



**Kenya Bureau of
Standards**

Standards for quality life

KEBS/T018/2019/2020

TO: ALL INTERESTED BIDDERS

REF: ADDENDUM NO.1 FOR KEBS/T018/2019/2020: SUPPLY, IMPLEMENTATION AND COMMISSIONING OF KEBS CYBERSECURITY SOLUTION FOR CLOUD EMAIL, SAAS AND IAAS

Reference is made to the above tender for supply, implementation and commissioning of kebs cybersecurity solution for cloud email, SaaS and IaaS. KEBS wishes to provide the following clarification.

1. What is the number of users for the said Cloud applications.

Response

Refer to the price schedule on page 28 of the tender document on the Quantity of Cloud SaaS for Office 365 Subscription for (1 year) + Support Services

2. How many users do you wish to cover?

Response

Refer to the price schedule on page 28 of the tender document on the Quantity of Cloud SaaS for Office 365 Subscription for (1 year) + Support Services

3. What API's do you want to protect? See list below (AS are able to connect directly into these apps and provide protection at the API level)

Response

Microsoft 0365 Applications i.e. Office, Teams, One drive, Share point

- Microsoft (Gold Partner and Cloud API Partner) - includes full stack of E license (Teams, OneDrive, SharePoint etc.)
- Google
- Box (member of the Box Trust Partner program, Elite Member of the Box Platform Partner program, and recipient of the coveted Box Customer Transformation Partner of the Year for 2015, the only ISV to receive an award)
- Dropbox
- Intralinks
- ServiceNOW
- Salesforce
- Egnyte

- Cisco
- Slack
- Workplace by Facebook
- SA

4.0 IaaS

For the IaaS / Public cloud coverage, we would need to understand:

- a) How many resources are assigned to AWS / Azure – Typically containers, storage, S3 budgets etc – Total number is fine across all IaaS

Response

The firewall solution will be based on the listed virtual cores as per the RFP specifications. It should support auto scaling to enforce security as per the business requirements.

- b) What size is the data store in GB's please – how much data are we scanning for DLP violations etc

Response

The security solution storage should be flexible adjusting to the underlying infrastructure and throughput as per demand. DLP should automatically adjust security policies and logging to any changes in the dynamic cloud environment.

5.0 How many VNETs are connected to the Firewalls VNET?

Response

Initial three VNETS with subnets for the frontend and backend subnets to ensure full traffic inspection.

6.0 How many Virtual Machines are in the VNETs?

Response

Consider two virtual machines per VNET.

7.0 Will the firewall inspect traffic between different VNET?

Response

The security solution should be able to inspect intra VNET traffic.

8.0 Will you wish to use the firewalls to inspect traffic between all the VMs?

Response

The firewall security solution should offer comprehensive lateral protection between the virtual machines.

9.0 Will you wish to use the firewalls to inspect traffic towards the internet?

Response

The firewall security solution should inspect inbound and outbound traffic to the cloud infrastructure.

10 Will large data transfers or SQL replication need to be inspected?

Response

The solution should be flexible and agile to protect all workloads including databases, applications and servers.

11. Are you connecting Client to Site VPN users? How many?

Response

The solution should support client/site and IPsec VPNs between the cloud infrastructure, on premise environment and partner networks.

12. Will Site to Site VPN's be connected? How Many?

Response

VPN connectivity should be unlimited, agile and easily configurable to facilitate growth of secure connections.

**NOTE THIS ADDENDUM SHALL BE CONSTRUED TO FORM PART OF THE
TENDER DOCUMENT**

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME

MANAGING DIRECTOR