Terms of Reference (TOR): Procurement, Setup, and Management of a Hybrid Firewall for Network Security

Tender Number:
GBM/PR/HFNS/Oct/2026/001

1. Introduction

The Green Belt Movement (GBM) seeks to strengthen its network security by procuring, setting up, and managing a hybrid firewall: a firewall appliance at its head office, plus protection for staff working remotely or in the field, all run from one console. The firewall will protect GBM's staff and devices against cyber threats, ensuring data integrity and secure connectivity for the office, the field, and the cloud services GBM uses.

Field	Detail
Sites to cover	Head office & remote
Staff on site	About 21
Total staff, including field staff and growth	Up to 60 (the planning figure for the contract term)
Staff devices	Up to 2 per person (laptop and phone)
Other devices without a user (printers, network phones, servers, others)	3 today, plus planned CCTV (cameras and recorder) and spare capacity, rounded up for safety
Internet link today	30 Mbps symmetrical fibre
Link planned over the term	Up to 200 Mbps, with an optional second link from another provider
Remote and VPN users	Up to 60
Cloud services in use	Microsoft 365 and Google Workspace; HR, payroll and accounting applications hosted in the cloud
Current network protection	Details provided to registered bidders at the briefing

Sizing basis. Annex A shows how every minimum in Section 3 is derived from these figures. Bidders size to the minimums, not to the 30 Mbps link. The appliance is expected to stay in service for several years, and the link is likely to grow.

2. Objective

To procure, set up, install and manage a hybrid firewall solution capable of protecting up to 60 staff and their devices, including a managed service (monitoring, updates, support, and reporting) for an initial 12 months, renewable yearly for up to 36 months in total.

GBM's budget for this work is limited. Bidders should propose the simplest design that meets the requirements. Optional items are priced separately (Section 7), and GBM chooses them after the award.

3. Scope of Work

The scope of work includes, but is not limited to, the items below. M means mandatory: a "No" disqualifies the bid. D means desirable and is scored. Performance figures must come from the manufacturer's published

datasheet, with the test conditions stated (packet size or traffic mix, cipher suites, and which security features were switched on). A figure given without its test conditions is treated as not provided.

3.1. Procurement

Supply of a firewall meeting the following requirements:

ID	Requirement	M/D
	Platform and design	
FW-01	Hybrid design: a managed next-generation firewall appliance at the head office plus cloud or agent protection for remote devices, managed from one console. The bidder states the product name and model of every component. The bidder may offer the appliance by purchase or by lease. Accepted platforms: Fortinet FortiGate and Sophos XGS, because both are supported by authorised partners and local engineers in Kenya. A bidder may propose another platform only with written confirmation from its manufacturer that it works with GBM's Microsoft 365 and Google Workspace sign-in and its existing network equipment, and it must still meet FW-03 to FW-07. Open-source firewall software and virtual-only appliances at the office are not accepted.	M
FW-02	Manufacturer authorisation form signed by the manufacturer and naming the exact model and the bidder. Manufacturer warranty and support for the whole term, and licences and support registered for GBM, with certificates provided.	M
	Performance (with the security features on unless stated)	
FW-03	Threat-protection throughput of at least 400 Mbps, measured with firewall, intrusion prevention, application control, malware protection and logging all enabled.	M
FW-04	NGFW throughput (firewall, intrusion prevention and application control) and intrusion-prevention throughput of at least 400 Mbps each.	M
FW-05	TLS inspection: throughput of at least 360 Mbps, at least 650 new inspected sessions per second, and at least 18,000 concurrent inspected sessions. Where the manufacturer does not publish new inspected sessions per second, the bidder provides the manufacturer's written confirmation of the figure. The bidder states the cipher suites and packet mix used in the manufacturer's test.	M
FW-06	Firewall-only figures (not scored beyond the minimum): throughput of at least 1 Gbps, at least 10,000 new sessions per second, and at least 500,000 concurrent sessions.	M
FW-07	IPsec VPN throughput of at least 200 Mbps and capacity for at least 60 concurrent remote users, with the test conditions stated.	M
FW-08	Headroom: the same hardware serves up to 60 staff and the link plan in Section 1 without replacement. Capacity can be increased in blocks of 10 users or devices at the rate-card price and added within 5 business days of a request.	M
FW-09	The bidder states what the firewall does when it runs short of resources: whether it keeps inspecting, blocks traffic, or passes traffic uninspected, and what alert it raises.	M
	Security features	
FW-10	Advanced threat protection: intrusion prevention, malware and ransomware blocking, and sandboxing or equivalent for unknown files, all in the subscription.	M
FW-11	Web, content, application, and DNS filtering, with categories and exceptions set by GBM.	M
FW-12	TLS inspection in two modes: certificate inspection for most traffic and deep inspection that can be applied to selected categories. The bidder supplies its recommended exclusion list (for example banking, health and messaging apps) and a plan for installing GBM’s certificate on devices.	M
	Connectivity	
FW-13	Dual internet links with automatic failover, link health checks, and policy-based routing. A second link is added later by GBM; the bidder configures it at the rate-card price.	M
FW-14	Segmentation into zones or VLANs (for example, staff, servers, guests) with default-deny rules between them.	M

ID	Requirement	M/D
FW-15	Remote-access VPN over IPsec (IKEv2) or SSL, as the bidder states, with multi-factor authentication through GBM's identity provider (Microsoft Entra ID, Google Workspace or equivalent), role-based access and automatic session timeout. The bidder states whether the VPN is the firewall's built-in VPN or a separate remote-access (agent or ZTNA) subscription, and if separate, shows the endpoint count and cost separately. A site-to-site tunnel to GBM's cloud-hosted ERP environment is set up when GBM asks.	M
	Management and logging	
FW-16	Centralised console with real-time monitoring and reporting. GBM staff get read-only access, and administrators get role-based access.	M
FW-17	Logs kept at least 12 months, stored in Kenya or a jurisdiction GBM approves, with no on-site log server needed. Monthly report covering blocked threats, top applications, VPN use and uptime.	M
	Optional items (priced on the rate card, not in the scored total)	
FW-18	A second appliance in a high-availability pair. The baseline is FW-28.	D
FW-19	Advice and configuration support when GBM adds a second internet provider.	D

3.2. Setup and Installation

- Delivery of the firewall to the designated location.
- Physical installation of the firewall within the existing network.
- Configuration of security policies tailored to GBM's operational needs, after an initial assessment of GBM's network.
- Integration with the current network infrastructure, devices, and sign-in.

ID	Requirement	M/D
FW-20	A dated deployment plan with a rollback step and a GBM approval point before cutover. GBM's target is go-live within 4 weeks of signing: assessment and configuration 1 week, deployment 1 week, testing, tuning and training 2 weeks. The bidder commits to a date in its bid.	M

3.3. Testing and Optimization

1. Comprehensive testing to ensure functionality, including intrusion detection, VPN performance, and traffic management.
2. Optimization of settings to balance security and performance.

ID	Requirement	M/D
FW-21	Testing before go-live: every rule validated, plus performance tests of traffic flow, VPN, intrusion inspection and filtering, with tuning.	M

3.4. Training

- Training of GBM's IT personnel on managing the firewall, monitoring traffic, and responding to security incidents.

ID	Requirement	M/D
FW-22	Training for two GBM ICT staff by the manufacturer or a certified engineer on the console, logs and reports, escalation and basic policy changes, plus documentation: configuration, administrator and user guides, support contacts and escalation path, and the reporting schedule.	M

3.5. Managed Service

Provision of a managed service plan that includes:

ID	Requirement	M/D
FW-23	24x7 monitoring of the appliance and the cloud service, with Severity 1 incidents handled within the response times below.	M
FW-24	Threat updates applied automatically. Critical firmware fixes are applied within 7 days, and within 72 hours if the flaw is being actively exploited, with written notice to GBM each time.	M
FW-25	Hardening: the management interface is never reachable from the internet, administrators use multi-factor authentication and named accounts, no default or shared passwords are used, and the configuration is backed up after every change.	M
FW-26	Change requests are handled within 1 business day (standard) or 4 hours (urgent). All changes need GBM's written approval and are logged.	M
FW-27	A quarterly review of firewall policies with a written report.	M
FW-28	Availability: a failed appliance is replaced or restored within 4 hours. The cloud layer is available at least 99.5% of the month.	M

Service levels. These are written into the contract.

Severity	Example	Response	Target fix or workaround
1. Critical	Internet or VPN down at head office, or the firewall has failed	30 minutes, 24x7	
2. High	Major function degraded, many users affected	2 hours, business hours	
3. Medium	Single-user or minor issue	4 hours, business hours	
4. Request	Standard change or information request	1 business day	

Each bidder proposes its own target fix or workaround time for each severity level in its draft SLA, according to its capacity. The times in the successful bid are written into the contract and used for the service credits.

Service credits. If monthly availability falls below the committed level (at least 99.5%), the bidder credits 5% of that month's fee for each 0.1 percentage point below it, up to 30%. Each missed Severity 1 response or fix time earns a credit of 2% of the monthly fee. Planned maintenance needs 5 business days' notice and may not exceed 4 hours a month. Availability below 99% in any 2 months of a 6-month period lets GBM terminate without penalty.

3.6. Data Protection and Exit

Data protection. The bidder acts as a data processor under the Kenya Data Protection Act, 2019 and signs a data processing agreement with GBM. It must be registered with the Office of the Data Protection Commissioner where the Act requires. It processes data only on GBM's instructions, keeps GBM data logically separate from other clients, tells GBM of any suspected breach without delay and within 24 hours at most, and does not move GBM data outside the agreed location without written consent. Logs and network data are confidential.

ID	Requirement	M/D
FW-29	On exit, the bidder gives GBM the full configuration and rule set within 14 days of a request, removes GBM data and issues a deletion certificate, and either removes the appliance or sells it at the buy-out price stated in Section 7. After the first 12 months GBM can end the contract on 90 days' notice. No exit fee applies beyond what the bidder priced.	M

4. Deliverables

1. Fully installed and operational firewall configured to GBM's requirements and tested.
2. Documentation, including:
   - Configuration details
   - User and administrator guides
   - Support, SLA and escalation contacts, and the reporting schedule
   - Warranty and support information, the manufacturer authorisation form, and licence certificates
3. Training completion report for the two GBM ICT staff.
4. Monthly service report and quarterly policy review report.
5. Signed data processing agreement.

5. Timeline

The project is expected to be completed within **4 weeks** from the date of contract signing:

- Assessment and configuration: 1 week
- Deployment and integration: 1 week
- Testing, tuning and training: 2 weeks
- Hardware delivery must be completed within the first 2 weeks.

The contract runs for 12 months and is renewable yearly, on satisfactory performance, for up to 36 months in total.

6. Vendor Requirements

Interested vendors must meet the following criteria. A bid missing any item is rejected before technical evaluation (pass or fail).

1. Authorised reseller or distributor of the proposed platform, shown by the manufacturer authorisation form in FW-02, which names the exact model and the bidder.
2. Proven experience delivering managed firewall or security services: three references from clients of similar size in the last 3 years, with contact names and numbers, and a contract, LPO or completion letter for at least two of them. Each reference should say how the bidder handled this year's firmware vulnerabilities. Experience in internet service provision alone does not count.
3. Capability to provide 24x7 monitoring, updates and incident response.
4. Certified technicians: at least two staff holding the manufacturer's current certification, and a named project lead and a deputy with a short CV and a copy of their current certificate. Certificates need no notarisation; GBM verifies them directly.
5. A Kenyan office and support staff.
6. Certificate of incorporation and CR12 showing directors and beneficial owners; a valid KRA tax compliance certificate and current business permit.
7. A signed bidder declaration (Annex C), including the Bribery Act, 2016 and conflict-of-interest statements.

7. Budget

Vendors are required to submit a comprehensive quotation using the table below with no lines added, removed or renamed. Prices are in Kenya shillings, excluding VAT, with VAT shown on the total line. Anything not priced is deemed included at no extra cost. Optional items are priced on the rate card, are left out of the total and the financial score, and are chosen by GBM after award. Bids are compared on the 36-month total because it includes hardware.

Item	Type	Unit price (KES, excl. VAT)	Quantity: 36 months	36-month total (KES)
Firewall appliance, by purchase (state model; write 0 if leased)	One-time		1	
Firewall appliance, by lease (write 0 if purchased)	Monthly		36	
Security subscriptions and manufacturer support for the appliance	Yearly		3	
Cloud or agent protection for remote devices for 40 field users	Monthly		36	
Assessment, configuration, testing and cutover	One-time		1	
Training for two GBM ICT staff and documentation	One-time		1	
24x7 monitoring and management, if not in the above	Monthly		36	
Total, excluding VAT				
VAT				
Total, including VAT				

Rate card (not scored, but binding for the contract term). Bidders state their price for: a second appliance in a high-availability pair (FW-18); configuration of a second internet link (FW-13, FW-19); each additional 10 users or devices per month (FW-08); additional site; additional VPN users; throughput upgrade; price of a 3-year prepaid subscription instead of yearly; buy-out price of the appliance at the end of year 1, year 2 and year 3; change requests beyond the included allowance; out-of-hours callout.

Commercial terms. All prices are in Kenya shillings and fixed for the first 12 months, including any hardware or subscription cost the bidder pays in dollars. Renewal prices are the year 2 and year 3 figures in the price template, and any increase beyond them is capped at 5% or the annual inflation rate published by the Kenya National Bureau of Statistics for the month before the renewal notice, whichever is lower, with 90 days' notice. Payment is monthly or quarterly in arrears, within 30 days of a correct invoice and a service report. Confidentiality, anti-corruption and the donor compliance conditions that apply to GBM are part of the contract.

8. Submission Requirements

Interested vendors must provide the following documents, as one technical proposal and one separate financial proposal, each as a PDF in separate files (or sealed envelopes if submitted in print):

1. Company profile and relevant experience.
2. Technical proposal, with no prices: understanding of GBM's environment; the compliance matrix (Annex B) with a datasheet or page reference for evidence on every line; the deployment plan with a timeline; the support model and a draft SLA covering fault logging, severity levels, response times,

escalation contacts and preventive maintenance. Keep it within 25 pages excluding annexes and datasheets.

3. Financial proposal, using the template in Section 7 and nothing else.
4. Proof of authorised dealership or partnership: the manufacturer authorisation form.
5. List and references of current clients, with the contract, LPO or completion letters required in Section 6.
6. Signed bidder declaration (Annex C) and the mandatory documents in Section 6.

Validity and rules. Bids stay valid for 90 days from the deadline. Late bids are not opened. GBM may ask a bidder to clarify, but not to change, its bid. Bid costs are the bidder's own. GBM may reject any bid above its available budget and may cancel the tender without liability.

---

9. Evaluation Criteria

Submissions are evaluated in three stages. The criteria and weights below are fixed when the tender is issued and are not changed after bids are opened.

1. **Preliminary check.** Mandatory documents in Section 6 and every M requirement in Section 3. Pass or fail.
2. **Technical score out of 100.** Bidders scoring below 70 are not opened financially.
3. **Financial score and award.** Financial proposals are opened only for bidders who passed stage 2.

Technical criterion	Marks
Compliance with the requirements, including desirable items	25
Relevant experience and verified references	30
Deployment plan and timeline	10
Qualifications of the named team and certifications	10
Support model and draft SLA (fault logging, severity levels, response times, escalation contacts, preventive maintenance)	15
Security, backup and data protection approach	10
Total	**100**

Performance claims are checked against the manufacturer's datasheet. A figure that is missing its test conditions, or that does not match the datasheet, counts as non-compliant for that line. Experience marks go only to references that can be verified: a reference with no contract, LPO or completion letter scores zero, and experience in internet service provision does not count. The final mark is 60% technical and 40% financial.

Final mark (out of 100) = 0.6 × technical score + financial score.

The financial score is calculated from the 36-month total cost including VAT (Section 7):

Financial score = 40 × (lowest total cost ÷ bidder's total cost)

The bidder with the highest final mark wins; a tie goes to the higher technical score. GBM will call all references and may ask shortlisted bidders for a demonstration. Evaluation is done by a panel of at least three GBM staff who sign a conflict-of-interest declaration, score independently on signed sheets, and then agree the result together. The scoring sheets are kept on file. All bidders are told the outcome in writing.

10. Contact Information

All inquiries should be addressed in writing to GBM Procurement Committee on this E-mail: **procurement@greenbeltmovement.org** no later than **16th October 2026 at 1700 hours**. Any inquiry made past this date will not be responded to. Answers are shared with every bidder. Contact with other GBM staff about this tender may lead to disqualification

Tender applications including technical and financial proposals must be physically submitted in sealed envelopes no later than **30th October 2026 at 1700 hours**. The application must be clearly labeled and the tender number**GBM/PR/HFNS/Oct/2026/001** indicated on the envelope, addressed to GBM Procurement Committee:

The Procurement Committee,
The Green Belt Movement,
Adams Arcade, Kilimani Road, Off Elgeyo Marakwet Road
P.O BOX 67545-00200, Nairobi

Note: ***Only inquiries are to be made through the E-mail and any full tender application sent through E-mail shall be rejected.***

Key dates

Step	Date
Tender issued	9th October 2026
Last day for written clarification questions	16th October 2026
GBM answers circulated to all bidders	20th October 2026
Bid submission deadline, 1900Hrs EAT	30th October 2026
Shortlisted bidders' demonstrations	16th November 2026
Notification of award	17th November 2026

Who may bid. Registered Kenyan companies, or foreign companies with a registered Kenyan entity and local support staff, that meet the mandatory requirements in Section 6.

Annex A: How the minimums were derived

The method counts users, then only the devices that have no user (printers, network phones, servers and other equipment), because a person's laptop and phone are covered by the per-user figure. The per-user and per-device rates are rules of thumb from industry sizing guidance.

Item	Calculation	Result
Users	Planning figure for the contract term	60
Devices without a user	3 today, plus planned CCTV (cameras and recorder) and spare capacity, rounded up for safety	20
New sessions per second, idle	60 users × 3 + 20 devices × 1	200
New sessions per second, peak	60 users × 7 + 20 devices × 2	460
Conservative ceiling, all staff devices counted (120 + 20 = 140)	Idle: 60 × 3 + 140 × 1. Peak: 60 × 7 + 140 × 2	320 idle, 700 peak
Concurrent sessions	100 per user or device: 100 × (60 + 20), ceiling 100 × (60 + 140)	8,000; ceiling 20,000
Threat-protection throughput (FW-03)	Link plan 200 Mbps × 2 directions	400 Mbps
TLS inspection throughput (FW-05)	90% HTTPS share × 400 Mbps	360 Mbps
TLS inspection new sessions per second (FW-05)	Ceiling peak 700 × 90% HTTPS share	630, minimum set at 650
TLS inspection concurrent sessions (FW-05)	Ceiling 20,000 concurrent sessions × 90% HTTPS share	18,000, minimum set at 18,000
Firewall-only new sessions per second (FW-06)	Ceiling peak 700 ÷ (1 − 0.91), allowing for the worst performance loss reported when features are switched on	About 7,800, minimum set at 10,000
Firewall-only concurrent sessions (FW-06)	Ceiling 20,000 ÷ 0.09	About 222,000, minimum set at 500,000
IPsec VPN (FW-07)	Link plan 200 Mbps; all 60 staff	200 Mbps, 60 users

Assumptions: the number of devices without a user; the link plan; the HTTPS share (90%); and the per-user and per-device session rates. If the link plan or the staff numbers change, the minimums scale with them.

Annex B: Compliance matrix

Bidders copy every requirement row from Section 3 and add the columns below. "Partial" or "No" on an M item disqualifies the bid. Evidence must be a datasheet or page reference, not a restatement of the requirement.

ID	Requirement	Product name and model (each component)	Comply (Yes / Partial / No)	How it is met	Evidence (document, page)
FW-01	[copied from Section 3]				

Annex C: Bidder declaration

To be signed by an authorised signatory on company letterhead. We, [company name], confirm that:

- We have read and accepted this Terms of Reference, including the service levels, data protection and exit terms.
- The information in our bid is true, and we will provide evidence on request.
- We have no conflict of interest with GBM staff, board members or evaluation panel members, or we have declared it in writing.
- We have not offered, and will not offer, any bribe, gift or improper inducement in connection with this tender, in line with the Bribery Act, 2016, and we will report any solicitation of a bribe to GBM management.
- We are not debarred or under investigation by any government or donor body.
- Our prices include all costs and remain valid for 90 days.

Field	Entry
Name	
Title	
Signature	
Date	
Company stamp	