BIDDING DOCUMENT

ADDENDUM NO. 1

National Competitive Bidding (NCB)

Package 02:

Procurement of Supply, Installation and Support of Virtual Web Application Firewall for Lanka Government Cloud (LGC 2.0) [IFB No: ICTA/GOSL/SER/NCB/2020/01/PK 02]

October 2020

Section V. Schedule of Requirements

1. List of Related Services

2. Technical Specifications

1.2 List of Related Services

Package No:	Item No	Description of Goods	Quantity Units	Delivery and Installation	Related Services
02	2.1	Virtual Web Application Firewall Solution for Throughput of minimum 25 Mbps	**2**	Within 6 Weeks from the date of Signing the Contract	Supply, Delivery, Installation, Commissioning and Maintenance
	2.2	Virtual Web Application Firewall Solution for Throughput of minimum 200 Mbps	**5**		

2. Technical Specifications

Bidders are required to state their compliance to specifications/requirements against each and every criterion of the specification sheets. Incomplete / non-compliant specification sheets will strongly lead to disqualification of the bidder without getting any clarifications.

Item No 2: Virtual Web Application Firewall Solution for Lanka Government Cloud (LGC 2.0)

Item No	Minimum Requirement	Compliance (Yes/No)	Remark / Reference Page#
2.1	The Virtual Appliance should be in the Gartner's MQ leaders or challengers for "Web Application Firewall" in any year in the last five published reports.		
2.2	The Solution should meet PCI DSS Compliance as per PCI DSS requirement and should provide reports for PCI DSS compliance.		
2.3	The solution should address and mitigate the OWASP Top 10 web application/ mobile application security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability is addressed by the solution)		
2.4	The proposed solution should be a VM (Virtual instance/Virtual machine) based solution.		
2.5	Virtual Appliance(instance/machine) should support on Redhat OpenStack Platform (KVM hypervisor)		
2.6	Solution should be able integrate with OpenStack HEAT template		
2.7	Proposed solution's Heat templates should follow the OpenStack Heat Orchestration Template (HOT) specification		
2.8	The proposed solution should be deployed leveraging separate WAF instance for each group of Ministries/Departments in high availability pair.		

Item No	Minimum Requirement	Compliance (Yes/No)	Remark / Reference Page#
2.9	The Proposed WAF Solution should be able to work in High Availability (HA) mode and should be deployed in an Active-Standby & Active-Active in both DC & DR		
2.10	The product should comply and support IPv4 and IPv6 both and NAT64		
2.11	Proposed WAF instance should be configurable in such a way that multiple network zones can be configured without sharing the data between them and without any compromise of security.		
2.12	The proposed solution should enable to redeploy, retire appliance as needed and align capacity with business requirements.		
2.13	- Removed -		
2.14	- Removed -		
2.15	Must be support dual-stack (IPv4 and IPv6) operation across all features "Should have full support IPv6. It should support all IPv6 scenarios: a. IPv4 on the inside and IPv6 on the outside b. IPv6 on the inside and IPv4 on the outside c. IPv6 on the inside and outside"		
2.16	Validation should be performed on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.		
2.17	When deployed as a proxy (either a transparent proxy or a reverse proxy), the Web application firewall should be able to digitally sign cookies, encrypt cookies, and to rewrite URLs.		
2.18	The Proposed WAF Solution should support both a Positive Security Model and a Negative Security Model. should provide regular update for CVE signatures.		
2.19	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for staging of policy and policy should move to Blocking ones Staging time is over.		
2.20	The solution must be able to block transactions with content matching for known attack signatures while allowing everything else.		
2.21	The solution must support and integrate with the web application vulnerability assessment tools (Web application scanners)		
2.22	Should be able to import Vulnerability scanner report from well known/qualified various vulnerabilities assessment tool and fixed those vulnerabilities within the waf using xml file.		
2.23	The solution must support both URL rewriting and content rewriting for http header and body when it is deployed in the reverse proxy mode.		
2.24	The solution must support user tracking using both form-based and certificate-based user authentication. Solution should support API security including support for uploading swagger file.		

Item No	Minimum Requirement	Compliance (Yes/No)	Remark / Reference Page#
2.25	The solution must be able to validate encoded data in the HTTP traffic.		
2.26	The solution must be able to identify Web Socket connections and provide security for WebSocket including exploit against Server abuse, login enforcement, XSS and SQL injection.		
2.27	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection\learning mode.		
2.28	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.		
2.29	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.		
2.30	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.		
2.31	The Proposed WAF Solution should have capability to mitigate, learn and adapt to unique application layer user interaction patterns to enable dynamic defenses based on changing conditions		
2.32	The Proposed WAF Solution should have Correlated Attack Validation capability or Correlation features which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.		
2.33	The Proposed WAF Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.		
2.34	The proposed WAF Solution should be configured with real-time threat intelligence on known malicious sources, such as: **Malicious IP Addresses**: Sources that have repeatedly attacked other websites **Anonymous Proxies**: Proxy servers used by attackers to hide their true location **TOR Networks**: Hackers who are using The Onion Router (TOR) to disguise the source of attack **IP Geolocation**: Geographic location where attacks are coming from and block access **Phishing URLs**: Fraudulent sites (URLs) that are used in phishing attacks.		
2.35	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript,		

Item No	Minimum Requirement	Compliance (Yes/No)	Remark / Reference Page#
	Image and Sound CAPTCHA challenges. This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot.		
2.36	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behavior analysis, reverse DNS lookup		
2.37	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.		
2.38	The Proposed WAF Solution should have Threat Intelligence to Identify New Attack Vectors. Community Defense feature gather suspicious Web requests, validate that requests are attacks, and transform identified attacks into signatures.		
2.39	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.		
2.40	Solution should support Behavioral L7 DDoS mitigation to detect attacks without human intervention.		
2.41	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.		
2.42	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks		
2.43	Proposed solution should have an option to receive spam IP feed and able to blacklist them to reduce spam messages in forums and user boards of customer web applications.		
2.44	The Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client-side malwares		
2.45	The Proposed WAF Solution should protect API based communication between client & servers using all the relevant WAF signatures.		
2.46	Should provide encryption for user input fields to protect from browser-based malwares stealing users credentials		
2.47	Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings		
2.48	The Proposed WAF Solution must support deployment as inline proxy, one arm mode or similar.		
2.49	On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time.		

Item No	Minimum Requirement	Compliance (Yes/No)	Remark / Reference Page#
2.50	The solution must allow administrators to add and modify signatures.		
2.51	Proposed Solution should have ability of HTTP response logging.		
2.52	Solution should offer protection for FTP and SMTP protocols.		
2.53	Solution should support user-written scripts, that provide flexibility to control application flows.		
2.54	Proposed Solution Attack log entry should have action to accept further request like this in policy or reject such an attack in future.		
2.55	Proposed Solution should have ability to differentiate DoS mitigation action based on Attacker Source IP, device fingerprint, URL or Geolocation.		
2.56	Proposed Solution should have ability dynamically generate signatures for L7 DoS attacks. It should also be possible to make the dynamic signatures persistent across reboot and shareable.		
2.57	Proposed solution should be able to track unused elements in the policy and suggest to remove them after a specified period of time		
2.58	Proposed Solution should have ability to automatically detect software technology used on backend side to define signature sets required for defined Proposed Solution policy.		
2.59	Proposed Solution should have ability to configure way to analyze request payload based on custom rules for each URL entry configured in the security policy		
2.60	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data.		
2.61	The solution must support regular expressions for the following purposes: Signatures 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.		
2.62	The WAF instance should have option to enable x-forwarder option per service to log actual client IP in webserver logs even deployed in Reverse Proxy mode.		
2.63	The proposed solution should support min 800 contexts or partitions or multiple profiling separately for each application without any additional license.		
2.64	Separate policies should be applied for different applications configured on the same WAF		
2.65	The solution should have pre-built templates for well-known applications eg, ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings		
2.66	All web facing applications are to be integrated to WAF without any limitation on the number of application. Solution should support the deployment modes based on application		

Item No	Minimum Requirement	Compliance (Yes/No)	Remark / Reference Page#
	needs		
2.67	Should support Integrated Web Application Load balancing that helps to reduce latency and gives singular window of management. WAF & Load balancer should be on the same virtual instance		
2.68	Solution should support below load balancing algorithm: Round Robin, Ratio, Least Connections, Weighted Least Connection, Ratio Least Connection or similar features.		
2.69	"Solution should support below persistence methods: Cookie Persistency Source Address Destination Address"		
2.70	Solution should support below monitors: FTP, Gateway ICMP, HTTP, HTTPS, ICMP, SOAP, TCP, TCP Half Open, UDP		
2.71	The proposed model should be scalable to support the following optional additional features to ensure application security and business continuity with licenses as below with or without additional cost: Remote Access via SSL VPN & SSO Solution - To control & secure user access of Internal Applications Global Server Load Balancing - To load balance the traffic across multiple sites based on Geo location, latency and other metrics DNS Firewall - To protect from dns based attacks DDoS Protection - To protect against L4 DDoS attacks		
2.72	Proposed solution should be able to integrate with external SSL visibility solution		
2.73	Proposed solution should also integrate with SIEM i.e. IBM Qradar		
2.74	The solution should also support sending of logs in CEF (Common Event Format) standard		
2.75	Management solution should support Role-Based Access Control or multiple user roles that facilitate separation of duties. i.e. Administrator (Super-User), Manager, SSL Certificate Manager		
2.76	Proposed solution should support multiple administration domains (or partitions) to configure and administer the system. This would include support for using remote authentication servers (e.g. LDAP, Windows AD, RADIUS and TACACS+) to store system user accounts.		
2.77	Where a single WAF instance maybe dedicated for an entire ministry, the Proposed solution should be able to delegate management of web application security contexts to individual department within specific		

Item No	**Minimum Requirement**	**Compliance (Yes/No)**	**Remark / Reference Page#**
	ministry. Individual department application security owners should have modification and visibility rights only to their own department.		
2.78	Proposed solution should provide account creation with access level that can Provides User roles that can be assigned such as Administrator, Resource Administrator, User Manager, Manager, Application Editor, Application Security Policy Editor, Operator, or Guest. It can be no access for user account to system resources Provide administrative partition(similar) where it limit user access to certain device objects which include entities that user accounts can manage and place in administrative partition.		
2.79	Proposed Solution should have Role-based management with user authentication. There should be web application security administrator (or similar)whom has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor(or similar) whom configure or view most parts of the web security policy object in specific controlled partition holding the policy and profile objects.		
2.80	Organization should be able to deploy or remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.		
2.81	Should be able to view and compare policies.		
2.82	Should be able to manage Bot Defense with real-time visibility to reflect the amount of automation traffic hitting the applications.		
2.83	Should provide extensive visibility into the health and performance of applications with dashboards to highlight applications with longest response time, top HTTP transactions, Top connections.		
2.84	Reporting and logging of all HTTP data and the application level including HTTP headers, form fields, and the HTTP body. Support proper Reporting and Logging facilities.		
2.85	Solution Should have centralized Management that provides a unified point of control for the Web Application Firewall. Push centralized software updates. **(Optional** if WAF appliance have self capable to get software updates directly and self management capability.)		
2.86	Solution should be able to manage policies, licenses, SSL certificates, Letsencrypt certificates, images, and configurations for all the WAF instances		
2.87	Should have predefined roles/permissions configurations to manage who can see application dashboards and edit and deploy services and policies for application delivery and security.		
2.88	Should be able to report events via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution.		
2.89	The solution must support generation/ both predefined as well as custom built reports as per Organization's requirements with both tabular views, pdf and data analysis graphical views.		
2.90	Solution should have the option to classify the bad or suspected bot type and provide detailed dashboard based on the bad/suspected BOT		

Item No	Minimum Requirement	Compliance (Yes/No)	Remark / Reference Page#
	types		
2.91	"The solution must have an integrated dashboard containing various features of alert and report generation including: a. CPU Usage b. Memory Usage c. Connections Statistics d. Throughput Statistics (Client Side and Server-Side throughput) e. Application services Status f. Application Server Status"		
2.92	OEM (principle) of the Proposed Solution should provide regular updates to geo-location database from their public downloads website		
2.93	should have Support Centers / Service Center or 24x7x365 TAC Support		