Maldives Marketing and Public Relations Corporations

Republic of Maldives

Information Sheet

To Acquire a Firewall for MMPRC

26/10/2020

Section 1 – Instruction to Tenderers		
1.	**General**	
1.1	Announcement Number:	(IUL)MMPRC-PRO/1/2020/25
1.2	Announcement Date:	26th October 2020
1.3	Project:	To Acquire a Firewall for MMPRC
2.	**Procedure of Tendering**	
2.1	**Eligible Tenderers:** A Tenderer may be a sole proprietor, private entity, or government-owned entity or any combination of them in the form of a joint venture, under an existing agreement, or with the intent to constitute a legally enforceable joint venture	
2.2	**Amendments to Tender Documents:** (a) At any time prior to the deadline for submission of Tenders, the MMPRC may amend the Tendering Document by issuing addenda. (b) Any addendum issued shall be part of the Tendering Document and shall be communicated in writing to all who have obtained the Tendering Document from MMPRC (c) To give prospective Tenderers reasonable time in which to take an addendum into account in preparing their Tenders, the Employer may, at its discretion, extend the deadline for the submission of Tenders	
2.3	Registration of Tenderers: To register please email to procurement@visitmaldives.com by Thursday, 05th November 2020 before 1415 hrs.	
2.4	Pre-bid meeting: Not applicable	
2.5	Clarifications of Bidding document, firewall specification: Thursday, 10th November 2020 before 1415 hrs.	
2.6	**Submission of Tenders:** Venue: Maldives Marketing & Public Relations Corporation, 2nd Floor, H. Zonaria, Male' Date: Tuesday, 18th November 2020 Time: 1000 hrs.	
3.	**Preparation of Tenders**	
3.1	**Cost of Tendering:** The Tenderer shall bear all costs associated with the preparation and submission of its Tender, and MMPRC shall in no case be responsible or liable for those costs, regardless of the conduct or outcome of the tendering process.	

3.2	**Language of Tender:** The Tender, as well as all correspondence and documents relating to the Tender exchanged by the Tenderer and MMPRC, shall be written in **English or Dhivehi** Language. Supporting documents and printed literature that are part of the Tender may be in another language provided they are accompanied by an accurate translation of the relevant passages in **English or Dhivehi**, in which case, for purposes of interpretation of the Tender, such translation shall govern.
3.3	**Documents Comprising the Tender:** (a) Cover Letter (b) Quotation (c) Copy of registration Certificate of Sole proprietorship / Partnership / Company / Corporative Society (d) Profile of the Tenderer (e) Copy of GST Registration Certificate (f) Tax Clearance Certificate issued by MIRA (g) Other documents, if required by this document
3.4	**Period of Validity of Tender:** (a) Tenders shall remain valid for 90 calendar days after the Tender submission deadline date prescribed by MMPRC. A Tender valid for a shorter period shall be rejected by MMPRC as nonresponsive. (b) In exceptional circumstances, prior to the expiration of the Tender validity period, MMPRC may request Tenderers to extend the period of validity of their Tenders. The request and the responses shall be made in writing.
3.5	**Tender Security (If required): Not Applicable**
3.6	**Format of Signing of Tender:** The Tenderer shall prepare one original of the documents comprising the Tender as described in Clause 3.3, and clearly mark it “Original”. Alternative Tenders, if permitted in accordance with clause 3.8, shall be clearly marked “Alternative”.
3.7	**GST/VAT:** The prices shall be quoted inclusive of GST/VAT.
3.8	**Alternative Tenders:** It is permitted to submit Alternative Tenders.
3.9	**Incomplete Tender:** Any tender that does not include all information and documents stated in clause 3.3 shall be considered as Incomplete Tender.
3.9	**Conflict of Interest:**

	A Tenderer shall not have a conflict of interest. All Tenderers found to have a conflict of interest shall be disqualified. A Tenderer may be considered to have a conflict of interest with one or more parties in this tendering process, if: (a) they have a controlling partner in common; or (b) they receive or have received any direct or indirect subsidy from any of them; or (c) they have the same legal representative for purposes of this Tender; or (d) they have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the Tender of another Tenderer, or influence the decisions of the Employer regarding this tendering process; or (e) a Tenderer participates in more than one Tender in this tendering process. Participation by a Tenderer in more than one Tender will result in the disqualification of all Tenders in which the party is involved. However, this does not limit the inclusion of the same subcontractor in more than one Tender; or (f) a Tenderer or any of its affiliates participated as a consultant in the preparation of the design or technical specifications of the contract that is the subject of the Tender; or (g) a Tenderer, or any of its affiliates has been hired (or is proposed to be hired) by MMPRC.
3.11	**Authorization:** The original and the Alternative Tender shall be signed by a person duly authorized to sign on behalf of the Tenderer. This authorization shall consist of a written confirmation and shall be attached to the Tender. The name and position held by each person signing the authorization must be typed or printed below the signature.
4.	**Submission and Opening of Tenders**
4.1	**Sealing of Tenders:**
4.2	**Deadline for Submission of Tenders:** **(a)** Tenders must be received by MMPRC at the address and no later than the date and time clause 2.6 of this document. (b) MMPRC may, at its discretion, extend the deadline for the submission of Tenders by amending the Tendering Document, in which case all rights and obligations of the MMPRC and Tenderers previously subject to the deadline shall thereafter be subject to the deadline as extended.

4.3	**Late Tender:** MMPRC shall not consider any Tender that arrives after the deadline for submission of Tenders, in accordance with clause 4.2. Any Tender received by MMPRC after the deadline for submission of Tenders shall be declared late, rejected, and returned unopened to the Tenderer.
4.4	**Submission Documents:** • Cover letter expressing interest. This letter should include the contract price and the delivery period. • Company Profile along with Business Registration Certificate, Tax Registration and Tax Clearance should be submitted. • Reference letters and proof of previous projects undertaken during the last 3 years of at least 3 clients • Methodology that will be used to train MMPRC staff • Timeline of delivery of the firewall
5.	**Evaluation**
5.1	The tender evaluations will be carried out as per the evaluation criteria stated under Section 2 of this document. No other evaluation criteria or methodologies shall be permitted.
6.	**Tender Security and Performance Guaranty (Not applicable)**
7.	**Advance Payment and Advance Payment Guarantee (Not applicable)**
8	**Penalty & Contract Termination**
8.1	**Penalty:** MMPRC shall have the right to withhold any payment of the Contract Price, if the Selected party fails to deliver any Works in accordance with the terms of the Agreement.
8.2	**Contract Termination:** If the Select Party fails to carry out any obligation under the Agreement, MMPRC may by notice require the Contractor to make good the failure and to remedy it within a specified reasonable time.

Section 2 – Evaluation Criteria

Area	Details	Marks
Contract Price	The party that proposes the lowest price shall get the highest marks. For others, marks will be awarded on pro rata basis	45
Profile	The company profile, registration certificate, tax registration certificate and tax clearance from MIRA should be submitted.	15
Past Experience	Reference letters and proof of previous projects undertaken during the last 3 years of at least 3 clients.	10
Delivery Period	Highest marks will be allocated to the party who proposes the reasonable time to submit the customized firewall.	15
Training for Staff	Highest marks will be allocated to the party who proposes the best method for training the existing staffs.	15
	TOTAL	**100**

Section 3 - FIREWALL REQUIREMENTS FOR MMPRC

1- Firewall Requirements

a) Proposed solution should be hardware-based appliance and rack mountable
b) The proposed solution should support High Availability Active-Active, active-passive
c) Support stateful protocol filtering, deep packet inspection, and detection of attacks within the payload.
d) The proposed firewall solution must be extensible to accommodate the companies growing needs and keep up with higher throughput requirements. (Currently we plan to cater for 100 live users and are planning for 50Mbps traffic over 2 WAN connections)
e) Provide a centralized web management console and out of band Ethernet interface for management that supports SSHv2 and SCP.
f) Provide multiple security zones and interfaces to partition the data center networks into more manageable highly controlled network segments.

2- General Features

a) VPN access
b) Identity based Firewall
c) Intrusion Prevention System (IPS)
d) Web Content and Application Filtering
e) Bandwidth Management
f) Solution should include Appliance reporting and retain log for minimum 1 year before rewriting
g) Networking: Dynamic routing (RIP, OSPF), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, BFD, tunnel content inspection
h) User Authentication through AD, Local and LDAP.
i) Country based blocking, FQDN support and should support Mix mode deployment
j) Must support Software Defined Networking (SDN)
k) Must support dual stacking of IPv4 and IPv6 protocols for all firewall features and functions.
l) Provide secure access to diverse applications that reside in the data centers (i.e. SQL Server, VoIP, Exchange, streaming video, video conferencing, Remote Desktop Services, web-based line of business applications, etc.)
m) Enable secure remote access to the authorized resources from inside and outside of the networks.
n) Zone-based network segmentation and zone protection; DoS protection against flooding of new sessions

3- Performance and Capacities

a) Firewall throughput: 3 Gbps
b) Threat Prevention throughput: 1 Gbps
c) Throughput Application Control (AVC): 1 Gbps
d) Throughput Application Control (AVC) and IPS: 1 Gbps
e) IPsec VPN throughput :1 Gbps
f) SSL VPN throughput: 1Gbps
g) Support 100 VPN users

4- Hardware Specification

a) Minimum interfaces supported: 4 Ethernet, 2 SFP+
b) Management I/O: 10/100/1000 out-of-band management port, (2) 10/100/1000, high availability, (1) RJ-45 console port, (1) Micro USB (optional)
c) Rack mountable? Yes Standard rack
d) Storage minimum 120GB SSD

5- Technical Specification

a) Support at least 1 Gbps sustained throughput with all firewall and associated security features enabled
b) Per firewall, Include a minimum of two (2) SFP+, and minimum of four 1000 Mbps copper Ethernet interfaces. All ports must be compatible and work with the existing network equipment
c) Must maintain user and application sessions when one of the high availability pairs (firewall devices) fails.
d) Ability to create security policy definitions per Microsoft Active Directory user, role, computer name, specific aspects of an application and security groups to identify, block or limit usage of applications and widgets like instant messaging, social networking, video streaming, VoIP, games, etc.
e) QoS: policy-based traffic shaping (priority, guaranteed, maximum) per application, per user, Per user group, per tunnel, based on DSCP classification. There should be advanced user and application controls such as ability to expand user groups, domain names as well as detailed user and application usage information in reports, logs and statistics.
f) **User identification and control:** VPNs, WLAN controllers, captive portal, proxies, Active Directory, eDirectory, Exchange, terminal services, syslog parsing, XML API. Provide solution must support agentless integration with Microsoft Active Directory and facilitate Microsoft AD user and group integration within the firewall security policy.

6- Web and Application filtering

a) The proposed firewall must deliver consistent controls to all users, regardless of location or device type.
b) Provide application function control to identify, allow, block or limit usage of applications and features within them.
c) Must include integrated intrusion detection and prevention (IPS) function that offers advanced detection capabilities such as exploit signatures, protocol anomalies, application controls and behavior-based detection

d) Granular, identity-based enforcement of the organization's policies over new evasive, web-based communication technologies (i.e. social media, web mail and popular remote access applications, P2P application sharing, etc.)
e) Integrated Web security gateway to protect from legacy, emerging/unknown, dynamic and scripted Web Malware. Web security gateway will help in controlling and mitigating security risks from network applications like instant messaging (IM) and peer –to-peer (P2P). Provide enhanced management and control, enabling real-time content analysis for both inbound and outbound web traffic.
f) Automatically prevent web-based attacks, including phishing links in emails, phishing sites, HTTP-based command-and-control, and pages that carry exploit kits
g) Stops in-process credential phishing

7- Threat Prevention

a) Intrusion Prevention System (IPS):
   i. Ability to determine if an unknown traffic is a threat or not.
   ii. IDS/ IPS must be able to detect and prevent protocol misuse, malware communications, tunneling attempts and generic attack types without signatures.
   iii. IPS/IDS must detect and block unsanctioned peer to peer traffic.
   iv. Provide protection from zero-day attacks and unknown threats.

b) Advance Threat Protection (ATP):
   i. Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall).

c) Ability to see all unknown traffic, on all ports, in one management location and quickly analyze the traffic to determine if it is
   i. An internal or custom application,
   ii. A commercial application without a signature, or
   iii. a threat.
   iv. Additionally, the firewall must provide the necessary tools to systematically manage it by controlling it via policy or custom signature

d) VPN
   i. IPSec, L2TP, PPTP, and SSL as part of basic Appliance, VPN redundancy, 3DES, DES, AES, MD5, SHA! Hash algorithms, IPsec NAT Transversal.
   ii. Client less VPN
   iii. Restrict VPN users to certain area of the network (Controlled VPN access).
   iv. VPN user's activity monitoring and reporting.

e) Load balance
   i. For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing. High availability: Active-Active. QoS, OSPF, RIPv2, Policy routing based on Application and User support Round Robin Load Balancing.

f) Command-and-control (C2) activity is stopped from exfiltrating data or delivering secondary malware payloads, while infected hosts are identified through DNS sink holing

8- Bandwidth Management

a) Load balancing between multiple WAN connections.
b) Dedicate specific users/ user groups or specific traffic to a specific WAN connection
c) Fair usage policy, Data quotas, selected action on reaching data quota.
d) Link aggregation

e) Traffic shaping by network address criteria like MAC address, IP address or other properties of client server protocols.
f) Traffic shaping of HTTP connections by URL or SSL connections by server certificate subject.
g) Scheduling filters for particular day or week period.

9- Monitoring and Reporting Systems

a) Should be able to report events via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution.
b) The solution must support the creation of custom log messages and provide system variable placeholders mechanism to make this use case possible.
c) The solution must be capable to store logs minimum 1 year.
d) Must offer adaptive real-time threat intelligence to improve firewall functions.
e) Must show internet usage, real time bandwidth, accessed areas or servers, approved requests, rejected requests
f) Must show user based, user group based, and firewall rule base for all the reports.
g) High risk applications, used users, usage, and blocked applications and its users must be available.
h) Intrusion attacks with source IP, destination IP or port must be available.
i) Push notifications for:
    i. Up/Down of interface
    ii. Hardware Failure
    iii. Critical Service failure (eg: VPN)
    iv. Must be sent over secure
    v. SMTP server and/or HTTP GET.

10- Training

a) The service provider must provide on-site training in implementation
b) Provide manufacturer certified training for two of our employees. To be trained to configure, operate and maintain the proposed solution.

11- Licenses / Subscription

a) Concurrent user software license for URL filtering and blocking, antispam, anti-phishing, and content filtering functionality, pattern file, and scan engine updates.
b) If there is separate cost for licensing, this cost should be per device and should NOT be based on per user or IP endpoint (should support unlimited users)
c) Subscription Year minimum 3 year

12- Support and maintenance

a) Should have support center in Male' and should have international support direct from OEM
b) Provide a list of the printed documentation provided for installation, operation, use, and administration of the whole solution.
c) Warranty:
    i. Minimum 3 years parts and replacement
d) Support:
    i. Minimum 3 years Onsite support