KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED

TERMS OF REFERENCE

Upgrade of Core Network Infrastructure

I. Introduction

KRA business operations are fully reliant on ICT systems and hence the need to ensure maximum uptime and availability of its IT Infrastructure and business systems throughout the year. The Authority embraces IT as a core competency by having the most up-to date IT infrastructure to support its business operations and align with changing technology landscape.

The core communication infrastructure currently operates on a Reference Architecture that has limitations in scalability/agility, visibility, reliability, management and performance. The network installed in 2017 has a challenge in adaptability to accommodate new technologies such as automation provisioning & orchestration AI and ML.

To address these limitations and accommodate growing network demands, a shift to a software-defined network is proposed. Additionally, there is a need to upgrade the load balancers to meet the traffic/throughput growth. The new technology will enhances performance, scalability, and redundancy, particularly in data center networks, making it well suited for modern communication infrastructures

II. Objective(s)

The primary objective of this initiative is to enhance KRA Data Center Network infrastructure to be more efficient, fast, reliable, secure, and scalable to meet the growing demands of modern applications and services.

This will entail, and not limited the following;

a) Migration the core data center network infrastructure from the existing aged reference architecture, to the modern Software Defined Network based on Leaf and Spine architecture associated with consistent with low latency, improved scalability and predictable performance.
b) Upgrading the data center core network throughput/bandwidth/speeds from the current 1/10G to 25/40/100G throughput to accommodate intensive data processing in Data Analytics, AI and ML.
c) Upgrade of the Application Delivery Controllers (Load Balancers, WAF and BIG-IP DNS) infrastructure.
d) Implementing a stretched network architecture across multiple data centers including the DR Site, to optimize failover mechanism, and hence improve Business Continuity Arrangement and readiness.
e) Implementing centralized and simplified network management, hence providing consistent policy enforcement across the entire network.
f) Robust methodology to ensure minimal disruption of services during the transition process. The new architecture is

expected to be compatible with existing network components and systems.

III. Scope of Works

Successful bidder will be required to undertake the following at minimum to ensure that the implementation of the modern data center infrastructure is completed in line with industry best practices, compliant with organizational and regulatory requirements

a) Assessment and Design:

- The bidder to undertake a detailed assessment of the existing data center infrastructure, with a view of identifying existing gaps and challenges.
- Designing the target futuristic robust architecture software defined network infrastructure to serve KRA up to 5 years.
- Determining the hardware and software requirements, confirm the exact bill of materials and quantities required to implement the new design

b) Implementation

- The bidder to supply, deliver, install and commission all the required hardware and software components for the SDN solution and Load Balancers. This should also include the provision of the solution design and architecture. These will include but not limited to the following;

1	Data Centre Application Load Balancer	12
2	Data Centre Spine Switches	6
3	Data Centre Leaf Switches	16
4	Centralized policy and management controller	6
5	IPN Equipment	6
6	Data Center WAN/Internet Router	8
7	Dark Fiber DWDM infrastructure	6
8	Campus Fiber Aggregation Switches	6

- In liaison with the KRA technical team, successful bidder to undertake an Original Equipment Manufacturer (OEM) led deployment of the new solution end to end.
- Perform quality assurance and validation by the OEM of the solution is mandatory requirement.
- Proper training of the Technical Staff on the new solution to ensure smooth transition and migration.
- Handholding and handover of the solution to KRA Infrastructure Team.
- The successful bidder is required to provide a mandatory four (4) year post warranty support and maintenance of all the solution hardware and software components.

c) Migration Strategy:

- Development of a phased migration plan to ensure continuity of service.
- Transitioning core routers, switches, and other networking devices from the reference model to SDN based on Leaf and Spine configuration.
- Updating or replacing software, protocols, and security measures as necessary.
- Testing and Validation:

- Post-migration testing to validate network performance, latency, redundancy, and failover capabilities.
- Ensure proper integration with existing applications and services.

d) Training and Documentation:

- Provide OEM led offsite training to at least fifteen (15) Data Center Network staff on the Leaf and Spine architecture and load balancers, with certifications.
- Document the new architecture and migration procedures.

IV. *Methodology*

The bidder to provide a methodology for a seamless delivery of the solution that will entail and not limited to the following phases;

a) Planning and Assessment**:**
   - Evaluate the current network to determine compatibility and gaps in its capabilities.
   - Define key performance indicators (KPIs) for the new architecture.

b) Design Phase**:**
   - Develop a high-level design of the Leaf and Spine topology.
   - Choose appropriate hardware, considering capacity, redundancy, and scalability.

c) Implementation:
   - Deploy new hardware and software components in phases to ensure smooth transition.
   - Reconfigure existing devices to fit into the new architecture.

d) Testing and Verification:

- Conduct stress testing, failover testing, and latency measurements.
- Verify the network meets the predefined KPIs.

e) Training and Handover**:**

- Conduct staff training sessions.
- Provide comprehensive documentation on the new architecture.

V. *Deliverables/Milestones/Outcomes*

The project will produce the following deliverables:

a) Project Plan: Detailing timelines, phases, and milestones.
b) Design & Architecture Documentation: Including diagrams of proposed Software Define Data Center network infrastructure based on Leaf and Spine architecture.
c) Migration Roadmap: A detailed guide for the phased implementation.
d) Post-Migration Testing Report: Including test results and any issues encountered.
e) Operational Documentation: Including network configurations, troubleshooting guidelines, and operational procedures.
f) Training Materials: Guides and materials for network staff training.

VI. *Organization and Staffing*

Bidders are expected to provide a brief description of their company, including experience in delivering similar projects by highlight Company's track record in the implementation of leave and spine architecture

a) Project Manager(1):

Bidders are expected to provide an individual responsible for leading the implementation of the proposed solution, ensuring that the project stays on schedule, meets all specifications, and adheres to quality standards.

Roles

i. Planning and Scheduling: Develops comprehensive project plans outlining tasks, timelines, and milestones to ensure structured progress.
ii. Budget Management: Oversees financial resources, ensuring that the project remains within the allocated budget.
iii. Team Coordination: Leads the project team, assigns tasks, and ensures effective communication among members.
iv. Risk Management: Identifies potential risks and implements strategies to mitigate them, safeguarding the project's success.

Key competence

i. Degree in Electrical/Electronic Engineering, Computer Science or Information Technology related field
ii. Professional certification in project management e.g. Prince2 , PMP or any other relevant internationally recognizable certification

b) Key Technical Personnel/Staff/Project Implementation Team

Include short biodata (CVs) of the key team members who will be involved in the project. Mention their qualifications, years of experience, and specific roles in previous similar projects.

a. Network Architects(1):

Role

i. Design the new Leaf and Spine architecture.
ii. Perform initial assessments and identify hardware requirements.

Key competence

i. Degree in engineering or Information technology related field
ii. Professional certification in network design

b. Network Engineers(3):

Role

i. Handle the installation and configuration of new equipment.
ii. Assist with testing and troubleshooting during the migration process.

Key Competence

i. Degree in engineering, Computer Science or Information technology related field
ii. Professional Certification in Network e.g. CCNA, CCNP, HCDA etc.
iii. At least one (1) Network engineer MUST have expert certification in the deployment and administration of F5 load balancers.

TABLE 1: VENDOR EVALUATION CRITERIA

Instructions to Bidders:

- Bidders MUST complete the Table below in the format provided.
- Bids MUST meet all mandatory (MUST) requirements in the Tables below in order to be considered for further evaluation.
- Bidders MUST provide a substantial response or clear commitment to meeting the requirements for all features irrespective of any attached technical documents in the table format (bidders Response) below. Use of Yes, No, tick, compliant, blank spaces etc. will be considered non-responsive.
- Bidders who do not comply with any of the below requirements will NOT be considered for further evaluation

NB: Bidders who shall meet the cut-off score for the technical and demonstration requirements shall be evaluated at the financial evaluation stage.

	Requirement	Evaluation Criteria	Max Score	Bidder Response (Narrative answers)
1	**Company Experience.** The bidder should have demonstrated expertise in implementing Software Defined Data Center Network by having previously implemented at least three (3) project of similar scope and complexity. The project should involve implementing Leaf & Spine based SDN infrastructure in an organization of similar size or bigger to KRA , and must have been done within the last five (5) years.	Bidders MUST submit recommendation letter for the project cited with copy of signed Contract or LSO to support. In addition, the recommendation letter should have: i. Contacts: postal address, telephone and email of the contact person. ii. A brief description of the project delivered. 10 Marks	10	
2	**Resource/Personnel Qualifications.** One(1) dedicated project manager with the following qualifications;	3 Marks for Qualified Staff (1 mark for degree, 2 marks for product professional certification)	9	

	Academic Qualifications: 1) University Degree in (Computer Science, IT, electronics or related fields) **Professional Qualifications** 2) Professional Certification in Prince2, PMP, or any other recognized project manager certifications. **Relevant experience.** 3) The project manager should preferably have over three (3) years of experience in the managing and coordination of implementation of IT projects	Bidders MUST attach a copy of the CV supported by copies of degree certificates and copies of the product specific professional certification for each technical staff.		
	Minimum three (3) Technical staff with the following academic and professional qualifications: **Academic Qualifications** 1) All the three (3) MUST have relevant University Degree in (Computer Science, IT, electronics or related fields) **Professional Qualifications** 2) **Two (2)** technical staff with Valid OEM Technical certification in the specific SDN solution proposed under this procurement.	3 Marks for each Qualified Staff (1 mark for degree/ diploma, 2 marks for product professional certification) Bidders MUST attach a copy of the CV supported by copies of degree/diploma certificates and copies of the product specific professional certification for each technical staff. Qualified Staff Relevant experience • Over 3 years– 5 Marks for each qualified staff	12	

	3) **One (1)** technical staff with Valid OEM Technical certification in the specific Load Balancer (F5) solution proposed under this procurement. **Staff Relevant experience.** 4) Each Qualified staff above should preferably have over three (3) years of experience in the implementation, support and maintenance in the relevant field i.e. Leaf & Spine based SDN solution & Load Balancers respectively.	• 2-3 years – 3 Marks for each qualified staff • 1-2 years – 1 Mark for each qualified staff Note: Bidders MUST submit a copy of the CV for each staff clearly indicating the years of experience in implementing and supporting SDN leaf & spine based solution and Load balancers respectively, and the applicable sites.		
4	**Technical Approach/ Methodology.** Bidder should demonstrate a good and clear understanding of KRA's Requirements in this tender. Bidder should propose an approach/ methodology and a work plan to capture the requirements and ensure they are comprehensively addressed in their proposed solution.	Bidders to demonstrate/provide evidence of a clear and detailed understanding of the solution, including: a) Technical Approach /Methodology of carrying out the assignment – 3 Marks b) Work plan (Bidder MUST provide work plan for the implementation and support of the solution – 3 Marks	6	
5	**Detailed Design & Architecture of the SDN Data Center solution**	Bidders should submit the proposed design and architecture for the SDN Data Center solution quoted covering the three [3]	10	

		data centres and including high-availability (HA) implementation.		
Total score for this section is 50/50 (100%) and cut-off score is 37.5/50 (75%) marks.			50	

TABLE 2: MANDATORY TECHNICAL REQUIREMENTS.

Note: Bidders MUST COMPLY WITH ALL THE MANDATORY requirements in order to be considered for further evaluation.

S/No	Requirement	Mandatory Specifications	Bidders' response (Please provide a Relevant narrative response)	Evaluation Remark (PASS or FAIL)
1	Product	The Proposed Software Defined Data Center Network (Leaf and Spine Solution) MUST be a reputable and widely deployed international brand. ALL products, Licenses and services MUST be sourced through the authorized OEM channels. Bidders MUST ensure that ALL components of the proposed solution **ARE NOT** scheduled to reach		

		their end of life/support within 5 years from the date of bid submission In this regard, Bidders MUST submit a Product introduction brief that includes the following details: Specific Brand, product, series, model etc. and relevant supporting brochures.		
2	Key solution Components	The proposed solution MUST be inclusive of the following components: a) Centralized management and automation controller. b) Infrastructure Layer-Leaf and Spine switches. c) Data Center extension network layer between the Primary , secondary and DR sites d) Application Layer- Applications and services that utilize the network, sending requests to the controller for network functions.		
3	Hardware and Software Requirements	The proposed solution MUST be based on dedicated OEM Hardware and software appliances deployed in High Availability (HA) across Data Center(s) (Primary, Secondary and DR).		

		The hardware appliance must be rack-mountable in standard 42U Rack.		
4	Training and capacity building	Successful bidder MUST provide Manufacturer Authorized administrator training (classroom) for twenty (15) KRA staff for all the solution components, leading to professional certification in the solution. Training proposals MUST include Course outline to be covered and duration.		
5	Vendor Support	Successful bidder MUST provide Unlimited Vendor onsite and online Implementation, Maintenance and Support Services covering the entire solution throughout the contract period on a 24*7*365 Basis. The vendor's staff providing support MUST have attained relevant OEM certifications. Bidder MUST demonstrate competence in delivering the solution by having acquired a high product partnership level with the OEM. The		

		successful bidder MUST also be backed by professional technical support from the OEM throughout the contract period. In this regard, Bidders MUST provide a letter from the OEM certifying the partnership Levels and commitment from the OEM referencing this tender and indicating OEM's willingness to provide oversight and support through the contract period.		
7	OEM Support & Local Presence	KRA runs mission critical services on a 24*7*365 basis. In order to guarantee availability of OEM online and onsite support on a 24*7*365 basis, OEMs for quoted products are required to have Local presence in Kenya and MUST have qualified technical staff with relevant professional training, experience and certifications in the implementation and support of the solution. Bidders MUST provide details of the Local office including location and staffing. Successful bidder MUST ensure that ALL products		

		(Hardware, Equipment, interfaces, accessories, Software and Services) MUST be covered under OEM technical support services throughout the contract period, including direct access to Manufacturer's technical assistance team, online troubleshooting / support tools.		

No	Evaluation Type	Max Score	Cut-Off Score
1.	Vendor Evaluation	20	16
2.	Technical Evaluation	70	60
3.	Post Qualification	10	8
	Total	**100**	**84**

EVALAUTION SCORING

VII. *CLAUSE BY CLAUSE-TECHNICAL SPECIFICATIONS FOR THE SUPPLY, DELIVERY, INSTALLATION AND COMMISIONING OF SOLUTIONS/COMPENENTS FOR THE UPGRADE OF CORE NETWORK INFRASTRUCTURE*

1. **APPLICATION DELIVERY CONTROLLER (LOAD BALANCER)**

(a) DMZ LOAD BALANCERS QTY: 4

S.N	Feature	Minimum Requirements	Bidders' Response	Score
1	Model and Technology	The load balancer must be a mature internationally recognized brand (bidder must specify brand and model) which has been in existence for more than 10 years and the specified model is not reaching end of support/life in the next 5 years.		***5***
		Proposed solution shall be in Leaders Quadrant for a minimum of 5 continuous years Gartner Magic Quadrant for Application delivery controller		***8***
2	General description features	The device should provide load-balancing and content switching functions with granular traffic control based on customizable Layer 4 through 7 rules with support for both IPv4 and IPv6 addresses, virtual IP addresses (VIPs) and server farms.		2
		The device should natively load-balance the following protocols in an IPv4 environment: HTTP/HTTPS, FTP, DNS, ICMP, SIP, RTSP, Extended RTSP, LDAP, RADIUS, SCCP and Microsoft RDP. In an IPv6 environment, it should natively load-balance HTTP, HTTPS and SSL protocols. The device should have generic protocol parsing capabilities that enable the configuration of application switching and persistence policies based on any information in the traffic		2

		payload for custom and packaged applications without requiring any programming.		
		The device should support translation and load balancing between IPv4 and IPv6 networks and provides flexibility to customers in planning their IPv6 migration.		2
		The device should have an Advanced WAF can identify and block attacks from application-layer encryption to protect against credential and data theft to L7 DDoS detection that uses machine learning and behavioral analytics. This Advanced WAF should provide the capability to provide Advanced Application Protection, Behavioral Analytics, Proactive Bot Defense, API Protocol Security, Anti-Bot Mobile SDK as well as the ability to provide Credential Protection.		2
3	Operational features	Throughput: Device throughput of at least 95 Gbps /95 Gbps L4/L7 Intelligent Traffic Processing L7 request per second :4.3M		3
		Maximum L4 concurrent connection 100M		2
		L4 HTTP requests per second :18M		2
		Hardware Compression with support for up to 50Gbps		3
		SSL throughput: at least 50 Gbps		2

		SSL TPS: at least 100,000 SSL TPS using 2K keys		2
		Maximum L4 connections per second: 100,000 complete transactions sustained rate		3
		Maximum L7 Requests per second: 30,000 complete transactions sustained rate.		2
		Concurrent connections: at least 1.5 million		3
		Memory: 128GB		2
4	Performance requirements	**Compression:** The device should delivers up to 50-Gbps hardware-accelerated data compression and provides faster application performance for application users.		2
		SSL acceleration: Should support SSL acceleration technology, which offloads the encryption and decryption of SSL traffic from external devices (servers, appliances, etc.), thereby allowing the device to look more deeply into encrypted data and apply security and application switching policies and help ensure compliance with internal and external regulations.		4
		TCP offload: Should direct website traffic in the most efficient manner by analyzing and directing incoming traffic at the request level. These capabilities enable granular application-layer policy and offload TCP processing from the web servers, saving CPU cycles.		2
5	Availability	**Predictors:** The device should have predictors or load- balancing algorithms enabled to select the		2

		best server to satisfy a client request.		
		Server health monitoring: Should be capable of checking the health of application servers and server farms through configuration of health probes.		2
		Redundancy: Should support Stateful failover capabilities to help ensure resilient network protection for enterprise network environments		2
		Persistence and stickiness: Should support stickiness to allow the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session.		2
6	Security	**DDOS Protection:** The device should protect the data centre and critical applications from distributed denial of service attacks and encrypts mission-critical content.		2

		Application Security: The device should provide deep protocol inspection capabilities, which enables IT professionals to comprehensively secure high-value applications in the data centre. It secures mission-critical applications and protects against identity theft, data theft, application disruption, and fraud and defends web-based applications and transactions against targeted attacks by professional hackers. **Advanced Web Application Firewall:** The device should be able to identify and block attacks from application-layer encryption to protect against credential and data theft to L7 DDoS detection that uses machine learning and behavioral analytics. This Advanced WAF should provide the capability to provide Advanced Application Protection, Behavioral Analytics, Proactive Bot Defense, API Protocol Security, Anti-Bot Mobile SDK as well as 8the ability to provide Credential Protection. Should be an ICSA certified network and application firewall that supports both the Negative and Positive Security Models. The proposed WAF should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection		10

		f. Form Field and Parameter Tampering and HPP tampering g. Sensitive information leakage h. Session high jacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling The proposed WAF should have an in-built geo location database at no additional cost XML bombs/DoS		
7	IP DNS/Global Traffic	The device MUST have the feature to intelligently provide name resolution for all the systems being load balanced.		5
8	Virtualized Services/ Instances	**Virtual contexts or instances:** Virtual contexts capability to provide a means for creating resource segmentation and isolation, allowing the appliance to act as if it were several individual virtual appliances within a single physical appliance.		4
		Role-based access control (RBAC): Allows organizations		5

		to specify administrative roles and restrict administrators to specific functions within the appliance or virtual contexts, allowing each administrator group to freely perform its tasks without affecting the other groups.		
8	Deployment and Management	**Function consolidation:** Should provide consolidation of application switching, SSL acceleration, data centre security, and other functions on one device. **Management:** Embedded browser-based GUI and SNMP. The Management Platform should provide for the detailed reporting of Security Events from the specified device.		3
9	Environmental requirements	The device must support and be supplied with redundant power supply units. Operating power: 128 watts Maximum power consumption: 345W Ambient temperature: 104°F (40°C) Relative humidity: 80%		1
10	Proof of Certification/ accreditation/ manufacturer's authorization	State and provide proof of a certification program subscription		3
11	Training and knowledge transfer	The bidder MUST provide a plan for off-site Training leading to certification and costed for, for at least five (5) technical officers at OEM's authorized labs and centers.		5

12	OEM professional services.	Vendor is to provide installation and configuration support for the Solution through OEM professional services.		5
13	Support and warranty	At least 3 years on parts, labour and software In addition, the equipment MUST include the manufacturer's premier technical support services including: Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, online troubleshooting / support tools and proactive problem diagnosis services.		10
Total Score				**114**
Cut off (85%)				**98**

(b) INTERNAL (LOAD BALANCER); QUANTITY: 4

S.N	Feature	Minimum Requirements	Bidders' Response	Score
1	Model and Technology	The load balancer must be a mature internationally recognized brand (bidder must specify brand and model) which has been in existence for more than 5 years and the specified model is not reaching end of support/life in the next 4 years.		*5*
		Proposed solution shall be in Leaders Quadrant for a minimum of 5 continuous years Gartner Magic Quadrant for Application delivery controller		*8*

2	General description features	The device should provide load-balancing and content switching functions with granular traffic control based on customizable Layer 4 through 7 rules with support for both IPv4 and IPv6 addresses, virtual IP addresses (VIPs) and server farms.		2
		The device should natively load-balance the following protocols in an IPv4 environment: HTTP/HTTPS, FTP, DNS, ICMP, SIP, RTSP, Extended RTSP, LDAP, RADIUS, SCCP and Microsoft RDP. In an IPv6 environment, it should natively load-balance HTTP, HTTPS and SSL protocols. The device should have generic protocol parsing capabilities that enable the configuration of application switching and persistence policies based on any information in the traffic payload for custom and packaged applications without requiring any programming.		2
		The device should support translation and load balancing between IPv4 and IPv6 networks and provides flexibility to customers in planning their IPv6 migration.		2
		The device should have an Advanced WAF can identify and block attacks from application-layer encryption to protect against credential and data theft to L7 DDoS detection that uses machine learning and behavioral analytics. This Advanced WAF should provide		2

		the capability to provide Advanced Application Protection, Behavioral Analytics, Proactive Bot Defense, API Protocol Security, Anti-Bot Mobile SDK as well as the ability to provide Credential Protection.		
3	Operational features	Throughput: Device throughput of at least 95 Gbps /95 Gbps L4/L7 Intelligent Traffic Processing L7 request per second :4.3M		3
		Maximum L4 concurrent connection 100M		2
		L4 HTTP requests per second :18M		2
		Hardware Compression with support for up to 50Gbps		3
		SSL throughput: at least 50 Gbps		2
		SSL TPS: at least 100,000 SSL TPS using 2K keys		2
		Maximum L4 connections per second: 100,000 complete transactions sustained rate		3
		Maximum L7 Requests per second: 30,000 complete transactions sustained rate.		2
		Concurrent connections: at least 1.5 million		3
		Memory: 128GB		3
4	Performance requirements	**Compression:** The device should delivers up to 10-Gbps hardware-accelerated data compression and provides faster application performance for application users.		2

		SSL acceleration: Should support SSL acceleration technology, which offloads the encryption and decryption of SSL traffic from external devices (servers, appliances, etc.), thereby allowing the device to look more deeply into encrypted data and apply security and application switching policies and help ensure compliance with internal and external regulations.		5
		TCP offload: Should direct website traffic in the most efficient manner by analyzing and directing incoming traffic at the request level. These capabilities enable granular application-layer policy and offload TCP processing from the web servers, saving CPU cycles.		2
5	Availability	**Predictors:** The device should have predictors or load- balancing algorithms enabled to select the best server to satisfy a client request.		2
		Server health monitoring: Should be capable of checking the health of application servers and server farms through configuration of health probes.		2
		Redundancy: Should support Stateful failover capabilities to help ensure resilient network protection for enterprise network environments		2
		Persistence and stickiness: Should support stickiness to allow the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real		2

		server for the duration of a session.		
6	Security	**DDOS Protection:** The device should protect the data centre and critical applications from distributed denial of service attacks and encrypts mission-critical content.		2
7		**Application Security:** The device should provide deep protocol inspection capabilities, which enables IT professionals to comprehensively secure high-value applications in the data centre. It secures mission-critical applications and protects against identity theft, data theft, application disruption, and fraud and defends web-based applications and transactions against targeted attacks by professional hackers. **Advanced Web Application Firewall:** The device should be able to identify and block attacks from application-layer encryption to protect against credential and data theft to L7 DDoS detection that uses machine learning and behavioral analytics. This Advanced WAF should provide the capability to provide Advanced Application Protection, Behavioral Analytics, Proactive Bot Defense, API Protocol Security, Anti-Bot Mobile SDK as well as the ability to provide Credential Protection. Should be an ICSA certified network and application firewall that supports both the Negative and Positive Security Models.		10

		The proposed WAF should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP tampering g. Sensitive information leakage h. Session highjacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling The proposed WAF should have an in-built geo location database at no additional cost XML bombs/DoS		
8	Virtualized Services/ Instances	**Virtual contexts or instances:** Virtual contexts capability to provide a means for creating resource segmentation and isolation, allowing the appliance to act as if it were several individual virtual appliances within a single physical appliance.		5
9		**Role-based access control (RBAC):** Allows organizations to specify administrative roles and restrict administrators to		10

		specific functions within the appliance or virtual contexts, allowing each administrator group to freely perform its tasks without affecting the other groups.		
10	Deployment and Management	**Function consolidation:** Should provide consolidation of application switching, SSL acceleration, data centre security, and other functions on one device. **Management:** Embedded browser-based GUI and SNMP. The Management Platform should provide for the detailed reporting of Security Events from the specified device.		3
11	Environmental requirements	The device must support and be supplied with redundant power supply units. Operating power: 128 watts Maximum power consumption: 345W Ambient temperature: 104°F (40°C) Relative humidity: 80%		3
12	Proof of Certification/ accreditation/ manufacturer's authorization	State and provide proof of a certification program subscription		3
13	Training and knowledge transfer	The bidder MUST provide a plan for off-site Training leading to certification and costed for, for at least five (5) technical officers at OEM's authorized labs and centers.		5
14	OEM professional services.	Vendor is to provide installation and configuration support for the Solution through OEM professional services.		20

15	Support and warranty	At least 3 years on parts, labour and software In addition, the equipment MUST include the manufacturer's premier technical support services including: Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, online troubleshooting / support tools and proactive problem diagnosis services.		15
Total Score				**139**
Cut off (85%)				**120**

2. SDN SOLUTION OVERVIEW

A. Mandatory Requirements

No	General Requirements	Bidder's Response (Narrative answers describing how solution meets specification)
1	The proposed solution MUST provide unified management interface that automates network operations and policy orchestration across the fabric	
2	Proposed solution MUST provide for centralized management of operations and policies, with policy changes distributed in real-time to switches, across the distributed access network infrastructure.	
3	The solution MUST support application classification using Deep Packet Inspection	
4	The solution MUST have the capability for macro segmentation and secure micro segmentation for devices/services operating in the DC	

5	The proposed solution MUST have the capability to interact & interoperate with legacy LAN running standard spanning tree protocols	
6	The proposed solution MUST support multi-cloud deployments	
7	The solution should support advanced analytics using integrated AI/ML capability to aid in troubleshooting & experience optimization	
9	The make and model proposed MUST be clearly mentioned; all the relevant product brochures and manuals must be submitted. All switches should be SDN capable with support for analytics ,MACsec and Cloudsec	
11	The solution design must be validated by OEM	
12	The solution must use a holistic systems-based approach with tight integration between hardware and software, between physical and virtual elements, an open ecosystem model, and SDN-specific Integrated Circuits.	
14	The solution must consist of policy controllers, spine and leaf switches, Multisite orchestrators, Inter-DC IPN Routers and OOB Switches	
15	The vendor must include instructor-led training and certification by OEM covering Operations and Troubleshooting the SDN solution for 15 staff	
16	The solution must have been named be a leader in the Gartner Magic Quadrant for Datacentre Networking for the last 3 years	
18	The traffic load balancing between spine/leaf will be based on a balancing algorithm based on traffic congestion and this balancing will be performed in hardware	
19	Connectivity of physical servers, virtual machines and virtual containers without the need for software gateways.	
20	Flexible and redundant architecture	

21	Controllers cannot be a point of failure. The fix should work in case all drivers crash.	
22	The solution MUST be deployed in High availability design	
24	ECMP support	
25	Microsegmentation by VM name, Datacenter name, DNS, IP, MAC, Tag,..., etc. It must be compatible with any type of endpoint, virtual or physical.	
27	Support for Policy Base Redirect on DCI scenarios	
28	To ensure the high availability and stability of the two CPDs, the control protocols will not extend between them.	
29	To support complete active-active schemes, the fabric must be able to locally export services with /32 prefixes.	
30	All hardware (Controllers, Spine, Leafs, Routers, ..) must be a single vendor	
31	Support for Fabric Extenders connected to Leafs	
32	Support for Multi-Tier topology connecting Leaf to Leaf	
33	Support for Border Gateways to connect to external VXLAN networks (non-SDN)	

B. Additional Requirements

No	General Requirements	Max Score
1	The solution should offer rapid drill-down from network-wide to device-level monitoring views.	5
2	The solution must integrate seamlessly to KRA's existing network	10
3	Must be a secure, open, and comprehensive SDN solution	10
4	Compatible with extended fabric connectivity connected to smaller branches via L3 connection.	5
5	Anycast gateway support.	5

6	The two CPDs will operate in active-active mode under the same cluster of controllers. There should not be independent management for each CPD.	15
	Total	**50**
	Cut off	**43**

3. DATA CENTRE SPINE SWITCHES (QTY= 6)

Item No	Feature	Minimum Specifications	Score	Bidder's Response (*Narrative answers describing how solution meets specification*)
1	General Descriptive Requirement	▪ Switch Must support controller-based and standalone operation. ▪ The Switch should support non-blocking Layer 2 switching and Layer 3 routing ▪ Switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy ▪ Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc should not require switch reboot and disrupt the functionality of the system ▪ Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification. ▪ The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied	Mandatory	

		▪ Switch Must have the latest stable version of the available software release		
2	Model and Technology	Mature internationally recognized brand, in existence for at least 10 years(bidder must specify brand and model)	10	
3	Hardware and Interface Requirement	▪ Switch should have a minimum 36x100G ports with 400G upgrade capability network interfaces: ▪ System Memory; 32GB ▪ System Buffer: 80MB ▪ SSD Storage; 128GB ▪ Switch should have console port ▪ Switch should have management interface for Out of Band Management ▪ Switch should be rack mountable and support side rails if required ▪ Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP ▪ Switch should support VLAN tagging (IEEE 802.1q) ▪ Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy ▪ Switch should support Configuration roll-back and check point ▪ Switch should support for different logical interface types like loopback,VLAN, SVI, Port Channel, multi chassis port channel/LAG etc	15	
4	Layer 2 features	▪ Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S ▪ Switch should support VLAN Trunking (802.1q) and should	15	

		support 4096 VLAN ▪ Switch should support basic Multicast IGMP v1, v2, v3 ▪ Switch should support minimum 96,000 no. of MAC addresses ▪ Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch ▪ Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port. ▪ Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server ▪ Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports ▪ Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities ▪ Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures		
5	Layer 3 features	▪ Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port interface ▪ Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing	10	

		▪ Switch should support static and dynamic routing using: a. Static routing b. OSPF V.2 using MD5 Authentication c. ISIS using MD5 Authentication d. BGP V.4 using MD5 Authentication e. Should support route redistribution between these protocols f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable) ▪ Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols ▪ Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality ▪ Switch should be capable to work as DHCP server and relay ▪ Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM e. IGMP V.1, V.2 and V.3 ▪ Switch should support Multicast routing of minimum 16 way Equal Cost Multi Path load splitting		
6	Advanced Features	▪ Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890 ▪ Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside	10	

		the data center ▪ Switch should support OpenFlow/Open Day light/Open Stack controller ▪ Switch should support Data Center Bridging		
7	IPv6 Features	▪ Switch should support for IPv6 connectivity and routing required for network reachability using different routing protocols such a. OSPF V.3 b. BGP with IPv6 c. IP v6 Policy based routing d. IP v6 Dual Stack etc. e. IP v6 Static Route f. IP v6 Default route g. Should support route redistribution between these protocols ▪ Switch should support multicast routing in IP v6 network using PIMv2 Sparse Mode ▪ a. SNMPv1, SNMPv2c, SNMPv3 ▪ b. SNMP over IP v6 with encryption support for SNMP Version 3 ▪ Switch should support syslog for sending system log messages to centralized log server in IP v6 environment ▪ Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events a. Ping b. Traceroute c. VTY d. SSH e. TFTP f. DNS lookup	5	
8	Availability	▪ Switch should have provisioning for connecting to 1:1/N+1 power supply for usage	5	

		and redundancy ▪ Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP		
9	Quality of Service	▪ Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point) c. Weighted Random Early Detection d. Strict Priority Queuing ▪ Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy ▪ Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	10	
10	Security	▪ Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail ▪ Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy ▪ Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4 ▪ Switch should support for external database for AAA using: a. TACACS+ b. RADIUS	10	

		▪ Switch should support MAC Address Notification on host join into the network for Audit trails and logging ▪ Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding ▪ Switch should support DHCP Snooping ▪ Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol ▪ Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN ▪ Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined ▪ Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes ▪ Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port ▪ Switch should support Spanning tree BPDU protection ▪ Switch should support for		

		MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed as per banks ISD rules		
11	Performance	▪ The switch should support at least 500k Match IPv4 routes, and over 800k entries for IPv6 in the routing table including over 120K multicast routes ▪ Switch should support Graceful Restart for OSPF, BGP etc. ▪ Should support over 500K Mac address entries ▪ Switch should support minimum 4k VRF instances ▪ The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure ▪ The switch should support hardware based load balancing at wire speed using LACP and multi chassis etherchannel/LAG ▪ Switch should support minimum 3.6 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non-blocking capacity) including the services: ○ Switching ○ IP Routing (Static/Dynamic) ○ IP Forwarding ○ Policy Based Routing ○ QoS ○ ACL and Other IP Services ○ g. IP V.6 host and IP V.6 routing	10	
12	Management	▪ Switch should support for embedded RMON/RMON-II for central NMS management and monitoring	10	

		▪ Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail ▪ Switch should provide remote login for administration using: a. Telnet b. SSH V.2 ▪ Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures ▪ Switch should support for management and monitoring status using different type of Industry standard NMS using: a. SNMP V1 and V.2 b. SNMP V.3 with encryption c. Filtration of SNMP using Access list d. SNMP MIB support for QoS ▪ Switch should support for basic administrative tools like: a. Ping b. Traceroute ▪ Switch should support central time server synchronization using Network Time Protocol NTP V.4 ▪ Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces ▪ Switch should support for predefined and customised execution of script for device mange for automatic and scheduled system status update for monitoring and management ▪ Switch should provide different privilege for login in to the system for monitoring and management		

		▪ Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding		
13	Indicator and port specification	▪ System status: Green (operational), amber (fault), flashing amber (POST boot up), and off (no power) ▪ Locator LED: Bright blue locator ▪ Port status: Green (link established), amber (administratively disabled), and flashing amber (fault) ▪ Fan status: Green (operational) and amber (fault) ▪ Power status: Green (operational) and amber (fault)	10	
14	Power and cooling fans	Hot-swappable fan trays Dual power supply Maximum 1000W power consumption	5	
15	Proof of Certification/accreditation/manufacturer's authorization	State and provide proof of a certification program subscription	10	
16	Training and knowledge transfer	The bidder MUST provide a plan for off-site Training leading to certification and costed for, for at least five (5) technical officers at OEM's authorized labs and centers.	25	
17	Support and warranty	At least 3 years on parts, labour and software In addition, the equipment MUST include the manufacturer's premier technical support services including:	20	

		Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, online troubleshooting / support tools and proactive problem diagnosis services.		
Total Scores			**180**	
Cut-off (85%)			**153**	

4. <u>DATA CENTRE LEAF SWITCHES</u> (QTY= Secondary (**16**))

Item No	**Feature**	**Minimum Specifications**	**Score**	**Bidder's Response** (*Narrative answers describing how solution meets specification*)
1	General Descriptive Requirement	▪ Switch should run in SDN mode and be managed by a controller ▪ The Switch should support non-blocking Layer 2 switching and Layer 3 routing ▪ Switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy ▪ Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc. should not require switch reboot and disrupt the functionality of the system ▪ Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification. ▪ The Switch and different modules used should function	20	

		in line rate and should not have any port with oversubscription ratio applied ▪ Switch Must have the latest stable version of the available software release		
2	Model and Technology	Mature internationally recognized brand, in existence for at least 5 years(bidder must specify brand and model)	5	
3	Hardware and Interface Requirement	▪ Switch should have the following interfaces: ○ 48 x 1G/10G/25G Multi Mode Fiber Interface ○ 6 x 40/100GbE QSFP ports ▪ System Memory; At least 16GB ▪ System Buffer: 40MB ▪ SSD Storage; 128GB ▪ Switch should have console port ▪ Switch should have management interface for Out of Band Management ▪ Switch should be rack mountable and support side rails if required ▪ Switch should have adequate power supply for the complete system ▪ usage with all slots populated and used and provide N+1 redundant ▪ Switch should have hardware health monitoring capabilities and should ▪ provide different parameters through SNMP ▪ Switch should support VLAN tagging (IEEE 802.1q) ▪ Switch should support IEEE Link Aggregation and Ethernet Bonding ▪ functionality to group multiple ports for redundancy ▪ Switch should support Configuration roll-back and check point ▪ Switch should support for different logical interface types	10	

		like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc		
4	Layer 2 features	▪ Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S ▪ Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN ▪ Switch should support basic Multicast IGMP v1, v2, v3 ▪ Switch should support minimum 96,000 no. of MAC addresses ▪ Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch ▪ Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port. ▪ Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server ▪ Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports ▪ Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities ▪ Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	5	
5	Layer 3 features	▪ Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port interface	10	

		▪ Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing ▪ Switch should support static and dynamic routing using: ▪ a. Static routing ▪ b. OSPF V.2 using MD5 Authentication ▪ c. ISIS using MD5 Authentication ▪ d. BGP V.4 using MD5 Authentication ▪ e. Should support route redistribution between these protocols ▪ f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable) ▪ Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols ▪ Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality ▪ Switch should be capable to work as DHCP server and relay ▪ Switch should provide multicast traffic reachable using: ▪ a. PIM-SM ▪ b. PIM-SSM ▪ e. IGMP V.1, V.2 and V.3 ▪ Switch should support Multicast routing of minimum 16 way Equal Cost Multi Path load splitting		
6	Advanced Features	▪ Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890 ▪ Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center	10	

		▪ Switch should support OpenFlow/Open Day light/Open Stack controller ▪ Switch should support Data Center Bridging ▪ Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.		
7	IPv6 Features	▪ Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such ▪ a. OSPF V.3 ▪ b. BGP with IP V.6 ▪ c. IP V.6 Policy based routing ▪ d. IP V.6 Dual Stack etc ▪ e. IP V.6 Static Route ▪ f. IP V.6 Default route ▪ g. Should support route redistribution between these protocols ▪ Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode ▪ a. SNMPv1, SNMPv2c, SNMPv3 ▪ b. SNMP over IP V.6 with encryption support for SNMP Version 3 ▪ Switch should support syslog for sending system log messages to centralized log server in IP V.6 environment ▪ Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events a. Ping b. Traceroute c. VTY d. SSH e. TFTP f. DNS lookup	5	

8	Availability	▪ Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy ▪ Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP ▪ Switch should support for BFD For Fast Failure Detection as per RFC 5880	10	
9	Quality of Service	▪ Switch system should support 802.1P classification and marking of packet using: ▪ a. CoS (Class of Service) ▪ b. DSCP (Differentiated Services Code Point) ▪ a. Weighted Random Early Detection ▪ b. Strict Priority Queuing ▪ Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy ▪ Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	5	
10	Security	▪ Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail ▪ Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy ▪ Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4 ▪ Switch should support for external database for AAA using:	10	

		▪ a. TACACS+ ▪ b. RADIUS ▪ Switch should support MAC Address Notification on host join into the network for Audit trails and logging ▪ Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding ▪ Switch should support DHCP Snooping ▪ Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol ▪ Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN ▪ Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined ▪ Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes ▪ Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port ▪ Switch should support Spanning tree BPDU protection ▪ Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be		

		flashed as per banks ISD rules		
11	Performance	▪ The switch should support over 1.7M longest prefix Match IPv4 routes, and over 800k entries for IPv6 in the routing table including over 120K multicast routes ▪ Switch should support Graceful Restart for OSPF, BGP etc. ▪ Should support over 500K Mac address entries ▪ Switch should support minimum 4,000 VRF instances ▪ The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure ▪ The switch should support hardware based load balancing at wire speed using LACP and multi chassis etherchannel/LAG ▪ Switch should support minimum 3.6 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non-blocking capacity) including the services: ○ Switching ○ IP Routing (Static/Dynamic) ○ IP Forwarding ○ Policy Based Routing ○ QoS ○ ACL and Other IP Services ○ g. IP V.6 host and IP V.6 routing	10	
12	Management	▪ Switch should support for embedded RMON/RMON-II for central NMS management and monitoring ▪ Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail ▪ Switch should provide remote login for administration using: ▪ a. Telnet ▪ b. SSH V.2	5	

		▪ Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures ▪ Switch should support for management and monitoring status using different type of Industry standard NMS using: ▪ a. SNMP V1 and V.2 ▪ b. SNMP V.3 with encryption ▪ c. Filtration of SNMP using Access list ▪ d. SNMP MIB support for QoS ▪ Switch should support for basic administrative tools like: a. Ping b. Traceroute ▪ Switch should support central time server synchronization using Network Time Protocol NTP V.4 ▪ Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces ▪ Switch should support for predefined and customised execution of script for device mange for automatic and scheduled system status update for monitoring and management ▪ Switch should provide different privilege for login in to the system for monitoring and management ▪ Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding		
13	Indicator and port specification	▪ System status: Green (operational), amber (fault), flashing amber (POST boot up), and off (no power) ▪ Locator LED: Bright blue locator ▪ Port status: Green (link established), amber (administratively disabled), and flashing amber (fault)	5	

		▪ Fan status: Green (operational) and amber (fault) ▪ Power status: Green (operational) and amber (fault)		
14	Power and cooling fans	Hot-swappable fan trays Dual power supply Maximum power consumption : 400Watts	10	
15	Proof of Certification/ accreditation /manufacturer's authorization	State and provide proof of a certification program subscription	15	
16	Training and knowledge transfer	The bidder MUST provide a plan for off-site Training leading to certification and costed for, for at least five (5) technical officers at OEM's authorized labs and centers.	25	
17	Support and warranty	At least 3 years on parts, labour and software In addition, the equipment MUST include the manufacturer's premier technical support services including: Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, online troubleshooting / support tools and proactive problem diagnosis services.	15	
Total Scores			**175**	
Cut off (85%)			**149**	

5. CENTRALIZED POLICY AND MANAGEMENT CONTROLLER (QTY=6)

Item No	Feature	Minimum Requirements	Score	Bidder's Response (*Narrative answers describing how solution meets specification*)

1	Model/Brand	Internationally recognized model and brand, which has been in existence for the last 10 years.	10	
2	General Description	▪ The proposed solution must be designed as Clos network topology architecture defined using Spine, Leaf switches with VxLAN overlay ▪ The proposed solution should have following functionalities: ▪ Flexibility: Should allow workload mobility anywhere in the DC & DR [Design shall consider additional DC's] ▪ Resiliency: should be able to sustain multiple link and device (Leaf & Spine), Controller failures. ▪ Performance: should be able to use full cross-sectional bandwidth (any-to-any) across all provisioned uplink ports using equal cost multi-pathing (ECMP). ▪ Operations: should provide flow analytics using hop-by-hop latency and packet drop info for specific flows with reason of drop [helps to identify, locate and analyse root-cause data path issues]. ▪ Multi-Data Center design: should provide a single pane for provisioning, monitoring, and management to deploy stretched policies across multiple Data centers. ▪ All relevant licenses for all the features and scale should be quoted along with switches and all these licenses and features should be available from project beginning. ▪ The proposed solution must support various Hypervisor encapsulation including VxLAN, 802.1ad, and VLAN 802.1q natively without any additional hardware/software or design change.	15	

		▪ The proposed solution architecture must be based on hardware VxLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. ▪ The proposed solution must support Role Based Access 1.6 (RBAC) Control in order to support Multi-tenant environment. ▪ Solution must provide API integration with major hypervisor and container platforms including but not limited to VMware, Microsoft, Kubernetes, and Red Hat and manage virtualized networking from the single pane of Glass - [Centralized Management] for visibility of VM/Containers at the controller level. ▪ The proposed solution must integrate with all proposed L4-L7 Physical and virtual appliances using single pane of glass [Centralized Management]. ▪ The proposed solution must provide deeper visibility in terms of latency and packet drops between any two endpoints on the fabric. ▪ The proposed solution must provide L2 & L3 extension across multiple sites/ Data Center's. ▪ Solution must provide integrated L2 switching, L3 routing, and firewall capabilities across the fabric with centralized policy management. ▪ Fabric must support VxLAN Switching/Bridging and VxLAN Routing. ▪ The solution must propose and include the hardware required to support greater or equal to 1000 workloads from day one to meet		

		future growth without any hardware upgrades and performance impact and manage workloads distributed across MDC&DR from day one. The hardware should capture and analyse flow and process telemetry from all workloads across MDC and DR ▪ Bidder should e hardware (i.e. Compute, Memory, storage, Operating Systems, DB, Network Switch, replication, all relevant related licenses, etc...) for the controllers with the required high availability deployment to avoid any single point of failure to support greater or equal to 1000 workloads ▪ All hardware and software component of appliance based solution must be hardened to ensure security of the system and all version of OS/firmware/patch update schedule/ best practices must be followed and shared by Bidder		
3	Software IOS release	Should be delivered with the latest version and supported IOS release running. The provided IOS MUST support advanced IP services.	10	
4	Remote Management Protocol	Support SNMP 3, HTTP, SSH-2	5	
5	Spine, Leaf and Interfaces	▪ Leaf switches to Spine connectivity should be through uplink port using line rate higher or equal to 100Gbps. ▪ Spine and Leaf switches quoted should be non- oversubscribed and perform at line rate. ▪ All switches including Spine and Leaf should be of line rate including access ports and uplink ports. All the interfaces should be non-blocking.	10	

		▪ Solution must support a minimum of 300 isolated routing domains (VRFs/VRs/Virtual Routers). ▪ The solution should support scale up and scale out without any service disruption ▪ The solution must support minimum of 4/6 leaf switches and scale up to 12 leaf switches per site without any design change ▪ The solution must support minimum of 2 spine switches and scale up to 16 spine switches without any design change. ▪ The solution must support a minimum of 200 tenants without any additional component upgrade or design change.		
6	Security	The solution must implement a zero-trust security model with: ▪ Default-deny policy enforcement ▪ RBAC with AAA integration (RADIUS, TACACS+, LDAP, AD) ▪ Micro-segmentation based on workload attributes (hostname, OS, tags, AD groups) ▪ Ability to integrate existing DMZ architectures ▪ Security enforcement for virtual, container, and bare-metal workloads ▪ Inter-site encryption using AES-256 or stronger ▪ Automated service insertion for L4-L7 security services ▪ Consistent policy application across all workload types	10	
7	Visibility and Dependency	▪ The analytics platform must capture and analyze flow and process telemetry from all workloads across MDC and DR, in near real time and store in a time-series for long data retention of minimum 24 months. ▪ The solution must provide capability to edit and modify the discovered policies to define and include more absolute protection policies like Bank's Information Security policy	10	

		and Cyber Security Policy. It must export the policy to Network fabric, security devices etc... ▪ The solution must integrate with orchestration tools to provide end to end automation & rich application context to the workload. ▪ The solution must enforce the generated application whitelist policy on the application host workload using built-in host firewall on the application workload. ▪ The solution must provide consistent enforcement across all sites & workloads (Bare metal, virtual, container) to achieve east-west application segmentation. ▪ The solution must integrate with external systems such as vCenter, Kubernetes, PowerVM, IPAM or CMDB to bring in additional context for each application workload.		
8	App Compliance	▪ The solution must track application whitelist policy in near real-time for any compliance deviations and generate alerts (including full details of all flows in or out of policy compliance). ▪ The solution must have integration with user identity system to give visibility into users accessing Data Center resources, their groups and roles and device posture to enable segmentation based on those attributes. ▪ The solution must provide Micro-segmentation capability (application tier level, workload) on application end host. ▪ The solution must provide micro segmentation capability on application end host at remote location sites even in offline mode. ▪ The solution must provide full audit logging of all system access and changes applied. ▪ The solution must provide the ability to simulate the	10	

		▪ policies using near real time data, without having to enforce the policy. ▪ The solution application policy must be dynamically updated and enforced as an application changes and evolves e.g scale-out, migration, DR etc... ▪ The solution must detect, remediate and notify of any brute force override of the segmentation policy implementation. ▪ The solution should support enforcement of application whitelist policies on external security devices including SDN, Load-balancer and Firewalls using open APIs. ▪ The solution should be able to provide visibility into workload package vulnerabilities and create policies to restrict access or quarantine workloads using these vulnerability attributes. ▪ Security Policy extends to non-virtual workloads such as Databases, Mainframe, Unix systems, auto-scale clusters such as Hadoop ▪ The entirenetwork fabric is a stateless firewall, with Denied packets logged by default, permit packets can be logged optionally ▪ Consistent policy enforcement across all workloads irrespective of cloud virtual and physical ▪ Should be zero trust ready with a white list forwardfing policy model ▪ Expressive Policy Model that provides complete Automation for Virtual and Physical L4-L7 services from proposed vendor and other vendors ▪ Should provide Real-time hop-by-hop visibility and telemetry ▪ The system should provice Health scores per application/tenant		
9	Power integration	Input of 240 V AC, 50 Hz with Dual Power Supply Units	5	

	and power input			
10	Management requirements	Ability to support: ▪ The solution must provide Centralized Management Appliance/ SD data Center Controller - Single pane of glass for managing, monitoring and provisioning the entire Fabric within Data Centre & Disaster Recovery. ▪ The solution Centralized Management must auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy. ▪ The solution Centralized Management should not participate in Data plane and control plane traffic path of the fabric. ▪ The solution Centralized Management must provide Anomaly and Advisory reports for compliance and audit. ▪ The solution Centralized Management should be able to store historical data to provide anomalies and trending information of each resource (environment, configuration & operational) and graphical representation of parameters for debug. ▪ The solution Centralized Management should provide an automated mechanism to find configuration deviations, security risks & non-compliances against segmentation rules by assessing current configuration, network security policies and generate alert for any deviation to provide assurance. ▪ The solution Centralized Management should provide network visibility and historical analysis between any two time	10	

		frames to identify any issues and changes including user information. ▪ The solution Centralized Management should provide pre-change analysis of the configuration to highlight any challenges and issues before pushing the configuration within the fabric to reduce the risk of network failures and human errors for a robust change management. ▪ The solution Centralized Management should provide instant visibility into any relevant and applicable bugs, security advisories, artificial Intelligence(AI) capabilities and field notices for running hardware and configuration. ▪ The solution Centralized Management should provide recommendations on software update & best practices based on installed platforms and running configuration in network. ▪ Solution must use open, standards-based protocols (e.g., NETCONF, RESTCONF, OpenFlow, OVSDB, gRPC) for southbound communication etc... or using Device APIs. ▪ The solution Centralized Management must run in redundancy to provide availability as well as to function during a standalone scenario. ▪ In the event of failure of the solution centralized management, the fabric must function with the current configuration and without any performance degradation. ▪ The solution Centralized Management must provide real-time device inventory and network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.		

		▪ All the infrastructures including hardware and licenses required by fabric controllers to support the listed features and scale, should be provided by the bidder.		
11	Proof of Certification /accreditation/manufacturer's authorization	▪ State and provide proof of a certification program subscription	10	
12	Training and knowledge transfer	▪ The bidder MUST provide a plan for off-site Training leading to certification and costed for, for at least five (5) technical officers at OEM's authorized labs and centers.	25	
13	Support and warranty	▪ At least 3 years on parts, labour and software ▪ In addition, the equipment MUST include the manufacturer's premier technical support services including: ✓ Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, online troubleshooting / support tools and proactive problem diagnosis services.	10	
Total Scores			**140**	
Cut off (85%)			**120**	

6. IPN EQUIPMENT (QTY=Primary(2) Secondary (2))

To provide layer 3 interconnectivity between the data centers and the SDN Fabric.

Item No	Feature	Minimum Specifications	Score	Bidder's Response (*Narrative answers describing how solution meets*

				specification)
1	General Descriptive Requirement	▪ Switch should run in SDN mode and be managed by a controller ▪ The Switch should support non-blocking Layer 2 switching and Layer 3 routing ▪ Switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy ▪ Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc should not require switch reboot and disrupt the functionality of the system ▪ Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification. ▪ The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied ▪ Switch Must have the latest stable version of the available software release	10	
2	Model and Technology	Mature internationally recognized brand, in existence for at least 5 years(bidder must specify brand and model)	10	
3	Hardware and Interface Requirement	▪ Switch should have the following interfaces: ○ 48 x 1G/10G/25G Multi Mode Fiber Interface ○ 6 x 40/100GbE QSFP ports ▪ System Memory; At least 16GB ▪ System Buffer: 40MB ▪ SSD Storage; 128GB ▪ Switch should have console port ▪ Switch should have management interface for Out of Band Management ▪ Switch should be rack mountable and support side rails if required ▪ Switch should have adequate power supply for the complete system	10	

		▪ usage with all slots populated and used and provide N+1 redundant ▪ Switch should have hardware health monitoring capabilities and should ▪ provide different parameters through SNMP ▪ Switch should support VLAN tagging (IEEE 802.1q) ▪ Switch should support IEEE Link Aggregation and Ethernet Bonding ▪ functionality to group multiple ports for redundancy ▪ Switch should support Configuration roll-back and check point ▪ Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc		
4	Layer 2 features	▪ Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S ▪ Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN ▪ Switch should support basic Multicast IGMP v1, v2, v3 ▪ Switch should support minimum 96,000 no. of MAC addresses ▪ Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch ▪ Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port. ▪ Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server ▪ Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports ▪ Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network	5	

		attacks and vulnerabilities ▪ Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures		
5	Layer 3 features	▪ Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port interface ▪ Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing ▪ Switch should support static and dynamic routing using: ▪ a. Static routing ▪ b. OSPF V.2 using MD5 Authentication ▪ c. ISIS using MD5 Authentication ▪ d. BGP V.4 using MD5 Authentication ▪ e. Should support route redistribution between these protocols ▪ f. Should be compliant to RFC 4760 Multiprotocol Extensions for BGP-4 (Desirable) ▪ Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols ▪ Switch should support multi instance MPLS routing using VRF, VRF Edge routing and should support VRF Route leaking functionality ▪ Switch should be capable to work as DHCP server and relay ▪ Switch should provide multicast traffic reachable using: ▪ a. PIM-SM ▪ b. PIM-SSM ▪ e. IGMP V.1, V.2 and V.3 ▪ Switch should support Multicast routing of minimum 16 way Equal Cost Multi Path load splitting	5	
6	Advanced Features	▪ Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890 ▪ Switch should support VXLAN (RFC7348) and EVPN or equivalent for	10	

		supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center ▪ Switch should support OpenFlow/Open Day light/Open Stack controller ▪ Switch should support Dta Center Bridging ▪ Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.		
7	IPv6 Features	▪ Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such ▪ a. OSPF V.3 ▪ b. BGP with IP V.6 ▪ c. IP V.6 Policy based routing ▪ d. IP V.6 Dual Stack etc ▪ e. IP V.6 Static Route ▪ f. IP V.6 Default route ▪ g. Should support route redistribution between these protocols ▪ Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode ▪ a. SNMPv1, SNMPv2c, SNMPv3 ▪ b. SNMP over IP V.6 with encryption support for SNMP Version 3 ▪ Switch should support syslog for sending system log messages to centralized log server in IP V.6 environment ▪ Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events a. Ping b. Traceroute c. VTY d. SSH e. TFTP f. DNS lookup	5	
8	Availability	▪ Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	10	

		▪ Switch should provide gateway level of redundancy in Ip V.4 and IP V.6 using HSRP/VRRP ▪ Switch should support for BFD For Fast Failure Detection as per RFC 5880		
9	Quality of Service	▪ Switch system should support 802.1P classification and marking of packet using: ▪ a. CoS (Class of Service) ▪ b. DSCP (Differentiated Services Code Point) ▪ a. Weighted Random Early Detection ▪ b. Strict Priority Queuing ▪ Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy ▪ Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	5	
10	Security	▪ Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail ▪ Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy ▪ Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4 ▪ Switch should support for external database for AAA using: ▪ a. TACACS+ ▪ b. RADIUS ▪ Switch should support MAC Address Notification on host join into the network for Audit trails and logging ▪ Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address	10	

		flooding ▪ Switch should support DHCP Snooping ▪ Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol ▪ Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN ▪ Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined ▪ Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes ▪ Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port ▪ Switch should support Spanning tree BPDU protection ▪ Switch should support for MOTD banner displayed on all connected terminals at login and security discrimination messages can be flashed as per banks ISD rules		
11	Performance	▪ The switch should support minimum 500k IPv4 routes, and over 800k entries for IPv6 in the routing table including over 120K multicast routes ▪ Switch should support Graceful Restart for OSPF, BGP etc. ▪ Should support over 500K Mac address entries ▪ Switch should support minimum 4000 VRF instances ▪ The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure	10	

		▪ The switch should support hardware based load balancing at wire speed using LACP and multi chassis etherchannel/LAG ▪ Switch should support minimum 3.6 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non-blocking capacity) including the services: o Switching o IP Routing (Static/Dynamic) o IP Forwarding o Policy Based Routing o QoS o ACL and Other IP Services o g. IP V.6 host and IP V.6 routing		
12	Management	▪ Switch should support for embedded RMON/RMON-II for central NMS management and monitoring ▪ Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail ▪ Switch should provide remote login for administration using: ▪ a. Telnet ▪ b. SSH V.2 ▪ Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures ▪ Switch should support for management and monitoring status using different type of Industry standard NMS using: ▪ a. SNMP V1 and V.2 ▪ b. SNMP V.3 with encryption ▪ c. Filtration of SNMP using Access list ▪ d. SNMP MIB support for QoS ▪ Switch should support for basic administrative tools like: a. Ping b. Traceroute ▪ Switch should support central time server synchronization using Network Time Protocol NTP V.4 ▪ Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces	5	

		▪ Switch should support for predefined and customised execution of script for device mange for automatic and scheduled system status update for monitoring and management ▪ Switch should provide different privilege for login in to the system for monitoring and management ▪ Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding		
13	Indicator and port specification	▪ System status: Green (operational), amber (fault), flashing amber (POST boot up), and off (no power) ▪ Locator LED: Bright blue locator ▪ Port status: Green (link established), amber (administratively disabled), and flashing amber (fault) ▪ Fan status: Green (operational) and amber (fault) ▪ Power status: Green (operational) and amber (fault)	5	
14	Power and cooling fans	Hot-swappable fan trays Dual power supply Maximum power consumption : 400Watts	5	
15	Proof of Certification/accreditation/manufacturer's authorization	State and provide proof of a certification program subscription	10	
16	Training and knowledge transfer	▪ The bidder MUST provide a plan for off-site Training leading to certification and costed for, for at least five (5) technical officers at OEM's authorized labs and centers.	20	
17	Support and warranty	At least 3 years on parts, labour and software In addition, the equipment MUST include the manufacturer's premier technical support services including: Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team,	15	

		online troubleshooting / support tools and proactive problem diagnosis services.		
Total Scores			**150**	
Cut off (85%)			**128**	

7. **DATA CENTRE CORE WAN ROUTERS** (QTY=Primary(**2**) Secondary (**2**))

Item No	**Feature**	**Minimum Specifications**	**Score**	**Bidder's Response** (*Narrative answers describing how solution meets specification*)
1	Model/Brand	Internationally recognized model and brand.	10	
2	Default Memory - Data Plane	At Least 4GB	5	
3	Default Memory - Control Plane	At least 6GB	5	
4	Maximum Throughput	At least 5Gbps	5	
5	Network ports	At least 3 integrated 10/100/1000 Ethernet ports with 2 ports capable of RJ-45 or SFP connectivity, plus additional 4 RJ-45 based 100/1000 Ethernet ports on the expansion slots.	10	
6	Software IOS release	Should be delivered with the latest version and supported IOS release running. The provided IOS MUST support advanced IP services.	10	
7	Remote Management Protocol	Support SNMP 3, HTTP, SSH-2	5	

8	Module support	▪ Enhanced network modular slots ▪ High performance WIC slots ▪ AIM slots ▪ PVDM slots ▪ EVM slots ▪ USB support	5	
9	Security	▪ Firewall software support ▪ Secure Sockets Layer support ▪ Network Admission control support	5	
10	VPN support	VPN hardware acceleration, DES, 3DES, AES128, AES192 and AES256, support IPSEC Pass-thru	5	
11	Transmission mode	Full/half duplex	5	
12	Power integration and power input	In-line PoE and input of 240 V AC, 50 Hz	5	
13	Management requirements	Ability to support: ▪ The firewall should be manageable via Telnet, SSH, Serial Console port, HTTPS, and via central management software ▪ Support integration with AAA such as Local, RADIUS, TACACS+, NT, RSA, and LDAP ▪ Ability to support SNMP and syslog ▪ Network Secure Event Logging (NSEL)	5	
14	Proof of Certification/accreditation/manufacturer's authorization	▪ State and provide proof of a certification program subscription	10	

15	Training and knowledge transfer	▪ The bidder MUST provide a plan for off-site Training leading to certification and costed for, for at least five (5) technical officers at OEM's authorized labs and centers.	15	
16	Support and warranty	▪ At least 3 years on parts, labour and software ▪ In addition, the equipment MUST include the manufacturer's premier technical support services including: ✓ Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, online troubleshooting / support tools and proactive problem diagnosis services.	15	
Total Scores			**120**	
Cut off (85%)			**102**	

8. DARK FIBER DWDM INFRASTRUCTURE (QTY=4)

Item No	Feature	Minimum Specifications	Score	Bidder's Response (*Narrative answers describing how solution meets specification*)
1.	General Descriptive Requirement	Optical Wavelength Division Multiplexing (WDM) solution for Data Centre Interconnect (DCI). The equipment MUST provide a seamless integration with the existing KRA network.	10	
2.	Model and Technology	Mature internationally recognized brand, in existence for at least 10 years (bidder must specify brand, model and series). The device MUST NOT be a product that has/is reaching end of life support/end of sale in two years' time.	10	
3.	Line redundancy	The solutions should support two dark fibre links and be able switch automatically to ensure high service availability.	15	
4.	Network Ports	Multi-rate and multi-protocol supporting at least 6*16 Fibre Channel (FC) and 6-10G Fibre-Ethernet ports. (Scalable to 32G and 40G). Should	8	

		be fully populated with relevant SFPs.		
5.	Channel Support	Minimum 40 wavelengths at 100GHz spacing or 80 wavelengths at 50GHz spacing	15	
6.	Other Features	Must support (IPv4 and IPv6) features, advanced quality of service (QoS), rate limiting, Access Control Lists (ACLs)	5	
7.	Compliance	IEEE 802.1Q, 802.1p, 802.3x	2	
		Ethernet: IEEE 802.3, 10BaseT, and 10BaseFL	3	
		Fast Ethernet: IEEE 802.3u, 100BaseTX, 10BaseFX	2	
		Gigabit Ethernet: IEEE 802.3z.	2	
		Standards-based interoperability with major network equipment vendors.	2	
8.	Network Monitoring	Compliant with IEEE SNMP standards. Capable of monitoring the Network up to Node Level. Management by a well-known and developed proprietary OS.	4	
9.	Security	Solution should support Supports AES-256 hardware-based encryption.	5	
10.	Software release	Should be delivered with the latest version and supported release	8	
11.	Power input	Dual power supply units	5	

		240 VAC, 50-60 Hz	3	
12.	Fan	Dual fan modules, field-replaceable	2	
13.	Implementation	The bidder should implement the solution to ensure 99.99% availability of dark fiber services via at least two redundant routes and different ISPs	10	
14.	Warranty & Support	Minimum 3 years on Parts, labour and software and next business day replacement for any hardware failure that may occur. In addition, the equipment MUST include the manufacturer's premier technical support services that include: Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, Online troubleshooting / support tools and proactive problem diagnosis services.	8	
Total Score			**119**	
Cut off (85%)			**101**	

9. MINIMUM TECHNICAL SPECIFICATIONS FOR 48 - PORT FIBER SWITCHES

No	Feature	Minimum Requirements	Score	Bidder's Response

1.	General Descriptive Requirement	Enterprise standalone, High-density, High performance, MultiGigabit Ethernet switch. Layer 2 switching and basic routing to be supported. The switch **MUST** provide a seamless integration with the existing KRA network.	10	
2.	Model and Technology	Mature internationally recognized brand, in existence for at least 10 years (bidder must specify brand, model and series). The device **MUST NOT** be a product that has/is reaching end of life support/end of sale in two years' time.	5	
3.	Network Ports	48 Ethernet 1G/10G SFP transceiver-based ports.	10	
4.	Routing and Layer 3 Features	Must support Advanced Layer 3 capabilities including OSPF, EIGRP, ISIS, RIP and routed access	5	
5.	Switching capacity	At least 3 Tbps	5	
6.	Other Features	Must support (IPv4 and IPv6) features, advanced quality of service (QoS), rate limiting, Access Control Lists (ACLs)	3	
7.	Compliance	IEEE 802.1Q, 802.1p, 802.3x	3	
		Ethernet: IEEE 802.3, 10BaseT, and 10BaseFL	2	
		Fast Ethernet: IEEE 802.3u, 100BaseTX, 10BaseFX	3	
		Gigabit Ethernet: IEEE 802.3z.	2	
		Compatible with different vendors' network equipment e.g. 3com, Nortel, Cisco.	3	
8.	Network Monitoring	Compliant with IEEE SNMP standards. Capable of monitoring the Network up to Node Level. Management by a well-known and developed proprietary OS.	4	
9.	Spanning Tree	Support for Spanning Tree Protocol Technology	3	

	Protocol Technology			
10.	VLAN support	Compliant with IEEE 802.1Q standards- should support VLANS/Network Segmentation.	5	
11.	Security	Port Level Security e.g. Port Filtering, Access Control Lists, Policy based routing etc. Management by a recognized proprietary operating system.	8	
12.	Operation	Auto negotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth.	5	
		Can support converged wired and wireless access.	3	
		Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance.	5	
13.	Software IOS release	Should be delivered with the latest version and supported IOS release	8	
14.	Power input	Dual power supply units	5	
		240 VAC, 50-60 Hz	3	
15.	Fan	Dual fan modules, field-replaceable	3	
16.	Warranty & Support	Minimum 3 years on Parts, labour and software and next business day replacement for any hardware failure that may occur. In addition, the equipment ***MUST*** include the manufacturer's premier technical support services that include: Accelerated hardware replacement options, Operating system updates, Access to Manufacturer's technical assistance team, Online troubleshooting / support tools and proactive problem diagnosis services.	10	

		The proposed product **MUST** have a manufacturer's local warranty & Support. KRA will verify with the manufacturer to ensure compliance.		
Total Scores			**113**	
Cut off (85%)			**96**	

Price Schedule for Proposed Core Network Infrastructure Upgrade

No	Item	Qty	Unit Cost (Ksh)	Total (Kshs
1	Data Centre Application Load Balancer	8		
2	Data Centre Spine Switches	6		
3	Data Centre Leaf Switches	16		
4	Centralized policy and management controller	2		
5	IPN Equipment	2		
6	Data Center WAN Router	4		
7	Dark Fiber DWDM infrastructure	2		
8	Campus Fiber Aggregation Switches	2		
9	Installation/Deployment Cost	1		
	GRAND-TOTAL			

c) Provision of additional equipment (if any) at the quoted unit rates as determined at the design stage

FINANCIAL REQUIREMENT

• N/B: Bidders to provide a detailed breakdown of how they have arrived at the total cost
• Grand Total Cost –To be carried Forward to the FORM FIN 2 Summary of Costs

VIII. *POST-QUALIFICATION/DUE DILIGENCE*

The Procuring Entity may conduct post-qualification/due diligence on the lowest evaluated bidder before the award of the contract. This process may include, but is not limited to;

1. Verification of Documentation – Confirming the authenticity of certifications, reference letters, and any other supporting documents submitted with the bid.
2. Reference Checks – Engaging with past and current clients to verify performance, service delivery, and adherence to contractual obligations.
1. Financial Capability Assessment – Evaluating the financial strength of the bidder to ensure their ability to sustain the project, including a review of audited financial statements.
2. Reference Site Validation – Reconfirming the ability of the bidder to provide the proposed product(s) and support, in accordance with the stated service levels, through a mandatory site visits to the provided reference sites by the evaluation team.

Failure to satisfactorily pass the post-qualification and due diligence process may result in the disqualification of the bidder, and the Procuring Entity reserves the right to consider the next lowest evaluated bidder or take any other appropriate action in accordance with procurement laws and regulations.