नेपाल धितोपत्र बोर्डबाट अनुमति प्राप्त

प.लि.नं. १२७४-६७/६८

CDSC

सिडिएस एण्ड क्लियरिङ्ग लिमिटेड

(नेपाल सरकारको स्वामित्व भएको)

CDS and Clearing Limited

(An Undertaking of Government of Nepal)

CDSC

पत्र संख्या :२०८२/८३-११
चलानी नं. : ६३५

मिति :२०८२/११/१४ गते

श्री सम्पूर्ण सेवा प्रदायक कम्पनीहरु.

बिषय : लागत अनुमान माग गरिएको बारे ।

महाशय

यस लि. को डाटा सेन्टरमा प्रयोग भईरहेका F5, R5800 Advanced WAF with Load Balancer तथा VMware Viztulation को License Renewal गर्नुपर्ने भएकोले संलग्न बमोजिमको Specification अनुसारको License खरिदका लागि लागत पेश गर्नुहुन सम्बन्धित सेवा प्रदायकहरुका लागि यो सुचना जारी गरिएको छ ।

संलग्न :

१. License Renewal का लागि आवश्यक Specification - एक थान ।

कन्चन सापकोटा
उपप्रबन्धक
प्रशासन तथा जनशक्ति महाशाखा

Request for the Cost estimation for the Product required for CDS and Clearing Limited:

1.	**VMware vSphere Foundation 288 Cores Including 3 Years OEM & Local Support**
2.	**License & support renewal of Advanced WAF** **(BIG-IP SERVICE: PREMIUM, (LEVEL 1-3) F5-BIG-LTM-R5800,** **BIG-IP SERVICE: PREMIUM, (LEVEL 1-3) F5-ADD-BIG-AWF-R5XXX and** **BIG-IP Subscription: Threat Campaigns License Advanced WAF (r5xxx)) x 2 Units for 3 Years** **or** **Replacement by new 2 Unit of Advanced WAF with Load balancer that is equivalent to existing F5-R5800(BIG IP) or higher technical specification support specified below that should be bundled with 3 Years license.**

Advanced WAF/ LOAD BALANCER	**Brand**	To be mentioned by the bidder, it should be of Reputed Brands those are Leaders/Challengers in the Gartner's Magic Quadrant report or Leader/Strong Performer in Forrester Wave report for Web Application Firewall at least once in last three years.
	Model	To be mentioned by the bidder
	Solution Architecture	**The proposed appliance should provide minimum 95 Gbps of L4 & 80 Gbps of L7 throughput.**
		The proposed appliance should support minimum 85 million L4 concurrent connections from day 1.
		The proposed appliance should support minimum 1.4 million L4 connections per second from day 1.
		The proposed appliance should support minimum 18 million L4 HTTP requests per second from day 1.
		The proposed solution should have minimum 2 x 100G/40G QSFP+/QSFP28 Gigabit Fiber ports & 8 x 25G/10G SFP28/SFP+ Gigabit Fiber ports. Bidder must provide 8 x 10 Gbps SFP+ pluggable optical Transceivers for each appliance.

		The proposed appliance should support minimum 40 Gbps of SSL based Hardware Offloading throughput from day 1. The SSL encryption & decryption process must be hardware-based processor for acceleration.
		The proposed appliance must support minimum SSL TPS of 80K with RSA 2K SSL TPS keys and SSL TPS of 50K with ECDHE-ECDSA P-256 TPS keys from day 1.
		The solution should provide HTTPS interface management for administering the WAF.
		The solution should provide SSH interface management for administering the WAF.
		The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot of appliance config 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.
		The solution should support High Availability for both TCP session mirroring and SSL session mirroring in full-proxy (Forward Proxy and Reverse Proxy) mode in Active-Standby HA Architecture.
	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 implementations 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 vulnerabilities like: -> 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.
	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.
	Protection from vulnerable attacks	The solution should support Application Layer DoS and DDOS attacks protection including nxdomain, low and slow attack and HTTP flood Attacks.
	Custom 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 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.
	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.
	CAPTCHA Fraud Detection	WAF should have capability to detect attack try to get around CAPTCHAS to determine whether the client is operated by a human user or false CATCHA farming fraud or Machine/Software tool request.
	Security Threat Protection from organized crime and nation states	WAF should have security signatures to protect applications from pervasive attacks that are often coordinated by organized crime and nation states by providing threat intelligence information to fingerprint and mitigate sophisticated attacks with nearly real-time updates by metadata.
	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 Attack Prevention Feature (Operational from Day 1)	Solution must have protection against Layer 7 Application DDOS type of attacks including stress-based DoS and Heavy URL attacks in full-Proxy Mode (Forward Proxy and Reverse Proxy) using machine learning mechanism from day 1.
		The solution should provide Geo location IP detection of clients and blocking based on Geographical region of the clients.
		The solution should protect heavy URL L7 DDOS attack which consume considerable server resources for each request.
		The solution should protect Single Page attack which loads a single HTML page and dynamically updates the user interacts with the application to overload the Page loading time and server response time.

		The solution must have detected DDoS attacks based on the volume (transactions per second) of incoming Application traffic and protect the DDOS attack automatically by Application thresholds.
		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 the application response time. The BOT defense feature should have Predefined Bot defense profile to enable quicker and easier BOT defense configuration.
		The solution must include a pre-configured list of comprehensive and accurate web attack signatures
	Behavioral DoS mitigation Technology	Solution must have Behavioral DoS mitigation Technology to detect DDOS attacks without human intervention.
	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
	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.

	Policy Management for different web applications	The solution should support different policies for different web application. The solution must have pre-Configured policies for known applications like Microsoft SharePoint, OWA, ActiveSync, SAP, Oracle Applications/Portal, PeopleSoft, Lotus Domino for quick deployment.
	Outbound data security	The solution should have protection against outbound data theft.
	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 user 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.
	URL access control	The solution should allow the administrator to restrict access to various HTTP and WEBDAV methods, including HEAD, CONNECT, TRACE, etc. on a per URL basis.
		The solution must have capability of blocking access to specific URL path based on client-source-IP.
		The solution must have capability to restrict Restricting specific user (Administrators / web-admin / SQL admins) login from outside of network.
	Browser based keyloggers Protection	The solution must be able to defend against browser based keyloggers that attempt to capture user's keystrokes and steal user credential using password field encryption mechanism.
	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.
	Flexible custom report generation	The solution must have the functionality within the UI out-of-the-box that enables the administrator to create customized report on demand.

	Integration with SIEM tools	The solution should support integration with SIEM tools like RSA, IBM or any other SIEM tool.
	PCI DSS Compliance	The proposed WAF should provide PCI DSS compliance reporting.
	OWASP Top 10—Report Dashboard	The proposed WAF should provide OWASP Top-10 reporting Dashboard.
	ISO Certification	The OEM/Manufacturer should have ISO 9001, ISO 14001 and ISO 27001 Certification. Bidder must submit the OEM's ISO certificates.
	ISCSA Certification	Proposed WAF should be ICSA certified.
	Manufacturer’s part number	Bidder should submit BOQ of proposed device including the detail’s part numbers and Manufacturer’s Warranty part number.
	Compliance & Reference	Bidder must submit the required performance document and compliance reference document for the proposed solution.
		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.
	License and Warranty	The manufacturer’s warranty part number should be mentioned, and a minimum 3 (three) year warranty for technical solution support along with all the required licenses should be provided for the proposed solution from the **date of commissioning.**
	Manufacturer Authorization Letter/Form	Must provide manufacturer authorization letter/form Original Equipment Manufacturer (OEM)- it should be directly emailed to the CDSC’s official email(info@cdsc.com.np)