INVITATION TO TENDER

ECMWF/ITT/2026/381

FRAMEWORK FOR PROCUREMENT OF NETWORK SECURITY LAYER

Volume II:

Specification of Requirements

ISSUED BY: ECMWF Administration Department Procurement Section
Date: August 2026
Version: Final

Table of Contents

Definitions

Definitions and acronyms used in this Invitation to Tender (ITT), i.e.: this document and its annexes, are listed here:

Acronym	Definition
BoM	Bill of Material
DC	Data Centre
ECMWF	European Centre for Medium-Range Weather Forecasts
EVPN	Ethernet Virtual Private Network
Framework (Agreement / Contract)	A master agreement or coordinated set of contracts that establishes the fundamental rules, terms, and pricing for future business or project transactions
Initial Purchase	List of items specified in Annex 1
ITT	Invitation to Tender
Lot	A list of specific items, that includes solution Requirements, hardware or services to be procured using the Framework resulting from this ITT
Lot 1	See “Initial Purchase”
Manufacturer	Original equipment manufacturer of the supplied hardware and software components
M&M	Management and Monitoring
MP-BGP	Multiprotocol Border Gateway Protocol
Network Security Layer	The set of infrastructures and services that are deployed across all of ECMWF sites to secure ECMWF’s mission-critical operations, systems and data, and support its digital resilience
OEM	Original Equipment Manufacturer
OOBM	Out-of-Band Management
Requirement	A singular documented physical or functional need that a design, product or process aims to meet
RFP	Request for Proposal
RFQ	Request for Quote
Security Control	Protective measures, technologies, and policies designed to protect ECMWF's IT infrastructure from unauthorised access, misuse, modification, or destruction
Tender	A response to this ITT
Tenderer	An organisation bidding for this ITT
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VXLAN	Virtual eXtensible Local Area Network

1. Background

1.1. Introduction

This Invitation to Tender (ITT) has been prepared by the European Centre for Medium-Range Weather Forecasts, (governed by its Convention and associated Protocol on Privileges and Immunities which came into force on 1 November 1975, and was amended on 6 June 2010) ("ECMWF") for the purposes of obtaining proposals from Tenderers for the procurement of a Network Security Layer.

ECMWF acquired its existing Network Security Layer infrastructure and services under an agreement that will expire late 2026.

1.2. ECMWF's Network and Security Infrastructure

ECMWF's network and security infrastructure is deployed in the Bologna Data Centre (DC) and the three office campuses: HQ in Reading and duty stations in Bologna and Bonn. The Network Security Layer component of the network and security infrastructure is deployed across all these environments to secure ECMWF's mission-critical operations, systems and data, and support its digital resilience. It includes an Out-of-Band Management network (OOBM) that is deployed in all these locations.

The following diagram provides a high-level overview of ECMWF's current Network Security Layer deployment across all its environments.

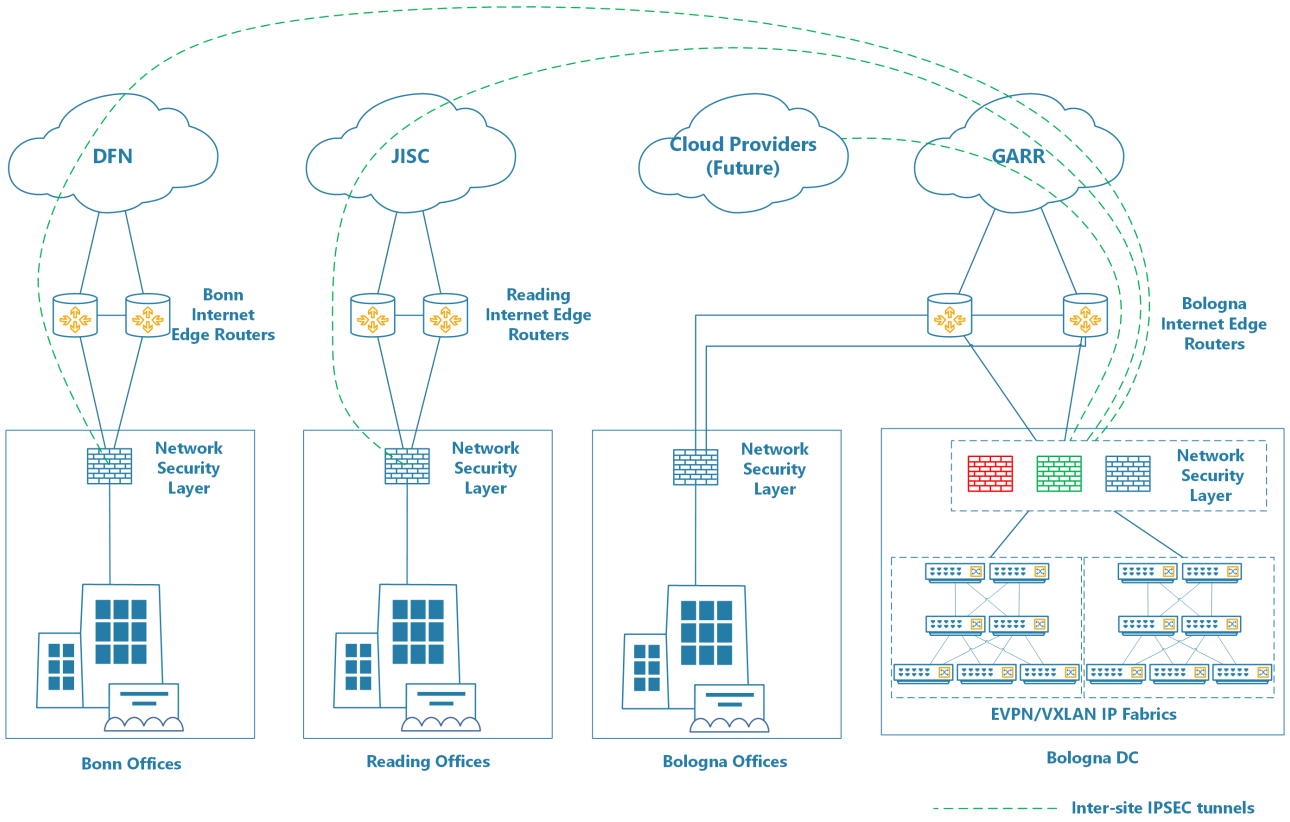

Figure 1: High-level diagram for ECMWF's current Network Security Layer

1.3. The Data Centre Environment – DC

ECMWF's Bologna DC environment consists of multiple interconnected IP Fabrics, with some IP Fabrics using Ethernet Virtual Private Network / Virtual eXtensible Local Area Network (EVPN/VXLAN) technologies, and some being pure Network Layer (L3) IP Fabrics. Logically, the network is broken down into different security zones to segregate systems of different type / different security environments. At the network level, this is achieved by having multiple Virtual Routing and Forwarding (VRF) instances configured on the IP Fabrics. All

traffic is allowed to pass freely within each VRF, and the traffic between VRFs must pass through the firewalls. The firewalls are attached as a "firewall-on-a-stick" rather than in-line, so that they could be bypassed for specific data flows. The firewalls actively participate in the routing topology and are used to exchange routing information between VRFs, using Multiprotocol Border Gateway Protocol (MP-BGP).

1.4. The Data Centre Management and Monitoring Environment – M&M

ECMWF's Bologna DC Management and Monitoring environment (M&M) consists of two interconnected collapsed core networks. Logically, each Management and Monitoring network is broken down into different security zones to segregate systems of different type / different security environments. At network level, this is achieved by having multiple VRF instances configured on network devices. All traffic is allowed to pass freely within each VRF, and the traffic between VRFs must pass through the firewalls. The firewalls are attached in-line, so that all the inter-VRF data flows must traverse them. The firewalls actively participate in the routing topology and are used to exchange routing information between VRFs, using MP-BGP. It is envisaged that future iterations of Management and Monitoring network will closely follow office campus environment blueprint.

1.5. The Office Campus Environment – Offices

Office campus environments consist of EVPN/VXLAN-based campus networks with topologies varying from IP CLOS Fabric to Collapsed Core, depending on size. Logically, each campus network is broken down into different security zones to segregate systems of different type / different security environments. At network level, this is achieved by having multiple VRF instances configured on network devices. All traffic is allowed to pass freely within each VRF, and the traffic between VRFs must pass through the firewalls. The firewalls are attached in-line, so that all the inter-VRF data flows must traverse them. The firewalls actively participate in the routing topology and are used to exchange routing information between VRFs, using MP-BGP.

1.6. The Out-of-band Network Environment – OOBM

The Out-of-Band Management (OOBM) Network provides a dedicated, independent management infrastructure across the three Offices and the DC environments, ensuring secure access during outages affecting these environments. Each site is equipped with its own redundant firewall cluster to protect OOBM traffic and enforce strict access controls. Analysts connect through VPN tunnels that terminate on the OOBM firewalls, enabling controlled and encrypted access to the relevant environment. Core management devices such as routers, switches, console servers and critical servers are directly connected to the OOBM network, ensuring that they remain accessible for troubleshooting, configuration, and recovery operations independently of the in-band network infrastructures.

2. Scope of the ITT

2.1. Objective

This ITT is expected to result in the setting up of a Framework Agreement with multiple suppliers, with the ultimate purpose of securing the best value for money in the provision of equipment/software and its associated maintenance and support services, and other services to build a Network Security Layer that will be purchased and installed by ECMWF at its Data Centre located in Bologna and its three offices sites located in Reading, Bologna and Bonn.

The ITT will also include:

- professional services for the design validation and onsite engineer presence during the deployment phase if and when required;
- training of ECMWF staff.

The suppliers admitted onto the Framework will be invited to compete for future purchases of similar types of equipment to those specified in Section 2.2. The initial Framework will be for four (4) years with the possibility of extension for a further two (2) years. The Framework awards (i.e. inclusion of suppliers onto the Framework) are subject to approval by ECMWF's governing body, its Council, which meets in early December 2026, so Framework contracts with selected suppliers cannot be signed before then. ECMWF may reopen the Framework on a competitive basis at a later date to add additional suppliers to the Framework on the same conditions.

In addition, this ITT intends to place an order for an Initial Purchase (Lot 1) comprising equipment from the supplier providing the best solution and value for money for this Initial Purchase, which has also been selected for the Framework. The contract for the Initial Purchase is anticipated to be awarded in December 2026 as well.

Suppliers must submit Tenders to supply the Initial Purchase for inclusion onto the Framework.

2.2. Security Controls

The table below summarises the Security Controls envisaged as a minimum within the scope of the ITT. The following information is provided for each control:

- The name of the Security Control;
- The mitigated risks addressed by the Security Control;
- The functions and features associated with the Security Control;
- The environment(s) in which the Security Control may/will be activated: Data Centre (DC), Management and Monitoring (M&M), Offices and Out-of-Band Management (OOBM).

Security Control	Mitigated risk	Functions / features	Environment(s)
Application control	Identifies and controls application usage (e.g., blocking peer-to-peer apps, social media)	Identify/block specific applications Control app usage Enforce policies based on app categories	Offices
Firewall	Controls traffic based on policies, IP addresses, ports and protocols	Packet filtering Stateful inspection Port/protocol control Network segmentation NAT	DC M&M Offices OOBM
Intrusion Detection System (IDS)	Insider threats Early threat detection	Monitoring, analysis and alerting of malicious traffic	DC Offices
Intrusion Prevention System (IPS)	Exploitation of known vulnerabilities Network-based malware Unauthorised access attempts Command and control (C2) traffic	Detect/block network threats and exploits Signature-based detection Anomaly detection Real-time alerts	DC Offices
SSL Decryption	Hidden malware or C2 traffic in encrypted streams Evasion of inspection tools Data exfiltration over HTTPS Undetected phishing sites	Decrypt and inspect SSL/TLS encrypted traffic Certificate validation Prevent hidden threats in encrypted traffic	DC Offices
Remote Access VPN	Eavesdropping MITM attacks IP exposure Loss of confidentiality	Encrypted tunnelling User authentication Secure remote access IP masking	DC M&M OOBM
Site-to-Site VPN	Eavesdropping MITM attacks IP exposure Loss of confidentiality	Encrypted tunnelling User authentication Secure remote access IP masking IPSEC AH/ESP support	DC Offices

Web Application Firewall (WAF)	OWASP Top 10 threats (e.g., SQL injection, XSS) Unauthorized API access Application-layer DoS attacks Session hijacking	Protect web apps from attacks (SQL injection, XSS, CSRF) HTTP/HTTPS traffic inspection Application-layer filtering	DC
Web Filtering	Access to malicious websites (phishing, malware) Data leakage via web uploads Non-compliance with browsing policies Drive-by downloads	Block/allow websites by category or URL Enforce browsing policies Block malicious sites URL reputation filtering	Offices

Table 1: List of Security Controls

It must be noted that:

- Not all Security Controls listed in the above table are included in the Initial Purchase;
- Additional Security Controls or auxiliary functions may be included over time as deemed necessary to address evolving threats, operational Requirements, or compliance obligations.

2.3. Key principles applicable to the Framework

The following principles apply to this ITT and to the operation of the Framework Agreement established as a result of this procurement.

Supplier participation	Tenders may be submitted by suppliers based in any country, subject to the applicable supply, delivery and support Requirements. ECMWF notes a preference for suppliers based in ECMWF Member States.
Manufacturer coverage	Tenderers representing any Manufacturer may respond to this ITT. ECMWF does not intend to restrict the Framework to a single Manufacturer or technology approach, provided that the proposed solution meets the applicable Requirements.
Scope of Lot 1 and future Lots	The Initial Purchase under Lot 1 concerns ECMWF's Data Centre Network Security Layer Requirements. Future purchases under the Framework may cover other security technologies, services, manufacturers, quantities, technical specifications, locations or support requirements.
Participation in future competitions	Suppliers admitted to the Framework will generally be invited to compete for future Lots. However, Framework suppliers invited to participate in a future competition will not be obliged to submit a quotation or proposal.
Evaluation of future Lots	Each future Lot will be evaluated against the evaluation criteria specified in the relevant Lot documentation. Where relevant and proportionate, ECMWF may also take account of prior performance under the Framework, including timely delivery, installation, acceptance and contract performance.
Standards and delivery locations	Equipment and services must comply with the applicable standards, specifications and regulatory requirements for the relevant delivery location. While ECMWF intends to use the Framework for its Data Centre in Bologna (Italy) and its office sites in Reading (UK), Bologna and Bonn (Germany), requirements may also arise for other locations, including non-EU locations. Any location-specific Requirements will be stated in the relevant Lot documentation.
Administrative, legal or funding conditions	Certain future purchases may be subject to specific administrative, legal, funding or eligibility conditions. Any such conditions will be clearly stated in the relevant Lot documentation and will be taken into account in determining the suppliers eligible to participate in the relevant future competition.

2.4. Future purchase process under the Framework

During the lifetime of the Framework, ECMWF may make further purchases of equipment, software, support services, professional services or related Network Security Layer Requirements. Each future purchase will be treated as a separate Lot and will be described in the relevant Lot documentation.

For each future Lot, ECMWF will specify the scope of the requirement, including, as applicable, the solution Requirements, hardware, software, services, quantities, manufacturers, technical specifications, support Requirements, delivery locations, installation Requirements and acceptance criteria. The level of detail provided may vary depending on the nature and maturity of the Requirement.

Future purchases will generally be subject to further competition among the suppliers admitted to the Framework. ECMWF may, however, determine the most appropriate procurement route for a specific Lot, taking into account the nature of the requirement, operational urgency, compatibility considerations, manufacturer-specific constraints or other relevant factors. Where justified by the requirement, ECMWF reserves the right to negotiate with one or more suppliers admitted to the Framework.

Each future Lot will be evaluated in accordance with the evaluation criteria stated in the relevant Lot documentation. These criteria may differ from those applied to the Initial Purchase, depending on the scope and nature of the requirement. Where relevant and proportionate, ECMWF may also take into account the supplier's prior performance under the Framework, including delivery, installation, acceptance, service quality and contract management performance.

It is envisaged that the total value of purchases made under the Framework over its maximum six-year duration may reach €8 million. This figure is provided for information purposes only and represents ECMWF's current estimate of the potential maximum expenditure under the Framework. It does not constitute a commitment or guarantee of any minimum or maximum volume, value or number of future orders. Inclusion on the Framework does not confer any entitlement to receive future business, and any purchases made under the Framework will be subject to ECMWF's operational requirements, available funding and the procedures described in this ITT.

2.5. Evaluation Criteria and Award Methodology for Framework Admission and Initial Purchase (Lot 1)

Tenders will be evaluated based on the evaluation criteria and weights shown in the table below.

Evaluation criteria	Weight
Tenderer's Credentials - Financial standing and Legal organization - Track record and references - Partner accreditations, quality assurance processes and management systems	20%
Quality of Proposal - Compliance with technical Requirements - Overall quality and completeness of technical solution - Quality of resources proposed (dedicated account manager, other technical or professional staff) - Logistics arrangements (delivery, installation, acceptance) - Support/maintenance service and warranty conditions	50%
Pricing and Payment Mechanism - Prices quoted for the equipment - Appropriateness of pricing mechanism proposed - Acceptance of specific ECMWF Requirements in terms of currency	30%

Table 2: Evaluation Criteria for Initial Purchase (Lot 1) and inclusion onto the Framework

Tenderers must comply with all Mandatory Requirements and achieve a mark of at least satisfactory (i.e. 60%) for each high-level evaluation criterion in order to be considered for inclusion onto the Framework and award of the Initial Purchase (Lot 1).

The contract for the Initial Purchase (Lot 1) will be awarded to the Tenderer who has passed the criteria for inclusion onto the Framework and proposed the best solution meeting Lot 1 Requirements.

3. Tender Requirement Instructions

Tenderers should note that they need to ensure that all Requirements are fully addressed, since a partial response may not be considered or evaluated. This includes the Requirements present in this section, in the other sections, in the annexes and in all the other relevant documents.

In this document, Requirements are categorised by the bold notations M, H or R to the left of the pertinent section.

Requirement category	Definition
M	denotes a MANDATORY Requirement: a Requirement that must be adhered to, or a performance Requirement that must be met in order that the tendered solution can be accepted by ECMWF. ECMWF will not consider a tendered solution that fails to meet a mandatory specification Requirement (marked M) unless the Tenderer offers valid reasons why the feature in question is either unnecessary for, or irrelevant to, the tendered solution or is deemed as an improvement over that specified.
H	denotes a HIGHLY DESIRABLE Requirement. The extent to which any tender meets Requirements listed as highly desirable (marked H) will be one of the factors taken into account in selecting the winning tender. If offered, the feature must be included in the overall price of the tender.
R	denotes a REQUEST for information. A response must be given to all such requests. Requests for information (marked R) are intended to provide a description of the construction, philosophy, operation and the cost implications of the tendered solution in areas that are regarded as being of particular importance. A clear response to such requests will be of assistance to ECMWF in the tender evaluation process.

Tenderers must address the Requirements listed in the table below together with the Requirements listed in the other sections of this document in accordance with the relevant instructions.

ECMWF seeks focused responses, rather than responses which include a significant amount of standard marketing material. If the Tenderer wishes to include marketing material in the proposal documentation set, it should be provided as discrete documents and limited to only marketing material which is directly relevant to the response and marked as “Marketing Material”, however ECMWF may, at its sole discretion, not evaluate any such marketing material.

M(1). Unless stated otherwise, Tenderers must provide a response to each Requirement listed in Volume II in a Word copy of this Volume II document, and relevant Annex documents. Unless stated otherwise, the response to each Requirement must be no longer than 1000 words.

M(2). Tenderers must ensure that all Requirements in this ITT are addressed and a response, in electronic format, is posted to ECMWF’s eProcurement Portal prior to the deadline; partial responses will not be considered. N.B. efforts have been made to remove duplicate Requirements, where this may occur, Tenderers are still required to address the Requirement and/or reference the first response.

M(3). Tender documentation must be written in English.

4. Specification of Requirements

4.1. Framework Contract

4.1.1. Manufacturers and Pre-sales technical support

H(4). It is highly desirable that potential Tenderers can provide Security Controls from a range of Manufacturers and are capable of providing ECMWF with technical expertise and guidance in the selection of the most suitable product for future acquisitions of equipment. Tenderers are asked to indicate how they can help ECMWF in identifying and providing Network Security Layer solutions to meet its scientific and business needs.

H(5). To enable ECMWF to take advantage of future technology developments it is highly desirable that Tenderers can provide access for ECMWF staff to equipment of different types and from different Manufacturers for evaluation, testing and benchmark purposes prior to purchase. Tenderers should confirm whether they can provide this facility, the likely location of test equipment (e.g. Tenderers premises, Supplier's premises or at ECMWF) and the typical terms and duration of access.

4.1.2. Logistics arrangements

4.1.2.1. VAT Exemption

ECMWF is an international intergovernmental organisation exempt from VAT on substantial purchases within the scope of its official activities in its host countries (United Kingdom, Italy, Germany), its other Member States and certain Co-operating States. Consequently, ECMWF in such circumstances is not liable for VAT. Further information may be found in the "VAT Guidance Note for Suppliers" document published at the ECMWF Suppliers webpage[1].

4.1.2.2. Deliveries to ECMWF's Data Centre in Bologna, Italy, from non-EU countries

Tenderers should note that the successful supplier(s) will be responsible for managing and coordinating all logistics associated with the delivery of equipment to ECMWF sites, irrespective of the country of origin of the goods or the delivery destination. This includes compliance with all applicable import, export, customs, VAT exemption and other regulatory requirements.

Where deliveries are made to ECMWF locations in Bologna (Italy), Bonn (Germany) or Reading (UK), specific ECMWF procedures may apply to facilitate customs clearance and the application of VAT exemptions. Details of these procedures will be provided to the successful supplier(s), who shall remain responsible for ensuring that all shipments are handled correctly and in accordance with the applicable requirements.

M(6). Tenderers shall describe the arrangements they have in place for the delivery of equipment and related services. In particular, Tenderers shall explain how they manage international shipments, customs formalities, and import/export requirements, including any previous experience with deliveries involving VAT exemptions, customs reliefs, or similar arrangements.

4.1.3. Support, maintenance and other professional services

A feature of the Framework is that a Lot could be used to specify only support services for equipment. Full details of the equipment would be provided to those contracted under this Framework, including equipment types, serial numbers, duration and level of support and current support status of the equipment. This will allow ECMWF to acquire support on equipment which has reached the end of its initial support period, purchased either through this Framework or any other contract.

M(7). Tenderers must specify the technical support services they can provide and those they will provide directly and those that will be provided by the OEM Manufacturer. Tenderers must provide details

[1] https://www.ecmwf.int/en/about/suppliers

of the applicable support and service levels for each provider, together with any associated service credits that would apply if those levels are not achieved.

4.1.4. Resources allocated to the contract

R(8). ECMWF will require the Tenderer to offer a dedicated account manager responsible for the contract and for any other matters related to the service. They will be the conduit to access pre-sales support, both internally and potentially directly with the Manufacturer. Tenderers are requested to explain their approach to managing the overall Framework contract, if selected, as well as individual orders awarded as result of Lot competitions and how this would be implemented.

4.1.5. Pricing mechanism

R(9). Whilst the default currency for this ITT and any future purchases (i.e. Lots) is the Euro (€), in some of the Lots ECMWF may require suppliers to provide quotes in Pound Sterling (£). Respectively, for those Lots the Contractor's invoices shall be submitted in Pound Sterling (£) and payments by ECMWF to the Contractor shall be made in Pound Sterling (£). Such a Requirement shall be explicitly notified in the Lot documentation issued at that time. Tenderers are requested to confirm their willingness to be paid in Pound Sterling (£) when this is requested in a Lot, as well as explain the currency conversion mechanism they will apply to ensure that ECMWF is still obtaining good value for money.

H(10). It is highly desirable that Tenderers offer guaranteed levels of discount on the Manufacturer's list price for components that may be acquired under future Lots. Tenderers are requested to describe the proposed discount structure and explain how Manufacturer list prices would be made available to ECMWF on an ongoing basis throughout the duration of the Framework.

4.1.6. Terms and conditions of the Framework contract

M(11). The terms and conditions for this contract are provided in Volume IV of the ITT documentation. Tenderers are requested to use Section 6 of Volume III to indicate their level of acceptance of the proposed terms and conditions and to identify any requested deviations. The degree of acceptance of the terms and conditions will form part of the evaluation. ECMWF remains open to discussing and negotiating specific contractual provisions with the preferred Tenderer(s), where appropriate.

For future Lots, selected suppliers will be engaged under the terms and conditions of the Framework Agreement concluded with them. The applicable terms will be based on Volume IV and any agreed amendments, depending on the type of purchase. For equipment, the terms for Goods will be applicable, for support services the terms for Services will be applicable, and for equipment purchased with ancillary support services the terms for Goods will be applicable.

ECMWF may require additional or alternative terms in writing in relation to specific goods and/or services, which will be notified in the documentation issued for a future purchase (Lot).

M(12). Please note that as a result of ECMWF's immunity from jurisdiction, any contract, including any sub-contract and any ensuing contract between ECMWF and a third party (e.g. maintenance/support agreements), resulting from this ITT must contain an arbitration clause which is offered by ECMWF to all contracting parties. Tenderers are requested to explicitly confirm their willingness and ability to comply with this Requirement and describe their approach in ensuring that such contracts comply with the above Requirement. Further information may be found in the "ECMWF's status: Arbitration" document published at the ECMWF Suppliers webpage.

Where extending existing systems previously purchased under a Lot from this Framework, it will be the option of ECMWF to offer the equipment needed for such an extension to the winner of the original Lot. This is to avoid complications of support within a single system. If the original Tenderer is judged to be unable to provide a competitive price for the extension, the equipment needed will be offered onto the Framework

instead as a separate Lot. This will not prevent the winner of the original Lot from bidding for the said extension.

4.1.7. User acceptance testing

Any hardware or software solutions that are provisioned in the context of this contract will need to be successfully tested by ECMWF before they could be accepted. In general, the test criteria will be defined based on the M/H/R requirements for a specific Lot and the Tenderer's response to those requirements, but ECMWF reserves the right to include arbitrary tests designed to ensure that the proposed solution(s) can be successfully integrated into ECMWF environment.

M(13). The Tenderer must confirm that any hardware or software solution provided under the Contract will be subject to user acceptance testing by ECMWF, based on the requirements for the relevant Lot, the Tenderer's response to those requirements, and any additional tests required by ECMWF, and that successful completion of such testing shall be a precondition for ECMWF's acceptance of the solution.

M(14). The Tenderer must confirm that it will work with ECMWF to define a set of user acceptance tests, based on the requirements for Lot 1, the Tenderer's response to those requirements, and any additional tests required by ECMWF, and that successful completion of such testing shall be a precondition for ECMWF's acceptance of the solution proposed for Lot 1.

4.2. Initial Purchase

The items specified in Annex 1 comprise the Initial Purchase (Lot 1). Tenderers responding to this ITT must bid for this Lot. Tenderers are requested to provide a detailed quote including breakdown of components and services. Prices given will be considered as firm, fixed and valid for a period of not less than six (6) months after the Closing Date of the ITT. Delivery and installation will be to ECMWF's Data Centre in Bologna, located at DAMA - Tecnopolo di Bologna, Via Stalingrado 84/3, 40128 Bologna, Italy.

4.3. Agreements for future purchases

ECMWF shall issue a Purchase Order which shall constitute a supplement to the signed Framework Agreement, along with ECMWF's Request for Proposal/Quote (RFP/RFQ) issued as part of the future purchase process and the accepted proposal/quote of the selected supplier.

5. Format of the Tender response

5.1. Presentation and Order of the Tender

The Tender response shall be presented as separate documents, which are to be uploaded to the respective question on the eProcurement Portal, as follows:

- Completed Volume III (Template for Tenderers – Administrative Information);
- Completed copy(ies) of Volume II and associated Annexes.

Note that for any information that has been provided as part of the Tender, but not specifically requested by ECMWF, then ECMWF shall, at its sole discretion, decide whether to utilise that further information within its evaluation process.

5.2. Volume III

M(15). Volume III (Template for Tenderers – Administrative Information), which can be found under the ITT Online Questionnaire must be completed by the Tenderers for the following information:

- Legal Entity and Contact Person Information:

  Information on the legal, commercial or professional status of the Tenderer, as well as contact details of the person who can be contacted by ECMWF in relation to the Tender. The Tenderer should also attach a copy of the official Company Registration Document and provide complete and accurate information on the Tenderer's shareholding structure and, if applicable, full details of its parent organisations up to and including the ultimate parent organisation.

- Economic and Financial Capacity:

  Financial information on the Tenderer's organisation to enable us to evaluate the Tenderer's financial status.

- Staff Resources
- Experience and References
- Additional questions:

  A set of questions which seek either information or confirmation from the Tenderer.

- Terms and Conditions:

  The terms and conditions for this contract are provided in Volume IV of the ITT documentation. Tenderers are invited to indicate whether they accept the terms and conditions, accept them subject to reservations, or reject them. Any reservations or objections should be clearly identified and justified. ECMWF will consider such responses as part of the overall evaluation of the tender.

Annex 1. Initial Purchase (Lot 1)

Architectural Vision

DC network will undergo architectural evolution in 2026-2027, to ensure that it continues to support current ECMWF strategic needs as well as catering for upcoming projects Requirements. As such, the Initial Purchase or Lot 1 items are scoped to fulfil the Requirements of future DC Network Security Layer.

It is anticipated that the next DC network infrastructure will be an evolution rather than a radical change from the existing one. The changes can be summarized as follows:

1. Individual IP Fabrics will be physically interconnected via a high-speed DC core, rather than via direct physical interconnection;
2. Individual IP Fabrics will be modelled as separate logical networks / failure domains, to eliminate fate sharing. As such, the current vision is that broadcast domains (VLANs) would not be stretched across multiple IP Fabrics;
3. Data Centre Interconnect (DCI) will be built between individual IP Fabrics where same VRFs / security zones are present in multiple IP Fabrics;
4. Network Security Layer functions and some other auxiliary services (e.g. Load Balancing) will be removed from individual IP Fabrics and will be provided via a redundant pair of independent Services Blocks, each of which would host all the necessary Network Security Layer functions and auxiliary services to facilitate operation of the DC at full capacity;
5. East-West and North-South firewall features could be implemented on shared or dedicated security appliance clusters;
6. Application controls, IPS, IDS, SSL decryption, Web filtering, Remote Access VPN and Site-to-Site VPN features could be implemented as part of firewall appliance clusters or via dedicated cluster of appliances;
7. Security layer appliances may be implemented either “on-a-stick” or “inline”;
8. High-speed DC core will be used to provide transit between IP Fabrics / Services Blocks but will be purposefully kept very simple / unaware of VRFs.

Aside from the points above, it is envisaged that architecture will remain broadly the same, with EVPN / VXLAN being used as IP Fabric control plane / data plane and VRFs being used for macro-segregation of traffic into different security zones.

This architectural vision is illustrated in the diagrams below.

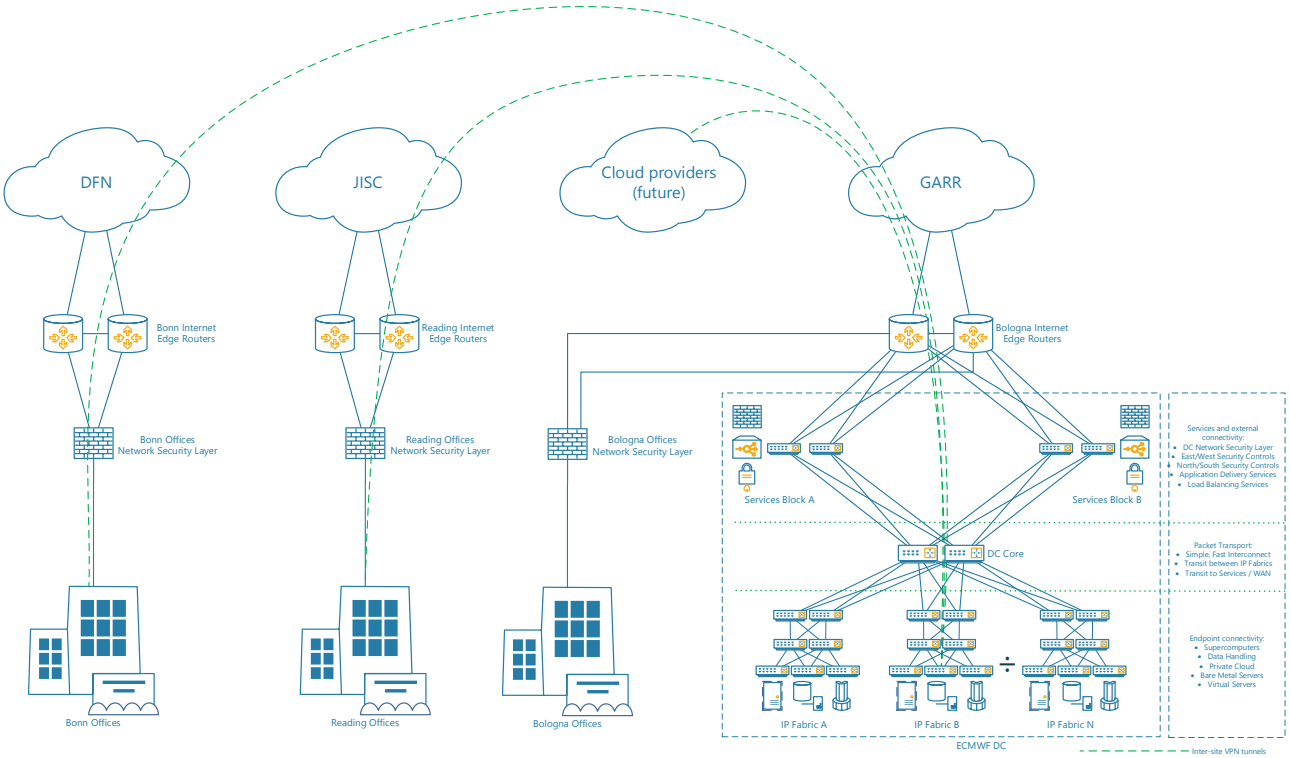

Figure 2: High-level diagram for ECMWF's Network Security Layer evolution – multisite topology

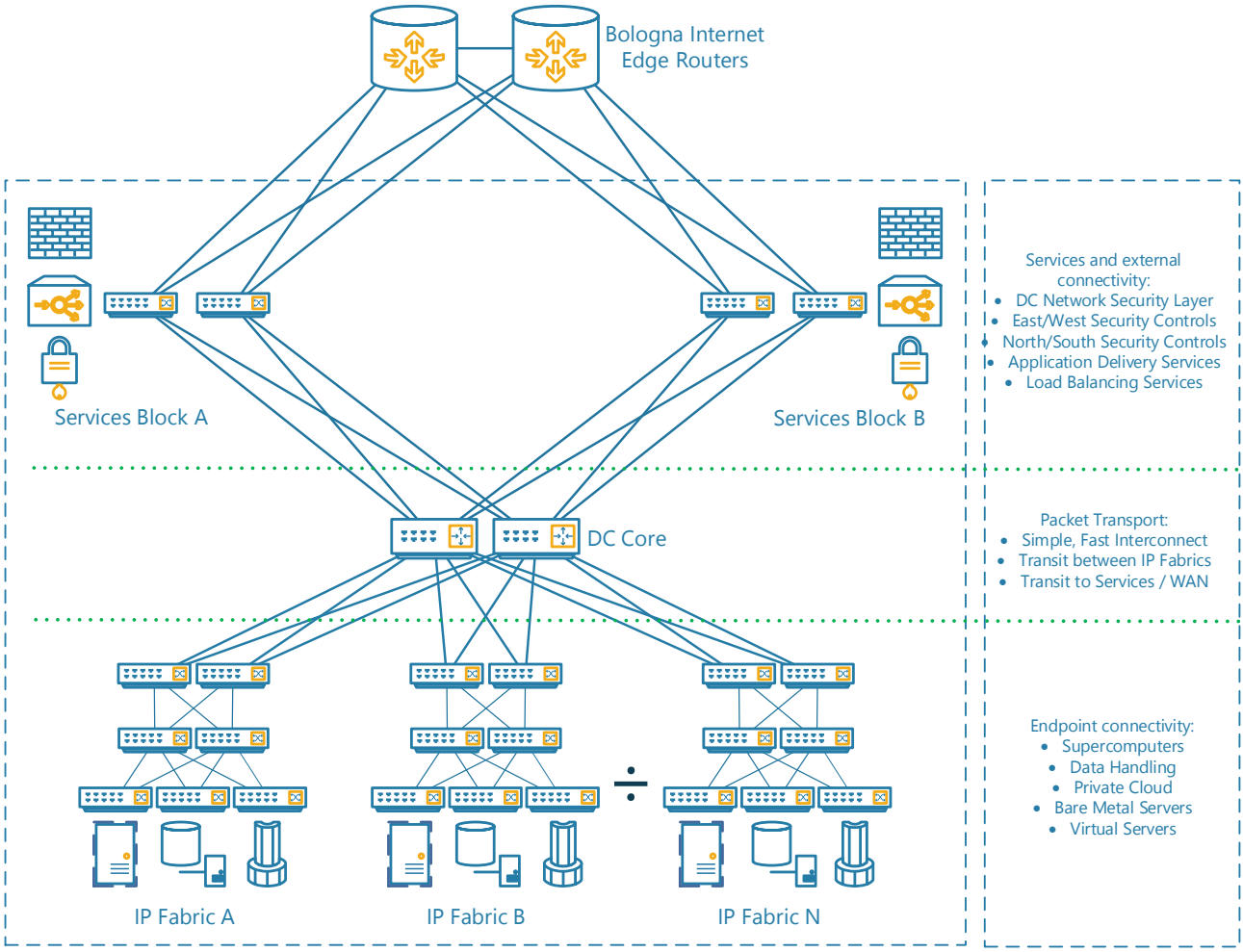

Figure 3: High-level diagram for ECMWF's Network Security Layer evolution – Bologna DC

Lot 1 is broken down into a series of items:

- Item 1 concerns Data Centre Network Security Layer appliances, providing Security Controls listed in the table below and proposal for this item must be provided by any Tenderer wishing to bid for Lot 1.
- Items 2 & 3 concern Security Controls that are provided by current Data Centre Network Security Layer appliances, but which could be provided by other means in the future. As such, Tenderers bidding for Item 1 are invited to optionally submit responses for Items 2 & 3, where the Requirements for those items could be met using the same Manufacturer as proposed for Item 1. It must be noted that the decision to include one or both of these two items in the initial order will be taken at a later stage.

Tenderers for Lot 1 must propose a solution to fulfil all the Requirements relating to Lot 1 from at least one and up to three Manufacturers.

For each item specified in this Annex, the Tenderer must provide a **detailed breakdown of components and costs for delivery and support in Bologna** using spreadsheet "BoM" annexed to this document. Prices shall be quoted in Euro (€).

M(16). Tenderers must complete a Word document copy of Volume II and spreadsheet "Volume II BoM" annexed to Volume II. If more than one solution is proposed, then separate Volume II and "Volume II BoM" spreadsheet must be completed for each additional solution.

M(17). Tenderers must provide and commit to the lead time for the delivery for Lot 1 after receipt of the Purchase Order pertaining to it.

M(18). Tenderers must commit to delivering all equipment pertaining to Lot 1 to ECMWF's Data Centre in Bologna, located at Tecnopolo di Bologna, Via Stalingrado 84/3, 40128 Bologna, Italy DAMA - Tecnopolo di Bologna, Via Stalingrado 84/3, 40128 Bologna, Italy.

Item	Description (Required technical specification / configuration)
1	**Data Centre Network Security Layer appliances.** Security Controls: • Network Firewall • Application controls • Intrusion Detection System (IDS) • Intrusion Prevention System (IPS) • TLS (SSL) Decryption/Inspection • Web Filtering See sections "Lot1/Item 1" below
2	**Data Centre Remote Access VPN functionality** Security Controls: Remote access VPN Constraint: use of the same Manufacturer as proposed for Item 1 See section "Lot1/Item 2 – DC Remote Access VPN" below
3	**Data Centre Site-to-site VPN functionality** Security Controls: Site-to-Site VPN Constraint: use of the same Manufacturer as proposed for Item 1 See sections "Lot1/Item 3 – DC Site-to-Site VPN" below

Lot 1/Item 1 – Proposed solution description

M(19). Tenderer must provide a summary of the technical solution or solutions that they propose to:

- Fulfil the network architecture described in section “Architectural Vision” above;
- Meet the Requirements listed in sections “Requirements for Lot 1/Item 1” below.

More than one solution can be proposed and only one Manufacturer can be used in each proposed solution. The response to this Requirement must be no longer than 2000 words for each proposed solution and diagrams are encouraged. The response for each solution should be focused on Requirements for this ITT and broadly cover the following areas:

a. Architectural overview (~50% or 1000 words)
b. Security control placement and high availability (~25% or 500 words)
c. Integration with ECMWF environment (~15% or 300 words)
d. Key design assumptions and constraints (~10% or 200 words)

R(20). Tenderers are invited to describe any additional features not listed in the ITT as Requirements, which the Tenderer feels may be relevant and beneficial to the proposed solution or solutions.

Lot 1/Item 1 – Throughput and performance

It is envisaged that future DC Network Security Layer will consist of multiple (at least two) sets of appliance clusters, one set per Service Block described in “Architectural Vision” section above. As such, the Requirements below should be provided **per set of appliance clusters,** rather than **per individual appliance**. Please note that unless explicitly stated otherwise, Requirements referring to DC Network Security Layer appliances apply to the overall proposed solution and may be fulfilled by one or more components within that solution.

M(21). Each set of DC Network Security Layer appliance clusters must provide minimum throughput / performance figures detailed in the table below. The figures are the combined total across all appliance clusters in a cluster set. Please note that equivalent architectures providing the same aggregate capacities may be proposed, subject to justification. The Tenderer must confirm that the solution(s) that they propose meets these Requirements:

Metric	Throughput / performance per cluster set
TCP Session Rate	>400K per second
TCP Sessions	> 4M
Throughput	≥800Gbps
Raw Stateful TCP (no NAT, no security)	≥800Gbps
Stateful TCP with NAT	≥400Gbps
TCP with Security (IPS)	≥100Gbps
TCP with Security (IDS)	≥100Gbps
Single TCP flow (RTT ≤ 1ms, MTU 9000)	≥10Gbps
Single TCP flow (RTT 20–30ms, MTU 1500)	≥10Gbps
SSL Inspection Throughput	≥100Gbps
SSL Inspection Concurrent Session	>1M
Network Scalability figures	
Number of BGP peers	>200
Number of prefixes	>100K
ECMP scale	4 next hops per prefix

H(22). It is highly desirable that each set of DC Network Security Layer appliance clusters would provide throughput / performance figures according to the table below. The figures are the combined total across all appliance clusters in a cluster set. Any caveats / deviations from the requested figures should be clearly stated by the Tenderer.

Metric	Throughput and performance per cluster set
TCP with Security (IPS)	≥200Gbps
TCP with Security (IDS)	≥200Gbps

Single TCP flow (RTT ≤ 1ms, MTU 9000)	≥20Gbps
Single TCP flow (RTT 20–30ms, MTU 1500)	≥20Gbps
SSL Inspection Throughput	≥200Gbps
SSL Inspection Concurrent Session	>2M
Network Scalability figures	
Number of BGP peers	>1000
Number of prefixes	>1000K
ECMP scale	8 next hops per prefix

Lot 1/Item 1 – Features and protocols

M(23). DC Network Security Layer appliances shall be capable of communicating with other systems using IPv4.

M(24). DC Network Security Layer appliances shall be capable of communicating with other systems using IPv6.

M(25). DC Network Security Layer appliances must support MP-BGP protocol, including IPv4 Unicast (AFI 1, SAFI 1) and IPv6 Unicast (AFI 2, SAFI 1) Address Families.

H(26). It is highly desirable that DC Network Security Layer appliances support MP-BGP protocol IPv4 Multicast (AFI 1, SAFI 2) and IPv6 Multicast (AFI 2, SAFI 2) Address Families.

H(27). It is highly desirable that DC Network Security Layer appliances support MP-BGP L2VPN EVPN (AFI 25, SAFI 70) Address Family.

M(28). DC Network Security Layer appliances must support BGP equal-cost multipath (ECMP).

H(29). It is highly desirable that DC Network Security Layer appliances support Virtual Routing and Forwarding (VRF) feature, to enable support for connectivity to multiple Security Zones.

M(30). DC Network Security Layer appliances must support BGP best path selection based on Local Preference, Local prefix injection, AS path length, Origin of the prefix, Multiple Exit Discriminator (MED), neighbour type and Interior Gateway Protocol (IGP) metric.

R(31). Tenderers shall give detail of how BGP route engineering on DC Network Security Layer appliances could be achieved by modifying the path selection criteria mentioned in Requirement M(30). or by use of communities via route maps / routing policies. It should be stated whether application of such policies is supported on per peering / direction / prefix basis.

H(32). It is highly desirable that DC Network Security Layer appliances support IGMPv3 and PIM-SSM protocols.

H(33). It is highly desirable that DC Network Security Layer appliances support inspection of VXLAN-encapsulated traffic.

H(34). It is highly desirable that DC Network Security Layer appliances support termination of VXLAN tunnels (i.e. act as a VTEP).

H(35). It is highly desirable that DC Network Security Layer appliances support Bidirectional Forwarding Detection (BFD) and any other protocol enhancements (BGP-based or otherwise), to aid in achieving faster network convergence after device / link failure.

R(36). Tenderers shall give details of any differences between IPv4 and IPv6 feature sets in terms of routing functionality (BGP / EVPN) and VRF / route scale.

M(37). DC Network Security Layer appliances must support fast failover (<10 seconds) in case of failure or scheduled maintenance of a cluster element with minimal disruption of traffic flow and performance

degradation. Tenderers shall give details of the methods used to achieve this, including timing estimates for the detection of network failure and network reconvergence time.

H(38). It is highly desirable that the aggregate bandwidths of 800Gbit/s can also be achieved when any one of the DC Network Security Layer appliances is unavailable.

H(39). It is highly desirable that the cluster capacity could be increased to at least double the figures specified in M(21) after the initial deployment, without major disruption. If this is possible, Tenderers should include relevant pricing / details / limitations.

M(40). The network connectivity from DC Network Security Layer appliances to other systems must, at a minimum, be based on 100Gbit/s Ethernet interface speeds.

H(41). It is highly desirable that the network connectivity from DC Network Security Layer appliances to other systems is based on 400Gbit/s Ethernet interface speeds.

H(42). It is highly desirable that DC Network Security Layer appliances support MTUs of >=9000 bytes for communication with other systems.

Lot 1/Item 1 – Management, administration and monitoring

M(43). The DC Network Security Layer appliances must support Multi Factor Authentication (MFA). The Tenderer is required to provide implementation details.

M(44). The DC Network Security Layer appliances must include a centralized management solution that provides the following features as a minimum:

- Configuration and policy management
- Device and firmware management
- Configuration revision control, enabling auditing
- MFA support

Tenderer must describe the solution and its implementation details and state any limitations to the features above.

H(45). It is highly desirable that a centralized solution for observability and trend analytics is provided for DC Network Security Layer appliances. The following features should be included:

- Data collection
- Data analytics and trends
- Reporting
- Minimum storage capacity of 72TB
- Capability to ingest 1TB of data per day at the minimum

Tenderer is required to provide implementation details and state any limitations to the features above.

Lot 1/Item 1 – Support of the Tendered Hardware and Software

M(46). Tenderers must explicitly undertake to provide spare parts and support for the hardware and software acquired under this ITT for at least five (5) years from the date of Contract signature. Where this involves an arrangement with the Manufacturer, responsibility for the provision of such support must in any case rest with the Tenderer.

R(47). Tenderers are invited to describe their policy regarding maintenance, spare parts and support for the hardware, firmware and software of the Initial Purchase (Lot 1) on reaching their respective end of life. In particular, any replacement policy or policies for components that will no longer be supported should be stated.

H(48). It is highly desirable that warranty / maintenance commitments would remain the responsibility of the selected supplier following a physical move of equipment from one of ECMWF's sites to another ECMWF's site. Tenderers are requested to confirm their ability to take on such a commitment and to describe their approach in successfully handling it.

Lot 1/Item 1 – Training

M(49). Tenderers must provide training and knowledge transfer programme, which must provide up to 10 ECMWF operational staff with sufficient understanding of the working of the software and hardware being tendered to enable them to provide effective day-to-day and emergency operational support including documentation, administrative tools, performance analysis, software upgrades and changes to configuration files.

R(50). Tenderers are invited to state which Manufacturer's and/or Tenderer's training programmes are available for ECMWF operational staff during the course of the Contract and state which of those have been included and costed for the Initial Purchase (Lot 1).

Lot 1/Item 1 – Transceivers and Cables

ECMWF would like to have the possibility to use non-OEM third-party transceivers. This section assesses the possibility and feasibility of doing so.

M(51). Tenderers must state what is their policy regarding support of third-party optic transceivers and direct attached cables.

M(52). Tenderers must specify whether the use of third-party optic transceivers and direct attached cables is possible in the proposed solution or solutions. Tenderers must also state the Manufacturer's policy in respect of such use.

R(53). Tenderers are invited to provide details of how support incidents will be handled if 3rd party optic transceivers and direct attached cables are being used on the Manufacturer's hardware.

M(54). Tenderers must confirm that the optic transceivers and direct attached cables used in the proposed solution or solutions are compatible with the proposed equipment.

M(55). Tenderers must confirm that the optic transceivers and direct attached cables used in the proposed solution or solutions are compliant with the applicable relevant standards.

M(56). Tenderers must confirm that all transceivers and direct attached cables undergo appropriate factory testing and post-coding validation. The tenderer must provide the details of testing / validation approach and evidence of testing / compatibility validation upon request.

M(57). Tenderers must confirm that in the event when optical transceivers and direct attached cables are excluded from support but purchased as part of the Contract, the optical transceivers and direct attached cables will fall under the standard warranty terms subject to the warranty period starting on the time of purchase.

H(58). It is highly desirable that limited lifetime warranty for the proposed transceivers and direct attached cables is five (5) years or more from the time of purchase.

H(59). Tenderers shall confirm that advanced product replacement for transceivers and direct attached cables is two (2) years or more from the time of purchase.

R(60). Tenderers are invited to provide information on failure rates of each transceiver and direct attached cables type of the proposed solution(s).

Lot 1/Item 2 – DC Remote Access VPN

M(61). The proposed solution must support secure remote access VPN functionality via either a native operating system client or a VPN client package that could be installed on Microsoft Windows and Apple Mac OS.

H(62). It is highly desirable that the proposed solution supports secure remote access VPN functionality via either a native operating system client or a VPN client package that could be installed on Linux, Android and Apple IOS.

H(63). It is highly desirable that the proposed solution support secure remote access VPN functionality via a web-based HTTPS portal hosted directly on the appliances.

M(64). Remote Access VPN functionality must support centralized user management for users authenticating to multiple VPN portals / appliances.

M(65). Remote Access VPN functionality must support password-based authentication with MFA.

H(66). It is highly desirable that Remote Access VPN functionality supports certificate-based authentication.

H(67). It is highly desirable that Remote Access VPN functionality supports phish-resistant MFA.

M(68). Remote Access VPN functionality must support at least 100Mbit bidirectional throughput per tunnel and 1Gbit aggregate throughput.

H(69). It is highly desirable that Remote Access VPN functionality supports at least 1Gbit bidirectional throughput per tunnel and 10Gbit aggregate throughput.

M(70). Remote Access VPN functionality must support at least 100 concurrent users and 1000 configured users.

H(71). It is highly desirable that Remote Access VPN functionality supports at least 200 concurrent users and 2000 configured users.

H(72). It is highly desirable that Remote Access VPN functionality supports both full tunnel and split tunnel implementations for client traffic

Lot 1/Item 3 – DC Site-to-Site VPN

M(73). The proposed solution must support secure site-to-site VPN functionality that supports IPSEC AH/ESP.

R(74). Tenderers are required to provide detail of any proprietary site-to-site VPN protocols and the advantages they may offer over IPSEC implementation.

H(75). It is highly desirable that the proposed solution supports establishment of eBGP peerings over site-to-site VPN tunnel to facilitate exchange of IPv4/IPv6 prefixes between tunnel endpoints.

M(76). Site-to-site VPN functionality must support password-based authentication of tunnel endpoints.

H(77). It is highly desirable that site-to-site functionality supports certificate-based authentication of tunnel endpoints.

M(78). Site-to-site VPN functionality must support at least 1Gbit bidirectional throughput per tunnel and 10Gbit aggregate throughput.

H(79). It is highly desirable that site-to-site VPN functionality supports at least 5Gbit bidirectional throughput per tunnel and 20Gbit aggregate throughput.

M(80). Site-to-site VPN functionality must support at least 10 concurrent tunnels.

H(81). It is highly desirable that site-to-site VPN functionality supports at least 50 concurrent tunnels.

Lot 1 – Pricing

ECMWF expects to see full pricing transparency in the Tender response and to be able to understand the figures first time without the need to clarify with the Tenderer in question.

Where applicable, please ensure that all and any conditions and/or restrictions are made explicit e.g. unanticipated expenditures (rush charges, etc.) and including the net pass-through of third-party costs/commissions/discounts.

M(82). Tenderers must quote prices on the following basis:

- Prices quoted by Tenderers in the Bill of Materials shall be firm and fixed;
- Prices should be firm and fixed for three (3) months after the closing date from receipt of Tenders and ECMWF can use these prices to place orders at Contract signature;
- Prices must be quoted in Euros (€) and ECMWF will use Euros (€) in the Contract;
- For purchases beyond the Initial Purchase, Tenderers must indicate the discount rate(s) that would be lied to the applicable catalogue/list prices. Any discount rate provided shall constitute the minimum discount guaranteed to ECMWF throughout the contract term and may be improved upon, but not reduced, for individual orders.

M(83). Tenderers must provide their pricing for the Bill of Materials for Initial Purchase using the "Volume II BoM" spreadsheet annexed with Volume II. Tenderers are invited to add as many lines as necessary to the spreadsheet to provide the pricing of all the elements required.

M(84). Tenderers must confirm that all related costs to cover all the items under Initial Purchase include the following:

- all hardware and software;
- all software licences relating to the Initial Purchase (if applicable);
- all maintenance and support services are required for 24 hours/day, 7 days/week for the equipment and software (if applicable) – support level options and associated SLAs must be detailed;
- delivery;
- training.

M(85). For the Initial Purchase, Tenderers must confirm that prices:

- encompass the costs of the mandatory features as described in this ITT;
- be quoted in Euros (€);
- be inclusive of shipping, delivery;
- be exclusive of all appropriate import duties and UK, German or Italian taxes.

H(86). Tenderers that use a reference Manufacturer's list price that is in a currency other than Euros (€) are requested to provide the currency exchange rate or rates applied to obtain the pricing in Euros (€).

M(87). Tenderers must provide quotes for different levels of the support services for the equipment listed in the "Volume II BoM" spreadsheet annex with Volume II provided for a period of one (1) year, three (3) years and five (5) years, assuming annual payments made at the start of each support service year.

H(88). In the case when third-party optic transceivers and direct attached cables are used in the proposed solution or solutions, Tenderers shall provide quote in the "Volume II BoM" spreadsheet annexed with Volume II document. Tenderers shall state the level of discount and mark-up off third-party list price.