Table of Contents

FOREWORD

Recommendations for corrections, additions or deletions shall be addressed to the:

General Manager: ICT

City Power Johannesburg (SOC) Ltd

P O Box 38766

Booysens

2016

1. INTRODUCTION

City Power hereby requests the services of ICT Security Services Partner that have expertise in ICT security solutions. The Implemented solution shall ensure prevention of malicious attacks, information leaks and business disruptions resulting from Cyber Attacks. These services are requested from experienced and certified/accredited ICT Service Providers.

2. SCOPE OF WORK

The appointed Service Provider shall supply and commission the acquired Next-generation firewall (NGFW) at our Head office in Reuven and the service provider shall comply to City Power's firewall standard/policy. The deployment should adhere to the recommended best practices provided by the OEM.

The scope of work shall include the following:

- Supply and commission Next Generation Firewall with licensing for three years
- Plan and execute the implementation, integration, testing, and deployment of the NGFW solution.
- Migrate the configurations (policies, rules, objects, etc.) from the current firewall to the new firewall.
- Provide three years of licensing for PA 3020 existing firewall.

3. NORMATIVE REFERENCES

The following documents contain provisions that, through reference in the text, constitute requirements of this specification. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

COBIT: *Control Objectives for Information and Related Technology. It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management*

KING IV: *Technology and Information Governance*

TOGAF: *The Open Group Architecture Framework is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture.*

POPI Act: *Protection of Personal Information Act, 2013*

GWEA: *Government Wide Enterprise Architecture framework*

4. DEFINITIONS

The definitions and abbreviations in the above documents (Normative Reference) shall apply to this specification. In addition, the following terms and acronyms are used in this document:

4.1 **NGFW**: Next-Generation Firewall, a network security device that provides granular control over applications, users, and content, as well as threat prevention and detection capabilities.

4.2 **PAN-OS:** Palo Alto Networks Operating System, the software that runs on Palo Alto Networks NGFWs and provides the core functionality and features.

4.3 **Panorama:** Palo Alto Networks centralized management system that provides visibility and control over multiple NGFWs.

4.4 **Prisma:** Palo Alto Networks cloud security suite that includes Prisma Access, Prisma SD-WAN, Prisma Cloud, and Prisma SASE.

4.5 **Cloud NGFW:** Palo Alto Networks cloud-delivered NGFW service that provides network security as a managed service for cloud environments such as AWS and Azure.

4.6 **App-ID:** Palo Alto Networks application identification technology that classifies traffic based on application signatures and characteristics.

4.7 **URL Filtering**: Palo Alto Networks URL filtering service that provides web filtering and enforcement based on URL categories and reputation.

4.8 **DNS Security:** Palo Alto Networks DNS security service that provides DNS-layer protection against malicious domains and phishing attacks.

4.9 **Wildfire:** Palo Alto Networks cloud-based malware analysis and sandboxing service that detects and prevents unknown and zero-day threats.

4.10 **Enterprise DLP:** Palo Alto Networks data loss prevention service that protects sensitive data from unauthorized exfiltration and exposure.

4.11 **IoT Security:** Palo Alto Networks Internet of Things security service that provides visibility and protection for IoT devices and networks.

4.12 **OT Security:** Palo Alto Networks operational technology security service that provides visibility and protection for industrial control systems and critical infrastructure.

4.13 **SASE:** Secure Access Service Edge, a network security model that combines network and security functions into a unified cloud service.

4.14 **CASB:** Cloud Access Security Broker, a security solution that provides visibility and control over cloud applications and data.

4.15 **AIOps:** Artificial Intelligence for IT Operations, a methodology that uses machine learning and automation to improve IT operations and performance.

5. TECHNICAL REQUIREMENTS

The requirements for the NGFW solution are based on the business and technical needs of City Power, as well as the best practices and standards for network security. The requirements are categorized into the following domains:

5.1 **Application Visibility and Control**: The NGFW solution shall provide granular visibility and control over the applications, users, and content that traverse the network, regardless of the port, protocol, or encryption. The NGFW solution shall support App-ID, URL Filtering, and DNS Security services to enable application identification, web filtering, and DNS protection. The

NGFW solution shall also support policy-based traffic shaping and prioritization to optimize network performance and user experience.

5.2 **Threat Prevention and Detection**: The NGFW solution shall provide comprehensive threat prevention and detection capabilities to protect the network from known and unknown attacks, such as malware, ransomware, exploits, and phishing. The NGFW solution shall support Wildfire, Enterprise DLP, IoT Security, and OT Security services to enable malware analysis, data protection, IoT device profiling, and OT network monitoring. The NGFW solution shall also support inline deep learning and zero-delay signatures to enable fast and accurate detection of zero-day threats and prevent patient zero infections.

5.3 **Cloud-Delivered Security Services**: The NGFW solution shall provide cloud-delivered security services that leverage the scalability, elasticity, and intelligence of the cloud. The NGFW solution shall support Prisma Access, Prisma SD-WAN, Prisma Cloud, and Prisma SASE services to enable secure access, SD-WAN, cloud security, and SASE capabilities. The NGFW solution shall also support Cloud NGFW for AWS and Azure to enable network security as a service for cloud environments.

5.4 **Management and Automation**: The NGFW solution shall provide centralized management and automation capabilities to simplify and streamline the administration and operation of the network security platform. The NGFW solution shall support Panorama, Prisma Cloud Manager, and PAN-OS to enable unified management, configuration, monitoring, and reporting of multiple NGFWs. The NGFW solution shall also support AIOps, API, and DevOps integrations to enable automated provisioning, orchestration, and optimization of the network security platform.

6. TRAINING

6.1 City power requires the necessary training for system administrators.

6.2 The Service Provider shall clearly outline the layout of the recommended enhanced training

6.3 The solution provider shall work closely with City power's resources during the implementation in a live environment to ensure practical knowledge transfer.

6.4 Training shall be on-site and form part of the implementation process.

6.5 The Service Provider shall also be required to provide training to City Power technical representatives on the system when enhanced features and functionality become available as the system is upgraded.

6.6 The suppliers shall provide technical support on system and equipment queries for the duration of the contract as of go-live date of the implemented solution.

7. DOCUMENTATION

The Service Provider shall provide all documentation required that includes but not limited manual, licences, and catalogues.
Documentation shall be in both hard and soft copy.

8. QUALITY MANAGEMENT

A quality management system/plan shall be set up to assure the quality during manufacture, installation, removal, transportation, and disposal. Guidance on the requirements for a quality management system may be found in the following standards: ISO 9001:2015. The details shall be subject to an agreement between the purchaser and supplier.

9. HEALTH AND SAFETY

A health and safety system/plan shall be set up to ensure proper management and compliance during manufacture, installation, removal, transportation, and disposal. Guidance on the requirements of a health and safety plan shall be found in ISO 45001:2018 standards. The details shall be subject to an agreement between City Power and the Supplier.

10. ENVIRONMENTAL MANAGEMENT

An environmental management system/ plan shall be set up to ensure the proper environmental management and compliance is adhered to during manufacturing, installation, removal, transportation, and disposal. Guidance on the requirements for an environmental management system shall be found in ISO 14001:2015 standards. The details shall be subject to an agreement between City Power and the Supplier. This is to ensure that the asset created conforms to environmental standards and City Power SHERQ Policy.

ANNEXURE A - BIBLIOGRAPHY

ANNEXURE B - REVISION INFORMATION

DATE	REV. NO.	NOTES
March 2023	0	First issue