

ADDENDUM NO 1

ATTENTION: TO ALL BIDDERS WHO ATTENDED THE COMPULSORY PHYSICAL BRIEFING SESSION

ARC Tender reference no: ARC/09/08/2026

Tender description: The Provision of Managed and Hosted Hybrid Mesh Firewall Services for a Period of Thirty-Six (36) Months.

1. Background:

The ARC-CO advertised tender No: ARC/09/08/2026 as follows:

- **Publication Date:** 21 August 2026
- **Compulsory briefing session:** 03 September 2026
- **Extension of Closing date:** 28 September 2026

It was noted during the compulsory briefing session that there was an omission on the scope of work and on required documents under administrative compliance and mandatory requirements as indicated below and therefore, Bid evaluation stage need to be amended as follows:

Incorrectly stated	Correct wording
6. SCOPE OF WORK The scope of work is provision of the managed firewall (physical/virtual) services which includes but not limited to the deployment, configuration, security monitoring, management, maintenance, proactive threat detection and blocking, firmware and patch management, updating and optimization to protect ARC network, systems applications and data against cyber security threats whilst ensuring compliance with security policies configuration and regulatory requirements.	6. SCOPE OF WORK <i>The scope of work is provision of the managed and “Hosted Hybrid Mesh” Firewall (physical/virtual) services which includes but not limited to the deployment, configuration, security monitoring, management, maintenance, proactive threat detection and blocking, firmware and patch management, updating and optimization to protect ARC network, systems applications and data against cyber security threats whilst ensuring compliance with security policies configuration and regulatory requirements.</i>
8. EXPECTED OUTCOMES Key Deliverables The successful bidder(s) must provide:	8. EXPECTED OUTCOMES Key Deliverables The successful bidder(s) must provide:

- The current-state assessment and due diligence report
- Detailed solution design/ architecture documentation
- Project Implementation and configuration plan (project charter)
- Migration and cut-over plan
- Security policies and baselines
- SOPs and runbooks
- Training and skills transfer
- Monthly SLA reports
- Monthly security incident reports
- Quarterly security posture review report
- Final project closure report
- Hosting in a secure data centre
- Centralised management and unified logging
- High availability and failover configuration
- Policy configuration and lifecycle management

Performance & Capacity

Incorrectly stated

Requirement	Minimum
Internet Throughput	36 Gbps
WAN Throughput	10 Gbps
VPN Users	2 000
IPS Throughput	5.7 Gbps
Concurrent Sessions	8 Million
New Connections/sec	300,000

11.1 PHASE 1: ADMINISTRATIVE REQUIREMENTS

1. Valid current Tax PIN number from SARS.
2. Current Central Supplier Database (CSD report) showing a tax compliant status for the duration of

- The current-state assessment and due diligence report
- Detailed solution design/ architecture documentation
- Project Implementation and configuration plan (project charter)
- Migration and cut-over plan
- Security policies and baselines
- SOPs and runbooks
- Training and skills transfer
- Monthly SLA reports
- Monthly security incident reports
- Quarterly security posture review report
- Final project closure report
- Hosting in a secure data centre
- Centralised management and unified logging
- *High availability “cluster” and failover configuration*
- Policy configuration and lifecycle management

Performance & capacity

Correct wording

Requirement	Minimum
Firewall Throughput	80 Gbps
IPS Throughput	12.5 Gbps
NGFW Throughput	9.8 Gbps
Threat Protection Throughput	7.1 Gbps
SSL Inspection Performance	High-performance TLS/SSL inspection
Concurrent Sessions	Up to 32 Million
New Sessions/sec	Up to 1.2 Million
IPsec VPN Throughput	Up to 55 Gbps

11.1 PHASE 1: ADMINISTRATIVE COMPLIANCE

1. *Current and updated Central Supplier Database report (CSD Report).*
2. *Valid PIN number from SARS.*
3. *Complete and Sign all the SBD forms.*

the tendering process. 3. Complete and sign all the Standard Bidding Document (SBD forms) 4. The master bid document should be completed, initialled and signed in full. 5. Valid BBBEE certificate / sworn affidavit.	4. <i>The master bid document should be completed, initialled and signed in full.</i> 5. <i>BBBEE Certificate or Sworn Affidavit should be submitted.</i> 6. <i>Resolution Letter to sign the documents should be submitted.</i> 7. <i>Joint Venture/ Sub Contracting Signed, dated Joint Venture Agreement – if applicable (to be signed by all parties, indicating the responsibilities of each partner and who the lead partner will be, and which partner is authorised to sign these documents).</i>
11.2 PHASE 2: MANDATORY REQUIREMENTS 1. The bidder must be an authorised partner/reseller of the proposed firewall solution and provide a valid letter as proof of OEM accreditation. 2. The bidder must have a minimum of three (3) reference letters from clients where similar services have been rendered within the seven (7) years. 3. Bidders must submit the minimum of three (3) CVs indicating the relevant experience of the above-mentioned scope of work and valid certification of security engineers for the firewall solution. 4. Bidder must be ISO/IEC 270033-4 certified and provide valid proof. 5. The bidder must attend the physical compulsory briefing session. N.B Failure to meet all the above requirements will disqualify your company	11.2 PHASE 2: MANDATORY REQUIREMENTS 1. <i>The bidder must be an authorised partner/reseller of the proposed firewall solution and provide a valid letter as proof of OEM accreditation.</i> 2. <i>The bidder must have a minimum of three (3) reference letters from clients where similar services have been rendered within the seven (7) years.</i> 3. <i>Bidders must submit the minimum of three (3) CVs indicating the relevant experience of the above mentioned scope of work and valid certification of security engineers for the firewall solution.</i> 4. <i>Bidder must be ISO/IEC 27033-4 certified OR ISO/IEC 27001 and provide valid proof.</i> ISO/IEC 27033-4 <i>Evidence: OEM letter confirming the proposed firewall/security gateway architecture conforms to ISO/IEC 27033-4 principles.</i> OR <i>ISO/IEC 27001 (Information Security Management System)</i> <i>Evidence: The bidder shall provide a valid ISO/IEC 27001 certificate covering its Managed Security Services, Security Operations Centre (SOC), cloud services, and hosting/data centre operations.</i> 5. <i>The bidder must attend the physical compulsory briefing session.</i> <i>N.B Failure to meet all the above requirements will disqualify your company</i>



NOTE: The signed confirmation and issued addendum must be submitted along with the bid document.

Further to the above, bidders must note that the Record of Addenda to tender document must be completed in full to acknowledge the changes made and is now a mandatory document.

Name of Bidder

Position

Signature

Date