Jabalpur Smart City Limited (JSCL)

ManasBhavan Wright Town, Jabalpur, M.P-482001,www.jscljabalpur.org,
Contact:admin@jscljabalpur.org, ceojscl@mpurban.gov.in,Mob .7611136800

JSCL/2018/876 Date: 27/9/18

Corrigendum

This is with reference to No. JCSL/2018/837/ADM/148 dated- 10-09-2018"**Appointment of Implementation Agency for Supply, Installation and Management of Digital Library with Library Management Software (LMS) Integrated with RFID at GANDHI BHAWAN LIBRARY, Jabalpur**" in various newspapers. This is to inform to all that following amendments has been made, which is as under:-

Revised Schedule

Last Date for Purchasing Bid online	29-09-2018, 04:00 PM
Last Date for Submission of Bid (On-line)	29-09-2018, 05:00 PM
Last Date for Submission of Bid (Hardcopy)	29-09-2018, 05:30 PM
Date of Technical Bid Opening	29-09-2018, 06:00 PM
Date of Technical presentations	01-10-2018
Date of Commercial Bid opening	01-09-2018

Revised Annexure 1: Financial Bid Formats

Form 1 - Summary

Financial Bid for Appointment of IA for Supply, Installation and Management of Digital Library with LMS with RFID at GANDHI BHAWAN LIBRARY, Jabalpur	
CAPEX	☐ 0.00
OPEX	☐ 0.00
Total Project Price	☐ **0.00**

Form - 2: CAPEX

No.	Line Item	Quantity Proposed	Unit base price (In INR)	Total Price (Exclusive of Taxes)	All taxes, levies, duties etc. as applicable (In INR), excluding GST (Per Unit)	Total Price including All taxes, levies, duties, etc.as applicable (In INR) excluding GST
1	2	3	4	5 = 3 * 4	6	7 = (6 + 4) * 3
1	Digital Library Platform prepectuallicence with unlimited users	1		☐ 0.00		☐ 0.00
2	Smart Self Teaching (Multi-Media Content in Hindi and English from Class 1 to 12) prepectuallicence with unlimited users	1		☐ 0.00		☐ 0.00
3	Test Preparation Platform prepectuallicence with unlimited users	1		☐ 0.00		☐ 0.00
4	Smart Language Lab prepectuallicence with unlimited users	1		☐ 0.00		☐ 0.00
5	Library Management System (LMS)Software solution perpetual license	1		☐ 0.00		☐ 0.00
6	Digital Library Mobile Application (for end users and admin)	1		☐ 0.00		☐ 0.00
7	Mega Display 85 inch LED 4K HD resolution scree	3		☐ 0.00		☐ 0.00
8	e-Library system: 40 Nos (20 Boys+20 Girls rooms)	40		☐ 0.00		☐ 0.00

9	Language Lab : 20 Nos with headphones & Mic	20		☐ 0.00		☐ 0.00
10	Test Prep : 60 Nos	60		☐ 0.00		☐ 0.00
11	Tablets with cover & stand (10 inch minimum)	10		☐ 0.00		☐ 0.00
12	Wifi Access Points	10		☐ 0.00		☐ 0.00
13	LAN SETUP (lumpsum for the complete project setup)	1		☐ 0.00		☐ 0.00
14	Server (Application)	2		☐ 0.00		☐ 0.00
15	Storage	1		☐ 0.00		☐ 0.00
16	IT Rack	1		☐ 0.00		☐ 0.00
17	Core Switch	1		☐ 0.00		☐ 0.00
18	Core Router	1		☐ 0.00		☐ 0.00
19	Access Switch	3		☐ 0.00		☐ 0.00
20	Firewall	1		☐ 0.00		☐ 0.00
21	RFID Tags for Books	20000		☐ 0.00		☐ 0.00
22	RFID Staff Station	1		☐ 0.00		☐ 0.00
23	RFID Library Security Gate Single Aisle (2 EAS Pedestals)	2		☐ 0.00		☐ 0.00
24	RFID Wi-Fi Handheld Reader for Shelf Management	1		☐ 0.00		☐ 0.00
25	Smart card printing for members	5000		☐ 0.00		☐ 0.00
26	RFID smart card	500		☐ 0.00		☐ 0.00
27	Library Label /Anti-Theft Sticker	20000		☐ 0.00		☐ 0.00
28	Work Stations -for Library Assistant and librarian	2		☐ 0.00		☐ 0.00
29	Turnstile Gate (for entrances - 2 on each entrance of building)	4		☐ 0.00		☐ 0.00
30	UPS (2 hour back up - 2KVA online UPS)	2		☐ 0.00		☐ 0.00
31	Data Entry of books and library materials on LMS	1		☐ 0.00		☐ 0.00
32	Printer	1		☐ 0.00		☐ 0.00
Total Price						☐ 0.00

Form 3 - OPEX

No.	Line Item	Quantity	O&M	Total	All taxes,	Total O&M

		Proposed	Cost per Year	O&M cost (Exclusive of Taxes) for 5 years	levies, duties etc. as applicable (In INR), excluding GST (Per Unit)	cost including All taxes, levies, duties, etc.as applicable (In INR) for 5 years (excluding GST)
1	2	3	4	5 = (3 * 4)*5 Years	6	7 = ((6 + 4) * 3)* 5 years
1	Project Manager (cost for man year is to be quoted)	1		☐ 0.00		☐ 0.00
2	Library Assistants	1		☐ 0.00		☐ 0.00
3	Digital Library Platform prepectuallicence with unlimited users (Cloud operations cost - for 5000 concurrent users)	1		☐ 0.00		☐ 0.00
4	Smart Self Teaching (Multi-Media Content in Hindi and English from Class 1 to 12) prepectuallicence with unlimited users (Cloud operations cost - for 5000 concurrent users)	1		☐ 0.00		☐ 0.00
5	Test Preparation Platform prepectuallicence with unlimited users (Cloud operations cost - for 5000 concurrent users)	1		☐ 0.00		☐ 0.00
6	Smart Language Lab prepectuallicence with unlimited users (Cloud operations cost - for 5000 concurrent users)	1		☐ 0.00		☐ 0.00
7	Library Management System (LMS)Software solution perpetual license	1		☐ 0.00		☐ 0.00
8	Digital Library Mobile Application (for end users and admin)	1		☐ 0.00		☐ 0.00
9	Mega Display 85 inch LED 4K HD resolution scree	3		☐ 0.00		☐ 0.00
10	e-Library system: 40 Nos (20 Boys+20 Girls rooms)	40		☐ 0.00		☐ 0.00
11	Language Lab : 20 Nos with headphones & Mic	20		☐ 0.00		☐ 0.00
12	Test Prep : 60 Nos	60		☐ 0.00		☐ 0.00
13	Tablets with cover & stand (10	10		☐ 0.00		☐ 0.00

	inch minimum)					
14	Wifi Access Points	10		☐ 0.00		☐ 0.00
15	LAN SETUP (lumpsum for the complete project setup)	1		☐ 0.00		☐ 0.00
16	Server (Application)	2		☐ 0.00		☐ 0.00
17	Storage	1		☐ 0.00		☐ 0.00
18	IT Rack	1		☐ 0.00		☐ 0.00
19	Core Switch	1		☐ 0.00		☐ 0.00
20	Core Router	1		☐ 0.00		☐ 0.00
21	Access Switch	3		☐ 0.00		☐ 0.00
22	Firewall	1		☐ 0.00		☐ 0.00
23	RFID Tags for Books	20000		☐ 0.00		☐ 0.00
24	RFID Staff Station	1		☐ 0.00		☐ 0.00
25	RFID Library Security Gate Single Aisle (2 EAS Pedestals)	2		☐ 0.00		☐ 0.00
26	RFID Wi-Fi Handheld Reader for Shelf Management	1		☐ 0.00		☐ 0.00
27	Smart card printing for members	5000		☐ 0.00		☐ 0.00
28	RFID smart card	500		☐ 0.00		☐ 0.00
29	Library Label /Anti-Theft Sticker	20000		☐ 0.00		☐ 0.00
30	Work Stations -for Library Assistant and librarian	2		☐ 0.00		☐ 0.00
31	Turnstile Gate (for entrances - 2 on each entrance of building)	4		☐ 0.00		☐ 0.00
32	UPS (2 hour back up - 2KVA online UPS)	2		☐ 0.00		☐ 0.00
33	Data Entry of books and library materials on LMS	1		☐ 0.00		☐ 0.00
34	Printer	1		☐ 0.00		☐ 0.00
Total OPEX						☐ 0.00

Page Reference and Section	Existing Clause	Revised Clause
Pg 117 ; Storage	Minimum usable storage capacity of 5 TB	Minimum usable storage capacity of 2 TB
Pg 35 ;Team Composition and Qualification Requirements	Diploma in Library Sciences with minimum 2 years of overall Experience	Diploma with minimum 2 years of overall Experience
Page 120; Internet Router	1. Chassis should have a minimum 16 x 1 SFP or more ports populated with Multi-mode 1G SR transceivers from day 1. In addition, it must have an additional 4 x 10G SFP+ ports populated with Multimode 10G SR transceivers. 2. There should not be any Single point of failure in the Router. All the main components like Supervisor / CPU module, management module, power supplies and fans etc should be in redundant configuration. It should have distributed forwarding and there should not be any performance degradation in case of any switching/routing engine failure. 3. It must have minimum two or more vacant interface payload slots (after populating all the required above interfaces). 4. Must have minimum of 40 Gbps or more per interface slot throughput with all the above asked redundancy. 5.All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet Size and have distributed forwarding architecture. 6.Must have minimum 1M IPv4 Routes, 200K IPv6 Routes, 32K IPv6 Multicast routes, 1M MAC Address and 4K active VLAN's . 7.Chassis must support 40G and 100G interface line cards from day 1 8.Must have minimum IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP, BFD, MPLS and Netflow/Jflow/Sflow.	This clause has been deleted

Page 127 ; AAA	**Servers:**1.Should support approach that combines AAA, NAC, BYOD and Guest Access by incorporating identity, health, physical/device information, and conditional elements into one set of policies. 2. Must have ability to scale to up to 40000 users 3. Solution must be Agnostic to existing wired and wireless network in place today and all leading enterprise Wired and wireless products which may add in network in future. 4. Shell protected by CLI/GUI providing configuration for base appliance settings. 5. Platform must support for clustering with N+1 redundancy model.	This clause has been deleted

Page 127 ; AAA	**Functionality** 1. Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates. 2. Support any type of networking equipment (wired and wireless) and a variety of authentication methods (802.1X, MAC auth, Web auth). 3. Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures. 4. Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by reports. Must organize user, authentication, and device information. 5. AAA server should have device profiling functionality for 5000 concurrent devices to enforce context aware policies. 6. It must provide functionality/services based on endpoint device OS for controlling access. 7. AAA should have integration functionality with multiple authentication database like AD, LDAP and enhance BYOD security. 8. AAA server must support both functionality integrated and with external RADIUS server for client device authentication. 9. All external facing interfaces are programmable, which means APIs are available to extend the system to support different authentication protocols, identity stores, health evaluation engines. 10. The solution Must be an easy-to-deploy hardware/virtual platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform: a. Built-in guest management and device/user onboarding b) Web based management interface with Dashboard. c) Reporting and analysis d) Data repository for user, device, transaction information e) Rich policies using identity, device, health, or conditional elements f) Deployment and implementation tools. 11. Correlation of user, device, and authentication information for easier troubleshooting, tracking etc. 12. AAA framework must allow separation of Authentication and Authorization sources.	This clause has been deleted

	13. Authentication or authorization support for LDAP, AD. 14. Should support multiple methods for device identification and profiling such as: a. Integrated, network based, device profiler utilizing collection via AD. b) Policy creation tools: Preconfigured templates; Wizard based interface; 15. Support the following enforcement methods: a. VLAN steering via RADIUS IETF attributes / Change of Authorization and VSAs b. Access control lists – both statically defined filter-ID/downloaded ACLs c. Must be able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication. d. Must support PKI deployment where TLS authentication requires validating client certificate from CA. Must also support AAA server certificate being Signed by external CA validating PKI Signed client certificates. e. Platform must be deployable in an out of-band model and support for clustering with N+1 redundancy model. f. Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.	

Page 130 ; End point malware protection for servers , workstation and devices	• The solution should be advanced endpoint protection offering that has multi-method prevention including a proprietary combination of malware and exploit prevention methods that pre-emptively blocking both known and unknown threats. • The security solution should support prevention of cyber breaches by preemptively blocking known and unknown malware, exploits and zero-day threats • The security solution should support protection and enables users to conduct their daily activities and use web-based technologies without concern for known or unknown cyber threats. • Should support threat intelligence • The proposed solution must prevent exploitation of unpatched OS like Windows XP/Windows 7 vulnerabilities • Should support protection against legacy systems with a lightweight agent that does not rely on Signatures or scanning. • Should support various operating systems. • Should support static analysis via machine learning for an instantaneous verdict for any unknown executable file before it is allowed to run. It should examine hundreds of the file's characteristics in a fraction of a second, without reliance on Signatures, scanning or behavioral analysis. • Should support inspection and analysis to rapidly detect unknown malware and automatically reprogram to prevent known malware by transforming it into known in about 5-10 minutes. • Should support trusted publisher execution restrictions to identify executable files that are among the "unknown good" because they are published and digitally Signed by trusted publishers • Should support Exploit Kit Fingerprinting Protection to protect Windows endpoints from	This clause has been deleted

	fingerprinting, a common technique used by exploit kits. • Should support Child Process Protection for Windows endpoints for prevention against script-based attacks used to deliver malware such as ransomware. • Should block malicious macros/file from running when launched from a Microsoft office process on Windows endpoints for the file formats: Microsoft Office 2003 to Office 2007—doc, xls Microsoft Office 2010 and later releases—docm, docx, xlsm, xlsx • Should support protection of Mac endpoints from dylib hijacking attack. • Should support Policy-Based Execution Restrictions to restrict specific execution scenarios, thereby reducing the attack surface of any environment. • Should support admin override policies to define policies, based on the hash of an executable file, to control what is allowed to run in any environment and what is not. This fine-grained whitelisting (or blacklisting) capability controls the execution of any file, based on user-defined conditions that tie into any object that can be defined with Active Directory. • Should support Memory Corruption Prevention to prevent the exploitation techniques that manipulate the operating system's normal memory management mechanisms for the application that opens the weaponized data file containing the exploit • Should support Logic Flaw Prevention that recognizes and blocks the exploitation techniques that allow an exploit to manipulate the operating system's normal application process and execution mechanisms. • Should prevent execution of attacker's commands that are embedded in the exploit file to recognize the exploitation techniques that allow the attacker's malicious code to execute	

	and blocks them before they succeed. • The Management software should be provided with the solution to manage the advance endpoint solution.	
Page 131 ; Database Management System	Database platform would be very high transactional database platform, the database platform would be required for analytics and predictions. The database platform must be scalable, highly available, secure and robust. Also able to store and process various data types. 1. The database platform should provide dynamic scalability, so as additional resources (i.e. nodes) can be added horizontally in the database cluster without any downtime. 2. Database should provide row level security based on the user. 3. Database provide transparent to application data encryption capabilities at the tables, columns, storage levels and should able to encrypt backups and the information over the network. 4.For database tier should blocks unauthorized SQL traffic before it reaches the database transactions. Also Should the system should prevents from sql injections, sql bypass and provide a secured layer for multiple databases. Able to provide Policy based auditing, sql analysis accurately where to substitute, entry in log, generate an alert, allow or block 5. For data security, database should provide access (of transactions tables) through the application only. It should restrict system users, DBA or any privileged user accessing the operational/transactional information through SQL Language / tools like Toad etc., using direct connection. 6.For data archival and data management database should support partitioning at table level on various criteria like list, range, and composite and dynamic periodic partitioning.	This clause has been deleted

	7. Database should OGC compliant and should support spatial and GIS data storage, including 3-D and LiDAR data storage, spatial Web services , vector and raster data formats, topology data model, Triangulated Irregular Network (TIN) data types, network data models and Linear Referencing system 8. From a high availability and scalability perspective database should provide active-active clustering with load balancing of all the database transactions, which provides a Single image of database concurrently accessed by multiple database nodes/servers without repartitioning or 3rd party transaction routing mechanisms.	
Page 120 ; Next Generation Firewall	NGFW Specification • The manufacturer of the offered NGFW solution shall have a track record of continuous improvement in threat detection (IPS) and shall have successfully completed NSS Labs' NGFW Methodology v7.0 testing with a minimum exploit blocking rate of at least 95% or security effectiveness of 99%. Bidder shall submit authentic reference certificate/report to comply. • The offered NGFW Solution shall be an integrated Next Gen Firewall platform which includes at least firewall, application control, user identity acquisition, IPS, Anti-Virus, Anti-Bot, Antispyware, URL Filtering, IPsec , event correlation and reporting and security policy management capabilities. • The offered NGFW shall support authentication protocols like Active Directory, LDAP, RADIUS,TACACS, password/token-based. • The offered solution shall be in High Availability (Active-Hot Standby/Active-Active) set of two hardware and shall include all licenses required for Firewall, IPSEC VPN, SSL VPN, Application Visibility and Control, User-ID, Intrusion prevention, Anti Virus / Malware, Antispyware, Antibot, URL filtering,	This clause has been deleted

Page 121 ; Next Generation Firewall	**Firewall** • The offered solution shall have state-full inspection based on granular analysis of communication and application state to track and control network flow. • The offered solution shall allow at least policy rule creation for application control, user based control, threat prevention, Anti-virus / malware, file filtering/content-filtering, QoS/Scheduling. • The offered Solution shall have support identification and control of all types of applications (Business, Social, Encrypted and Custom) within the environment without requiring any license/subscription/blade. It shall provide detailed analysis on sessions consumed, data transferred and threats involved through the applications. • The offered solution shall have application identification capabilities for application visibility and shall operate at Layer 7 for Application filtering requirement. The required license/subscription shall be included from day one. Moreover NGFW should also perform State full inspection. • Active-Active deployment not only provide High Availability but should also increase the overall BW, concurrent connections and CPS. • The offered solution shall have deployment with interfaces servicing Layer 3, Layer 2, Transparent and Tap modes. • The NGFW shall have the functionality of Geo Protection to block the traffic country wise incoming as well as outgoing and shall detect and prevent embedded threats with in SSL traffic. • The solution should account for all seven layers of the OIA model dividing networking and security into discrete components . • Solution should comply with PCI DSS however not a relevant certification for federal government. • The solution should not allow for application and network traffic cache poisoning.	This clause has been deleted

	• URLF and application NGFW products should not allow HTML evasion techniques	
Page 121 ; Next Generation Firewall	• The IPS shall be based at least on the exploit Signature, Application control, Protocol anomalies and behaviour based detection and shall support different Custom IPS and Application policies / rule-sets for different users and groups. • The IPS shall support Vulnerability and Exploit Signatures, Protocol validation, Anomaly detection and constantly updated with new defences against emerging threats. • The IPS shall provide automated mechanism to activate and manage new Signature from updates. • The IPS should detect and block DNS tunnelling attempts The solution should allow for third party Signature import such as Snort. • The IPS should scan all parts of the session in both directions. • IPS must have a software based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory/ Latency. • IPS must provide an automated mechanism to activate or manage new Signatures from updates. • IPS must be able to collect packet capture for specific protections. • IPS and/or Application Control must include the ability to detect and block P2P & evasive application. • Solution must enforce Citrix Enforcement/protection	This clause has been deleted
Page 122 ; Next Generation Firewall	•The offered solution shall have the scalability to scan & secure SSL traffic , TLS traffic passing through firewall and shall perform inspection to detect & block malicious content download and upload through SSL. •The offered solution shall be able to get auto update with Malware and Phishing URL categories based on the latest malicious and phishing Site. •The offered solution shall support DNS-based	This clause has been deleted

	Signatures to detect specific DNS lookups for hostnames that have been associated with malware. •The offered solution shall have ability to block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time). •The offered Solution shall be able to detect & Prevent the Bot infected machine and unique communication patterns used by BOTs i.e. Information about Botnet family. •The offered solution shall proactively protect against threats contained in emailed and web. •The URLF solution should enforce 'safe search'. •The URLF solution should filter and allow for HTTPS without SSL Inspection. •Ability to Enforce bandwidth and/or time limits to select website or Web 2.0 applications. •Application control database must contain more than 3000 unique applications. •The solution must have an easy to use, searchable interface for applications and URLs	
Page 122 ; Next Generation Firewall	Hardware and Interfaces •Offered Solution must support more than 10Gbps of NGFW throughput, including firewall, Application control and IPS scanning full session in both direction. •Offered NGFW solution must support at least 60K new connection per second and 5 Million of concurrent Connections. •Offered NGFW Must support up to 4x 40G ports and should be supplied with 10 10/100/1000Base-T Ports on day-1. •The offered NGFW shall have local in-built storage of 200 Gb or more to ensure system works without any trouble	This clause has been deleted
Page 122 ; Next Generation	NGFW Management •The management system shall provide central logging, Analysis, customizable Granular	This clause has been deleted

Firewall	Application Centric Reporting and provide overall status of the network traffic and attack going through the firewall, including potential problems that may need attention. •It shall have central management reporting, logging and analyser / correlation solution. •The Centralized management solution shall be able to manage all functions specified in NGFW specification from central console. •The system shall provide analysis of traffic pattern using graphs and charts. •The Central Management system should be software based and should be able to build management server on Open Servers and VM infrastructure. Central NGFW Management should be able to manage at least 5 gateway on day1, It should be able to accommodate more firewalls to be managed in future with just license upgrade. •The solution shall be able to provide different level of users account and access management, with support for external authentication server, specifically RSA Secure ID and/or Active directory. •The solution shall be able to audit any changes made to rules or configuration with full details, support systems configuration rollback to previously saved configurations on box and policy validation. •NGFW shall have ability to lock objects and rules while modifying it, avoiding administrator collision when there are multiple people doing changes in configuration at same point of time. •The Security management system shall provide Compliance monitoring framework so that it can monitor compliance status of these devices in the real time. •Solution must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant segment. •Solution must be able to segment the rule base in favour of delegation of duties in which changes	

	in one segment will not affect other segments. •Solution must have the granularity of administrators that works on parallel on same policy without interfering each other. •Solution must be able to install threat related protections and access related rules separately in order to allow managing it by separate teams. •Solution must provide the option to save the entire policy or specific part of the policy. •Solution must combine policy configuration and log analysis in a Single pane, in order to avoid mistakes and achieve confidence of the change.	
Page 123 ; Next Generation Firewall	Anti – APT Specifications •Anti-APT & Sandboxing solution must have advance technology to prevent malware at exploit stage to prevent attack technique itself such as ASLR, ROP, DEP etc. •Anti-APT solution must Sandbox files on premise itself, no document shall be sent to public cloud. However proposed Solution must also support Cloud Sandboxing with same setup without any additional hardware/software component. All licenses for ON premise sandboxing and Cloud sandboxing must be included. •Sandbox / Anti-APT solution must support 2 Gbps of throughput. •Each appliance in Sandbox on-prem must be supplied with at least 2x10 G ports. •Proposed Anti-APT solution must support of having at least 28 Virtual Machine. •The solution should support deployment in inline block mode. •The solution should support deployment in MTA (Mail Transfer Agent) mode, inspect TLS & SSL. •The solution should support deployment in TAP/SPAN port mode The solution must provide the ability to Protect against zero-day & unknown malware attacks before static Signature protections have been created: • Anti-APT solution must be able to prevent unknown malware patient-0 in web browsing in	This clause has been deleted

	real time. •Anti-APT solution must be able to prevent unknown malware patient-0 in email in real time. •The Sandbox engine should support multiple OS's such as XP and Windows7, 8,10 32/64bit. •The solution must support prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft. •The engine should detect API calls, file system changes, system registry, network connections, system processes. •Sandbox solution must support emulation of file sizes larger than 10 - 50 Mb in all types it supports. •The solution shall support sandbox behaviour based inspection and protection of unknown viruses and zero-day malware, Sandbox solution must be able to block new discovered zero day malware by itself without being dependent on connectivity to cloud and without being dependent on Signature creation at cloud and Signature pushed back to appliance to be able to block it.	
Page 123 ; Next Generation Firewall	Anti APT Management Specifications : •Centralised / Management Solution Anti-APT management should be able to manage all functions and appliance of Anti-APT from centralise console. • Centralised / Management Solution Anti-APT management must support additional Anti-APT appliances from same management with just license upgrade. •Centralised / Management Solution Anti-APT solution must generate detailed report on suspected file. The detailed report must include :screen shots, time lines, registry key creation/modifications, file and processes creation, Network activity detected. •Centralised / Management Solution Anti-APT solution must log all files inspected in Sandbox. •Central Management / Management Solution	This clause has been deleted

	should help in identifying which APT device is running at lower version and needs to be updated. •Solution must allow the creation of filters based on any characteristic of the event such as security application, source and destination IP, service, event type, event severity attack name, country of origin and destination, etc. •The event correlation application must supply a graphical view events based on time. •Solution must include the option to search inside the list of events, drill down into details for research and forensics. •Solution must include predefined hourly, daily, weekly and monthly reports. Including at least Top events, Top sources, Top destinations, Top services, Top sources and their top events, Top destinations and their top events and Top services and their top events. •Solution must support automatic report distribution by email, upload to FTP/Web server and an external custom report distribution script. •The solution should provide an integrated dashboard and analysis system that could provide a Single view into all the analysis performed across all the different data sources.	
Page 124 ; Web Application Firewall	Architecture : •The proposed device should be a dedicated purpose built hardware Web Application Firewall appliance. It should not be a part of UTM, ADC device, Firewall module or Router functionality. •The appliance should have minimum 4 x10G SFP+ data interfaces from day one. • The appliance should support Minimum 64GB RAM and 1*SSL AIACS/FGPA/cards with network virtual function support. •Support for various deployment scenarios including bridge mode, transparent proxy mode, router mode, reverse proxy and passive/promiscuous mode. **Deployment and availability**	**This is changed to Firewall.** **Physical Attributes**: Modular design and Internal redundant power supply. **Interfaces: a)** Minimum 2 * 10 Gig Port with necessary modules. b) 4 x GE, upgradable to 8 GE c) Console Port 1 number **Performance and Availability:**a) Encrypted throughput: minimum 1 Gbps. b) Concurrent connections: up to

	•Should support all deployment Mode like Inline Transparent Proxy, inline Reverse Proxy, Inline Flow-based Protection ,One-arm Reverse Proxy & One-arm Mirror Protection (Detection & Block). •Should support High availability mode like Active-Active & Active-Passive. •Should support Fail Open Bypass Card. Should support Distributed Deployment with Centralized Management. •Emergency Mode, when the connections exceed pre-set threshold, the traffic will be forwarded directly in layer 3. **Features** •The device should have abuse detection, tracking, Profiling and should support Abuse response and real time incident management. •Devices should be able inspect HTTP and HTTPS traffic on TCP port 80 & 443. •should support Software FeatureData Leak Prevention like Web site Cloaking, Outbound Data Theft Protection. •Software Protocol Validation like HTTP/HTTPS Protocol Validation, Form Field Metadata Validation, XML Protocol conformance, XML/SOAP profile enforcement. •Should support Prevention from Malicious Robots, Leech, Malicious Scan, URL access control, Parameter Tampering, Brute Force login, Remote File Inclusion Attacks, Stateful firewall, Correlation rules to detect complex, multi-stage attacks. •Should be able to detect attempts to abuse form inputs and establish vectors for injection and cross-site scripting attacks. •Should mitigate OWASP Top 10 attacks like SQL Injection, Cross site Scripting, XSS Session Hijacking, Directory Traversal, Malicious Encoding and Illegal Encoding, CSRF, Form Field Tampering, Buffer Overflow, Cookie Protection. •Must protect web application against buffer overflow and layer7 DDOS attacks.	250,000. c) Simultaneous VPN tunnels: 2000. **Routing Protocols :** Static Routes ;RIPv1, RIPv2; OSPF. **Protocols** : TCP/IP; RTP; IPSec, DES/3DES/AES ; FTP, HTTP,HTTPS,SNMP, SMTP; DHCP, DNS ,Support for IPv4 and IPv6 ; IPSEC. **Other Support** : 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS, Support multilayer firewall protection, Traffic shaping, Bandwidth monitoring **QoS** QoS features like traffic prioritisation, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies. **Management** : Console, SSHv2, Browser based configuration ; SNMPv1, SNMPv2, SNMPv3

	•Emergency Mode, when the connections exceed pre-set threshold, the traffic will be forwarded directly in layer. •Should Support Web Application Vulnerability Scanner Integration. • Must protect web application against parameter tampering and must have inbuilt controls to block invalid files, filtering of sensitive words in HTTP request and response.•Should be able to detect suspicious application errors that indicate abuse including illegal and unexpected response codes. • Should be PCI Compliance ready. •Should have support for Threat Intelligence, Integrate intelligence from the vendors. •Should be able to detect when an attacker is attempting to request files with suspicious extensions, prefixes, and tokens. •Should support creation of the policies for HTTP/HTTPS headers to ensure critical infrastructure information is not exposed. Response and request headers can be stripped, mixed, or filtered. • Should support anti-defacement for Windows and Linux driver-level Web Keeper and distributor clients. •Should have Built-in Web Vulnerability Scanner. •Should be able to detect and prevent attackers from finding hidden directories. inbuilt security control to limit the action of crawling and scanning. •Should be able to detect attempts to abuse non-standard HTTP/HTTPS methods such as TRACE. • Should be able to detect attempts to manipulate application behaviour through query parameter abuse. Solution must support behaviour analysis to detect and prevent day 0 attacks. •Should maintain a profile of known application abusers and all of their malicious activity against the application.	

	•Should enable application administrators to re-identify abusive users and apply persistent responses across sessions. •Should be able to process SSL traffic using passive decryption or using equivalent technology. •Customized response. •Should enable administrators to respond to application abuse with session specific warnings, blocks abusive application and undertake additional checks for the same. •Block connection and return arbitrary error/custom message. •Should support network based security controls including ACL's, IP blacklist/whitelist and URL blacklist/Whitelist. •Anti-DDOS protection with syn flood, UDP flood, ICMP flooding, command and control protection. •Reporting, Logging & Monitoring. •Sends alert emails when specific incidents or incident patterns Occur. •Enable command line interface for custom reporting. Should capture, log and display traffic related data to analyse for security incidents. •Should enable SNMP system logging and able to send alerts to a centralized EMS solution. •Should support auditing - Tracks changes to the system made by the administrators in the configuration interface, security monitor and report generation. •Should be able to send security incidents via syslog. **Remote access** •Proposed device support remote access which should be 100% client less for web based applications.•must support for CIFS file share and provision to browse, create and delete the directories through web browser. •should maintain original server access control policies while accessing the file resources.	

	•must support Single Sign-On (SSO) for web based applications and web based file server access. • Should have secure access solutions for mobile PDAs, Andriod smart phones, Ipad, Iphones. •Should Support IPV6. •Proposed device must provide machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources. •Should support following Authentication methods: - LDAP, Active directory, Radius, secureID, local database, and certificate based authentication and anonymous access. **Management** •The appliance should have SSH CLI, Direct Console, SNMP, and Single Console per Cluster with inbuilt reporting. •The appliance should provide detailed logs and graphs for real time and time based statistics •Should capture, log and display traffic related data to analyse for security incidents. •Should support XML-RPC for integration with 3rd party management and monitoring of the devices. •The appliance should have extensive report and logging with inbuilt tcpdump like tool and log collecting functionality •Should be able to send security incidents via syslog	
Page 118 ,Core Switch	•Must be a chassis based switch and have minimum 32 x 40G QSFP+ or more ports distributed across minimum two or more interface line-cards fully populated with Mode Fiber Transceiver. In addition, it must have 48x 10G Base T ports and 48x 1/10G SFP+ ports fully populated with multi-mode fiber transceiver. •There should not be any Single point of failure in the switch. All the main components like CPU module, switching fabric, power supplies and fans	**Ports** • 24 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) • Can have FCoE ports if FCoE solution is offered • Extra 2 or higher Uplink ports (40GE) • All ports can auto-negotiate

	etc. should be in redundant configuration. •It must have minimum five or more vacant interface payload slots (after populating all the required above interfaces). •Chassis must support 40G / 100G interface line cards (as required). •Must have minimum of 2.56 Tbps full duplex or more per interface slot throughput. •All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture. •Must have minimum 128K IPv4 Routes, 32K IPv6 Routes, 12K ACL's, 70K MAC Address, 4K active VLAN's and 4 hardware queues per port. •Must support minimum of 32 no of ports per LAG / vLAG / Ether channel. •Must have minimum IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP and Netflow/ Jflow/ Sflow. •Must support the separation of data and control plane, to be controlled by SDN Controller, utilizing openflow or equivalent protocol.	between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports. **Switch type** Layer 2 **MAC** Support 32K MAC address. **Backplane** :Capable of providing wire-speed switching for fully populated switch. **Throughput** :Required throughput to achieve non-blocking performance for switch when all ports are populated. **Port features :** Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks **Flow Control** :Support IEEE 802.3x flow control for full-duplex mode ports. **Protocols :** • IPV4, IPV6 • Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1X Security standards • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • DHCP support

		• Support up to 1024 VLANs • Support IGMP Snooping and IGMP Querying • Support Multicasting • Should support Loop protection and Loop detection, **Access Control** • Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication **VLAN** • Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent **Protocol and traffic** • Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number **Management** • Switch needs to have a console port for management via a console terminal or PC

		• Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface **Resiliency** • Dual load-sharing power supplies • Redundant fans Switch should support FCoE& IPv6 from day one
Page 119, Core Router	•Chassis must have a minimum 8 x 1 SFP or more ports populated with Multi-mode 1G SR transceivers from day 1. In addition, it must have an additional 4 x 10G SFP+ ports populated with Multimode 10G SR transceivers. •There should not be any Single point of failure in the Router. All the main components like Supervisor / CPU module, management module, power supplies and fans etc should be in redundant configuration. It should have distributed forwarding and there should not be any performance degradation in case of any switching/routing engine failure. •It must have minimum two or more vacant interface payload slots (after populating all the required above interfaces). •Should have minimum of 40 Gbps or more per interface slot throughput with all the above asked redundancy.	**Multi Services** Should deliver multiple IP services over a flexible combination of interfaces. **Port** As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements. **Speed** :As per requirement, to cater to entire bandwidth requirement of the project.

	•All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture. •Must have minimum 160k IPv4 Routes, 8K IPv6 Routes, 5K IPv6 Multicast routes, 200k MAC Address and 4K active VLAN's. •Chassis must support 40G and 100G interface line cards •Must have minimum IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP, BFD, MPLS and Netflow/Jflow/Sflow.	**Interface Modules :** Must support minimum 2* 10G Port with necessary SFP+ Modules. Must have capability to interface with variety interfaces. **Protocol support** Must have support for TCP/IP, PPP Must support IPSEC VPN Must have support for integration of data and voice services Routing protocols of RIP, OSPF, and BGP. Support IPV4 & IPV6 **Manageability** Must be SNMP manageable **Scalable** • The router should be scalable. For each slot multiple modules should be available. • The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future. **Traffic Control** Traffic Control and Filtering features for flexible user control policies. **Bandwidth :** Bandwidth on demand

		for cost effective connection performance enhancement. **Remote Access :** Remote access features **Redundancy :** Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis • All interface modules, power supplies should be hot-swappable **Security** • MD5 encryption for routing protocol • NAT • URL based Filtering • RADIUS Authentication • Management Access policy • IPSec / Encryption L2TP **Qos Features** • RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate
Corrigendum ,Access	•Must be a chassis based switch and have minimum 32 x 40G QSFP+ interface line-cards	**Ports** • 48 (as per density required)

Switch	fully populated with Mode Fiber Transceiver. In addition, it must have 48x 10G Base T ports and 48x 1/10G SFP+ ports fully populated with multi-mode fiber transceiver. •There should not be any Single point of failure in the switch. All the main components like CPU module, switching fabric, power supplies and fans etc. should be in redundant configuration. •It must have minimum five or more vacant interface payload slots (after populating all the required above interfaces) •Chassis must support 40G / 100G interface line cards (as required) •Must have minimum of 2.56 Tbps full duplex or more per interface slot throughput. •All the interfaces / line-cards should be non-blocking and wire-speed for 64 bytes of packet size and have distributed forwarding architecture. •Must support minimum of 32 no of ports per LAG / vLAG / Ether channel. •Must have minimum IPv6 Static routes, OSPFv3, PIM Sparse / Dense mode (SM /DM), Policy-based routing (PBR), Virtual routing and forwarding (VRF), BGP and Netflow/ Jflow/ Sflow. •Must support the separation of data and control plane, to be controlled by SDN Controller, utilizing openflow or equivalent protocol. • Must have minimum 128K IPv4 Routes, 32K IPv6 Routes, 12K ACL's, 70K MAC Address, 4K active VLAN's and 4 hardware queues per port.	1G/ 10G Ethernet ports (as per internal connection requirements) • Can have FCoE ports if FCoE solution is offered • Extra 2 or higher Uplink ports (40GE) • All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports. **Switch type** Layer 3 **MAC** Support 32K MAC address. **Backplane** :Capable of providing wire-speed switching for fully populated switch. **Throughput** :Required throughput to achieve non-blocking performance for switch when all ports are populated. **Port features :** Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks **Flow Control** :Support IEEE 802.3x flow control for full-duplex mode ports. **Protocols :** • IPV4, IPV6 • Support 802.1D, 802.1S, 802.1w, Rate limiting

		• Support 802.1X Security standards • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • DHCP support • Support up to 1024 VLANs • Support IGMP Snooping and IGMP Querying • Support Multicasting • Should support Loop protection and Loop detection, **Access Control** • Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication **VLAN** • Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent **Protocol and traffic** • Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable

		application types: TOS, DSCP, Port based, TCP/UDP port number **Management** • Switch needs to have a console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface **Resiliency** • Dual load-sharing power supplies • Redundant fans Switch should support FCoE& IPv6 from day one

EXECUTIVE DIRECTOR

JABALPUR SMART CITY LIMITED