



CSIR-CENTRAL ELECTROCHEMICAL RESEARCH INSTITUTE
KARAIKUDI – 630 006
(Council of Scientific & Industrial Research)

Phone: 04565- 227206 Fax: 04565- 227204, 227206 E-mail: spo@cecric.res.in
purchase@cecric.res.in

No: PUR/PT/3/2011-12

Date: 26.08.2011

TENDER NOTICE

Sealed tenders are invited under Two-bid system (Part-I TECHNICAL BID & Part-II COMMERCIAL BID) from reputed manufacturers and their accredited/sole selling agents for “Supply, Installation, Commissioning and Satisfactory Demonstration and support” of the following items.

SL. NO	DESCRIPTION OF ITEMS	QTY	EMD		
			INR	US\$	EURO
1	Unified Threat Management System And Corporate Academic License For Antivirus	1 No	120000/-	2650/-	1810/-

Tender Documents can be downloaded from CECRI website <http://www.cecric.res.in> at Free of Cost.

Tender documents can also be had from the Office of the Stores & Purchase Officer, CECRI, Karaikudi on payment of Tender fee Rs.300/- by Demand Draft drawn in favour of the Director, CECRI, Karaikudi payable at Karaikudi. EMD by Demand Draft / Bank Guarantee should be submitted along with the Part I-Technical BID.

Last date for submission of Tenders : **19.09.2011 up to 11.00 AM (IST)**
Date of opening of Technical Bids : **19.09.2011 at 11.30 AM (IST)**

Director, CECRI reserves the right to reject any or all the tenders without assigning any reason or to accept them either in part or in full.

STORES & PURCHASE OFFICER

REQUEST FOR PROPOSAL (RFP)

FOR

Purchase, Installation, Commissioning and Support of

UNIFIED THREAT MANAGEMENT SYSTEM

AND

CORPORATE ACADEMIC LICENSE FOR ANTIVIRUS



**CSIR-Central Electrochemical Research Institute
Karaikudi 630006**

Table of Contents

1. Instructions to Bidders	4
1.1. Introduction and Background.....	4
1.2. Existing Network	4
1.3. Objectives.....	4
1.4. Submission of Proposals.....	5
1.4.1 Bid Security/EMD	6
1.4.2 Eligibility Criteria for Bidders.....	7
1.4.3 Technical Proposal	7
1.4.4 Financial Proposal.....	8
1.5 Disqualifications.....	9
1.6 Evaluation Process	9
2. Terms of Reference	10
2.1 Scope of Work	10
2.1.1 Specifications for Unified Threat Management System Appliance (UTM)	12
2.1.1.1 Technical Specification for UTM at CSIR-CECRI, KARAIKUDI	12
2.1.1.2 Components of Training	21
2.1.2.1 Specification of Antivirus at CSIR-CECRI, KARAIKUDI.....	22
3. Annexures	27
3.1 Annexure-1: Notice of Intent to Bid	27
3.2 Annexure-2: Proposal covering letter.....	28
3.3 Annexure-3 Technical Bid	31
3.4 Annexure- 4 Technical Bid Format:.....	33
3.5 Annexure- 5: Bid Security/EMD Form	35
3.6 Annexure -6: Proforma of Performance Bank Guarantee.....	36
3.7 Annexure -7: Proforma For Price Bid	37

1. Instructions to Bidders

1.1. Introduction and Background

CSIR-CECRI, Karaikudi is a research laboratory under Council of Scientific and Industrial Research, New Delhi and is an autonomous body under the Ministry of Science and Technology. CSIR-CECRI is declared as academic institution and is eligible for academic pricing for software licensing.

1.2. Existing Network

Networking

Local Area Network:

A switch-based network has been installed at CSIR-CECRI Campus, Karaikudi and all switches were connected through UTP Cat 5 Cables.

Connectivity:

- 1Gbps LAN connectivity with Layer 3 switches
- Internet through dedicated 1:1
- 8 Mbps Lease Line on Fibre through BSNL at KARAIKUDI and 1 Gbps Lease Line from National Knowledge Network (NKN) through National Informatics Centre, New Delhi.

Router:

Lease Line is terminated in CISCO Router

Servers:

Servers at CSIR-CECRI, KARAIKUDI. (20 in Nos.)

- Xeon Server loaded with Windows Server 2003 / 2008 R2 dedicated for Website, database, proxy, Antivirus etc.
- 10 servers are fully populated Two Way servers

Client Machine

Presently there are approx 750 machines, installed at CSIR-CECRI, KARAIKUDI. Machines include Servers, Computers and Laptops are working in networking environment with windows operating system (Vista and XP and Windows 7).

1.3. Objectives

CSIR-CECRI proposes to buy Unified Threat Management System (UTM) Hardware based and Antivirus solution with three years comprehensive on site warranty. The main objective of this proposal is to secure the CSIR-CECRI, KARAIKUDI network from Virus, Spamware, Malware, and Intrusion at the gateway level as well as the desktop level.

1.4. Submission of Proposals

The proposals shall be submitted in two-bid format (one each for Technical Bid & Earnest Money Deposit (EMD) and Financial Bid)

- a) Technical details, as per Annexure 3 & 4*
- b) Financial details (Summary as per Terms of reference)*

The Bidder shall submit Technical Bid and Financial Bid documents in separate wax sealed envelopes clearly marking Technical and Financial Bid on the top left hand corner. The two sealed covers should be enclosed in a bigger cover which should also be sealed and duly superscribed. Sealed proposals may be dropped in the Tender Box placed at CSIR-CECRI, KARAIKUDI, latest by **19.09.2011 11.00 A.M. (IST)**

The envelope should be addressed to:

**The Stores and Purchase Officer
CSIR-CECRI
KARAIKUDI - 630006
SIVAGANGA DISTRICT,
TAMILNADU
INDIA**

Following are the Terms and Conditions for the tender bid submission:

1. The tenderer cannot bid in **consortium**
2. Award of the contract resulting from this tender will be based upon the most responsive bidder whose offer will be the most advantageous to CSIR-CECRI in terms of cost, functionality and other factors as specified.
3. The bid will be given to single vendor based on the lowest evaluated quote.
4. CSIR-CECRI reserves the right to reject any or all offers and discontinue this tender process without obligation or liability to any potential Bidder
5. All proposals received after the specified date and time shall not be considered for award of work.
6. The Stores and Purchase Officer, CSIR-CECRI, KARAIKUDI will not accept delivery of proposals by Fax or E-mail. Proposals received by Fax or E-mails shall be treated as defective, invalid and rejected.
7. The original and copies of the bid, each consists of the documents listed in instructions, shall be typed and shall be signed by the bidder or a person(s) duly authorized to bind the bidder to the contract.
8. The Council of Scientific and Industrial Research will be under, no legal obligation to provide employment to any of the personnel of the contractor after expiry of agreement period and the Council recognizes no employer-employee relationship between the Council and the personnel deployed by the contractor.
9. The bids complete in all respect addressed to Stores and Purchase Officer, CSIR-CECRI, KARAIKUDI, should reach at the following address latest by **19.09.2011 11.00 A.M. (IST)**. **The Stores and Purchase Officer, CSIR-CECRI, KARAIKUDI - 630006, SIVAGANGA DISTRICT, TAMILNADU, INDIA.**
10. The Technical Bid for Supply, Installation, Implementation, Support and Training of Unified Threat Management System and Antivirus will be opened on 19.09.2011-11.30A.M.(IST) in the Office of SPO at CSIR-CECRI, KARAIKUDI in the presence of bidders who chose to be present.

1.4.1 Bid Security/EMD

- a. The Bidder shall furnish, as part of its Technical proposal, Earnest Money Deposit (EMD) **as seen at page no.1 of this document**.
- b. The Bid Security/EMD shall be in the form of Demand Draft/Bankers' Cheque/ Bank Guarantee drawn in favour of CSIR-CECRI, KARAIKUDI issued by a Scheduled Bank. The Bid Security/EMD shall be valid for a period of **90** days beyond the final bid validity period.
- c. The Bid Security/EMD must invariably be submitted in the Technical Bid Cover.
- d. Any proposal not sealed shall be rejected by the CSIR-CECRI, KARAIKUDI
- e. The Bid Security/EMD provided by the Bidder whose proposal is accepted shall be repaid or discharged when the Performance Security has been duly submitted when the vendor and vendee enter into and execute a Contract.

- f. Bid Security/EMD of unsuccessful bidders will be returned within and not later than **30** days of award of contract to the successful bidders.
- g. Bid Security/EMD will be provided as per **Annexure-5**.
- h. Forfeitures of Bid Security/EMD:
The Bid Security/EMD may be forfeited:
 - _ if a bidder withdraws its bid during the period of validity of his proposal as specified by the bidder in his proposal; or
 - _ in the case of the successful bidder, in case the bidder fails -
 - o to sign the contract or
 - o to furnish performance security as mentioned at **Annexure-6** of the RFP

1.4.2 Eligibility Criteria for Bidders

Following criteria has been defined for eligibility of firm (copy of the documentary evidence must be submitted.) The firms that qualify the below mentioned criteria need only apply.

- a. The bidder should have had an average annual turnover of Rs. 25,00,000/- (Twenty five Lakh) or above during the last 3 financial years in installing , implementation and selling security related products, solutions and services i.e. for the financial years 2008-09,2009-10 & 2010-11.
- b. The bidder should have experience of selling, installing and providing support for the UTM, Antivirus or any cyber security related products, for at least 3 organizations like banks, financial institutions, Insurance Companies, Government departments or any other listed companies.
- c. The bidder should have at least one implementation/technical support office near Karaikudi with overnight journey.
- d. The bidder should have to submit the proof for the eligibility criteria including Service Tax Registration, PAN Number issued in the name of firm etc.

1.4.3 Technical Proposal

Following are the terms and conditions for the Technical Proposal

- 1. The bidder is required to install and implement UTM and Antivirus solution at CSIR-CECRI, Karaikudi
- 2. The bidder is required to give 3 years comprehensive onsite warranty for UTM and 3 years software license for antivirus and free update for 3 years.
- 3. Bidder must have quote one OEM product on one Tender document.
- 4. The installation of the software will be done in all the requisite Desktops, Laptops and Servers free of charge by the Vendor up to the satisfaction of CSIR-CECRI, KARAIKUDI Team.

5. Built-in feature of UTM Antivirus must be different from Antivirus being offered for the desktop.
6. OEM will provide free of cost certification training on UTM and Antivirus. The components of training is defined at 2.1.1.2 Components of Training
7. Vendor/ OEM will provide all the updates and upgrades including version upgrades (including their reinstallation) free of cost during the valid licensed period (warranty period)
8. The Vendor will give unlimited number of support call with 4 hour response time.
9. One Resident Engineer (Certified Network Security Personnel) should be made available in CSIR-CECRI, KARAIKUDI on all working days (Monday - Saturday between 9.00 AM to 5.30 PM for Technical support for managing system / facility and other services of UTM / anti virus / firewall. In case of emergency services during holidays and after working hours, the same will be made available at no extra charges during the warranty period of 3 years.
10. The software packages (academic licensing) to be offered should be legally valid, licensed and latest version along with the complete set of manuals and at least one set of media.
11. OEM should provide 24 x 7 e-mail, toll free number telephonic support for unlimited number of incidents

1.4.4 Financial Proposal

Following are the terms and conditions for the Financial Proposal

1. This tender is for a fixed price bid.
2. The financial proposal shall be priced in Indian Rupees.
3. The Financial proposal shall clearly indicate, and submit the Financial Summary Sheet, which should include the total costs of product (UTM + Antivirus), installation of the product with 3 years comprehensive onsite warranty and quote separately for another 2 years as described in the Terms of Reference (TOR) as well as taxes namely Value Added Tax (VAT) and Service Tax etc. wherever applicable.
4. The quotations shall be fixed and shall not allow for any fluctuation in costs of labour, transport, etc. No adjustment shall be made to the contract value for any fluctuation arising following submission of tender.

1.4.5. DELIVERY :

Delivery of the ordered items and installation & commissioning are expected to be completed within 15 days (fifteen days) from the date of issue of Letter of Intent / Purchase Order/Work Order. However, tenderer must mention its earliest delivery schedule in their tender.

1.4.6. PAYMENT TERMS :

The payment terms will be as under :-

1. 65% of the total order value after the receipt of supply in good condition.
2. 25% on satisfactory installation, testing and commissioning.
3. Balance 10% on submission of Performance Bank Guarantee of equivalent amount, as per format enclosed as **Annexure-6**, valid upto warranty period plus two months.
4. All the payments will be made through crossed DD/ Account payee DD payable at Karaikudi _____ in favour of The Director, CSIR-CECRI, Karaikudi.
5. Cost of Resident Support Engineer will be paid every quarter against claim.

1.5 *Disqualifications*

CSIR-CECRI may at its sole discretion and at any time during the evaluation of Proposal, disqualify any bidder, if the bidder has:

- a. Submitted the Proposal documents after the scheduled date and time;
- b. Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements;
- c. Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years;
- d. Submitted a proposal that is not accompanied by required documentation or is non responsive;
- e. Failed to provide clarifications related thereto, when sought;
- f. Submitted more than one Proposal;

1.6 *Evaluation Process*

A two-stage procedure (i.e Technical Bid and Financial Bid) will be adopted for evaluation of proposals. The process for evaluation of proposals is as given below:

a) Technical Evaluation: An Evaluation Committee will assess all the Technical bids received. The committee may ask for Demo or Presentation. The Technical bids will be evaluated based on the required technical specifications. Bids which do not meet the technical specifications will be rejected and financial bids of these firms will not be opened.

b) Financial Bid Evaluation: Financial Bids of the firms which meet the Technical Specifications will be opened by the Tender opening Committee.

The price bid must be in accordance with the Proforma at **Annexure -7** and failure to do so shall result in rejection of the tender. The price Bid shall be evaluated on the

basis of overall charges for items no. 1 to 6 mentioned in the Annexure - 7. The contract shall be awarded to lowest out of technically qualified bidders.

The rates should be quoted both in figures and words. The rates quoted shall be net and firm. No upward changes in the rate will be acceptable during the period of contract.

Taxes and Duties: The taxes and duties should be quoted separately and clearly. The terms such as Taxes and duties as applicable or at actual should not be mentioned in the quotation. In the event of an increase in taxes/duties, the extra liability on account of these taxes shall be borne by CSIR-CECRI. Similarly in the event of abolition / reduction of taxes/duties, the savings accruing to the bidder shall be passed on to CSIR-CECRI.

Discrepancies in Prices: Any discrepancy between quoted prices in figures and that in words, if noted, will be sorted out in the following manner.

- (i) If there is a discrepancy between the unit price and the total price; the unit price shall prevail and the total price will be corrected accordingly.
- (ii) If there is an error in a total corresponding to the addition or subtraction of subtotals, the sub totals shall prevail and the total shall be corrected.
- (iii) If there is a discrepancy between words and figures, the amount in words shall prevail unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to above.
- (iv) If there is such discrepancy in a bid, the same is to be conveyed to the bidder and if the bidder does not agree to the observation of the CSIR-CECRI, the tender is liable to be rejected.

Conditional or ambiguous tenders are liable to be rejected summarily.

2. Terms of Reference

2.1 Scope of Work

1. The bidder is required to supply, install, implement and support of UTM and Antivirus solution
2. The bidder is required to give 3 years comprehensive onsite warranty.
3. The bidder is required to give comprehensive On-site Technical support for managing system/facility management for 3 years, which may be further extendable for another 2 years.

The installation of the software will be done in all the requisite Desktops, Laptops and Servers free of charge by the Vendor up to the satisfaction of CSIR-CECRI, KARAIKUDI Team.

OEM will provide free of cost certification training on UTM and Antivirus. The components of training is described 2.1.1.2.

Vendor/ OEM will provide all the updates and upgrades (Hardware/Software) including version upgrades (including their reinstallation) free of cost during the valid licensed period/ warranty period.

One Resident Engineer (Certified Network Security Personnel) should be made available in CSIR-CECRI, KARAIKUDI on all working days (Monday - Saturday) between 9.00 AM to 5.30 PM for technical support for managing system / facility and other services of UTM /anti virus / firewall. In case of emergency services during holidays and after working hours, the same will be made available at no extra charges.

The software packages (academic) to be offered should be legally valid, licensed and latest version along with the complete set of manuals and at least one set of media.

OEM should provide 24 x 7 e-mail, toll free number telephonic support for unlimited number incidents.

2.1.1 Specifications for Unified Threat Management System Appliance (UTM)

Hardware based UTM

2.1.1.1 Technical Specification for UTM at CSIR-CECRI, KARAIKUDI

Number of users at CSIR-CECRI, KARAIKUDI-750 (including PC, Laptop and Servers)

Table 1: Technical Specifications for Unified Threat Management System Appliance (UTM)

S. No.	Description of Models & Related Items to be quoted	Compliance (Yes / No)
1.	Identity based UTM Model (Specify Product and Model)	
	i) UTM Appliance Throughput	
	i) Concurrent Sessions : 10,00,000 and 50,000 new sessions/Sec with "Always On" IPS	
	ii) TCP Firewall Throughput (Mbps): 5000	
	iii) Antivirus Throughput (Mbps) : 200-250	
	iii) IPS Throughput (Mbps) : 250-350	
	iv) VPN Throughput (Mbps) : 100-150	
	ii) 8 nos. of 10/100/1000 Fast Ethernet Port and populated with 2x10Gb ports	
	iii) Appliance should have Hot swappable redundant power supply	
	iv) Warranty & Software Subscription for three years (on-site comprehensive) covering 24x7 Support with the following functionality :	
	i) Administration, Authentication & Configuration	
	ii) Identity based Policy Controls	
	iii) Firewall Requirements	
	iv) Bandwidth Management	
	v) Intrusion Detection and Prevention (IDP)	
	vi) Gateway Anti-virus and Anti-spyware	
	vii) Gateway Anti-spam	
	viii) Web Content & application Filtering	
	ix) Multiple ISP Load Balancing and Failover	
	x) Reporting	
	xi) Virtual Private Network (VPN)	
	Detailed Specifications as under Table-2 & Table-3	

Table - 2 Technical Detailed Specifications for Unified Threat Management System

S. No.	Technical Specifications	Compliance (Yes / No)	Remarks
A	Administration, Authentication & Configuration		
A.1	The proposed system should support LDAP, RADIUS & Active Directory and in built database of the appliance for User Authentication		
A.2	The proposed system should provide Single Sign-on Integration for Windows Authentication		
A.3	The proposed system should provide dynamic DNS support with NATed IP detection facility		
A.4	The proposed system should have facility to generate daily, weekly, monthly, and yearly Bandwidth Utilization Graphs (like MRTG) for all the defined ISP Links		
A.5	The proposed system should allow Network admin to view amount of upload and download Data transfer done by each user separately in real time basis		
A.6	The proposed system should allow Network admin to view bandwidth consumed by each individual user in the network on real time basis		
A.7	The proposed system should be able to generate real time traffic reports - Application wise & user wise		
A.8	The proposed system should provide facility for Web-based & Secure console based remote administration		
A.9	The proposed system should able to function as SNMP agent and should be SNMP v1, v2c and v3 compliant		
A.10	The proposed system should be centrally managed by Enterprise Wide Management Console.		
A.11	The proposed system should be centrally monitored by Enterprise Wide Management Console.		
A.12	LAN Bypass facility in Bridge mode		
B	Identity based Policy Controls		
B.1	<p>Surfing Quota Policy</p> <p>The proposed system should support creation of time base (quota) (ex: 100 Hours, 200 Hours) policy for individual users and group</p> <p>The proposed system should support creation of Weekly Cyclic policy of limited period of internet surfing based on Individual users & groups</p> <p>The proposed system should support creation of Surfing Quota policies based on combination of Hours & Validity in terms of Day, Week, Month & Yearly (ex: 8 Hours of Daily surfing valid till 1 Year).</p>		

B.2	<p>Access Time Policy</p> <p>The proposed system should support creation of policy to control Internet access time for individual users and group</p> <p>The proposed system should support creation of policy to control Internet access time based on time and days of the week (ex: Internet access to be only allowed to specific users or group during working hours 9:00 AM to 6:00 PM from Monday to Saturday)</p>		
B.3	<p>Data Transfer Policy</p> <p>The proposed system should provide facility to allocate Data transfer Quota (1 GB, 2 GB, 100 MB etc) to individual user policies or group policies or group policies based on User Identity</p> <p>The proposed system should support creation of daily, weekly, yearly upload and download based policies for user & group basis (eg. 1 GB Upload & 1GB Download of Data transfer allowed every Month or Year)</p> <p>The proposed system should provide facility to allocate Data transfer Quota on shared basis between group users</p>		
C	Firewall Requirements		
C.1	The firewall should be dedicated standalone appliance		
C.2	The proposed system should be ICSA / EAL4+ certified.		
C.3	The proposed system should be able to create firewall rules based on usernames and not on Hosts / Subnets (e.g. Rule can be created based on the named of network admin (like john, harry) to allow certain privilege access such as ftp, ssh without the need of providing hostnames, IP or Subnets)		
C.4	The proposed system should have firewall with stateful packet filtering technology & must support one-to-one and dynamic user based NAT with a facility to create rules based on usernames, Source & Destination IP address, Hosts, network, IP Range.		
C.5	The firewall of the proposed system should be able to support transparent mode/Bridge mode for Seamless deployment into an existing network without changing IP configurations in the network.		
C.6	<p>The firewall of the proposed system should provide multi-zone security architecture as follows:</p> <p>User assignable zones on different physical interfaces</p> <p>Different IDP policies between different zones</p> <p>Multiple IDP policies for each zone</p>		
C.7	The firewall of the proposed system should provide Pre-defined services based on port numbers and Layer 7 application signatures and ability to create user-definable services which can be used to define firewall		

	rules.		
D	Bandwidth Management		
D.1	The proposed system should have integrated Bandwidth Management		
D.2	The proposed system should be able to set guaranteed and burstable bandwidth per User and group of Users		
D.3	The proposed system should be able to create Bandwidth Policies based on applications and not on IP or Ports		
D.4	The proposed system should provide user based and layer 7 based visibility and bandwidth utilization for every connection established through that system		
E	Intrusion Detection and Prevention (IDP)		
E.1	The proposed system should have signature and anomaly base intrusion detection and prevention system		
E.2	The proposed system should support the creation of custom IDP signatures		
E.3	The proposed system should be able to provide multiple IDP policies and allow attaching an IDP policy to a firewall rule. This should help the administrator in defining customized IDP policies as per his requirements of security and alerts		
E.4	The proposed system should report internal alerts based on username and not on hostnames or IP addresses.		
E.5	The proposed system should automatically update the attack signatures database from a central database server		
E.6	The proposed system should be able to detect and block HTTP proxy traffic		
E.7	The proposed system should be able to detect and block P2P based Instant Messaging application like Skype		
E.8	The proposed system should be able to detect and block Instant Messaging applications like Windows Live Messenger, Rediff bol etc and other port independent applications using IDP signatures.		
F	Gateway Anti-Virus and Anti-Spyware		
F.1	The proposed system should have an integrated Anti-Virus solution and should be able to provide real-time detection of viruses and malicious code at the gateway for HTTP, SMTP, POP3, IMAP,VPN and FTP over HTTP Internet traffic		
F.2	The Basic Virus Signature Database of the proposed system should comprise of the complete Wild List Signatures and variants as well as malware like phishing mails and spyware. The antivirus system should not be share-ware, free-ware		

F.3	The proposed system should have facility to add signature / Disclaimer in emails		
F.4	The proposed system should have facility to send notification of virus information to admin email id		
F.5	The proposed system should have configurable policy options to block different file types such as Executables, Dynamic files		
F.6	The proposed system should have configurable policy options to block customized file type attachments like .doc, .xls, .ppt etc		
F.7	In SMTP Antivirus scanning subsystem, if email message is either infected, suspicious or protected attachment, then following options should be there to either deliver original email or do not deliver or remove attachment and deliver. Similarly notification to administrator on either of the above options should be available		
F.8	In SMTP system, it should support facility to create customized scanning rules		
F.9	Customized scanning rules should allow policies to be applicable on sender/recipient email addresses or address groups for notification settings, quarantine settings and file extension blocking		
F.10	The proposed system should be able to update signature database automatically at a preconfigured interval with the frequency of less than 1 hour and through manual update action also		
F.11	The HTTP AntiVirus gateway should be able to scan sites based on source, destination and URL regular expressions		
F.12	The HTTP Anti Virus system should be able to bypass source & destination Hosts		
F.13	The HTTP Anti Virus should have scanning options of real mode and batch mode with option to restrict file size for scanning		
F.14	The proposed system should be able to provide alerts and reports based on username, protocol, IP address, sender, recipient, subject and Virus-names		
G	Gateway Anti-Spam		
G.1	The proposed system should have an integrated Anti-Spam solution in the Appliance.		
G.2	The proposed system should have ability to filter SMTP, POP3 and IMAP traffic		
G.3	The proposed system should have configurable policy options to select what traffic to scan for spam		
G.4	The proposed system should have facility to mark a copy of all incoming and outgoing emails to administrator defined email address		

G.5	The proposed system should have an option of having a configurable spam policy per email address or address group		
G.6	The proposed solution should be able to tag email subject based on the spam filter matching criteria		
G.7	The proposed system should minimally provide SPAM filtering based on: IP address Black/White list Real-time black hole List (RBL) or Open Relay Database List (ORDBL) servers		
G.8	The proposed system should be able to provide alerts and reports based on username, mail protocol IP address, sender, recipient, subject and spam-categories		
G.9	The proposed system should provide option to enable/disable antispam functionality for SMTP authenticated traffic.		

G.10	The proposed system should have ability to filter Image based spam i.e. email message with the text embedded in an image file.		
G.11	Should support spam detection using Recurrent Pattern Detection (RPD) to identify spam out breaks		
H	Web Content Filtering and Application control		
H.1	The proposed system should have integrated Web Filtering solution in the appliance		
H.2	Websites & its category information should be locally stored inside the Appliance & it should not query third party or Remotely Hosted Servers on Data centres		
H.3	System should have facility to block Web based upload of the attachments		
H.4	The proposed system should provide web content filtering features as follows: URL database should have at least 8 million sites and 60+default categories Should block URLs based on regular expressions Should have support for URL exclusion list based on regular expressions Should be able identify & block Google cached links based on its categories Should be able to identify URL Translation Web server and block requests to such servers		
H.5	The proposed system should provide application control features as follows: Should be able to block famous chat and instant messaging communication like yahoo, jabber, msn, AOL messenger etc and other applications based on signatures and independent of ports Should be able to block file upload through IM, FTP protocols		

H.6	The proposed system should be able to customize block message for each categories		
H.7	The proposed system should be able to log and report usernames, request IP address, domain name, URL, website category and category type		
H.8	The proposed system should be able to identify traffic based on productive, neutral & unproductive websites as specified by admin		
H.9	The proposed system should provide default Internet Access policy for unauthenticated HTTP Proxy users.		
I	Multiple ISP Load Balancing and Failover		
I.1	The proposed system should have integrated multiple ISP Load balancing and failover for outbound traffic		
I.2	The proposed system should support load balancing and failover for more that 2 ISP link		

I.3	The proposed system should be able to do weighted round robin based load balancing of traffic over multiple link based on the weight assigned to each link		
I.4	The proposed system should be able to detect link failure based on user configurable set of rules based on ICMP, TCP ;and UDP		
J	Reporting solution		
J.1	The proposed system should have reporting solution. The reports should be accessible through HTTP/HTTPS/Client based.		
J.2	The proposed system should provide individual users download & Upload traffic reports		
J.3	The box should provide on box reporting, if additional hardware required should be provided by the bidder bundled with the UTM box and the hardware should be quad core processor based rack mountable, including all hardware and software warranty for the quoted period.		
J.4	The proposed system should provide user based, group based and IP address based reports for traffic discovery, Gateway level Anti Virus & Anti Spam, Intrusion detection and prevention and Web Content Filter		
J.5	The proposed system should provide reports in HTML/Graphical/CSV/PDF format		
J.6	The proposed system should have configurable options to send the reports on mail to designated email addresses		
J.7	The proposed system should have options to create users with different access rights (E.g. users who can only view report and not manage the system)		
J.8	The proposed system should be able to provide connection wise reports for user, application, source		

	and destination IP address and source and destination port and protocol		
J.9	The reporting solution of the proposed system should be able to provide detailed reports about the mail activity passing through the system		
J.10	The reporting solution of the proposed system should be able to provide detailed Audit log for auditing and tracking system		
J.11	Logging : The proposed solution must have support for Syslog server It must have support to enable Syslog for a particular policy		
K	Virtual Private Network (VPN)		
K.1	The proposed system should allow to create and establish IPSec (Net-to-Net, Host-to-Host and Road warrior connection), L2TP and PPTP VPN connection		
K.2	The proposed system should allow PSK and Digital Certificate based Authentication.		
K.3	The proposed system should support Connection fail over for Net-to-Net, Host-to-Host and Road warrior connection		
K.4	The proposed system should support following Encryption algorithm:3DES, DES, AES Twofish, Blowfish, Serpent		
K.5	The proposed system should support external Certificate Authorities		
K.6	The proposed system should provide a facility to export the Toad Warrior connection configuration for use by the VPN client		
K.7	The proposed should support most commonly available VPN IPSec Clients		

Table - 3 : General UTM Specifications

S.No.		General UTM Specification	Compliance (Yes/No)	Remarks
1.	Licensing	The proposed solution must be licensed per unit & there should not be any license limit on number of sessions, firewall rules, maximum number of connections, no of nodes/desktops, no of IPs, domains etc for all modules		
2.	Certification	The product should have following certification at time of implementation: Checkmark UTM Level 1 ICSA		

		certified / EAL4+ certified / FCC/CE certification for Firewall Module.		
3.	Mounting	Product should be 1U or 2U 19" Rack Mountable Chassis (Mounting kit/ brackets to be supplied and fixed)		
	Firmware/ software Warranty	The above product should be covered under 3 years complete/ comprehensive warranty that includes firmware and software upgrades and all signature updates for all the components supplied in the device for 3 years		
	Hardware Warranty	The above Hardware product should be covered under 3 years complete/ comprehensive warranty that includes Hardware replacement within 24 hours in case of Hardware Device Failure		
	Bundling	All the necessary cables, connectors, external software media, manuals or any other hardware and software should be bundled and included for all operations listed above		
	Satisfactory Installation Reports	At least three installations in India of the device (of the same model or range of the model quoted in the bid) in successful operation for at least one year as reckoned from date of BID opening. (attach the list with customer address and contact details and customer satisfaction certificate and copy of purchase orders excluding commercial details / Price)		

2.1.1.2 Components of Training

Training Schedule
Day 1
Trainers Introduction, Delegate Introduction
Basics of Networking & Security
Identity Based UTM
About the Product
Deployment

Day 2
Firewall
User Authentication
Configuration
Content filter and Application control

Day 3
Bandwidth Management
Intrusion Prevention System (IPS)
Intrusion Detection System (IDS)

Day 4
Gateway Anti Virus / Anti-Spyware / Anti Spam
Virtual Private Network (VPN)
Multilink Manager

Day 5
Routing
Reporting
Administration

2.1.2. Specifications for Antivirus

2.1.2.1 Specification of Antivirus at CSIR-CECRI, KARAIKUDI

Number of users at CSIR-CECRI, KARAIKUDI-750 (including PC and Servers)

(A) **Anti Virus and anti spyware solution for Desktops, Laptops & Servers**

S/N (1)	CSIR-CECRI Requirement (2)	Specify Yes or No (3)	Remarks (4)
Antivirus for Desktops, Laptops and Servers			
	MAKE AND MODEL :		
1.	Software must provide Virus protection at Servers and Desktop level and also provide a centralized management console		
2.	Solution must provide automated and centralized download from the Internet to single management console. The distribution of antivirus signatures should happen seamlessly from a single management console to all systems which are under networking across the organization, across different Windows platforms. The machines which are not under network should be updated manually.		
3.	Software must include audit trail logging and reporting capability. It should provide centralized logs and reports of all virus events on Desktops, Laptops and servers, including files checked, viruses found and responses taken. The centralized reporting should include reports like top 10 viruses, top infected machines and other such reports.		
4.	Must protect against all kinds of viruses, trojan horses and worms including: boot sector, master boot sector, memory resident, file multipartite, macro etc.		
5.	Must support exclusion list by file extensions		
6.	Must have quarantine capabilities so as to quarantine a system that has been infected.		
7.	Must scan Floppy disks, CD ROM , all external media and Network Drives automatically in real-time when accessed		

8.	Must scan compressed file archives in ZIP, ARJ, RAR and Microsoft Compressed formats. It should also protect from viruses hiding in compressed files, such as Internet downloads and e-mail attachments		
9.	Must provide a variety of ways to handle viruses, including: cure, rename, move, report, delete or purge		
10.	Must have the capability to automatically copy a file before curing- creating a temporary backup		
11.	Must have heuristic scanning to allow rule -based detection of unknown viruses.		
12.	Should support multiple platforms - eg. Windows 2000 ((Professional / Server / Advanced Server) / XP (Professional / Home) / 2003 (Standard / Enterprise Edition), Vista, Windows 7, Windows 2008 (Standard / Enterprise Edition), Linux, any future OS update and browsers like Internet Explorer, Firefox,Google Chrome, Safari etc.,		
13.	Must have hands-free signature updates down to the desktop		
14.	Must ensure real time protection even during the signature and engine updating process.		
15.	The solution shall provide periodical signature updates (daily) and signature updates shall be provided free regardless of the validity of maintenance contract.		
16.	The solution should have incremented updates facility		
17.	It should have the facility of scheduled scanning		
18.	It should give a pop-up alert box to the user to disinfect, delete, quarantine or block access to that file whenever an infection is found in it (user defined)		
19.	Have detailed system information (of IP address, System name, type of infection etc)of all clients on the console		
20.	Be able to be installed on Notebook Computers		
21.	Be able to schedule a scan and clean clients from the Management console.		
22.	The anti virus solution should have the phone home facility to enforce policy and licensing		

	check		
23	The solution must have lock down facility so that user can not change the real time settings		
24	The solution must have real time scanning, local scanning, Scheduled scanning		
25.	<p>The anti virus should use the following method to detect the computer virus</p> <p>Integrity Check: Examines the program's file size to see if it has increased, which may be indicative of a virus. This method is used primarily to check the integrity of the Critical Disk Area information.</p> <p>Interrupt Monitoring: Monitors all program system calls in an attempt to detect and thwart the sequence of system calls indicative of virus activity.</p> <p>Signature Scanning: Looks for a unique pattern, determined by the OEM, that serves as a sign that a given virus is present. With the knowledge of what to look for and where to look for it, Antivirus software automatically locates and deals with the virus.</p>		
26	The solution must have content update facility which includes latest version of signature files, scan engines, and program updates, and are available for all supported versions and platforms.		
27	The solution must provide the logs for real time scanning, local scanning, shell scanning, general events like signature updates		
28	Port Blocking - All the administrator/user to turn off(block) specified ports from either outbound or inbound traffic.		
29	Web Reputation- Protects against web-based malware, data theft.		
30	Virtual ditching- Protect endpoint against vulnerability exploits before patches are deployed.		

Anti spyware

1.	Must be able to totally protect from spyware, adware, Malware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents, in real time.		
2.	Must be able to support Interactive scan on demand.		
3.	Should have centralized management and reporting capabilities to deliver reports like top spyware, by category, by infected machines, by risk priority etc.		
4.	Real time Active protection on memory, process termination / file removal of pests in active memory.		
5.	Must be able to scan from the desktop according to preset or customized configurations.		
6.	Should have centralized update/download mechanism which should be able to download details of latest spyware and push the same across all the Desktops, Laptops.		
7.	The solution must be able to auto-quarantine or auto-delete spyware or Adware without end-user interaction.		
8.	The solution should have the pest exclusion policy by pest name, pest category and pest path		
9.	The anti spyware solution should have Content updates contain the latest version of signature files, scan engines, and program updates, and are available for all supported versions and platforms.		
Management Console			
1.	The management console should have dashboard which will give the information about product version, license version, signature update status, Viruses, spyware, infected PCs, per virus report, per pest report. The reports should be by user, by action, by branch, by subnet etc. The report should be daily, weekly, monthly and quarterly basis.		

2.	The user can have customized reports using any freeware database like Ingres or SQL Express		
3.	The management console can create the anti virus policy for real time, schedule scanning, signature distribution, send for analysis whenever you submit a virus to OEM for further analysis.		

Annexures

3.1 Annexure-1: Notice of Intent to Bid

Letter Dated Date/Month/Year

The Stores and Purchase Officer
CECRI
KARAIKUDI - 630006

Dear Sir,

RE: : Notice of Intent to Submit the Proposal

This is to notify you that our firm/company intends to submit a proposal in response to RFP No..... Primary and Secondary contacts for our firm / company are :

	Primary Contact	Secondary Contact
Name :		
Title :		
Company Name :		
Address :		
Phone :		
Fax :		
E-mail :		

Sincerely,
[BIDDER'S NAME]
Title
Signature
Date

3.2 Annexure-2: Proposal covering letter

Letter Dated Date/Month/Year

The Store and Purchase Officer
CECRI
KARAIKUDI - 630006

Dear Sir,

Re: Supply, Installation, Implementation, Support and Training of UTM System and Antivirus Solution CSIR-CECRI, Karaikudi

In response to the RFP for "**Supply, Installation, Implementation, Support and Training of UTM and Antivirus Solution for CSIR-CECRI, Karaikudi**" issued by the Stores and Purchase Officer, CSIR-CECRI, KARAIKUDI -630 006, we herewith submit our proposal. The following documents have been included as part of the proposal:

S.No	Enclosed documents
1.	Technical bid (sealed and marked)
2.	Commercial bid (sealed and marked)
3.	EMD amount in the form of DD as mentioned in section 1.4.1 of this RFP.
4.	Additional information if any

1. Having examined the tender Documents and Appendices thereto and Addenda Numbers Thereto we, the undersigned, offer to provide the said services, in conformity with the said Contract, Terms of Reference and Appendices thereto and Addenda for the sum indicated as per the attached Financial Proposal.

2. We acknowledge having received the following Addenda to the bid documents:

Addendum No.

Date

.....

.....

3. We undertake if our proposal is accepted to provide the services comprised in the contract within **7 days** of the receipt of notification of award from CSIR-CECRI
4. If our proposal is accepted we will obtain, within **15 days** of receipt of notification of award, the guarantee of a scheduled commercial bank to be jointly and severally bound with us in a form of Performance Guarantee.
5. We agree to execute the work in the form set out in the tender Documents with such alterations or additions thereto as may be necessary to adapt such agreement to the circumstances of this tender and notice of award within **15 days** after notification of your intention to accept this proposal
6. Unless and until a formal agreement is prepared and executed this proposal together with your written acceptance thereof shall constitute a binding contract between us and shall be deemed for all purposes to be the contract agreement.
7. We understand that you are not bound to accept the lowest or any bid you may receive, nor to give any reason for the rejection of any bid and that you will not defray any expenses incurred by us in bidding.

Dated this day of

Signature

In the capacity of

Duly authorised to sign bids for and on behalf of

(IN BLOCK CAPITALS)

Address:

.....

Witness:

.....

Address:

Occupation:

.....

Sincerely yours

(Signature) (In the capacity of)

Duly authorized to sign the Tender Response for an on behalf of :

(Name and address of Company) Seal/Stamp of bidder

Witness Signature :

Witness Name :

Witness Address :

CERTIFICATE AS TO AUTHORIZED SIGNATORIES

I, certify that I amof the, and that Who signed the above Bid is authorized to bind the corporation by authority of its governing body.

(.....)

Date

(Seal here)

3.3 Annexure-3: Technical Bid

Letter Dated Date/Month/Year

The Stores and Purchase Officer
CSIR-CECRI
KARAIKUDI - 630006

Dear Sir,

Sub:- Technical bid for Supply, Installation, Implementation, Support and Training of UTM and Antivirus

Having examined the tender document, the receipt of which is hereby duly acknowledged, we, the undersigned, offer _____.

To meet such requirements and provide such services as required are set out in the tender document, we attach hereto the tender technical response as required by the tender document, which constitutes our proposal.

If our proposal is accepted, we will obtain a performance bank guarantee in the format given in the tender document issued by a Scheduled Commercial Bank in India, acceptable to the CSIR-CECRI, KARAIKUDI, **for a sum of 10% of value of contract** for due performance of the contract. We agree for unconditional acceptance of all the terms and conditions set out in the tender document and also agree to abide by this tender response for a period of SIX (plus ONE) MONTHS from the date fixed for tender opening and it shall remain binding upon us with full force and virtue, until within this period a formal contract is prepared and executed, this tender response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and CSIR-CECRI, KARAIKUDI

We have read and understood the criteria spelt out for evaluating the technical bids as mentioned in this RFP. If the committee invites us to make a presentation in a date, time and location determined by The Stores and Purchase Officer, CSIR-CECRI, KARAIKUDI, we will be glad to be there and present the solution proposed by us and the key points of our proposal. During technical bid evaluation, if you find some parts of the proposal ambiguous and uncertain, you may seek oral clarifications.

We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to CSIR-CECRI, KARAIKUDI, is true, accurate, and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead CSIR-CECRI, KARAIKUDI, as to any material fact.

We agree that you are not bound to accept the lowest or any tender response you may receive. We also agree that you reserve the right in absolute sense to reject all or

any if the products/service specified in the tender response without assigning any reason whatsoever. It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of 2011

(Signature) (In the capacity of)

Duly authorized to sign the Tender Response for and on behalf of :

(Name and Address of Company) Seal/Stamp of bidder

Witness Signature :

Witness Name :

Witness Address :

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I, certify that I am of the, and that
who signed the above Bid is authorized to bind the corporation by authority of its governing body.

(.....)

Date

(Seal here)

3.4 Annexure -4: Technical Bid Format

I General Information

General Information			
Sno	Particulars	Details to be furnished	
A	Details of Prime Bidder (Company)		
	Name		
	Address		
	Telephone / Mobile	Fax	
	Email	Website	
	Details of Authorized person		
	Name		
	Address		
	Telephone / Mobile	Email	

II Information about the Company

Information about the Company	
ii) Does the firm/company should have been in operation for a period of at least 3 years as of 01.07.2011	Give Page no. Where proof is given
ii) Does the firm/company have provided attested copies of the valid? a. PAN No. b. Service Tax Registration No.	Give Page no. Where proof is given
iv) Does the Firm/Company have a branch within the proximity reach of Karaikudi.	Give Page no. Where proof is given
v) Does the Firm/Company have an experience of installing, implementing and support of UTM , Antivirus or cyber security related products in organizations like banks, financial institution, Insurance Companies or Government departments and any listed companies during the last 3 years?	Give Page no. Where proof is given
vi) Details of Technical manpower (Certified Network Security Personnel)	

III Financial Details as per Audited Balance Sheet

i) Does the firm/company have an average turnover of Rs.25,00,000/- (Twenty five Lakhs) annually during the last 3 financial years in selling security related products and solutions (Proof of this need to be attached) Give Page no	Year	Turnover in Rs.
	2008-09	
	2009-10	
	2010-11	
Total Turnover (the last three years in selling security related products and solutions): Give Page no. where proof is given		

IV. The bidder should give an OEM authorization letter particularly for this tender enquiry on OEM letter head.

V. The bidder should give unpriced bid mentioning the brand and model quoted for the tender document.

VI. An undertaking from the bidder that the OEM will provide 5 days free of cost certified training as per the components of training defined at Annexure 2.1.1.2.

VII. An undertaking from the bidders where the bidder agree to the Terms and Conditions mentioned in Technical proposal see 1.4.3 of RFP

VIII. The bidder is required to submit the compliance of the UTM being offered by them as per the detail list of "Specifications for Unified Threat Management System (UTM) mentioned in the section 2.1.1 (Table 1, Table 2, Table 3). The bidder is required to submit the technical specifications (brochures, leaflets etc. of the make / model of UTM) with regards to the make / model being offered by them. The page No. of Technical specifications submitted by the bidder should appear in the compliance sheet in the separate column.

IX. The bidder is required to submit the compliance of Antivirus Solution being offered by them as per the detail list of "Specifications for Antivirus" mentioned in the section 2.1.2.1. The bidder is required to submit the technical specifications (brochures, leaflets etc. of the Antivirus) with regards to the Antivirus solution being offered by them. The page No. of Technical specifications submitted by the bidder should appear in the compliance sheet in the separate column.

3.5 Annexure- 5: Bid Security/EMD Form

Whereas (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) (hereinafter called "the Bid").

KNOW ALL PEOPLE by these presents that WE (name of bank) of (name of country), having our registered office at (address of bank) (hereinafter called "the Bank"), are bound unto (name of Purchase) (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 its 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 its 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 and including forty five (90) days 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)

with date & seal

3.6 Annexure- 6: Proforma of Performance Bank Guarantee

To: _____ (Name of Purchaser) WHEREAS _____ (Name of Supplier) hereinafter called "the Supplier" has undertaken, in pursuance of Contract No.

_____ dated _____ 20_____ to supply _____ (Description of Goods and Services) hereinafter called "the order". **AND WHEREAS** it has been stipulated by you in the said order that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the order.

AND WHEREAS we have agreed to give the Supplier a Guarantee:

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total of _____(Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the order and without cavil or argument, any sum or sums within the limit of _____ (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the _____ day of _____ 20_____.

Signature and Seal of Guarantors

.....
.....
.....

Date .

Address:
.....

All correspondence with reference to this guarantee shall be made at the following address:

Annexure -7: Proforma For Price Bid

A:

S.No.	Details	Qty.	Company/Make and Model No	Rate Per Unit	Tax If Any	TOTAL
1	Price for the UTM with 3 years on site Hardware and software warranty	01				
2	Price for Antivirus Solution (License -750 Users)	750				
4	Price for Installation and Implementation/Commissioning of UTM System	01				
5	Price for installation of Antivirus Solution in Servers and clients	750				
6	Price for Support (1 Resident Engineer) for 1x3 years	01				
Total						

B :

S.No.	Details	Qty.	Company/Make and Model No	Rate Per Unit	Tax If Any	TOTAL
1	Price of extended (on site Hardware and software) Warranty for additional 2 Years after expiry of 3 years.	01				
2	Price for Support (1 Resident Engineer) for additional 2 Years after expiry of 3 Years.	01				
Total						

Grand Total (A+B) : Rs.....

* **Offer valid for 3 months from the date of opening of the tender.**

Signature of Authorized person with seal of firm

Date:

Seal
-----X-----

Name

STORES & PURCHASE OFFICER

