



REQUEST FOR QUOTATION NO. RfQ26/03382

Provision of Next Generation Firewalls, Network Switches and Related Services for Moldelectrica

UNDP through the “Greening the future, advancing rights and stability Moldova” Project kindly requests your quotation for the Request for Quotation no. **RfQ26/03382: Provision of Next Generation Firewalls, Network Switches and Related Services for Moldelectrica** as detailed in line items section of this RFQ.

This Request for Quotation comprises the following documents:

Section 1: This RFQ document generated by the online system

Section 2: RFQ Instructions and Data

Annex 1: Schedule of Requirements

Annex 2: Quotation Submission Form

Annex 3: Technical and Financial Offer

Annex 4: Technical Responsiveness Table

When preparing your quotation, please be guided by the RFQ Instructions and Data. Please note that quotations must be submitted directly in the system responding to the questions and uploading required documents by the date and time indicated in the online portal. It is your responsibility to ensure that your quotation is submitted before the deadline. Quotations received after the submission deadline outside the online portal, for whatever reason, will not be considered for evaluation.

Quotations must be submitted directly in Quantum NextGenERP supplier portal following the link: <http://supplier.quantum.partneragencies.org/> using the profile you may have in the portal (please log in using your username and password).

Follow the instructions in the user guide to search for the tender using search filters, namely **Negotiation ID: UNDP-MDA-01120** and subscribe to the tender in order to get notifications in case of amendments of the tender document and requirements.

In case you have never registered before, follow this link to register a profile:

<https://estm.fa.em2.oraclecloud.com/fscmUI/redwood/supplier-registration/register-supplier/registersupplier-verification?id=TUW16eK6qsD94MNMxATNMoyCOHny7FmchTkUZsdOqrAW4sy6L5xSAB033Q%3D%3D> **Please note that the access link to the Supplier registered profile is sent from Oracle within up to 3 days. In case you have not received the access link after 3 days since registration, you should address for support to UNDP at the email address: sc.md@undp.org.** In case you encounter errors with registration (e.g. system states Supplier already is registered), you should address for support to UNDP at the email address: sc.md@undp.org.

Computer firewall could block *oracle* or *undp.org* extension and Suppliers might not receive the Oracle notifications. Please turn down any firewalls on your computers to ensure receipt of email notification.

Do not create a new profile if you already have one. Use the forgotten password feature in case you do not remember the password or the username from previous registration.

Should you require further clarifications on the application through the Quantum online portal, kindly contact the Procurement Unit at sc.md@undp.org. Please pay attention that the bid shall be submitted online through the Quantum system and any bid sent to the above email shall be disqualified.

Should you require further clarifications on the Request for Quotation, Terms of Reference or other requirements, kindly communicate using the messaging functionality in the portal.

Deadline for Submission of Offers (Date and Time), which is visible in the online procurement system will be final. System will not accept submission of any bid after that date and time. It is the responsibility of the bidder to make sure that the bid is submitted prior to this deadline for submission.

Bidders are advised to upload bid documents and to submit their offer a day prior or well before the date and time indicated under the deadline for submission of Offers. Do not wait until last minute. If Bidder faces any issue during submitting offers at the last minutes prior to the deadline for submission, UNDP may not be able to assist on such a short notice and will not be held liable in such instance. UNDP will not accept any offer that is not submitted directly through the System.

Thank you and we look forward to receiving your quotation.

UNDP Moldova

SECTION 2: GENERAL INSTRUCTIONS

Introduction	Bidders shall adhere to all the requirements of this RFQ, including any amendments made in writing by UNDP. This RFQ is conducted in accordance with the UNDP Programme and Operations Policies and Procedures (POPP) on Contracts and Procurement Any Bid submitted will be regarded as an offer by the Bidder and does not constitute or imply the acceptance of the Bid by UNDP. UNDP is under no obligation to award a contract to any Bidder as a result of this RFQ. UNDP reserves the right to cancel the procurement process at any stage without any liability of any kind for UNDP, upon notice to the bidders or cancellation of the tender in the online portal.
Deadline for the Submission of Quotation	Deadline is indicated in the online portal. If any doubt exists as to the time zone in which the quotation should be submitted, refer to http://www.timeanddate.com/worldclock/.
Method of Submission	Quotations must be submitted as follows: NextGenERP supplier portal following this link: http://supplier.nextgenerp.partneragencies.org/ using the profile you may have in the portal. Follow the instructions in the user guide to search for the tender using Negotiation ID. In case you have never registered before, follow this link to register a profile: https://estm.fa.em2.oraclecloud.com/fscmUI/redwood/supplierregistration/register-supplier/register-supplier-verification?id=TUW16eK6qsD94MNMxATNMoyCOHny7FmchTkUZsdOqrAW4sy6L5xSAB033Q%3D%3D Do not create a new profile if you already have one. Use the forgotten password feature in case you do not remember the password or the username from previous registration. ▪ File Format: All attachments must be in PDF format unless otherwise instructed by UNDP. ▪ File names must be in Latin alphabet/keyboard and clearly indicate the content of the document to facilitated review. ▪ All files must be free of viruses and not corrupted.
Cost of preparation of quotation	UNDP shall not be responsible for any costs associated with a Supplier's preparation and submission of a quotation, regardless of the outcome or the manner of conducting the selection process.

Supplier Code of Conduct, Fraud, Corruption,	All prospective suppliers must read the United Nations Supplier Code of Conduct and acknowledge that it provides the minimum standards expected of suppliers to the UN. The Code of Conduct, which includes principles on labour, human rights, environment and ethical conduct may be found at: https://www.un.org/Depts/ptd/about-us/unsupplier-code-conduct Moreover, UNDP strictly enforces a policy of zero tolerance on proscribed practices, including fraud, corruption, collusion, unethical or unprofessional practices, and obstruction of UNDP vendors and requires all bidders/vendors to observe the highest standard of ethics during the procurement process and contract implementation. UNDP's Anti-Fraud Policy can be found at http://www.undp.org/content/undp/en/home/operations/accountability/audit/office_of_audit_andinvestigation.html#anti
Gifts and Hospitality	Bidders/vendors shall not offer gifts or hospitality of any kind to UNDP staff members including recreational trips to sporting or cultural events, theme parks or offers of holidays, transportation, or invitations to extravagant lunches, dinners or similar. In pursuance of this policy, UNDP: (a) Shall reject a bid if it determines that the selected bidder has engaged in any corrupt or fraudulent practices in competing for the contract in question; (b) Shall declare a vendor ineligible, either indefinitely or for a stated period, to be awarded a contract if at any time it determines that the vendor has engaged in any corrupt or fraudulent practices in competing for, or in executing a UNDP contract.
Conflict of Interest	UNDP requires every prospective Supplier to avoid and prevent conflicts of interest, by disclosing to UNDP if you, or any of your affiliates or personnel, were involved in the preparation of the requirements, design, specifications, cost estimates, and other information used in this RFQ. Bidders shall strictly avoid conflicts with other assignments or their own interests, and act without consideration for future work. Bidders found to have a conflict of interest shall be disqualified. Bidders must disclose in their Bid their knowledge of the following: a) If the owners, part-owners, officers, directors, controlling shareholders, of the bidding entity or key personnel who are family members of UNDP staff involved in the procurement functions and/or the Government of the country or any Implementing Partner receiving goods and/or services under this RFQ. The eligibility of Bidders that are wholly or partly owned by the Government shall be subject to UNDP's further evaluation and review of various factors such as being registered, operated and managed as an independent business entity, the extent of Government ownership/share, receipt of subsidies, mandate and access to information in relation to this RFQ, among others. Conditions that may lead to undue advantage against other Bidders may result in the eventual rejection of the Bid.
Currency of Quotation	Quotations shall be quoted in the currency indicated in the portal.

Joint Venture, Consortium or Association	If the Bidder is a group of legal entities that will form or have formed a Joint Venture (JV), Consortium or Association for the Bid, they shall confirm in their Bid that : (i) they have designated one party to act as a lead entity, duly vested with authority to legally bind the members of the JV, Consortium or Association jointly and severally, which shall be evidenced by a duly notarized Agreement among the legal entities, and submitted with the Bid; and (ii) if they are awarded the contract, the contract shall be entered into, by and between UNDP and the designated lead entity, who shall be acting for and on behalf of all the member entities comprising the joint venture, Consortium or Association. Refer to Clauses 19 – 24 under Solicitation policy for details on the applicable provisions on Joint Ventures, Consortium or Association.
Only one Bid	The Bidder (including the Lead Entity on behalf of the individual members of any Joint Venture, Consortium or Association) shall submit only one Bid, either in its own name or, if a joint venture, Consortium or Association, as the lead entity of such Joint Venture, Consortium or Association. Bids submitted by two (2) or more Bidders shall all be rejected if they are found to have any of the following: • they have at least one controlling partner, director or shareholder in common; or • any one of them receive or have received any direct or indirect subsidy from the other/s; or • they have the same legal representative for purposes of this RFQ; or • they have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about, or influence on the Bid of, another Bidder regarding this RFQ process; • they are subcontractors to each other's Bid, or a subcontractor to one Bid also submits another Bid under its name as lead Bidder; or • some key personnel proposed to be in the team of one Bidder participates in more than one Bid received for this RFQ process. This condition relating to the personnel, does not apply to subcontractors being included in more than one Bid.
Price variation	No price variation due to escalation, inflation, fluctuation in exchange rates, or any other market factors shall be accepted at any time during the validity of the quotation after the quotation has been received.
Alternative Quotes	If alternative quote is permitted, it may be submitted only if a conforming quote to the RFQ requirements is submitted. Where the conditions for its acceptance are met, or justifications are clearly established, UNDP reserves the right to award a contract based on an alternative quote. If multiple/alternative quotes are being submitted, they must be clearly marked as "Main Quote" and "Alternative Quote" directly in the portal and in any supporting document as relevant.
Contact Person for correspondence, notifications and clarifications	Must be submitted directly in the portal using the messaging functionality. Any delay in UNDP's response shall be not used as a reason for extending the deadline for submission, unless UNDP determines that such an extension is necessary and communicates a new deadline to the Proposers.
Right not to accept any quotation	UNDP is not bound to accept any quotation, nor award a contract or Purchase Order
Right to vary requirement at time of award	At the time of award of Contract or Purchase Order, UNDP reserves the right to vary (increase or decrease) the quantity of services and/or goods, by up to a maximum twenty-five per cent (25%) of the total offer, without any change in the unit price or other terms and conditions.

Publication of Contract Award	UNDP will publish the contract awards on the websites of the CO and the corporate UNDP Web site.
Policies and procedures	This RFQ is conducted in accordance with UNDP Programme and Operations Policies and Procedures
UNGM registration	Any Contract resulting from this RFQ exercise will be subject to the supplier being registered at the appropriate level on the United Nations Global Marketplace (UNGM) website at www.ungm.org . The Bidder may still submit a quotation even if not registered with the UNGM, however, if the Bidder is selected for Contract award, the Bidder must register on the UNGM prior to contract signature.

SECTION 2: SPECIAL INSTRUCTIONS

General Conditions of Contract	Any Purchase Order or contract that will be issued as a result of this RFQ shall be subject to one of the General Conditions of Contract below as applicable in each case specified in the Requirements section Applicable GTC: ☒ General Terms and Conditions / Special Conditions for Contract. Applicable Terms and Conditions and other provisions are available at https://www.undp.org/procurement/business/how-we-buy
Special Conditions of Contract	☒ Cancellation of PO/Contract if the delivery/completion is delayed by 30 days ☒ Liquidates damages shall be imposed as follows: Percentage of contract price per week of delay: 2.5% up to a maximum of 10%, after which UNDP may terminate the contract.
Duties and taxes	Article II, Section 7, of the Convention on the Privileges and Immunities provides, inter alia, that the United Nations, including UNDP as a subsidiary organ of the General Assembly of the United Nations, is exempt from all direct taxes, except charges for public utility services, and is exempt from customs restrictions, duties, and charges of a similar nature in respect of articles imported or exported for its official use. All quotations shall be submitted net of any direct taxes and any other taxes and duties, unless otherwise specified in the requirements section. All prices must: ☒ be exclusive of VAT and other applicable indirect taxes
Eligibility	A vendor who will be engaged by UNDP may not be suspended, debarred, or otherwise identified as ineligible by any UN Organization or the World Bank Group or any other international Organization. Vendors are therefore required to disclose to UNDP whether they are subject to any sanction or temporary suspension imposed by these organizations. Failure to do so may result in termination of any contract or PO subsequently issued to the vendor by UNDP. It is the Bidder's responsibility to ensure that its ultimate beneficial owners, employees, joint venture members, sub-contractors, service providers, suppliers and/or their employees meet the eligibility requirements as established by UNDP. Bidders must have the legal capacity to enter a binding contract with UNDP and to deliver in the country, or through an authorized representative.
Language of quotation	English, Romanian Including documentation, catalogues, instructions and operating manuals.
Quotation validity period	Quotations shall remain valid for 60 (sixty) days from the deadline for the Submission of Quotation.
Partial Quotes	☒ Not Allowed
Alternative Quotes	☒ Not permitted
Payment Terms	☒ 100% within 30 days after receipt of goods and submission of payment documentation.
Conditions for Release of Payment	☒ Written Acceptance of Goods, based on full compliance with RFQ requirements

Clarifications	Bidders must send their inquiries and requests for clarifications using the messaging functionality in the portal. <u>PLEASE PAY ATTENTION: QUOTES SHALL NOT BE SUBMITTED TO ANY EMAIL ADDRESS BUT ONLY THROUGH THE PORTAL.</u> Requests for clarification from bidders will not be accepted any later than 3 (three) days before the submission deadline. Responses to request for clarification will be communicated directly in the portal.
Documents to be submitted	☒ Annex 2: Quotation Submission Form duly completed and signed ☒ Annex 3: Technical and Financial Offer duly completed and signed and in accordance with the Schedule of Requirements in Annex 1 ☒ Annex 4: Technical Responsiveness Table duly completed and signed ☒ Detailed technical description of the offered goods (including brochures/user manuals, datasheet, configuration guide) ☒ Company Profile, including detailed portfolio/previous corporate experience in similar fields related to the assignment ☒ Copy of registration documents ☒ List of 3 (three) completed and/or ongoing contracts for similar goods supplied within the past 3 (three) years including the following information: • Name of previous contracts • Client & Reference Contact • Details including e-mail • Contract Value • Period of activity / Delivery period Copies of provided relevant contracts might be requested during the evaluation process. ☒ Certificates of quality and origin for the goods offered ☒ Statement of Warranty of minimum 36 months for the offered goods (hardware Items #1–4), in accordance with Schedule of Requirements in Annex 1 ☒ Statement regarding the availability of an authorized service center to handle warranty/hardware repair issues ensuring the comprehensiveness after-sales services accompanied by: • Letter signed by both parties confirming the relationship between the supplier and service provider; • Official documentation stating that the Partner is a registered business in the country; • A detailed profile of the service provider; • Description of procedure and time estimates for service provision. ☒ Statement of satisfactory Performance (references) from at least 3 (three) top clients in terms of Contract value in similar field? ☒ Environmental Compliance Certificates, Accreditations, if any ☒ Export/Import Licenses, if applicable ☒ Manufacturer's Authorization Form (MAF) for bidders that are not the manufacturer of the offered goods and ensuring validity of warranty and after-sales support
Evaluation method	☒ The Contract will be awarded to the lowest price substantially compliant offer
Evaluation criteria	☒ Full compliance with all requirements as specified in Annex 1 ☒ Full acceptance of the General Conditions of Contract ☒ Minimum of 3 (three) years of proven experience in supply of IT Equipment ☒ Minimum 2 (two) similar contracts (in terms of type and volume of goods) successfully completed during past 3 (three) years ☒ Availability of certificates of quality and origin for the offered goods

	☒ Warranty for a minimum period of 36 months for the offered goods (hardware Items #1–4), in accordance with Schedule of Requirements in Annex 1 ☒ Availability of a local authorized representative, dealer, partner, or service provider in the Republic of Moldova capable of handling warranty claims, hardware repair/replacement (RMA), and after-sales support services for the offered equipment, including: • Technical support on the overall use and operation of the supplied hardware and software, with a response time of no more than twenty-four (24) hours (or one (1) working day); • Remote technical support with a response time of no more than one (1) working day and on-site technical intervention in the Republic of Moldova, where required, within no more than five (5) working days from receipt of the service request, unless a shorter timeframe is required under the warranty conditions applicable to the offered equipment; • Brand new replacement within a maximum of one (1) month if Purchased Unit is beyond repair (within warranty period). ☒ Delivery Lead Time: 60 days ☒ Manufacturer's Authorization Form (MAF) for bidders that are not the manufacturer of the offered goods
--	--

Type of Contract to be awarded	☒ Contract Face Sheet (Goods and-or Services)
Expected date for contract award.	25 th of October 2026

ANNEX 1: SCHEDULE OF REQUIREMENTS

- List of goods and services under this procurement

#	Name	Quantity
1	Next Generation Firewall (Table A)	8
2	Access Switch 24+4 ports (Table B)	8
3	Core Switch (Table C)	1
4	Next Generation Firewall Substation (Table D)	40
5	Training for System Administrators	1

General requirements for all deliverables:

Req	Description
1	The supplier shall demonstrate that the proposed hardware and software are authorized for supply and use in the Republic of Moldova. The bidder shall provide a valid Manufacturer Authorization Form (MAF), or equivalent official confirmation issued by the manufacturer, confirming that the bidder is authorized to offer and supply the proposed products, licenses, subscriptions and related support services in the Republic of Moldova.
2	Network equipment proposed shall not originate from a manufacturer that has been assessed by the European Union, a competent national cybersecurity/national security authority, or through an applicable coordinated EU security risk assessment as presenting supplier-security risks that the Contracting Authority determines cannot be sufficiently mitigated for the intended critical function. Where such an assessment exists, the supplier shall demonstrate, through documented technical, organizational and contractual measures, that the risks identified in that assessment do not apply to the proposed equipment or have been adequately mitigated. In the absence of satisfactory evidence, the proposed equipment shall be considered non-compliant. The proposed equipment for all positions should be produced and licensed by the same developer/company.
3	The Supplier must demonstrate that the products offered are as per the specification stipulated in the tender document, and as committed by the supplier, without any extra cost to the Moldelectrica.
4	The supplier undertakes that in respect of licensed software items, these shall be supplied with the authorized license certificate, and that it shall be sourced from an authorized source.
5	Communications (oral and written) must be conducted, and documentation must be submitted in English or Romanian. The licenses and any services provided must also be in the English or Romanian language.
6	After the supplier delivers the products, all rights and obligations will be assigned to the beneficiary of the solution, Moldelectrica.
7	The solutions must include all the licenses necessary for its operation, to the parameters and values requested in these specifications, including those related to extensibility, and there must not be any limitation.
8	For the hardware components the minimum required warranty is 36 months while the technical support and subscriptions are for a period of at least 3 years.
9	During the warranty the Supplier will replace defective components in no more than seven (7) calendar days.
10	Solutions must include access to the manufacturer's web portal in order to contact technical support and download updates for a period of at least 3 years.
11	The proposed solution must be delivered with all necessary cables for connection in rack.
12	The Supplier shall include, at no additional cost, the following consumables for the entire scope of supply under the contract (8 NGFWs, 8 access switches, 1 core switch and 40 substation firewalls): • UTP Cable Category 6A/6E: minimum 300 meters; • RJ45 Connectors Category 6A/6E: minimum 200 pieces; • UTP Patch Cords Category 6A/6E: minimum 50 pieces of each approximate length: 0.5 m, 1 m, 3 m, 5 m and 10 m; • Single-Mode LC-LC Optical Patch Cords: minimum 30 pieces of each approximate length: 0.5 m, 1 m, 2 m, 3 m, 5 m, 10 m and 20 m;

	- Single-Mode LC-SC Optical Patch Cords: minimum 30 pieces of each approximate length: 0.5 m, 1 m, 2 m, 3 m and 5 m; - Single-Mode SC-SC Optical Patch Cords: minimum 30 pieces of each approximate length: 0.5 m, 1 m, 2 m, 3 m and 5 m. The above quantities are aggregate quantities for the entire scope of supply and shall not be interpreted as quantities required per site or per equipment unit. All costs shall be included in the offered price.
13	All delivered components (hard, soft, licenses) must be updated to the latest stable version.
14	All requirements are minimum and mandatory. An equivalent solution is acceptable where the bidder demonstrates equal or better functionality, performance, security, support and interoperability.

Table A: Next Generation Firewall (8 units)

Req.	Description
1	The proposed solution must allow the detection and filtering of traffic by content.
2	The proposed solution must allow the detection and filtering of Distributed Denial of Service (DDoS) type attacks, by defining policies.
3	The proposed solution must allow the detection and filtering of applications.
4	The proposed solution must allow the establishment of antivirus and web/URL filtering rules. Anti-spam, email reputation or an equivalent email-related protection mechanism shall be available where supported by the proposed NGFW security bundle or may be satisfied by an existing integrated email-security control.
5	The proposed solution must allow establishing the rules of the QoS and traffic shaping.
6	The proposed solution must allow establishing the rules of the firewall according to the criteria of GeoIP.
7	The proposed solution must allow the application of network traffic blocking rules with source or destination addresses BootNet, which is periodically updated.
8	The proposed solution must allow the establishment of filtering rules web – web inspection/Filter.
9	The proposed solution must ensure the minimum requirements to ensure high availability: - Operation Active-Active and/or Active-Passive, or an equivalent high-availability mode supported by the proposed platform - Functionality Stateful Failover (Firewall and VPN) - Detection and notification for non-functional equipment - Network connection monitoring - Functionality Link Failover
10	The proposed solution must ensure the minimum requirements for ensuring the monitoring of the hardware components: Support syslog. Support SNMPv3 and, where required for legacy monitoring, SNMPv2c. Email notification for alerts. Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.
11	The solution must allow the creation/division and management of logical/virtual devices, offering the possibility to allocate, reserve or limit hardware and software resources for each instance. Each instance must function as an independent logical/virtual instance, ensuring complete isolation between different instances for independent security and administration. Each logical/virtual instance shall support independent configuration and administration of routing tables, NAT, firewall policies, VPN instances, security policies, and assigned physical and logical interfaces. Functionalities include, but are not limited to: Allocation, reservation or limitation of resources per instance, such as network interfaces and processing capacity. Dedicated physical CPU cores shall not be mandatory. The ability to configure and manage routing tables, firewall policies, and distinct security settings for each instance.

	Support for advanced traffic segregation and isolation functionalities, including physical and logical separation of network traffic between instances. The facility to perform specific management and monitoring operations for each instance, ensuring the flexibility and scalability necessary to meet the varied security needs of the organization. The solution must also include user access management functionality, allowing specific access rights and privileges to be assigned to different user groups. This should ensure that administrators can finely control and restrict user access to different instances and their respective resources while maintaining a high level of security and operational integrity.
12	The proposed solution must allow filtering of traffic of at least 20Gbps.
13	The proposed solution must have tunneling capability IPSec(VPN) at least 10 Gbps.
14	The proposed solution must have SSL traffic inspection capability of at least 1Gbps.
15	The proposed solution must have the ability to inspect traffic by enabling the IPS functionality of at least 2Gbps.
16	The proposed solution must have the ability to establish up to 1,5 million simultaneous TCP sessions.
17	The proposed solution must have the ability to establish at least 56,000 new sessions per second.
18	Each piece of hardware must contain at least 4 x 1GE SFP, with SFP modules included.
19	Each piece of hardware must contain at least 16 x 1GE RJ45.
20	Each piece of hardware must contain at least 2 x 10GE SFP+, with SFP modules included.
21	Each piece of hardware must contain at least one dedicated out-of-band management interface (RJ45 Ethernet, SFP/SFP+ Ethernet or equivalent).
22	Each piece of hardware must contain at least one dedicated console interface (RJ45 serial, USB, USB-C or equivalent).

Table B: Access Switch 24+4 ports (8 units)

Req.No.	Description
1	The proposed solution must ensure the minimum requirements to ensure high availability: - Operation using a multi-device redundancy mechanism appropriate to the proposed architecture - Detection and notification for non-functional equipment - Network connection monitoring - Functionality Link Failover - Multi-Chassis Link Aggregation (MCLAG), MLAG, stacking or an equivalent multi-device redundancy mechanism
2	The proposed solution must ensure the minimum requirements for ensuring the monitoring of hardware components: - Real-time and historical data monitoring - Support syslog - Support SNMPv3 and, where required for legacy monitoring, SNMPv2c - Email notification for alerts - Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.
3	The proposed solution must include switching capacity of at least 55Gbps.
4	The proposed solution must have a network latency of max 4 us.
5	The proposed solution must have a forwarding rate of at least 80 Mpps.
6	Each piece of hardware must contain at least 4 x 10GE SFP, with SFP modules included (2 SR and 2 LR).
7	Each piece of hardware must contain at least 24 x 1 GE PoE. PoE Power Budget min 350 W.
8	Each piece of hardware must contain at least one dedicated console interface (RJ45 serial, USB, USB-C or equivalent).
9	The proposed solution must support at least 4000 VLANs.
10	The proposed solution must support IEEE 802.1Q VLAN encapsulation.
11	The proposed solution must support Jumbo Frame as a minimum 9000 bytes.
12	The proposed solution must support Link Aggregation Control Protocol (LACP), IEEE 802.3ad

13	The proposed solution must support at least 8000 MAC addresses
14	The proposed solution must support at least or similar: - Port-based VLAN - MAC-based VLAN - SVI (Virtual Switch interface) - Persistent MAC (sticky MAC) - ARP inspection - ACL - DHCP Snooping - BPDU Guard - IP Source Guard - Uni-Directional Link Detection (UDLD) or equivalent link-failure detection mechanism - Per-port broadcast, multicast, unicast storm control - SPAN/RSPAN - PVST Interoperation, where required, or equivalent spanning-tree interoperability - Storm Control - STP BPDU Guard - STP Root Guard - Loop Guard

Table C: Core Switch (1 unit)

Requirement No.	Description
1	The proposed solution must ensure the minimum requirements to ensure high availability: - Operation using a chassis or multi-device redundancy mechanism such as stacking, MLAG/MCLAG or equivalent - Detection and notification for non-functional equipment - Network connection monitoring - Functionality Link Failover
2	The proposed solution must ensure the minimum requirements for ensuring the monitoring of hardware components: - Real-time and historical data monitoring - Support syslog - Support SNMPv3 and, where required for legacy monitoring, SNMPv2c - Email notification for alerts - Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.
3	The proposed solution must include switching capacity of at least 800Gbps.
4	The proposed solution must have a network latency of max 2 us.
5	The proposed solution must have a forwarding rate of at least 1300 Mpps.
6	Each piece of hardware must contain at least 2 x 40/100GE QSFP+, with QSFP modules included.
7	Each piece of hardware must contain at least 24 x 10GE SFP+, with SFP modules included.
8	Each piece of hardware must contain at least one dedicated console interface (RJ45 serial, USB, USB-C or equivalent).
9	The proposed solution must support at least 4000 VLANs.
10	The proposed solution must support IEEE 802.1Q VLAN encapsulation.
11	The proposed solution must support Jumbo Frame as a minimum 9000 bytes.
12	The proposed solution must support Link Aggregation Control Protocol (LACP), IEEE 802.3ad
13	The proposed solution must support at least 64000 MAC addresses
14	The proposed solution must support at least or similar: - Port-based VLAN - MAC-based VLAN - SVI (Virtual Switch interface)

	Persistent MAC (sticky MAC) ARP inspection ACL DHCP Snooping BPDU Guard IP Source Guard Uni-Directional Link Detection (UDLD) or equivalent link-failure detection mechanism Per-port broadcast, multicast, unicast storm control SPAN/RSPAN PVST Interoperation, where required, or equivalent spanning-tree interoperability IEEE 802.1ad, IEEE 802.1AX, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1Qbb, IEEE 802.1s, IEEE 802.1w, IEEE 802.3ad, IEEE 802.3ae, IEEE 802.3ba, 802.3bm, IEEE 802.3x Storm Control STP BPDU Guard STP Root Guard Loop Guard
15	The proposed solution must support routing protocols at least RIP, OSPF, BGP

Table D: Next Generation Firewall Substation (40 units)

Req No.	Description
1	The proposed solution must allow the detection and filtering of traffic by content.
2	The proposed solution must allow the detection and filtering of Distributed Denial of Service (DDoS) type attacks, by defining policies.
3	The proposed solution must allow the detection and filtering of applications.
4	The proposed solution must allow the establishment of antivirus and web/URL filtering rules. Anti-spam, email reputation or an equivalent email-related protection mechanism shall be available where supported by the proposed NGFW security bundle or may be satisfied by an existing integrated email-security control.
5	The proposed solution must allow establishing the rules of the QoS and traffic shaping.
6	The proposed solution must allow establishing the rules of the firewall according to the criteria of GeoIP.
7	The proposed solution must allow the application of network traffic blocking rules with source or destination addresses BootNet, which is periodically updated.
8	The proposed solution must allow the establishment of filtering rules web – web inspection/Filter.
9	The proposed solution must ensure the minimum requirements to ensure high availability: Operation Active-Active and/or Active-Passive, or an equivalent high-availability mode supported by the proposed platform Functionality Stateful Failover (Firewall and VPN) Detection and notification for non-functional equipment Network connection monitoring Functionality Link Failover
10	The proposed solution must ensure the minimum requirements for ensuring the monitoring of the hardware components: Support syslog. Support SNMPv3 and, where required for legacy monitoring, SNMPv2c. Email notification for alerts. Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.
11	The solution must allow the creation/division and management of logical/virtual devices, offering the possibility to allocate, reserve or limit hardware and software resources for each instance. Each instance must function as an independent logical/virtual instance, ensuring complete isolation between different instances for independent security and administration. Each logical/virtual instance shall support independent configuration and administration of routing tables, NAT, firewall policies, VPN instances, security policies, and assigned physical and logical interfaces.

	Functionalities include, but are not limited to: Allocation, reservation or limitation of resources per instance, such as network interfaces and processing capacity. Dedicated physical CPU cores shall not be mandatory. The ability to configure and manage routing tables, firewall policies, and distinct security settings for each instance. Support for advanced traffic segregation and isolation functionalities, including physical and logical separation of network traffic between instances. The facility to perform specific management and monitoring operations for each instance, ensuring the flexibility and scalability necessary to meet the varied security needs of the organization. The solution must also include user access management functionality, allowing specific access rights and privileges to be assigned to different user groups. This should ensure that administrators can finely control and restrict user access to different instances and their respective resources while maintaining a high level of security and operational integrity.
12	The proposed solution must allow filtering of traffic of at least 10Gbps.
13	The proposed solution must have tunneling capability IPSec(VPN) at least 6 Gbps.
14	The proposed solution must have SSL traffic inspection capability of at least 0,9Gbps.
15	The proposed solution must have the ability to inspect traffic by enabling the IPS functionality of at least 1Gbps.
16	The proposed solution must have the ability to establish up to 0,7 million simultaneous TCP sessions.
17	The proposed solution must have the ability to establish at least 35,000 new sessions per second.
18	Each piece of hardware must contain at least 10 x 1GE RJ45.
19	Each piece of hardware must contain at least one dedicated console interface (RJ45 serial, USB, USB-C or equivalent).

Training for System Administrators

	IT Staff Training Services
1	General Training Requirements: • Participants: Minimum four (4) representatives of the Beneficiary. • Language: Romanian or English; training materials in Romanian or English. • Training provider: Official manufacturer training course delivered by the manufacturer or an authorized training partner/instructor. • Certification: Official certificate of completion issued or recognized by the manufacturer. • Content: Training shall include practical hands-on exercises relevant to the equipment and technologies supplied. • Venue and delivery: Training shall be conducted offline at the Beneficiary's premises in Chisinau, Republic of Moldova. • Logistics and costs: The Supplier shall organize and cover all training-related costs, including instructor, materials, equipment and any other organizational costs required for delivery.
2	Module A - Firewall Administration Duration: minimum 2 days, 4-8 hours per day. The training shall cover at least: Firewall architecture and administration; Security policies, objects, interfaces and zones; NAT and routing; IPsec and remote access VPN; Security profiles (IPS, Anti-Malware, Web/DNS Filtering and Application Control); SSL/TLS inspection; Logging, monitoring and troubleshooting; High Availability; Backup, restore and software/firmware upgrade; Firewall interaction with other network equipment owned by the beneficiary.

3	Module B - Network Switch Duration: minimum 2 days, 4-8 hours per day. The training shall cover at least: Switch architecture and administration; VLANs and trunking; Spanning Tree and loop prevention; Link aggregation / LACP; Layer 2 and Layer 3 switching; Routing and ACLs; Port security and network segmentation; PoE/PoE+, where applicable; Stacking/MLAG or equivalent redundancy; SFP/SFP+/QSFP interfaces; Monitoring, backup, upgrade and troubleshooting; Integration with the Beneficiary's existing network infrastructure.
---	--

• **Delivery Requirements**

Delivery Requirements	
Delivery date and time	Bidder shall deliver the goods in 60 days after Contract signature.
Delivery Terms (INCOTERMS 2020)	DDP
Customs clearance (must be linked to INCOTERM)	☒ Supplier/Bidder UNDP shall provide a Tax Exemption letter for Customs clearance.
Exact Address(es) of Delivery Location(s)	Moldelectrica central site MD 2012, Republica Moldova, mun. Chişinău, str. V. Alecsandri, 78.
Warranty Period	36 months for hardware Items #1–4; technical support and subscriptions for at least 36 months
Local Service Support	Availability of a local authorized representative, dealer, partner, or service provider in the Republic of Moldova capable of handling warranty claims, hardware repair/replacement (RMA), and after-sales support services for the offered equipment, including: • Technical support on the overall use and operation of the supplied hardware and software, with a response time of no more than twenty-four (24) hours (or one (1) working day); • Remote technical support with a response time of no more than one (1) working day and on-site technical intervention in the Republic of Moldova, where required, within no more than five (5) working days from receipt of the service request, unless a shorter timeframe is required under the warranty conditions applicable to the offered equipment; • Brand new replacement within a maximum of one (1) month if Purchased Unit is beyond repair (within warranty period).

ANNEX 2: QUOTATION SUBMISSION FORM

Bidders are requested to complete this form, including the Company Profile and Bidder's Declaration, sign it and return it as part of their quotation along with Annex 3: Technical and Financial Offer. The Bidder shall fill in this form in accordance with the instructions indicated. No alterations to its format shall be permitted and no substitutions shall be accepted.

Name of Bidder:	Click or tap here to enter text.	
RFQ reference:	RfQ26/03382:JET_Provision of Next Generation Firewalls, Network Switches and Related Services for Moldelectrica	Date: Click or tap to enter a date.

Company Profile

Item Description	Detail
Legal name of bidder or Lead entity for JVs	Click or tap here to enter text.
Legal Address, City, Country	Click or tap here to enter text.
Website	Click or tap here to enter text.
Year of Registration	Click or tap here to enter text.
Legal structure	Choose an item.
Are you a UNGM registered vendor?	☐ Yes ☐ No If yes, insert UNGM Vendor Number
Quality Assurance Certification (e.g. ISO 9000 or Equivalent) (If yes, provide a Copy of the valid Certificate):	☐ Yes ☐ No
Does your Company hold any accreditation such as ISO 14001 or ISO 14064 or equivalent related to the environment? (If yes, provide a Copy of the valid Certificate):	☐ Yes ☐ No
Does your Company have a written Statement of its Environmental Policy? (If yes, provide a Copy)	☐ Yes ☐ No
Does your organization demonstrate significant commitment to sustainability through some other means, for example internal company	☐ Yes ☐ No

policy documents on women empowerment, renewable energies or membership of trade institutions promoting such issues <i>(If yes, provide a Copy)</i>				
Is your company a member of the UN Global Compact	☐ Yes ☐ No			
Bank Information	Bank Name: Click or tap here to enter text. Bank Address: Click or tap here to enter text. IBAN: Click or tap here to enter text. SWIFT/BIC: Click or tap here to enter text. Account Currency: Click or tap here to enter text. Bank Account Number: Click or tap here to enter text.			
Previous relevant experience: 3 (three) contracts in the field of supply of IT equipment completed in the past 3 (three) years				
Name of previous contracts	Client & Reference Contact Details including e-mail	Contract Value (please indicate currency)	Period of activity (month/ year)	Types of activities undertaken

Bidder's Declaration

Yes	No	
☐	☐	Requirements and Terms and Conditions: I/We have read and fully understand the RFQ, including the RFQ Information and Data, Schedule of Requirements, the General Conditions of Contract, and any Special Conditions of Contract. I/we confirm that the Bidder agrees to be bound by them.
☐	☐	I/We confirm that the Bidder has the necessary capacity, capability, and necessary licenses to fully meet or exceed the Requirements and will be available to deliver throughout the relevant Contract period.
☐	☐	Ethics: In submitting this Quote I/we warrant that the bidder: has not entered into any improper, illegal, collusive or anti-competitive arrangements with any Competitor; has not directly or indirectly approached any representative of the Buyer (other than the Point of Contact) to lobby or solicit information in relation to the RFQ ;has not attempted to influence, or provide any form of personal inducement, reward or benefit to any representative of the Buyer.
☐	☐	I/We confirm to undertake not to engage in proscribed practices, , or any other unethical practice, with the UN or any other party, and to conduct business in a manner that averts any financial, operational, reputational or other undue risk to the UN and we have read the United Nations Supplier Code of Conduct : https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct and acknowledge that it provides the minimum standards expected of suppliers to the UN.
☐	☐	Conflict of interest: I/We warrant that the bidder has no actual, potential, or perceived Conflict of Interest in submitting this Quote or entering a Contract to deliver the Requirements. Where a Conflict

Yes	No	
		of Interest arises during the RFQ process the bidder will report it immediately to the Procuring Organization's Point of Contact.
☐	☐	Prohibitions and Sanctions: I/We hereby declare that our firm, ultimate beneficial owners, affiliates or subsidiaries or employees, including any JV/Consortium members or subcontractors or suppliers for any part of the contract is not under procurement prohibition by the United Nations, including but not limited to prohibitions derived from the Compendium of United Nations Security Council Sanctions Lists and have not been suspended, debarred, sanctioned or otherwise identified as ineligible by any UN Organization or the World Bank Group or any other international Organization.
☐	☐	Bankruptcy: I/We have not declared bankruptcy, are not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against them that could impair their operations in the foreseeable future.
☐	☐	Offer Validity Period: I/We confirm that this Quote, including the price, remains open for acceptance for the Offer Validity.
☐	☐	I/We understand and recognize that you are not bound to accept any Quotation you receive, and we certify that the goods offered in our Quotation are new and unused.
☐	☐	By signing this declaration, the signatory below represents, warrants and agrees that he/she has been authorized by the Organization/s to make this declaration on its/their behalf.

Signature: _____

Name: Click or tap here to enter text.

Title: Click or tap here to enter text.

Date: Click or tap to enter a date.

ANNEX 3: TECHNICAL AND FINANCIAL OFFER - GOODS AND SERVICES

Bidders are requested to complete this form, sign it and return it as part of their bid along with Annex 2: Quotation Submission Form. The Bidder shall fill in this form in accordance with the instructions indicated. No alterations to its format shall be permitted and no substitutions shall be accepted.

Name of Bidder:	Click or tap here to enter text.	
RFQ reference:	RfQ26/03382: JET_Provision of Next Generation Firewalls, Network Switches and Related Services for Moldelectrica	Date: Click or tap to enter a date.

Bidders must include all costs related to the performance of the services in their quotation price (delivery of all goods and equipment, transport costs, unloading at the delivery site, installation etc.)

Bidders shall fill up the financial offer table for the all the items they are applying.

Currency of the Quotation: USD Dollars for both local and international vendors or MDL Moldovan Leu for local vendors (VAT exclusive)						
INCONTERMS DDP Chisinau						
Item No	Description	UOM	Qty	Unit price [please insert currency]	Transportation, Insurance, and other Costs [please insert currency]	Total price [please insert currency]
1	Next Generation Firewall (Table A)	pcs	8			
2	Access Switch 24+4 ports (Table B)	pcs	8			
3	Core Switch (Table C)	pcs	1			
4	Next Generation Firewall Substation (Table D)	pcs	40			
5	Training for System Administrators	service	1			
Total Final and All-inclusive Price [please insert currency]						

Compliance with Requirements

	You Responses		
	Yes, we will comply	No, we cannot comply	If you cannot comply, pls. indicate counter - offer
Full compliance with all requirements as specified in Annex 1	☐	☐	Click or tap here to enter text.
Delivery Term (INCOTERMS): DDP	☐	☐	Click or tap here to enter text.
Delivery Lead Time: 60 days	☐	☐	Click or tap here to enter text.
Warranty: minimum 36 months for hardware Items #1–4; technical support/subscriptions: minimum 36 months	☐	☐	Click or tap here to enter text.
Local Service Support	☐	☐	Click or tap here to enter text.
Validity of Quotation: 60 days	☐	☐	Click or tap here to enter text.
I, the undersigned, certify that I am duly authorized to sign this quotation and bind the company below in event that the quotation is accepted.			
<i>Exact name and address of company</i> Company Name Click or tap here to enter text. Address: Click or tap here to enter text. Phone No.: Click or tap here to enter text. Email Address: Click or tap here to enter text.		Authorized Signature: _____ _____ Date: Click or tap here to enter text. Name: Click or tap here to enter text. Functional Title of Authorised Signatory: Click or tap here to enter text. Email Address: Click or tap here to enter text.	

ANNEX 4: TECHNICAL RESPONSIVENESS TABLE

Bidders are requested to complete this form, sign it and return it as part of their bid along with Annex 2: Quotation Submission Form and Annex 3: Technical and Financial Offer. The Bidder shall fill in this form in accordance with the instructions indicated. No alterations to its format shall be permitted and no substitutions shall be accepted.

Name of Bidder:	Click or tap here to enter text.	
RFQ reference:	RfQ26/03382: JET_Provision of Next Generation Firewalls, Network Switches and Related Services for Moldelectrica	Date: Click or tap to enter a date.

Bidders shall supplement the information provided in the tables below with detailed description of the offered goods, including Product Data Sheet.

Bidders shall complete every requirement below and provide the exact offered value or feature, brand/model, SKU/part number and official manufacturer evidence reference. A generic 'Comply' statement without supporting evidence may be treated as non-responsive.

Technical Responsiveness Matrix

#	Technical requirements	Conformity (Yes/No)	Offered Brand, Model and Exact characteristics <i>(Technical characteristics should not be less/worse than those listed in Annex 1: Schedule of Requirements)</i>
			Brand/ model <i>(please indicate)</i>
General requirements for all deliverables			
1	The supplier shall demonstrate that the proposed hardware and software are authorized for supply and use in the Republic of Moldova. The bidder shall provide a valid Manufacturer Authorization Form (MAF), or equivalent official confirmation issued by the manufacturer, confirming that the bidder is authorized to offer and supply the proposed products, licenses, subscriptions and related support services in the Republic of Moldova.		
2	The Supplier must demonstrate that the products offered are as per the specification stipulated in the tender document, and as committed by the supplier, without any extra cost to the Moldelectrica.		
3	The supplier undertakes that in respect of licensed software items, these shall be supplied with the authorized license certificate, and that it shall be sourced from an authorized source.		
4	Communications (oral and written) must be conducted, and documentation must be		

	submitted in English or Romanian. The licenses and any services provided must also be in the English or Romanian language.		
5	After the supplier delivers the products, all rights and obligations will be assigned to the beneficiary of the solution, Moldelectrica.		
6	The solutions must include all the licenses necessary for its operation, to the parameters and values requested in these specifications, including those related to extensibility, and there must not be any limitation.		
7	For the hardware components the minimum required warranty is 36 months while the technical support and subscriptions are for a period of at least 3 years.		
8	During the warranty the Supplier will replace defective components in no more than seven (7) calendar days.		
9	Solutions must include access to the manufacturer's web portal in order to contact technical support and download updates for a period of at least 3 years.		
10	The proposed solution must be delivered with all necessary cables for connection in rack.		
11	The Supplier shall include, at no additional cost, the following consumables for the entire scope of supply under the contract (8 NGFWs, 8 access switches, 1 core switch and 40 substation firewalls): • UTP Cable Category 6A/6E: minimum 300 meters; • RJ45 Connectors Category 6A/6E: minimum 200 pieces; • UTP Patch Cords Category 6A/6E: minimum 50 pieces of each approximate length: 0.5 m, 1 m, 3 m, 5 m and 10 m; • Single-Mode LC-LC Optical Patch Cords: minimum 30 pieces of each approximate length: 0.5 m, 1 m, 2 m, 3 m, 5 m, 10 m and 20 m; • Single-Mode LC-SC Optical Patch Cords: minimum 30 pieces of each approximate length: 0.5 m, 1 m, 2 m, 3 m and 5 m; • Single-Mode SC-SC Optical Patch Cords: minimum 30 pieces of each		

	approximate length: 0.5 m, 1 m, 2 m, 3 m and 5 m. The above quantities are aggregate quantities for the entire scope of supply and shall not be interpreted as quantities required per site or per equipment unit. All costs shall be included in the offered price.		
12	All delivered components (hard, soft, licenses) must be updated to the latest stable version.		
13	All requirements are minimum and mandatory. An equivalent solution is acceptable where the bidder demonstrates equal or better functionality, performance, security, support and interoperability.		
Table A: Next Generation Firewall			
1	The proposed solution must allow the detection and filtering of traffic by content.		
2	The proposed solution must allow the detection and filtering of Distributed Denial of Service (DDoS) type attacks, by defining policies.		
3	The proposed solution must allow the detection and filtering of applications.		
4	The proposed solution must allow the establishment of antivirus and web/URL filtering rules. Anti-spam, email reputation or an equivalent email-related protection mechanism shall be available where supported by the proposed NGFW security bundle or may be satisfied by an existing integrated email-security control.		
5	The proposed solution must allow establishing the rules of the QoS and traffic shaping.		
6	The proposed solution must allow establishing the rules of the firewall according to the criteria of GeoIP.		
7	The proposed solution must allow the application of network traffic blocking rules with source or destination addresses BootNet, which is periodically updated.		
8	The proposed solution must allow the establishment of filtering rules web – web inspection/Filter.		
9	The proposed solution must ensure the minimum requirements to ensure high availability:		

	• Operation Active-Active and/or Active-Passive, or an equivalent high-availability mode supported by the proposed platform • Functionality Stateful Failover (Firewall and VPN) • Detection and notification for non-functional equipment • Network connection monitoring • Functionality Link Failover		
10	The proposed solution must ensure the minimum requirements for ensuring the monitoring of the hardware components: • Support syslog. • Support SNMPv3 and, where required for legacy monitoring, SNMPv2c. • Email notification for alerts. • Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.		
11	The solution must allow the creation/division and management of logical/virtual devices, offering the possibility to allocate, reserve or limit hardware and software resources for each instance. Each instance must function as an independent logical/virtual instance, ensuring complete isolation between different instances for independent security and administration. Each logical/virtual instance shall support independent configuration and administration of routing tables, NAT, firewall policies, VPN instances, security policies, and assigned physical and logical interfaces. Functionalities include, but are not limited to: • Allocation, reservation or limitation of resources per instance, such as network interfaces and processing capacity. Dedicated physical CPU cores shall not be mandatory. • The ability to configure and manage routing tables, firewall policies, and distinct security settings for each instance. • Support for advanced traffic segregation and isolation functionalities, including physical and logical separation of network traffic between instances. • The facility to perform specific management and monitoring operations for each instance, ensuring the flexibility and scalability necessary to meet the varied security needs of the organization.		

	The solution must also include user access management functionality, allowing specific access rights and privileges to be assigned to different user groups. This should ensure that administrators can finely control and restrict user access to different instances and their respective resources while maintaining a high level of security and operational integrity.		
12	The proposed solution must allow filtering of traffic of at least 20Gbps.		
13	The proposed solution must have tunneling capability IPSec(VPN) at least 10 Gbps.		
14	The proposed solution must have SSL traffic inspection capability of at least 1Gbps.		
15	The proposed solution must have the ability to inspect traffic by enabling the IPS functionality of at least 2Gbps.		
16	The proposed solution must have the ability to establish up to 1,5 million simultaneous TCP sessions.		
17	The proposed solution must have the ability to establish at least 56,000 new sessions per second.		
18	Each piece of hardware must contain at least 4 x 1GE SFP, with SFP modules included.		
19	Each piece of hardware must contain at least 16 x 1GE RJ45.		
20	Each piece of hardware must contain at least 2 x 10GE SFP+, with SFP modules included.		
21	Each piece of hardware must contain at least one dedicated out-of-band management interface (RJ45 Ethernet, SFP/SFP+ Ethernet or equivalent).		
22	Each piece of hardware must contain at least one dedicated console interface (RJ45 serial, USB, USB-C or equivalent).		
Table B: Access Switch 24+4 ports			
1	The proposed solution must ensure the minimum requirements to ensure high availability: - Operation using a multi-device redundancy mechanism appropriate to the proposed architecture - Detection and notification for non-functional equipment - Network connection monitoring		

	• Functionality Link Failover • Multi-Chassis Link Aggregation (MCLAG), MLAG, stacking or an equivalent multi-device redundancy mechanism		
2	The proposed solution must ensure the minimum requirements for ensuring the monitoring of hardware components: • Real-time and historical data monitoring • Support syslog • Support SNMPv3 and, where required for legacy monitoring, SNMPv2c • Email notification for alerts • Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.		
3	The proposed solution must include switching capacity of at least 55Gbps.		
4	The proposed solution must have a network latency of max 4 us.		
5	The proposed solution must have a forwarding rate of at least 80 Mpps.		
6	Each piece of hardware must contain at least 4 x 10GE SFP, with SFP modules included (2 SR and 2 LR).		
7	Each piece of hardware must contain at least 24 x 1 GE PoE. PoE Power Budget min 350 W.		
8	Each piece of hardware must contain at least one dedicated console interface (RJ45 serial, USB, USB-C or equivalent).		
9	The proposed solution must support at least 4000 VLANs.		
10	The proposed solution must support IEEE 802.1Q VLAN encapsulation.		
11	The proposed solution must support Jumbo Frame as a minimum 9000 bytes.		
12	The proposed solution must support Link Aggregation Control Protocol (LACP), IEEE 802.3ad		
13	The proposed solution must support at least 8000 MAC addresses		
14	The proposed solution must support at least or similar: • Port-based VLAN • MAC-based VLAN • SVI (Virtual Switch interface) • Persistent MAC (sticky MAC) • ARP inspection		

	• ACL • DHCP Snooping • BPDU Guard • IP Source Guard • Uni-Directional Link Detection (UDLD) or equivalent link-failure detection mechanism • Per-port broadcast, multicast, unicast storm control • SPAN/RSPAN • PVST Interoperation, where required, or equivalent spanning-tree interoperability • Storm Control • STP BPDU Guard • STP Root Guard • Loop Guard		
Table C: Core Switch			
1	The proposed solution must ensure the minimum requirements to ensure high availability: • Operation using a chassis or multi-device redundancy mechanism such as stacking, MLAG/MCLAG or equivalent • Detection and notification for non-functional equipment • Network connection monitoring • Functionality Link Failover		
2	The proposed solution must ensure the minimum requirements for ensuring the monitoring of hardware components: • Real-time and historical data monitoring • Support syslog • Support SNMPv3 and, where required for legacy monitoring, SNMPv2c • Email notification for alerts • Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.		
3	The proposed solution must include switching capacity of at least 800Gbps.		
4	The proposed solution must have a network latency of max 2 us.		
5	The proposed solution must have a forwarding rate of at least 1300 Mpps.		
6	Each piece of hardware must contain at least 2 x 40/100GE QSFP+, with QSFP modules included.		
7	Each piece of hardware must contain at least 24 x 10GE SFP+, with SFP modules included.		

8	Each piece of hardware must contain at least one dedicated console interface (RJ45 serial, USB, USB-C or equivalent).		
9	The proposed solution must support at least 4000 VLANs.		
10	The proposed solution must support IEEE 802.1Q VLAN encapsulation.		
11	The proposed solution must support Jumbo Frame as a minimum 9000 bytes.		
12	The proposed solution must support Link Aggregation Control Protocol (LACP), IEEE 802.3ad		
13	The proposed solution must support at least 64000 MAC addresses		
14	The proposed solution must support at least or similar: • Port-based VLAN • MAC-based VLAN • SVI (Virtual Switch interface) • Persistent MAC (sticky MAC) • ARP inspection • ACL • DHCP Snooping • BPDU Guard • IP Source Guard • Uni-Directional Link Detection (UDLD) or equivalent link-failure detection mechanism • Per-port broadcast, multicast, unicast storm control • SPAN/RSPAN • PVST Interoperation, where required, or equivalent spanning-tree interoperability • IEEE 802.1ad, IEEE 802.1AX, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1Qbb, IEEE 802.1s, IEEE 802.1w, IEEE 802.3ad, IEEE 802.3ae, IEEE 802.3ba, 802.3bm, IEEE 802.3x • Storm Control • STP BPDU Guard • STP Root Guard • Loop Guard		
15	The proposed solution must support routing protocols at least RIP, OSPF, BGP		
Table D: Next Generation Firewall Substation			
1	The proposed solution must allow the detection and filtering of traffic by content.		

2	The proposed solution must allow the detection and filtering of Distributed Denial of Service (DDoS) type attacks, by defining policies.		
3	The proposed solution must allow the detection and filtering of applications.		
4	The proposed solution must allow the establishment of antivirus and web/URL filtering rules. Anti-spam, email reputation or an equivalent email-related protection mechanism shall be available where supported by the proposed NGFW security bundle or may be satisfied by an existing integrated email-security control.		
5	The proposed solution must allow establishing the rules of the QoS and traffic shaping.		
6	The proposed solution must allow establishing the rules of the firewall according to the criteria of GeoIP.		
7	The proposed solution must allow the application of network traffic blocking rules with source or destination addresses BootNet, which is periodically updated.		
8	The proposed solution must allow the establishment of filtering rules web – web inspection/Filter.		
9	The proposed solution must ensure the minimum requirements to ensure high availability: • Operation Active-Active and/or Active-Passive, or an equivalent high-availability mode supported by the proposed platform • Functionality Stateful Failover (Firewall and VPN) • Detection and notification for non-functional equipment • Network connection monitoring • Functionality Link Failover		
10	The proposed solution must ensure the minimum requirements for ensuring the monitoring of the hardware components: • Support syslog. • Support SNMPv3 and, where required for legacy monitoring, SNMPv2c. • Email notification for alerts.		

	• Support sFlow, NetFlow, IPFIX or an equivalent flow-export/telemetry mechanism.		
11	The solution must allow the creation/division and management of logical/virtual devices, offering the possibility to allocate, reserve or limit hardware and software resources for each instance. Each instance must function as an independent logical/virtual instance, ensuring complete isolation between different instances for independent security and administration. Each logical/virtual instance shall support independent configuration and administration of routing tables, NAT, firewall policies, VPN instances, security policies, and assigned physical and logical interfaces. Functionalities include, but are not limited to: • Allocation, reservation or limitation of resources per instance, such as network interfaces and processing capacity. Dedicated physical CPU cores shall not be mandatory. • The ability to configure and manage routing tables, firewall policies, and distinct security settings for each instance. • Support for advanced traffic segregation and isolation functionalities, including physical and logical separation of network traffic between instances. • The facility to perform specific management and monitoring operations for each instance, ensuring the flexibility and scalability necessary to meet the varied security needs of the organization. • The solution must also include user access management functionality, allowing specific access rights and privileges to be assigned to different user groups. This should ensure that administrators can finely control and restrict user access to different instances and their respective resources while maintaining a high level of security and operational integrity.		
12	The proposed solution must allow filtering of traffic of at least 10Gbps.		
13	The proposed solution must have tunneling capability IPSec(VPN) at least 6 Gbps.		
14	The proposed solution must have SSL traffic inspection capability of at least 0,9Gbps.		

15	The proposed solution must have the ability to inspect traffic by enabling the IPS functionality of at least 1Gbps.		
16	The proposed solution must have the ability to establish up to 0,7 million simultaneous TCP sessions.		
17	The proposed solution must have the ability to establish at least 35,000 new sessions per second.		
18	Each piece of hardware must contain at least 10 x 1GE RJ45.		
19	Each piece of hardware must contain at least one dedicated console interface (RJ45, USB, USB-C or equivalent).		
Training for System Administrators			
1	General Training Requirements Number of participants: minimum 4 representatives of the Beneficiary. Training language: Romanian or English. Training materials may be provided in Romanian or English. Training shall be an official manufacturer training course, delivered by the manufacturer or an authorized training partner or instructor. Participants shall receive an official certificate of completion/attendance issued or recognized by the manufacturer. Training shall include practical hands-on laboratory exercises relevant to the supplied equipment and technologies.		
2	Module A - Firewall Administration Duration: minimum 2 days, 4-8 hours per day. The training shall cover at least: Firewall architecture and administration; Security policies, objects, interfaces and zones; NAT and routing; IPsec and remote access VPN; Security profiles (IPS, Anti-Malware, Web/DNS Filtering and Application Control); SSL/TLS inspection; Logging, monitoring and troubleshooting; High Availability; Backup, restore and software/firmware upgrade;		

	Firewall interaction with other network equipment owned by the beneficiary.		
3	Module B - Network Switch Duration: minimum 2 days, 4-8 hours per day. The training shall cover at least: Switch architecture and administration; VLANs and trunking; Spanning Tree and loop prevention; Link aggregation / LACP; Layer 2 and Layer 3 switching; Routing and ACLs; Port security and network segmentation; PoE/PoE+, where applicable; Stacking/MLAG or equivalent redundancy; SFP/SFP+/QSFP interfaces; Monitoring, backup, upgrade and troubleshooting; Integration with the Beneficiary's existing network infrastructure.		