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 – 1: Notice inviting Tender

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

Date of Tender: 26, September, 2018

Last date of Submission: 16 October, 2018 till 12:00 P.M

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

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 Year)"** is to be submitted on or before 3.30 p.m. of **October 16, 2018 till 12:00 P.M.** 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 **October 16, 2018 till 12:00 P.M.** 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.

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 ` 50 lakhs 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)

Specification
Integrated Security Appliance which is capable of supporting Firewall, VPN, IPS, Web filtering, IPv6 ready, Gateway Antivirus and e-Mail filtering capabilities should be supported which will be configured as per requirement at a later stage.
Product support should be (24X7)
Appliance based firewall, Should be VPNC, ICSA Firewall & Anti virus
Vendor to support appliance for at least 3 years from the date of purchase order.
Number of Network Interfaces to be mentioned exactly as supported by the device, Vendor to quote with minimum of (12) 10/100/1000 copper gigabit, 4x2.5 Gbe SFP, 4x2.5 GBE, 2 USB, 1 console interface.
Appliance should have dedicated 1Gbe management interface
Should support firewall throughput of at least 3 Gbps or higher
Should support VPN throughput of at least 1.5 Gbps or higher
Should support at least 225000 concurrent sessions and at least 15000 new sessions per second
The device should not have license restriction on number of users
Should support at least 1000 IPSec Site-to-Site VPN tunnels and 1000 no of IPSec Remote access VPN
Should support at least 350 concurrent SSL VPN users
The firewall should be able to support dynamic load balancing for data passing through the firewall, If external firewall load balancers are required same is to be mentioned.
Dual WAN/ISP support: Should support automatic ISP failover as well as ISP load sharing and load balancing for outbound traffic.
Traffic Management: option to configure traffic shaping on a per policy basis for specific application/specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.
Should not have 2nd gen proxy inbuilt on to the appliance to avoid latency
The appliance Should support 256 VLAN interfaces (802.1q)
Appliance should support IPSec NAT Traversal
should support OSPF, RIP V1 and V2 routing protocol.
It should support IPV6
Bandwidth Control/ Restriction per IP Address group & Per policy should be available.
Should Support NAT without degrading the performance of the firewall

Should support authentication using XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix
Should have Layer 2 bridge or transparent mode
should have at least 1.4 Gbps of IPS throughput or higher
IPS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.
Appliance should have atleast 22 classes of DOS & DDOS & scanning attacks and attack protection
Should not have any point of failure devices like hard drives inbuilt on the appliance rather should support flash
Should have all security functionalities inbuilt on single appliance
The IPS and or UTM should be configured in a manner, so that in case if the either fails the traffic should not be affected , without any manual intervention.
Should do real time scanning rather than proxy based scanning of all the traffic passing through the appliance.
Signatures should have a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (eg. for severity level: high, medium, low)
Should be able to generate graphical reports on top attacks, source for attack etc.
Should have the option to schedule reports for automatic generation & email it to admin
Vendor updates its attack signature database regularly and it should be configurable to update the signatures automatically without manual intervention.
Vendor makes new attack signatures and new major software releases available for download from their Web site
Should be a integrated solution with appliance based firewall on a single chasis with multicore processor.
Should not be an ASIC's based solution rather should be quad core or higher processor for faster processing.
The proposed solution should have minimum 600 Mbps of Anti malware throughput or higher
Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3,HTTP, FTP etc. Internet traffic
The proposed solution should be licensed per unit as against per user
Should support full Deep packet inspection through put of 600 MBPS or higher.
Vendor to declare IMIX internet mix for appliance and should not be less than 700 MBPS
Vendor to declare UTM/Deep packet inspection throughput and should submit valid document for the same
Antivirus Gateway should have option to configure to respond to virus detection in several ways

Automatic Frequent updates of virus pattern files Should be available from the vendor without manual intervention
Should not buffer traffic before scanning for virus or ips.
Should have facility to block files based on file extensions
Should be an unlimited user based appliance
Should have capability to scan unlimited file size without buffering them
The proposed solution should be scalable and offer fault tolerance to safeguard against hardware failures. The failover should be capable of taking over the traffic without any manual intervention and session loss.
The solution should support load balancing for the AV or UTM ,for the traffic which needs to be scanned in case appliance fails
Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.
Web content filtering solution should work independently without the need to integrate with proxy server, there should not be any prxoy inbuilt in to the UTM
Should have facility to block URLs based on categories
The proposed solution should be licensed per unit as against per user.
URL database should have at least 15 million sites and 50 + categories.
URL Database should be updated regularly by the OEM automatically
Should be able to block different categories/sites based on users/groups.
Should have facility to configurable policy options to block web sites based on banned words.
Should have application control and intelligence inbuilt in the systems without support of external device.
Application control should have more than 5500 + applications inbuilt and should have granular control over the application
Should have configurable policy options to define the URL exempt list
The solution should be able to block spywares/adwares etc.
The solution Should have options to block java applets, activeX as well as cookies
Vendor should have RBL database of known spam sources to validate/check whether the mail is a spam or not
Should not slow down the performance of UTM on enabling antispam
Should have configurable spam actions for detected spam mails
Logging and reporting solution should be supported.
The solution should generate the reports for the firewall, gateway level AV, IPS web filtering requested.
Should support deep packet SSL to decrypt HTTPS traffic for scanning transparently, and then re encrypt to send to destination if no threat found
The solution shall have readymade templates to generate reports like complete reports or attack reports, bandwidth report etc.

The solution should help to analyze/understand Attacks over various protocols like http, ftp, SMTP etc
The solution should help to analyze/understand the live application usage in the network
Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks
Should have options to generate reports in different formats
The solution should have configurable options to send the reports as a mail to the designated email address
Should have configurable parameters to send alert emails based on event type.
Should have configurable parameters to set alert.
The solution should have configurable options to schedule the report generation
The solution should be running its own syslog server or integrated server to collect the logs
If separate server/appliance is required for the logging & reporting, the BOM & cost should be included in the proposed solution..
The solution should have sandboxing services available on the same platform
sandboxing service should use atleast 3 scanning engine for scanning suspicious traffic
one of the scanning engines for sandboxing should have 100% NSS labs recommendation on malware catch rate
admin should be able to upload malicious file manually for sandboxing purposes
sandboxing engine should also have 0% false positive from NSS labs
sandboxing service should not be appliance based rather on cloud
admin should to receive detailed report of each & every file sent for sandboxing
there should be an option to hold the file at gateway leve untill verdict for same is declared
vendor to submit valid doc for NSS labs 100% catch rate for sandboxing engine
The appliance should do re assembly free deep packet inspection of traffic passing through it.
There should not be any file size limitation to be scanned at GAV level.
Appliance should not have proxy inbuilt on to the appliance for content filtering purposes
All the UTM functionalities along with IPSEC & SSL VPN functionalities should be on single platform

All the UTM services should be quoted with 3 yrs. support & services
UTM services should consist of Gateway Anti-virus, anti spyware, IPS , application control, intelligence & visualization, anti bot , geo IP filtering form day one
24x7 support should be quoted
24x7 support should be available from day one
Sandboxing services should be available from day
All the features /services/licenses required to run sandboxing should be available from day one

Part A: Details of the Company:

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 ` 50 lakhs 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		

Declaration:–

I, _____, hereby certify that "I am not debarred by Department of Commerce or any Ministry/Department concerned."

Date:

Name and Signature of Bidder / printer with Corporate Seal

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			
3.	Installation of Firewall	1			
4.	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.
2. All Payments will be made through Electronic Mode to the Bank Account of the selected Tenderer.

Date:

Name and Signature of Bidder / printer with Corporate Seal

Convenor (LPC)