REQUEST FOR PROPOSAL

Proposal for implementation of Firewall

BANK OF BARODA, Territory office, Mauritius, having its office at Bank of Baroda Building, 2nd floor, P B No. 553, No. 32, Sir William Newton Street, Port Louis, Mauritius invites tenders for supply of Firewalls, installation, configuration and integration at Port Louis and Curepipe branches.

Sealed proposals Technical bid & financial bid (separately) are invited from service providers for installation of Firewall on Bank's Networks

Requirements		
Srno	Description	Quantity
1	**Firewalls with 3 years warranty:** **(**supply, Implementation and Maintenance) Two firewalls to be deployed in active passive HA mode with auto failover at Bank Port Louis Office. Two firewall to be deployed at Banks DR Site at Curepipe Branch Specification for firewall is attached. EOL/EOS should not be before 5years from date of installation	4

Scope of Work

- Cabling between devices within the bank
- Mounting of Firewall
- Firewall Installation, configuration, clustering, testing etc
- Firewall security zoning and policy
- installation of antivirus, web filtering etc
- Documentation of the setup
- AMC and Support

UPTIME GUARANTEE

Vendor will have to guarantee a minimum uptime of 99%, calculated on a monthly basis.
Uptime percentage - 100% less Downtime Percentage.
Downtime percentage - Unavailable Time divided by Total Available Time, calculated on a monthly basis.
Unavailable Time - Time involved while any part of the core configuration or system software component is inoperative or operates inconsistently or erratically

SUBMISSION DETAILS

As part of the submission the vendor should submit the following details in two separate envelops for **technical** and Financial bids:
a) Undertaking Letter from Principal Vendor / OEM – A letter of undertaking from the vendor on the following points:
I) Agreeable to all terms & conditions as detailed in the tender.
II) The organization is in the business of firewall at least for a period of last 3 years.
III) The model offered meets all the technical requirements requested.
IV) Sufficient quantity of spares will be kept as stock during the Warranty / AMC period at the Vendor's side.

V) Any technical problem would be resolved within 24 hrs of call reported (including time for procuring spare parts) and having technically qualified engineers to service.
VI) Escalation Matrix with First Level Support, Second Level Support, Regional & Zonal head, Country Head Details along with their Name, Contact Number (LL & Mobile), E-Mail ID.
b) Undertaking Letter from OEM – A letter of undertaking from the vendor on the following points:
I) If submitting tender as a partner - letter of authorization from the principal vendor or OEM.
II) If submitting tender as a partner - Under taking from OEM to support the product in Warranty as well as in AMC period if bidder/vendor's integrator fails to do so.

EVALUATION METHODOLOGY
Bank will open the commercials of only those vendors who have submitted valid Undertaking Letters as mentioned in "Point: SUBMISSION DETAILS". The vendor quoting the lowest commercial shall qualify as the L1/successful vendor/bidder. The vendor is expected not to add any conditions / deviations in the commercial bid. Any such conditions / deviations may make the bid liable for disqualification

NORMALIZATION OF BIDS
The Bank will go through a process of evaluation and normalization of the bids to the extent possible and feasible to ensure that vendors are more or less on the same ground of evaluation. After the normalization process, if the Bank feels that any of the bids needs to be normalized and that such normalization has a bearing on the price bids; the Bank may at its discretion ask all the empanelled vendors to resubmit the commercial bids once again for scrutiny. The Bank can repeat this normalization process at every stage of bid submission or till the Bank is satisfied. The vendors agree that they have no reservation or objection to the normalization process and all the vendors will, by responding to this tender, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The vendors, by submitting the response to this tender, agree to the process and conditions of the normalization process.

OTHER TERMS AND CONDITIONS
Please note that any response which does not provide any / all of the information in the specified formats shall be rejected and the Bank shall not enter into any correspondence with the vendor in this regard.
The Bank reserves the right to accept or reject the tender in whole or in parts without assigning any reason thereof. The bank's decision will be final and the bank will not entertain any correspondence in this regard. Bank will not assume any responsibility in case of delay or non-delivery of responses by post, courier, etc within the stipulated time.

Mere response to the tender will not entitle nor confer any right on the vendors for supply/sale to the bank.
Those vendors who do not fulfil any one of the required specifications and not meeting other criteria will not be considered.
Following conditions will apply on bidder.
1. The bidder in its own capacity without any joint venture / consortium / subcontracting arrangement should have Experience in implementation and Support of Infrastructure sites in Mauritius (Minimum Three active sites with at least one in Banking sector) with customer and contact details in the last 3 years. The contracts must be active until validity of the bid submission. This must be supported by recommendation letters from all the entities.
2. The bidder in its own capacity without any joint venture / consortium / subcontracting arrangement should be a direct authorized partner of the manufacturers proposed for all components in the solution stack. Bidder to submit OEM's letter of authorization for supply and support.

3. The bidder in its own capacity without any joint venture / consortium / subcontracting arrangement should have OEM Certified professional Engineers in Mauritius. Please submit CV along with certificates, national ID cards / work permit.
4. The bidder in its own capacity without any joint venture / consortium / subcontracting arrangement must have successful & verifiable track record of at least one (supply & implementation) banking Infrastructure in Mauritius.
5. The bidder in its own capacity should be a registered business entity in Mauritius in similar trade.
6. Average Annual turnover must not be less than USD 350,000 or equivalent per year in the last 3 years with a sustained positive net operating cash flow. The company will be required to present its certified cash flow statements / balance sheet for two years. Company should be in profit for the last three years.
7. Bidder to submit latest Tax clearance certificate from MRA.
8. Bidder to provide information that any of its subsidiary or associate or holding company or companies having common director/s or companies in the same group or promoters / management or partnership firms / LLPs having common partners has not participated in the bid process.

DELIVERY TIMELINES
Delivery should be within 4 weeks from the date of purchase order at our Port Louis and Curepipe branches.

WARRANTY
The product supplied should be with 3 year warranty from the date of invoice.
Three year comprehensive warranty from date of installation. And bidder to provide onsite maintenance, troubleshooting support 24 x 7 during warranty period up to unlimited number of calls.
All equipments supplied to be registered with manufacturer for future warranty / AMC support.
Performance Bank Guarantee : Performance Bank Guarantee 10% of agreed total value of Contract for 6 months post implementation of the firewalls

SUPPORT SERVICES
Support services should include the following:
a. OEM / Partner has to provide onsite, Telephonic, Email & Web based Support (24x7) for the 3 years warranty period.
b. OEM / Partner have to provide Patches / Updates / Upgrades / Bug Fixes during the 3 years warranty period.

CONFIDENTIALITY
The Vendor shall keep confidential any information obtained under the contract and shall not divulge the same to any third party without consent in writing by BANK. In case of non-compliance of the confidentiality agreement, the contract is liable to be cancelled by BANK. Further, BANK shall have right to regulate vendor staff.

INFORMATION AND SECRECY
The Vendor must provide a written undertaking to the bank to comply with the secrecy provision. The Vendor will follow professional ethics and conduct in performing their duties. The Bank has right to terminate the services of the Vendor if it fails to comply with the conditions imposed. The external and internal auditors of the bank will be given right to review the books and internal controls of the Vendor. Any weaknesses highlighted during the audit must be promptly rectified especially where such weaknesses may affect the integrity of the internal controls of the bank.

Commercial Bid				
Sr. No.	Item Make Model	Quantity	Unit Price with 3 Years Warranty	Fixed Cost
A		4		
	Total cost of ownership for 3 years (TCO)			
Sr. No.	Item Make Model	Quantity	Unit Price	Recurring Cost
B				
	Total cost of ownership for 3 years (TCO)			

Note	
All the commercial value should be quoted in USD or MUR	
b) The price should be inclusive of all	
c) The vendor needs to clearly indicate if there are any recurring costs included in the above bid and quantify the same. In the absence of this, the vendor would need to provide the same without any charge.	
d) The above price should include supply, installation, integration and maintenance	
e) Further, we confirm that we will abide by all the terms and conditions mentioned in the Tender document	
Date	Seal and Signature of the Bidder
Place	

Vendors may visit the sites for the installations upon request from IT Department (Port Louis)

We shall appreciate interested firms/companies to send their complete proposal including details of Total cost and break up of cost and other clauses like Terms of Payment, Warranty, Annual maintenance Cost etc at our Bank by **17.06.2019 15.00 hrs** in a sealed envelope marked **"Proposal for Firewall"** to the attention of:

The Vice-President
Bank of Baroda
Sir William Newton Street
Port Louis

No submissions after 15.00 hours shall be accepted.

Bank reserves the right to accept or reject any offer without assigning any reasons whatsoever.

Any decision taken by Bank at any point of time in connection with this process shall be final and conclusive and no claim or dispute of any kind in this regard shall be entertained

VICE PRESIDENT,
BANK OF BARODA,
MAURITIUS TERRITORY
Place : Port Louis, Mauritius
Date: 27.05.2019

The above should abide to the following specifications

Sr. No	General Requirements	Compliance (FC, PC, NC)	Comments
A	***General Requirements:***		
A.1	The proposed solution should be covered by 3 Years 24x7 support with NBD hardware replacement		
A.2	Capable to integrate with SIEM and PIM		
A.3	Capable to integrate with Enterprise monitoring tools (HPOV)		
A.4	Bidder should have OEM certified atleast 2 engineers based on Uganda for local support (Certificates copy and work permit copy to be submitted)		
A.5	EOL/EOS should not be before 5years from date of installation. Also device should not be declared end of sale during installation.		

Sr. No	Firewalls Features (3 Units)	Compliance (FC, PC, NC)	Comments
B	***General Requirements:***		
B.1	The solution must be appliance based and should facilitate multi-application environment.		
B.2	Should must be a leader in both Gartner UTM and Enterprise Firewall Quadrants		
B.3	The platform must use a security-hardened, purpose-built operating system, and should support the deployment option in NGFW and UTM mode.		
B.4	The platform should use hardware acceleration (SPUs) to optimize the packet, encryption/decryption and application level content processing.		
B.5	Licensing: should be per device license for unlimited users for Firewall / VPN (IPSec & SSL) and other features. There should not have any user/IP/host based licenses .		
B.6	The solution must support Virtualization (i.e. Virtual Systems / Virtual Domains).		
B.7	Each Virtual Domain should be allowed to connect to Specific 3rd Party Authentication service, AD, Radius, Tacacs or other…		
B.8	Should support more than one ISP with automatic ISP failover		
B.9	Should have support for Explicit Proxy and Transparent Proxy		
B.10	Must form the heart of the security fabric by integrating networking and security solutions and 3rd party fabric solutions		
B.11	Must have a fabric compliance tool that automates the analysis of the security fabric deployment to identify potential vulnerabilities and propose best practices to improve the security effectiveness of the deployment		

C.1	Should support a minimum of 18x1GE RJ45 interfaces & 16x1GE SFP		
C.2	Should support purpose built processors (SPUs)		
C.3	Should support a firewall throughput of at least 20Gbps		
C.4	Should support a minimum of 4 million concurrent Sessions		
C.5	Should support a minimum of at least 300,000 new sessions per second		
C.6	Should support a IPS throughput of at least 5Gbps		

D	***Security Requirements:***		
D.1	Must support Web Filtering		
D.2	Must support an integrated NGIPS engine		
D.3	Must support an integrated Anti-Malware engine		
D.4	Must support an integrated Application Control engine		
D.5	Must support the ability to identify unknown malware by using a cloud based sandbox solution		
D.6	Must support Botnet IP/Domain reputation services		
D.7	Must support Mobile Security Services		

E	***Firewall Features Requirement:***		
E.1	The Firewall should be ICSA Labs certified for Enterprise Firewall or EAL 4 certified, if not the same model		
E.2	It should be possible to operate the firewall in "bridge mode" or "transparent mode" apart from the standard NAT mode		
E.3	The Firewall must provide NAT functionality, including PAT.		
E.4	Should support "Policy-based NAT"		
E.5	The Firewall should provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP		
E.6	Firewall should support Voice based protocols like H.323, SIP, SCCP, MGCP etc and RTP Pinholing.		
E.7	The Firewall should support User-Group based Authentication (Identity based Firewalling) & Scheduling		
E.8	IPv6 support for both NAT and Transparent Mode		

F	***Authentication Requirements:***		
F.1	Support for authentication at the firewall policy level (Local and Remote)		
F.2	Support for RSA SecureID or other Token based products		
F.3	Support for external RADIUS, LDAP and TACACS+ integration for User and Administrator Authentication		
F.4	Support for Native Windows Active Directory or Novell eDirectory Integration		
F.5	Should support authentication based on LDAP Groups		
F.6	Should support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators		

G	***Encryption / VPN Requirements***		
G.1	The VPN should be integrated with firewall and should be ICSA Labs certified for both IPSec and SSL-TLS		
	Should support the following protocols:-		
a	DES & 3DES		
b	MD5, SHA-1 & the more secure SHA-256 authentication		
c	Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.		
d	Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm		
e	The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)		
G.2	Should support Hub and Spoke VPN topology		
G.3	IPSec NAT Traversal & Dead Peer Detection should be supported		
G.4	IPSec VPN should support XAuth over RADIUS and RSA SecurID or similar product.		
G.5	Should have integrated SSL VPN with no user license slab restriction. Please specify if the product does not follow the required licensing policy		
G.6	Should support SSL Two-factor Authentication with Digital Certificates		
G.7	Should support Single Sign-On Bookmarks for SSL Web VPN		
G.8	Should support Windows, Linux and MAC OS for SSL-VPN (Should have always-on clients for these OS apart from browser based access)		
G.9	Should support NAT within IPSec/SSL VPN tunnels		
G.10	Should also support PPTP and L2TP over IPSec VPN protocols.		

H	***High Availability Requirements:***		
H.1	The device must support Active-Active as well as Active-Passive redundancy.		
H.2	The Firewall must support stateful failover for both Firewall and VPN sessions.		
H.3	The HA Architecture should have the ability for Device Failure Detection and Notification as well as Link Status Monitor		
H.4	Should support VRRP and Link Failure Control		

I	***DataCenter Optimization:***		
I.1	Should support Server Load Balancing with features like HTTP persistence		
I.2	Should support TCP Multiplexing		
I.3	Should support HTTPS Offloading with flexible Digital Certificate Management		
I.4	Should have support for WCCP and ICAP protocols		

J	***Administration/ Management Requirements:***		
J.1	The device must support Web UI (HTTP/HTTPS) and CLI (Telnet / SSH) based Management		
J.2	Should have configurable option to define remote access to the Firewall on any interface and restrict the same to a specific IP/Subnet (i.e. Trusted Hosts for Management)		
J.3	There must be a means of connecting directly to the firewall through a console connection (RJ45 or DB9)		
J.4	The device should have SNMPv2c and SNMPv3 support (for sending alerts to NMS in case of threats and system failures).		
J.5	Provision to generate automatic notification of events via mails / syslog		
J.6	Provision to send alerts to multiple email recipients		
J.7	Support for role based administration of firewall		
J.8	Should support simultaneous login of Multiple Administrators.		
J.9	Should have provision to customize the dashboard (eg: by selecting suitable Widgets)		
J.10	The Firewall must provide a means for exporting the firewall rules set and configuration to a text file via Web or TFTP		
J.11	Support for Image upgrade via FTP, TFTP and WebUI		
J.12	Should support system software rollback to the previous version after upgrade		
J.13	Event Management Raise and monitor important events to present the IT administrator with unprecedented insight into potentially anomalous behavior and have Indicator of compromise module.		
J.14	Import/Export Templates After building a report, export and modify the configuration		
J.15	View logs in real-time or historical		
J.16	Select from traffic, event and full security logs		
J.17	Browse by device,		
J.18	Log filtering and search capabilities		
J.19	Granular inspection with the log details pane		
J.20	Deliver and monitor Secure SD-WAN from one console across your network		
J.21	Manage all products, including firewalls,		

K	***Network IPS:***		
K.1	Should have integrated Network Intrusion Prevention System (NIPS) and should be ICSA Labs certified.		
K.2	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
K.3	Should have protection for 3000+ signatures		
K.4	Able to prevent denial of service and Distributed Denial of Service attacks.		
K.5	Should be able to exclude certain hosts from scanning of particular		

	signatures		
K.6	Supports CVE-cross referencing of threats where applicable.		
K.7	Should provide the facility to configure Profile based sensors (Client/Server) for ease of deployment		
K.8	Should support granular tuning with option to configure Overrides for individual signatures.		
K.9	Supports automatic Attack database updates directly over the internet. (i.e. no dependency on any intermediate device)		
K.10	Supports attack recognition inside IPv6 encapsulated packets.		
K.11	Supports user-defined signatures (i.e. Custom Signatures) with Regular Expressions.		
K.12	Supports several prevention techniques including Drop-Packet, TCP-Reset (Client, Server & both) etc. List all prevention options		
K.13	Should offer a variety of built-in responses including dashboard alerts, syslog / email notifications, SNMP traps and Packet Capture log. List all response options, excluding prevention responses		
K.14	Should Identify and control over 1000+ applications (i.e. Application control feature)		
K.15	Should perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc		
K.16	Should control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc		

L	***Gateway Antivirus***		
L.1	The appliance should facilitate embedded anti virus support which is ICSA Labs certified		
L.2	Should include Antispyware and Worm Prevention		
L.3	Should have option to schedule automatic updates of the new virus pattern.		
L.4	Gateway AV should be supported for real-time detection of viruses and malicious code for HTTP,HTTPS, FTP, SMTP, SMTPS, POP3 and IMAP, NNTP and IM		
L.5	Should have configurable policy options to select what traffic to scan for viruses		
L.6	Should have option to configure to respond to virus detection at the gateway in several ways ie. Delete the file, Alert email, Quarantine etc		
L.7	Should have options to prevent user downloads based on file extension as well as file type		
L.8	Should have support for “Flow-Based Antivirus Scanning Mode” for high throughput requirements		
L.9	The solution should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
L.10	Should have an ability of Antivirus scanning for IPv6 traffic		

M	*Advanced Threat Protection*		
M.1	The solution should be tightly integrated with the cloud threat mitigation in order to make the protection more effective and updated so as to minimize the occurrence of false positives.		
M.2	The solution should have multi layer of detection process with the malicious code emulation and execution in the VM environment.		
M.3	The solution should be able to inspect the web session to detect and notify the malicious web activity including malicious file downloads through the web/internet.		
M.4	The solution should be able to store payload and artifacts of the detected threats for further analysis and incident time lines that is with the third party as well.		
M.5	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executable, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks.		
M.6	The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution should also assign a unique identification number to each identified/detected threat for future reference.		
M.7	The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration		
M.8	The solution should be part of an integrated model therefore it should interact with other security network element in order to give full proof detection and correction model rather than having a point product.		
M.9	The solution must be able to detect and report malware by using multiple client environments (operating systems with multiple service pack levels) supporting both x64 and x86 architectures.		
M.10	The solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions		
M.11	The solution should be based on algorithm, which should be able to detect maximum Malware or rogue elements with each signature.		
M.12	The solution should have ability to block all outbound call- back communication initiated by the internal clients (infected)		

N	***Web Content Filtering***		
N.1	The appliance should facilitate embedded Web Content Filtering feature		
N.2	Web content filtering solution should work independently without the need to integrate with External proxy server.		
N.3	Should have facility to block URL' based on categories. Should support HTTP and HTTPS based traffic.		
N.4	URL database should have more than 2 billion URLs under 70+ categories.		
N.5	Should be able to block different categories/sites based on User Authentication.		
N.6	Should have configurable parameters to block/allow unrated sites. Should have option to locally rate sites.		
N.7	Should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable		
N.8	Should have options to customize the “Blocked Webpage Message” information displayed to end users		
N.9	Should have facility to schedule the configurations so that non-work related sites are blocked during office hrs and allow access to all sites except harmful sites during non office hrs. Should also have time-based quota		
N.10	The solution should have options to block java applets, ActiveX as well as cookies		
N.11	The solution should be able to block URLs hosting spywares / adwares etc.		
N.12	Should have configurable policy options to define the URL exempt list		

O	***AntiSpam***		
O.1	Should have integrated support for AntiSpam for the following protocols: SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS		
O.2	AntiSpam database should have updates for Real-Time Blacklist and Open Relay Database Servers		
O.3	Automatic Real-Time Updates of AntiSpam database		
O.4	Should perform MIME Header Check		
O.5	Should have facility for Keyword/Phrase Filtering		
O.6	Should be configurable for IP Address Blacklist and Exempt List		

P	***Certifications***		
P.1	Should have support for the following certifications:		
P.2	FIPS-140-2 for Client VPN software		
P.3	OS should be “IPv6 Phase II Ready” certified		

****