UNIVERSITY OF CALICUT
CALICUT UNIVERSITY INSTITUTE OF ENGINEERING AND TECHNOLOGY

No:32608/CUIET-A-ASST-1/2013/CU Date:03.09.2015

TENDER NOTICE

Tenders are invited for the purchase of UTM Firewall to Calicut University Institute of Engineering and Technology, Kohinoor, with the following hardware & software specifications:

A) General Requirements

The Prodcut should be ISO cerified.
The Firewall should support "Stateful" packet inspection technology& should be ICSA & Common criteria EAL4+ Certified.
Appliance should be Rack Mountable.
The platform must use a hardened OS.
The proposed device should support High Availability Active/Passive and Active/Active.
Licensing should be as per device and not user/IP based (should support unlimited users).
Firewall Architecture should be on Multicore parallel processing.
The firewall should be supplied with the support for RIP v2, OSPF & BGP routing protocols
All the multicast traffic to pass through the firewall.
The firewall system should bandwidth management.
The firewall system should have SSL VPN functionality.
The device should support for user authentication at the firewallsystem for all TCP/IP applications .
Proposed solution should have Integrated Web filter, Application control, gateway Antivirus, IPS, Bandwidth Managemet .
Proposed Solution should support future integrations of Web-application firewall with out HW change .
Proposed Solution should have IPv6 ready Gold Logo Certification.
Proposed Solution should block attacks such as DoS, port scanning, IP/ICMP/TCP-related.
Proposed Solution should support On-appliance reporting with minimum 250 Gb drive or Shall be external hardware solution supporting the same.

B) INTERFACE &CONNECTIVITY REQUIREMENTS

The platform must be supplied with at least 10 Nos. of 10/100/1000Mbps fixed copper interfaces.
The platform should support VLAN tagging (IEEE 802.1q)
The device should support Outbound ISP Loadbalancing & failover among minimum 3 ISP as well as Inbound DNS based loadbalancing .

C) PERFORMANCE REQUIREMENTS

The Product must support at least 30,00,000 concurrent connections
The Product must support at least 85,000 new sessions per second processing.

The Product should support a minimum of 10,000 Mbps Firewall Throughput.
The product should support minimum IPS throughput of 3000 Mbps.
The Product should support Antivirus throughput of minimum 2500 Mbps.

D) FIREWALLLOGGING, AND REPORTING REQUIREMENTS

The proposed UTM must have On-Appliance, integrated reporting solution with minimum 250GBHard drive or External hardware based solution supporting the same.
The proposed UTM should allow customization of reports.
The proposed UTM should allow exporting of reports in PDF and Excel format.
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.
The proposed UTM should provide data transfer reports on the basis of application, username, IP address.
The proposed UTM should facilitate sending of reports on email address.
The proposed UTM should support Auditing facility to track all activity carried out on the appliance.
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.
The proposed UTM should have customizable email alerts/automated Report scheduling .
The proposed UTM should provide reports for all blocked attempts by users/IP address.

E) 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.

F) INTRUSION PREVENTION SYSTEM

The proposed UTM should have signature-based and protocolanomaly- based Intrusion Prevention System.
IPS must have the ability to add Custom signatures via GUI.
Proposed solution should be either ICSA labs or Westcoast labs checkmark certified with a minimum of 4000 +signatures.
Separate logs for IPS is required which can be analysed from the console.
IPS should be integrated system with firewall.

G) WEB FILTERING&APPLICATION CONTROL

Proposed UTM should have category based Web filtering Solution with 85+web-categories as well as an Application control database of 2000 or more Signatures.

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.

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

H) BANDWIDTH MANAGEMENT

Proposed UTM should support traffic shaping User-Identity & Application based.

Proposed UTM should support to assign bandwidth Guaranteed as well as burstable/threshold .

Proposed UTM should support for Control of Bandwidth assigned to Web-Categories based on Business relevance or web category based traffic management .

Proposed UTM report Bandwidth utilization happening over ISPs.

I) 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,

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.

9.Solution Should support future integration of Web Application firewall protection without HW change with

minimum of 1000 Mbps WAF throughput as well as minimum2000 HTTP request per second.

10.The proposed solution should support protocol like HTTP/0.9/1.0/1.1 &XML.

11.The proposed solution should support below-

a) Cookie Protections Measures
b) Session Attacks Mitigation
c) Cryptographic URL and Parameter Protection
d) Strict Request Flow Enforcement
e) HTTPS (SSL) encryption offloading
f)Banner-grabbing Protection
g) Hidden field manipulation Protection
h) SQL injection Protection
i) OS command injection Protection
j) Cross-site scripting Protection (XSS)
k) Dangling pointer Protection
l)Stealth commanding Protection
m) Buffer overrun Protection
n) URL Hardening engine
o)Form field meta data validation
p) Directory traversal prevention
q) Response control
r) Outbound data theft Protection
s) Protocol limit checks

J) Should be quoted with 3 year Subscription & 24 * 7 support (License)

Tender forms can be downloaded from the University website www.universityofcalicut.info.

Cost of Tender form : 0.2% of the cost of tender rounded to the nearest multiple of 100 subject to a minimum of Rs.400/- and a maximum of Rs.1,500/-+VAT@5%).

EMD : 1% of the quoted rate subject to a minimum of Rs.1,500/- drawn in favour of the Finance Officer,University of Calicut.

Sealed and superscribed tenders should reach the undersigned on or before 19/09/2015.

Dr. Rahmathunza I.
Principal