Eskom

Group IT Scope of Work

Secure Web Gateway (SWG) Managed Services for a Period of Five (5) Years

1. Scope of work/Business requirements

The supplier is required to provide Secure Web Gateway (SWG) Managed Services for a period of five (5) years:

a. On-Premise Forward Proxy Capability:

1. Ability to process cloud-based traffic: The technology must be able to efficiently process internet traffic between internal Eskom devices and cloud services (i.e.O365, AWS etc.)
2. Multi-Breakpoint Architecture ability: The solution must have a capability of accommodating a multiple internet breakout architecture.
3. Anti-Malware for advanced threats: ability to protect web the roaming user from viruses, worms, and Trojans with real-time AV scanning of all internet content
4. Caching - The solution must store program instructions that are frequently referenced
5. Video/streaming optimisation: The solution must have the ability to optimise Video/streaming content.
6. High Availability: The solution must possess the ability to operate on fail-over architecture.
7. Encrypted traffic: The solution should analyse encrypted data traffic.
8. Load balancing - The solution should be integrated to the load balancing solution deployed in Eskom.
9. File reputation: The solution should check the reputation of each file against an extensive database.
10. Data Loss Prevention (DLP): The solution must support various protocols (e.g. ICAPS) in order to integrate to full DLP solution.
11. Filtering options: The ability to filter on URL, IP addresses, Port numbers, Keywords, File types and categories.
12. Authentication: Ability to integrate with AD, LDAP and other IAM solutions. Service provider to provide a list of IAM solutions their solution can integrate with.
13. Sandboxing: Ability to intercept, detonate and analyse files (encrypted) whose reputation is not verified
14. Policy: Implement granular access policies based on users, groups, time of day, location, network address, user agent, and other attributes to meet customised business requirements
15. Zero Trust capability
16. API capability – ability to utilise various API's
17. Logging: Provide the ability to integrate to a SIEM solution.
18. Centralised reporting: Report on usage, groups, malware, cyber-attacks, trends etc.
19. Centralised Management Console: The management of the solution must be centralised.

b. Off-Premise Forward Proxy Capability:

1. Ability to process cloud-based traffic: The technology must be able to efficiently process internet traffic between internal Eskom devices and cloud services (i.e.O365, AWS etc.)
2. Multi-Breakpoint Architecture ability: The solution must have a capability of accommodating a multiple internet breakout architecture.
3. Anti-Malware for advanced threats: ability to protect web the roaming user from viruses, worms, and Trojans with real-time AV scanning of all internet content
4. Caching - The solution must store program instructions that are frequently referenced

5. Video/streaming optimisation: The solution must have the ability to optimise Video/streaming content.
6. High Availability: The solution must possess the ability to operate on fail-over architecture.
7. SSL Interception: The solution should intercept and analyse encrypted data traffic.
8. Load balancing - The solution should be integrate to the load balancing solution deployed in Eskom.
9. File reputation: The solution should check the reputation of each file against an extensive database.
10. Data Loss Prevention (DLP): The solution must support various protocols (e.g. ICAPS) in order to integrate to full DLP solution.
11. Filtering options: The ability to filter on URL, IP addresses, Port numbers, Keywords, File types and Categories.
12. Authentication: Ability to integrate with AD, LDAP and other IAM solutions. Service provider to provide a list of IAM solutions their solution can integrate with.
13. Sandboxing: Ability to intercept, detonate and analyse files (encrypted) whose reputation is not verified
14. Policy: Implement granular access policies based on users, groups, time of day, location, network address, user agent, and other attributes to meet customised business requirements
15. Zero Trust capability
16. API capability – ability to utilise various API's
17. Logging: Provide the ability to integrate to a SIEM solution.
18. Centralised reporting: Report on usage, groups, malware, cyber-attacks, trends etc.
19. Centralised Management Console: The management of the solution must be centralised.

c. Training

1. Provide online / classroom administration training with certification for five (5) Eskom personnel:
   i. Basic and advanced administrator level training
   ii. Training must be provided in the first year of the contract

SIGNED BY:

15 September 2022

MMUTLE KGAMPE — **DATE**
SENIOR ADVISOR: GROUP IT- SECURITY

B Jelliman

15 September 2022

BERESFORD JELLIMAN — **DATE**
CHIEF ADVISOR: GROUP IT- SECURITY

16-09-2022

SITHEMBILE SONGO — **DATE**
SENIOR MANAGER: GROUP IT- SECURITY