




**Establishment & General Services Division, BCBL, Head Office,**  
Eunoos Trade Center, Level-22, 52-53, Dilkusha, Dhaka.

**Invitation for Tender**

|                          |  |   |
|--------------------------|--|---|
| Invitation for Tender    |  |   |
| 01.                      | Agency   | Bangladesh Commerce Bank Limited  |
| 02.                      | Procuring Entity Name  | Bangladesh Commerce Bank Limited, Estt & GSD Division, Head Office, Dhaka   |
| 03.                      | Procuring Entity District  | Dhaka, Bangladesh   |
| 04.                      | Invitation Ref No  | Tender # 2021/02  |
| 05.                      | Date   | 08/04/2021  |
| 06.                      | Procurement Method   | Limited Tendering Method  |
| 07.                      | Budget and Source of Fund  | Own source of BCBL  |
| 08.                      | Tender Package Name  | Web Application Firewall(WAF) for Our BCB Mobile App & E-KYC Solution Security.   |
| 09.                      | Tender Publication Date  | 08/04/2021  |
| 10.                      | Tender last selling date   | 21/04/2021  |
| 11.                      | Tender closing date & time   | 22/04/2021, 1.00 PM   |
| 12.                      | Tender opening date & time   | 22/04/2021, 3.30 PM   |
| 13.                      | Name & Address of Selling Tender Document  | Establishment & General Services Division, BCBL, Head Office, Eunoos Trade Center, Level-22, 52-53, Dilkusha, Dhaka.  |
|                          | Address of Receiving Tender Document   | Establishment & General Services Division, BCBL, Head Office, Eunoos Trade Center, Level-22, 52-53, Dilkusha, Dhaka. & <a href="mailto:etender@bcbl.com.bd">etender@bcbl.com.bd</a> Tender last receiving Date & Time: 22/04/2021, 1.00 PM. |
|                          | Address of Opening Tender Document   | Mini Conference Room, BCBL, Head Office, Eunoos Trade Center, Level-22, 52-53, Dilkusha, Dhaka.   |
| INFORMATION FOR TENDERER |  |   |
| 14.                      | Eligibility of Tenderer  | As per Tender Document.   |
| 15.                      | Brief Description of Goods   |   |
|                          | Web Application Firewall(WAF) for Our BCB Mobile App & E-KYC Solution Security.                                |   |
| PROCURING ENTITY DETAILS |  |   |
| 16.                      | Name of Official Inviting Tender   | Nazim Anwar   |
| 17.                      | Designation of Official Inviting Tender  | Senior Asst. Vice President   |
| 18.                      | Address of Official Inviting Tender  | Establishment & General Services Division, BCBL, Head Office, Eunoos Trade Center, Level-22, 52-53, Dilkusha, Dhaka.  |
| 19.                      | Contact details  | 02-47111036   |
| 20.                      | The procuring entity reserves the right to accept or reject any or all tenders (partly or fully) at any stage. |   |

  
Nazim Anwar  
Senior Asst. Vice President

Web Application Firewall(WAF) for Our BCB Mobile App & E-KYC Solution Security.

| Bangladesh Commerce Bank (BCB) Load Balancer, Web Application Firewall, Mobile APP Protection, & API Security Solution Specification |   |
|--|---|
| Product Names/Items  | Description of requirements   |
| Brand  | Reputed Brand those are leaders/Challengers in the Gartner's and Forrester Quadrant report for Web Application Firewall as per the latest report.   |
| Model  | To be mentioned by the bidder   |
| Country of origin  | To be mentioned by the bidder   |
| Manufacturing Country  | To be mentioned by the bidder   |
| Quantity   | 01 (One)  |
| Solution Architecture  |   |
| Solution Architecture Requirement  | The proposed solution as dedicated Virtual appliance based Next Generation Load Balancer, Web Application Firewall (WAF) with Mobile Application Protection and L7 DDOS Solution should be on single OS platform. Should have option to add Customizable Authentication Feature, DNS and Global Server Load Balancing Feature on same single OS platform based on future requirement.                                       |
|  | Proposed solution OEM must have complete API security and management module including API Gateway. Proposed WAF, API Security & L7 DDOS solution license should be perpetual.   |
| Proxy support  | The solution must support both Forward Proxy and Reverse proxy mode as a full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication.  |
| Traffic Segmentation   | The solution should support VRF, VXLAN, IPv6 VXLAN multipoint tunnels functionality for traffic & routing separation.   |
| Throughput   | Must be a Virtual appliance with hardened OS and available for VMware vSphere, Citrix XEN-Server, KVM, Community XEN and Microsoft Hyper-V. Bidder must be consider required OS / Virtualization license for deployment along with server hardware.   |
|  | The proposed solution should provide minimum L4 & L7 throughput of 200 Mbps   |
|  | Bangladesh Commerce Bank (BCB) will ensure Minimum 8 Core CPU, memory 16 GB and 200 GB HDD thin provisioning and for management access, one VMXNET3 vNIC or Flexible vNIC and data plane access, three VMXNET3 vNICs in Mellanox/Inter SR-IOV feature.  |
| Load Balancing   | The solution must have application-level load balancing including the ability to act as HTTP 2.0 Proxy.   |
|  | The solution must support TLSv1.0, TLSv1.1, TLSv1.2 and TLSv1.3 on both Client and Server side.   |
|  | The solution must have full proxy architecture with HTTP Keep-Alive to allow the load balancer system to minimize the number of server-side TCP connections by making existing connections available for reuse by other clients for TCP optimization.   |
|  | The solution must have server load balancing algorithms like (but not limited to) round robin, weighted round robin, least connection, Persistent IP, Hash IP, hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID, hash header, Observed, Predictive, Least session, least connections, super http, least latency, weighted round robin and TCL based script for customized algorithm etc. |
|  | The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers.   |
|  | The Load Balancer shall improve the user's experience by increasing server response time. Shall support Caching web content that saves network bandwidth requirements and reduce loads on backend web servers.  |
|  | The solution must have ICAP integration with other security devices for file scanning.  |
|  | The solution must have script-based functions support for content inspection, traffic matching and monitoring of HTTP, XML, generic TCP. Load balancer should support Policies to customize new features in addition to existing feature/functions of load balancer   |

|   |   |
|---|---|
|   | The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or a number of other factors. This enables organization to deliver customized application responses to users.  |
|   | To maximize outbound bandwidth, the Load Balancer shall automatically compress content to minimize network traffic between application servers and the end user.  |
|   | The proposed solution must be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session mirroring and persistence mirroring, HTTP Compression, caching etc. in active-passive mode. All the features should be enabled in Full-Proxy Mode.   |
|   | It should have the capability of Rate shaping & QoS Support to optimize and handle heavy Layer 4 through 7 traffic loads while delivering Latency Sensitive Applications  |
| <b>WAF Security Solution Requirements</b>     |   |
| Application Layer Encryption                  | WAF must have capability to protect Credential Attacks Protects against attacks that can steal credentials from the user's browser through browser-based malware, from data in transit and/or from the server without installing any agent at client machine.   |
| Industry Standard Cipher & Encryption Support | The WAF solution must support all major cipher suites like Camellia Ciphers Suites, SSLv3 and TLSv1.3 implementation for strong encryption from day 1. The WAF solution must support elliptic curve cryptography (ECC) acceleration in hardware.  |
| Application security vulnerabilities          | The solution must address and mitigate the OWASP Top Ten web application security vulnerability.  |
| Customizable authentication                   | Solution should support to function as Portal access, app tunnel, and network access with AAA server authentication and high availability and Step-up authentication, including multi-factor authentication (MFA) in future if required without any additional hardware change.   |
|   | The solution should support template-based access to authorized applications process to create customized portal to allow only those applications and resources a user is authorized to access.   |
|   | The solution should support inspection of the user's endpoint device with OS type, antivirus software, firewall, file, process, Windows OS registry value validation and comparison, device MAC address, CPU ID, HDD ID, mobile device UDID and jailbroken or rooted status through a web browser and through client to examine security posture and determine if the device is part of the customer domain. Based on the results, it can assign dynamic Access Control Lists to deploy user identity, data/application context and application-aware security. |
| Custom Security Policy Enforcing              | The solution must have ability to merge automatically built security policy with a manually built security policy or policy built from Industry standard Dynamic Analysis Security Testing (DAST) tools XML report.   |
| Security model approach                       | The solution must support both the positive and negative security model approach.   |
| OWASP Top 10—the foundational list            | Specially to protect against the of the most seen application vulnerabilities. This Top 10 currently includes:  |
|   | · Injection attacks   |
|   | · Broken Authentication   |
|   | · Sensitive data exposure   |
|   | · XML External Entities (XXE)   |
|   | · Broken Access control   |
|   | · Security misconfigurations  |
|   | · Cross Site Scripting (XSS)  |
|   | · Insecure Deserialization  |
|   | · Smarter bot detection using machine learning  |
|   | · Robust and rapid attack response  |
|   | · Advanced dashboarding capabilities  |
|   | · Real-time actionable threat intelligence  |
| Protection from vulnerable attacks            | The solution should support Network, DNS, and Application layer DoS and DDOS attacks protection including nxdomain, stress-based DOS and Heavy URL attacks.   |

|  |   |
|--|---|
| Security Rules                                 | The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria or capable with violation correlation engine. This should be possible without need to write any script/code.   |
| Protection from web-based attacks              | The solution should support protection against common attacks such as SQL Injection, Cross-site Scripting, Cookie or Form Tempering etc.  |
| Virtual patching                               | The solution must support integration with industry leading Dynamic Analysis Security Testing (DAST) tools of IBM, HP, Rapid7 etc. to perform virtual patching for its protected web applications.  |
| Webshell Attack Detection                      | The solution should have the capability of Webshell/Backdoor Detection.   |
| WebSocket and Secure WebSocket Protection      | The solution should have the capability of inspection and protection for WebSocket and Secure WebSocket of application.   |
| Malware/BOT Attack Detection                   | WAF should have capability of Proactive BOT Defense (both detection and Protection) mechanism beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating JavaScript and CAPTCHA challenges or equivalent. The BOT defense feature should have Predefined Bot Defense profile to enable quicker and easier BOT defense configuration. The signature should be updated periodically. |
| Brute Force Attack Detection                   | WAF should have capability of Brute Force attack detection by CAPTCHA challenges to clients and should be capable to redirecting Brute force attack traffic to Honey Pot page/System.   |
| CAPTCH Farming Attack Detection                | WAF should have capability to detect attack try to get around CAPTCHAS by farming out the CAPTCHA images to pools of user that respond.   |
| Security Engine                                | The solution must have in-built security engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol & application levels over time & correlate them to distinguish between attacks & valid user traffic.  |
| Malware protection from Man-in-The-Browser     | The WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks.   |
| L7 DDOS Protection for Application             | Solution must have protection against Layer 7 Application DDOS type of attacks in full-Proxy Mode (Forward Proxy and Reverse Proxy) using machine learning mechanism form day 1.  |
| Behavioral DoS mitigation technology           | Solution must have behavioral DoS mitigation Technology to detect DDOS attacks without human intervention.  |
| Upload protection                              | The solution should have protection against viral/infected file uploads through ICAP integration with 3rd party/antivirus/Sandbox solution.   |
| Pre-configured list of signatures              | The solution must include a pre-configured list of comprehensive and accurate web attack signatures.  |
| Staging for New Signature Update               | The solution must have signature staging feature for new signature update which will apply the new signatures to the web application traffic but does not block the application by trigger those new attack signatures. This feature is required to reduce the number of violations triggered by false-positive matches regarding new signature update.   |
| Worm protection                                | The solution must have web worm protection.   |
| CSRF checkbox attack protection                | The solution must have CSRF checkbox attack protection and mitigate Buffer overflows.   |
| Rate Limiting                                  | The solution must have Rate Limiting for Client and Application communication to limit the TCP communication during DDOS Attack.  |
| Protection against Cross- site Request Forgery | The solution should have protection against Cross-site Request Forgery.   |
| Protection against web site cloaking.          | The solution should have protection against web site cloaking.  |
| Outbound data security                         | The solution should have protection against outbound data theft.  |
| Anonymous request blocking                     | The solution should be able to detect and block request coming from anonymous proxies.  |

|  |   |
|--|---|
| Signature protection                                     | The solution should at the minimum query signature the signature service daily and automatically downloads and apply the new signatures. Before enforcing the new signature, there should be a feature to test as staging mode for application protection.  |
| Dynamic protection                                       | The solution should be able to encrypt the user credentials in real time i.e. when the user is typing the credentials for the web application in his/her browser for any web application that is behind the WAF. This feature should be agentless and should not require installation of any kind of software either on client end or on the application end.   |
| Geological threat protection                             | The proposed solution should have capability of Geo Location Blocking.  |
| Cloaking error situations                                | The solution should be able to "cloak" error responses to hide sensitive server related information in the response body and response headers.  |
| Detection and protection technology against threats.     | The solution profiling technology should be able to detect and protect against threats which are specific to the custom code of the web application. After the learning phase, the solution must be able to understand the structure of each protected URL and must be able to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.                         |
| Mobile Application Protection                            | Web application firewall must have protection from mobile app-based attacks. Solution must have capability to protect against the mobile application based attacks through Bot protection SDK for mobile platform which Whitelist establish trust based on an embedded software package within the application code and corresponding cookie verification to protect application against attacks generated from mobile. |
| Mobile Application Security Protection                   | The solution should have mobile app fusion process with the following hardening functionalities must be supported:  |
|  | • Obfuscation   |
|  | • Tamper protection   |
|  | • Checksum validation   |
|  | • App integrity scan  |
|  | • Anti-reversing  |
|  | Support the detection of compromised devices Jailbroken or Rooted with the ability to allow or block access of these, to the application  |
| Validation of different web services and ensure security | The solution must have the ability to logging events that include information about the request, action taken, name of the App, version, or if the device was jailbroken or rooted.   |
|  | The solution should be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.  |
|  | The solution should be able to protect web applications that include Web services (XML) content.  |
|  | The solution must have the ability to automatically update Certificate bundles from the appropriate CA's without any user intervention.   |
|  | The solution must be able to encrypt the user credentials of the protected applications in real time by encrypting the password without any agent either on the client side or on the server side. This feature could be activated at any time with additional license on the WAF when required.  |
|  | The solution should provide a mode whereby it can rewrite HTTP applications to HTTPS on-the-fly, e.g. by modifying all outbound content, and redirect incoming HTTP requests to the HTTPS.  |
|  | The solution should protect session tokens, i.e. cookies:   |
|  | a. Sign cookies, to prevent clients from changing them  |
|  | b. Encrypt cookies, to hide contents.   |
|  | c. Prevent Cookie Replay attacks  |
|  | d. Allow for exempting certain cookies from security checks   |
|  | The solution should support protection of XML Web Services with common web application as well as XML specific attacks.   |
|  | It should be possible to force conformance with full WS-I Basic specification.  |
|  | The solution should provide for validating XML Documents and protecting against XML, DOS, and injection attacks (SQL, OS, XSS injection, etc.).   |
|  | The solution should provide for validating SOAP messages, headers, and body against a WSDL schema.  |

|   |   |
|---|---|
| Supporting regular expressions                          | The solution must support regular expressions for the following purposes:   |
|   | - Signature definition  |
|   | - Sensitive data definition   |
|   | - Parameter type definition   |
|   | - Host names and URL prefixes definition  |
|   | - Fine tuning of parameters that are dynamically learnt from the web application profile.   |
|   | Vulnerability Assessment scanner support  |
|   | The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Qualys, Rapid 7, IBM APP scan etc. to virtually patch web application vulnerabilities.   |
|   | Monitoring Appliance  |
|   | The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode. The solution must be able to support Proxy SSL functionality also wherein the WAF will be able to inspect the SSL traffic without offloading it on to itself. |
| API Protection  | The solution must have API inspection, rate limiting, behavioral analysis, anti-automation, detects application program interface (API) threats and API protocol security check to secure REST API, JSON, XML/SOAP and Gateway APIs.  |
| Sensitive data masking                                  | The solution must support masking of sensitive data in alerts.  |
| Integration with security devices                       | The solution should integrate with syslog to work with any solution and support known log formats.  |
| Integration with SIEM tools                             | The solution should support integration with SIEM tools like Arcsight, Splunk or any other SIEM tool.   |
| PCI DSS Compliance                                      | The proposed WAF should provide PCI DSS compliance reporting.   |
| <b>Device Administration</b>                            |   |
| Troubleshooting   | The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot of appliance configuration and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link.                                     |
| Modify Signature  | The solution must allow administrators to add & modify signatures.  |
| Role based access                                       | The solution support role-based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator and Administrator.  |
| <b>OEM/Solution/Manufacturer Qualification Criteria</b> |   |
| Gartner or Forrester Report for WAF                     | OEM should be in the Gartner's and Forrester Leader's or challengers Quadrant report for Web Application Firewall as per the latest WAF report.   |
| ICSA Certification                                      | The Solution should be ICSA certified with publicly available reference for WAF & DDOS.   |
| Customer Reference                                      | OEM should have at least 5 customer references in Bangladesh in recent 3 years and At least 3 customer references should be publicly available for WAF.   |
| ISO 9001, ISO 14001 and ISO 27001 Certification         | The OEM/Manufacturer should have ISO 9001, ISO 14001, and ISO 27001 Certification. Bidder must submit the OEM's certificates.   |
| Design & Deployment Requirement                         | Respective bidder also needs to ensure that the final deployment of the Web & Mobile application security solution is done based on the standards design guideline and best practices keeping in mind the data center compliance requirements and operational requirements.   |
|   | Bidder has to ensure that the final deployment is done by the OEM certified resources to validate design standards and best practices. The cost of the implementation should quote as separate implementation cost.   |
| Manufacturer's part number                              | Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number.   |
|   | Bidder must submit the required performance document and compliance reference document for the proposed solution.   |
| Compliance & Reference                                  | Bidder must provide the detail compliance report with reference. The reference URL / information of RFP technical specification compliance should be publicly available, referenceable, and accessible document.  |

|                              |   |
|------------------------------|---|
| Warranty                     | Manufacturer's warranty part number should be mentioned, minimum 3 (three) Full years warranty for technical solution support with Patch & New Software Upgrade should be provided for the proposed solution from the date of commissioning.  |
| AMC                          | Bidder must ensure AMC year on year after three years for total offering and only subscriptions license separately.   |
| Training                     | At least three person training on WAF.  |
| Installation & Commissioning | Bidder must carry out on site installation, testing and commissioning by OEM authorized service partner in consultation with Bangladesh Commerce Bank Ltd. In consultation with Bangladesh Commerce Bank (BCB), bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the network functional and shall provide respective documentation to IT Division. |