MORMUGAO PORT TRUST
FINANCE DEPARTMENT
(INFORMATION TECHNOLOGY CELL)

Ref.No. FA/IT(7-NW)/2016/165 **Date : 18.07.2016.**

Subject : Limited Tender Enquiry for **Supply, Installation, Testing and Commissioning Of Next Generation Firewall.**

Dear Sir,

Sealed Bids in two parts (Cover I - Technical Bid & Cover II – Price Bid) are invited for **Supply, Installation, Testing and Commissioning Of Next Generation Firewall.** Interested firms may send their bids in a sealed covers as per instructions specified in Terms and Conditions (Part – I of the Tender) addressed to **Asst. Director (EDP), IT Cell,1st Floor, Main Administrative Building, Headland Sada, Goa – 403 804.(Phone Nos.: 0832 – 2594416, 2594419)** latest by 15:00 hrs. on 28th July 2016 (Wednesday). Technical Bids will be opened on the same day at 15:30 hrs. in the office of Asst. Director(EDP) in the presence of interested bidders or their authorized representatives.

The quotation without EMD will not be considered.

Mormugao Port Trust is not responsible for any transitional/postal delays.

.

Mormugao Port Trust reserves the right to accept or reject any quotation in full or part thereof without assigning any reason.

The Terms and Conditions of the tender are specified in Part – I of the tender.

The specifications for supply, installation, testing and commissioning of UTM/Next Generation Firewall are specified in Part-II of the tender.

Yours faithfully,

Financial Adviser &
Chief Accounts Officer

PART – I

TERMS AND CONDITIONS

The Terms and conditions governing the **"SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL as per specifications at Annexure I at MPT, GOA**" are as follows.

1) The technical and Price Bids should be submitted in two separate sealed covers, super scribing **"Part-I Technical Bid for "SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL" Tender No., due date and "Part-II Price Bid for "SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL" Tender No., due date. Both the bids should be kept in a single cover by super scribing tender for "SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL"** sealed and addressed to Asst. Director(EDP), Finance Department, Mormugao Port Trust, Headland Sada, Goa-403 804. **Offer sent through fax will not be accepted.**

2) The Minimum Eligibility Criteria is as follows :

2.1) The Bidder should have experience in supply, installation & commissioning of firewalls having executed two orders of minimum value of Rs. 4 lakhs each during the last three years.

2.2) The bidder if not OEM, should obtain authorization from the OEM of firewall as per format specified in Annexure.

2.3) The firewall to be supplied should be as per specifications indicated in Part II of the tender.

3) Overwriting and corrections should be attested properly. The bid should be complete in all respects and should be duly signed. Incomplete and unsigned bids will not be considered at all.

4) All relevant technical literature pertain to items quoted **with full specifications** (Drawing, if any), information about the products quoted, including brochures if any should be included in the Technical Bid.

5) A list of **reputed clients** to whom the firm has supplied similar items to be included in the technical bid.

In the TECHNICAL BID, the Bidder should furnish the Name and address of the Purchasers placed orders on similar equipment with order No, date, Description and quantity, Date of Supply along with Contact person Telephone No, Fax No, and e mail address of Purchaser along with copies of respective Purchase Orders.

6) Bid should be **valid for a period of 90 days** from the date of tender opening.

7) The Supply, installation, testing and **Commissioning of the firewall** has to be completed within three weeks from the date of Purchase Order. If the supplier fails to carry out the commissioning of the firewall, MPT reserves the right to **levy liquidated damages** at the rate of 0.5% per week or part thereof up to maximum of 5%.

8) Warranty shall commence from the date of installation and acceptance of the complete equipment supplied under the Purchase Order / Contract.

9) **Technical bid should contain EMD.**

Bidders shall submit **EMD** along with their tender, by **Demand Draft** drawn in favor of MPT, on any nationalized bank for a sum of Rs.14,000/- (Rupees Fourteen Thousand only) payable at Mormugao Harbour/Vasco-da-Gama only.

Tender without EMD in the envelope containing technical bid shall be summarily rejected. The EMD of unsuccessful bidders shall be returned within 30 days of the award of contract.

The earnest money will be liable to be forfeited, if the tenderer withdraws or amends/impairs or derogates from the tender if any respect within the period of validity of his tender.

10) Please **specify the Make/Brand** and Name of the Manufacturer with address, country of origin.

11) The Purchaser requires that the bidders, suppliers and contractors observe the highest standard of ethics during the procurement and execution of such contracts. In pursuit of this policy, the following are defined:

"Corrupt practice" means the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of a public official in the procurement process or in contract execution:

"Fraudulent practice" means a misrepresentation or omission of facts in order to influence a procurement process or the execution of contract;

"Collusive practice" means a scheme or arrangement between two or more bidders, with or without the knowledge of purchaser, designed to establish bid prices at artificial, noncompetitive levels; and

"Coercive practice: means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the procurement process or affect the execution of contract;

The purchaser will reject a proposal for award if it determines that the Bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for the contract in question; The Decision of Tender Committee, MPT shall be final and binding.

12) Bidders that do not manufacture the goods it offers to supply shall submit Manufacturer's/OEM's Authorization form on the letterhead of the Manufacturer duly signed and stamped by a person with the proper authority to sign documents that are binding on the Manufacturer as per the format specified in Annexure II should be submitted failing which the quotation will not be considered.

13) **The order acknowledgement** should be from the principals and if the Indian Agent is empowered to quote and to furnish order acknowledgement, a copy of agreement entered by you with the Indian Agent to be furnished.

14) **Compliance Statement:** Equipments point-by-point comparison/compliance statement with **technical specifications** indicated in the tender as per Annexure I, should be enclosed in the Technical Bid as well as any other extra features of the equipment be shown separately therein.

15) Prices quoted in the Price Bid should be in Indian rupees only. The Price Bid should be written both in words and figures at appropriate place as per format provided Annexure V.

16) **Technical Bid should contain** all details and specifications of the equipment offered, UTM device comprehensive warranty, subscription licenses, installation, training, post-warranty, service support **WITHOUT PRICE** and **Price Bid should contain** details of the price(s) of the item(s) quoted in the technical bid. The Technical bid should not contain any references to the pricing.

In case the technical bid contains any direct or indirect reference to quoted price the bid is liable to be rejected.

17) The prices quoted in the price bid should include the cost of packing, forwarding and freight for delivery to MPT, Goa. The Price Bid/financial quote should in the format specified at Annexure V.

18) Tender Committee reserves the right to open the bids. Only technical bids will be opened on the date and time mentioned in the tender document. The price bids of those tenderers whose technical bids are found to be meeting our specifications only will be opened in their presence at date and time to be notified later.

19) The firm to the full satisfaction of the MPT should carry out the **installation and commissioning of the Firewall** at the MPT premises **within a period of three weeks from the date of Purchase Order**.

20) Asst. Director(EDP) or any officer designated by him will assess the product supplied/installed for their quality and their conformity to the specifications provided by the firm in their quotations. Any item(s) identified by the Asst. Director(EDP) to be not as per the specifications or are found to be of inferior quality will be rejected, and the bills towards the supply will not be processed for payment till proper replacements are provided.

21) **No advance payment** will be made. Payment shall be made after supply, installation and acceptance of the equipment by MPT. The payment will be authorized after submission of a Bank Guarantee for 10% value of the order towards warranty guarantee. The **performance Bank Guarantee** as per format specified in Annexure VI should be furnished within 15 days from the date of placement of order from a reputed bank (scheduled bank in India **or** foreign bank operating in India) valid till 180 days after the warranty period.

22) Supplier should undertake to support the product for a minimum period of 5 years (post-warranty).

23) In the event of failure of firewall appliance during the three years of comprehensive warranty/support, the supplier should provide compatible appliance within 24 hours and retain the same till the defective unit is replaced.

24) Two sets of operational, service/troubleshooting manuals and diagrams to be supplied with "**SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION /UTM FIREWALL".**

25) **The submission of tender** shall be deemed to be an admission on the part of the tenderer that he had fully acquainted himself with the specifications, drawings etc. and no claim other than what stated in the tender shall be paid in the event of award of Purchase Order.

26) Expenditure involved towards any extra materials required for labour involved for successful installation of the equipment, if not quoted for, would have to be borne by the tenderer.

27) **Acceptance of this tender** form and submission of the quote within the stipulated time would be treated as:

27.1) The tenderer has understood all requirements as described in our Tender document.

27.2) Acceptance to provide/establish all the facilities mentioned in our tender without any price escalation, if the tenderer finds it necessary to add any hardware or software or any other materials during implementation.

27.3) Agreeing to execute order to the satisfaction of MPT or its authorized representatives within the stipulated time.

28) **Installation and Training charges** should be clearly indicated including the scope of training.

29) Tender should clearly define the **infrastructure facilities required** for installation and commissioning of the equipment.

30) MPT will not be liable for any obligation until such time MPT has communicated to the successful bidder of its decision to release the Purchase Order.

31) **MPT will not be responsible for any postal delays.**

32) Bidders shall note that MPT will not entertain any correspondence or queries on the status of the offers received against this Tender Invitation.

33) Tenders from Manufacturers/Suppliers/Tenderers whose performance was not satisfactory in respect of quality of supplies and delivery schedules in any organizations, are liable for rejection. The tenders that do not comply with the above criteria and other terms & conditions are liable for rejection.

34) MPT does not bind to accept the lowest quotation and reserves the right to himself, to reject or partly accept any or all the quotations received without assigning any reason.

35) All disputes arising in connection with executing the purchase order will be subject to the Jurisdiction of the Courts in Goa only.

PART - II

TECHNICAL SPECIFICATIONS FOR SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF UTM/NEXT GENERATION FIREWALL.

Sl. No.	Technical Specifications
1	The Firewall must be appliance based and should facilitate multi-application environment.
2	The Firewall should be ICSA Labs certified for ICSA 4.0 and EAL 4 certified, if not the same model
3	The platform should be based on real-time, secure embedded operating system
4	Should support minimum 10 virtual firewall or more
5	The proposed system shall support unlimited IP/User license for Firewall / VPN (IPSec & SSL)/ IPS/WCF/AV
6	Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance
7	The device should belong to a family of products that attains NSS Approved (UTM) Certification
8	The device should belong to a family of products that attains IPv6 Ready Phase 2 & IPv6 Certification
9	Proposed Firewall Vendor should be in the Leaders' Quadrant of Gartner Magic Quadrant for the last 4 consecutive years in UTM.
10	The OEM must attain ISO certification that covers scope of the Quality Management System which includes the design, development and manufacturing of network security products and the delivery of associated security services and support
11	OEM should have direct technical support centre in India.
12	OEM should have direct RMA Centre in India for Hardware Warranty.
13	OEM should have direct product training facility with certified trainer in India. And should provide training to Tow person of organization along with product certification.
14	The Firewall Appliance should be rack mountable and shall not exceeding 2U
B.	**Networking & System Performance Requirements:**
1	The Firewall should support a minimum of 16 x 10/100/1000 interfaces & 2 X 10/100/1000 SFP Fiber Interface with auto sensing capacity
2	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
3	The Firewall should support IEEE 802.1q VLAN Tagging with about 1024 VLANs supported (in NAT/Route mode)
4	Should support automatic ISP failover as well as ISP load sharing for outbound traffic
5	The Firewall should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS, RIPng
6	The Firewall should support Static, Policy Based, and Multicast routing
7	The Firewall should support throughputs of 3 Gbps or better for both small & large packets
8	The firewall should support throughput of at least 1.3 Gbps of AES - IPSEC VPN
9	Should support concurrent session more than 3 Million
10	Should support new session per second more than 75,000
11	Should support and IPS throughput of 1.7 Gbps or better
12	Should support and GAV throughput of upto 1100 Mbps

13	Should support Site to Site VPN Tunnels up to 2,000
14	Should support Client to Site VPN Tunnels up to 2,000
15	Should support firewall Policies minimum 10,000
16	Should support End Point Protection Client up to 1000
17	Should support Access Point Centralize Management minimum 200 AP
18	Should support Two Factor Authentication Token minimum 900
C.	**Operating System & Management Requirements:**
1	Be proprietary to prevent inheriting common OS vulnerabilities
2	Resided on flash disk for reliability over hard disk
3	Allow multiple OS firmware image for booting options
4	Upgradeable via Web UI or TFTP
5	Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk
6	The system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access
7	The proposed system shall be able to limit remote management access from certain trusted network or host with corresponding administrator account
8	The proposed system should be able to facilitate administration audits by logging detailed activities to event log for management & configuration updates
9	The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACAS+
10	The Firewall must be capable of clustering multiple firewalls together into a redundant and highly available active-active configuration without any extra license cost for creating HA.
D.	**Firewall Requirements:**
1	The Firewall should support deployment modes as; “Stealth Mode” or “Route Mode" or "Transparent Mode” or "Proxy Mode".
2	The proposed system should have integrated Traffic Shaping / QoS functionality
3	Should support DHCP server & DHCP Agent functionality
4	The Firewall should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)
5	The Firewall should support Inbound Port Forwarding with optional inbound Load Balancing
6	Should support IPv6 ACL to implement security Policy for IPv6 traffic
7	All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc
8	Should be able to inspect HTTP and FTP traffic when these are deployed using non standard port (i.e when HTTP is not using standard port TCP/80)
E.	**High Availability Requirements:**
1	The firewall must support Active-Active as well as Active-Passive redundancy.
2	The Firewall must support clustering of multiple active firewalls, and the firewalls must load balance the traffic between them to share the load.
3	The cluster should support simple and minimal downtime during upgrade
F.	**IPSEC VPN Requirements:**
1	The IPSEC VPN and SSL VPN capability shall minimally attain Internet Computer Security Association (ICSA) Certification or equivalent
2	The proposed system shall comply/support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional external solution, hardware or modules:

3	The device shall utilize inbuilt hardware VPN acceleration supported for:
3.1	IPSEC (DES, 3DES, AES) encryption/decryption
3.2	SSL encryption/decryption
4	The system shall support the following IPSEC VPN capabilities:
4.1	Multi-zone VPN supports.
4.2	IPSec, ESP security.
4.3	Supports Aggressive and Dynamic mode
4.4	Support perfect forward secrecy group 1 and group 2 configuration
4.5	MD5 or SHA1 authentication and data integrity.
4.6	Automatic IKE (Internet Key Exchange) and Manual key exchange.
4.7	Supports NAT traversal
4.8	Supports Extended Authentication
4.9	Supports Hub and Spoke architecture
4.10	Supports Redundant gateway architecture
4.11	DDNS support
G.	**SSL VPN Requirements:**
1	The Firewall should be integrated solution and there should be no user based licensing for SSL VPN.
2	The Firewall should support for TWO modes of SSL VPN:
2.1	Web-only mode: for thin remote clients equipped with a web browser only and support web application such as: HTTP/HTTPS PROXY, FTP, SMB/CIFS, SSH, VNC, RDP
2.2	Tunnel mode, for remote computers that run a variety of client and server applications
3	The system shall provide SSL VPN tunnel mode that supports 32 and 64-bit Windows operating systems
4	The proposed solution shall allow administrators to create multiple bookmarks to add to a group and make these bookmarks available for SSL-VPN users.
H.	**Network Intrusion Detection & Prevention System Requirements:**
1	The IPS capability shall minimally attain Internet Computer Security Association (ICSA) NIPS or NSS Certification
2	Should have a built-in Signature and Anomaly based IPS engine on the same unit
3	Able to prevent denial of service and Distributed Denial of Service attacks.
4	Signature based detection using real time updated database
5	The device shall allow administrators to create Custom IPS signatures
6	Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.
7	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)
8	Security check updates do not require reboot of the unit.
9	Supports attack recognition inside IPv6 encapsulated packets.
10	Supports user-defined signatures with Regular Expressions.
11	Supports several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc. List all prevention options
12	SSL Inspection for IPS
I.	**Antivirus System Requirements:**
1	The Antivirus capability shall minimally attain Internet Computer Security Association (ICSA)/equivalent AV Certification
2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy

3	The System should be able to scan following Protocols:
3.1	HTTP and HTTPS
3.2	SMTP, SMTPS
3.3	FTP, FTPS
3.4	POP3, POP3S
3.5	IMAP, IMAPS
3.6	Instant Messenger (AIM, YAHOO!, MSN, ICQ, SIMPLE)
3.7	NNTP
4	The proposed system shall provide ability to allow, block and intercept (allow but quarantine) attachments or downloads according to file extensions and/or file types
5	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
6	The solution should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus
J.	**Web & Application Content Filtering System Requirements:**
1	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.
2	URL database should have minimum 200 million sites and 75 + categories.
3	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
4	Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies.
5	Shall include Web URL block
6	Shall include Web Exempt List
7	The proposed solution should be able to replace the web page when the web page matches the Web Filtering blocking criteria.
8	The proposed solution shall be able to identify, retrieve and rate the actual URL of the cache content commonly available in search engines such as Yahoo and Google.
9	The solution shall allow administrators to create multiple new local URL filtering categories besides dynamic categories
10	Should have application control feature
11	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, BitTorrent etc.
12	Should have minimum database of 3300 types of application awareness
K.	**Data Leak Prevention Requirements:**
1	Should have the ability to prevent data loss through SMTP, SMTPS, FTP, HTTP, HTTPS & IM
2	Should have built in pattern database
L	**User Authentication**
1	The proposed Firewall shall be able to support various form of user Authentication methods simultaneously , including:
2	Local Database entries
3	LDAP server entries
4	RADIUS server entries
5	TACACS+ server entries
6	Native Windows AD (Single sign on capability)
7	Two-factor authentication without any external Hardware.
8	Citrix Agent support for Single Sign On

9	The solution shall be capable of providing Windows AD single sign-on by means of collector agents which broker between users when they log on to the AD domain and the device.
10	The proposed appliance shall support inbuilt 2 factor authentication services and database using tokens, email and SMS. Hardware Token supported should be 1000. If this service is not available on the box, provide an external server for authentication.
11	System should also have capability to identify devices (ex. Android, Iphone, Windows etc) & should be able to write policies on basis of device identity
12	Should also support Authentication-based routing
M	**Wireless Security**
1	Integrated wireless Controller support required & Number of Manageable Wireless access points support required
2	Wireless Security features like WEP,WPA-PSK & WPA-ENT should be supported
3	Should have a inbuilt DHCP Server to assign IP Addresses to specific SSID's and should support DHCP Relay
4	Should have ability to detect wireless as well as on-wire rogue AP
5	Total number of AP's supported 512
6	Should support on-box Guest Management Feature
7	Administrators shall be able to setup per SSID, a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.
8	Administrators shall be able to view client monitor which illustrate wireless access situation
9	Wireless Deployment should support wired AP's i.e AP's connected on LAN as well as Wireless Bridged AP's i.e AP's connected by Wireless backhaul.
10	Should support Wireless IDS for following types of intrusion detection among others:
11	1.1 Unauthorized Device Detection
12	1.2 Rogue/Interfering AP Detection
13	1.3 Adhoc Network Detection and Containment
14	1.4 Wireless Bridge Detection
15	1.5 Misconfigured AP Detection
16	1.6 Weak WEP Detection
17	1.7 Multi Tenancy Protection
18	1.8 MAC OUI Checking
N	**BYOD**
1	create policies based on device type
2	identify and monitor the types of devices connecting to your networks, wireless or wired
3	use MAC address based access control to allow or deny individual devices
4	enforce endpoint control on devices that can run Client Endpoint Control software
O	**Client Reputation**
1	Should be able to provide information by tracking client behavior and reporting on the activities you determine are risky or otherwise noteworthy.
2	Bad Connection Attempts
3	Packets that are blocked by deny security policies.
4	Intrusion Protection
5	Malware Protection
6	Web Activity
7	Application Protection
8	Geographical locations that clients are communicating with.
P	**End Point Protection**

1	The solution should have Anti-virus, Web filtering, Application Control, IPSec & SSL VPN, vulnerability scan etc features.
2	The solution should have VB100 certification
3	The solution should support Android & iOS along with Windows & MAC
4	Should be managed from a single console
5	Can be deployed in the network through Active Directory
6	Should have the feature of rootkit removal
7	Should identify system & application vulnerability
8	Should have the application firewall protection to block any specific application
9	Should have the option of creating customized MSI installer package
10	The software should support windows XP or higher
11	Should have the quarentine feature
12	The solution can work standalone or centrally managed
13	Should have the client certificate support
Q	**Support and Warranty**
1	Should have 24X7 Warranty and Support from OEM for Product Hardware and Firmware/OS
R	**License**
1	Commercials need to be quoted for Three Years 24X7 Fully Bundle Hardware Appliance with licenses and features as per above specification. (Exp. Gateway Antivirus, spyware, web/url filtering, content and application filtering, SSL VPN & IPS) all Hardware Component and Licenses should be installed from day one and License period will be counted from date of activation.

Annexure I

TECHNICAL COMPLIANCE STATEMENT FOR SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL.

Sl. No.	Specification	COMPLIED/ NOT COMPLIED	EXTRA FEATURES
1	The Firewall must be appliance based and should facilitate multi-application environment.		
2	The Firewall should be ICSA Labs certified for ICSA 4.0 and EAL 4 certified, if not the same model		
3	The platform should be based on real-time, secure embedded operating system		
4	Should support minimum 10 virtual firewalls or more		
5	The proposed system shall support unlimited IP/User license for Firewall / VPN (IPSec & SSL)/ IPS/WCF/AV		
6	Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance		
7	The device should belong to a family of products that attains NSS Approved (UTM) Certification		
8	The device should belong to a family of products that attains IPv6 Ready Phase 2 & IPv6 Certification		
9	Proposed Firewall Vendor should be in the Leaders' Quadrant of Gartner Magic Quadrant for the last 4 consecutive years in UTM.		
10	The OEM must attain ISO certification that covers scope of the Quality Management System which includes the design, development and manufacturing of network security products and the delivery of associated security services and support		
11	OEM should have direct technical support centre in India.		
12	OEM should have direct RMA Centre in India for Hardware Warranty.		
13	OEM should have direct product training facility with certified trainer in India. And should provide training to Tow person of organization along with product certification.		
14	The Firewall Appliance should be rack mountable and shall not exceeding 2U		
B.	**Networking & System Performance Requirements:**		
1	The Firewall should support a minimum of 16 x 10/100/1000 interfaces & 2 X 10/100/1000 SFP Fiber Interface with auto sensing capacity		
2	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.		
3	The Firewall should support IEEE 802.1q VLAN Tagging with about 1024 VLANs supported (in NAT/Route mode)		
4	Should support automatic ISP failover as well as ISP load sharing for outbound traffic		

5	The Firewall should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS, RIPng		
6	The Firewall should support Static, Policy Based, and Multicast routing		
7	The Firewall should support throughputs of 3 Gbps or better for both small & large packets		
8	The firewall should support throughput of at least 1.3 Gbps of AES - IPSEC VPN		
9	Should support concurrent session more than 3 Million		
10	Should support new session per second more than 75,000		
11	Should support and IPS throughput of 1.7 Gbps or better		
12	Should support and GAV throughput of upto 1100 Mbps		
13	Should support Site to Site VPN Tunnels up to 2,000		
14	Should support Client to Site VPN Tunnels up to 2,000		
15	Should support firewall Policies minimum 10,000		
16	Should support End Point Protection Client up to 1000		
17	Should support Access Point Centralize Management minimum 200 AP		
18	Should support Two Factor Authentication Token minimum 900		
C.	**Operating System & Management Requirements:**		
1	Be proprietary to prevent inheriting common OS vulnerabilities		
2	Resided on flash disk for reliability over hard disk		
3	Allow multiple OS firmware image for booting options		
4	Upgradeable via Web UI or TFTP		
5	Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk		
6	The system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access		
7	The proposed system shall be able to limit remote management access from certain trusted network or host with corresponding administrator account		
8	The proposed system should be able to facilitate administration audits by logging detailed activities to event log for management & configuration updates		
9	The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACAS+		
10	The Firewall must be capable of clustering multiple firewalls together into a redundant and highly available active-active configuration without any extra license cost for creating HA.		
D.	**Firewall Requirements:**		
1	The Firewall should support deployment modes as; “Stealth Mode” or “Route Mode" or "Transparent Mode” or "Proxy Mode".		
2	The proposed system should have integrated Traffic Shaping / QoS functionality		

3	Should support DHCP server & DHCP Agent functionality		
4	The Firewall should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)		
5	The Firewall should support Inbound Port Forwarding with optional inbound Load Balancing		
6	Should support IPv6 ACL to implement security Policy for IPv6 traffic		
7	All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc		
8	Should be able to inspect HTTP and FTP traffic when these are deployed using non standard port (i.e when HTTP is not using standard port TCP/80)		
E.	**High Availability Requirements:**		
1	The firewall must support Active-Active as well as Active-Passive redundancy.		
2	The Firewall must support clustering of multiple active firewalls, and the firewalls must load balance the traffic between them to share the load.		
3	The cluster should support simple and minimal downtime during upgrade		
F.	**IPSEC VPN Requirements:**		
1	The IPSEC VPN and SSL VPN capability shall minimally attain Internet Computer Security Association (ICSA) Certification or equivalent		
2	The proposed system shall comply/support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional external solution, hardware or modules:		
3	The device shall utilize inbuilt hardware VPN acceleration supported for:		
3.1	IPSEC (DES, 3DES, AES) encryption/decryption		
3.2	SSL encryption/decryption		
4	The system shall support the following IPSEC VPN capabilities:		
4.1	Multi-zone VPN supports.		
4.2	IPSec, ESP security.		
4.3	Supports Aggressive and Dynamic mode		
4.4	Support perfect forward secrecy group 1 and group 2 configuration		
4.5	MD5 or SHA1 authentication and data integrity.		
4.6	Automatic IKE (Internet Key Exchange) and Manual key exchange.		
4.7	Supports NAT traversal		
4.8	Supports Extended Authentication		
4.9	Supports Hub and Spoke architecture		
4.10	Supports Redundant gateway architecture		
4.11	DDNS support		
G.	**SSL VPN Requirements:**		
1	The Firewall should be integrated solution and there should be no user based licensing for SSL VPN.		
2	The Firewall should support for TWO modes of SSL VPN:		

2.1	Web-only mode: for thin remote clients equipped with a web browser only and support web application such as: HTTP/HTTPS PROXY, FTP, SMB/CIFS, SSH, VNC, RDP		
2.2	Tunnel mode, for remote computers that run a variety of client and server applications		
3	The system shall provide SSL VPN tunnel mode that supports 32 and 64-bit Windows operating systems		
4	The proposed solution shall allow administrators to create multiple bookmarks to add to a group and make these bookmarks available for SSL-VPN users.		
H.	**Network Intrusion Detection & Prevention System Requirements:**		
1	The IPS capability shall minimally attain Internet Computer Security Association (ICSA) NIPS or NSS Certification		
2	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
3	Able to prevent denial of service and Distributed Denial of Service attacks.		
4	Signature based detection using real time updated database		
5	The device shall allow administrators to create Custom IPS signatures		
6	Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.		
7	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)		
8	Security check updates do not require reboot of the unit.		
9	Supports attack recognition inside IPv6 encapsulated packets.		
10	Supports user-defined signatures with Regular Expressions.		
11	Supports several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc. List all prevention options		
12	SSL Inspection for IPS		
I.	**Antivirus System Requirements:**		
1	The Antivirus capability shall minimally attain Internet Computer Security Association (ICSA)/equivalent AV Certification		
2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy		
3	The System should be able to scan following Protocols:		
3.1	HTTP and HTTPS		
3.2	SMTP, SMTPS		
3.3	FTP, FTPS		
3.4	POP3, POP3S		
3.5	IMAP, IMAPS		
3.6	Instant Messenger (AIM, YAHOO!, MSN, ICQ, SIMPLE)		
3.7	NNTP		

4	The proposed system shall provide ability to allow, block and intercept (allow but quarantine) attachments or downloads according to file extensions and/or file types		
5	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
6	The solution should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
J.	**Web & Application Content Filtering System Requirements:**		
1	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.		
2	URL database should have minimum 200 million sites and 75 + categories.		
3	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.		
4	Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies.		
5	Shall include Web URL block		
6	Shall include Web Exempt List		
7	The proposed solution should be able to replace the web page when the web page matches the Web Filtering blocking criteria.		
8	The proposed solution shall be able to identify, retrieve and rate the actual URL of the cache content commonly available in search engines such as Yahoo and Google.		
9	The solution shall allow administrators to create multiple new local URL filtering categories besides dynamic categories		
10	Should have application control feature		
11	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, BitTorrent etc.		
12	Should have minimum database of 3300 types of application awareness		
K.	**Data Leak Prevention Requirements:**		
1	Should have the ability to prevent data loss through SMTP, SMTPS, FTP, HTTP, HTTPS & IM		
2	Should have built in pattern database		
L	**User Authentication**		
1	The proposed Firewall shall be able to support various form of user Authentication methods simultaneously , including:		
2	Local Database entries		
3	LDAP server entries		
4	RADIUS server entries		
5	TACACS+ server entries		
6	Native Windows AD (Single sign on capability)		

7	Two-factor authentication without any external Hardware.		
8	Citrix Agent support for Single Sign On		
9	The solution shall be capable of providing Windows AD single sign-on by means of collector agents which broker between users when they log on to the AD domain and the device.		
10	The proposed appliance shall support inbuilt 2 factor authentication services and database using tokens, email and SMS. Hardware Token supported should be 1000. If this service is not available on the box, provide an external server for authentication.		
11	System should also have capability to identify devices (ex. Android, Iphone, Windows etc) & should be able to write policies on basis of device identity		
12	Should also support Authentication-based routing		
M	**Wireless Security**		
1	Integrated wireless Controller support required & Number of Manageable Wireless access points support required		
2	Wireless Security features like WEP,WPA-PSK & WPA-ENT should be supported		
3	Should have a inbuilt DHCP Server to assign IP Addresses to specific SSID's and should support DHCP Relay		
4	Should have ability to detect wireless as well as on-wire rogue AP		
5	Total number of AP's supported 512		
6	Should support on-box Guest Management Feature		
7	Administrators shall be able to setup per SSID, a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.		
8	Administrators shall be able to view client monitor which illustrate wireless access situation		
9	Wireless Deployment should support wired AP's i.e AP's connected on LAN as well as Wireless Bridged AP's i.e AP's connected by Wireless backhaul.		
10	Should support Wireless IDS for following types of intrusion detection among others:		
11	1.1 Unauthorized Device Detection		
12	1.2 Rogue/Interfering AP Detection		
13	1.3 Adhoc Network Detection and Containment		
14	1.4 Wireless Bridge Detection		
15	1.5 Misconfigured AP Detection		
16	1.6 Weak WEP Detection		
17	1.7 Multi Tenancy Protection		
18	1.8 MAC OUI Checking		
N	**BYOD**		
1	create policies based on device type		
2	identify and monitor the types of devices connecting to your networks, wireless or wired		
3	use MAC address based access control to allow or deny		

	individual devices		
4	enforce endpoint control on devices that can run Client Endpoint Control software		
O	**Client Reputation**		
1	Should be able to provide information by tracking client behavior and reporting on the activities you determine are risky or otherwise noteworthy.		
2	Bad Connection Attempts		
3	Packets that are blocked by deny security policies.		
4	Intrusion Protection		
5	Malware Protection		
6	Web Activity		
7	Application Protection		
8	Geographical locations that clients are communicating with.		
P	**End Point Protection**		
1	The solution should have Anti-virus, Web filtering, Application Control, IPSec & SSL VPN, vulnerability scan etc features.		
2	The solution should have VB100 certification		
3	The solution should support Android & iOS along with Windows & MAC		
4	Should be managed from a single console		
5	Can be deployed in the network through Active Directory		
6	Should have the feature of rootkit removal		
7	Should identify system & application vulnerability		
8	Should have the application firewall protection to block any specific application		
9	Should have the option of creating customized MSI installer package		
10	The software should support windows XP or higher		
11	Should have the quarantine feature		
12	The solution can work standalone or centrally managed		
13	Should have the client certificate support		
Q	**Support and Warranty**		
1	Should have 24X7 Warranty and Support from OEM for Product Hardware and Firmware/OS		
R	**License**		
1	Commercials need to be quoted for Three Years 24X7 Fully Bundle Hardware Appliance with licenses and Features as per above specification. (Exp. Gateway Antivirus, spyware, web/url filtering, content and application filtering, SSL VPN & IPS) all Hardware Component and Licenses should be installed from day one and License period will be counted from date of activation.		

Annexure II

AUTHORISATION FROM MANUFACTURER/OEM

To
FA & CAO,
Mormugao Port Trust,
Administrative Building,
Headland Sada, Goa 403 804.

Sub: Manufacturers' Authorization form against Tender No:_____

We_____(Name of the Manufacturer) who are official manufacturers of _____(Type of goods manufactured) having factories at _____(full address of Manufacturer's factories) do hereby authorize _____ (Name of the Bidder) to submit a bid against your Tender No. _____ for the _____Goods manufactured by us and to subsequently negotiate and sign the contract.

We hereby extend our full guarantee and warranty with respect to the Goods offered by the above firm

Manufacturer's Name:
Signature of Authorized
representative of the Manufacturer:

Duly authorized to sign this Authorization on behalf of : _____(Name of the Bidder)
Date:

Annexure III

TENDER ACCEPTANCE UNDERTAKING

To

FA & CAO,
Mormugao Port Trust,
Headland Sada, Goa.

Having examined the tender document for **SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL**, we the undersigned, hereby offer to supply, install anc commission the equipment in conformity with all specifications and conditions set out in the tender document.

We have enclosed all the relevant documents as per the tender.

We understand that you are not bound to accept the lowest or any tender received.

Date :

(Signature of Bidder)

Name :

Firm :

Designation :

Seal

ANNEXURE IV

\

PARTICULARS/DOCUMENTS TO BE FURNISHED BY THE TENDERER IN THE TECHNICAL BID COVER

a. **Name of the Tenderer**

b. **Full postal address with Telephone, Telefax, Email**

c. **Please specify whether Public Limited, Company, Private Organization or Partnership Firm**

d. **Nature of the Business**

e. **Date of Establishment**

f. **Yearly Turnover (Financial Year 2015-16)**

g. **C.S.T. / S.T. NO.**

h. **Address & Telephone Nos. of your branch office in GOA (please specify whether Distributing/Servicing/Marketing the products)**

i. **Technical Compliance Statement enclosed**

j. **Reference of reputed Customers enclosed**

k. **Copies of Purchase Orders executed and value thereof**

l. **Authorization from Manufacturer/OEM attached**

m. **E.M.D. enclosed in Technical BID.**

n. **Infrastructure facilities required for installation & commissioning attached**

o. **Technical Specifications/Literature/Brochure attached**

p. **Tender Acceptance Undertaking attached**

Annexure V

PRICE BID FORMAT

Sl. No.	Particulars	Qty	Unit	Base Price (Rs.)	VAT (Rs.)	Service Tax (Rs.)	Total Price (Rs) (5+6+7)
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Next Generation Firewall/UTM with one year Comprehensive Hardware Warranty, Firmware Updates, Online Support & 1 year license for subscription with 24x7 support by OEM including cost of packaging, forwarding, freight etc. for delivery to MPT, Goa. as per specifications mentioned in the Part II of the Tender	1	No.				
2	Additional Two Years Bundle License Subscription with Comprehensive Hardware Warranty & 24/7 Support	1	No.				
3	Installation, Configuration, Training and On-Site Support	1	No.				
	Total						

(Rupees _____ only)

_____

(Signature of Bidder)

Name :

Firm :

Designation :

Seal

Annexure VI

FORM OF BANK GUARANTEE FOR SECURITY DEPOSIT

TENDER No. FA/IT(7-NW)/2016/165

In consideration of the Board of Trustees of the Mormugao Port Trust (hereinafter called "The Board") having offered to accept the terms and conditions of the proposed agreement between _____ and _____ (hereinafter called "the said Contractor(s)" for the work _____(hereinafter called "the said agreement") having agreed to production of an irrevocable Bank guarantee for Rs. _____ (Rupees _____ only) as a security/guarantee from the Contractor(s) for compliance of his obligations in accordance with the terms and conditions in the said agreement.

1. We _____ (hereinafter referred to as the "Bank") hereby undertake to (indicate the name of the Bank) pay to the Board an amount not exceeding Rs. _____ (Rupees _____ only) on demand by the Board.

2. We_____ do hereby undertake to pay the amounts due and payable (indicate the name of the Bank) under this Guarantee without any demur, merely on a demand from the Board stating that the amount claimed is required to meet the recoveries due or likely to be due from the said Contractor(s). Any such demand made on the bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this Guarantee shall be restricted to an amount not exceeding Rs. _____ (Rupees _____ only).

3. We, the said Bank, further undertake to pay to the Board any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) in any suit or proceeding pending before any Court or Tribunal relating thereto, our liability under this present being absolute and unequivocal. The payment so made by us under

this bond shall be a valid discharge of our liability for payment thereunder, and the Contractor(s) shall have no claim against us for making such payment.

4. We _____ further agrees that the Guarantee herein contained shall (indicate the name of the Bank) remain in full force and effect during the period that would be taken for the performance of the said agreement, and it shall continue to be enforceable till all the dues of the Board under or by virtue of the said agreement have been fully paid, and its claims satisfied or discharged, or till the Engineer-In-Charge, on behalf of the Board, certifies that the terms and conditions of the said agreement have been fully and properly carried out by the said Contractor(s), and accordingly discharges this Guarantee.

5. We _____ further agree with the Board that the Board (indicate the name of the bank) shall have the fullest liberty without our consent, and without effecting in any manner our obligations hereunder, to vary any of the terms and conditions of the said agreement or to extend time of performance by the said Contractor(s) from time to time or to postpone for any time or from time to time any of the powers exercisable by the Board against the said Contractor(s) and to forbear or enforce any of the terms and conditions relating to the said agreement, and we shall not be relieved from our liability by reason of any such variation or extension being granted to the said Contractor(s) or for any forbearance, act of omission on the part of the Board or any indulgence by the Board to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

6. This guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s).

7. We _____ lastly undertake not to revoke this Guarantee except with (indicate the name of the Bank) the previous consent of the Board in writing.

8. This Guarantee shall be valid upto _____ unless extended on demand by the Board. Notwithstanding anything mentioned above, our liability against this Guarantee is

restricted to Rs. _____ (Rupees _____ only), and unless a claim in writing is lodged with us within six months of the date of expiry or extended date of expiry of this Guarantee all our liabilities under this Guarantee shall stand discharged.

Dated the _____ day of _____ For _____

(indicate the name of the Bank)