

TERMS OF REFERENCE FOR THE APPOINTMENT OF A SUITABLY QUALIFIED AND OEM CERTIFIED BIDDER FOR THE PROVISION OF A FIREWALL REFRESH WITH MONITORING TOOL, SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM), INTRUSION PREVENTION SYSTEM, URL FILTERING, AND DATA LOSS PREVENTION (DLP) SOLUTIONS FOR THE DEPARTMENT OF MINERAL AND PETROLEUM RESOURCES (DMPR) FOR THREE (3) YEARS. THIS INCLUDES THE IMPLEMENTATION OF FIREWALL HARDWARE, SOFTWARE, MAINTENANCE, AND SUPPORT.

1. BACKGROUND

1.1 Current Firewall Landscape and Architecture: The current environment consists of two pairs of Check Point physical enterprise-grade firewalls deployed in high-availability (HA) mode in one datacenter (Sita), supported by a virtualized management server and an event logging/monitoring server for centralized administration, reporting, and threat visibility. The infrastructure is outdated, and the hardware is out of warranty and support.

1.2 Current Challenges: The infrastructure hardware is outdated, out of warranty and no longer supported.

1.3 Deployment Sites

The new firewall solution will be deployed across all DMPR Regional sites to ensure proper separation of site separation and ensure that other sites do not affect the other sites.

Table 1: List of DMPR sites

Province	Office
1.Gauteng	Pretoria (HQ), Trevena Campus and SITA (main site), Braamfontein, Johannesburg
2.Mpumalanga	Witbank
3.Free State	Welkom
4.Limpopo	Polokwane: Dorp and Landros Mare

5.North-West	Klerksdorp Rustenburg Mafikeng
6.Northern Cape	Kimberly Springbok
7.Eastern Cape	Port Elizabeth Umtata East London
8.Western Cape	Cape Town
9.Kwazulu Natal	Durban

2. CONTRACT PERIOD

- 2.1 The duration of the contract is 36 months from the date of signature of the service level agreement.

3. OBJECTIVE

- 3.1 The primary objective of refreshing the firewall system is to enhance the cybersecurity posture of DMPR by ensuring robust protection of sensitive information and reinforcing the resilience of the network infrastructure against external threats. This upgrade will offer advanced defence mechanisms against malicious attacks, unauthorized access, and a wide range of electronic threats originating outside the organization.
- 3.2 The refreshed firewall will play a vital role in enforcing network security policies, monitoring and controlling traffic, and preventing data breaches. It will also support improved threat detection and response capabilities, aligning with DMPR's broader cybersecurity strategy.

4. SCOPE OF WORK

The capable and qualified supplier will be expected to provide the following services at DMPR Headquarters (HQ) and regional offices:

- 4.1 Firewall solution that will assist the DMPR with its network defence in depth approach.
- 4.2 Migration of the current firewall configuration to the proposed firewall solution.
- 4.3 The firewall should support “Stateful” policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.
- 4.3 It should support the Firewall, IPSEC VPN & Bandwidth Management as integrated security functions.
- 4.4 The hardware platform & firewall with integrated IPSEC VPN application has to be from the same OEM.
- 4.5 The solution must include High Availability (HA). Appliance should support for Active –Active connections for HA requirements.
- 4.6 Licensing should be per device and not user/IP based (should support unlimited users).
6. Firewall should be supplied with the support for dynamic routing protocols, like RIP v2, OSPF, & BGP.
- 4.7 Firewall should support the multicast protocols as a multicast host, by participating in DVMRP, IGMP and PIMDM / PIM-SM.
- 4.8 Proposed Firewall OEM should be in the Leaders & Challengers Quadrant of Gartner Magic Quadrant for Enterprise Firewall.
- 4.9 Proposed Firewall must have an integrated IPS.
- 4.10 Hardware, software support, and maintenance requires 24/7 throughout the contract period with the responsive time of 4 hours to resolve, on-site and telephonic support, and includes swapping out equipment. Security equipment maintenance and license.
- 4.11 Support includes software assurance (the supply, installation, and commissioning of the latest software and firmware versions where possible).
- 4.12 Provide Root Cause Analysis (RCA) report and Design Documentation as and when needed. In the event of a service failure, it will be expected of the prospective Service Provider to conduct a root cause analysis, following best practices, and produce a report covering at least the following:
 - The root cause and contributing factors of the service failure,
 - The corrective actions undertaken to restore the service,

- Preventive actions to avert a recurrence,
- Implementation plan to put into practice preventative actions, and,
- Close-out report annexure which confirms the successful implementation of the preventative actions.

Note: The close-out report will follow the DMPP's process but form an integral part of the root-cause report and must be attached for the root-cause report to be considered closed.

4.13 Installation and Commissioning:

4.13.1 The service provider must handle the end-to-end deployment of the proposed firewall solution.

4.13.2 Physical installation and cabling of the firewall equipment

4.13.3 High Availability (HA) configuration across all datacentres
Interconnectivity (heartbeat, sync, etc.)

4.13.5 Integration with existing DMPP infrastructure (e.g., switching, routing, DNS, syslog, NTP)

4.13.5 Policy and Configuration Migration: Where applicable, the service provider must 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

4.13.6 **Documentation:** The service provider must produce and deliver system documentation including: Final design document Configuration guides Change control logs As-built reports.

4.14.7 Critical component of the proposed solution is a comprehensive SLA for a Three (3) year period that will include change and configuration management, as well as incident and event management.

- 24x7 Service Desk for single point of contact and escalations
- Level 1 and Level 2 support from bidder. The support should be on-site. Includes support for day-to-day operational issues as and when these arise.
- Level 3 and Level 4 support from OEM or the accredited service provider.

- Provide login to DMPR for web access to OEM portal.
- Monitored email support.
- Remote assistance using Remote Desktop and a Virtual Private Network (VPN) where available.
- Planned or Emergency Onsite assistance.
- Monthly system health check
- License management
- Hardware appliance guarantee
- The number of calls per month over 12 months per category.
- The restore time of all calls logged (incidents and requests).
- The % of incidents completed within 4-hour resolution.
- The % of requests completed within an 8-hour resolution.
- The % of calls re-opened.

4.13.7 To provide complete technical training to three (3) DMPR officials by the OEM or accredited service provider on behalf of the OEM on system design, configuration, operation, maintenance, management and administration of the system along with DNS setup, firewall appliances, appliance monitoring software, Security Information and Event Management (SIEM), Data Loss Protection (DLP), etc.

Staff Knowledge Transfer and Training: The service provider must provide initial handover sessions and knowledge transfer to DMPR's.

- internal technical staff, covering:
- Management interface and monitoring
- Logging/reporting procedures
- Basic troubleshooting
- Update and patch procedures.

4.14 Bidders are urged to complete the attached Cost Breakdown table to enable DMPR to understand the cost drivers.

Cost Drivers	% breakdown
Licensing and Software	%

Installation and Configuration	%
Hardware	%
Annual Maintenance/Support	%
Once-Off Training	%
Contingency/Miscellaneous	%
Total cost	100%

5.1 DELIVERABLES OR PROJECT OUTPUT AND OR OUTCOME

5.1 The expected outputs are:

- 5.1.1 The service provider should submit a detailed configuration plan on sign-off of installation based on scope technical specifications
- 5.1.2 Detailed project implementation plan of how the proposed solution will be deployed
- 5.1.3 Provide Firewall hardware infrastructure.
- 5.1.4 Sample solution technical/ solution management reports
- 5.1.5 Bi-Weekly and monthly status and progress reports
- 5.1.6 Project closing Report: Project conclusion documentation outlining work completed, lessons learned and recommendations for next steps.
- 5.1.7 SLA document will be drawn up with a successful bidder. Service provider to provide draft with clear deliverable, categories/ classification of service, turnaround times as a minimum
- 5.1.8 Review or develop Firewall policies, procedures and processes
- 5.1.9 Firewall architecture
- 5.1.10 Assessment report of current setup, data utilization and improvements thereof with aim to reduce any existing inefficiencies
- 5.1.11 Warranty Document detailing what will be covered and duration as minimum and License Packs/Portal
- 5.1.12 Skill transfer plan

6. EVALUATION CRITERIA

This bid will be evaluated in four stages, i.e. functionality, mandatory requirements, administrative compliance and point scoring system.

6.1 Gate 01 – Mandatory requirements

The following requirements are mandatory. Bidders who do not comply with the mandatory requirements will be disqualified.

- (i) Bidders must be accredited by the OEM (submit proof on letter head of the OEM)
- (ii) Bidders must have OEM Gold Reseller Partner or higher accreditation for software or the equivalent of Gold Reseller Partner
- (iii) Bidders must have OEM Gold Reseller Partner or higher accreditation for hardware or the equivalent of Gold Reseller Partner
- (iv) Project Manager must have certification in Project Management and the certification of the proposed solution(s)
- (v) Team members must have certification in Firewall solution proposed.
- (vi) Bidders must have at least two key personnel who are engineers with firewall Certification.

6.2 Gate 02 - Functionality

Bidders will be scored in terms of the functional requirements indicated in the table below. The corresponding points and weightings will be used to calculate the overall score a bidder has achieved. The minimum threshold for this bid is **60%**. Bidders who score less than **60%** will be disqualified. Only bidders that score **60%** and more will be considered further.

NO	CRITERIA	SCORING	WEIGHTS
1	Company Experience: (i) Bidders should have successfully implemented Firewall projects with minimum 1250 number of users in the past 7 years. (ii) Bidders must demonstrate successful implementation of Firewall projects at multiple sites (regional presence) (Provide proof in the form of either an appointment letter or purchase order or contract document AND testimonial indicating that they have successfully implemented Firewall project, what the user base was, contract period and geographical presence. The testimonial(s) must be signed and on a letterhead of company that received the services,) NB: “Successfully implemented” means that the solution has been configured in the client’s production environment.	5 or more projects = 5 points 4 projects = 4 points 3 projects = 3 points 2 projects = 2 points 1 or less project 0 point or Evidence did not attach 0 point.	20

2	PROJECT MANAGER EXPERIENCE The project manager should have relevant experience specifically in the project management of the implementation of the Firewall projects. Proof of CV attached.	Five (5) years or more = 5 points Four (4) years = 4 points Three (3) years = 3 points less than three (3) Years = 0 points or Evidence not attached.	20
3.	TEAM MEMBERS EXPERIENCE (iii) The technical team members should have relevant experience specific to the configuration and implementation of Firewall solution proposed. Proof of CV attached.	More than four (4) years = 5 points four (4) years = 4 points three (3) years = 3 points two (2) years = 2 points One (1) year = 1 point If CV did not attach 0 point will be allocated	20
4	PROJECT PLAN AND METHODOLOGY Project methodology to be used to execute and deliver the artifacts of the project in line with the scope of work's seven (7) aspects stated hereunder.	Seven or more aspects covered = 5 points Less than the seven (6-5) aspects covered = 3 points	20

	➤ Defined tasks ➤ Timelines ➤ Resources responsible for tasks as per provided CV. ➤ Clear dependencies. ➤ Rollout plan for implementation at for all the sites. ➤ Migration plan of historical Firewall data from old to new infrastructure. ➤ Skills transfer plan and implementation thereof (The proposal should detail the dependencies of the Department to ensure successful implementation of project)	Less than the five (5) aspects or not attached = 0 points	
5	TECHNICAL PROPOSAL The company's technical proposal should clearly demonstrate that they understood the TOR requirements. In line with scope of work point from (4.1 to 4.6)	Company proposal attached in line with TOR and scope of work, proposal aligned to implementation and methodology = 5 Points Company proposal attached not in line with TOR and scope of work, and proposal not aligned to implementation and methodology OR not attached = 0 Points	20

		If proposal did not attach 0 points will be allocated	
--	--	--	--

Formula; $\frac{A}{B} \times 100 = C\%$

Where: A = Total score for the bid under consideration

B = Maximum possible score

C = Percentage score for the bid under consideration

6.3 Gate 03 - Administrative compliance

- (i) Compliance to the specification / Terms of Reference.
- (ii) Fully completed SBDs (Duly signed and dated) listed hereunder:
 - SBD 1
 - SBD 4
 - SBD 6.1
- (iii) The following will be regarded as noncompliance.
 - Price amendments / other amendments without signature/initials.
 - Use of correctional fluid
 - Completion of the bid document in coloured ink other than black ink

6.4 Gate 04 – Point Scoring System

Bids will be evaluated on the 80/20 preference point system as outlined in the Preferential Procurement Regulation of 2022.

- Price points = 80
- Preferential points = 20

6.4.1 The bidder that scores the highest points in this phase will be awarded the tender.

6.4.2 Should more than one bidder score the same number of points; the award will be made to the bidder who scores more points on specific goals.

7. TECHNICAL PROPOSAL

- 7.1** The company's technical proposal should clearly demonstrate that they understand the TOR requirements, have adequate resources (be able to service all regions) to execute the project within the stipulated turnaround times.
- 7.2** The proposal should also include a detailed implementation approach.
- 7.3** Must clearly indicate technology maturity and the proposed technology's standing in the industry.
- 7.4** All shortlisted service providers will be expected to give a presentation where points will be allocated.
- 7.5** Migration plan of historical Firewall data from old to new infrastructure

8. REPORTING REQUIREMENTS

- 8.1** This project will be implemented in line with the Scope of work and will be managed based on the following:
 - 8.1.1** The service provider will report to the Chief Information Officer or delegated official.
 - 8.1.2** The service provider will be expected to provide various reports monthly (e.g., project status report) in the form of Portable Document Format (PDF)/Microsoft standard format, as well as provide any other project-related report/s as requested by the Department.
 - 8.1.3** The service providers will be expected to have compulsory meetings with the Department in accordance with the service level agreement for the duration of the contract agreement. In case of emergencies, either party may propose a meeting, and both parties must reasonably avail themselves of such a meeting.
 - 8.1.4** The service provider will be expected to provide all the project management documents in line with the DMPR methodology.

9. ROLES AND RESPONSIBILITIES

- 9.1 The Department will be responsible for:**
 - 9.1.1** Provide documentation of the current infrastructure.
 - 9.1.2** Provide access to the current infrastructure.
 - 9.1.3** Provide rack space, power, and cooling for any equipment to be installed onsite.

9.1.3 Manage and monitor the delivery of services through the SLA, which will include periodic performance review.

9.2 The Service provider will be responsible for:

9.2.1 The Service Provider shall perform strictly in accordance with the requirements of the Terms of Reference and Service Level Agreement.

9.2.2 The Service Provider shall at all material times act diligently, reasonably, and with care when dealing with all Departmental information and/or intellectual property belonging to the Department.

10 CONFIDENTIALITY OF INFORMATION

10.1.1 All information shared during this bidding process and implementation of this project should be appointed, remains the property of DMPR and should be kept with the highest confidentiality and cannot be used or shared for any other purpose.

11 PAYMENT

11.1 The Department will not make an upfront payment to a successful service provider. Payments will only be made in accordance with the delivery of service that will be agreed upon by both parties, and receipt of an original invoice.

12 TAX CLEARANCE CERTIFICATE

12.1 Bidders must ensure compliance with their tax obligations.

12.2 Bidders are required to submit their unique personal identification number (pin) issued by SARS to enable the organ of state to view the taxpayer's profile and tax status.

12.3 Application for tax compliance status (TCS) or PIN may also be made via e-filing. To use this provision, taxpayers will need to register with SARS as e-filers through the website www.sars.gov.za.

12.4 A bidder may also submit a printed TCS together with the proposal.

12.5 In proposals where consortia / joint ventures/subcontractors are involved. Each party must submit separate proof of TCS / pin / CSD number.

- 12.6** Where no TCS is available, but the bidders are registered on the central supplier database (CSD), a CSD number must be provided.
- 12.7** The potential service provider/s must ensure compliance with their tax obligations.
- 12.8** The potential service provider/s is/are required to submit their unique personal identification number (PIN) issued by SARS to enable the organ of state to view the taxpayer's profile and tax status.
- 12.9** Application for tax compliance status (TCS) or pin may also be made via e-filing. To use this provision, taxpayers will need to register with SARS as e-filers through the website www.sars.gov.za.
- 12.10** The potential service provider may also submit a printed TCS together with the proposal.
- 12.10.1 In proposals where consortia / joint ventures / sub-contractors are involved, each party must submit a separate proof of TCS / PIN / CSD number.
- 12.10.2 Where no TCS is available, but the potential service provider/s is registered on the central supplier database (CSD), a CSD number must be provided.

14. COST / PRICING

- 14.1.** Bidders are requested to provide a quoted proposal regarding the work to be undertaken.
- 14.2.** Bidders are required to indicate a ceiling price based on the total estimated time for completion of all phases and including all expenses, inclusive of all applicable taxes for the project. The total cost must be VAT inclusive and should be quoted in South African Rands (i.e., ZAR).
- 14.3.** Bidders should provide hourly rates as prescribed by Department of Public Service and Administration (DPSA), Auditor- General (AG) or the body regulating the profession of the consultant.
- 14.4.** Bidders should provide (Subsistence & Travel (S&T)) rates that are aligned to the National Treasury instruction note as follows:
- i) Hotel Accommodation – R1700 per night per person, including breakfast, dinner, and parking.
 - ii) Air travel must be restricted to economy class.

- iii) Claims for kilometres may not exceed the rates approved by the Automobile Association of South Africa.

15. CONDITIONS OF THE CONTRACT

- 15.1 The appointed service providers will enter into a Service Level Agreement prior to commencement of the project.
- 15.2 The Department reserves the right to terminate the appointment of any part thereof; at any stage of completion, the Department should decide not to proceed with the project.
- 15.3 Should the contract between the Department and the service provider be terminated by either party due to reasons not attributed to the service providers, the service providers will be remunerated for the appropriate portion of work completed.

16. FORMAT OF SUBMISSION OF PROPOSAL

- 16.1 Bidders are requested to submit one (1) copy of the technical proposals plus the original.
- 16.2 Bidders are requested to index their proposals for easy reference.

17. PRE-BID MEETING / BRIEFING SESSION DETAILS

- 17.1 A compulsory briefing session will be held on **05 February 2026 at 10:00 through Microsoft Teams:**

Meeting ID: 315 906 673 590 10

Passcode: Dr3tY2eE

18. CLOSING DATE

Proposals must be submitted on or before **20 February at 11:00** at the Department of Mineral and Petroleum Resources, at Building 2 C, Trevenna Campus, C/o Meintjes and Francis Baard Street, Sunnyside, 0007, in the bid box Department of Mineral and Petroleum Resources. **No late bids will be accepted.**

19. ENQUIRIES

19.1 All general enquiries relating to bid documents should be directed to:

Mr. Tebogo Katjeni

Tel No: (012) 444 3197

E-mail: Tebogo.Katjeni@dmpr.gov.za

19.2 Technical enquiries can be directed to:

Mr T. Mudau

Tel No: (012) 4443296 / 071 362 4709

E-mail: Godfrey.Mudau@dmpr.gov.za