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
CIN: U25193KL1966GOI002621

Invitation for Bids

Supply and installation of Unified Threat Management (UTM) Boxes under Buyback Scheme.

Date	:	**15.06.2015**
IFB No.	:	**HLL/CHO/IT/UTM /2015/**

The schedule of the bid is given below.

Last date and time for receipt of bids	**: 24.06.2015 at 15:00 Hrs**
Time and date of opening of Bids	**: 24.06.2015 at 15:30 Hrs**

HLL/CHO/IT/UTM /2015/ Dated 15th June 2015

Dear Sir,

Sub: Supply and Installation of Unified Threat Management (UTM) Boxes under Buyback Scheme

HLL Lifecare Limited, Thiruvananthapuram invites the competitive bids from the eligible bidders for the supply and installation of **Unified Threat Management (UTM) Boxes (4 Nos)** for our Corporate Head Office, HLL Bhavan, Poojappura, Thiruvananthapuram under buyback scheme. The details of the new requirement are given in **Annexure- 1** and the details of old items are given in **Annexure-2.**

The terms and conditions of the bid are given below.

1. The respective bidder should have a minimum of 2 years experience in the supply and installation of UTMs, for which the documentary proof like copies of purchase orders/client certificates can be submitted along with the bid.
2. The OEM should have service support centre in South India.
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 (For new items and old items separately) as per the format for price schedule enclosed as **Annexure – 3**
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 **3 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 bids will be evaluated on the basis of the total price of all the items quoted. The total price of the items is calculated as follows.

   Total Price = Total price of the new items – Total price of the used items.
10. Necessary user manuals/CDs/DVDs/accessories/license documents are to be supplied along with the equipment.
11. The onsite warranty and subscription package of the device should be for the period of minimum **Three (3)** years from the date of installation. All the defective parts should be replaced and all subscription related issues should be addressed during the warranty period at free of cost.

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. The OEM should have 24x7 toll free maintenance support.

15. All breakdown calls should be attended within 3 hours of intimation.

16. Successful bidder has to arrange their own transport to shift the used items to their site/office after the supply of new items.

17. 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,

18. 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.

19. Bids should be submitted on or before **15:00 Hrs on 24.06.2015** and the same **will be opened at 15.30 Hrs on the same day** at Corporate Head Office, Poojappura, and 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.

20. Any bid received after the deadline will be rejected.

21. HLL Lifecare Limited reserves the right to accept or reject any or all of the bids without assigning any reason whatsoever.

22. 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).

23. No Email or fax bids will be accepted.

24. 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,

Manager (IT)

Annexure-1

UTM Boxes (for IT Applications) – 2 Nos.

	SPECIFICATIONS	Qty
GENERAL REQUIREMENTS	1. The Firewall should support "Stateful" packet inspection technology& should be ICSA & Common criteria EAL4+ Certified. 2. Appliance should be Rack Mountable. 3. The platform must use a hardened OS. 4. The proposed device should support High Availability Active/Passive and Active/Active. 5. Licensing should be as per device and not user/IP based (should support unlimited users). 6. Firewall Architecture should be on Multicore parallel processing. 7. The firewall should be supplied with the support for RIP v2, OSPF & BGP routing protocols 8. All the multicast traffic to pass through the firewall. 9. The firewall system should bandwidth management. 10. The firewall system should have SSL VPN functionality. 11. The device should support for user authentication at the firewall system for all TCP/IP applications 12. Proposed solution should have Integrated Web filter, Application control, gateway Antivirus, IPS, Antispam & Web-application. 13. Proposed Solution should have IPv6 certification. 14. Proposed Solution should block attacks such as DoS, port scanning, IP/ICMP/TCP-related. 15. Proposed Solution should have Encryption support of AES 128-256 bit, 3DES 56-168 bit. 16. Proposed Solution should have Password, RADIUS, X.509, SecurID authentication methods.	**2 Nos**
INTERFACE & CONNECTIVITY REQUIREMENTS	1. The platform must be supplied with at least 8 Nos. of 10/100/1000Mbps fixed copper interfaces. 2. The platform should support VLAN tagging (IEEE 802.1q) 3. The device should support Outbound Load Balancing and Failover among a minimum of 3 ISP Links.	
PERFORMANCE REQUIREMENTS	1. The Product must support at least 60,00,000 concurrent connections. 2. The Product must support at least 1, 30,000 new sessions per second processing. 3. The Product should support a minimum of 25,000 Mbps Firewall Throughput. 4. The product should support minimum IPS throughput of 7000 Mbps. 5. The Product should support Antivirus throughput of minimum 2000 Mbps.	
FIREWALL LOGGING, AND REPORTING REQUIREMENTS	1. The proposed UTM must have On-Appliance, integrated reporting solution with minimum 200GBHard drive. 2. The proposed UTM should allow customization of reports 3. The proposed UTM should allow exporting of reports in PDF and Excel format. 4. The proposed UTM should provide detailed reports for all files uploaded via HTTP or HTTPS protocol. The report should include username/IP address/URL/File name/Date and Time. 5. The proposed UTM should provide data transfer reports on the	

	basis of application, username, IP address. 6. The proposed UTM should facilitate sending of reports on email address. 7. The proposed UTM should support Auditing facility to track all activity carried out on the appliance. 8. The proposed UTM should be capable of forensic analysis to help organizations reconstruct the sequence of events that occurred at the time of security breach. 9. The proposed UTM should have customizable email alerts/automated Report scheduling. 10. The proposed UTM should provide reports for all blocked attempts by users/IP address.	
FIREWALL 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 NAT functionality, including dynamic and static NAT translations. 3. The Firewall must provide filtering capability that includes parameters like identity, source addresses, destination addresses, source and destination port numbers, protocol type etc. 4. The Firewall should be able to filter traffic even if the packets are fragmented. 5. The Firewall should support authentication protocols like LDAP, RADIUS, Microsoft AD etc 6. The Firewall should provide advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications 7. Support for Filtering TCP based applications 8. Should support CLI & GUI based access to the firewall modules 9. Local access to firewall modules should support role based access. 10. The proposed UTM should support user-defined multi-zone security architecture. 11. Solution should support country based blocking.	
INTRUSION PREVENTION SYSTEM	1. The proposed UTM should have signature-based and protocol-anomaly-based Intrusion Prevention System. 2. IPS must have the ability to add Custom signatures via GUI. 3. Separate logs for IPS is required which can be analysed from the console. 4. IPS should be integrated system with firewall.	

WEB FILTERING&APPLICATION CONTROL	1. Proposed UTM should have category based Web filtering Solution as well as an Application control database of 2000 or more Signatures. 2. The proposed Web filter solution should be able to block HTTPS based URLs, URL based on regular expression, URL translation request and any HTTP / HTTPS upload traffic. 3. The proposed solution must identify (Allow/Block/Log) the applications regardless of port, protocols, encryption including SSL/TLS. 4. The proposed UTM must be capable of blocking the Applications that allow file transfer, Online Games, Instant Messengers (Including Non-English Versions), Peer-to-Peer (P2P) applications (Including Non-English Versions), Browser Based Proxy (Regardless of IP address or Port Number), 5. Web 2.0 based applications (Facebook, CRM etc), Applications that provide Remote Control, All type of streaming media (Both Web and Software Based), VOIP Applications, HTTPS based Micro-Apps like Facebook chat, YouTube video upload etc.	
BANDWIDTH MANAGEMENT	1. Proposed UTM should support traffic shaping User-Identity & Application based. 2. Proposed UTM should support to assign bandwidth Guaranteed as well as burstable/threshold. 3. Proposed UTM should support for Control of Bandwidth assigned to Web-Categories based on Business relevance or web category based traffic management. 4. Proposed UTM report Bandwidth utilization happening over ISPs.	
GATEWAY ANTIVIRUS	1. Gateway Antivirus solution should be ICSA labs or West coast Labs Checkmark certified. 2. Solution should support AV scanning for SMTP, SMTPS, POP3, IMAP, HTTP, HTTPS & FTP protocol. 3. For SMTP &SMTPS traffic, the proposed UTM 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 administrator 4. The proposed UTM should support multiple anti-virus policies based on sender/recipient email address or address group, notification setting, quarantine setting and file extension setting. 5. The proposed UTM should update the signature database at a frequency of less than one hour and it should also support manual update. 6. For POP3 and IMAP traffic, the proposed UTM should strip the virus infected attachment and then notify the recipient and administrator. 7. The proposed UTM should scan http traffic based on username, source/destination IP address or URL based regular expression. 8. The proposed UTM should provide the option to bypass scanning for specific HTTP traffic.	
GATEWAY ANTISPAM	1. The proposed UTM should have ICSA Certification or West coast Labs Checkmark certified for Anti-Spam. 2. The proposed UTM should support spam scanning for SMTP, POP3, and IMAP.	

	3. The proposed UTM must allow mail archiving to store copies of incoming and outgoing mails from particular email address(s). 4. The proposed UTM should support multiple configurable policies based on email ID/address group, for quarantine setting, etc. 5. The proposed UTM must support on-appliance quarantine facility 6. The proposed UTM should support language independent spam detection. 7. The proposed UTM should block image based spam mails i.e. email message with text embedded in an image file.	

UTM Boxes (for Web Applications) – 2 Nos.

	SPECIFICATIONS	Qty
GENERAL REQUIREMENTS	1. The Firewall should support "Stateful" packet inspection technology& should be ICSA & Common criteria EAL4+ Certified. 2. Appliance should be Rack mountable 3. The platform must use a hardened OS. 4. The proposed device should support High Availability Active/Passive and Active/Active. 5. Licensing should be as per device and not user/IP based (should support unlimited users). 6. Firewall Architecture should be on Multicore parallel processing. 7. The firewall should be supplied with the support for RIP v2, OSPF & BGP routing protocols 8. All the multicast traffic to pass through the firewall. 9. The firewall system should have bandwidth management. 10. The firewall system should have SSL VPN functionality. 11. The device should support for user authentication at the firewall system for all TCP/IP applications 12. .Proposed solution should Integrated Web filter, Application control, gateway Antivirus, IPS, Antispam & Web-application. 13. Proposed Solution should have IPv6 certification. 14. Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related 15. Encryption support of AES 128-256 bit, 3DES 56-168 bit. 16. Password, RADIUS, X.509, SecurID authentication methods.	**2 Nos**
INTERFACE & CONNECTIVITY REQUIREMENTS	1. The platform must be supplied with at least 8 Nos. of 10/100/1000Mbps fixed copper interfaces. 2. The platform should support VLAN tagging (IEEE 802.1q) 3. The device should support Outbound Load Balancing and Failover among a minimum of 3 ISP Links.	
PERFORMANCE REQUIREMENTS	1. The Product must support at least 9,00,000 concurrent connections 2. The Product must support at least 30,000 new sessions per second processing. 3. The Product should support a minimum of 6,000 Mbps Firewall Throughput. 4. The product should support minimum IPS throughput of 1500 Mbps	

	5. The Product should support Antivirus throughput of minimum 500 Mbps.	
FIREWALL LOGGING AND REPORTING REQUIREMENTS	1. The proposed UTM must have On-Appliance, integrated reporting solution with minimum 200GBHard Drive. 2. The proposed UTM should allow customization of reports 3. The proposed UTM should allow exporting of reports in PDF and Excel format. 4. The proposed UTM should provide detailed reports for all files uploaded via HTTP or HTTPS protocol. The report should include username/IP address/URL/File name/Date and Time. 5. The proposed UTM should provide data transfer reports on the basis of application, username, IP address. 6. The proposed UTM should facilitate sending of reports on email address. 7. The proposed UTM should support Auditing facility to track all activity carried out on the appliance. 8. The proposed UTM should be capable of forensic analysis to help organizations reconstruct the sequence of events that occurred at the time of security breach. 9. The proposed UTM should have customizable email alerts/automated Report scheduling. 10. The proposed UTM should provide reports for all blocked attempts by users/IP address.	
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 NAT functionality, including dynamic and static NAT translations. 3. The Firewall must provide filtering capability that includes parameters like identity, source addresses, destination addresses, source and destination port numbers, protocol type etc. 4. The Firewall should be able to filter traffic even if the packets are fragmented. 5. The Firewall should support authentication protocols like LDAP, RADIUS, Microsoft AD etc. 6. The Firewall should provide advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications 7. Support for Filtering TCP based applications 8. Should support CLI & GUI based access to the firewall modules 9. Local access to firewall modules should support role based access. 10. The proposed UTM should support user-defined multi-zone security architecture. 11. Solution should support country based blocking.	
INTRUSION PREVENTION SYSTEM	1. The proposed UTM should have signature-based and protocol-anomaly-based Intrusion Prevention System. 2. IPS must have the ability to add Custom signatures via GUI. 3. Separate logs for IPS is required which can be analysed	

	from the console. 4. IPS should be integrated with firewall.	
WEB FILTERING&APPLICATION CONTROL	1. Proposed UTM should have category based Web filtering Solution as well as an Application control database of 2000 or more Signatures. 2. The proposed Web filter solution should be able to block HTTPS based URLs, URL based on regular expression, URL translation request and any HTTP / HTTPS upload traffic. 3. The proposed solution must identify (Allow/Block/Log) the applications regardless of port, protocols, encryption including SSL/TLS. 4. The proposed UTM must be capable of blocking the Applications that allow file transfer, Online Games, Instant Messengers (Including Non-English Versions), Peer-to-Peer (P2P) applications (Including Non-English Versions), Browser Based Proxy (Regardless of IP address or Port Number), 5. Web 2.0 based applications (Facebook, CRM etc), Applications that provide Remote Control, All type of streaming media (Both Web and Software Based), VOIP Applications, HTTPS based Micro-Apps like Facebook chat, YouTube video upload etc.	
BANDWIDTH - MANAGEMENT	1. Proposed UTM should support traffic shaping User-Identity & Application based. 2. Proposed UTM should support to assign bandwidth Guaranteed as well as burstable/threshold. 3. Proposed UTM should support for Control of Bandwidth assigned to Web-Categories based on Business relevance or web category based traffic management. 4. Proposed UTM report Bandwidth utilization happening over ISPs.	
GATEWAY ANTIVIRUS	1. Gateway Antivirus solution should be ICSA Labs or West coast Labs Checkmark certified. 2. Solution should support AV scanning for SMTP, SMTPS, POP3, IMAP, HTTP, HTTPS & FTP protocol. 3. For SMTP &SMTPS traffic, the proposed UTM should support following actions for infected, suspicious or protected attachments mails. e. Drop mail f. Deliver the mail without attachment g. Deliver original mail h. Notify administrator 4. The proposed UTM should support multiple antivirus policies based on sender/recipient email address or address group, notification setting, quarantine setting and file extension setting. 5. The proposed UTM should update the signature database at a frequency of less than one hour and it should also support manual update. 6. For POP3 and IMAP traffic, the proposed UTM should strip the virus infected attachment and then notify the recipient	

	and administrator. 7. The proposed UTM should scan http traffic based on username, source/destination IP address or URL based regular expression. 8. The proposed UTM should provide the option to bypass scanning for specific HTTP traffic.	
GATEWAY ANTISPAM	1. The proposed UTM should have ICSA Certification or West coast Labs Checkmark certified for Anti-Spam. 2. The proposed UTM should support spam scanning for SMTP, POP3, and IMAP. 3. The proposed UTM must allow mail archiving to store copies of incoming and outgoing mails from particular email address(s). 4. The proposed UTM should support multiple configurable policies based on email ID/address group, for quarantine setting, etc. 5. The proposed UTM must support on-appliance quarantine facility 6. The proposed UTM should support language independent spam detection. 7. The proposed UTM should block image based spam mails i.e. email message with text embedded in an image file.	

Annexure 2

Sl.No	Item Description	Qty
1	Watchguard XTM 1050 UTM	2 Nos
2	Checkpoint T110 UTM	1 No.

Annexure-3

Sl.NO	Description ofitem / work	Unit	Qty	Basic Price(Rs)	Taxes/ Duties (Rs)	Other incidental costsif 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…….