REQUEST FOR QUOTATION

Supply and Deployment of Firewall Appliance

REF No	MKIQ34/2022
Description	Supply and deployment of firewall appliance
Business Address	7 Umsinsi Junction, La Mercy, Durban
Closing date and time to submit proposals.	18 July 2022, 16h30
Quotations and SCM queries must be emailed to: Hand delivered submissions will NOT be accepted.	Sinenhlanhla.ngqulunga@moseskotane.com
Technical queries must be emailed to:	Asanda.tose@moseskotane.com / 0832689575

a) Disclaimer

- MKI reserves its right not to appoint.
- MKI reserves its right to negotiate the price with the winning bidder.

b) Terms and Conditions

- Proposals must be emailed by no later than 18 July 2022, 16:30. Quotations received after the closing time and date will not be considered.
- All prices must be all inclusive. Only firm prices will be accepted. Non-firm prices (including prices subject to rates of exchange variations will not be considered)
- Bid validity period: 60 days.
- Proposals will be evaluated on the 80/20 preference points system.

1. Background

In computer networks, the most vulnerable to attacks are those that provide services outside the local area network, such as websites, email, etc, due to the increase in the potential of these hosts being compromised, as a rule of thumb they are placed into their sub-network to protect the rest of the network if an intruder were to attack the network.

Moses Kotrane Institute requires a firewall to meet security requirements such as the Data Security Standard, which specifically require firewalling. Several types of firewall technologies are available.

Moses Kotane Institute requires a reputable service provider to supply and deploy capabilities, to ensure Transmission Control Protocol/Internet Protocol (TCP/IP) layers can be examined, TCP/IP communications are composed of four layers that work together to transfer data between hosts. When a user wants to transfer data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer, with each layer adding more information. The lowest layer sends the accumulated data through the physical network, with the data then passed upwards through the layers to its destination. Simply put, the data produced by a layer is encapsulated in a larger container by the layer below it.

2. Technical Requirements

Firewalls are devices that control the flow of network traffic between networks and hosts that employ differing security postures. While firewalls are often discussed in the context of Internet connectivity, they are applicable in other network environments. Moses Kotane Institute enterprise networks seek to employ a firewall to restrict connectivity to and from the internal networks used to service more sensitive functions of the organisation, such as Finance, hosts, and personnel data. By employing a firewall to control connectivity to these areas, Moses Kotane Institute can prevent unauthorised access to its systems and resources. The inclusion of an appropriate firewall provides an additional layer of security.

With the rise in remote working, cybercriminals have been hard at work infiltrating systems to steal data and disrupt business operations. Therefore, Moses Kotane Institute requires a

comprehensive platform with cybersecurity capabilities to protect the IT enterprise environment, including applications, data, and users from every part of the organisation, across the LAN, Web and Cloud platforms. The rapid pace of technological change has created the following opportunities to ensure the Moses Kotane Institute IT enterprise environment is fully secured.

3. Scope

Functional Requirements	MINIMUM MANDATORY REQUIREMENT
1. Base Firewall	**1.1.SD-WAN and Cloud Security** The solution should include networking, routing, and SD-WAN capabilities with a zone-based stateful firewall, NAT, VLAN support, multiple WAN link options with SD-WAN routing, fail-over, and fail-back **1.2.Secure Wireless** Should have a built-in wireless controller for wireless access points. Plug and play access point discovery and support SSIDs, hotspots, gust networks, and diverse encryption and security standards. **1.3.VPN (Virtual Private Network)** Should provide standards-based site-to-site remote access VPN (Free up security capacity of the firewall) with support for IPsec and SSL. Connect remote access VPN client for Windows and Macs and offer seamless and easy deployment and configuration options. Ensure SD-RED layer2 site-to-site tunnels offers a lightweight robust VPN alternative. **1.4.Reporting** Provide on-box reporting to ensure IT environment gains valuable insight into threats, users, applications, web activity and more.
2. Network Protection	**2.1.Next-Gen Intrusion Prevention System** Provide advance protection from all types of modern attacks. It should go beyond traditional server and network resources to protect users and applications on the network. **2.2.Security Heartbeat** Should have the capability to create a link between central firewall administration protected endpoints and the firewall to identify threats faster, simplify investigation, and minimize impact from attacks. It should easily

	incorporate heartbeat status into the firewall policies to automatically isolate compromised systems. **2.1.Advanced Threat Protection** Ensure instant identification and immediate response to today's most sophisticated attacks. It should have multi-layered protection that identifies threats instantly with a security heartbeat that provides emergency response. **2.2.Advanced VPN Technologies** This should add unique and simple VPN technologies, including a clientless HTML5 self-service portal for remote access as well as utilise lightweight secure SD-RED (Remote Ethernet Device) VPN technology.
3. Network Traffic	**3.1.Encrypted Traffic** Ensure TLS Inspection 1.3 with industry-leading performance, visibility, policy tools, and built-in intelligence to remove any blind spot in the protection solution. • TLS 1.3 without downgrading • Intelligent traffic selection • Pre-packaged exception list • Power policy engine • Cover all ports/protocols • Support all modern cypher suites • Unmatched visibility and error handling
4. Web Protection	**4.1.Power-user and group web policy** The solution should provide enterprise-level secure web policy controls to ensure easy management of sophisticated user and group web controls. Ensure application of policy-based upon uploaded web keywords indicating inappropriate use or behaviour. **4.2.Application Control QoS (Quality of Service)** The solution should enable user-aware visibility and control over many applications with granular policy and traffic-shaping (QoS) options based on

	application category, risk, and other characteristics. Should also ensure synchronised application control that automatically identifies all the unknown, evasive and custom applications on the network. **4.3.High-performance scanning** Should ensure optimization for top performance SSL inspection to provide ultra-low latency inspection and HTTPS scanning while maintaining performance.
5. Zero-Day Protection	5.1.Guarantee a firewall that leverages industry-leading machine learning technology to instantly identify the latest ransomware and unknown threats before they propagate into the networked environment. • Ensure data science mining capabilities • Multiple Machine Learning Models • Static File Analysis • Dynamic file analysis • Dynamic intelligence analysis and reporting
6. Cloud Capabilities	**6.1. Cloud Sandbox** Guarantee Zero-day dynamic file analysis to ensure the use of next-generation sandbox technology powered by deep-learning and best technology capabilities, it should also provide Moses Kotane Institute with the best protection against zero-day threats such as ransomware and targeted coming in through phishing, spam and web downloads. • Ensure dynamic sandboxing analysis • Guarantee pharming protection • HTTPS scanning • Protection from unwanted application control attacks

7. Security	**7.1. Synchronised Security** Ensure security heartbeat to manage threats and share health and other valuable information to enable an automated and coordinated response to isolate threats and prevent lateral movement. • Ensure security heartbeat monitoring • Guarantee destination heartbeat protection • Synchronised application control **7.2. User Identity** The appliance should be able to identify users based on policies and unique user risk analysis and profiling to provide knowledge and power to regain control of users before they become a significant threat to the Moses Kotane Institute Network. • User Identity that is powered by all firewall policies and reporting capabilities. • User Threat Quotient (UTQ) to identify top user risks on the network. • Able to synchronise with the User ID • Flexible authentication including directory services • Two-factor Authentication (2FA) One-time Password Support for Access to key system areas.
8. Data Protection	**8.1. Email and Data** Protect Moses Kotane Institute emails from spam, phasing and data loss with unique all-in-one protection that combines policy-based email encryption with DPL and anti-spam. • Full MTA store and forward support • Live anti-spam • SPX encryption • Policy-based DLP

	• Self-server user portal +
9. Hardware Features	**9.1.Technical Specifications:** a. Physical Specifications • 1 U Rackmount b. Environment • Power supply • POE edition enabled c. Performance • 35 000 Mbps of Firewall Throughput • Firewall IMIX of 20 000 Mbps • IPS Throughput of 7000 Mbps • 6 500 000 concurrent connections • 1400 Mbps of Threat Protection Throughput • 1450 Mbps of SSL/TSL Throughput d. Physical interface • Integrated 120 GB SATA-III SSD • Ethernet interface (8 X GbE copper, 2 X SFP Fiber) • Management ports (1 x RJ45 MGMT, 1 x COM RJ45, 1 x Micro-USB (cable incl.))
10. Other Features	a. 130 hours Premium technical support per year b. Standard 24x7 unlimited telephone and email support, including weekends and holidays. c. All software patches/updates are to be performed by the Administrator. d. Hybrid support for update and testing of new updates. e. Implementation of firewall policies as required by MKI. f. Support for the server where the firewall is installed such as but not limited to installation and set-up when necessary. g. Training and certification of two in-house engineers.

3. Delivery

Delivery of all components and their peripherals shall be within 15 working days upon execution of the contract. Setup, implementation, and testing of all components shall be within 30 calendar days upon delivery of all the components and their peripherals. Only quotations from platinum and gold partners that are duly certified and authorised by the manufacturer to provide, sell, configure, and support the firewall appliance shall be accepted. The certification from the manufacturer authorising the supplier to provide such a product should be submitted together with the quotation. Quotations that do not include the Certification shall not be accepted/considered for award. Prospective bidder/s should have at least two Security Expert. Training certificates of the certified security professionals should be attached to the quotation. All product updates/upgrades are to be to be performed by certified security professionals. A supplier must have the capacity to escalate product technical issues directly to the manufacturer. Any costs necessary for the supplier to fulfil it obliges in the supply, delivery, installation, and commissioning of the firewall shall be deemed included in the financial proposal. Any cost incurred in the fulfilment of the obligations that were not included in the financial proposal shall be shouldered by the supplier with the lowest complying quotation.

4. Mandatory Compliance Requirements (the following to be submitted with the quotation)

a) Proof of registration on the Treasury Central Supplier Database.
b) Valid tax clearance certificate / pin.
c) Proof of company registration, where applicable.
d) Valid BBBEE certificate by a SANAS accredited agency/company or sworn affidavit.
e) Bank letter confirming the company banking details.
f) Supplier declaration of interest (attached hereinto)

Note: Failure to comply with the above mandatory requirements will lead to disqualification.

DECLARATION OF INTEREST

1. Any legal person, including persons employed by the state[1], or persons having a kinship with persons employed by the state, including a blood relationship, may make an offer or offers in terms of this invitation to bid (includes a price quotation, advertised competitive bid, limited bid or proposal). In view of possible allegations of favouritism, should the resulting bid, or part thereof, be awarded to persons employed by the state, or to persons connected with or related to them, it is required that the bidder or his/her authorised representative declare his/her position in relation to the evaluating/adjudicating authority where-

   - the bidder is employed by the state; and/or

   - the legal person on whose behalf the bidding document is signed, has a relationship with persons/a person who are/is involved in the evaluation and or adjudication of the bid(s), or where it is known that such a relationship exists between the person or persons for or on whose behalf the declarant acts and persons who are involved with the evaluation and or adjudication of the bid.

2. **In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.**

2.1 Full Name of bidder or his or her representative: …….

2.2 Identity Number: ……

2.3 Position occupied in the Company (director, trustee, shareholder[2]): ……..

2.4 Company Registration Number: ……..……

2.5 Tax Reference Number: ……

2.6 VAT Registration Number: ……....

2.6.1 The names of all directors / trustees / shareholders / members, their individual identity numbers, tax reference numbers and, if applicable, employee / persal numbers must be indicated in paragraph 3 below.

[1]"State" means –

(a) any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No. 1 of 1999);
(b) any municipality or municipal entity;
(c) provincial legislature;
(d) national Assembly or the national Council of provinces; or
(e) Parliament.

[2]"Shareholder" means a person who owns shares in the company and is actively involved in the management of the enterprise or business and exercises control over the enterprise.

2.7	Are you or any person connected with the bidder presently employed by the state?	**YES / NO**
2.7.1	If so, furnish the following particulars:	
	Name of person / director / trustee / shareholder/ member: ……..……	
	Name of state institution at which you or the person connected to the bidder is employed : ……	
	Position occupied in the state institution: ……	
	Any other particulars: …… …… ……	
2.7.2	If you are presently employed by the state, did you obtain the appropriate authority to undertake remunerative work outside employment in the public sector?	**YES / NO**
2.7.2.1	If yes, did you attached proof of such authority to the bid document?	**YES / NO**
	<u>(Note: Failure to submit proof of such authority, where applicable, may result in the disqualification of the bid.</u>	
2.7.2.2	If no, furnish reasons for non-submission of such proof:	
	…… …… ……	

2.8 Did you or your spouse, or any of the company's directors / trustees / shareholders / members or their spouses conduct business with the state in the previous twelve months? **YES / NO**

2.8.1 If so, furnish particulars:
……..
……..
……...

2.9 Do you, or any person connected with the bidder, have any relationship (family, friend, other) with a person employed by the state and who may be involved with the evaluation and or adjudication of this bid? **YES / NO**

2.9.1 If so, furnish particulars.
……...
……..…
……

2.10 Are you, or any person connected with the bidder, aware of any relationship (family, friend, other) between any other bidder and any person employed by the state who may be involved with the evaluation and or adjudication of this bid? **YES/NO**

2.10.1 If so, furnish particulars**.**
……
……
……

2.11 Do you or any of the directors / trustees / shareholders / members of the company have any interest in any other related companies whether or not they are bidding for this contract? **YES/NO**

2.11.1 If so, furnish particulars:
……
……
……

3 Full details of directors / trustees / members / shareholders.

Full Name	Identity Number	Personal Tax Reference Number	State Employee Number / Persal Number

4 DECLARATION

I, THE UNDERSIGNED (NAME)……

CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 2 and 3 ABOVE IS CORRECT. I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 23 OF THE GENERAL CONDITIONS OF CONTRACT SHOULD THIS DECLARATION PROVE TO BE FALSE.

…….. ……

Signature Date

…… ……

Position Name of bidder