REQUEST FOR PROPOSAL (RFP)

FOR SERVICES

Project Title:	**Next Generation Firewall Solution**
Nature of the services	Provision and maintenance of a Next Generation Firewall Solution (5-year plan)
Location:	Home-based with possible travel to SPC locations (Suva, Noumea, Honiara, Pohnpei, …)
Date of issue:	25/10/2024
Closing Date:	25/11/2024
SPC Reference:	RFP24-6712

Contents

PART 1: INTRODUCTION 3

1.1 ABOUT THE PACIFIC COMMUNITY (SPC) 3

1.2 SPC'S PROCUREMENT ACTIVITIES 3

1.3 SPC'S REQUEST FOR PROPOSAL (RFP) PROCESS 3

PART 2: INSTRUCTIONS TO BIDDERS 4

2.1 BACKGROUND 4

2.2 SUBMISSION INSTRUCTIONS 4

2.3 CLARIFICATIONS 5

2.4 EVALUATION 5

2.5 CONTRACT AWARD 5

2.6 KEY DATES 6

2.7 LEGAL AND COMPLIANCE 6

2.8 COMPLAINTS PROCESS 7

PART 3: TERMS OF REFERENCE 8

PART 4: PROPOSAL EVALUATION MATRIX 19

4.1 EVALUATION CRITERIA & SCORE WEIGHT 19

4.2 FINANCIAL EVALUATION 21

PART 5: PROPOSAL SUBMISSION FORMS 22

ANNEX 1: BIDDER'S LETTER OF APPLICATION 22

ANNEX 2: CONFLICT OF INTEREST DECLARATION 23

ANNEX 3: INFORMATION ABOUT THE BIDDER AND DUE DILIGENCE 25

ANNEX 4: TECHNICAL PROPOSAL SUBMISSION FORM 28

ANNEX 5: FINANCIAL PROPOSAL SUBMISSION FORM 31

Part 1: INTRODUCTION

1.1 About the Pacific Community (SPC)

The Pacific Community (SPC) is the principal scientific and technical organisation of the Pacific region, established by treaty in 1947 with the signing of the Agreement Establishing the South Pacific Commission (the Canberra Agreement).

SPC has our headquarters in Noumea, New Caledonia and has regional offices in Fiji, the Federated States of Micronesia and Vanuatu, as well as an office in France. SPC works across the Pacific and has staff in nearly all of our Pacific Island Country and Territory members.

SPC works for the well-being of Pacific people through the effective and innovative application of science and knowledge and is guided by a deep understanding of Pacific Island contexts and cultures. Our unique organisation covers more than 20 sectors and is renowned for knowledge and innovation in such areas as fisheries science, public health surveillance, geoscience and conservation of plant genetic resources for food security.

For more information about SPC and the work that we do, please visit our website: https://www.spc.int/.

1.2 SPC's procurement activities

SPC's procurement activities are guided by the principles of high ethical standards, value for money, open competition and social and environmental responsibility and are carried out under our Procurement Policy.

SPC's *Procurement Policy* provides the framework for ensuring that SPC obtains the best value for its purchases, in terms of both cost and quality; demonstrates financial probity and accountability to its members and development partners; manages and prevents the potential for conflicts of interest; reduces its environmental impact and manages any other risks.

At SPC, all procurement follows the same main steps: planning; statement of needs; requisition; solicitation; evaluation; award; receipt; and payment. Different procedures apply depending on the value of the goods, services and works to be procured.

For further information or enquiries about SPC's procurement activities, please visit the procurement pages on our website: https://www.spc.int/procurement or email: procurement@spc.int.

1.3 SPC's Request for Proposal (RFP) Process

At SPC, procurement valued at more than EUR 45,000 must be advertised through a Request for Proposal (RFP) with any bids received evaluated by SPC's Procurement Committee to determine the offer that provides the best value for money.

This RFP sets out SPC's requirements and it asks you, as a bidder, to respond in writing in a prescribed format with pricing and other required information. The RFP contains detailed instructions and templates to enable you to submit a compliant bid. It sets out the overall timetable; it confirms the evaluation criteria that SPC will use to evaluate proposals; it explains the administrative arrangements for the receipt of the bids; and it sets out how bidders can request further information.

Your participation confirms your acceptance of SPC's conditions of participation in the RFP process.

Part 2: INSTRUCTIONS TO BIDDERS

2.1 Background

SPC invites you to submit a bid to deliver the services as specified in **Part 3**.

SPC has advertised this RFP on its website and may send it directly to potential vendors. The same specifications, submission and other solicitation requirements will be provided to all vendors.

SPC has compiled these instructions to guide prospective bidders and to ensure that all bidders are given equal and fair consideration.

Please read the instructions carefully before submitting your bid. For your bid to be considered, you must provide all the prescribed information by the closing date and in the format specified.

2.2 Submission instructions

Your submission must be clear, concise and complete and should only include information that is necessary to respond effectively to this RFP. Please note that you may be marked down or excluded from the procurement exercise if your submission contains any ambiguities or lacks clarity.

Your proposal must include the following documents (annexes of Part 5 of the RFP):

a) Bidder's Letter of Application (Annex 1);
b) Conflict of Interest Declaration (Annex 2);
c) Information about the bidder and Due diligence (Annex 3);
d) Technical proposal submission form (Annex 4) and a technical memo consisting of:
    1. A presentation of your company
    2. CV and qualifications of the allocated personnel
    3. Presentation of the proposed solution
    4. 3 examples of similar contract or mission (in the last 5 years)
    5. Any other document to support your proposal
e) Financial proposal submission form (Annex 5) and the signed price schedule in PDF and Excel (Annex 5.1).

Your proposal must be submitted in **two separate emails**.

You must submit your **Technical proposal** (Annexes 1 to 4 and all their supporting documents) in English or in French as an attachment to one email. No financial information may appear in the technical proposal.

You must submit your **Financial proposal** (Annex 5) in a separate email. All prices in the proposal must be presented in **EUR or XPF**. Your Financial proposal is to be password protected. SPC will request the password in the event that it is required.

Both emails are to be sent to **procurement@spc.int** with the subject line of your email as: **Submission RFP24-6712 – Next Generation Firewall Solution**.

Your proposal must be received no later than **25/11/2024** by **8 am Noumea time (GMT + 11)**. Only one bid per bidder is permitted.

SPC will send a formal acknowledgement to each proposal received before the deadline.

SPC reserves the right to exclude from consideration any proposal not received by the deadline, with incomplete information or in incorrect form.

2.3 Clarifications

You may submit questions or seek clarifications on any issue relating to this RFP. The questions are to be submitted in writing to **procurement@spc.int** with the subject line: **Clarification RFP24-6712 – Next Generation Firewall Solution**. The deadline for submission of clarifications is **18/11/2024** by **8 am Noumea time (GMT + 11)**.

Details will be kept of any communications between SPC and bidders. This assists SPC to ensure transparency of the procurement process. While SPC prefers written communication in the RFP process, at any point where there is phone call or other conversation, SPC will keep a record or a file note of the exchange with prospective bidders.

2.4 Evaluation

Validity

Each proposal will be assessed for compliance with the submission requirements by the Bids Opening Committee. At this stage, basic due diligence will also be undertaken.

To assist in the examination, evaluation and comparison of proposals, SPC may ask the bidder for clarification of its proposal or additional information. The request for clarification will be in writing.

Technical

All valid proposals will be assessed against the technical evaluation criteria set out in Part 4. The criteria are provided with weighted scores according to the relative importance of each. SPC will not change the evaluation criteria set out in the RFP at any stage of the procurement process. Any changes in the evaluation criteria will result in the RFP process being re-issued.

Bidders are expected to familiarise themselves with local conditions and take these into account in preparing their proposal. Where minimum qualifications are set as specific evaluation criteria (which may include educational qualification, professional accreditation or certification, licensing, experience and expertise), proposals submitted must necessarily meet these criteria.

Shortlisted bidder's presentation

Bidders that are short-listed during the RFP evaluation process shall be required to conduct a presentation to, and respond to queries of, SPC's Procurement Technical Evaluation Committee. The bidders will be provided an opportunity to provide an overview of the operational aspect of the services they are proposing.

Financial

Any bids that pass the minimum technical evaluation requirements will pass onto financial evaluation.

During the financial evaluation, if there is a discrepancy between the unit price and the total price, the lower price shall prevail. If there is a discrepancy between words and figures the amount in words will prevail.

The total cost of the proposal must be submitted inclusive of taxes in accordance with the applicable legislation, and is not subject to revision.

2.5 Contract award

SPC may award the contract once the Procurement Committee has determined that a bidder has met the prescribed requirements and the bidder's proposal has been determined to be the most responsive to the RFP documents, provide the best value for money and best serve the interests of SPC.

SPC's *General Terms and Conditions of Contract* will apply to any contracts awarded under this RFP, unless otherwise agreed. Any requested changes to the General Terms and Conditions of Contract must be foreshadowed in the submission. In the absence of requests for changes, the General Conditions of Contract and the terms of the PSA contract shall be deemed to be known, understood, and accepted by the bidder.

The award of the contract will be made by contract signed and dated by both parties.

2.6 Key dates

Please see the proposed procurement timetable in the table below. This timetable is intended as a guide only and while SPC does not intend to depart from the timetable, it reserves the right to do so at any stage.

STAGE	DATE
RFP advertised	25/10/2024
Deadline for seeking clarification	18/11/2024
RFP Closing Date	25/11/2024

2.7 Legal and compliance

Child and vulnerable adult protection: SPC is committed to the well-being of children and vulnerable adults. All SPC contractors are required to commit to the principles of SPC's Child and Vulnerable Adult Protection Policy (XI.G Manual of Staff Policies). Breach of this requirement can result in SPC terminating any contract with a successful bidder. Any allegations of potential misconduct in relation to this RFP involving children or vulnerable adults should sent to complaints@spc.int.

Confidentiality: Unless otherwise agreed by SPC in advance or where the contents of the RFP are already in the public domain when **shared** with the bidder, bidders shall at all times treat the contents of the RFP and any related documents as confidential. SPC will also treat the information it receives from the bidders as confidential.

Conflict of interest: Bidders must take all necessary measures to prevent any situation of conflict of interest. You must notify SPC in writing as soon as possible of any situation that could constitute a conflict of interest during the RFP process. If you have any familial connection with SPC staff, this must be declared, and approval will then be sought for you to engage in the RFP process. Breach of this requirement can result in the exclusion of the bidder from the RFP process or in SPC terminating any contract with a successful bidder.

Cost of preparation of proposals: Under no circumstances will SPC be liable for any proposal submission costs, expenditure, work or effort that you may incur in relation to your provision of a proposal (including if the procurement process is terminated or amended by SPC).

Currency, validity, duties, taxes: Unless specifically otherwise requested, all proposals should be in EURO or Pacific Francs and must be net of any direct or indirect taxes and duties and shall remain valid for 120 days from the closing date. The successful bidder is bound by their proposal for a further 60 days following notification they are the preferred bidder so that the contract may be awarded. No price variation due to escalation, inflation, fluctuation in exchange rates, or any other market factors shall be accepted at any time during this period.

Eligibility: Bidders are required to disclose to SPC whether they are subject to any sanction or temporary suspension imposed by any international organisation, or whether they are subject to bankruptcy proceedings. You may not be bankrupt or suspended, debarred, or otherwise identified as ineligible by any international organisation. Failure to disclose such information may result in debarment and termination of any contract issued to the bidder by SPC.

Fraud and corruption: SPC has zero tolerance for fraud and corruption. All contractors have an obligation to report potential fraud and corruption. Breach of this requirement can result in the exclusion of the bidder from the RFP process or in SPC terminating any contract with a successful bidder. Allegations of potential misconduct by an SPC staff member or contractor involving fraud or corruption can be sent to complaints@spc.int.

Good faith: The information in this RFP is provided by SPC in good faith. No representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability will be accepted by SPC in relation to the adequacy, accuracy, completeness or reasonableness of this RFP or any information provided by SPC in relation to this RFP.

Modifications: Any clarifications, corrections or modifications will be published on the SPC website prior to deadline. In the event a bidder has submitted a bid before the clarification, correction or modification, the bidder will be informed and may modify the bid. The modified bid will still need to be received before the deadline.

No offer of contract or invitation to contract: This RFP is not an offer to contract or an invitation by SPC to enter into a contract with you.

Privacy: The bidder is to comply with the requirements of applicable legislation and regulatory requirements in force for the use of personal data that is disclosed for the purposes of this RFP. SPC will handle any personal information it receives under the RFP in line with its Privacy Policy, and the Guidelines for handling personal information of bidders and grantees.

Right to amend, seek clarity, withdraw, not award: SPC reserves the right to: (1) amend, add to or withdraw all or any part of this RFP at any time, or to re-invite bids on the same or any alternative basis; (2) seek clarification or documents in respect of any bidder's submission; (3) choose not to award a contract as a result of this RFP; (4) make whatever changes it sees fit to the timetable, structure or content of the procurement process, depending on approvals processes or for any other reason. Please note that while SPC will not change the evaluation criteria set out in the RFP without the RFP process being re-issued, SPC does reserve the right at the time of award of contract to vary the quantity of services and goods specified in the RFP and to accept or reject any proposal at any time prior to award of the contract without incurring any liability to the affected bidder or any obligation to inform the affected bidder/s of the grounds for SPC's action.

Right to disqualify: SPC reserves the right to disqualify: (1) any bidder that does not submit a proposal in accordance with the instructions in this RFP; (2) any bidder that misrepresents information to SPC; (3) any bidder that directly or indirectly canvasses any SPC employee concerning the award of a contract.

Use of material: Bidders shall not use the contents of the RFP or any related material for any purpose other than for the purpose of considering submitting, or submitting, a bid to SPC.

Warranty, representation, assurance, undertaking: The bidder acknowledges and agrees that no person has any authority to give any warranty, representation, assurance or undertaking on behalf of SPC in connection with any contract which may (or may not) follow on from this RFP process.

2.8 Complaints process

Bidders that consider they were not treated fairly during any SPC procurement process may lodge a protest. The protest should be addressed to complaints@spc.int. The bidder must provide the following information: (1) full contact details; (2) details of the relevant procurement; (3) reasons for the protest, including how the alleged behaviour negatively impacted the bidder; (4) copies of any documents supporting grounds for protest; (5) the relief that is sought.

Part 3: Terms of Reference

A. Background/context

Overview: Our organization seeks a Next-Generation Firewall (NGFW) solution to enhance our network security, safeguard sensitive data, and meet compliance requirements. We are looking to implement a technical Next Generation Firewall solution directly enhances the security and reliability of the Organization IT infrastructure. This RFP aims to identify a vendor capable of providing a comprehensive NGFW solution that aligns with our current infrastructure and future scalability needs. The chosen solution should offer robust security features, seamless integration, and ease of management.

Objectives: The objective of this RFP is to engage a vendor to deliver the required firewall solution. This competitive process allows us to evaluate the ability of the bidders to meet our security requirements, technical specifications, and budget constraints and deliver such a solution.

Geographical spread and logistics: The widespread geographical nature of the project, including diverse locations across Pacific Island Countries and Territories (PICTs), presents unique challenges in terms of delivery, installation, and maintenance. It demands a solution that is both versatile and reliable under varying conditions.

Challenges and Specificities: Our organization consists of 1 site in New Caledonia, 3 interconnected sites in Fiji and 2 additional satellites sites in Pacific Island Countries and Territories (PICTs): Pohnpei and Tonga. We require a solution that can protect against a wide range of threats, including advanced persistent threats, malware, and intrusion attempts. We also require features such as deep packet inspection, application control, intrusion prevention, and threat intelligence integration.

Bidder Participation Requirements: We encourage all vendors to respond with detailed proposals, including information on solution capabilities, architecture, deployment methods, and pricing models. Vendors should also provide customer references, case studies, and any relevant certifications to demonstrate their expertise in deploying NGFW solutions. Bidders are encouraged to propose solutions for one or more sites. However, if a bidder opts to respond for only one site, they must provide justification and demonstrate that they have explored and evaluated the feasibility of addressing multiple sites. This approach ensures a comprehensive consideration of the project's scope and encourages bidders to offer solutions that are scalable and adaptable to different locations.

Environmental and Social Responsibility: The project places a high emphasis on environmental and social responsibility. The chosen solution must align with these values, reflecting the organization's commitment to sustainable and ethical practices.

B. Functional Requirements

Requirement No	Type	Feature	Description
FR.01	Mandatory	Virtualization Capabilities	The NGFW solution must support virtualized instances for east-west communication within internal VLANs, enabling traffic filtering between users and servers. This capability is crucial across Noumea, Nabua.

FR.02	Mandatory	Dedicated/Physical Deployment	The solution must preferably a dedicated physical firewall units for north-south communication, providing a robust and secure gateway for internet and external connections.
FR.03	Mandatory	Basic Firewall Features	Include NAT, Bandwidth Management/Traffic Shaping, DMZ, DDOS protection, WAF, Virtual instances, QOS, and OSPF.
FR.04	Mandatory	Management Capabilities	A user-friendly management interface, supporting both GUI and command-line methods. Integration with AD, Entra, LDAP and IdP (OKTA) is required, along with secure remote management capabilities. Centralized cloud-based management is highly preferred to streamline configuration and monitoring across all sites.
FR.05	Mandatory	Centralized Management	The NGFW solution must be centrally managed, either through cloud-based or on-premises systems, for streamlined administration and monitoring.
FR.06	Mandatory	Advanced Security Features	Support for Layer 7 protocol rules, Application Firewall, TSL/SSL inspection, IPsec and GRE tunnels. The NGFW must be capable of handling advanced security features while maintaining high performance for both virtualized and physical deployments.
FR.07	Mandatory	Meshed WAN and MAN Support	Ability to create a meshed WAN over public internet and MAN links over private pathways, allowing flexibility in network design.
FR.08	Mandatory	Regular Security Updates	Regular updates to appliances and software, with a proven track record from the manufacturer. The NGFW must have advanced evasion technique detection and granular security capabilities.
FR.09	Mandatory	Security Features	The solution must provide a SIEM and XDR solution and/or being compatible with the major XDR and SIEM solution of the market.
FR.10	Mandatory	Reporting and Logging	Comprehensive reporting, including bandwidth, protocol, and endpoint-based data. Logging should be easily readable, with various formats and integration with SIEM and XDR systems. This should be available across virtualized and physical deployments.
FR.11	Mandatory	Physical Requirements	High Availability, stackable units, low noise, redundant PSUs, and suitable heat and power specifications. The physical units should meet these criteria for dedicated deployments.

FR.12	Mandatory	Performance and Throughput	The NGFW should support at least 500 Mbps throughput (1 Gbps preferred), with other throughput requirements specified in the given list (e.g., SSL VPN throughput, Firewall throughput, etc.). Ensure the virtualized instances meet similar performance standards.
FR.13	Mandatory	Cloud Proxy Integration	Ability to create GRE and IPsec tunnels to cloud proxy providers, allowing secure connectivity to external services. Inbound traffic support for cloud private access providers (e.g., Zscaler ZPA) is also required.
FR.14	Mandatory	Advanced Filtering Features	Web URL filtering, Malware filtering, IDS/IPS, Sandboxing, Client VPN access, and Cloud deployment options.
FR.15	Mandatory	VPN Solution	The NGFW should provide a VPN endpoint solution. This solution should ensure that the client automatically connect to the nearest endpoints or to a specific one if defined. The VPN gateway solution should also ensure that a VPN endpoints can also be deployed in the cloud and linked back to the firewall infrastructure to ensure staff abroad can connect to a close VPN Gateway in order to minimise the connectivity distance and RTT when VPN Access is needed. The VPN solution should also be capable of split-tunnelling to offload heavy traffic (like YT or Netflix) directly to the Internet instead of using the VPN link when connected to VPN endpoint.
FR.16	Optional	Site-Specific Requirements	The NGFW must be deployable across all specified sites: Suva, Fiji, Noumea, New Caledonia, Pohnpei, FSM, etc. This includes different buildings within the same site (e.g., Suva has multiple locations), emphasizing consistent deployment and security across these sites.
FR.17	Mandatory	Training for Network Administrators	Include comprehensive training programs for network administrators. The training should ideally lead to certification, ensuring that administrators are fully equipped to manage and maintain the NGFW network efficiently. This training should cover system management, troubleshooting, security protocols, and best practices.
FR.18	Mandatory	Vendor Support	Vendor support is crucial for the successful implementation and ongoing maintenance of the NFW solution. The support team must be located in the Pacific Region or as close as possible to ensure timely and relevant assistance. This proximity is essential for understanding local challenges and providing quick responses to service requests or technical issues.

FR.19	Mandatory	Management Capabilities	The NGFW solution should have the capability of managing each local NGFW node directly using a modern administration interface for the case that the Internet links are down and we need to some configuration change to overcome the situation and adapt the routing and rules.

C. Design Requirements

Requirement No	Category	Feature	Description
DR.01	Mandatory	Architecture Design	The NGFW architecture should support a mix of virtualized and physical deployments, accommodating east-west traffic (internal VLANs, user-server communication) and north-south traffic (external connections, internet access).
DR.02	Mandatory	Network Segmentation	The design must support robust network segmentation to ensure security between internal VLANs and controlled traffic flows across different segments. This is critical for east-west traffic filtering and should apply across all sites.
DR.03	Mandatory	High Availability	The NGFW design should include high availability (HA) configurations to ensure redundancy and minimize downtime, providing failover capabilities for critical infrastructure.
DR.04	Mandatory	Scalability	The NGFW design should be scalable to accommodate future growth in bandwidth, user count, and additional sites. The architecture should allow for easy expansion, both in terms of virtualized instances and dedicated hardware units.
DR.05	Mandatory	Centralized Management	The NGFW solution must offer centralized management, ideally from a cloud-based platform. This design aspect ensures consistent configuration, monitoring, and control across all sites, facilitating streamlined administration.
DR.06	Mandatory	Secure Remote Access	The design must support secure remote access for management and monitoring purposes. This includes integration with AD, Entra, LDAP and IdP for authentication, ensuring secure and controlled access to the NGFW system.
DR.07	Mandatory	Inter-Site Connectivity	The NGFW design must facilitate inter-site connectivity through secure tunnels (IPsec, GRE), allowing for meshed WAN and MAN configurations. This feature enables seamless communication between sites, with appropriate security and encryption measures.

DR.08	Mandatory	WAN load-balance	The NGFW must provide the ability to connect and load balance between multiple WAN links.
DR.09	Optional	WAN optimisation	The NGFW solution could provide WAN optimization capabilities in order to enhance the speed and the traffic send through the link
DR.10	Mandatory	Comprehensive Logging and Reporting	The design should include comprehensive logging and reporting capabilities, allowing detailed monitoring of network traffic, security events, and resource usage. Integration with SIEM systems and other monitoring tools is also required.
DR.11	Mandatory	Physical Infrastructure	The NGFW design must accommodate physical infrastructure requirements, including stackable units, redundancy in power supplies, and appropriate heat and noise levels. This is particularly relevant for dedicated units deployed for north-south communication.
DR.12	Mandatory	Performance Optimization	The NGFW design should ensure optimal performance, meeting or exceeding specified throughput requirements (e.g., Firewall throughput, SSL VPN throughput). The architecture should support high traffic loads while maintaining security and stability.
DR.13	Mandatory	Cloud Integration	The design should allow for integration with cloud-based services, including cloud proxy providers and cloud private access providers (e.g., Zscaler). This feature ensures compatibility with external services and cloud-based applications.
DR.14	Mandatory	Site-Specific Adaptability	The NGFW design must be adaptable to specific site requirements, including varying staff counts and connectivity needs. The design should accommodate both larger central sites (e.g., Suva, Noumea) and smaller satellite locations (e.g., Pohnpei, Solomons), ensuring consistent security and connectivity.
DR.15	Mandatory	Environmental and Social Responsibility	A strong emphasis will be placed on selecting products and brands that demonstrate a strong commitment to environmental and social responsibility. This includes use of recycled materials in product manufacturing, energy-efficient operation, compliance with international environmental standards such as Energy Star, RoHS, and WEEE, evidence of corporate policies prioritizing sustainable and socially responsible practices, and recyclable or eco-friendly packaging materials.

DR.16	Mandatory	Compliance with Regulations and Bans	Vendors must ensure their products are not listed on any prohibited or banned lists from major governing bodies, specifically: Products should not be on the United States National Defence Authorization Act (NDAA) banned list, must comply with all European Union restrictions and not be part of any ban list from European countries, adhere to data protection and privacy standards (GDPR, ISO 27001, etc.), comply with EMC standards and not interfere with other devices and services, and verify that the products do not originate from companies under trade restrictions or embargoes imposed by the United States, United Kingdom, Australia, New Zealand, or any European Union countries and also in PICTS.
DR.17	Mandatory	Power and Frequency Regulation Compatibility	It is crucial that the solution is compatible with the power and frequency regulations of the areas where they will be deployed. This includes adherence to electrical safety standards relevant to each location, compliance with environmental standards and regulations (RoHS, etc.), compatibility with the local power supply voltage and frequency specifications, and ensuring the APs can efficiently operate within the power regulation frameworks without causing interference or violating any regional electrical compliance requirements.
DR.18	Mandatory	Proposal Documentation	Vendors are expected to provide detailed information on their compliance with these requirements in their proposals, including certifications, product datasheets, and corporate responsibility reports. This approach ensures that the organization not only meets its technical and operational needs but also upholds its commitment to environmental stewardship and ethical practices.

D. Technical Requirements

Requirement No	Type	Feature	Description
TR.01	Mandatory	Firewall Throughput	The NGFW should provide a minimum throughput of 1 Gbps to support high-traffic environments. This applies to both virtualized and physical deployments, ensuring adequate bandwidth for different types of traffic.
TR.02	Mandatory	East-West Throughput	The NGFW must provide a minimum throughput of 40 Gbps with source, destination, protocols and packets filtering for east-west communication between internal VLANs, users, and servers

TR.03	Mandatory	Concurrent Sessions	The NGFW must support a minimum of 150,000 concurrent sessions to handle large numbers of users and connections.
TR.04	Mandatory	New Sessions Per Second	The NGFW should be capable of processing at least 8,000 new sessions per second to maintain efficient traffic flow during peak times.
TR.05	Mandatory	IPsec Tunnel Throughput	The solution must offer a minimum IPsec tunnel throughput of 500 Mbps to support secure inter-site communication.
TR.06	Mandatory	SSL VPN Throughput	The NGFW must support a minimum SSL VPN throughput of 500 Mbps, providing secure remote access for users.
TR.07	Mandatory	GRE Tunnel Throughput	A minimum throughput of 1Gbps for GRE tunnels is required to support meshed WAN configurations across public Internet pathways.
TR.08	Mandatory	TLS/SSL Inspection	The NGFW should support TLS/SSL inspection to ensure secure data transmission and detect encrypted threats.
TR.09	Mandatory	Object Management	The NGFW should provide a object management system when designing the ruleset. At best it should use the AD / Entra / LDAP security groups to groups the devices or users, or provide a way of grouping objects (devices, users, group of protocols, …) to ease the rule management and reduce the amount of rules in the system and allow a dynamic update of those groups either externally when connected to AD/Entra or internally if internally managed.
TR.10	Mandatory	Stateful Inspection and Packet Filtering	The NGFW must offer stateful inspection and robust packet filtering capabilities to control traffic flows and detect anomalies.
TR.11	Mandatory	Redundant Power Supplies	The NGFW hardware must include at least two redundant power supplies to ensure high availability and minimize downtime.
TR.12	Mandatory	High Availability Support	The solution should support high availability (HA) configurations for physical units, providing failover capabilities and reducing the risk of service interruptions.
TR.13	Mandatory	Integration with AD, LDAP and IdP providers	The NGFW must integrate with Active Directory, LDAP, Azure AD (Entra) and IdP (like OKTA) for authentication, providing secure and seamless user management. This is required for both management and remote access.
TR.14	Mandatory	Logging and Integration	The solution must offer comprehensive logging capabilities and support integration with SIEM systems, and external logging, graphing and alerting systems.

TR.15	Mandatory	Cloud-Based Centralized Management	The NGFW should support cloud-based centralized management, allowing for consistent configuration and monitoring across all sites.
TR.16	Mandatory	Physical Considerations	The NGFW hardware should meet specific physical requirements, including 1RU unit size, noise levels below 60 dBA, and operating temperature between 0-40°C and a relatively high humidity usually present in tropical areas.
TR.17	Mandatory	Support for Optional Features	The NGFW should support additional security features such as Web URL filtering, Malware filtering, IDS/IPS, and Sandboxing. These optional features enhance the overall security posture.
TR.18	Mandatory	Compatibility	The NGFW must be compatible with other products or systems it's expected to work with, including software, hardware, and connectivity standards.
TR.19	Mandatory	Lifespan	The NGFW should have a demonstrated lifespan that meets or exceeds the industry standard for similar products.
TR.20	Mandatory	Wear and Tear	The NGFW should maintain functionality and appearance after normal or even rigorous use.

E. Timeline

Timely Execution:

To ensure timely project execution, especially with the impending current Firewall as a Service solution timing in May 2025, is essential to ensure seamless transition before that date and avoid operational lapses.

F. Delivery Requirements

Delivery Timeline: The solution must be delivered within the specified timeframe agreed upon post-award. The urgency and critical nature of the deployment necessitate adherence to the project schedule to avoid operational disruptions.

Supply Chain Risks: Bidders must identify potential supply chain risks associated with the delivery of the physical system and propose viable mitigation strategies. This includes considerations for the current global logistics landscape, potential delays in manufacturing, and transportation challenges.

Compliance with Regulations: All products and services provided must comply with the SPC General Terms and Conditions of Contract, including insurance requirements, delivery terms, and any applicable legal and regulatory standards. This ensures that all contractual obligations are met and that the project adheres to established guidelines and best practices.

Customs and Quarantine Clearances: The bidder is responsible for managing all aspects of customs and quarantine clearances at the port of entry. This includes ensuring that all necessary documentation is prepared and submitted in a timely manner to facilitate smooth importation and compliance with local regulations.

Transportation Modes: The bidder must specify the modes of transportation used for the transfer of products, considering the most efficient and cost-effective options while ensuring the safety and integrity of the goods during transit.

Delivery Confirmation: Upon delivery, detailed checks will be required to confirm the receipt and condition of the product. This includes verification against the purchase order, inspection for damage, and confirmation that all components and documentation are included as per the technical specifications.

Penalties for Late Delivery: In the event of delayed delivery beyond the agreed timeline without prior approval or reasonable justification, penalties may be applied as specified in the contract. This clause is intended to ensure timely project execution and mitigate the impact of delays on operational efficiency.

Mitigation of Risks: Bidders should highlight any potential risks to the delivery schedule, including manufacturing delays, logistical challenges, or regulatory hurdles, along with proposed strategies to address these risks, ensuring proactive planning and risk management throughout the delivery process.

G. Warranty Requirements (when applicable)

Warranty Coverage: The solution must come with a comprehensive warranty covering defects in materials and workmanship for a minimum specified period post-deployment. This warranty should include clear terms regarding what is covered, the process for claiming warranty service, and the expected resolution time.

After-Sales Service: Detailed information on after-sales support services must be provided, including availability (hours/days), contact methods (phone, email, online portal), and the typical response time for addressing issues. The bidder must ensure that support is readily accessible and capable of resolving any issues promptly to minimize downtime.

Spare Parts Availability: The bidder must guarantee the availability of spare parts for all hardware components of the NGFW system for a period of 5 years. This ensures that any necessary repairs or replacements can be carried out efficiently, maintaining the system's operational integrity. The Organisation would however buy some spare part onsite to minimise any outage. A couple of essential non-user element could be purchased.

Software Updates: The proposal should include provisions for regular software updates to address security vulnerabilities, add new features, and ensure compatibility with evolving technology standards. Details on the frequency of updates and the process for their implementation should be provided.

Technical Support: Access to technical support services is essential for troubleshooting and resolving complex issues. The bidder must outline the levels of technical support offered (SLAs), including any tiered support structures, and the qualifications of the support personnel.

Training for Maintenance: To empower the organization's internal teams, the bidder should offer training on system maintenance and basic troubleshooting. This training can help reduce dependency on external support for minor issues and enhance system understanding.

Additional Services: Any additional warranty or support services beyond the standard offerings should be clearly described. This may include options for extended warranties, on-site support, dedicated account management, or customized service level agreements (SLAs) to meet specific organizational needs.

Warranty and Support Documentation: All warranty terms and after-sales support details must be documented clearly in the contract. This documentation should be easily accessible and serve as a reference for the organization to understand their entitlements and the procedures for accessing support services.

H. Reporting and contracting arrangements

Contract Terms and Conditions: A formal contract with the Organization is needed and will link the winning bidder and the Organisation for a period of five years. This contract need to outline the terms and conditions under which the Next-Generation Firewall solution will be provided, implemented, and supported. The contract will start from the date of contract execution. The contract term includes both the implementation phase and ongoing support and maintenance. The contract will specify the level of support and maintenance to be provided by the vendor throughout the five-year term. This includes:

- Regular software updates and security patches
- 24/7 technical support
- On-site assistance
- Scheduled maintenance and system health checks

Primary Contact: The contractor must designate a primary contact person or division responsible for overseeing the project's execution. This individual or team will serve as the main point of communication for coordinating activities, addressing concerns, and facilitating the smooth implementation of the NGFW system.

Reporting Frequency: The contractor is required to provide regular updates on the progress of the deployment. The frequency of these reports should be agreed upon at the project's outset, with options ranging from weekly to monthly, depending on the project phase and complexity. Critical milestones or phases may necessitate more frequent communication.

Content of Reports: Reports should cover the status of the project, including progress made, any issues encountered, and resolutions implemented. They should also forecast upcoming activities, highlight any potential risks or delays, and outline strategies for mitigation. The aim is to ensure transparency and keep all stakeholders informed and engaged throughout the project lifecycle.

Collaboration and Meetings: The contractor must identify key stakeholders within the organization with whom they will need to collaborate or meet regularly. This includes IT staff, project managers, and any other personnel whose input or cooperation is essential for the project's success. The contractor should outline how these interactions will be managed, including the scheduling of meetings, the format (in-person, virtual), and the expected outcomes.

Role of External Entities: If the project involves collaboration with external entities, such as telecom providers or third-party vendors, the contractor should describe the nature of this collaboration, including the roles and responsibilities of each party. This ensures that there is a clear understanding of how external contributions will be integrated into the project.

Documentation and Approval: The contractor must specify the process for obtaining approval or acceptance of deliverables at each stage of the project. This includes identifying who within the organization has the authority to sign off on work completed and the criteria for acceptance.

Change Management: The contractor should outline procedures for managing changes to the project scope, timeline, or budget. This includes how change requests are submitted, reviewed, and approved, ensuring that any modifications are documented and communicated effectively to all stakeholders.

I. Scope of Bid Prices and Schedule Payments

Comprehensive Cost Breakdown: Bidders must provide a detailed breakdown of all costs associated with the deployment of the NGFW solution (a price schedule is provided to the bidders to make their proposals). This includes, but is not limited to, hardware and software expenses, installation fees, training services, and any ongoing support or maintenance costs. The aim is to ensure transparency and allow for accurate budget planning.

Payment Milestones: Payment will be structured around clearly defined milestones that correspond to significant phases or deliverables within the project. Bidders are required to outline these milestones, along with the percentage of the total contract price allocated to each. This approach facilitates progress tracking and aligns payment with the achievement of specific outcomes.

Conditions for Payment Release: Specific conditions or documentation required prior to the release of payments for each milestone must be detailed. This could include the completion of installation, successful system testing, training completion, or other criteria that signify the fulfillment of contractual obligations.

Penalties and Incentives: Any penalties for late delivery or failure to meet specified requirements should be clearly stated, along with any incentives for early completion or exceeding project expectations. This ensures that the bidder is accountable for their performance and timelines.

Risk Mitigation for Price Fluctuations: Strategies to address potential fluctuations in costs or currency exchange rates during the project duration should be included. This could involve fixed-price agreements or clauses that outline how price adjustments will be handled, providing financial predictability for both parties.

Warranty and Post-Deployment Support Costs: Costs associated with warranty coverage and post-deployment support services should be explicitly stated. This includes the duration of the warranty, what is covered, and the cost of extended support services if applicable.

Milestone/deliverables	% payment
Initial Delivery of Equipment	30 %
Completion of Installation (1 or more sites)	20 %
Final Commission and acceptance	20 %
Training and Handover	30 %

J. Annexes to the Term of Reference

Number of Users per site:

Site Name	Number of User (approx)
GEM	70
Nabua	140
Lotus	150
Narere	105
Noumea	574
Solomon	10
Pohnpei	22

While SPC acknowledges that bidders may require undertaking an on-site discovery assessment in order to prepare their tender response, details of each site will be provided upon request.

Part 4: PROPOSAL EVALUATION MATRIX

4.1 Evaluation criteria & Score Weight

A two-stage procedure will be utilised to evaluate the proposals, with evaluation of the **Technical proposal** being completed prior to any **Financial proposal** being opened and compared.

The competencies which will be evaluated are detailed in Part 3.

The evaluation matrix bellow also reflects the obtainable score specified for each evaluation criterion (technical requirement) which indicates the relative significance or weight of the items in the overall evaluation process.

The technical component, which has a total possible value of 700 points, will be evaluated using the following criteria.

Evaluation criteria	Score Weight (%)	Points obtainable
Mandatory requirements		
1. Administrative Compliance: Includes submission of all required documents such as Bidder's Letter of Application, Conflict of Interest Declaration, etc. 2. Financial Stability: Review of financial statements to assess the bidder's economic stability. Having sound financial statement audited over the last 5 years. 3. Demonstrated recent (last 5 years) experience ability and confidence in delivering service and support in the field of this RFP to large clients across multiple sites and locations preferably in the Pacific Region. Provide a minimum of 3 referees' reports. 4. Company Qualifications: Minimum 5 years of experience, staff qualifications, compliance with professional accreditations and certifications, etc. Provide evidence of technical expertise with relevant industry certifications. 5. Compliance and Standard: Adherence to international standards and regulatory requirements, including environmental and social responsibility	Bidders will be disqualified if any of the requirements are not met	
Technical requirements		
Solution Compatibility and Integration	14 %	98
Ability to integrate with existing systems and platforms, such as Active Directory, LDAP, and other identity management solutions and logging and		

reporting capability with integration to external logging, graphing and alerting systems. Ability to meet the following requirements: Solution with high availability, scalable horizontally and vertically, support of redundant WAN links and with direct node plus centralized management. Integrate a VPN solution: multiplatform clients/server and site2site IPSEC/GRE		
Security Features Advanced security capabilities like URL filtering, intrusion detection and prevention, deep packet inspection and threat intelligence integration.	14 %	98
Performance and Scalability Throughput requirements, concurrent session handling, and future scalability. 500 Mbps of combined minimum Internet throughput support for each node. Minimum of 500 Mbps VPN IPSEC and SSL throughput support for each node. Minimum of 1Gpbs for GRE tunnels throughput. Minimum of 1Gbps of firewall throughput support for each node. 40Gps of minimum combined East-West throughput for the sites with HCI solution. Minimum of 150k concurrent sessions with 8k new session/sec	14 %	98
Management and Usability Ease of management through GUI, cloud-based controls, and comprehensive reporting tools. Support object management in the administration interfaces.	14 %	98
Reliability and Support Vendor's support structure, SLA terms, availability of regional support, response times, and training provisions.	14 %	98
Innovation and Value-Add Ability to provide a comprehensive and turnkey solution with regional support and training. Unique features that provide additional value, such as energy efficiency, green procurement compatibility, or enhancements to operational efficiency.	16 %	112
Warranty and support		
Evaluation on the warranty coverage, after sales service offered, spare part availability, technical support, training, warranty documentation provided,…	14 %	98

Total Score	**100 %**	**700**
Qualification score	**70 %**	**490**

4.2 Financial evaluation

The financial component of the proposal will be scored on the basis of overall costs for the delivery of the services and financial incentives and benefits provided to SPC. The lowest financial proposal will be awarded maximum 300 points and other financial offers and incentives will be awarded points as per the formula below:

Financial Proposal score = (Lowest Price / Price under consideration) x 300

Part 5: PROPOSAL SUBMISSION FORMS

Annex 1: BIDDER'S LETTER OF APPLICATION

Dear Sir /Madam:

Having examined the Solicitation Documents, the receipt of which is hereby duly acknowledged, we the undersigned, offer to supply the required services for the sum as may be ascertained in accordance with the Financial Proposal attached herewith and made part of this proposal.

We acknowledge that:

- SPC may exercise any of its rights set out in the Request for Proposal documents, at any time;
- The statements, opinions, projections, forecasts or other information contained in the Request for Proposal documents may change;
- The Request for Proposal documents are a summary only of SPC's requirements and is not intended to be a comprehensive description of them;
- Neither the lodgement of the Request for Proposal documents nor the acceptance of any tender nor any agreement made subsequent to the Request for Proposal documents will imply any representation from or on behalf of SPC that there has been no material change since the date of the Request for Proposal documents, or since the date as at which any information contained in the Request for Proposal documents is stated to be applicable;
- Excepted as required by law and only to the extent so required, neither SPC, nor its respective officers, employees, advisers or agents will in any way be liable to any person or body for any loss, damage, cost or expense of any nature arising in any way out of or in connection with any representations, opinions, projections, forecasts or other statements, actual or implied, contained in or omitted from the Request for Proposal documents.

We undertake, if our proposal is accepted, to commence and complete delivery of all items in the contract within the time frame stipulated.

We understand that you are not bound to accept any proposal you may receive and that a binding contract would result only after final negotiations are concluded on the basis of the Technical and Financial Components proposed.

For the Bidder: *[insert name of the company]*
Signature: Name of the Bidder's representative: *[insert name of the representative]* Title: *[insert Title of the representative]* Date: *[Click or tap to enter a date]*

Annex 2: CONFLICT OF INTEREST DECLARATION

INSTRUCTIONS TO BIDDERS

What is a conflict of interest?

A conflict of interest may arise from economic or commercial interests, political, trade union or national affinities, family, cultural or sentimental ties, or **any other type of relationship or common interest between the bidder and any person connected with the contracting authority** (SPC staff member, consultant or any other expert or collaborator mandated by SPC).

Always declare a conflict

The existence of a potential or apparent conflict of interest does not necessarily prevent the bidder concerned from taking part in a tender process. **However, the declaration of the existence of such a conflict by the persons concerned is essential and allows SPC to take appropriate measures to mitigate it and prevent the associated risks.**

Bidders are therefore invited to declare any situation, fact or link which, to their knowledge, could generate a real, potential or apparent conflict of interest.

Declaration at any time

Conflicts of interest may arise at any time during the procurement process or the implementation of a contract (e.g. new partner in the project) or as a result of a change in personal life (e.g. marriage, inheritance, financial transaction, creation of a company). If such a relationship is found and could be perceived by a reasonable person as likely to influence a decision, a declaration of the situation is necessary. In case of doubt, a conflict situation must be declared.

Declaration for any person involved

A declaration must be completed for each person involved in the tender (principal representative of the bidder, possible subcontractors, consultant, etc.)

Failure

Failing to declare a potential conflict of interest may result in the bidder being refused a contract or placed on SPC's list of non-responsible suppliers.

DECLARATION

I, the undersigned, *[name of the representative of the Bidder]*, acting in the name and on behalf of the company *[name of the company]*, declare that:

☐	To my knowledge, I am not in a conflict-of-interest situation
☐	There is a potential conflict of interest with regard to my *[Choose an item].* relationship with *[name of the person concerned]* in his or her capacity as *position/role/personal or family link with the person concerned]*, although, to the best of my knowledge, this person is not directly or indirectly involved in any stage of the procurement process
☐	I may be in a conflict of interest with regard to my *[Choose an item]* relationship with *[name of the person concerned]* in his or her capacity as *position/role/personal or family link with the person concerned]*, as this person is, to the best of my knowledge, directly or indirectly linked to the procurement process
☐	To my knowledge, there is another situation that could potentially constitute a conflict of interest: *[Describe the situation that may constitute a conflict of interest]*

In addition, I undertake to:

- declare, without delay, to SPC any situation that constitutes a potential conflict of interest or is likely to lead to a conflict-of-interest;
- not to grant, seek, obtain or accept any advantage, whether financial or in kind, to or from any person where such advantage constitutes an unfair practice or an attempt at fraud or corruption, directly or indirectly, or constitutes a gratuity or reward related to the award of the contract;
- to provide accurate, truthful and complete information to SPC in connection with this procurement process.

I acknowledge that I and/or my company and/or my business partners who are jointly and severally bidding on the **RFP 24-6712** may be subject to sanctions such as being placed on SPC's list of non-responsible vendors, if it is established that false statements have been made or false information has been provided.

For the Bidder: *[insert name of the company]*

Signature:

Name of the representative: *[insert name of the representative]*
Title: *[insert Title of the representative]*
Date: *[Click or tap to enter a date]*

Annex 3: INFORMATION ABOUT THE BIDDER AND DUE DILIGENCE

Please complete the following questionnaire and provide supporting documents where applicable.

VENDOR INFORMATION			
Are you already registered as an SPC vendor?		☐ Yes	☐ No
1. Please provide information related to your entity.			
Company name	*[Enter company name]*	**Address**	*[Enter address]*
Director/CEO	*[Enter name of the executive person]*	**Position**	*[Enter position of the executive person]*
Business Registration/License number	*[Enter company registration/license number (or tax number)]*		
Date of business registration	*[Enter date of business registration]*		
Country of business registration	*[Enter country of business registration]*		
Status of the entity: ☐ For-profit entity (company), ☐ NGO, ☐ International organisation, ☐ Government body, ☐ University, ☐ Association, ☐ Research Institute, ☐ Other: *[insert details]*			
2. Please provide relevant documentation to support and verify the legal existence of the entity, the authority of its officer and proof of its address, such as:			
☐ Delegation of authority or power of attorney document ☐ Certificate of business registration/license ☐ Memorandum, Articles or Statutes of Association ☐ Telephone, water, or electricity bill in the name of the entity ☐ Bank account details bearing the name of the entity			
3. How many employees does your company and its subsidiaries have?	*[provide answer]*		
4. Do you have professional insurance against all risks in respect of your employees, sub-contractors, property and equipment?		☐ Yes	☐ No
If 'No', what type of business insurance do you have?	*[provide answer]*		
5. Are you up to date with your tax and social security payment obligations?		☐ Yes	☐ No
If 'No', please explain the situation:	*[Provide details]*		
6. Is your entity regulated by a national authority?		☐ Yes	☐ No
If 'Yes', please specify the name:	*[Insert name of the national regulation authority]*		
7. Is your entity a publicly held company?		☐ Yes	☐ No
8. Does your entity have a publicly available annual report?		☐ Yes	☐ No
Please send SPC your audited financial statement from the last 3 financial years if available			

DUE DILIGENCE					
9. Does your entity have foreign branches and/or subsidiaries?				☐ Yes	☐ No
If you answered 'yes' to the previous question, please confirm the branches:					
• Head Office & domestic branches				☐ Yes	☐ No
• Domestic subsidiaries				☐ Yes	☐ No
• Overseas branches				☐ Yes	☐ No
• Overseas subsidiaries				☐ Yes	☐ No
10. Does your entity provide financial services to customers determined to be high risk including but not limited to:					
Foreign Financial Institutions	☐ Yes	☐ No	Casinos	☐ Yes	☐ No
Cash Intensive Businesses	☐ Yes	☐ No	Foreign Government Entities	☐ Yes	☐ No

Non-Resident Individuals	☐ Yes	☐ No	Money Service Businesses	☐ Yes	☐ No
☐ Other, *please provide details:*			*[Provide details]*		
11. If you answered 'yes' to any of the boxes in question 10, does your entity's policies and procedures specifically outline how to mitigate the potential risks associated with these higher risk customer types?				☐ Yes	☐ No
If 'Yes', please explain how:	*[Provide explanation]*				
12. Does your entity have a written policy, controls and procedures reasonably designed to prevent and detect fraud, corruption, money laundering or terrorist financing activities?				☐ Yes	☐ No
If 'Yes', please send SPC your policy in English.					
If 'No', what process does your entity have in place to prevent and detect money laundering or terrorist financing activities?	*[provide answer]*				
13. Does your entity have an officer responsible for anti-corruption, or anti-money laundering and counter-terrorism financing policy?				☐ Yes	☐ No
If 'Yes', please state that officer's contact details:	*[Insert name and contact details]*				
14. Has your entity or any of its current or former directors or CEOs ever filed for bankruptcy?				☐ Yes	☐ No
If 'Yes', please provide details:	*[Provide details]*				
15. Has your entity or any of its current or former directors or CEOs ever been the subject of any investigations or had any regulatory or criminal enforcement actions resulting from violations of any laws or regulations, including those relating to money laundering or terrorism financing?				☐ Yes	☐ No
If 'Yes', please provide details:	*[Provide details]*				

SOCIAL AND ENVIRONMENTAL RESPONSIBILITY (SER)

16. Does your entity have a written policy, controls and procedures to implement its Social and Environmental Responsibility (SER) commitments?	☐ Yes	☐ No
If 'Yes', please send SPC your policy in English.		
If 'No', what process does your entity have in place to ensure your social and environmental responsibility?	*[provide answer]*	
Does your Policy or Process cover the followings? ☐ Child protection ☐ Human rights ☐ Gender equality ☐ Social inclusion ☐ Sexual harassment, abuse or exploitation ☐ Environmental responsibility		
Please, outline the major actions you have undertaken in these areas:	*[provide answer]*	
17. Does your entity have an officer responsible for Social and Environmental Responsibility (SER)?	☐ Yes	☐ No
If 'Yes', please state that officer's contact details:	*[Insert name and contact details]*	

SUPPORTING DOCUMENTS (where relevant)

• Business registration/license proof	☐
• Bank account details document	☐
• Address of the entity and Authority of officer proofs	☐
• Audited financial statement from the last 3 financial years	☐
• Fraud, corruption, anti-money laundering and counter terrorist financing Policy	☐
• SER Policy	☐

I declare that the particulars given herein above are true, correct and complete to the best of my knowledge, and the documents submitted in support of this form are genuine and obtained legally from the respective issuing authority.

I declare that none of the funds received or to be received by my company will be used for criminal activities, including financing terrorism or money laundering.

By sending this declaration to SPC, I agree that my business and personal information may be used by SPC for due diligence purposes. I also understand and accept that SPC will treat any personal information it receives in connection with my proposal in accordance with its Privacy Policy, and the Guidelines for handling personal information of bidders and grantees.

For the Bidder: *[insert name of the company]*
Signature: Name of the representative: *[insert name of the representative]* Title: *[insert Title of the representative]* Date: *[Click or tap to enter a date]*

Annex 4: TECHNICAL PROPOSAL SUBMISSION FORM

Please complete the tables below (detailed version of these tables can be found in the TORs):

Functional Requirements:

Requirement No	Type	Feature	Requirement included in service offering (yes, no, or comment)
FR.01	Mandatory	Virtualization Capabilities	
FR.02	Mandatory	Dedicated/Physical Deployment	
FR.03	Mandatory	Basic Firewall Features	
FR.04	Mandatory	Management Capabilities	
FR.05	Mandatory	Centralized Management	
FR.06	Mandatory	Advanced Security Features	
FR.07	Mandatory	Meshed WAN and MAN Support	
FR.08	Mandatory	Regular Security Updates	
FR.09	Mandatory	Security Features	
FR.10	Mandatory	Reporting and Logging	
FR.11	Mandatory	Physical Requirements	
FR.12	Mandatory	Performance and Throughput	
FR.13	Mandatory	Cloud Proxy Integration	
FR.14	Mandatory	Advanced Filtering Features	
FR.15	Mandatory	VPN Solution	
FR.16	Optional	Site-Specific Requirements	
FR.17	Mandatory	Training for Network Administrators	
FR.18	Mandatory	Vendor Support	
FR.19	Mandatory	Management Capabilities	

Design Requirements

Requirement No	Category	Feature	Requirement included in service offering (yes, no, or comment)
DR.01	Mandatory	Architecture Design	
DR.02	Mandatory	Network Segmentation	
DR.03	Mandatory	High Availability	
DR.04	Mandatory	Scalability	
DR.05	Mandatory	Centralized Management	
DR.06	Mandatory	Secure Remote Access	
DR.07	Mandatory	Inter-Site Connectivity	
DR.08	Mandatory	WAN load-balance	
DR.09	Optional	WAN optimisation	
DR.10	Mandatory	Comprehensive Logging and Reporting	
DR.11	Mandatory	Physical Infrastructure	
DR.12	Mandatory	Performance Optimization	
DR.13	Mandatory	Cloud Integration	
DR.14	Mandatory	Site-Specific Adaptability	
DR.15	Mandatory	Environmental and Social Responsibility	
DR.16	Mandatory	Compliance with Regulations and Bans	
DR.17	Mandatory	Power and Frequency Regulation Compatibility	
DR.18	Mandatory	Proposal Documentation	

Technical Requirements

Requirement No	Type	Feature	Requirement included in service offering (yes, no, or comment)
TR.01	Mandatory	Firewall Throughput	
TR.02	Mandatory	East-West Throughput	
TR.03	Mandatory	Concurrent Sessions	
TR.04	Mandatory	New Sessions Per Second	

TR.05	Mandatory	IPsec Tunnel Throughput	
TR.06	Mandatory	SSL VPN Throughput	
TR.07	Mandatory	GRE Tunnel Throughput	
TR.08	Mandatory	TLS/SSL Inspection	
TR.09	Mandatory	Object Management	
TR.10	Mandatory	Stateful Inspection and Packet Filtering	
TR.11	Mandatory	Redundant Power Supplies	
TR.12	Mandatory	High Availability Support	
TR.13	Mandatory	Integration with AD, LDAP and IdP providers	
TR.14	Mandatory	Logging and Integration	
TR.15	Mandatory	Cloud-Based Centralized Management	
TR.16	Mandatory	Physical Considerations	
TR.17	Mandatory	Support for Optional Features	
TR.18	Mandatory	Compatibility	
TR.19	Mandatory	Lifespan	
TR.20	Mandatory	Wear and Tear	

In addition to this technical proposal submission form (Annex4), please provide a technical memo consisting of:

1. A presentation of your company
2. CV and qualifications of the allocated personnel
3. Presentation of the proposed solution
4. 3 examples of similar contract or mission (in the last 5 years)
5. Any other document to support your proposal

For the Bidder: *[insert name of the company]*

Signature:

Name of the representative: *[insert name of the representative]*
Title: *[insert Title of the representative]*
Date: *[Click or tap to enter a date]*

Annex 5: FINANCIAL PROPOSAL SUBMISSION FORM

The financial offer must be submitted with the attached price schedule (Annex 5.1) in excel and .pdf format, dated, stamped/signed.

For the Bidder: *[insert name of the company]*
Signature: Name of the representative: *[insert name of the representative]* Title: *[insert Title of the representative]* Date: *[Click or tap to enter a date]*