehensive on warranty including updates and upgrades)	1		
	Cost of Additional 2 years Comprehensive on warranty including updates and upgrades	1		
	VAT @ ______ % on Amount			
	Grand Total			

(Signature of Supplier with seal and date)

Name:

Designation:

Mobile No: