SOUTH AFRICA

Electoral Commission

Auction 0010559261

Next Generation Firewall Appliances

IMPORTANT NOTICE

Failure to comply with the completion of the auction conditions and the required information or submission of the required stipulated documents indicated below shall invalidate a bid.

1 Introduction

1.1 The Electoral Commission (IEC) is seeking to procure 2 pairs of Next Generation Firewall appliances with five (5) years support and maintenance for both its Production and Disaster Recovery sites.

1.2 The firewalls must be delivered with a centralised management control centre for configuring, managing, and monitoring the firewalls, allowing administrators to set security policies, manage firewalls and devices, track events, install updates, and ensure compliance.

1.3 The firewalls must be delivered with assurance tools that have the capability to identify/discover firewall vulnerabilities, security misconfigurations, non-optimised firewall rules/configurations, provide automated mitigations of security gaps, discover and identify firewall rules with no associated traffic/usage (or redundant firewall rules); as well as allow the Electoral Commission to demonstrate compliance to standards/regulations such as NIST, OWASP, POPIA etc.

1.4 Bidders must place a bid on the Votaquotes (e-Procurement) system and then provide all the required documentation before the due dates as specified in this document and on the Votaquotes web site. In order to participate in this auction, bidders must be registered and approved on Votaquotes (e-Procurement).

2 Background Information

2.1 The Electoral Commission has invested extensively in ICT technologies, which provide a platform to effectively support and enable its business processes and to meet its goal of providing a free and fair election process in an open and transparent environment. The Electoral Commission's ICT Department intends to continue running a highly efficient, secure and stable ICT environment making full use of industry standards, best practices and disciplines based upon stable, secure and reliable technologies.

2.2 The current environment consists of a pair of physical enterprise-grade firewalls deployed in high-availability (HA) mode in the production and disaster recovery datacentres, supported by a virtualised management server and an event logging/monitoring server for

centralised administration, reporting, and threat visibility.

2.3 The proposed technology solution should maintain a similar architecture, namely, a pair of physical firewalls configured for HA operation, centralised management, and comprehensive event/log management while meeting or exceeding the technical, performance, and security requirements outlined in this auction.

2.4 The Electoral Commission wants to use different firewall brands for perimeter and internal firewalls to take advantage of defence in depth principle and to mitigate single-vendor risks and single point of failure, as a result the proposed technology cannot be Fortinet FortiGate appliances.

3 Technical Specifications

3.1 The technical specification for the required solution is as specified below. It must be noted that the technical specifications below are the minimum requirements; the only exception that may be accepted will be in case where the bidder's specification is better. Anything below specification will be disqualified.

3.2 The proposed solution must consist of enterprise-grade physical Next-Generation Firewall (NGFW) appliances, deployed in a high-availability (HA) configuration across the production and disaster recovery data centres. The solution must support resilient operation with automatic failover and minimal service disruption.

3.3 The physical firewall appliances must be supported by a virtualised management server and a centralised event logging/monitoring server for centralised administration and policy management, event logging and monitoring, reporting and analytics, and threat visibility across all managed firewall appliances.

3.4 The physical firewall appliances include an integrated or companion security assurance and policy analysis capability that has the capability to identify and report in firewall vulnerabilities and security misconfigurations, detect non-optimised, redundant and unused or shadowed firewall rules/configurations, provide automated mitigations of security gaps, discover and identify firewall rules with no associated traffic/usage (or redundant firewall rules); provide automated or guided recommendations to remediate

identified security gaps, as well as support compliance validation against recognised standards and regulations including but not limited to NIST, OWASP, POPIA.

3.5 The solution must be supplied with 5 years' Original Equipment Manufacturers (OEM) backed support and maintenance that includes Hardware and software support; firmware and security updates, 24x7x365 support availability, with maximum of 4 hours Mean Time to Resolve for critical incidents; advanced hardware replacement, including swapping of faulty equipment and security licensing and entitlement for the contract period.

3.6 The solution shall be supplied with installation and configuration services. The bidder will be responsible for the end-to-end deployment of the proposed firewall solution, including physical installation and cabling, high availability (HA) configuration across the two datacentres, interconnectivity (heartbeat, sync, etc.). The solution shall also be supplied with rules migration services where applicable. The bidder is expected to assess and migrate existing security policies, rule sets, VPN configurations, objects, and NAT rules to the new platform, ensuring functional equivalence, optimisation and cleanup of legacy rules, validation and user acceptance testing (UAT) of migrated policies. Depending on the winning solution, this item may be partly activated or not be activated at all.

3.7 The solution must integrate with existing Electoral Commission's networking infrastructure including switches, routers, Directory and Authentication Services (Active Directory), Security Incident and Events Management (FortiSIEM), ManageEngine Service Desk ITSM, and Time Synchrionization services (Network Time Protocol (NTP))

3.8 The solution must support horizontal and/or vertical scalability to accommodate future growth including expansion of throughput, session capacity and security services without requiring a complete platform replacement.

3.9 The proposed solution must include transparent and clearly defined licensing for: Core firewall functionality, Security services and subscriptions and Management and logging capabilities

3.10 The solution shall be supplied with knowledge transfer and training of Electoral Commission staff covering at a minimum the following: management interface and monitoring, logging/reporting procedures, troubleshooting, update and patch procedures. Depending on the winning solution, this item may not be activated.

3.11 The successful bidder must produce and deliver system documentation including final design document, configuration guides, change control logs and As-built reports

3.12 The solution must meet or exceed the minimum compliance requirements below:

	Solution Component	Category	Requirement	Requirement Details
1.	Firewall	Hardware	Network Interfaces	The NGFW appliance must support high-speed interfaces capable of 10Gbps, 25Gbps, 40Gbps and/or 100Gbps connectivity.
2.	Firewall	Hardware	Fiber Ports	Minimum of four (4) high-speed fiber ports per firewall appliance.
3.	Firewall	Hardware	Interface Types	Each NGFW appliance must support a combination of copper and fiber interfaces, including but not limited to RJ-45, SFP+, QSFP+, or equivalent modular interfaces.
4.	Firewall	Hardware	Power Redundancy	Each NGFW appliance must be equipped with at least two (2) redundant hot-swappable power supplies.
5.	Firewall	Hardware	Processing Architecture	The NGFW must utilise a multi-core processing architecture capable of separating management, control plane, and traffic inspection functions to improve performance and reduce latency.
6.	Firewall	Security & Authentication	Authentication Integration	The solution must integrate with enterprise authentication systems including LDAP, Active Directory, RADIUS, Kerberos, and cloud-based identity providers.
7.	Firewall	Performance	Firewall Throughput	The solution must provide high capacity stateful firewall throughput suitable for large enterprise and data centre environments. Performance figures must be provided under real-world conditions.
8.	Firewall	Performance	NGFW Throughput	The solution must provide high NGFW throughput with security services enabled (e.g. IPS, application control, malware protection).
9.	Firewall	Performance	Threat Prevention Throughput	The solution must sustain threat prevention throughput with advanced security services enabled, including IPS, malware protection, and application inspection.
10.	Firewall	Performance	IPSec VPN Throughput	The solution must support high-capacity IPSec VPN throughput

	Solution Component	Category	Requirement	Requirement Details
				suitable for large-scale site-to-site and remote access deployments.
11.	Firewall	Performance	Concurrent Sessions	The NGFW must support a high number of concurrent sessions suitable for enterprise-scale environments.
12.	Firewall	Performance	New Session Rate	The solution must support a high new-session establishment rate without degradation of performance.
13.	Firewall	High Availability	HA Modes	The solution must support both Active-Active and Active-Passive high-availability modes, including clustering where applicable.
14.	Firewall	VPN	VPN Capabilities	The solution must support IPSec and SSL VPNs, hub-and-spoke and full-mesh topologies, strong cryptographic algorithms, and NAT traversal.
15.	Firewall	Network Segmentation	Segmentation	The solution must support static and dynamic network segmentation using zones, VLANs, subnets, user identity, device posture, and application context.
16.	Firewall	NAT	Network Address Translation	The solution must support source and destination NAT, static NAT, dynamic NAT, and policy-based NAT.
17.	Firewall	Traffic Management	Traffic Prioritisation	The solution must support traffic prioritisation and quality-of-service enforcement based on users, applications, zones, and policies.
18.	Firewall	Network Access	Access Control	The solution must control network access based on IP addresses, FQDNs, protocols, ports, users, and applications.
19.	Firewall	Advanced Security	Zero-Day Protection	The solution must provide protection against known and unknown threats using behavioural analysis, anomaly detection, and machine-learning-assisted techniques.
20.	Firewall	Advanced Security	Behavioural Analysis	The solution must support behavioural-based threat detection to identify anomalous activity and evolving attack patterns.
21.	Firewall	Logging & Analytics	Log Querying	The solution must provide advanced log filtering, correlation, and analytics capabilities. Natural-language querying may be proposed as a value-added feature.

	Solution Component	Category	Requirement	Requirement Details
22.	Firewall	Application Control	Application Identification	The solution must provide application identification and control, allowing granular policy enforcement per application and application category.
23.	Firewall	Intrusion Prevention	Integrated IPS	The solution must include an integrated IPS using signature-based, anomaly-based, and protocol-analysis techniques.
24.	Firewall	Malware Protection	Anti-Bot	The solution must provide integrated anti-bot and command-and-control traffic detection.
25.	Firewall	Malware Protection	Anti-Virus	The solution must include integrated antivirus and malware inspection across supported protocols including HTTP, HTTPS, FTP, SMTP, POP3, and IMAP.
26.	Firewall	Messaging Security	Anti-Spam	The solution must support anti-spam capabilities for applicable traffic types.
27.	Firewall	DNS Security	DNS Protection	The solution must provide integrated DNS security to detect malicious domains and prevent DNS-based attacks.
28.	Firewall	Inspection	Deep Packet Inspection	The solution must inspect packet payloads to detect protocol violations, malware, and policy violations.
29.	Firewall	Advanced Threat	Threat Emulation	The solution must support sandbox-based or equivalent techniques for analysing unknown files and payloads.
30.	Firewall	Advanced Threat	Threat Extraction	The solution must support safe content extraction or equivalent techniques to prevent delivery of malicious content.
31.	Firewall	Phishing Protection	Phishing Detection	The solution must provide phishing detection and prevention capabilities across supported protocols.
32.	Firewall	DDoS Protection	DDoS Mitigation	The solution must include mechanisms to detect and mitigate volumetric and application-layer DDoS attacks.
33.	Firewall	Web Security	Web Filtering	The solution must provide web filtering and content categorisation with configurable policy enforcement.
34.	Firewall	Traffic Inspection	HTTPS Inspection	The solution must support HTTPS traffic inspection subject to policy and regulatory requirements.
35.	Firewall	Proxy	Proxy Capability	The solution may support explicit or transparent proxy functionality.

	Solution Component	Category	Requirement	Requirement Details
36.	Firewall	Encryption	SSL/TLS Inspection	The solution must support SSL/TLS inspection including TLS 1.2 and TLS 1.3 for visibility into encrypted traffic.
37.	Firewall	Authentication	Multi-Factor Authentication	The solution must support MFA integration for administrative and VPN access, including integration with email, SMS, or authenticator applications.
38.	Firewall	Routing	Routing Protocols	The solution must support dynamic and static routing protocols including OSPF, BGP, and policy-based routing.
39.	Management	Administration	Centralised Management	The solution must include a centralised management interface with role-based access control.
40.	Management	Operations	Centralised Control	The management platform must allow configuration, monitoring, policy management, firmware updates, and compliance enforcement across all firewalls.
41.	Management	Reporting	Log Retention	The solution must support historical log retention for a minimum period as defined by organisational policy (minimum 12 months).
42.	Management	Reporting	Reporting Tools	The solution must provide customizable reporting including security events, compliance reports, and drill-down analytics.
43.	Compliance & Assurance	Best Practices	Configuration Validation	The solution must support real-time best-practice and configuration compliance checks.
44.	Compliance & Assurance	Risk Identification	Policy & Config Analysis	The solution must identify vulnerabilities, misconfigurations, and non-optimised firewall rules.
45.	Compliance & Assurance	Remediation	Mitigation Guidance	The solution must provide automated or guided remediation recommendations for identified risks.
46.	Compliance & Assurance	Policy Optimisation	Rule Usage Analysis	The solution must identify unused, redundant, or shadowed firewall rules.
47.	Compliance & Assurance	Regulatory Compliance	Standards Alignment	The solution must support compliance validation against standards such as NIST, OWASP, and POPIA.
48.	Support & Maintenance	Support	OEM Support	The solution must include OEM-backed enterprise support services accessible via web, telephone, and email.

	Solution Component	Category	Requirement	Requirement Details
49.	Support & Maintenance	SLA	Incident Response	The solution must include 24×7×365 support with defined response times for critical and non-critical incidents.
50.	Support & Maintenance	Software	Firmware Updates	The solution must include access to firmware, software, and security updates.
51.	Support & Maintenance	Hardware	Hardware Replacement	The solution must include advanced hardware replacement for faulty components.
52.	Support & Maintenance	Asset Management	OEM Portal	The solution must include access to an OEM asset and license management portal.

4 Planning Assumptions

The Electoral Commission has made the following assumptions:

4.1 The Electoral Commission will provide technical resources for the installation and configuration of the supplied firewalls

4.2 Wherever the need arises the successful bidder shall do initial equipment configuration of operating systems, patches and environmental specific requirements.

4.3 The delivery of the of the solution required must be completed within the days as stipulated in the delivery and implementation schedule below.

4.4 The bidder's change control management process must be flexible enough to align to the Electoral Commission's change management processes.

4.5 The recommended service provider shall provide all relevant details needed to ensure successful operations capability within the organization.

5 General Auction Conditions

The following standard bid conditions must be adhered to and complied with; failing which the bid will be disqualified.

5.1 All bids must be placed online on eProcurement website https://votaquotes.elections.org.za.

5.2 Bidders must complete and submit Appendix A: Technical Bid Response to demonstrate

compliance with the required technical specification.

5.3 The bidder must provide at least three (3) contactable reference of past services of a similar nature (Next Generation firewalls) that the bidder provided or was involved in. Reference details must include the following: customer name, contact person, contact details (telephone, email, physical address) and Fortinet products delivered, the number of units delivered and the timeframe. Bidders are to use *Appendix C: Guideline Reference Table* as guideline.

5.4 The bidder must be authorized to sell and install the solution supplied.

5.5 An OEM letter of proof of the reseller agreement/authorization must accompany the written documentation for this bid.

5.6 Should the reseller authorization be from a distributor, then a proof of authorization authorizing the distributor to resell and/or to authorize others by the OEM must be submitted together with the reseller authorization from the distributor.

5.7 The bidder must include a formal proof of OEM statement of licensing stating associated services terms and conditions.

5.8 Bidder must have at least three (3) years' experience in providing the solution required. A company profile or details of company experience on a letterhead must be submitted as part of the bid's response.

5.9 The bidder must also include a CV of a resource that is qualified to perform installations on the proposed solution. The qualifications of the resource must also be attached to the CV.

5.10 The bidder must include a project plan for the implementation of the solution.

5.11 Bidders must provide solutions that are based on a standard existing product in the market and not products specifically designed and/or cloned for this bid. The Electoral Commission may require market penetration indicators and references. The bidder must provide a data sheet for the proposed product.

5.12 Bidders must adhere to the delivery schedule in **Section 10**

6 Quality Control

The following quality control conditions must be adhered to and complied with, failing which the bid may be disqualified.

6.1 The bidder takes responsibility for the completeness and quality of their bid submission.

6.2 The Electoral Commission may also call on bidders to make presentations in order for the Electoral Commission to ensure full compliance with all its requirements and as part of the bid evaluation process prior to the conclusion of the adjudication of the bid. Any such request for presentations shall only be for clarification purposes in support of mandatory requirements that must be adhered to as part of the written submission requirements of this bid. Failure to submit mandatory requirements shall not be rectified by the call for presentations.

6.3 Any restrictions or conditions associated with any elements of the service offering/s must be detailed. The Electoral Commission reserves the right to reject conditions which are considered unfavourable to its business or unacceptable.

6.4 The bidder must provide the associated support and maintenance for the duration of the contract. The support and maintenance must include all services as per product code.

6.5 The submission of a bid implies acceptance of the terms specified in the provisions laid down in the specifications, the procurement regulations and additional documents where applicable.

6.6 Bidders are expected to examine carefully and respect all instructions and standard formats contained in these specifications

6.7 A bid that does not contain all the required information and documentation will be disqualified.

6.8 Although the Electoral Commission will only deal with the principal service provider, if a bidder plans to sub-contract any of the services in this bid, they are required to attach copies of sub-contracting agreements in their bid response documentation.

6.9 Bidders are advised to refer to this Appendix D: Bid Evaluation Criteria to ensure that they have addressed all critical bid requirements which will be used to assess the bids

6.10 Notwithstanding any shortcomings in these specifications, service providers must ensure that the proposed solution will form a workable and complete solution.

6.11 The Electoral Commission will issue a formal purchase order to the successful bidder

before any services can be delivered.

6.12 Awarding of the bid to the successful bidder will be subject to the Electoral Commission's due diligence audit requirements, where applicable.

6.13 The Electoral Commission reserves the right and discretion to amend the quantities or cancel or not award this bid based on any reason including operational or financial requirements.

6.14 Awarding the bid to a successful bidder will be subject to the bidder entering into a service level agreement (SLA) with the IEC that will formalize and regulate the final deliverables and associated processes and procedures.

6.15 There will be monthly SLA meetings with the successful bidder for the duration of the contract to monitor and manage the SLA.

7 Pricing Requirements

Completion of the detailed pricing schedule by responding to each item is compulsory. Failure to complete and submit this detailed pricing schedule as part of the bid submission shall lead to disqualification.

7.1 Total bid price must be submitted online on the eProcurement (Votaquotes) portal.

7.2 The total bid price on the Appendix B: Pricing Schedule must be the same as the total bid price submitted online.

7.3 All costs associated with the hardware, software licensing, and associated support must be included in the total bid price. The total bid price must be inclusive of all factors which may contribute the cost of fulfilling the bid, factors such as:

a) Hardware costs
b) Installation, Customization and Migration Costs
c) Software license subscription including OEM-backed support and maintenance costs for 60 months.
d) Support and maintenance will be paid annually in advance and not for the 5 years at once.
e) Delivery costs to the Electoral Commission's national office in Centurion, Gauteng, South Africa.

7.4 Bid prices must be VAT inclusive and must be firm for a period of 180 days.

7.5 The Electoral Commission reserves the right to adjust costs by excluding some cost factors.

7.6 All costs associated with the solution must be captured on the pricing schedule - no additional costs will be entertained.

7.7 The solution must be a complete solution.

8 Adjudication and Award of Contract

8.1 Bidders are advised to refer to the Appendix D: Bid Evaluation Criteria to ensure that they have addressed all critical bid requirements.

8.2 The bid will be awarded to a bidder whose solution successfully conforms to specifications and is able to deliver the services, and in terms of the provisions of the Preferential Procurement Policy Framework Act, 2000 and specifically the Preferential Procurement Regulations, 2022.

8.3 The Electoral Commission will issue a formal order before any services can be delivered

8.4 It should be noted that the Electoral Commission seeks to gain the best solution technically and financially.

8.5 Awarding the bid to a successful bidder is subject to the bidder entering into a service level agreement (SLA) with the Electoral Commission that will formalize and regulate the final deliverables and associated processes and procedures.

9 Supplier Performance

9.1 Upon notification of the Electoral Commission's intention to award a contract, the successful bidder may be required to enter into a service level agreement (SLA/contract) with the Electoral Commission.

9.2 The purpose of the SLA (if applicable other than what the Electoral Commission's standard purchase orders provide for) is to fix performance criteria within the key requirements of this request for quotation, namely quantity, quality and delivery.

9.3 The SLA may contain elements such as supplier progress milestones, delivery

schedules, quality checkpoints and invoicing procedures.

9.4 The Electoral Commission reserves the right to reject any services delivered not conforming to the above.

9.5 Where previously-agreed delivery schedules are not met by a supplier, the Electoral Commission shall have the right to appoint an alternative supplier to make good the shortfall in supply. Any additional costs incurred by the Electoral Commission in obtaining such corrective services or products from another source will be for the account of the defaulting supplier.

10 Delivery and Implementation Timeframe

10.1 The successful bidder will be need to complete implementation of the solution within three (3) months of receiving a formal Purchase Order from the Electoral Commission

10.2 Delivery will be at the Electoral Commission's National Office in Centurion, Gauteng, South Africa. The DR site is also in Centurion area.

11 Written Submissions

11.1 All submissions must be received before the closing date and time for submissions as stipulated on the eProcurement website https://votaquotes.elections.org.za

11.2 Submissions received after the final date and time will lead to bids being disqualified and not considered.

11.3 All bids must be placed online on eProcurement website https://votaquotes.elections.org.za.

Supporting documentation can be submitted in any or both of the following options:

- Upload to the auction site.
- Place in the Electoral Commission tender box situated in the foyer of the Electoral Commission National Office in Centurion at the following address before the closing date and time of this auction

  Election House
  Riverside Office Park,

1303 Heuwel Avenue,
Centurion,
0157

Note: Clearly mark your submission: For the attention of Procurement and Asset Management Department – Auction 0010559261

11.4 Failure to submit all of the required documentation before the closing date and time shall invalidate the bid. It remains the responsibility of the bidder to confirm receipt of the required documentation with the Electoral Commission Procurement and Asset Management Department.

11.5 The following supporting documents must be submitted as part of the written submissions. Failure to submit these will lead to the bid being disqualified:

11.5.1 Completed technical specifications in accordance with the requirements in Appendix A: Technical Bid Response Sheet to demonstrate compliance with the bid specification as per 5.2

11.5.2 Three (3) relevant contactable References, as per Appendix C: Guideline Reference Table **as per 5.3**

11.5.3 Completed pricing schedule in Appendix B: Pricing Schedule **as per 7.2.**

11.5.4 A letter of proof of the reseller agreement either from the OEM or an authorized distributor; (i.e. if the reseller is authorized by a distributor). If the reseller agreement is from a distributor, then proof from the OEM authorizing the distributor needs to be included as per 5.4, 5.5 and 5.6

11.5.5 A statement of service, describing the service and support that is covered under the license renewal process including

the roles of the bidder and the Original Equipment Manufacturer (OEM) as per 5.7

11.5.6 Company Profile showing relevant experience as per 5.8

11.5.7 CV of the resource that will be responsible for the installation as per 5.9

11.5.8 Project Implementation Plan as per 5.10

11.5.9 Data Sheet(s) of the proposed solution as per 5.11

12 Briefing Session or Enquiries

12.1 There will be no briefing session for this requirement.

13 Enquiries

All enquiries regarding this bid must be submitted exclusively through the VotaQuotes platform. This requirement supports the principles of fairness, openness, and transparency in the procurement process.
All questions and the official responses will be published on the public VotaQuotes website (www.votaquotes.elections.org.za) where the bid is advertised.
Bidders are responsible for regularly monitoring the platform for any updates, clarifications, or additional information published during the bidding period.
No telephonic, email, or other forms of communication regarding bid enquiries will be accepted or responded to.
An enquiry cut-off date applies to all bids. The final date and time for submitting enquiries is published on the VotaQuotes platform under the specific bid listing

14 Closing Date

The closing date and time of this auction is specified on the eProcurement (Votaquotes) website in accordance the bidding requirements. The closing date and time is determined by the clock on the Electoral Commission’s servers and is not negotiable.

Bidders must also take note supporting documentation must be delivered before closing date and time of the submission of supporting documentation.

15 Appendix A: Technical Bid Response Sheet

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet.** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
1.	Firewall	Firewall Architecture	4 x Enterprise Grade Firewalls	The proposed solution consists of enterprise-grade physical Next-Generation Firewall (NGFW) appliances, deployed in a high-availability (HA) configuration across the production and disaster recovery data centres.	3.2			
2.				The solution supports resilient operation with automatic failover and minimal service disruption	3.2			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
3.	Proposed Solution	Operational Compatibility	Integration	The solution integrates with existing Electoral Commission's networking infrastructure including switches, routers, Directory and Authentication Services (Active Directory), Security Incident and Events Management (FortiSIEM), ManageEngine Service Desk ITSM, and Time Synchrionization services (Network Time Protocol (NTP))	3.7			
4.	Firewall	Hardware	Network Interfaces	The NGFW appliance must support high-speed interfaces capable of	3.12			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet.** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
				10Gbps, 25Gbps, 40Gbps and/or 100Gbps connectivity.				
5.	Firewall	Hardware	Fiber Ports	Minimum of four (4) high-speed fiber ports per firewall appliance.	3.12			
6.	Firewall	Hardware	Interface Types	Each NGFW appliance must support a combination of copper and fiber interfaces, including but not limited to RJ-45, SFP+, QSFP+, or equivalent modular interfaces.	3.12			
7.	Firewall	Hardware	Power Redundancy	Each NGFW appliance must be equipped with at least two (2)	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
				redundant hot-swappable power supplies.				
8.	Firewall	Hardware	Processing Architecture	The NGFW must utilise a multi-core processing architecture capable of separating management, control plane, and traffic inspection functions to improve performance and reduce latency.	3.12			
9.	Firewall	Security & Authentication	Authentication Integration	The solution must integrate with enterprise authentication systems including LDAP, Active Directory,	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
				RADIUS, Kerberos, and cloud-based identity providers.				
10.	Firewall	Performance	Firewall Throughput	The solution must provide high capacity stateful firewall throughput suitable for large enterprise and data centre environments. Performance figures must be provided under real-world conditions.	3.12			
11.	Firewall	Performance	NGFW Throughput	The solution must provide high NGFW throughput with security services enabled (e.g. IPS, application control, malware protection).	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
12.	Firewall	Performance	Threat Prevention Throughput	The solution must sustain threat prevention throughput with advanced security services enabled, including IPS, malware protection, and application inspection.	3.12			
13.	Firewall	Performance	IPSec VPN Throughput	The solution must support high-capacity IPSec VPN throughput suitable for large-scale site-to-site and remote access deployments.	3.12			
14.	Firewall	Performance	Concurrent Sessions	The NGFW must support a high number of concurrent sessions suitable for enterprise-scale environments.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
15.	Firewall	Performance	New Session Rate	The solution must support a high new-session establishment rate without degradation of performance.	3.12			
16.	Firewall	High Availability	HA Modes	The solution must support both Active-Active and Active-Passive high-availability modes, including clustering where applicable.	3.12			
17.	Firewall	VPN	VPN Capabilities	The solution must support IPSec and SSL VPNs, hub-and-spoke and full-mesh topologies, strong cryptographic algorithms, and NAT traversal.	3.12			

Technical Bid Response Sheet

Completion of this technical response sheet by the bidder is compulsory.
Bidder must respond to each and every item in the response sheet.
Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.

	Solution Component	Category	Requirement	Compliance Minimum Requirement	Reference	Bidder must indicate whichever is applicable		Bidder must substantiate their selection in the space provided or refer to a section of their proposal
						Yes	No	
18.	Firewall	Network Segmentation	Segmentation	The solution must support static and dynamic network segmentation using zones, VLANs, subnets, user identity, device posture, and application context.	3.12			
19.	Firewall	NAT	Network Address Translation	The solution must support source and destination NAT, static NAT, dynamic NAT, and policy-based NAT.	3.12			
20.	Firewall	Traffic Management	Traffic Prioritisation	The solution must support traffic prioritisation and quality-of-service enforcement based on users, applications, zones, and policies.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
21.	Firewall	Network Access	Access Control	The solution must control network access based on IP addresses, FQDNs, protocols, ports, users, and applications.	3.12			
22.	Firewall	Advanced Security	Zero-Day Protection	The solution must provide protection against known and unknown threats using behavioural analysis, anomaly detection, and machine-learning-assisted techniques.	3.12			
23.	Firewall	Advanced Security	Behavioural Analysis	The solution must support behavioural-based threat detection to identify	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
				anomalous activity and evolving attack patterns.				
24.	Firewall	Logging & Analytics	Log Querying	The solution must provide advanced log filtering, correlation, and analytics capabilities. Natural-language querying may be proposed as a value-added feature.	3.12			
25.	Firewall	Application Control	Application Identification	The solution must provide application identification and control, allowing granular policy enforcement per application and application category.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
26.	Firewall	Intrusion Prevention	Integrated IPS	The solution must include an integrated IPS using signature-based, anomaly-based, and protocol-analysis techniques.	3.12			
27.	Firewall	Malware Protection	Anti-Bot	The solution must provide integrated anti-bot and command-and-control traffic detection.	3.12			
28.	Firewall	Malware Protection	Anti-Virus	The solution must include integrated antivirus and malware inspection across supported protocols including HTTP, HTTPS, FTP, SMTP, POP3, and IMAP.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
29.	Firewall	Messaging Security	Anti-Spam	The solution must support anti-spam capabilities for applicable traffic types.	3.12			
30.	Firewall	DNS Security	DNS Protection	The solution must provide integrated DNS security to detect malicious domains and prevent DNS-based attacks.	3.12			
31.	Firewall	Inspection	Deep Packet Inspection	The solution must inspect packet payloads to detect protocol violations, malware, and policy violations.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
32.	Firewall	Advanced Threat	Threat Emulation	The solution must support sandbox-based or equivalent techniques for analysing unknown files and payloads.	3.12			
33.	Firewall	Advanced Threat	Threat Extraction	The solution must support safe content extraction or equivalent techniques to prevent delivery of malicious content.	3.12			
34.	Firewall	Phishing Protection	Phishing Detection	The solution must provide phishing detection and prevention capabilities across supported protocols.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
35.	Firewall	DDoS Protection	DDoS Mitigation	The solution must include mechanisms to detect and mitigate volumetric and application-layer DDoS attacks.	3.12			
36.	Firewall	Web Security	Web Filtering	The solution must provide web filtering and content categorisation with configurable policy enforcement.	3.12			
37.	Firewall	Traffic Inspection	HTTPS Inspection	The solution must support HTTPS traffic inspection subject to policy and regulatory requirements.	3.12			
38.	Firewall	Proxy	Proxy Capability	The solution may support explicit or transparent proxy functionality.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
39.	Firewall	Encryption	SSL/TLS Inspection	The solution must support SSL/TLS inspection including TLS 1.2 and TLS 1.3 for visibility into encrypted traffic.	3.12			
40.	Firewall	Authentication	Multi-Factor Authentication	The solution must support MFA integration for administrative and VPN access, including integration with email, SMS, or authenticator applications.	3.12			
41.	Firewall	Routing	Routing Protocols	The solution must support dynamic and static routing protocols including OSPF, BGP, and policy-based routing.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
42.	Management	Administration	Centralised Management	The solution must include a centralised management interface with role-based access control.	3.12			
43.	Management	Operations	Centralised Control	The management platform must allow configuration, monitoring, policy management, firmware updates, and compliance enforcement across all firewalls.	3.12			
44.	Management	Reporting	Log Retention	The solution must support historical log retention for a minimum period as defined by organisational policy (minimum 12 months).	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
45.	Management	Reporting	Reporting Tools	The solution must provide customizable reporting including security events, compliance reports, and drill-down analytics.	3.12			
46.	Compliance & Assurance	Best Practices	Configuration Validation	The solution must support real-time best-practice and configuration compliance checks.	3.12			
47.	Compliance & Assurance	Risk Identification	Policy & Config Analysis	The solution must identify vulnerabilities, misconfigurations, and non-optimised firewall rules.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
48.	Compliance & Assurance	Remediation	Mitigation Guidance	The solution must provide automated or guided remediation recommendations for identified risks.	3.12			
49.	Compliance & Assurance	Policy Optimisation	Rule Usage Analysis	The solution must identify unused, redundant, or shadowed firewall rules.	3.12			
50.	Compliance & Assurance	Regulatory Compliance	Standards Alignment	The solution must support compliance validation against standards such as NIST, OWASP, and POPIA.	3.12			
51.	Support & Maintenance	Support	OEM Support	The solution must include OEM-backed enterprise support services	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
				accessible via web, telephone, and email.				
52.	Support & Maintenance	SLA	Incident Response	The solution must include 24×7×365 support with defined response times for critical and non-critical incidents.	3.12			
53.	Support & Maintenance	Software	Firmware Updates	The solution must include access to firmware, software, and security updates.	3.12			
54.	Support & Maintenance	Hardware	Hardware Replacement	The solution must include advanced hardware replacement for faulty components.	3.12			

Technical Bid Response Sheet Completion of this technical response sheet by the bidder is compulsory. Bidder must respond to each and every item in the response sheet. Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder must indicate whichever is applicable**		**Bidder must substantiate their selection in the space provided or refer to a section of their proposal**
						Yes	**No**	
55.	Support & Maintenance	Asset Management	OEM Portal	The solution must include access to an OEM asset and license management portal.	3.12			

16 Appendix B: PRICING SCHEDULE

PRICING SCHEDULE

Completion of this Price Breakdown response sheet by the bidder is compulsory.

Bidder must respond to each and every item in the response sheet.

Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.

	Product Code	Description	Quantity	Unit / Annual Cost	Total Cost
1.		Next Generation Firewalls and Software	4	R…….	R……
2.		Management Appliance / Solution	1	R…….	R……
3.		Assurance / Compliance Solution	1	R…….	R……
4.		Annual Support and Maintenance	5	R…….	R……
*TOTAL BID PRICE inclusive of VAT					R……

***The total bid price is the bid price that must be placed on eProcurement (auction). No any other additional costs will be accepted for bid evaluation and adjudication purposes.**

16.1 Appendix B1 – Optional Installation, Customization and Migration Costs

PRICING SCHEDULE – Implementation Costs **Completion of this Pricing Schedule response sheet by the bidder is compulsory. .**					
	Product Code	**Description**	**Quantity**	**Unit / Annual Cost**	**Total Cost**
1.		Installation, Customization and Migration Costs	4	R……	R……
Total Implementation Costs					R……

17 Appendix C: Guideline Reference Table

Reference #1

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Product	
	Services Provided	
Service Value	Budget (estimate)	
	Number of hardware devices supplied	
	When was this done?	

Reference #2

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Product	
	Services Provided	
Service Value	Budget (estimate)	
	Number of devices supplied	
	When was this done?	

Reference #3

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Product	
	Services Provided	
Service Value	Budget (estimate)	
	Number of devices supplied	
	When was this done?	

18 Appendix D: Bid Evaluation Criteria

Bidders are advised to refer to this section to ensure that they have addressed all critical bid requirements which will be used for the assessment of the bids. Bidders are NOT expected to complete and submit this section.

18.1 Stage 1: Assessment of Bidder's Disclosure

All bids received will be evaluated and assessed in respect of the mandatory information provided in the Bidder's Disclosure (SBD4) as well as the register for restricted suppliers and tender defaulters.

Any potential issues that may arise or transgressions that may identified will be pursued in accordance with statutory obligations and requirements.

In this regard, the following must be noted:

18.1.1 The Electoral Commission must, as part of its supply chain management (SCM) processes, identify and manage all potential conflicts of interest and other disclosures made by a person participating in procurement process to enable the accounting officer or delegated authority to make informed decisions about the person participating in the SCM process.

18.1.2 As such, the Bidders Disclosure form, issued as Standard Bidding Document (SBD) 4, is attached herewith for all entities who participate in the bid process.

18.1.3 As part of the evaluation of the procurement process, the information provided by a person on the SBD4 form must be evaluated.

18.1.4 In so doing, it must be noted that if the bid evaluation establishes that:

(a) a person within the bidding entity is an employee of the State, the Electoral Commission's CEO must request the relevant accounting officer/accounting authority whether the person-

(i) Is prohibited from conducting business with the State in terms of Section 8 of the Public Administration Management Act, 2014; or

(ii) has permission to perform other remunerative work outside of their employment, where the PAMA does not apply to such employee;

(b) the conduct of a person constitutes a transgression of the Prevention and Combating of Corrupt Activities Act, 2004;

(c) the conduct of a person constitutes a transgression of the Competition Act, 1998, the conduct must be reported to the Competition Commission; and

(d) the conduct of a person must be dealt with in terms of the prescripts applicable to the Electoral Commission.

18.1.5 If it is established that a person has committed a transgression in terms of the above, or any other transgression of SCM prescripts, the bid may be rejected and the person may be restricted.

18.1.6 The Electoral Commission's CEO must inform National Treasury of any action taken against a person within 30 days of implementing the action.

18.1.7 During the bid evaluation process, the Electoral Commission must in addition to other due diligence measures, establish if a person is not listed in-

(a) the Register of Tender Defaulters; and

(b) the list of restricted suppliers.

18.1.8 A bid related to a restricted bidder or tender defaulter shall be rejected.

18.1.9 The under-mentioned assessment criteria will be used to evaluate the elements relating to SBD4, CSD registration, tax compliance, restricted suppliers and tender defaulters:

	Assessment Criteria	**Bidder Requirement (YES/NO)**	**Comments**
1.	Bidder is registered on the National Treasury Central Supplier Database (CSD). *		
2.	Bidder is tax compliant. **		
3.	The bidder is not an employee of the state.		
4.	Having certified the SBD4, it is accepted that the bidder's conduct does not constitute a transgression of the Prevention and Combating of Corrupt Activities Act.		
5.	Having certified to the SBD4, it is accepted that the bidder's conduct does not constitute a transgression of the Competition Act.		
6.	The bidder is not a tender defaulter as per the register published on the National Treasury website.		

	Assessment Criteria	Bidder Requirement (YES/NO)	Comments
7.	The bidder is not a restricted supplier as per the register published on the National Treasury website.		

* No bid shall be accepted if a supplier is not registered on the National Treasury Central Supplier Database (CSD).

** A bidder must be tax compliant before a contract is awarded. A bid will be disqualified if the bidder's tax affairs remains non-compliant as per the provisions of National Treasury Instruction No 09 of 2017/2018 Tax Compliance Status Verification.

18.2 Stage 2: Key Qualifying Criteria

Stage 2 – Key Qualifying Criteria				
Failure to comply with any of the requirements below will result in the bid being disqualified				
No.	**Description**	**Yes**	**No**	**Comments**
1.	Did the bidder place their bid online as per 5.1			
2.	Did the bidder complete and submit technical specification as per 5.2? (Appendix A: Technical Bid Response Sheet)			
3.	Did the bidder complete and submit pricing schedule as per 7.2? (Appendix B: Pricing Schedule)			
4.	Did the bidder submit references showing past experience as per 5.3			
5.	Is the bidder authorized to sell the solution as per 5.4, 5.5 and 5.6?			
6.	Did the bidder submit a statement of service, describing the service and support that is covered under the contract including the roles of the bidder and the Original Equipment Manufacturer (OEM) as per 5.7			
Overall Stage 2 Outcomes:	**Assessment Comments:**			
	Bid qualifies for further consideration: (YES/NO):			

19 Stage 3: Technical Evaluation

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
1.	Firewall	Firewall Architecture	4 x Enterprise Grade Firewalls	The proposed solution consists of enterprise-grade physical Next-Generation Firewall (NGFW) appliances, deployed in a high-availability (HA) configuration across the production and disaster recovery data centres.	3.2			
2.				The solution supports resilient operation with automatic failover and minimal service disruption	3.2			
3.	Proposed Solution	Operational Compatibility	Integration	The solution integrates with existing Electoral Commission's networking infrastructure including switches, routers, Directory and Authentication Services (Active Directory), Security Incident and Events Management (FortiSIEM), ManageEngine Service Desk ITSM, and Time Synchrionization services (Network Time Protocol (NTP))	3.7			
4.	Firewall	Hardware	Network Interfaces	The NGFW appliance must support high-speed interfaces capable of 10Gbps,	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
				25Gbps, 40Gbps and/or 100Gbps connectivity.				
5.	Firewall	Hardware	Fiber Ports	Minimum of four (4) high-speed fiber ports per firewall appliance.	3.12			
6.	Firewall	Hardware	Interface Types	Each NGFW appliance must support a combination of copper and fiber interfaces, including but not limited to RJ-45, SFP+, QSFP+, or equivalent modular interfaces.	3.12			
7.	Firewall	Hardware	Power Redundancy	Each NGFW appliance must be equipped with at least two (2) redundant hot-swappable power supplies.	3.12			
8.	Firewall	Hardware	Processing Architecture	The NGFW must utilise a multi-core processing architecture capable of separating management, control plane, and traffic inspection functions to improve performance and reduce latency.	3.12			
9.	Firewall	Security & Authentication	Authentication Integration	The solution must integrate with enterprise authentication systems including LDAP, Active Directory, RADIUS, Kerberos, and cloud-based identity providers.	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. **Failure to comply with any of the requirements below mayresult in the bid being disqualified.**								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
10.	Firewall	Performance	Firewall Throughput	The solution must provide high capacity stateful firewall throughput suitable for large enterprise and data centre environments. Performance figures must be provided under real-world conditions.	3.12			
11.	Firewall	Performance	NGFW Throughput	The solution must provide high NGFW throughput with security services enabled (e.g. IPS, application control, malware protection).	3.12			
12.	Firewall	Performance	Threat Prevention Throughput	The solution must sustain threat prevention throughput with advanced security services enabled, including IPS, malware protection, and application inspection.	3.12			
13.	Firewall	Performance	IPSec VPN Throughput	The solution must support high-capacity IPSec VPN throughput suitable for large-scale site-to-site and remote access deployments.	3.12			
14.	Firewall	Performance	Concurrent Sessions	The NGFW must support a high number of concurrent sessions suitable for enterprise-scale environments.	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
15.	Firewall	Performance	New Session Rate	The solution must support a high new-session establishment rate without degradation of performance.	3.12			
16.	Firewall	High Availability	HA Modes	The solution must support both Active-Active and Active-Passive high-availability modes, including clustering where applicable.	3.12			
17.	Firewall	VPN	VPN Capabilities	The solution must support IPSec and SSL VPNs, hub-and-spoke and full-mesh topologies, strong cryptographic algorithms, and NAT traversal.	3.12			
18.	Firewall	Network Segmentation	Segmentation	The solution must support static and dynamic network segmentation using zones, VLANs, subnets, user identity, device posture, and application context.	3.12			
19.	Firewall	NAT	Network Address Translation	The solution must support source and destination NAT, static NAT, dynamic NAT, and policy-based NAT.	3.12			
20.	Firewall	Traffic Management	Traffic Prioritisation	The solution must support traffic prioritisation and quality-of-service	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
				enforcement based on users, applications, zones, and policies.				
21.	Firewall	Network Access	Access Control	The solution must control network access based on IP addresses, FQDNs, protocols, ports, users, and applications.	3.12			
22.	Firewall	Advanced Security	Zero-Day Protection	The solution must provide protection against known and unknown threats using behavioural analysis, anomaly detection, and machine-learning-assisted techniques.	3.12			
23.	Firewall	Advanced Security	Behavioural Analysis	The solution must support behavioural-based threat detection to identify anomalous activity and evolving attack patterns.	3.12			
24.	Firewall	Logging & Analytics	Log Querying	The solution must provide advanced log filtering, correlation, and analytics capabilities. Natural-language querying may be proposed as a value-added feature.	3.12			
25.	Firewall	Application Control	Application Identification	The solution must provide application identification and control, allowing granular	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
				policy enforcement per application and application category.				
26.	Firewall	Intrusion Prevention	Integrated IPS	The solution must include an integrated IPS using signature-based, anomaly-based, and protocol-analysis techniques.	3.12			
27.	Firewall	Malware Protection	Anti-Bot	The solution must provide integrated anti-bot and command-and-control traffic detection.	3.12			
28.	Firewall	Malware Protection	Anti-Virus	The solution must include integrated antivirus and malware inspection across supported protocols including HTTP, HTTPS, FTP, SMTP, POP3, and IMAP.	3.12			
29.	Firewall	Messaging Security	Anti-Spam	The solution must support anti-spam capabilities for applicable traffic types.	3.12			
30.	Firewall	DNS Security	DNS Protection	The solution must provide integrated DNS security to detect malicious domains and prevent DNS-based attacks.	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
31.	Firewall	Inspection	Deep Packet Inspection	The solution must inspect packet payloads to detect protocol violations, malware, and policy violations.	3.12			
32.	Firewall	Advanced Threat	Threat Emulation	The solution must support sandbox-based or equivalent techniques for analysing unknown files and payloads.	3.12			
33.	Firewall	Advanced Threat	Threat Extraction	The solution must support safe content extraction or equivalent techniques to prevent delivery of malicious content.	3.12			
34.	Firewall	Phishing Protection	Phishing Detection	The solution must provide phishing detection and prevention capabilities across supported protocols.	3.12			
35.	Firewall	DDoS Protection	DDoS Mitigation	The solution must include mechanisms to detect and mitigate volumetric and application-layer DDoS attacks.	3.12			
36.	Firewall	Web Security	Web Filtering	The solution must provide web filtering and content categorisation with configurable policy enforcement.	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
37.	Firewall	Traffic Inspection	HTTPS Inspection	The solution must support HTTPS traffic inspection subject to policy and regulatory requirements.	3.12			
38.	Firewall	Proxy	Proxy Capability	The solution may support explicit or transparent proxy functionality.	3.12			
39.	Firewall	Encryption	SSL/TLS Inspection	The solution must support SSL/TLS inspection including TLS 1.2 and TLS 1.3 for visibility into encrypted traffic.	3.12			
40.	Firewall	Authentication	Multi-Factor Authentication	The solution must support MFA integration for administrative and VPN access, including integration with email, SMS, or authenticator applications.	3.12			
41.	Firewall	Routing	Routing Protocols	The solution must support dynamic and static routing protocols including OSPF, BGP, and policy-based routing.	3.12			
42.	Management	Administration	Centralised Management	The solution must include a centralised management interface with role-based access control.	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. **Failure to comply with any of the requirements below mayresult in the bid being disqualified.**								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
43.	Management	Operations	Centralised Control	The management platform must allow configuration, monitoring, policy management, firmware updates, and compliance enforcement across all firewalls.	3.12			
44.	Management	Reporting	Log Retention	The solution must support historical log retention for a minimum period as defined by organisational policy (minimum 12 months).	3.12			
45.	Management	Reporting	Reporting Tools	The solution must provide customizable reporting including security events, compliance reports, and drill-down analytics.	3.12			
46.	Compliance & Assurance	Best Practices	Configuration Validation	The solution must support real-time best-practice and configuration compliance checks.	3.12			
47.	Compliance & Assurance	Risk Identification	Policy & Config Analysis	The solution must identify vulnerabilities, misconfigurations, and non-optimised firewall rules.	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. Failure to comply with any of the requirements below mayresult in the bid being disqualified.								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
48.	Compliance & Assurance	Remediation	Mitigation Guidance	The solution must provide automated or guided remediation recommendations for identified risks.	3.12			
49.	Compliance & Assurance	Policy Optimisation	Rule Usage Analysis	The solution must identify unused, redundant, or shadowed firewall rules.	3.12			
50.	Compliance & Assurance	Regulatory Compliance	Standards Alignment	The solution must support compliance validation against standards such as NIST, OWASP, and POPIA.	3.12			
51.	Support & Maintenance	Support	OEM Support	The solution must include OEM-backed enterprise support services accessible via web, telephone, and email.	3.12			
52.	Support & Maintenance	SLA	Incident Response	The solution must include 24×7×365 support with defined response times for critical and non-critical incidents.	3.12			
53.	Support & Maintenance	Software	Firmware Updates	The solution must include access to firmware, software, and security updates.	3.12			

Stage 3 – Technical Evaluation - Technical Disqualifying Factors. **Failure to comply with any of the requirements below mayresult in the bid being disqualified.**								
	Solution Component	**Category**	**Requirement**	**Compliance Minimum Requirement**	**Reference**	**Bidder's Indication**		**Comments**
						Yes	**No**	
54.	Support & Maintenance	Hardware	Hardware Replacement	The solution must include advanced hardware replacement for faulty components.	3.12			
55.	Support & Maintenance	Asset Management	OEM Portal	The solution must include access to an OEM asset and license management portal.	3.12			
Overall Stage 3 Outcomes:			**Assessment Comments:**					
			Bid qualifies for further consideration: (YES/NO):					

19.1 Stage 4: Technical Scoring

Bid Evaluation Criteria Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (48/64)					
	Product Description	**Available Score**	**Points Allocation**	**Actual Score**	**Comments**
1	Relevant Reference	30	References: a) Customer Details (Customer name, Contact Person, Email Telephone) = 2 points b) Product/Solution = 2 points c) Description of Services provided = 2 points d) Value (Budget Estimate) = 1 point e) Value (Number of devices Supplied) = 1 point for 1 device and 2 points for more than 1 device f) Was this done in the past 36 months? = 1 point **Total for references = maximum 10 points per reference (3 references)**		
	Relevant Experience	6	Experience. (Max 6 points) a) ≥ 3 and < 5 years' experience (4 points). b) Bidder has more than 5 years' experience (6 points)		

Bid Evaluation Criteria Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (48/64)					
	Product Description	**Available Score**	**Points Allocation**	**Actual Score**	**Comments**
	Support and Maintenance	10	The solution is supplied with a 5 years' Support and Maintenance with the following: a) 4-hour MTTR (5 points) b) 24 x 7 x 365 support (5 points)		
	Scalability	4	The solution supports scaling to accommodate future growth including expansion of throughput, session capacity and security services without requiring a complete platform replacement a) Vertical Scaling (add higher capacity components e.g. RAM, CPU etc) (2 points) b) Horizontal Scaling (add more machines) – 2 points		
	Data sheet (s)	6	Bidder has included data sheet(s) covering the following: a) Firewall Appliances solution (2 points) b) Firewall Management solution (2 points) c) Compliance and Assurance solution (2 points)		

Bid Evaluation Criteria Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (48/64)					
	Product Description	**Available Score**	**Points Allocation**	**Actual Score**	**Comments**
	CV & Project Plan	8	a) Bidder has included a CV of a resource to implement the solution (2 points) b) Bidder has included a project implementation plan (4 points) c) The project plan makes provision for project documentation including design, configuration guides, and as-built reports (2 points)		
Overall Stage 4 Outcomes:		**Assessment Comments:**			
		Bid qualifies for further consideration: (YES/NO):			

19.2 Stage 5: Adjudication of Bids

Only bids that comply with the requirements and conditions of the RFQ and that meet the minimum criteria in the bid evaluation process as stipulated above will be considered for bid adjudication purposes.

Acceptable bids must be market related.

This bid is deemed not to exceed R50 million including VAT.

Therefore, the 80/20 preference point system (PPPFA scoring) in terms of the Preferential Procurement Policy Framework Act, 2005 (PPPFA) and the Preferential Procurement Regulations, 2022 shall apply in the adjudication process of this RFQ where all acceptable bids received are equal to or below R50 million including VAT. Preference points will be allocated as follows:

B-BBEE Status Level of Contributor	Number of Points
1	20
2	18
3	14
4	12
5	8
6	6
7	4
8	2
Non-compliant contributor	0

Bid Evaluation Committee

	Evaluation Committee Member's Name	**Signature**	**Date**
1			
2			
3			
4			
5			

Overall Adjudication Outcomes:

_____

_____