TENDER DOCUMENT

Tender Notification No. 61/2016/IT Dept/GVMC/ NXFW Appliance - Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam Dated 27/07/2016

Tender for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam as per document attached.

Cost of Tender Document: Rs. 1000/-

Last Date & Time for Submissions of Bids: _____

Tender Document issued to

TABLE OF CONTENTS

GREATER VISKHAPATNAM MUNCIPAL CORPORATION (GVMC), VISAKHAPATNAM

NOTICE INVITING TENDER

Sealed tenders (Technical and Financial Bids) are invited from eligible bidders for Tender for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam.

The Tender Document may be view from the GVMC Website: www.gvmc.gov.in. The complete Tender documents may be purchased on payment of non refundable fee of Rs. 1000/- through DD Drawn in favor of **"COMMISSIONER, GVMC, VISAKHAPATNAM"** and submitting the DD at OSD(IT), IT Section.

For Commissioner, GVMC
Visakhapatnam

TENDER DOCUMNET

Tender Notification No. **61/2016/IT Dept/GVMC/ UTM Appliance- Supply , installation, Configuration ,Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam Dated 23/07/2016**

Subject: **Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam**

The GVMC invites sealed tenders (Technical and Commercial Bids) are invited from eligible bidders for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam

The tender form containing the details of terms and conditions duly filled in along with the demand draft of **Rs. 28000 /- as Earnest money** in favor of **COMMISSIONER, GVMC, VISAKHAPATNAM** should reach to the Commissioner, GVMC, Tenneti Bhavan, Ramnagar, Visakhapatnam – 530002 by 3.00 PM on **10/08/2016** and shall be opened on same day at 4.00 PM. One representative of the firm may be present at the time of opening of the Technical Bid.

All interested eligible bidders are requested to submit their bids duly filled in as per the criteria given in this document:

1. Technical Bid and EMD of **Rs. 28000 /-** should be sealed in a separate envelope subscribing "Technical Bid"
2. Commercial Bid should be sealed in a separate envelope subscribing "Commercial Bid "

Both Technical and Commercial Bid envelopes should be enclosed and sealed in a separate envelope subscribing the "Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam". The sealed envelope should be addressed to:

The Commissioner, GVMC, Tenneti Bhavan, Ramnagar, Visakhapatnam – 530002

Last Date of Submission: 10/08/2016 up to 3:00 PM

for Commissioner
GVMC, Visakhapatnam

CHAPTER 1:

Eligibility Criteria of Tenderer / Bidder

1. Eligibility Criteria

(a) Bidder should be ISO Certified and Original Equipment Manufacturer (OEM) / Authorized Partner of Principal UTM Vendor/ Dealers /Distributors are eligible participate and a letter of Authorization from OEM should be enclosed.

(b) The bidder should have experience of providing and implementing Security Solutions (UTM/Firewall) with onsite support and successful execution of at least 3 similar works to any Govt. / PSU / Autonomous bodies /reputed Public listed companies for any 3 years during the past 5 years. Proofs to be enclosed.

(c) The Bidder should have professionals certified on the UTM security solution and they propose against this quotation. Proof of the same shall be enclosed.

(d) The Bidder should have local Office or Service Center in Visakhapatnam for past five years (Proof of any local statutory registration certificate to be produced).

(e) The bidder should have an **Average Annual Turnover of more than Rs. 5.00 Crores for the last three years 2013-14, 2014-15 and 2015-16** in respect of IT sales and services for maintaining IT infrastructure. This has to be substantiated by the Balance sheet of the Firm / Company for the relevant years duly certified by CA.

(f) The bidder should have valid Sales Tax /VAT/Service Tax Registration Certificate.

(g) The firm should not be blacklisted / barred by Government of India or any regulatory body in India. Self declaration to be submitted.

(h) Failure of submission of any of the documents in Technical Bid will make the bid rejected as non-responsive. GVMC will have the option to treat some documents as mandatory/optional in the benefit of the GMVC.

2. Schedule of Invitation to Tender

(a)	Name & Address of the Purchaser	IT Section, GVMC, Tenneti Bhavan, Ram Nagar, Visakhapatnam,530002
(b)	Place of submitting Tender	IT Section, GVMC, Tenneti Bhavan, Ram Nagar, Visakhapatnam,530002
(d)	Cost of Tender Documents	Rs. 1000/-
(e)	Start Date for issue of tender schedules	27/07/2016@ 11.00 AM
(f)	Last Date for issue of tender schedule	10/08/2016 up to 1.00 PM
(g)	Last Date & Time for submission of Tender is on or before	10/08/2016 up to 3.00 PM
(h)	Date & Time of Opening of tender	10/08/2016 @ 4.00 PM
(i)	Date till which the Tender is valid	30 Days from the date of opening of Financial Bid

Note: GVMC shall not be responsible for non-receipt/non-delivery of the tender documents due to any reasons whatsoever.

for Commissioner
GVMC, Visakhapatnam

CHAPTER 2: SCOPE OF WORK

1) This project provides for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam
2) Vendor has to propose the best security solution and should do the necessary configuration and apply policies to secure entire network of GVMC and Zonal Offices.
3) GVMC has Web Server "gvmc.gov.in" It can be used to view the information of GVMC and can do the online payment for taxes. It should be configured with Web Application Firewall to protect against attacks like SQL Injections, Cross-site Scripting, Session Hijacking, URL Tampering, cookie poising and other types of attacks.
4) GVMC has Connectivity from Main Office to 8 Nos Zonal Offices through BSNL Leased Lines & OFC and also having connectivity to Some Banks and GVMC Water supply offices through VPN Connectivity. The proposed solution should provide secured access to the Main office network.
5) The network should be configured in such a way that all zonal offices and other sites will be connected through firewall to GVMC Datacenter. And necessary restrictions and policies should be applied.
6) The successful bidder should coordinate with IT Section and implement the necessary security policies as per requirement of IT Section, GVMC. Any required details will be given by IT Section, GVMC to the successful bidder at time of implementation.
7) Remote VPN and Site to Site VPN should be configured to allow access from outside of the GVMC network.
8) The successful bidder should propose best security solution and should be implemented.
9) The successful bidder should support in implementing the security solution according to any major modifications done in network after completion 1st time successful configuration i.e Vendor should support whenever necessary in modification of configuration of firewall in the 3 years of time.

2. Technical Specifications:

This section provides required technical specifications of the product

I. System Level Specifications

1. The proposed appliance should have at least one of the following certifications EAL4+ / ICSA / NSS-Lab.
2. Proposed solution should be hardware based appliance. It should have inbuilt Flash/HDD Storage.
3. Proposed solution should comply with FCC and CE norms
4. The proposed solution should match the following criteria

    a) Must have a 64-bit hardware platform
    b) Proposed appliance should contain 8Gb Ethernet ports or more ports and should have minimum 2 slots to support Flexi port Modules of 8Gb Ethernet Ports / 1GbE Fiber / 10GbE Fiber ports.
    c) 2,00,000 New Sessions per second
    d) 60,00,000 concurrent sessions
    e) 28,500 Mbps Firewall Throughput (UDP)
    f) 20,000 Mbps Firewall Throughput (TCP)
    g) 8,500 Mbps IPS Throughput
    h) 1750 Mbps WAF Protected Throughput
    i) 5000 Mbps or above Anti-Virus throughput
    j) 4000 Mbps or above Fully Protected Throughput
    k) 750 Mbps or above SSL VPN throughput
    l) 100 or above SSL VPN Connections
    m) 4000 or above concurrent VPN connections
    n) 10000 concurrent web sessions through web cache.
    o) Appliance should be supplied with 4GB RAM and it can be upgradable.
    p) UTM appliance should have internal storage of minimum 250 GB.

5. The proposed solution must support USB Port 3G/4G and WiMAX for backup connectivity
6. All features should have equivalent support for IPV4 & IPV6, unless explicitly specified.
7. The proposed solution should support unrestricted user/node license or minimum of 700 nodes.
8. The proposed solution must work as a standalone HTTP proxy server with integrated Firewall, Anti-Virus, Anti-Spam, Content filtering, IPS and Application Control. Option to enable / disable any service should be available.
9. The proposed solution must support User and Role based policy configuration for security and Internet bandwidth management.
10. The proposed solution should provide on-appliance reports / dedicated reporting server based not only on IP addresses but also usernames.
11. The appliance should generate audit trail and have secure interface to transfer it to the remote system.

II. Administration, Authentication and General Configuration

1. The proposed solution should support administration via secure communication over HTTPS, SSH version 2 or above and from Console Terminal.

2. Solution must support multiple administrators working in parallel. All the policies and objects on which Administrator 1 is working should be locked for all other administrators. However, administrators can work on policy rules and objects that are not locked. Changes done by Administrator-1 should not be visible to other administrators till the time Administrator-1 publishes the changes.
3. Solution must allow administrator to choose to login in read-only or read-write mode.
4. The proposed solution should be able to export and import configuration backup including user objects.
5. The proposed solution must be deployable in Route (Layer 3) and Transparent Mode (Layer 2), individually and simultaneously.
6. The proposed solution should support policy-based routing.
7. The proposed solution should support integration with Windows Active Directory, LDAP, RADIUS or Local Database for user authentication.
8. The proposed solution must support SSL/TLS connections to LDAP/Active Directory servers.
9. The proposed solution must support Automatic Transparent Single Sign On (SSO) for user authentication. SSO must be proxy independent and should support user authentication for network applications like *http, https, ssh, git, skype etc.*
10. The proposed solution should provide bandwidth utilization graphs on daily, weekly, monthly and yearly basis for each one of the ISP links terminating on the UTM appliance.
11. The proposed solution should provide real time data transfer/ bandwidth utilization details with respect to individual users / IP addresses/ applications.
12. The proposed solution should support NTP.
13. The proposed solution should support user/IP address/MAC address binding that can map username to corresponding IP and MAC addresses for security reasons.
14. The proposed solution should support version roll back functionality.
15. The proposed solution should be able to force-logout users upon session time-out, quota exceeded (over-download) and idle time-out.
16. The proposed solution should support group-based user creation for administration purposes.
17. The proposed solution should support SNMP v1, v2c and v3.
18. The proposed solution must provide flexible, granular role-based, application based and flow based bandwidth management, GUI for administration for configuring hosts, networks, services, access rules, bandwidth allocation, VPN, NAT, etc.
19. The proposed solution must provide support for multiple authentication servers for each module (e.g. firewall, VPN etc).
20. The proposed solution must support multiple Thin Client (Microsoft TSE, Citrix) authentication mechanisms and must be able to differentiate between requests originating from the same IP address.
21. The proposed solution must support:
    a) DHCP/DHCPv6 Server,
    b) DHCP/DHCPv6 Relay Agent,
    c) DNS/DNSv6 Proxy,
    d) Bandwidth reservation for critical applications like DNS,
    e) Customizable login and security settings.

22. The proposed solution must provide customizable administrator password complexity setting.
23. The proposed solution should support event-triggered alerts/alarms, based on preset thresholds.

III. Firewall:

1. The proposed solution should have EAL4+ / ICSA / West Coast Labs Checkmark certification
2. The proposed solution should be a standalone appliance with secured OS.
3. The proposed solution should support stateful inspection with sessions identified by usernames, and in the presence of dynamic NAT and PAT.
4. The proposed solution should use User Identity as a matching criterion along with Source/Destination IP/Subnet/group/port in firewall rules.
5. The proposed solution should facilitate the application of UTM policies related to AV/AS, IPS, content filtering, bandwidth policy and policy-based routing decisions on the firewall rule itself.
6. The proposed solution should support user-defined multi-zone security architecture.
7. The proposed solution should have predefined applications based on port/signature and also should support creation of custom applications based on port/protocol number.
8. The proposed solution should support inbound NAT load balancing with different load balancing methods like First Alive, Round Robin, Random, Sticky IP and failover, with server health check by TCP or ICMP probe.
9. The proposed solution should support 802.1q VLAN tagging.
10. The proposed solution should support dynamic routing like RIP1,RIP2, OSPF.
11. The proposed solution must support IPv6 as per www.ipv6ready.org guidelines.
12. The proposed solution must support IPv6 Dual Stack Implementation.
13. The proposed solution must support tunneling like 6in4, 6to4, 4in6,6rd.
14. The proposed solution must support all IPv6 configurations on GUI.
15. The proposed solution must support DNSv6.
16. The proposed solution must support DoS protection against IPv6 attacks.
17. The proposed solution must support spoof prevention on IPv6.
18. The proposed solution must support the 802.3ad standard for Link Aggregation.
19. The proposed solution must support Application-based Bandwidth Management, which allows the administrator to create application based bandwidth policies.
20. The solution should be able to address all aspects of the Advanced Persistent Threat (APT) lifecycle, including: Blocking known malware sources, blocking known malware, identifying and blocking unknown or zero-day malware attacks, protecting against client-side vulnerabilities, blocking command and control back-door traffic, blocking server-side vulnerabilities, and advanced application and user control.
21. The proposed solution must support sandbox based inspection and protection of unknown viruses and malware.

IV. Gateway Antivirus, Anti-Spyware and Anti-Spam

1. The proposed solution should have an integrated Anti-Virus capability.
2. The proposed solution should have an EAL4+ / ICSA / West Coast Labs Checkmark certification.
3. The proposed solution must work as an SMTP proxy rather than an MTA or relay server.
4. The proposed solution should support scanning for SMTP, SMTPS, POP3, IMAP, FTP, HTTP, HTTPS, web sockets and FTP over HTTP protocols.

5. The proposed solution should be able to detect the latest phishing URLs in email content and warn the end-user.
6. The basic virus signature database of the proposed solution should comprise all wild list signatures and variants, as well as those for malware, like phishing and spyware.
7. The basic virus signature database of the proposed solution should comprise of all the viruses "in the wild" and variants. Further, it should also contain database of all known malware/spyware used for phishing and accessing/stealing information without the end user's knowledge.
8. The proposed solution should be able to block dynamic/executable files based on file extensions.
9. The proposed solution should support multiple customizable antivirus policies based on user groups and applications.
10. The proposed solution should update the signature database at a frequency of less than one hour and it should also support manual updates.
11. For POP3 and IMAP traffic, the proposed solution should strip the virus infected attachment and then notify the recipient and the administrator.
12. The proposed solution should scan http traffic based on username, source/destination IP address and URL based regular expressions.
13. The proposed solution should provide the option to bypass scanning for specific HTTP traffic.
14. The proposed solution should support real mode and batch mode for HTTP virus scanning.
15. The proposed solution should be able to scan files irrespective of the filename extension.
16. The proposed solution should be able to provide reports based on username, IP address, sender, recipient, virus names and time window etc from archived data.

V. Web Filtering:

1. The solution should protect users from downloading virus/malware- embedded files by stopping viruses/malware at the gateway itself. It should provide real-time security scanning.
2. The proposed solution should stop incoming malicious files with updated signatures & prevent access to malware-infected websites and unblock the sites when the threats have been removed.
3. The proposed solution should be able to categorize URLs into at least 75 predefined categories, and the categories should be customizable. The solution should have the capabilities to block, permit, allow & log protocols HTTP, HTTPS, FTP, Web socket and others. It should also list the protocols that it supports.
4. The proposed solution should have the ability to identify and block proxy avoidance techniques, for example, Tor network, open Internet VPN sites.
5. The proposed solution should provide cloud-based web categorization for real time filtering and zero day attacks.
6. The proposed solution must be able to work as a standalone transparent proxy.
7. The proposed solution must have the following features built in:
    a) Should be able to block HTTPS based URLs
    b) Should be able to block URLs based on regular expressions
    c) Should support exclusion list based on regular expressions
    d) Should be able to block any HTTP / HTTPS upload traffic
    e) Should be able to block Google cached websites based on category.

f) Should be able to block websites hosted on Content Distribution Network companies such as Akamai.
g) Should be able to identify and block requests coming from a host behind a proxy server on the basis of username and IP address.
h) Should be able to identify and block URL translation requests.

8. The proposed solution should support application control blocking features as follows
    a) Should be able to block known chat applications like Yahoo, MSN, AOL, Google, Rediff, Jabber, WhatsApp, Viber etc.
    b) Should support YouTube Education Filter
    c) Should support blocking of File transfer on known Chat applications and FTP protocol.

9. The proposed solution must block HTTP or HTTPS based anonymous proxy requests.
10. The proposed solution should allow customization of Access Denied message for each category.
11. The proposed solution should be CIPA compliant and should have predefined CIPA based Internet access policy.
12. The proposed solution should be able to classify traffic as Productive and Non-productive, as specified by administrator.
13. The proposed solution should have specific categories that broadly classify websites. For eg. Websites that reduce employee productivity, bandwidth choking sites or malicious websites.
14. The proposed solution should be able to generate reports based on username, IP address, URL, groups, categories and category type.
15. The proposed solution should support creation of Internet access policies based on time etc. for individual users or user group.
16. The proposed solution must provide logging and extensive controls on Instant Messaging (IM) traffic for Yahoo and MSN messengers such as log of chat sessions for all or specific set of users.

VI. Virtual Private Network

1. The proposed solution should have an EAL4+ / ICSA / West Coast Labs Checkmark certification.
2. The proposed solution should support IPsec (Net-to- Net, Host-to-Host, Client-to-site), L2TP, PPTP and SSL VPN connections.
3. The proposed solution should support DES, 3DES, AES encryption algorithms.
4. The proposed solution should support pre-shared keys as well as digital certificate based authentication.
5. The proposed solution should support multiphase IPSec VPN negotiations.
6. The proposed solution should support external certificate authorities.
7. The proposed solution should support export facility for Client-to site configuration which ensures hassle-free VPN configuration in remote Laptops/Desktops.
8. The proposed solution should support commonly available IPsec VPN clients.
9. The proposed solution should support local certificate authority & should support creation/renewal/deletion of self-signed certificates.

10. The proposed solution should support VPN failover for redundancy purposes wherein more than one connection is grouped together. If one connection goes down, it automatically switches over to another working connection, ensuring zero downtime.
11. The proposed solution should support threat free IPsec/L2TP/PPTP VPN tunneling.
12. The proposed solution must support VPN client from Apple iOS, Windows mobile and Android.
13. The proposed solution must provide on-appliance SSL VPN solution with Web Access (Clientless), Web Application Access (most commonly used protocols), Full Tunnel and Split Tunnel control. The solution should provide per user / group SSL VPN access (which involves free licenses for unlimited users).

VII. Logging and Reporting

1. The proposed solution must support authentication to comply with Internet Privacy laws.
2. The proposed solution must have on-appliance / dedicated server reporting solution.
3. The proposed solution should interwork with any reporting solution.
4. The proposed solution should allow exporting of reports in PDF, HTML and CSV formats.
5. The proposed solution should support secure logging of Antivirus, Antispam, Content Filtering, Traffic discovery, IPS, Firewall activity on syslog compatible server.
6. The proposed solution should provide detailed reports for all files uploaded via the HTTP or HTTPS protocol. The report should include username/IP address/URL/File name/Date and Time.
7. The proposed solution should provide data transfer reports on the basis of application, username and IP address.
8. The proposed solution should provide connection-wise reports for user, source IP, destination IP, source port, destination port or protocol.
9. The proposed solution should facilitate sending of reports on email addresses.
10. The proposed solution should provide audit reports in compliance with SOX, HIPAA, PCI, FISMA and GLBA.
11. The proposed solution should support auditing facilities to track all activity carried out on the appliance.
12. The proposed solution should support multiple syslog servers for remote logging.
13. The proposed solution should forward logging information of all modules to syslog servers.
14. The proposed solution should have customizable email alerts/automated report scheduling
15. The proposed solution should provide reports for all blocked attempts by users/IP addresses.
16. The proposed solution must be capable of analyzing logs and reports derived from proprietary devices including UTMs, Proxy Firewalls and Syslog-compatible devices.
17. The proposed solution must be capable of providing Multiple Dashboard Report, along with the facility to customize the dashboards.
18. The proposed solution should be capable of forensic analysis to help organizations reconstruct the sequence of events that occurred at the time of a security breach.
19. The proposed solution should provide zone-based reporting.
20. The proposed solution should provide complete BYOD visibility.
21. The proposed solution should support customizable logging levels (verbose to minimal).
22. The proposed solution should allow rebranding or customization of reports.
23. The Proposed solution should provide report for hacking attempts / attacks on web server.

VIII. Application Control Solution

1. The proposed solution must provide inbuilt Application Filtering and control solutions.
2. The proposed solution must identify (Allow/Block/Log) the applications regardless of port, protocols and encryption, including SSL/TLS.
3. The proposed solution's application database must get updated automatically without any manual intervention.
4. The proposed solution must give identity based reports (username along with IP).
5. The proposed solution must be capable of blocking the following type of applications:
6. Applications that allow file transfer
    a) Online Games
    b) Instant Messengers (Including Non-English Versions).
    c) Peer-to-Peer (P2P) applications (Including Non-English Versions)
    d) Browser Based Web Proxy (Regardless of IP address or Port Number)
    e) Web 2.0 based applications (Facebook, CRM etc.)
    f) Applications that provide Remote Control
    g) All type of streaming media (Both Web and Software Based)
    h) VOIP Applications
7. The proposed solution must be capable of identifying hidden applications running over standard ports (80, 443, 22 etc.)
8. Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance.
9. Application Intelligence should have controls for Instant Messenger, Peer-to-Peer and Malware Traffic etc.
10. The solution should allow for third party signature.

IX. Intrusion Prevention System (IPS):

1. The proposed solution should be Checkmark certified.
2. The proposed solution must provide protection from attacks like Mail Attack, FTP Attack, HTTP Attack, DNS Attack, ICPM Attack, TCP/IP Attack, DOS and DDOS Attack, TelNet Attack.
3. The proposed solution should support multiple customizable IPS policies based on Zones, Categories and user etc.
4. The proposed solution must provide SCADA-aware IPS with pre-defined category for ICS and SCADA signatures
5. The proposed solution should update the signature database automatically and it should also support manual updates.
6. The proposed solution should support Protocol Anomaly detection

X. Web Application Firewall (WAF):

1. The Proposed solution should have On Appliance WAF with Positive Protection Module and should be worked on Unique Intuitive Website Flow Detector Technology.
2. The Proposed solution must provide protection against SQL Injections, Cross-Site Scripting (XSS), Session Hijacking, URL Tampering, Cookie poisoning etc.

3. The Proposed solution should automatically identify and block manipulation of browser data to prevent attempts to escalate user privileges through cookie-poisoning, gain access to other accounts through URL query string parameter tampering, and more
4. The Proposed solution should support and protect web environments like IIS, Apache against manipulation of Web environment for malicious intentions.
5. The Proposed solution should also have feature like HTTPS(SSL) encryption offloading, Reverse Proxy for incoming HTTP/HTTPS traffic
6. The Proposed solution should provide alerts and logs showing type of attacks, sources and action taken
7. The Proposed solution should support for HTTP 0.9/1.0/1.1
8. The Proposed solution should support Minimum 10 servers

XI. Load Balance:

1. The UTM should support Active/Active High Availability feature.
2. The UTM should support Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing.
3. The UTM should support QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.
4. Proposed UTM solution must be capable to detect device failure, link and path failure
5. UTM appliance failover should be complete stateful in nature without any manual intervention.
6. Proposed UTM shall synchronize the following for HA:
   a) All sessions
   b) Decryption Certificates
   c) All threat and application signatures
   d) All configuration changes
   e) Forwarding Information Base (FIB) tables

XII. Bandwidth Management:

1. The UTM should support 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.

XII. License for UTM (Unified Threat Management)

Three Years comprehensive value subscription for Next Generation Firewall Appliance with Web and Application Filter, Web Application Firewall (WAF), IPS, Gate Way Antivirus, spyware, Anti-Spam, Outbound Spam Protection, Reporting Software, Firewall and VPN and 24*7 support License. License period will be counted after activation.

3. ACCEPTANCE CRITERIA:

The successful bidder has to implement the solution at the site and complete the necessary integration of the appliance with the core network infrastructure deployed at GVMC and demonstrate the performance of the equipment to the GVMC technical Team.

The GVMC technical team and the technical team of the successful bidder will arrive at a mutually acceptable acceptance test plan (ATP) which will form the basis of the acceptance.

The warranty services will start only after the appliance is accepted by the GVMC.

4. SERVICE LEVEL AGREEMENT

1. The bidder has to ensure that the solution proposed, as a total turnkey solution to meet the stated requirements, delivers an uptime guarantee of 99.5% measured on a monthly basis, with mean time to restore in the event of a failure not exceeding 4hours.
2. **In the event of a failure of any of the sub-systems or components of the proposed solution, the bidder has to ensure that the defects are rectified before the end of the next working day.**
3. Failure to meet the above requirement will result in extension of the warranty services by 3 days for delay of each day during the warranty period.
4. Therefore, the bidder along with the OEM has to put systems and processes in place to address the above during the period of the contract.

5. WARRANTY:

1. Warranty services for the system supplied by the successful bidder should be valid for a period of 3 years from the date of acceptance of the equipment. Warranty service charges (in Indian rupees) have to be explicitly mentioned as a separate line item in the Commercial Bid.
2. During the warranty period, the bidder shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all the systems supplied.
3. During the warranty period, the bidder shall attend to all the hardware problems on site and shall replace the defective parts at no extra cost to the purchaser.
4. During the warranty period, the bidder shall attend to all failures relating to software installation, configuration, management and performance. Periodic maintenance w.r.t. software upgrades, updates, and patches, as well as preventive maintenance, are the responsibilities of the bidder.

6. DELIVERABLES

During the deployment phase of the project GVMC, Visakhapatnam requires the following deliverables:

1. DEPLOYMENT PLAN

Written documentation of the deployment approach and recommendations for seamless integration of the UTM device in live network with minimum downtime.

2. DETAILED TECHNICAL REPORT

GVMC network specific document developed for the use of GVMC, Visakhapatnam technical staff which discusses: the methodology employed, positive security aspects identified, detailed technical vulnerability findings, an assignment of a risk rating for each vulnerability, supporting detailed exhibits for vulnerabilities when appropriate, and detailed technical remediation steps.

3. TRAINING

Appropriate number of training sessions for GVMC Technical staff for effective operations and management of the appliance.

4. PRESENTATION & EXECUTIVE SUMMARY REPORT

A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.

for Commissioner
GVMC, Visakhapatnam

Chapter 3: INSTRUCTIONS TO THE BIDDER

1. General instructions

The offers complete in all respect, in prescribed formats, should be submitted on or before the time and date fixed for the receipt of offers as set forth herewith in the tender documents. Offers received after stipulated time and date shall be summarily rejected.

2. Deposit of Earnest Money

a) Tenders submitted without Earnest Money deposit shall be rejected.

b) The bidder shall be required to deposit Earnest Money of **Rs. 28000 /- (Rupees Twenty Eight Thousand only)** through fixed deposit receipt / Bank guarantee/Bank Draft/Pay Order drawn in favor of the **COMMISSIONER, GVMC, VISAKHAPATNAM payable at Visakhapatnam from any Nationalized Banks in an acceptable form. The EMD must accompany the "Technical bid and Terms and conditions."** hereafter referred as 'Technical Bid', otherwise the offer shall not be considered.

c) The EMD shall remain deposited with GVMC till the period of validity of offer. No interest shall be payable by GVMC on EMD.

d) The EMD deposit is liable to be forfeited, if the bidder withdraws amends, impair or derogates from the tender in any respect, within the period of validity of his offer.

e) The EMD of the successful bidder shall be returned after the successful completion license period.

3. Last date for Submission of Tender Document:

Sealed Technical and Commercial Bids placed separately in a single sealed envelope complete in all respect, along with the earnest money, should reach to the Commissioner, GVMC, Tenneti Bhavan, Ramnagar, Visakhapatnam – 530002 by 3 PM on 10/08/2016 and shall be opened on same day at 4.00 PM.

4. Submission of Bid

a) The bidder should submit bids in two parts viz. 'Technical Bid' and 'Commercial Bid'. The Technical Bid should be sealed in a separate sealed envelope along with DD for EMD, subscribing '**Tender for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam'** and 'Commercial Bid' should be sealed in a separate sealed envelope subscribing '**Tender for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam".** Both Technical and Commercial Bid envelopes should be enclosed and sealed in a separate envelope marked as 'Bid for **Tender for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam**'. The bid should be addressed to: **The Commissioner, GVMC, Tenneti Bhavan, Ramnagar, Visakhapatnam – 530002.**

b) All prices and other such information like discounts etc. having a bearing the price shall be written both in figures and words in the prescribed form. All the papers submitted with the

bids as above for Technical and Commercial Terms and Conditions must be signed by the bidder. Where there is a difference between amount quoted in words and figures, the amount quoted in words shall prevail. The Excise Duty, Sales Tax, WCT, service tax or any other Govt. duties etc. as applicable should be quoted separately, failing which, GVMC shall have no liability to pay these charges, and the liability shall be that of the bidder.

c) Each page of the bids shall be numbered. It must bear the signature and seal of the bidder at the bottom. All offers shall be either typewritten or written neatly in indelible ink. Any correction should be properly authenticated.

5. Technical Bid

The Technical bid must be submitted in a **spiral bounded** report format containing the documents arranged and labeled as per the following index**. It may be noted that if the documents of Technical Bid are found without spiral binding, the same shall be summarily rejected.**

a) Covering letter duly signed by the authorized person **(Annexure –I).**
b) DD/Pay Order towards Earnest money.
c) Company Profile as per format in **Annexure – II.**
d) Documentary evidences in respect of eligibility criteria. Each document should be labeled on the top right so as to indicate the eligibility criteria serial number.
e) Letter from the Principal/OEM (in case of third party item) supporting the bidder for entire AMC period including.
a) Compliance to all terms and conditions laid down in this Tender Document. A copy of the tender document, duly signed on each page with seal, must be enclosed.
f) Compliance to the Scope of work laid down in this Tender Document.
g) Supporting technical material, including brochures
h) Any deviation to the scope of work or terms and conditions Failure of submission of any of the document in Technical bid will make the bid rejected as non responsive. GVMC will have the option to treat some documents as mandatory /optional in the benefit of the Municipal Corporation i.e GVMC.

Note: Technical Bid with loose or unlabelled papers will be summarily rejected.

6. Financial Bid

The Financial bid should be according to the format given in the Tender Document. The financial bid should contain followings:

a) Covering Letter from the Bidder duly signed.
b) Unit rate of Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam Chapter -4.
c) Taxes, if any must be indicated.
d) Total bid amount in terms of INR for a year covering all licenses in the chapter -5.

e) The Financial Bid shall be opened only for the technically short-listed vendors on specified date and time in GVMC. One representative from the company may be present, if they desire so, at the opening of the Financial Bid.

f) The commercial bid should contain among other things, payment terms, warranty, installation and commissioning charges. These charges will be paid only after successful supply, installation and acceptance. GVMC will enter into a contract with the successful bidder which will detail all contractual obligations during the warranty period.

g) **GVMC will select the vendor on the basis of overall lowest bid quoted by technically short-listed bidder.** The decision of the GVMC arrived at as above, shall be final and representation of any kind shall not be entertained on the above. Any attempt by any vendor to bring pressure of any kind may disqualify the vendor for the present tender and the vender may be liable to be debarred from bidding for the GVMC tenders in future for a period of three years.

h) GVMC shall have no obligation to convey reason for rejection of any bid. It shall be opened for GVMC to reject even the lowest bidder, in the interest of the Corporation and no reason need to be given thereof.

7. Clarification of Bids

To assist in the examination, evaluation and comparison of bids the GVMC may, at its discretion, ask the Bidder(s) for clarification(s) of the bid. The request for clarification and the response shall be in writing.

8. Effect and Validity of Offer

(a) The submission of any offer connected with these specifications and documents shall constitute an agreement that the bidder shall have no cause of action or claim, against GVMC for rejection of his offer. GVMC reserves the right to reject or accept any offer or offers at its sole discretion and any such action will not be called into question and the bidder shall have no claim in that regard against the maintenance service.

(b) The offer shall be kept valid for acceptance for a minimum period of **30** (Thirty) calendar days from the date of opening of Financial Bid.

(c) The offer shall be deemed to be under consideration immediately after they are opened and until such time the official intimation of award of contract is made by GVMC to the bidder. While the offer is under consideration, if necessary, GVMC may obtain clarification on the offer by requesting for such information from any or all of the bidders either in writing or through personal contacts as may be considered necessary. Bidder shall not be permitted to change the substance of their offer, after the offer has been opened.

(d) GVMC shall not be responsible for any delay in submission of the tender bids. The offer submitted by the bidder through ***telex/telegram/fax or e-mail would not be considered*** as a valid offer. No further correspondence will be entertained in this matter.

(e) In case of bidders whose tenders are not considered for placing order, the earnest money deposit shall be refunded without any interest within one month of the decision. In the case of bidders whose tender are accepted for placing the order, EMD Amount will be considered as Security Deposit, which will be valid for the entire period of the contract plus two months.

(f) In case GVMC notice that the market rates have come down from the time when rates were finalized in the rate contract/order or there is a need for re-asking the offer based on market trends, GVMC, may ask the technically short-listed vendors to re-quote the maintenance cost and the vendor shall be selected on the basis of procedure given earlier. The time difference between such re-quotes shall be minimum 3 month except in case of the Union Government budget.

GVMC reserves the right to award the contract to any of the bidders irrespective of not being lowest, taking into consideration the interest of GVMC and in this respect, decision of GVMC shall be final.

9. Tender Opening and Selection of ISO Certified Company for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam

Only the 'Technical Bids' part will be opened at the notified location on 10/08/2016 at 4:00 PM in the presence of bidders or their representatives, who wish to be present. Technical bids will be evaluated and after technical evaluation of the offer received, the financial bids of only those vendors who are found technically suitable shall be opened. Only technically qualified bidder will be informed by post/fax/phone/email about the opening of the Financial Bid at appropriate time.

Bidders will be selected by the following steps given as under:

a) Short-listing of eligible vendors satisfying the technical qualification requirements laid in this Tender document.
b) Selection of bidder as the Service Provider who offers the lowest price and meets the commercial qualification requirements from the technically qualified short listed vendors.

c) If GVMC considers necessary, revised financial bids may be asked from the short listed vendors. Such bids should be submitted **within two days of the intimation to this effect in sealed envelopes on specified date and time.** The revised bids shall not be for amount more than the one quoted earlier for an item. **Any vendor quoting higher rates for the same item quoted earlier in their revised bid shall be disqualified for further consideration and EMD submitted may be forfeited**.

10. Acceptance of offer

The tender shall be processed as per standard procedure. GVMC, however, reserves the right to reject any tender without disclosing any reason. GVMC would not be under obligation to give any clarifications to those vendors whose tenders have been rejected.

11. Signing of Agreement

The successful bidder(s) shall execute an Agreement as per the format prescribed by GVMC based on this Tender Document and agreed Terms and Conditions.

for Commissioner
GVMC, Visakhapatnam

Chapter 4:

Annexure - I

BID PROPOSAL SHEET/FORWARDING LETTER

Bidder's Proposal Reference No. & Date:

Bidder's Name & Address:

Person to be contacted:

Designation:

Telephone No.: Fax No.: E-Mail Id:

The Commissioner
GVMC,
Visakhapatnam
530002

Subject: Tender for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam.

Dear Sir,

We, the undersigned Bidder, having read and examined in detail the specifications and scope of the work as specified in the tender document and all other bidding documents in respect of **Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam** do hereby propose to provide the services as in the bidding document.

PRICE AND VALIDITY

All the prices mentioned in our proposal are in accordance with the terms as specified in bidding documents. All the prices and other terms and conditions of this proposal are valid for a period of 90 calendar days from the date of opening of financial bids.

EARNEST MONEY

We have enclosed the required earnest money in the form of Bank Draft/Pay Order/ _____ Bank Guarantee in the Technical Bid. The details are as under:

Earnest Money Amount: Rs_____

DD/Pay Order No. _____Date_____ Bank and Branch_____

DEVIATIONS

We declare that all the services shall be performed strictly in accordance with the Technical specifications and terms mentioned in the Tender document. No Technical deviation will be acceptable and any technical deviation is liable to the rejection of tender.

BID PRICING

We further declare that the prices stated in our proposal are in accordance with your Terms & Conditions in the bidding document. We further understand that the quantities as specified in this Tender may increase or decrease at the time of Award of Purchase Order or at a later stage as per the requirements of GVMC.

QUALIFYING DATA

We confirm that we satisfy the qualifying criteria and have attached the requisite documents as documentary proofs. In case you require any further information/documentary proof in this regard during evaluation of our bid, we agree to furnish the same in time to your satisfaction.

We hereby declare that our proposal is made in good faith, without collusion or fraud and the information contained in the proposal is true and correct to the best of our knowledge & belief.

We understand that the GVMC is not bound to accept the lowest or any bid that it may receive.

Thanking you,

Yours faithfully,

(Authorized Signatory)

Date:
Place:
Business Address:

Name:
Designation:
Seal

ANNEXURE- II

Technical Bid

Sl No	Description of Company / Firm	Detailed to be filled up	Page Number of this tender Document where copy /certificate is attached
1	Name of Firm/Company		
2	Address		
3	Telephone No.		
	Mobile		
	Fax:		
4	Type of Organization (whether sole proprietorship/ partnership/private limited or		
5	Name of the Proprietor/ Partners/Directors of the Organization/Firm		
6	Service Tax No & VAT Nos. of the Firm		
7	TAN number of the firm / company		
8	PAN number of the firm/ company		
9	letter of Authorization from OEM		
10	Total number of Engineers working in the Organization		
11	Whether EMD submitted or not indicate the BC / DD No. and date with amount of the EMD Yes/No)		
12	(**Average annual**)**turnover of the Company of Rs. 5.00 Cr. in the last three years with the Details of the Net Profit & Loss**		

	duly certified by CA. **2013-14**		
	2014-15		
	2015-16		
13	ITR of Company for the last three years, **2013-14, 2014-15, 2015-16 (Proof enclosed)**		
14	DD/Pay Order/Cash Receipt toward tender document fee		
15	ISO Certified or equivalent **(Attach certificate)**		
16	Service Centre in Visakhapatnam. Please confirm (Proof enclosed) (Authorized Signatory of the firm)		
17	**Details of Organization provided to antivirus solution (for 3 Companies)** **(Proofs to be attached)** Name of the organization Contact Person		

(Authorized Signatory of the firm)

Annexure – III

Commercial Bid

Tender for Supply, installation, Configuration, Training and Onsite support of Next Generation Firewall Appliance for GVMC, Visakhapatnam

Sl NO	Material Description	Total Qty	Quoted Price (Rs) (Inclusive of all taxes)	Total Quoted Amt (Rs)
1	**Cyberoam CR750iNG-XP Next Generation Firewall Appliances with 3 years comprehensive value subscription for Network Security and all the specifications mentioned in "Chapter-2"** a) Web and Application Filter b) IPS c) Gateway Antivirus d) Gateway Anti Spam e) Web Application Firewall f) Outbound Spam Protection g) Reporting Software h) Firewall and VPN i) 24X7 Support	**01**		

Total in Figures = (Rs. _____)

Total in Words = (_____)

(Authorized Signatory)

for Commissioner
GVMC, Visakhapatnam