



The Institute of Cost Accountants of India

**Tender for supply and installation of 1 Nos. 1U Rack
Hardware mountable firewall at Delhi**

Tender Document

Table of Contents

Chapter	Description	Page No.
1	Notice Inviting Tender	2-3
2	Instructions to Bidders	4-6
3	Technical Specifications & Standards for Unified Threat Management (UTM)	7-10
4	Technical Format	11-12
5	Financial Bid Format	13



Chapter – 1: Notice inviting Tender

Ref. No.IT/001-2018/1:

Date of Tender: 31,July, 2018

Last date of Submission: 21 August, 2018 till 12.00 HRS.

Subject: Tender for supply and installation of 1 Nos rack mountable hardware firewall (3 Years)

1. Bids are invited in two bid format (Technical Bid & Financial Bid) from the reputed manufacturers / authorized dealers / sales partners as per qualification criteria given in the Tender Document for the supply and installation of 1 Nos rack mountable hardware firewall as per the specification given in tender document.
2. **Submission of Tender:** Quotation signed by the bidder in a sealed envelope, superscribed with “**Tender for supply and installation of 1 Nos rack mountable hardware firewall (3 Years)**” is to be submitted in the Tender Box of the Institute at CMA Bhawan, 3rd Floor, 3, Institutional Area, New Delhi - 110003.
3. The last date of the submission of quotation is of **August 21, 2018 till 12.00 hrs.** The quotation must be valid for minimum 60 days from the date of submission of quotations.
4. The Institute is not bound to accept the lowest tender and reserves the right to cancel any or all the Tenders without assigning any reason thereof.



1.	Type of work	supply and installation of 1 Nos rack mountable hardware firewall (3 Years)
2.	Date of Announcement of Tender	31.07.2018 (Tuesday)
3.	Last date for submission of Tender	21 August, 2018 (Tuesday) at 12:00 Hrs. (The Technical bid and Commercial Bid are to be sealed in separate envelope super-scribing Technical Bid and Commercial Bid respectively)
4.	Date of Opening of Technical Bid	21 August, 2018 (Tuesday) at 3:00 PM
5.	Date of Opening of Price bids	24 th August, 2018 (Friday) at 11:00 AM
8.	Address of Submission	Tender Box, 3 rd Floor, CMA Bhawan, 3 Institutional Area, Lodi Road, New Delhi-110 003.
9.	Mode of Submission of Tender documents	By hand or through post/courier so as to reach before the last date & time of tender submission i.e. 21 st August, 2018 on or before 12.00 hrs.)
10	Contact Person	Mr. Ashish Tiwari, Jt. Director (IT) Email id : - it.jd1@icmai.in Landline: 011-24666106 (to be contacted- Monday to Friday during office hours.)

Tender Document to be downloaded from the official website:

www.icmai.in

CONVENER TENDER COMMITTEE



Chapter – 2: Instructions to Bidders

Pre-qualification criteria for the Bidders

The Eligible bidder should satisfy the below mentioned criteria and should submit valid Documentary evidence for the below mentioned points:

1. The Bidder should be a company registered in India (Attach a copy of Certificate).
2. The Bidder should be in business of supplying and installing firewalls for at least 5 years.
3. The bidder should have an average turnover of `50lakhs or above during audited financial years 2015-16, 2016-17 and 2017-18 and submit the copy of the audited annual accounts for these years along with the copy of PAN No and GSTIN No
4. The bidder should have supplied and installed the firewall in at least three organizations (preferably in Govt. Departments/Ministries/PSU/Autonomous bodies) during the last three years. Detail of such projects and references to be provided.
5. The bidder must be the manufacturer / authorized dealer / sales partner of the quoted product. A copy of authorization letter from the manufacturer is required in case the bidder is authorized dealer / sales partner.



General Instructions

1. **Taxes:** The percentage of all the taxes, duties, levies, must be quoted in clear terms separately. If the taxes are not mentioned separately, it will be presumed that the rates quoted are inclusive of all taxes.
2. **Delivery :**The Supply and installation of Firewall must be made within four weeks from the date of issue of supply order. The installation location would be a data centre in Delhi. The supply should be effected as per specifications furnished in Specifications and other details of tender document. In case there is any specific schedule of delivery on the part of bidder, it should be clearly mentioned in the bid.
3. **Warranty :** All tendered items shall be under three years on site comprehensive warranty support from the date of installation including free spare parts, kits etc excluding the consumable.
4. Any bid received after the last date & time for receipt of the given in the Tender Document will be rejected.
5. The quoted rates of offer will be valid for a period of 60 days.
6. Work order will be communicated to successful bidder by email.
7. Taxes shall be paid as applicable and quoted by the vendor.
8. The statutory tax deductions on the payment made by the Institute would be done as per the prevalent Tax laws of Government of India.
9. The bidder should sign each and every page of this document and attach it with the bid document.
10. The committee reserves the right to reject any/ all quotations without assigning any reason there for.



11. For any further clarification/information please contact Shri Ashish Tewari, Joint Director, IT, ICAI (Phone 011-24666106) on any Working Day (Mon-Friday) during Office Hours.
12. The delivery charges and installation Charges (if any) should be included in the price quoted. No extra charges shall be payable for delivery.
13. Conditional / Incomplete bids shall be rejected.
14. The financial bid should strictly be in the format specified in the tender document.
15. This Tender shall be governed by the laws of India for the time being in force and subject to exclusive jurisdiction of Courts at Delhi.
16. It is not obligatory on the part of the management to accept the lowest offer. Management may summarily reject any or all the offers against the tender without assigning any reason to the bidders participating in the tender.
17. Vendor shall ensure getting proper license /permission from the concerned authorities wherever applicable.



Chapter – 3

Technical Specifications & Standards for Unified Threat Management (UTM)

Basic Criteria

- The quoted OEM for UTM should have presence in India from more than last five years.
- OEM should have support Centre in India.
- Appliance should have ICSA certification for Firewall.
- The proposed solution should support High Availability Active-Active mode
- The proposed UTM should be a leader in Gartner's Magic Quadrant for UTM

Appliance Throughput

- Firewall throughput of 15 Gbps
- Minimum 3 Gbps of Antivirus Throughput
- Minimum 15,000,000 Concurrent sessions
- Minimum 8 Gbps of IPS throughput
- Minimum 200,000 New Sessions/second
- Minimum 2 Gbps of IPsec VPN throughput
- Minimum of 2000 IPsec Site to Site tunnel support and 100 SSL VPN user support. License for the same should be included in the BOM.
- Minimum of 8 x GBE Interfaces and 2 x GE SFP with expansion slot to accommodate more ports if required.

General Features

- Should be appliance based and rack mountable
- Identity based Firewall
- Intrusion Prevention System
- Gateway Anti-virus
- Gateway Anti-spam with DLP functionality
- Web Content & Application Filtering
- Web Application Firewall
- Bandwidth Management
- Inbuilt-on Appliance Reporting



- High Availability (Active-Active & Active-Passive)
- Network: OSPF, Round Robin load balance, RIPv2, BGP, equal & unequal cost load balance, High Availability, QoS, etc. Round Robin Balance, Server Load Balancing.
- Support for user authentication over SMS.
- Country Based Blocking, FQDN support and should support MIX mode deployment
- 4 Eye Authentication feature for data integrity.

Gateway Antivirus, Anti-Spyware and Anti-Spam

- Virus, Worm, Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, MIME header check, and Redirect spam mails to dedicated email address, image-spam filter, Spam Notification, Zero hour Virus outbreak protection. Recurrent pattern Detection Technology for AS. Self Service Quarantine area. Should have dual AV engine, Email Encryption, Recipient self-registration SPX password management, DLP engine with automatic scanning of emails and attachments for sensitive data

Web and Application Filtering:

- URL, Keyword, File type block, Block Java applets, cookies, ActiveX, Block malware, phishing, pharming URL, block P2P application, anonymous proxies, Customized block on group basis. Minimum of 89 categories with more than 160 million URLs supported. 2000+ application support categorized into Characteristics, Technology, Category and Risk Level.
- The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS.
- Blocking personal Gmail and allowing only hosted email domains.

Wireless Security and Control:

- Should act as a wireless controller, Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center, Central monitor and manage all APs and wireless clients through the built-in wireless controller, Support for IEEE 802.1X (RADIUS authentication), Wireless repeating and bridging meshed network mode with supported APs



Security Features

- **Intrusion Prevention System (IPS):** For different attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, Source and Destination NAT, TelNet Attack. Signatures: Default (5000+), Custom , IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates, Protocol Anomaly Detection.
- **Web Application Firewall (WAF):**
Should have an option of WAF with Positive Protection Module, Protection against SQL Injections, Cross Site Scripting (XSS), Session Hijacking, URL tampering, Cookie Poisoning, Reverse Proxy, Dual AV Engine, Extensive Logging and reporting. If external, then has to be quoted separately.
- **Advance Threat Protection:**
Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
- **VPN:**
IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal.
- **Load Balance:**
For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.
- **Bandwidth Management:**
Application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Group, Firewall Rule, URL and Applications.

Monitoring and Reporting System:

- Includes Integrated Web Based reporting,, Monitoring & Logging, **Monitoring suspicious activity and alerts**, Graphical real-time and historical monitoring,



email notification of reports, viruses and attacks reports. IPS, Web filter, Antivirus, Anti-spam system reports. IP and User basis report, 45+ Compliance reports and 1200+ drilled down reports on the appliance.

- Should provide User Threat Quotient (UTQ) report for actionable security intelligence, helping Administrators identify risky users with ease within the organization's network.

License for UTM (Unified Threat Management)

- Three Year round the clock support for Gate Way Antivirus, spyware, Anti-Spam, WAF, content and application filtering. IPS, reporting and support, Upgrades.
- License period will be counted after activation.



Chapter – 4: Tender Format

PLACE:

DATE:

To

The Covenor (Tender Committee)
The Institute of Cost Accountants of India
3, Institutional Area, Lodhi Road
New Delhi -110003

Dear Sir,

1. I/We hereby offer to supply and install 1 No of firewall as per details specified in Chapter – 3.
2. Should this tender be accepted, I/We hereby agree to abide by and fulfill the terms and conditions of this tender document.
3. All information and documents as required to be submitted and Instructions to tenderers are enclosed.

S.No.	Details Requested	Provide Details	Compliance (Yes/No)
1.	Name of the Company/ Vendor		
2.	Year of Incorporation/ Establishment		
3.	PAN No. (copy attached)		
4.	GSTIN (copy attached)		
5.	TAN/ TIN No (copy attached)		



6.	Complete Address (with Phone, Mobile, Email of the contact person)		
8.	Whether supplied an installed the server work at Govt. Departments/Ministries/PSU/Autonomous bodies during last three years ending March 2018. (attach proof)		
9.	Turnover of last three consecutive years (It should not be less than `50lakhs per year attach proof)		
10.	Provide details of Helpdesk support with the Escalation procedure and matrix for customer complaints.		
11.	RTGS & Bank Account Details		
12.	Any other details		

Signature:

Name of the Authorized Signatory:

Name of the Company/Firm:

Contact No.:

Seal of the Company/Firm:



Chapter – 5

Financial Bid Format.

S No	Description	Qty.	Price (in INR)	Taxes (Pl. Specify breakup of taxes) (in INR)	Total (in INR)
1.	Firewall (Specifications given in Chapter No 3)	1			
2.	Installation of Firewall	1			
3.	Any other charges to be specified clearly	1			
Total					
Total (in words) Rupees.....					

Commercial Terms and conditions

1. Payment for supply and installation will be made within one month from the date of satisfactory completion of job and receipt of Invoice.

All Payments will be made through Electronic Mode to the Bank Account of the selected Tenderer.

Signature:

Name of the Authorized Signatory:

Name of the Company/Firm:

Contact No.:

Seal of the Company/Firm: