FIJI REVENUE AND CUSTOMS SERVICE

SPECIFICATIONSFOR

TENDER 09/2019 - **Supply of Next Generation Firewall Appliance & Web Application Firewall**

TABLE OF CONTENTS

Advertisement

The following are excerpts and addendums from the advertisement for Fiji Revenue and Customs Service as it originally appeared in the local media and should be used as the basis to submit your proposals:

FIJI REVENUE AND CUSTOMS SERVICE

TENDER 09/2019 - Supply of Next Generation Firewall Appliance & Web Application Firewall

The Fiji Revenue and Customs Service (FRCS) invites tenders from individuals and companies who are interested in supplying '**Enterprise Firewall Solution**' to Fiji Revenue and Customs Service.

Interested bidders are required to access the tender specifications from the FRCS website. For further information, interested parties may contact tenders@frcs.org.fj.

Submissions should be delivered in a sealed envelope clearly marked **'Tender 09/2019 – Enterprise Firewall Solution'** addressed and posted to:

The Chairman
FRCS Tender Board
Fiji Revenue and Customs Service
Private Mail Bag
Suva, Fiji

OR hand delivered to FRCS Head Office, Building 3, Level 3, Nasese Complex or email to tenders@frcs.org.fj no later than 12pm on Friday 20th September 2019.

Bidders are welcome to be present during the opening of bids.

WORLD CLASS VISION

1.0 General Terms and Conditions

Following general terms and conditions will apply.

1.1 Format of Response

Each bidder must provide a formal letter of transmittal that must:

a. Be signed by an authorized representative of the organization and must state that the signing official is authorized to legally bind the organization;

b. Include the names, titles, office addresses and office telephone numbers of the persons authorized by the organization to conduct negotiations on the proposal, including their expected roles in negotiations; and

c. Provide a contact name, address, facsimile number and email address which FRCS will use in serving notices to the bidder.

1.2 Late Submissions

Submissions received within Five minutes of the closing time will be accepted. Five minutes is allowed as variation for any timing difference.

1.3 Applicants to Inform Themselves

Each applicant should:

a. Examine this specifications document; and any documents referred to within; and any other information made available by FRCS to the applicants;

b. Obtain any further information about the facts, risks and other circumstances relevant to the tender by making all lawful inquiries;

c. Ensure that the submission, and all information on which its proposal is based, is true, accurate and complete.

By submitting their proposal, applicants will be deemed to have:

a. Examined the tender specifications and any other information made available in writing by FRCS to the applicants.

b. Examined all information relevant to the risks, contingencies, and other circumstances having an effect on their proposal and which is obtainable by the making of reasonable inquiries.

1.4 Bidder's Risk

FRCS accepts no responsibility, liability, or obligation whatsoever for costs incurred by or on behalf of any bidder in connection with the EOI or any participation in the tender process.

1.5 Selection of Preferred Applicant

No proposal will necessarily be selected by FRCS as the preferred solution/s. The FRCS Evaluation Committee may decide not to accept any proposal or reject all proposals at any time. FRCS reserves the right to cancel this tender and pursue an alternative course of action at any time.

Selection of Preferred Applicant will not be acceptance of the proposal and no binding relationship will exist between the preferred applicant(s) and FRCS until a written agreement acceptable by FRCS is executed by an authorized officer of FRCS and the successful applicant(s).

1.6 Conduct of Applicants

Conduct of Applicants or any of their consortium members, may affect the outcome of their tender responses, including non-consideration of the proposal. Applicants warrant to FRCS that they (and their consortium members) have not and will not engage in any of the following activities in relation to this tender process:

a. Lobbying of or discussions with any politician or political groups during this tender process;
b. Attempts to contact or discuss the tender process with officers, any member or staff or contractor currently working in FRCS or any agent of this Department; Exception to Evaluation Committee members.
c. Provision of gifts or future promise of gifts of any sort to the previously mentioned personnel;

d. Accepting or providing secret commissions;

e. Seeking to influence any decisions of FRCS by an improper means; or otherwise acting in bad faith, fraudulently or improperly.

1.7 Currency

All currency in the proposal shall be quoted in Fiji Dollars and prices shall be VAT Inclusive.

1.8 Corporate Information

Each applicant must provide the following information:

a. Details of the corporate and ownership structure, including identification of any holding company or companies and parent companies (Business license and Business Registration);

b. Profiles of the company and any parent entity. If the company is a subsidiary, the applicant must provide full details of the legal and financial relationship between the subsidiary and parent. The names of all directors and officers of the company;

c. A full description of current operations of the company including the most recent audited financial statement;

d. A copy of the company's Certificate of Incorporation;

e. Confirmation that the company has the capacity to bid for the Services and that there is no restriction under any relevant law to prevent it from bidding;

f. Provision of details of any legal proceedings that are being done against the company.

1.9 Qualifications and Capability

Each Applicant must:

a. Be Tax and Customs compliant. Tax Identification Number (TIN) must be quoted in the proposal. (Tax, VAT and FNPF).

b. Be able to demonstrate that it will be able to meet its financial obligations under this tender.

1.10 Mergers, Acquisitions, Sales of Applicant

Where such information is publicly accessible, the Applicant must indicate whether any mergers, acquisitions or sales are planned presently or during the year following the submission of the proposal.

1.11 Enquiries

- All questions and enquiries regarding this tender are to be made in writing via email or official letter.
- All questions and inquiries will be responded to in writing by email.
- Verbal responses will not have any binding on either party.

2.0 Financial Proposal

2.1 Cost Matrix

Bidders should provide their cost breakdown in the following format.

COST MATRIX			
Category	**Description**	**Cost**	**Annual Support Fees**
Enterprise Firewall Appliance (HA)	**Hardware**		
	-- add rows as needed		
	Software		
	-- add rows as needed		
	Licenses		
	-- add rows as needed		
	Others (specify)		
	-- add rows as needed		
	Total		
WAF	**Hardware**		
	-- add rows as needed		
	Software		
	-- add rows as needed		
	Licenses		
	-- add rows as needed		
	Others (specify)		
	-- add rows as needed		
	Total		

3.0 Detailed System/Equipment Requirements

3.1 Technical Specifications –

- The tender submission should contain detailed specifications of the proposed solution including supplier contacts for queries and clarifications.

3.2 Compliance –

Compliance should be

i. Full Compliance(FC)
ii. Partial Compliance(FC)
iii. Non Compliance(NC)

Reference to documents supporting compliance to be provided.

Supply of Next Generation Firewall Appliance (HA) – Minimum Requirements

	Requirements	Compliance (FC, PC, NC)	Reference:
1	The proposed solution should be covered by 3 Years 24x7 Vendor support with NBD hardware replacement.		
2	The solution must be **Appliance** based and Must facilitate multi-application environment.		
3	Must be a leader in both Gartner UTM and Enterprise Firewall Quadrants.		
4	The platform Must use hardware acceleration to optimize the packet, encryption/decryption and application level content processing.		
5	Licensing: Must be per device license for unlimited users for Firewall and other features. There Must not have any user/IP/host based licenses.		
6	The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
7	Must have support for Explicit Proxy and Transparent Proxy		
8	Must support more than one ISP with automatic ISP failover		
9	Must have security fabric integrations to different security sensors and tools together to collect, coordinate, and respond to malicious behaviour anywhere it occurs on the network in real time including 3rd party security products		
10	The equipment MUST have capability to uplink to at least 4x 40/100GE ports on the core switching infrastructure and MUST have a minimum of additional 24 x 1/10/25 GE SFP Slots.		
11	Must have at least 1 GE RJ45 Management Port plus USB and Console access.		
12	Must support at least 50 Million Maximum Concurrent Sessions		
13	Must support at least 90 Gbps Real World/Production NGFW Throughput		
14	Must support at least 60 Gbps Real World/Production Threat Protection Throughput		
15	Must support at least 2 hard disk slots with SSD storage of not less than 4TB.		
16	Must support at least 1000 SSL VPN licenses		
17	Must have the following licenses included Application Control, IPS, AV, Web Filtering and Sandbox		
18	Must support at least 44 Gbps Real World/Production IPS Throughput		
19	Must support at least 34 Gbps Real World/Production NGFW Throughput		
20	Must support at least 23 Gbps Real World/Production Threat Protection Throughput		
21	Must support a throughput of at least 200Mbps packets/sec		
22	Must support a minimum of 400,000 new sessions/sec		
23	Support for external RADIUS and LDAP integration for User and Administrator Authentication		

24	Support for Native Windows Active Directory		
25	The VPN Must be integrated with firewall and Must be ICSA Labs certified for both IPSec and SSL-TLS		
26	Must have integrated SSL VPN with no user license slab restriction		
27	Must support at least 20,000 concurrent SSL-VPN Users		
28	Must support NAT within IPSec/SSL VPN tunnels		
29	The device must support Active-Active as well as Active-Passive redundancy		
30	The Firewall must support stateful failover for both Firewall and VPN sessions		
31	The HA Architecture Must have the ability for Device Failure Detection and Notification as well as Link Status Monitor		
32	Must support the following protocols:-		
	• DES & 3DES		
	• MD5, SHA-1 & the more secure SHA-256 authentication		
	• Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.		
	• Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm		
33	The device Must have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).		

Supply of Web Application Firewall (WAF) – Minimum Requirements

	Web Application Firewall	**Compliance (FC, PC, NC)**	**Reference:**
1	Licensing: Should be per device license for unlimited users for WAF and other features. There should not have any user/IP/host based licenses.		
2	The solution must be able to integrate with the proposed NGFW by synchronizing WAF protections and sharing of threat information to both deeply scan suspicious files and share infected internal sources.		
3	Must include minimum of 2x 10GbE and 1Gbe Mgt, including required transceivers		
4	Must Include Redundant Power Supply		
5	Must support Caching and Compression		
6	Must include High Availability		
7	Must support Load Balancing		
8	Must include 5 years warranty and 24x7 support response		
9	Must include Vulnerability Remediation Service		
10	Must support at least 30,000 HTTPS trans/sec		
11	Should automatically and dynamically builds a security model of protected applications by continuously monitoring real time user activity		
12	Should Protect against:		
	o OWASP Top 10 and API Protection		
	o Cross Site Scripting		
	o SQL Injection		
	o Cross Site Request Forgery		
	o Session Hijacking		
13	Must support AV for File Upload		
14	Must include Vulnerability Scanner Integration		
15	Must support Cookie signing and encryption		
16	Must support IP Reputation		
17	Must support IP Geolocation		
18	Must Support URL Encryption		
19	Must support Malware detection		
20	Must include two-factor authentication integration		
21	Must support Protocol validation		
22	Must support Brute force protection		
23	Must support Threat scoring and weighting		
24	Must support Syntax-based SQL detection		
25	Must support Operating system intrusion signatures		
26	Must provide Known threat and zero-day attack protection		
27	Must support Application DDoS prevention		
28	Must support Outbound Data Theft Protection		
29	Must support Ongoing and automated protection against botnets and malicious sources		

30	Must support Bot dashboard help analysing traffic from malicious robots, crawlers, scanners and search engines		
31	Must provide Geo IP analytics and security		
32	Must support Credential Stuffing Defense		
33	Must support machine learning to automate application and content inspection		
34	Must have LDAP, RADIUS, and SAML support		
35	Must have SSL client certificate support		
36	Must support CAPTCHA and Real Browser Enforcement (RBE)		
37	Must support flow analysis and application performance — Netflow, SFlow, Cisco AVC, NBAR		

Terms & conditions may vary and will depend on the assessment undertaken by FRCS. When making a submission, bidders must submit two (2) hard copies with one marked "original" and the other marked "copy" and one (1) soft copy emailed to tenders@frcs.org.fj or presented to FRCS via a secured USB drive. All clarifications can be directed via email to tenders@frcs.org.fj.

END