HLL Lifecare Limited
(A Government of India Enterprise)

Corporate and Registered Office,
HLL Bhavan, Poojappura,
Thiruvananthapuram– 695 012
Kerala, India.
Phone: 0471 – 2354949
Website: www.lifecarehll.com

Invitation for Bids

Supply and installation of Unified Threat Management (UTM) Box

Date	:	**15th November 2014**
IFB No.	:	**HLL/CHO/IT/UTM /2014/**

The schedule of the bid is given below.

Last date and time for receipt of bids	**: 15.00 Hrs on 01.12.2014**
Time and date of opening of Bids	**: 15.30 Hrs on 01.12.2014**

HLL/CHO/IT/UTM /2014/ Dated 15th November 2014

Dear Sir,

Sub: Supply and installation of Unified Threat Management (UTM) Box.

HLL Lifecare Limited, Thiruvananthapuram invites the competitive bids from the eligible bidders for the supply of **Unified Threat Management (UTM) Box** for our Corporate Head Office, HLL Bhavan, Poojappura, Thiruvananthapuram. The details are given in **Annexure-I.**

The terms and conditions of the bid are given below.

1. The respective bidder should have minimum two years' experience in supply , installation and maintenance of IT security devices like firewall, UTM etc for which the documentary proof viz.,copies of purchase orders/client certificates can be submitted along with the bid
2. The respective bidder should have service support centre at Thiruvananthapuram or in Kerala.
3. The respective bidder should be an authorized supplier for the quoted product for which Manufacturer Authorization Form is to be submitted along with the bid.
4. The prices should be quoted as per the format for price schedule enclosed as **Annexure – II.**
5. The prices quoted shall be valid for a period of 90 days from the date of opening of bids.
6. The exact details of all the quoted items should be mentioned with complete technical specifications supported with illustrative literatures / catalogues / brochures.
7. The items should be delivered within 4 weeks from the date of placement of order.
8. Penalty @ 0.50 % per week's delay subject to a maximum of 5 % is applicable for delayed delivery.
9. The bid shall be evaluated by taking the total amount quoted for all the items.
10. Necessary user manuals/CDs/DVDs/accessories/license documents are to be supplied along with the equipment.
11. The onsite warranty should be for the period of minimum Three (3) years from the date of installation. All the defective parts should be replaced at free of cost during the warranty period.

12. Bids should be clear in all respects and those with ambiguous clauses shall be rejected.
13. The supply order shall be placed on the lowest responsive bidder.
14. Payment will be released within 30 days from the date of successful supply, installation and acceptance by HLL. For claiming the payment, the following documents are to be submitted.
    a. Three copies of Invoice
    b. Delivery/Installation report duly signed by the concerned person of HLL and representatives of the supplier.
    c. Warranty certificate if any,
15. The bids should be submitted at the following address.

    Associate Vice President (IT)
    HLL Life care Limited
    Corporate and Registered Office,
    HLL Bhavan, Poojappura,
    Thiruvananthapuram – 695 012,
    Phone: 0471- 2354949.

16. Bids should be submitted on or before **15:00 Hrs on 01.12.2014** and the same **will be opened at 15.30 Hrs on the same day** at Corporate Head Office, Poojappura, Thiruvananthapuram in the presence of the representative of the bidder who chooses to attend. If the bid opening day is declared as holiday for HLL, the bid will be opened at the next working day of HLL.
17. Any bid received after the deadline will be rejected.
18. HLL Lifecare Limited reserves the right to accept or reject any or all of the bids without assigning any reason whatsoever.
19. The envelopes containing the bid shall bear the Bid Number with date and the words “DO NOT OPEN BEFORE ……..” (Here insert the time and date of bid opening).
20. No Email or fax bids will be accepted.
21. Any dispute arising out of the tender/bid document/ evaluation of bids/issue of purchase order shall be subject to the jurisdiction of the competent court at Thiruvananthapuram only.

Thanking you,

Yours faithfully,

Senior Manager (Hardware)

Annexure-I

	Specifications	Qty
GENERAL REQUIREMENTS	1. The Firewall should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc. 2. Appliance shall be rack mountable/Desktop Form factor 3. The platform must use a hardened OS. 4. Appliance should support for Active – Active connections. It should not depend upon any 3rd party alliance. 5. Licensing should be as per device and not user/IP based (should support unlimited users) 6. Firewall Architecture should be on multiple tiers (firewall module, logging & policy management server, and the GUI/ WebUI Console) 7. The firewall should be supplied with the support for RIP v2, OSPF & BGP routing protocols 8. The firewall should all the multicast traffic to pass through the firewall system 9. The firewall system should have a provision to handle the bandwidth management, if the same is required in future 10. The firewall system should have a provision of adding the SSL VPN functionality in future, if the same is required.	1
INTERFACE & CONNECTIVITY REQUIREMENT	1. The platform must be supplied with at least 8 nos. of 10/100/1000Mbps of fixed copper interfaces. 2. The platform should support VLAN tagging (IEEE 802.1q) 3. The firewall should support ISP link load sharing. 4. The firewall interfaces have to support the unnumbered IP address.	
TECHNICAL REQUIREMENTS:	1. Stateful Inspection Firewall 2. Integrated Multi site management 3. Built in storage capacity of 250GB minimum for storing logs. 4. Power Input of 100 – 230V (50-60Hz) 5. The box should be capable of upgrading to new versions/products in case a new feature is released by the OEM. 6. Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related 7. Encryption support of AES 128-256 bit, 3DES 56-168 bit. 8. Password, RADIUS, X.509, SecurID authentication methods 9. Integrated certificate authority (X.509) 10. Should support star & mesh topology for VPN usage 11. Should have an integrated IPS 12. Should support unlimited policies.	
PERFORMANCE REQUIREMENTS:	1. The Firewall must support at least 1000000 concurrent connections 2. The Firewall must support at least 25000 new sessions per second processing. 3. The Firewall should support upto 3000 Mbps of Firewall Throughput. 4. The product should support minimum combined UTM throughput of 500 Mbps	

	5. The appliance should support integrated IPS throughput of at least 700 Mbps. 6. The appliance should support Antivirus throughput of at least 950 Mbps	
FIREWALL LOGGING, STATISTICS AND REPORTING REQUIREMENTS:	1. The Firewall must provide at a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall 2. Support to log in detail all connections which are blocked 3. Support to log in detail all connections which go through the Firewall 4. Provision to report all successful connections inbound 5. Provision to report all successful connections outbound 6. Support to generate performance statistics on real-time basis 7. Capability to produce reports which measure usage	
FIREWALL FILTERING REQUIREMENTS:	1. The Firewall should also support the standard Layer 3 mode of configuration with Interface IP's. It should be possible to protect the firewall policies from being compromised. 2. The Firewall must provide state engine support for all common protocols 3. The Firewall must provide NAT functionality, including dynamic and static NAT translations 4. The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type 5. The Firewall should be able to filter traffic even if the packets are fragmented. 6. The Firewall should support authentication protocols like LDAP, RADIUS and have support for firewall passwords, smart cards, & token-based products like SecurID, LDAP-stored passwords, RADIUS Servers and X.509 digital certificates. 7. The Firewall should provide advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications 8. Support for Filtering TCP based applications 9. Should support CLI & GUI based access to the firewall modules 10. Local access to firewall modules should support role based access 11. Local access to the firewall modules should support authentication protocols – RADIUS. 12. Integrated IPS should support hybrid attack detection/prevention with multiple attack protections methods, like Protocol Anomaly, Signature-Based, Day-Zero Protection, etc 13. Integrated IPS should protect setup against vulnerabilities in the applications of the protected systems by carrying out deep packet inspection	
INTRUSION PREVENTION	1. Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related 2. Blocks attacks such as DNS cache poisoning, FTP bounce,	

SYSTEM.	improper commands 3. Signature-based, behavioural, and protocol anomaly 4. IPS should be a integrated system with firewall 5. IPS should have option to configure country based blocking 6. IPS should be able to prevent evasion mechanisms 7. IPS must have the ability to add signature exceptions via Console(Not CLI) 8. Separate logs for IPS is required which can be analyzed from the console. Separate logs for other components like FW, VPN, Applications etc are also required from the console	
ADMINISTRATION/ MANAGEMENT REQUIREMENTS:	1. Any changes or commands issued by an authenticated user should be logged to a database. 2. The Firewall must send SNMP traps to Network Management Servers (NMS) in response to System failures. 3. Provision to generate automatic mail alerts 4. The Firewall must not support any non-secure means of access to the Firewall. 5. Support for role based administration of firewall	
USER AUTHENTICATION REQUIREMENTS:	1. Support for user authentication at the firewall system for the different TCP/IP applications, like HTTP, SMTP, Telnet & RSH. 2. Support for integration with the RSA Secure ID as the strong user authentication mode	
USER IDENTITY	1. Should have integrated Identity Control 2. Should Support User based Policies 3. Should support User, Machine awareness 4. Time based polices 5. Should support Clientless and agent less authentication 6. Should have Captive portal authentication 7. Identity agent based authentication. 8. Application based logs 9. User based logs 10. Should support bandwidth allocation based on applications 11. Should not use any agents to be installed for AD/LDAP query	

Annexure-II

Sl.NO	Description of item / work	Unit	Qty	Basic Price (Rs)	Taxes/ Duties (Rs)	Other incidental costs if any (Rs)	Total Price for each unit (Rs)	Amount (Rs)
1	**2**	**3**	**4**	**5**	**6**	**7**	**8= 5+6+7**	**9= 4 * 8**

Total Price (in Figure) : Rs……

Total Price (in words) : Rs. ……..