CLARIFICATIONS

Procurement Process:	
Reference of Procurement:	*ECMWF/RFI/2025/381*
Title of Procurement:	Network Security Layer
Edition:	3rd edition
Date of Issue:	12/11/2025

Issued by ECMWF Administration Department, Procurement Section

ECMWF/RFI/2025/381 REQUEST FOR CLARIFICATION FORM
3rd series of clarification

#	Page/Part/Article/Section	Question	Answer by ECMWF	Date - answer is published by ECMWF
1	TAPs	Please indicate how many TAPs and on which interfaces are required in the DC office?	TAPs will likely be connected to the Internet Edge Routers, and as such will be in position to capture both DC and Offices traffic in Bologna.	24/10/2025
2	TAPs	The exact copy of the traffic intercepted by the TAPs (Test Access Points), to which monitoring tool should it be sent?	The respondent is invited to propose a solution.	24/10/2025
3	TAPs	Considering the high throughput requested, we ask to approve the adoption of dedicated TAP devices.	Agreed.	24/10/2025
4	TAPs	"RFI 381 Document.pdf" par. "5.1 Security Controls" reports that TAPs should be considered for DC and Offices, but the TAP throughput and performance requirements is reported only for DC in par. "5.1.1.1 Throughput and performance requirements for the DC environment" and not in par. "5.1.1.2 Throughput and performance requirements for the Offices and OOBM environments". For what environments should you consider introducing TAPs? DC only or DC and Offices?	TAPs will likely be connected to the Internet Edge Routers, and as such will be in position to capture both DC and Offices traffic in Bologna. DC requirements are higher than Offices, so should be sufficient to cover both use cases.	24/10/2025
5	TAPs	To identify the correct TAPs type to propose, we would like to ask: - For what type of links TAPs are expected to be used? Fiber or Copper? In case of Fiber, will it be Singlemode or Multimode? What speed are the links? What connectors are expected to use (LC or MPO)? - How many links will use TAPs?	Fibre links only for TAPs. Ideally two links will be used, using either single mode or multimode fibre (ECMWF can do either), either MPO or LC is fine. Interface speed should be at the minimum 100Gbit, ideally 400Gbit.	24/10/2025
6	Power Supply	What type of power supply is required for firewalls? AC or DC?	AC.	24/10/2025
7	Contract	The duration of the contract is set at 4 years. On the Annex 1 document, in the F2 request, it mentions "All software subscriptions for a period of one (1) year and three (3) years (when applicable)" and "All maintenance and support for a period of one (1) year and three (3) years (when applicable);". Does the prices, of subscriptions and maintenance for 1 year and for 3 years, depend on the fact that you assume that to have 4 years of the contract you normally have to order 1+3 years?	The information requested in F2 is for pricing analysis and is not related to the contract duration. This is for the moment an information. The duration of the contract will be indicated during the ITT.	24/10/2025
8	Firewall	Is a HA configuration required for all firewalls, whether DC, Offices or OOBM?	Yes. Firewalls for DC, Offices and OOBM should use either active-active or active-passive HA.	24/10/2025
9	Firewall	Please indicate the type of interfaces required and the number of firewalls for each site (DC, Office, OOBM).	DC firewalls should offer a number of 400Gbit (minimum, 2, ideally 4+) and / or 100Gbit interfaces (minimum 4, ideally 8+) interfaces to achieve the required throughput, factoring in HA / resiliency. Exact number of interfaces will depend on the proposed clustering / HA mechanisms. Offices firewalls should offer a number of 10/25Gbit interfaces (8+). OOBM interfaces should offer a number of 1/10Gbit interfaces (8+)	24/10/2025
10	Firewall	When SSL IPSEC is reported in firewall performance, does it refer only to the IPSEC protocol?	Yes. The "SSL IPSEC" entries in tables of sections 5.1.1.1 and 5.1.1.2 refer to "VPN IPSEC".	24/10/2025
11	Firewall	The performance of firewalls intended for Offices and OOBM networks is identical, which leads to oversized machines for the OOBM network. Can you decline less stringent performance for OOBM firewalls?	Smaller platforms could be proposed for OOBM firewalls.	24/10/2025
12	Firewall	Please confirm that the quantities of firewalls required are correct: - DC: 2 production firewalls + 2 OOBM firewalls - Offices: n.6 production firewalls + n.6 OOBM firewalls	DC should have 2x independent firewall clusters (i.e. 4+ firewall appliances), using either active-active or active-passive HA. Each Offices site should have either active-passive or active-active HA firewall cluster (overall, 6+ firewall appliances). Each site should have two separate OOMB firewalls (i.e. 6 appliances, Bologna DC + Bologna Offices share 2x OOMB firewalls)	24/10/2025
13	Management product	Is a HA configuration required for the management product?	It is desirable	24/10/2025
14	Management product	Please indicate the type of interfaces required and the quantity for the management product.	It depends on the solution proposed, i.e. whether it is Cloud, VM or hardware-based. If hardware, it depends on projected data rates, minimum 10Gbit interfaces.	24/10/2025
15	Management product	Should the management product be physical or virtual?	This should be decided by the respondent based on the proposed design and on advantages/disadvantages that should be explained as part of the response.	24/10/2025

#	Page/Part/Article/Section	Question	Answer by ECMWF	Date - answer is published by ECMWF
16	Monitoring product	Is an HA configuration required for the monitoring product?	It is desirable	24/10/2025
17	Monitoring product	Please indicate the type of interfaces required and the quantity for the monitoring product.	It depends on the solution proposed, i.e. whether it is Cloud, VM or hardware-based. If hardware, it depends on projected data rates, minimum 10Gbit interfaces.	24/10/2025
18	Monitoring product	Should the monitoring product be physical or virtual?	This should be decided by the respondent based on the proposed design and on advantages/disadvantages that should be explained as part of the response.	24/10/2025
19	Virtual	In the case of virtual solutions for management and monitoring, is it also necessary to provide for the supply of the hw (server), on which to run them, and any hypervisor licenses?	No, ECMWF will use existing hypervisors in this case. The respondent should provide the hypervisor specification requirements if the chosen solution is a virtual one.	24/10/2025
20	WAF	Considering the high throughput requested, we ask to approve the adoption of dedicated WAF appliances.	The solution could be a dedicated platform or included in another platform, e.g. firewall.	24/10/2025
21	WAF	Is a HA configuration required for the WAF?	It is desirable.	24/10/2025
22	WAF	Please indicate the type of interfaces required and the quantity for the WAF.	This is dependent on the proposed solution but at a minimum 25Gbit, ideally 100Gbit or 400Gbit interfaces.	24/10/2025
23	WAF	Should WAF be used as a reverse proxy? Please report more details on the type of services requested.	No, WAF should be transparent. Load balancers can be used for reverse proxy functionality, if required.	24/10/2025
24	WAF	Is the throughput of the WAF ≥ 40Gbps referred to the hhtps protocol or only to the hhtp protocol?	It is likely to be a mixture but predominantly HTTPS (80% HTTPS in current environment).	24/10/2025
25	Annex1	Could you clarify the next sentence reported on Annex 1 paragraph 9? Does this mean that compliance with the requirements expressed in the RFI document must also be included in the answers to the questions in Annex 1? "Please ensure that the content of the section(s) listed in the following column is (are) fully addressed in the response: "Relevant section(s) in the Instructions and Specifications document."	The answer to the questions must cover all the elements listed in the section(s) pointed at in column "Relevant section(s) in the Instructions and Specifications document." when applicable.	24/10/2025
26	Generic	Are ECMWF adverse to using part of their existing infrastructure as a component of the new security solution or would you prefer a standalone solution which is completely isolated and separate from existing components?	ECMWF is only considering a new network security layer that is independent from the existing one.	04/11/2025
27	TAPs	Let us ask the question again: how many TAPs should we consider? This is our idea, if we install the TAPs in the LAN, behind the Internet edge routers, we should consider 4 TAPs (1 TAP for the DC FW1 interface, 1 TAP for the DC FW2 interface, 1 TAP for the Bologna office FW1 interface, and 1 TAP for the Bologna office FW2 interface. Is this correct?	It would be beneficial to have flexibility where we connect TAPs on ad hoc basis. Normally they would be connected to IERs (two ports total), but having spare capacity to connect them elsewhere, would be beneficial.	04/11/2025
28	Firewall OOBM	In response to a previous question, you agreed to use OOBM firewall models that are less powerful than the requirements in section "5.1.1.2 Throughput and performance requirements for the Offices and OOBM environments." This question was asked because we assume the tasks to be performed on OOBM firewalls do not require high performance. Can you please provide us with an additional table dedicated to OOBM firewalls?	**MetricThroughput per OOBM firewall node** TCP Session Rate>1K TCP Sessions>50k Throughput10Gbps Raw Stateful TCP (no NAT, no security)10Gbps Stateful TCP with NAT5Gbps Single TCP flow (RTT ≤ 1ms)≥4Gbps Single TCP flow (RTT 20–30ms)≥2Gbps SSL Inspection Throughput5Gbps SSL Inspection Concurrent Session>10K Application Control Throughput1Gbps Web FilteringN/A SSL VPN2Gbps SSL IPSEC≥1Gbps Network scalability figures Number of BGP peers>10 Number of prefixes>1K ECMP scale4 next hops per prefix	04/11/2025
29	Generic	Do you want us to provide cables for all solutions? If so, what size?	All necessary hardware and software components should be included in the proposed solutions. Cable length are expected to be 3 meters.	04/11/2025
30	WAF	When referring to "transparent," does it mean that the WAF is not inline? If it is not inline, how should mitigation be performed?	The WAF solution should be deployed inline in the data path between a client and a web application.	04/11/2025
31	WAF	Regarding WAF throughput, does it refer to Layer 7 or Layer 4 traffic? Is it all application traffic to be protected?	The WAF throughput refers to Layer 7. All application traffic is to be protected.	04/11/2025

#	Page/Part/Article/Section	Question	Answer by ECMWF	Date - answer is published by ECMWF
32	WAF	Please provide more details about the type of application traffic to be protected (e.g., HTTP, API, etc.) and, if available, the approximate percentage of each.	This will be confirmed during the ITT phase, but WAF protection is likely to include API and HTTPS traffic. We are unable to give percentages at this time.	04/11/2025
33	WAF	Please specify, if known, the number of new TCP sessions per second that the WAF must protect.	The current figures are around ~300 sessions per second in average,~1500 sessions per second at peak time.	04/11/2025
34	TAPs	Could you please provide a more comprehensive description of the Test Access Points (TAPs)	At this RFI phase, ECMWF believes the information included in the Instructions and Specifications document, combined with the subsequent clarification responses, provides sufficient detail for respondents to propose a solution.	04/11/2025
35	TAPs	What portion of the traffic you are willing the TAPs to inspect?	The aim is for full visibility of traffic relevant to security monitoring, prioritising north-south traffic at the perimeter and key east-west segments in the data center. TAPs should capture 100% of traffic on selected monitored links.	04/11/2025
36	TAPs	What is your expectation in terms of the type of TAP - active or passive?	Passive.	04/11/2025
37	Firewall	Regarding the OOBM networks do you expect to keep the current network design and terminate VPN tunnels on the OOBM firewalls?	SSL VPN tunnels will be terminated on OOBM firewalls for emergency remote network analyst access.	04/11/2025
38	Firewall	Will the OOBM network firewall clusters be connected to existing circuits or we need to provide new circuits as well?	OOBM firewalls will make use of existing circuits and no new circuits will need to be provided.	04/11/2025
39	Firewall	Will office firewall clusters be connected to existing circuits or we need to provide new circuits as well?	Offices and DC firewalls will be connected to Internet Edge routers and make use of existing circuits; no new circuits will need to be provided.	04/11/2025
40	Generic	What are your expectations in terms of co-management - would this be vendor-managed, mixed model or unmanaged?	All devices will be managed by ECMWF analysts.	04/11/2025
41	Generic	What type of co-management will you require - read-only or write?	All devices will be managed by ECMWF analysts, no co-management will be necessary.	04/11/2025
42	Firewall	When discussing IPSec tunnels what is the expected number of tunnels on each firewall cluster type (DC, office, OOBM)?	The expected number of IPSec tunnels is as follows: DC <10, Offices <10, OOBM - none.	04/11/2025
43	Generic	If PoC is required at a later stage, what features/functionalities will you be looking to test?	This is beyond the scope of the RFI.	04/11/2025
44	SSL VPN	Is supporting SSL VPN a strict requirement for this RFI as this will influence the vendor selection on our side and affect financial aspects as well?	Supporting SSL VPN is a strict requirement, unless a suitable alternative could be proposed. A dedicated hardware device for SSL VPN could be considered.	04/11/2025
45	Generic	Do you intend to keep the existing internet providers or you are looking for new connectivity options as part of this RFI?	This is beyond the scope of the RFI.	04/11/2025
46	Generic	Can you provide an estimated average number of users that will pass through each of the DC and office firewalls?	The estimated average number of endpoints is as follows: DC: 10000s of endpoints (bare-metal servers and VMs; a percentage requiring NAT); Offices - <1000 users, <50 servers (a percentage of which will use NAT).	04/11/2025
47	Generic	Are we correct in assuming VXLAN and EVPN are already set up, and you will be managing those? What kind of switches will be/are used here?	Correct. Current vendor is Juniper Networks, but any proposed solution should be vendor-agnostic.	04/11/2025
48	Firewall	Would you please detail the usage of PIM-SSM within the DC Firewalls 1) What is the business use case? 2) Is it a pass through requirement?	The usage of PIM-SSM within the DC is as follows: 1) Retrieval of weather observations data via EUMETSAT's EUMETCast service 2) Current design relies on PIM + IGMPv3 support, so DC Firewalls participate in multicast topology.	04/11/2025
49		Could you please confirm whether the potential purchase will be made from Italy?	This is beyond the scope of the RFI.	12/11/2025
50		IDS and IPS are listed as distinct functions. While we appreciate that one is typically detection only and one is inline for prevention, can you detail how you see the differences in the two, at a functional level?	The current descriptions of the IDS and IPS disctinct functions should provide sufficient detail for the RFI response.	12/11/2025
51		The SSL decryption requirement defines specific threats in the decrypted HTTP layer (e.g. malware/C2) for which mitigation is required. Is this list comprehensive? For example, in the DC we'd expect IPS to also be required, unless the firewalls would be deployed after SSL/TLS offload.	It is anticipated that SSL decryption, IPS and certain other security features would be deployed to expect just some, rather than all East-West and North-South data flows. It is not possible at this stage to provide a full and comprehensive list of threats to be mitigated.	12/11/2025

#	Page/Part/Article/Section	Question	Answer by ECMWF	Date - answer is published by ECMWF
52		Could you give more detail on the 'Test Access Point' requirement? Throughput is high here – but it's not clear whether there are needed functions within the firewalls or this refers to processing of traffic from external devices at high speed.	This function is expected to be independent from the firewall.	12/11/2025
53		Are cloud solutions permitted? For example, cloud-based URL databases for Web Filtering categorization functionality.	Cloud solutions are permitted in principle under certain conditions that will need to be discussed and agreed with ECMWF.	12/11/2025
54		The 'raw stateful tcp' numbers mention "no security". Is there an expectation that this traffic/some traffic would completely bypass security modules on the firewall, i.e. would be handled in a stateless way?	Figure in question is the expected throughput with L3-4 stateful firewall only, i.e. no NAT, IPS or any other security features. The figures that follow detail the expected throughput with NAT and IPS/IDS features enabled.	12/11/2025
55		Can you clarify whether the numbers are incremental? For example, 800Gbps is listed for raw stateful tcp, and 400Gbps is listed for stateful tcp with NAT in the DC use case. Would this imply that the platform needs to support 1.2Tbps, or can we take the 'throughput' value (800Gbps in DC case) as the overall maximum irrespective of the security service combinations?	800Gbps can be taken as the overall maximum value	12/11/2025
56		Session to throughput ratio (4M to 800Gbps in DC case) suggests extremely high throughput per session compared to a 'typical' DC. We suspect this is due to the unique nature of ECMWF traffic patterns, but can we just get a clarification that these numbers are correct?	This is correct and factors in minimum future growth. For reference, the current figures observed on the firewall are 200Gbit full duplex, with around 500-800k sessions.	12/11/2025
57		SSL Inspection throughput is very high. This is a service which can have a significant performance impact and affect our offer to ECMWF. Is this throughput required at all times in each use case? Are there possibilities to reduce this burden on the firewalls (for example, is there any SSL offload technology in ECMWF DC?)	It is anticipated that SSL Inspection, IPS and certain other security features would be deployed to expect some rather than all East-West and North-South data flows. It is not possible at this stage to provide a full and comprehensive list of threats to be mitigated.	12/11/2025
58		Can you clarify 'SSL VPN' versus 'SSL IPSec'? Is the former using browser based technology and the latter is a VPN client with IPSec fallback?	The requirements here are for site-to-site VPN to facilitate secure transport between branch sites (IPSEC requirement) and a secure remote access VPN for analysts (client and/or browser-based SSL VPN). Alternative proposals that would fulfil both of these requirements could be considered. The "SSL IPSEC" entries in tables of sections 5.1.1.1 and 5.1.1.2 refer to "VPN IPSEC".	12/11/2025
59		For the "Observability and trend analytics' requirement, can you clarify the format and data types required? KPIs for system monitoring using e.g. SNMP? Syslog collection for threat analysis?	Format and data types should be based on standard protocols, which need to be specified in the responses.	12/11/2025
60		Is there an existing Threat Analysis function (e.g. an ECMWF SIEM platform) or should this be provided? Is the same true for KPI monitoring – such as an SNMP station?	A SIEM solution is beyond the scope of this RFI. A threat analysis function solution to manage and monitor the Network Security Layer could be proposed as part of the response.	12/11/2025
61		Threat Analysis function may be provided by software-only offerings. Can an ECMWF Storage network be leveraged for data retention?	Use of ECMWF storage infrastructure could be considered when proposing software-only solution for the threat analysis function.	12/11/2025
62		Are ECMWF adverse to using part of their existing infrastructure as a component of the new security solution or would you prefer a standalone solution which is completely isolated and separate from existing components?	ECMWF is only considering a new network security layer that is independent from the existing one.	12/11/2025
63		Is responding to this RFI a prerequisite for participating in the ITT?	No	12/11/2025