

GOVT. POLYTECHNIC, MUMBAI

49, ALI YAVAR JUNG MARG; KHERWADI; BANDRA(EAST); MUMBAI- 400 051.
TELEPHONE NO. 26474780; 26474580

=====

No:- GPM/STORE/TEQIP/COMP/U.T.M.Appliance./2007-08/ 2751 Date:11.12.2007

QUOTATION (E-5)

To.
M/s.

Dear Sirs,

Sub: INVITING OF QUOTATIONS FOR UNIFIED THREAT MANAGEMENT
APPLIANCE FOR COMPUTER DEPT.

With reference to above, you are informed that the Govt. of India has received a credit from the International Development Association (IDA) in various currencies equivalent to U\$\$ 25oMillions towards the cost of TEQIP Project and intends to apply part of the proceeds of this credit to eligible payments under the contract for which this supply order is issued. Kindly arrange to send the goods, as per specifications in the enclosed Annexure, to this Institute on terms and conditions given as follows.

TERMS AND CONDITIONS

- 1) **PRICES** :- Rates are for free of cost delivery to the site of the consignee and inclusive of all taxes except octroi charges. Octroi exemption certificate should be obtained from this institute well in advance wherever applicable. If taxes applicable it should be quoted separately.
- 2) **INSPECTION** :- Inspection by this institute at consignee's site only. The entire materials ordered will have to be offered for inspection & free satisfactory trial in open conditions as demanded and will be rejected if it is not as per specifications and is not received in good conditions. 100% Payment will be released by the undersigned only after delivered the goods a) as per specifications, b) installation, c) free working trial d) free training to staff and against submission of bank guarantee.
- 3) **DELIVERY** :- The Goods should be supplied in good working conditions on or before **30 Days** from the date of issue order. You will be liable for action as per "failure & termination" clause which reads as follows:
" If the supplier fails to deliver the goods or any installment thereof within the period fixed for such delivery in the contracts or as extended or at time repudiates the contracts before the expiry of such period, the purchaser may without prejudice to his other rights:
a) Recover from the supplier as agreed liquidated damages and not by way of penalty a sum equivalent to 2% of the price of the any goods (including taxes, duties, freight etc) which the supplier has failed to deliver within the period fixed

for delivery in the contract or as extended for each month or part of month during which he delivery of such goods may be in arrears where delivery thereof is accepted after expiry of the aforesaid period OR

- b) Cancel the contracts or a portion thereof and it so desired, purchase or authorize the purchase of Goods not so delivered or others of a similar description (where goods exactly complying with particulars are not in the opinion of the purchaser, which shall be final, readily procurable) at the risk and cost of the supplier. It shall however, be in the discretion of the Purchaser to obtain or not the Performance Guarantee Bond from the firm/firms on whom the contract is placed at the risk and expense of the defaulting firm.

Where action is taken under sub-clause (b) above, the Supplier shall be liable for any loss which the Purchase may sustain on that account provided the purchase , or if there is an agreement to purchase such agreement is made, in case of failure to deliver the goods within the period fixed for such delivery in the contract or as extended, within nine month from the date such failure and in case of repudiation of the contract before the expiry of the aforesaid period of delivery within nine months from the date of cancellation of the contract. The supplier shall not be entitled to any gain on such purchase and the manner and method of such purchase shall be in entire discretion of the Purchaser. It shall not be necessary for the purchaser to serve a notice of such purchase on the supplier.

- 4) **SECURITY DEPOSIT** :- Bank guarantee @ 5 % of the total cost is required to be submit to this office as a security deposit within 15 days from the date of issued this supply order. This deposit is liable to be forfeited to Government of Maharashtra in, event of non- fulfillment of the terms and conditions on which this order will be issued.. Warranty clause conditions is also applicable to security deposit. No supply should be initiated without submission of security deposit.
- 5) **BILL** :- Bill for the goods to be supplied in compliance of this contract must be prepared in triplicate and send to this office for payment. Government shall not incur any liability to pay interest on bill the payment of which is delayed for any reason whatsoever.
- 6) **CERTIFICATE** :- Bill should incorporate therein the certificate regarding Sales tax, VAT taxes etc. under “ Certificate that the goods on which tax under the central Sales Tax Act 1956, has been charged/ have been exempted, under the said acts of rule made there under, and that in the case of supplies against contracts the relevant contracts includes a specific provisions that the amount is payable to Govt. by the supplier in respect of the supplies.
- 7) On-site **warranty for Three years period** from the date of installation.
- 8) Installation , Commissioning and Training are the responsibilities of the supplier and shall be at supplier’s cost, unless stated specifically.
- 9) The supplier should be authorized dealer of supplying brand mentioned in the specifications should have **turn over not less than Rs.2 Cr.(Rs. Two Cores)of each**, last three years. For verification vendors should submit certified audit report

and Sales Tax clearance certificate of last three years. The quotations will be invalid if documents not attached.

10) Evaluation of Quotations

The Purchaser will evaluate and compare the quotations determined to be substantially responsive i.e. which

- a) are properly signed ; and
- b) conform to the terms and conditions, and specifications.
- c) Evaluation will be with respect to base price

The Quotations will be evaluated for EACH SCHEDULE ONLY. All items in Schedule should be quoted.

11) Award of contract

The Purchaser will award the supply order to the supplier whose quotation has been determined to be substantially responsive and who has offered the lowest evaluated quotation price.

11.1 Notwithstanding the above, the Purchaser reserves the right to accept or reject any quotations and to cancel the procurement process and reject all quotations at any time prior to the award of contract.

11.2 The supplier whose offer is accepted will be notified of the award of contract by the Purchaser prior to expiration of the quotation validity period. The terms of the accepted offer shall be incorporated in the purchase order.

12) The supply shall be for all the items as described above. Corrections, if any, shall be made by crossing out, initialing, dating and re writing.

The rates quoted by the supplier/dealer shall be fixed for the duration of the contract and shall not be subject to adjustment on any account. The Prices should be quoted in Indian Rupees only Each Supplier/Dealer shall submit only one quotation.

13) Validity of Quotation

Quotation shall remain valid for a period not less than 45 days after the deadline date specified for submission.

14) Any disputable matters are entertained at jurisdiction of this office only

15) **The quotation should be submit on or before 26.12.2007(up to 4p.m.) only. Postal delay will not be condone. Quotation last date is extended from 26.12.2007 (up to 4 p.m.) to 10.1.2008 (up to 4p.m.)**

PRINCIPAL

STORE KEEPER

STORE OFFICER

PROCUREMENT
OFFICER

ANNEXURE

01	<p>Unified threat management appliance specification.</p> <p>1.1 General</p> <p>1.1.1 Device should have identity based firewall, VPN, anti-virus, anti-spam,intrusion detection & prevention, content filtering, bandwidth management & multi-link manager.</p> <p>1.1.2 Device should support DHCP, Wi-Fi & Roaming Users</p> <p>1.1.3 4 number of Ethernet ports</p> <p>1.1.4 Configurable LAN/WAN/DMZ ports</p> <p>1.1.5 Remote connectivity over the internet through PPTP,L2TP ,IPSec VPN</p> <p>1.1.6 Prevents dos & flooding attacks from internal & extrnal sources</p> <p>1.1.7 Scans incoming &outgoingHTTP,FTP ,IMAP,pop3 & smtp traffic</p> <p>1.1.8 Product should be installed in at least 15 universities in india</p> <p>1.1.9 Product should be CIPA compliant</p> <p>1.1.10 All specifications mentioned herewith should be avialible on a single appliance.</p> <p>1.2 Appliance requirements</p> <p>1.2.1 The proposed system should be capable of supporting: A) 4 numbers of 100 mbps Ethernet ports. B) Should comply FCC and CE norms.</p> <p>1.3 Administration,Authentication & Configuration</p> <p>1.3.1 User Data & Policies export & import facility in CSV Format</p> <p>1.3.2 User Authentication with Windows NTLM Databse, LDAP, & Active Directory & in built databse of the appliance</p> <p>1.3.3 Single Sign-on Integration with Windows Authentication</p> <p>1.3.4 Bandwidth Utilization Graphs (like MRTG) of Multiple ISP Links on Day, Month, Week, Yearly basis</p> <p>1.3.5 Message Broadcasting to Individual Logged in Users via Web Based or through Login client software</p> <p>1.3.6 Network admin must be able to view amount of upload & Download Data transfer done by each user separately in real time basis</p> <p>1.3.7 Network admin must be able to view bandwidth consumed by each individual user in the network in real time basis</p> <p>1.3.8 System should be provide real time traffic reports by Application wise & user wise</p> <p>1.3.9 Web-based & Secure console based remote administration</p> <p>1.4 Identity based Policy Controls</p> <p>1.4.1 Surfing Policy Quota *Facility to create Weekly Cyclic quota of limited period of internet surfing based on Individual usernames & groups *Surfing policies can be allocated on shared basis between group of users individual user wise *Surfing policies based on combination of Hours & Validity in term of Day, Week, Month & Yearly (ex:8 Hours of Daily surfing valid</p>	01
----	--	----

	<p>till 1 Year) *Policies based on time quota (ex:100 Hours,200 Hours) should be possible based on Individual Users & Groups</p> <p>1.4.2 Access Time Policy Quota *Policies to control Internet access time for users & groups should be available based on time & days of 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> <p>1.4.3 DataTransfer Policy Quota *Facility to allocated Data transfer Quota (1 GB, 2 GB, 100 MB etc) to individual user policies or group policies based on User Identity *Should provide feature to create separate upload and download based policies for Daily, Weekly, Yearly Quota on user & group basis (ex. 1 GB Upload & 1 Gb Download of Data transfer allowed every Month & Year) *Data transfer Quota should also be allocated on shared basis on users</p> <p>1.5 Firewall Requirement</p> <p>1.5.1 The firewall should be dedicated standalone appliance</p> <p>1.5.2 Firewall rules can be created based on usernames & not on Hosts/Subnets (eg .rule can be created in the name of network admin)like john, harry) to allow certain privilege access sucj as ftp,ssh without need of providing hostnames,IP or Subnets)</p> <p>1.5.3 The firewall should have stateful packet filtering technology & must support one –to-one & dynamic user based NAT with an facility to create rules based on usernames, Source & Destination Ip address, Hosts,network,Ip Range.</p> <p>1.5.4 The firewall should be based on a hardened Os, which is capable of delivering network protection services at all layers along with options of network gateway level anti virus, anti spam, intrusion detection & prevention, content filtering, multiplr ISP load balancing & failover solutions.</p> <p>1.5.5 The firewall should support transparent mode/Bridge mode for Seamless deployment into an existing network without changing IP configuration in the network.</p> <p>1.5.6 The firewall should provide multi-zone security architecture as follows: *User assignable zones on different physical interfaces *Differnt IDP Policies between different zones *AntiVirus, AntiSpam,IDP, Web filter different zones.</p> <p>1.5.7 The firewall should at least provide the following system performance: *Concurrent session: 370000 *New sessions: 4000 *Firewall throughout at least 200mbps</p> <p>1.5.8. Provide Pre-defined services based on port numbers & Layer 7 application signatures & ability to create user-definable services which can be used to define firewall rules.</p> <p>1.6 Bandwidth Management</p> <p>1.6.1 The proposed system should have integrated Bandwidth Management</p> <p>1.6.2 The proposed system should be able to set guaranteed & burstable bandwidth per User & group of User</p>	
--	---	--

1.6.3 System should be able to create Bandwidth Policies based on applications & not on IP or Ports

1.6.4 The proposed system should provide user based & layer 7 based visibility & bandwidth utilization for every connection established through that system

1.7 Intrusion Detection & Prevention (IDP)

1.7.1 The proposed system should have signature & anomaly base intrusion detection & prevention system

1.7.2 The proposed system should be able to provide multiple IDP policies & allow attaching an IDP policy to a firewall rule. This should help the administrator in defining customized IDP policies as per his requirement of security & alerts

1.7.3 Reporting of internal alerts should be based on usernames & not on hostnames or IP addresses.

1.7.4 The attack signatures should be automatically updated from a central database server

1.8 Gateway Anti-Virus

1.8.1.a The proposed system should have an integrated Anti-Virus solution & should be able to provide real-time detection of viruses & malicious code at the gateway for HTTP,SMTP, POP3,IMAP & HTTP Internet traffic

1.8.1.b The Basic Virus Signature Database should comprise of the complete Wild List Signatures & variants as well as malware like phishing mails & spy ware. The ant virus system should not be share-ware, free-ware

1.8.1.c Facility to add signature/Disclaimer in emails

1.8.1.d Facility to provide notification of email virus information to admin email id

1.8.1.e Facility to store infected emails in Quarantined section in the appliance itself

1.8.1.f The proposed system should have configurable policy options to block different file types such as Executables, Dynamic

1.8.1.g The proposed system should have configurable poplcy options to block customized file type attachments like. doc,.xls,.ppt etc

1.8.1.h 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, Do no deliver or remove attachment & deliver. Similarly notification to administrator on either of the above options should be available

1.8.1.i In terms of SMTP the Proposed system should not act as mail relay or MTA by itself unless configured

1.8.1.j In SMTP system, it should be support facility to create customized scanning rules

1.8.1.k Customized scanning rules should allow policies to be applicable on sender/recipient email addresses or address groups for notification settings, quarantine settings & file extension blocking

1.8.1.l The proposed system should be able to update with the frequency less than 1 hour its signature database automatically at a preconfigured interval & through manual update

1.8.1.m In terms of POP3 & IMAP system, if virus us detected in the email, the

virus affected attachment should be stripped from the message & the message body should be replaced with a notification message.

1.8.1.n The HTTP Anti Virus gateway should be able to scan sites based on source, destination & URL regular expressions for Virus scanning

1.8.1.o The HTTP Anti Virus system should be able to bypass source, destination Hosts

1.8.1.p The HTTP Anti Virus should have scanning options of real mode & batch mode with option to restrict file size for scanning

1.8.1.q Support Personalized Individual User Quarantine support.

1.8.1.r The proposed system should be able to provide alerts & reports based on username, protocol, IP address, sender, recipient, subject & virus-names

1.8.2 Gateway Anti-Spam

1.8.3 The proposed system should have an integrated Anti-Spam solution in the Appliance

1.8.4 Should have ability to filter SMTP, POP3 & IMAP traffic

1.8.5 The Proposed system have configurable policy options to select what traffipc to scan for spam

1.8.6 Facility to mark a copy of all incoming & outgoing emails to administrator defined email address

1.8.7 The proposed system should have an option of having a configurable spam policy per email address or address group or size of mail.

1.8.8 The propose system should be able to tag email subject based on the spam filter match criteria

1.8.9 The proposed system should minimally provide SPAM filtering base on :

1.8.10 The proposed system should be able to provide alerts & reports based on username, mail protocol IP address, sender, recipient, subject & spam-categories

1.8.11 It should act as a Spam Proxy server

1.8.12 It should block image based spam mail

1.9 Web filtering & Application control

1.9.1 The proposed system should have integrated Web Filtering solution in the appliance

1.9.2 Websites & its category information should be locally stored inside the Appliance & it should not query third party or Remote Hosted Servers on Data centres

1.9.3 System should have facility to block Web based upload of file attachments

1.9.4 The web content filtering solution should also be able to work as an independent HTTP proxy server

1.9.5 The proposed system should provide web content filtering features as follows:

*URL database should have at least 8 million sites & 60+ default categories .

*Should block URLS based on regular expressions

*Should have support for URL exclusion list based on regular expression

	<ul style="list-style-type: none"> *Should be able identify * Block Google cached links based on its categories *Should be able to block websites which are hosted on akamai *Should be able to identify requests behind a proxy server & block by requests by IP addresses & username which are even behind a proxy server *Should be able to identify URL Translation Web server & block requests to such servers 		
1.9.6	<p>The proposed system should provide application controls features as follows:</p> <ul style="list-style-type: none"> *Should be able to block famous chat & instant messaging communication like yahoo, jabber msn, AOL messenger etc & other applications based on signatures & independent of ports. *Should be able to block file upload through IM, FTP protocols. *Should be able to block users from accessing public HTTP proxies running on port 80 as well as any other port 		
1.9.7	The proposed system should have support for user authentication from Windows PDC, Windows AD, LDAP server & Internal Database		
1.9.8	Should be able to customize block message for each categories		
1.9.9	Should be able to log & report usernames, request IP address, domain name, URL, website category & category type		
1.9.10	Should be able to identify traffic based on productive, neutral & unproductive websites as specified by admin		
1.10	Multiple ISP Load Balancing & Failover		
1.10.1	The proposed system should have integrated multiple ISP load balancing & failover for outbound traffic		
1.10.2	Multiple link load balancing & failover should be possible for more than 2 ISP Links		
1.10.3	The proposed system should be able to do weighted round robin based load balancing of traffic over multiple links based on the weight assigned to each link		
1.10.4	The proposed system should be able to detect link failure based on user configurable set of rules based on rules based on ICMP, TCP & UDP		
1.11	Reporting solution		
1.11.1	The proposed system should have integrated reporting solution running on the same appliance. The reports should be accessible through HTTP or HTTPS		
1.11.2	Reports should be available based on individual users download & Upload traffic		
1.11.3	The proposed system should provide user based, group based & IP address based reports for traffic discovery, Gateway level Anti Virus & Anti Spam, Intrusion detection & prevention & Web Content Filter		
1.11.4	The proposed system should provide reports in HTML, Graphical CSV format		
1.11.5	The proposed system should have configurable options to send the reports on mail to designated email addresses		

	<p>1.11.6 The proposed system should have options to create users with different access rights(E.g users who can only view reports & not manage the system)</p> <p>1.11.7 The proposed system should be able to provide connection wise reports for user, application, source & destination IP address & source & destination port & protocol</p> <p>1.11.8 The reporting solution should be able to provide detailed reports about the mail activity passing through the system</p> <p>1.12 High Availability</p> <p>1.12.1 Appliance must have Active/Passive & Active/Active High availability to prevent single point of Failure</p> <p>1.13 Virtual Private Network (VPN)</p> <p>1.13.1 The proposed system should allow to create & establish IPSec (Net-to-Net, Host-to-Host & Road warrior connection</p> <p>1.13.2 The proposed system should allow Preshared key & Digital Certificate based Authentication.</p> <p>1.13.3 The proposed system should support Connection fail over for Net-to-Net, Host-to-Host & Road warrior connection.</p> <p>1.13.4 The proposed system should support following Encryption algorithm: 3DES, DES,AES, Twofish, Blowfish, Serpent</p> <p>1.13.5 ies</p> <p>1.13.6 The proposed system should provide a facility to export the Road Warrior connection configuration for use by the VPN client</p> <p>1.13.7 The proposed should support most commonly available VPN IPSec Clients.</p> <p>1.13.8 The proposed system should provide local Certificate Authority & should provide facility to create/renew/delete self-signed certificates.</p> <p>1.13.9 The proposed system should have preloaded 3rd party Certificate Authority including Verisign/Entrust.Net/Microsoft & provide facility to upload any 3rd party Certificate Authority</p>	
	<p>PRINCIPAL</p>	
	<p>OFFICE COPY</p>	
	<p>STORE KEEPER STORE OFFICER PROCUREMENT OFFICER</p>	

--	--	--	--