REQUEST FOR INFORMATION

FOR A NETWORK SECURITY LAYER FOR ECMWF

ECMWF/RFI/2025/381

INSTRUCTIONS AND SPECIFICATIONS

September 2025

TRADEMARKS

All names or descriptions used in this Request for Information (RFI) that are trademarks, trade or brand names, or other references to proprietary products are hereby acknowledged as the property of their respective owners. No entry, term or definition in this RFI should be regarded as having any implication as to the validity or otherwise of any trademark.

The appearance of any proprietary name or reference in this document should not in itself be taken to imply a preference for one product over another unless specifically stated otherwise.

Table of Contents

Definitions

Definitions and acronyms used in this Request for Information (RFI), i.e.: this document and its annexes, are listed here:

AD	Active Directory
BGP	Border Gateway Protocol
DC	ECMWF Data Centre in Bologna
ECMP	Equal-Cost Multi-Path
ECMWF	European Centre for Medium-Range Weather Forecasts
EVPN	Ethernet Virtual Private Network
FIB	Forwarding Information Base
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPS	Intrusion Protection System
IPSEC	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITT	Invitation to Tender
LAG	Link Aggregation Group
L2VPN	Layer 2 Virtual Private Network
LDAP	Lightweight Directory Access Protocol
MP-BGP	Multiprotocol - Border Gateway Protocol
NAT	Network Address Translation
NLRI	Network Layer Reachability Information
Offices	ECMWF three office campuses: HQ in Reading and duty stations in Bologna and Bonn
OOBM	Out-of-Band Management infrastructure deployed in all of ECMWF three locations (Reading, Bologna and Bonn)
PIM-SSM	Protocol Independent Multicast - Source-Specific Multicast
PoC	Proof of Concept
RFI	Request for Information
RIB	Routing Information Base
RTT	Round-Trip Time
SSL	Secure Sockets Layer
TAP	Test Access Point
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VXLAN	Virtual eXtensible Local-Area Network
WAF	Web Application Firewall

1. Introduction

1.1. Purpose

The purpose of this Request for Information (RFI) is to provide information relevant to the procurement of a future Network Security Layer for the European Centre for Medium-Range Weather Forecasts (ECMWF), so that feedback from potential participants can be considered prior to issuing an Invitation to Tender (ITT).

This RFI has been written with the expectation that responses will primarily come from providers who would be able to respond to a future ITT for the provision of the complete or subset(s) of the service. However, the purpose, primarily, is to gather information. Responses are therefore welcome from providers of key technology elements.

Specifically, we seek to do the following:

- Identify technical specifications: help clarify the technical specifications of the hardware, such as performance and security features.
- Explore market landscape: provide insight into industry trends, available solutions, and vendor capabilities, allowing ECMWF to better understand the market.
- Establish the level of interest and capabilities of providers in working with ECMWF to achieve its goals and identify any barriers to providers responding to a future ITT.

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

The replacement Network Security Layer is currently expected to be installed in our Bologna data centre as well as at our three offices sites (Reading, Bologna and Bonn) at the end of 2026 and in the course of 2027.

ECMWF's goals can be found in the strategy. The current strategy for the period 2025-2034 is available here:

https://www.ecmwf.int/en/about/what-we-do/strategy

The purpose of the strategic review is to enable ECMWF to maintain its leading role in Numerical Weather Prediction by responding to fast-paced developments including:

- The evolution of Artificial Intelligence/Machine Learning (AI/ML) models and consequent disruptive changes to the value chain;
- The increasing relevance of environmental monitoring products and services for policy making;
- The development of initiatives to digitally enable environmental programmes such as the European Commission's Destination Earth and the opportunities and challenges for ECMWF and its Member States.

For this RFI, ECMWF is interested in the specification, configuration and indicative costs of building blocks that could be put together to provide security, resilience and the performance to meet the requirements of the ECMWF strategy.

1.2. Role of ECMWF

ECMWF is an independent intergovernmental organisation supported by 35 States. ECMWF is both a research institute and a 24/7 operational service, producing and disseminating numerical weather predictions to its Member States. The organisation was established in 1975 and now employs around 500 staff from more than 35 countries. ECMWF is one of the six members of the Co-ordinated Organisations, which amongst others also include the European Space Agency (ESA) and the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT).

Information on ECMWF's activities can be found at:

https://www.ecmwf.int/en/about .

ECMWF has headquarters in Reading, UK, with additional sites in Bologna, Italy, and Bonn, Germany.

1.3. Conditions for submission of a response

1.3.1. Disclaimers

This is an RFI issued solely for information and planning purposes and does not constitute a solicitation for a system. ECMWF does not commit to issue a related Invitation to Tender (ITT). ECMWF reserves the right to change the details of this RFI or withdraw this RFI at any time. Respondents are solely responsible for all expenses associated with responding to this RFI.

Nothing contained in this RFI, or any other communication made between the respondent and ECMWF, or its representatives shall constitute an agreement, contract or representation between ECMWF and any other party. Receipt by a respondent of this RFI does not imply the existence of a contract or commitment by or with ECMWF for any purpose.

While ECMWF has taken all reasonable steps to ensure, as at the date of this document, that the facts which are contained in this RFI are true and accurate in all material respects, ECMWF does not make any representation or warranty as to the accuracy or completeness or otherwise of this RFI, or the reasonableness of any assumptions on which this document may be based. ECMWF accepts no liability to respondents whatsoever and however arising and whether resulting from the use of this RFI, or any omissions from or deficiencies in this document.

ECMWF may use the information included in a response for any reasonable purpose connected with this RFI or any future ITT.

1.3.2. Timetable

This RFI will close at 14:00 UK local time on Tuesday 11 November 2025

ECMWF envisages the following schedule for this project:

30 September 2025	Issue of this RFI
1 – 28 October 2025	Written communication between ECMWF and vendors to clarify the RFI specifications
28 October 2025	Last date for submission of clarification questions for this RFI
11 November 14:00 UK local time	Close of RFI
January 2026	Issue of Invitation to Tender for new Network Security Layer
March 2026	Receipt of tenders
March – May 2026	Evaluation of tenders and negotiation of contract terms
	Selection of the winning tender
June 2026	Submission of the contract to ECMWF's Council for approval, followed by signature of the contract.
End of 2026/Beginning of 2027	Start of installation of new Network Security Layer

1.3.3. Confidentiality

The contents of this RFI together with all other information, materials, specifications or other documents provided by ECMWF, or prepared by respondents specifically for ECMWF, shall always be treated as confidential by the respondents unless it is already in the public domain. Respondents shall not disclose any such information, materials, specifications or other documents to any third parties or to any other part of the respondents' group or use them for any purpose other than for the preparation and submission of a response to this RFI nor shall respondents publicise ECMWF's name or the project without the prior written consent of ECMWF. Respondents shall ensure that all third parties to whom disclosure is made shall keep any such information, materials, specifications or other documents confidential and not disclose them to any other third party except as set out above.

ECMWF reserves the right to retain all documents submitted by respondents in response to the RFI. Any information in such documents that is proprietary and confidential to the respondent will be handled confidentially by ECMWF provided it is clearly and specifically identified as such. Such obligation shall not apply if such information is or was obtained from other sources that do not bind ECMWF as to confidentiality or if the information is in the public domain. ECMWF may make responses available for evaluation purposes to authorised people including its

governing body, committees, and professional advisers in addition to ECMWF's own personnel under the same conditions of confidentiality.

Please also note that all Personally Identifiable Information (PII) requested by ECMWF or provided by respondents will be treated in accordance with the ECMWF Policy on Personally Identifiable Information Protection (PIIP). It is available at https://www.ecmwf.int. ECMWF shall process all PII submitted in the response for the sole purposes of assessing the response. In doing so, ECMWF may share such PII with consultants or external advisors.

1.3.4. Enquiries and contact procedure.

In order to be kept up to date with any clarification responses or amendments to the RFI, the invitee is requested to confirm to the email address procurement@ecmwf.int whether or not it will be submitting a response and must provide a contact point and contact details to which email notification of the publication of any additional information will be sent. Please give the contact point's name, title, address and location, telephone number and email address.

Any other enquiries or requests for clarification of any matters arising from this RFI should also be sought from procurement@ecmwf.int and must be made in writing by email, no later than the last date for submission of clarification questions indicated in section 1.3.2

Where ECMWF supplies further information, it will make this information available to all recipients of this RFI who have indicated their intention to submit a response and provided ECMWF with an e-mail address for communication of additional information.

1.3.5. Format of the response

Annex 1 document is to be used to provide the response to this RFI. Please do not provide general advertising material with the response.

1.3.6. How to submit a response

Responses must be written in English.

The respondent must submit their response to RFI381@ecmwf.int as an email with attachments containing its complete response to this RFI. The attachments must contain a printable version of the response in Microsoft Word format, Rich Text Format (RTF) or Adobe Portable Document Format (PDF) and in Microsoft Excel format for any spreadsheets. The email should confirm that a duly authorised director or senior officer of the respondent has submitted the response.

The subject of the email must be:

Response to RFI/2025/381 for a Network Security Layer for ECMWF.

2. Contract length and timing.

ECMWF has typically procured the Network Security Layer under a service contract for an initial term of four (4) years. ECMWF shall have the option to extend on an annual basis thereafter to a maximum term of six (6) years.

3. Terms and Conditions - Arbitration and VAT

At the end of the ITT process, the terms and conditions of contract will be negotiated with the preferred bidder (s).

Suppliers should note that because of ECMWF's immunity from jurisdiction, any contract resulting from this future ITT must contain the following arbitration clause which is offered by ECMWF to all contracting parties.

Respondents are required to confirm their agreement to this clause in their response to the Annex 1 - Submission form.

"This Agreement [OR Contract OR Licence] is governed by and shall be construed in accordance with the laws of England and Wales. The parties shall attempt to settle any dispute between them in an amicable manner. If the dispute cannot be so settled, it shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by three arbitrators appointed in accordance with the said rules; sitting in London, England. The proceedings shall be in the English language and for the avoidance of doubt this arbitration agreement shall also be governed by the laws of England and Wales. In accordance with Sections 45 and 69 of the Arbitration Act 1996, the right of appeal by either party to the English courts on a question of law arising in the course of any arbitral proceedings or out of an award made in any arbitral proceedings is hereby agreed to be excluded.

Nothing in this Agreement [OR Contract OR Licence] is meant to be construed as a waiver of any of the privileges and immunities conferred upon ECMWF, an inter-governmental organization, through its Convention and Protocol."

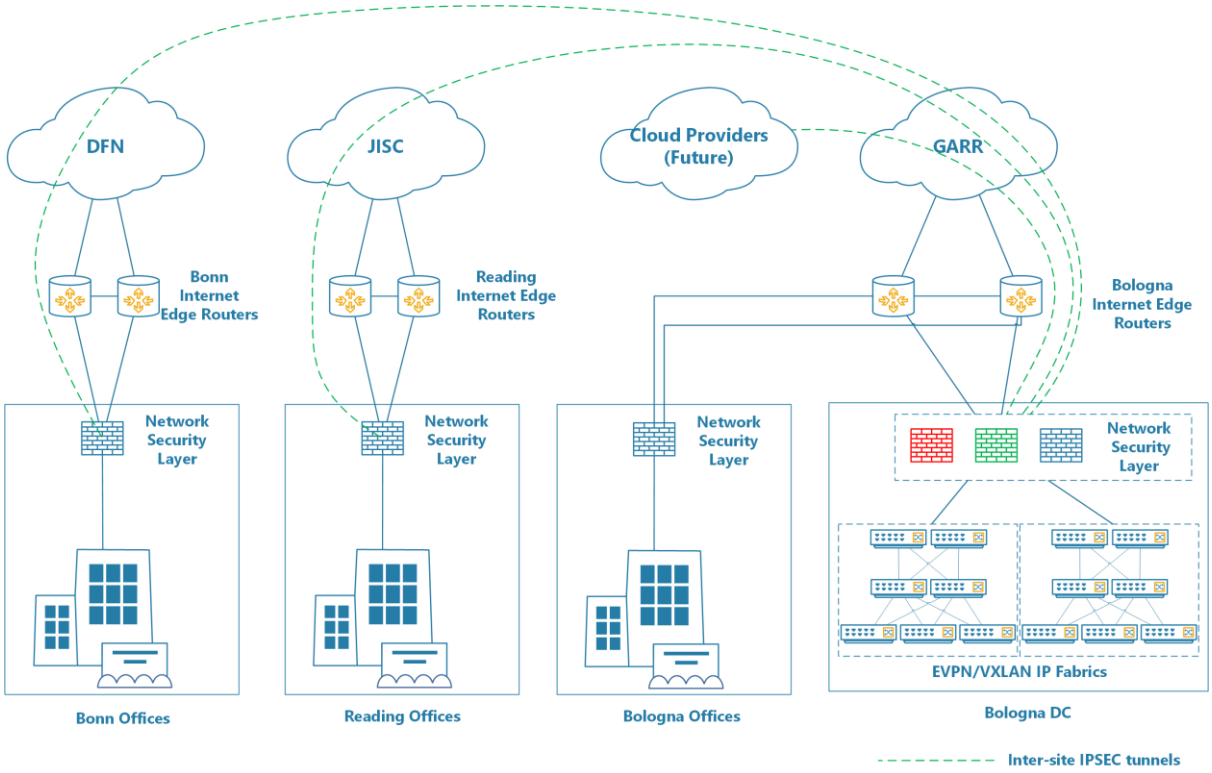
Please also note that ECMWF is exempt from VAT.

Further information may be found at http://www.ecmwf.int/en/about/suppliers in document "ECMWF's status: Arbitration and VAT".

4. Background

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 (Offices). 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 ECMWF's Network Security Layer deployment across all its environments.



4.1. The Bologna Data Centre Environment – DC

ECMWF's Bologna DC environment consists of multiple interconnected IP Fabrics, with some IP Fabrics using 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 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 MP-BGP.

4.2. 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 duty stations 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.

4.3. 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, 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.

5. Scope

ECMWF's requirements within the scope of this RFI consist of:

1. A set of security controls that apply to specific environments.
2. A set of capabilities required to manage and monitor the performance of the Network Security Layer.

5.1. Security Controls

The table below summarises the security controls within the scope of the RFI. 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 will be activated.

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 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
SSL VPN with certificate authentication	Eavesdropping MITM attacks IP exposure Loss of confidentiality	Encrypted tunnelling User authentication Secure remote access IP masking	DC OOBM
Test Access Points (TAPs)	Dropped packets Security vulnerabilities Configuration errors	Monitor and analysis of network traffic	DC Offices
VPN IPSEC	Eavesdropping MITM attacks IP exposure Loss of confidentiality	Encrypted tunnelling User authentication Secure remote access IP masking	DC Offices
Web Application Firewall (WAF)	OWASP Top 10 threats (e.g., SQL injection, XSS) Unauthorized API access Application-layer DoS attacks	Protect web apps from attacks (SQL injection, XSS, CSRF) HTTP/HTTPS traffic inspection Application-layer filtering	DC

	Session hijacking		
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

5.1.1. Throughput and performance requirements per environment

This section details the throughput requirements per environment.

5.1.1.1 Throughput and performance requirements for the DC environment

The below table summarises the throughput requirements **per cluster of appliances** for the DC environment.

Metric	Throughput and performance per cluster
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)	≥200Gbps
TCP with Security (IDS)	≥200Gbps
Single TCP flow (RTT ≤ 1ms)	≥25Gbps
Single TCP flow (RTT 20–30ms)	≥10Gbps
SSL Inspection Throughput	≥200Gbps
SSL Inspection Concurrent Session	>2M
WAF	≥40Gbps
SSL VPN	≥10Gbps
SSL IPSEC	≥20Gbps
TAPs	≥400Gbps
Network Scalability figures	
Number of BGP peers	>1000
Number of prefixes	>100K
ECMP scale	8 next hops per prefix

5.1.1.2 Throughput and performance requirements for the Offices and OOBM environments

The below table summarises the throughput requirements **per node** for the Offices and OOBM environments.

Metric	Throughput per node
TCP Session Rate	>100K
TCP Sessions	>1M
Throughput	40Gbps
Raw Stateful TCP (no NAT, no security)	40Gbps
Stateful TCP with NAT	20Gbps
Single TCP flow (RTT ≤ 1ms)	≥4Gbps
Single TCP flow (RTT 20–30ms)	≥2Gbps
SSL Inspection Throughput	20Gbps
SSL Inspection Concurrent Session	>500K
Application Control Throughput	10Gbps
Web Filtering	10Gbps
SSL VPN	2Gbps

SSL IPSEC	≥10Gbps
Network scalability figures	
Number of BGP peers	>100
Number of prefixes	>10K
ECMP scale	4 next hops per prefix

5.1.2. Features and protocols required for the appliances

The table below summarises the required features and protocols for the appliances in the applicable environment.

Environment	Features/protocols
DC	• BGP • IGMPv3 • PIM-SSM • EVPN (desirable) • VXLAN (desirable) • VRF • IPv4/IPv6 support: feature parity between IPv4/IPv6 protocols, especially with respect to routing protocol support and route scale
Offices	• BGP • EVPN (desirable) • VXLAN (desirable) • VRF • IPv4/IPv6 support: feature parity between IPv4/IPv6 protocols, especially with respect to routing protocol support and route scale
OOBM	• BGP • VRF • IPv4/IPv6 support: feature parity between IPv4/IPv6 protocols, especially with respect to routing protocol support and route scale

5.2. Capabilities for management and monitoring

The table below summarises the set of capabilities required to manage and monitor the Network Security Layer.

The following information is provided for each capability:

- The name of the capability.
- The expected functions and features associated with the capability.
- The environment(s) for which the capability will be used.

Capability	Functions / features	Environment(s)
Centralised configuration management	Centralised configuration and policy management. Centralised devices and firmware management. Configuration revision control, enabling auditing.	DC Offices OOBM
Observability and trend analytics	Centralised solution for: • Data collection • Data analysis • Reporting Minimum storage capacity: 72 TB Up to 1 TB/day	DC Offices OOBM

6. Technical Questions

Please see Annex 1

7. Financial and Non-Technical Questions

Please see Annex 1