REQUEST FOR PROPOSAL

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.

Details as under

Description	Configuration	Quantity
Firewall	Information gathering and solution design Installation of Firewall and firmware upgrade Firewall clustering Firewall security zoning and policy Configuration of IPS, antivirus, web filtering etc Integration with banking services	4

The above should abide to the following specifications

Sr. No.	**Required Minimum Specifications** **Make & Model: _____**	Bidder's compliance (Yes / No)	Bidder's remarks
A	Industry Certifications and Evaluations		
1	The proposed vendor must have a track record of continuous improvement in threat detection and must have successfully completed NSS Labs'		
2	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.		
3	Each Appliance should have at least 16 X GE RJ-45 Ethernet interface & 1 GE Management, & Console Interface. The networks switches supports 1Gb interface, hence relevant optics or cables for connecting with the switches needs to be factored.		
B	Platform Requirement		
1	The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes.		
2	The device should have functionality of hardware / Software Fail Open		
3	The solution should support Active/Passive load balancing with stateful Failover		
C	Performance & Scalability		
1	Should have minimum Inspected throughput of 2 Gbps for all kinds of real word traffic after enabling the IPS and Application visibility feature		
2	Should support minimum 1 million concurrent connections or more and minimum 12000 new connection per second with Application Visibility and Control.		

Sr. No.	**Required Minimum Specifications** **Make & Model: _____**	Bidder's compliance (Yes / No)	Bidder's remarks
3	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades. Firewall Appliance should have on-box storage capacity for OS images & log storage		
D	URL Filtering		
1	Should be able to create policy based on URLs specifying in the rules		
2	Should be able to define URL category based on Risk level		
E	AMP		
1	Appliance should be capable of working in Inline Blocking mode without depending on other network components like a separate FW, IPS or Web Security Appliance. AMP license should be given from day 1.Solution should be capable of identifying zero days threat and same should be considered from day one.		
2	Solution should be capable of blocking call-backs to CnC Servers		
3	Solution should be capable of blocking threats based on both signatures and behaviour		
4	The anti-APT Solution should be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behaviour of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.		
5	Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.		
6	The solution should be capable to analysis & block TCP and UDP protocols to identify attacks and malware communications. At a minimum, the following protocols are supported for real-time inspection, blocking and control of downloaded files: HTTP, SMTP, POP3, IMAP, Netbios-ssn and FTP.		
7	The solution should be capable of protecting against spear phishing attacks		
8	The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.		

Sr. No.	**Required Minimum Specifications** **Make & Model: _____**	Bidder's compliance (Yes / No)	Bidder's remarks
9	**The solution should detect and classify mobile devices as mobile devices. For example: iPad, iPhone and Blackberry devices. These devices should be discovered and related back to the user, applications, and possible services they offer**		
10	The solution should be capable of whitelisting trusted applications from being inspected and not an entire segment to avoid business applications from being affected & in turn productivity		
11	The solution should be capable of blocking traffic based on geo locations to reduce the attack landscape and to protect communication to unwanted destinations based on geography		
12	The solution shall be able to detect attacks on 64-bit operating systems		
13	All the devices shall be managed centrally and should be capable of • Centralized, life cycle management for all sensors • Aggregating all events and centralized, real-time monitoring and forensic analysis of detected events • Must provide a highly customizable dashboard		
14	**The proposed solution must be capable of passively gathering information (without active scanning) about network hosts and their activities**		
15	The proposed solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.		
16	The proposed solution must be capable of passively detecting pre-defined services, such as FTP, HTTP, POP3, Telnet, etc., as well as custom services.		
17	The proposed solution must be capable of storing user-defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.		
18	The proposed solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.		
19	The proposed solution must have a granular rule mechanism that allows specifying what type of traffic and transfer context will be subject to the process of analysis and prevention of advanced malware in real time.		
20	The proposed solution must Detect, control access and inspect for malware at least the following file types:		

Sr. No.	**Required Minimum Specifications** **Make & Model: _____**	Bidder's compliance (Yes / No)	Bidder's remarks
	Microsoft Office files, executables, multimedia, compressed documents, Windows dump files, pdf, jarpack, install shield.		
21	The proposed solution must have capability to Analysis of APTs and malwares must be performed in real-time using hybrid analysis capabilities, using various analysis and control strategies, including simultaneously, whether the local, remote or hybrid execution technology for the determination of advanced malware.		
22	The proposed solution must allow granular definition of the type of compressed files to be analysed, including traffic control options and their access to preventive actions.		
23	The NBA capability must provide the ability to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
24	**Should provide out of box Categories based on Application types, Security Risk level etc**		
F	Management		
1	The management platform must be available in virtual form factor.		
2	The management platform must be accessible via a web-based interface and ideally with no need for additional client software		
3	The management platform must provide a highly customizable dashboard.		
4	The management appliance should be able to support 25 appliance if required in future		
5	The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.		
6	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward		
7	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
8	Should support REST API for monitoring and config programmability		
9	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
10	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		

Sr. No.	**Required Minimum Specifications** **Make & Model: _____**	Bidder's compliance (Yes / No)	Bidder's remarks
11	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
12	The management platform must risk reports like advanced malware, attacks and network		
13	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.		
14	Centralized Management Server should be deployed in VM (to be provided by Bank) and all necessary license should be provided from day one.		
G	Licensing Requirement		
1	Solution should have enterprise license without any restrictions.		
2	Solution should be on Distributed Architecture for Threat Prevention along with Dedicated Management, Logging and Reporting Framework.		
3	The offered product part codes have to be General Availability Part codes and not custom built. There should be reference of Products to the public website of the OEM		
4	Any third party product required to achieve the functionality should be provided with the necessary enterprise version license of software/appliance		
H	High Availability Requirements:		
1	The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.		
2	The HA solution should support Active/Active or Active/Passive load balancing with state full Failover		
3	The High Availability should be supported in the Firewall from the day one and without any extra license		
4	The upgrade of HA pair should be seamless without any downtime		
5	HA solution deployed should support hitless upgrade for both Major and Minor codes		
I	Logging & Reporting		
1	Must integrate with centralized logging & reporting solution of same OEM for better reporting		
2	Also should have feature to integrate with syslog & SNMP server		

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 **18.02.2019 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: 29.01.2019