2021

الجمهورية اليمنية
شركة يمن موبايل للهاتف النقال
إدارة المشتريات والمخازن

المواصفات الفنية

لمشروع شراء وتوريد وتركيب وتشغيل

نظام جدار الحماية للتطبيقات

Web Application Firewall (WAF)

Technical Specification

1- Deplyment Requiremnts:

- We have two main Data Centers At Sana'a city with many web applications that accessed from internet or from external 3rd parties API applications.
- We need the solution to protect the access to these web applications with 2 single nodes appliance Web Application Firewall that can be upgraded to work in cluster mode by adding a second node in future.

2- The Statements Of Complaince SOC:

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
	WAF Functions Requirements		
	Hardware Architecture and Performance		
1	Appliance 500k-650K L7 requests per second		
2	L4 connections per second: 250K-500k		
3	L4 HTTP requests per second: 1M-2M		
4	L4 concurrent connections: 28M-40M		
5	Throughput: 10-20 Gbps L4/L7 SSL 6.5K-10K TPS (2K keys)		
6	The proposed solution should be Support different deployment modes.		
7	Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address.		
8	The proposed solution should provide the admin to manually accept false positives		
9	The proposed solution should be able to restrict traffic both on the basis of number of files in a request and the size of the file in a request.		
10	The proposed solution should be able to expandable in future.		
13	The Proposed WAF Solution should support line-speed throughput and submillisecond latency so as not to impact Web application performance.		
14	When scaling the solution, the solution must support a scale-out approach by having only to add more WAF appliances as needed.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
15	The Proposed WAF Appliance should support 4 X 1 G Copper and 2 Fiber 10G SFP+ at minimum and be populated from Day1 i.e. 3 separate segments can be configured. These interfaces should be upgradable\ degradable to 1G SFP/ 1G Copper without any cost to Yemen Mobile Company.		
	Administration and Management Requirements		
1	The Proposed Appliance should include a Web based single administration interface.		
2	The Proposed Appliance should have an out-of-band management port.		
3	Management solution should be capable to manage all the proposed WAF appliances and up to 10 appliance at minimum		
4	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		
5	The solution should support the following authentication mechanism for accessing the solution In-built authentication in the solution - Kerberos authentication - LDAP authentication - RADIUS authentication		
6	The solution must be able to operate in FIPS (Federal Information Processing Standard) 140-2 compliance mode.		
7	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.		
8	Ease of Management, Simplify creation for the security policies to immediately address common attacks on web applications, including HTTP(S) attacks.		
9	able to automatic learning to minimize the configuration errors, and ensure the overall effectiveness of each policy.		
10	Ease of management support simplify policy creation, can deploy WAF with security policies that immediately address common attacks on web applications, including HTTP(S) attacks.		
	Deployment and Operational Requirements		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
1	The Proposed WAF Solution must support deployment as inline proxy, one arm mode or transparent bridge mode.		
2	The solution appliance must have the option to support dual hot-swap hard drives and dual hot-swap power supplies for high availability		
3	The Proposed WAF Solution should support Monitoring Mode and Enforcement Mode of Deployment. In monitoring mode, the administrator can view alerts, attacks, server errors, and other unauthorized activity. In enforcement mode, the Web application firewall must proactively block attacks.		
4	The Web application firewall must protect both HTTP Web applications and SSL (HTTPS) Web applications. For SSL-enabled Web applications, the Web application firewall must decrypt SSL traffic between the client and server, and re-encrypt it before forwarding.		
5	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.		
6	The Web application firewall should be able to protect Web applications that include Web services (XML) content. Ideally, the XML protection should be similar to the Web application protection -with automated learning modes.		
7	The appliance should have feature of Inbuilt Packet logging and capture on demand		
8	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection.		
9	The solution must allow administrators to add and modify signatures.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
10	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		
11	The appliance should have option to enable **x-forwarder-to** option per service to log actual client IP in webserver logs		
12	The proposed solution should support unlimited context or partitions without any additional license. Segmentation controls application flow to respective gateway per server and should help multiple segment controls for various applications		
13	The proposed solution should have ability to divide a single setup in to multiple policies operating independently without compromising on network security		
14	Separate policies should be applied for different applications configured on the same WAF		
15	The solution should have pre-built templates for well-known applications. 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		
16	Solution should support the deployment modes without any limitation on the number of application.		
17	Dynamically boost performance with application optimization and acceleration technologies like fast caching, compression, and TCP optimization with centralized management, to easily scale to handle large volumes of traffic.		
18	WAF should detect Backend Server Failure and route the traffic to available server and should have capability of Load Balancing across the multiple servers		
19	WAF should have feature set to learn the application automatically whenever there is a change in application structure and should create a policy automatically for the newly learned application structure.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
	High Availablity Requirements		
1	The appliance should support Cluster failover with less than 3 second failover time. The End user session should be maintained during failover.		
	Support Requirements		
1	The Proposed WAF Solution should be provided with hardware replacement warranty and Ongoing Software Upgrades for all major and minor releases during the completion of project		
2	Original Equipment Manufacturer should have Stocking of Spares to ensure that the SLA is not breached		
3	Original Equipment Manufacturer of the Proposed Solution Vendor should provide regular updates to geo-location database from their public downloads website		
4	Original Equipment Manufacturer should have Support Centers / Service Center in the Middle East.		
	Security Requirements		
1	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	The Proposed WAF Solution should have an option to be configured in Reverse proxy mode.		
3	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.		
4	The Proposed WAF Solution should support both a Positive Security Model and a Negative Security Model.		
5	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.		
6	The solution must be able to block transactions with content matching for known attack signatures while allowing everything else.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
7	The solution must identify and mitigate the OWASP Top Ten web application security vulnerabilities.		
8	The WAF shall be able to identify and block OWASP Top Ten Ten attack classes in real time.		
9	The solution must support both URL rewriting and content rewriting for http header and body when it is deployed in the reverse proxy mode.		
10	The solution must support user tracking using both form-based and certificate-based user authentication.		
11	The solution must be able to validate encoded data in the HTTP traffic.		
12	The solution must be able to identify Web Socket connections.		
13	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.		
14	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.		
15	The solution must be able to protect web applications that include Web services (XML) content.		
16	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.		
17	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.		
18	The solution's profiling / learning mode must be able to recognize changes to the web application and simultaneously protect web applications at the same time.		
19	The solution profiling technology must be able to detect and protect against threats which are specific to the custom code of the web application. After the profiling/learning phase, the solution must be able to understand the structure of each protected URL.		
20	The Proposed WAF Solution should support automatic updates to the signature database, ensuring complete protection against the latest application threats.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
21	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.		
22	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.		
23	The Proposed WAF Solution Should support ICAP integration with other security devices for file scanning (industry leading security solutions i.e Symantec, MacAfee, Trend Micro and others.		
24	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 - Comment Spammers: IP addresses of known active comment spammers		
25	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 benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript/CAPTCHA challenges or other mechanisms. 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.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
26	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, framework etc.		
27	The Proposed WAF Solution should have Community Defense feature or should have a Crowd-Sourced 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. Equipped with Community Defense, Web Application Firewalls can spot attacks witnessed by other Web Application Firewalls-protected websites, it distributes these feeds in near-real time to fortify the entire community (of WAF) against Emerging threats.		
28	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.		
29	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks		
30	The Proposed WAF Solution must protect website user accounts from attack and takeover.		
31	The Proposed WAF Solution must have an option to have "Comment Spam IP Feed" to Block IPs to reduce spam messages in forums and user boards of customer web applications.		
32	The Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client side malwares		
33	The Proposed WAF Solution should protect API based communication between client & servers using all the relevant WAF signatures.		
34	The Proposed WAF Solution should protect Mobile Apps (both IOS & Android based) communication between client & servers using all the relevant WAF signatures.		
35	Protection Against Application Attacks, providing comprehensive geolocation attack protection from layer 7 DDoS, and zero-day web application attacks.		
36	can prevent execution of fraudulent transactions, stop in-browser session hijacking, and secure AJAX applications and JSON payloads.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
37	can defend against content and cookie modification, brute force login attempts and HTTP Parameter Pollution attacks.		
38	Support SSL offloading to maximize the utilization of the applications they protect, to keep processing work running smoothly.		
39	can terminate SSL traffic, expose what is inside it, and make security decisions based on the encrypted data.		
40	Automatic Attack Detection , malware and bot activity detection to investigate whether a web client source is human, an automated browser script, or even a headless browser.		
41	Bot-defense capabilities to deliver always-on protection - preventing automated web scraping from ever materializing.		
42	Able to detect attacks designed to run JavaScript, respond to challenges, and mimic human and browser capabilities without overburdening the applications it protects.		
43	Device ID and Fingerprinting ,Browser fingerprinting captures browser attributes in order to identify client or re-identify a visiting user, user agent, or device.		
44	Behavioral Analysis, can analyze and understand volumetric traffic patterns and then scan for anomalous behavior based on a set of related rules to assesses average server response time, transactions per second, and sessions that request too much traffic to use as a baseline for determining whether an attack has commenced.		
45	Should support authentication Gateway, secure single sign-on,two-step verification to avoid distributed attack.		
46	able to detect an anomaly when either too many sessions are opened from an IP address or when the number of sessions exceeds a set threshold, to make it easier to predict, identify, and respond to attacks.		
47	Should have feature set to learn the application automatically whenever there is a change should create a policy automatically for the newly learned application.		
48	WAF capabilities should include features that address the role in maximizing throughput factors directly :		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
	- Caching copies of regularly requested web content to reduces repeated requests to back-end servers.		
	- Automatic content compression to provide more efficient network transport.		
	- Hardware-based SSL acceleration to speed SSL processing and reduces the burden on back-end web servers.		
	- Load balancing web requests across multiple back-end web servers to optimize the performance.		
	- Connection pooling reduce back-end server TCP overhead by allowing multiple requests to use the same back-end connection.		
	Integration and Compliance Requirements		
1	PCI DSS Compliance		
2	Proposed solution should also integrate with Syslog kiwi, SIEM i.e. Solarwind Orion.		
3	Proposed solution should be able to integrate with external SSL visibility solution i.e. Kemp,F5 etc.		
	logging and Reporting		
1	Centralized Logging for any changes, Management, Configuration and Learned Policy Synchronization across proposed WAF Devices		
2	Unique transaction ID should be assigned to every HTTP transaction (a transaction being a request and response pair) and included with every log message.		
3	The following report formats are deemed of relevance: Word, RTF, HTML, PDF, XML, etc.		
4	The proposed solution should be able to log full session data once a suspicious transaction is detected.		
5	The proposed solution should be able to generate comprehensive event reports with filters like: a. Date or time ranges b. IP address ranges c. Types of incidents d. Geo Location of attack source		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
6	should have a mechanism for protection of unauthorized access on the Log Database by system administrator and should maintain an auditable chain of custody.		
7	Should Provide Application Performance Monitoring. Should Provide the Server Side, Network Side and User side latency statistics		
8	Should support content-based application monitoring for HTTP/HTTPs, FTP, POP3, IMAP, SIP, SMTP, RADUIS, LDAP, Oracle, MySQL and SOAP. (complete URI of GETs, POST Bodies, etc.).		
9	Should support External Customized Monitors to perform extended health-checks on application that has no built-in monitor template.		
10	The proposed solution should be configured to provide alerts/notifications of malicious attacks targeting the network of scope.		
11	Advanced incident handling for security operating centers (SOCs) and network operating centers (NOCs)		
12	The Web application firewall must:		
13	Report the events, alerts, HTTP data and the application level including HTTP headers, form fields, and the HTTP body((complete URI of GETs, POST Bodies, etc.).		
14	Support proper reporting and logging facilities.		
15	Should be able to report events via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution.		
16	Solution should have the option to classify the bad or suspected bot type and provide detailed dashboard based on the bad/suspected BOT types		
17	The ability to collect and analyze the data to provide visibility into attack and traffic trends, long-term data aggregation for forensics, acceleration of incident response, and identification of unanticipated threats before exposure occurs.		
18	Provide reports on web-based attempts to gain access to sensitive data, subvert the database, or execute DoS attacks against the database.		
	Training Requirements		
1	Original Equipment Manufacturer Certified Training for four Yemen Mobile employees each time after implementation & in 2nd & 4th year of operation.		

Sr. No	Product Specifications	Bidders Compliance (Yes / No)	Bidders Remarks, if any
	Bidder Requirements		
1	The proposed appliance must be latest but stable solution and must not be END OF LIFE/END OF SUPPORT/END OF ENGINEERING SUPPORT (which includes all kind of support viz. Hardware, Software etc.) till next five years from the contract start date or till the contract validity.		
2	If Proposed hardware appliance becomes End Of Life during said contract period,Original Equipment Manufacturer should continue to provide at least latest software and WAF signature updates till the contract is valid or provide new appliance without any additional cost to Yemen Mobile Company.		
3	Able to provide WAF Release quickly and dynamically, to offer more frequent release (quarterly vs. annually) to decrease the exposure and reduce the risk of applications becoming compromised by a new or emerging threat , by providing automatic signature updates in addition to the manual or scheduled option.		