# Section 5a: Schedule of Requirements and Technical Specifications/Bill of Quantities

**SPECIFICATION**

**for the computer and networking equipment   
for the Ministry of Digital Transformation of Ukraine**

**ITB/2022/453**

**PROMPT #UKR-0000198875**

**1. BACKGROUND**

In the conditions of martial law, a significant emphasis in the activities of the Ministry of digital transformation of Ukraine (MDT) and subordinate institutions is placed on ensuring the failure resistance of the information and communication systems of the Unified State Web Portal of Electronic Services (the “Diia” Portal), the Integrated Electronic Identification System, the Qualified Provider of Electronic Trust Services "Diia", the Central Certification body, increasing the level of cyber security, countering existing threats and attacks, supporting more productive and stable operation of the mentioned information and communication systems.

The current state of the attacks by Russia on the critical infrastructure of Ukraine obliges to reformat the objects of the critical infrastructure to the regime of disaster-resistant functioning. This determines the creation of backup software and technical complexes, which are not inferior to the main ones in terms of their functionality and performance.

Considering the importance and urgency of establishing a stable operation of information and communication systems, the MDT, together with the "Diia" State owned enterprise analysed the technical condition of the equipment of the main and reserve technical sites, which ensures the operation of the relevant information systems, and established the need to backup active network equipment, cryptographic information protection equipment, firewalls and necessary passive network equipment.

Taking into account the strategic importance of an urgent solution to the issue of ensuring uninterrupted operation of information and communication systems, the holder of which is the MDT, the MDT approached DIA Support project with a request to support the procurement of the specified server equipment.

**2. MAIN OBJECTIVE OF THE ASSIGNMENT AND SCOPE OF WORK**

Procurement and delivery of following equipment:

**Lot 1 – Network cables** (Technical specification, contained in the Table 1):

* Network cable 0.5 m. length – 15 pcs.
* Network cable 1 m. length – 20 pcs.
* Network cable 2 m. length – 20 pcs.
* Network cable 3 m. length – 20 pcs.
* Network cable 4 m. length – 20 pcs.
* Network cable 5 m. length – 25 pcs.

**Lot 2 – USB cables and adaptors:**

* USB/COM adapter (Technical specification, contained in the Table 2) – 4 pcs.
* USB 3.0 extender 1.5 m length (Technical specification, contained in the Table 3) – 4 pcs.
* USB 3.0 extender 2 m length (Technical specification, contained in the Table 3) – 4 pcs.
* Power extender with USB ports (Technical specification, contained in the Table 4) - 2 pcs.
* USB hub (Technical specification, contained in the Table 5) – 3 pcs.
* Network adapter USB/RJ-45 (Technical specification, contained in the Table 6) – 2 pcs.

**Lot 3 – External hard drive** (Technical specification, contained in the Table 7) – 2 pcs.

**Lot 4 – Router** (Technical specification, contained in the Table 8) – 2 pcs.

**Lot 5 – Networking equipment**

* Router/Firewall (Technical specification, contained in the Table 9) - 2 pcs.
* Network screen (Technical specification, contained in the Table 10) - 2 pcs.
* Switch (Technical specification, contained in the Table 11) - 4 pcs.

**Delivery Terms:** DAP, Kyiv, Ukraine.

**Address of delivery:** Vasylia Tiutiunnyka str. 5V (5В), Kyiv, Ukraine

Delivery procedure details will be provided to contract awarded bidder.

Table 1

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Design of cable/adapter | * RJ-45 connector / on both sides |
| Number of cores | * 8 |
| Conductor structure | * copper (Cu) |
| Category Ethernet | * Cat 6 |
| outer shell material | * LSZH |
| Operating temperature | * -10...75°C |
| Data transfer rate | * Not less than 10 Gb/s |
| Patch cord diameter | * no more than 3.8 mm |
| PoE compliance | * must be supported by IEEE 802.3af/802.3at (48 cables in a bundle) and 802.3bt type 3 and type 4 (24 cables in a bundle) PoE applications |
| Warranty obligations | * at least 12 months from the manufacturer |

Table 2

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Type | * USB/COM adapter |
| Controller | * PL2303 |
| Type | * USB 2.0 |
| Output Type | * COM |
| Length | * 1.5 m |

Table 3

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Type | * USB Extender |
| Input Type | * USB 3.0 AM |
| Type Output | * USB 3.0 AF |

Table 4

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Type | * Power extender with USB |
| Number of power sockets | * At least 3 |
| Filter connection type | * Europlug with grounding (Type F) |
| Maximum load current | * Not less then 10 A |
| Type of power sockets | * Europlug with grounding (Type F ) |
| Number of USB ports | * Not less then 6 |
| Power of USB ports | * 5V, not less then 3.4A -17W |
| Type of USB ports | * USB AF |

Table 5

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Type | * USB Hub |
| Output ports | * Ethernet, HDMI, USB 3.0, USB Type-C |
| Connection interface | * HDMI, RJ45, USB 3.0, USB Type-C |
| Compatible | * At least with Apple, Asus, HP, Lenovo, Dell |
| Number of USB outputs, | * At least 4 |
| Fast charging support | * Maximum power up to 100W |
| Laptop connection type | * Type-C |
| Maximum transfer speed | * 5 Gbit/s |

Table 6

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Type | * [Network card FE](https://hotline.ua/ua/computer/setevye-adaptery/558986/) |
| Connection interface | * USB 2.0 |
| Maximum connection speed | * 100 Mbit/s |
| External connectors | * 1xRJ-45 |

Table 7

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Type | * External hard drive |
| Capacity | * Not less then 5 TB |
| Form factor | * [2.5"](https://hard.rozetka.com.ua/ua/hdd/c80084/21297=3889/) |
| technology | * [HDD](https://hard.rozetka.com.ua/ua/hdd/c80084/31580=38160/) |
| Connection interface | * [USB 3.2 Gen 1](https://hotline.ua/ua/computer/zhestkie-diski/942/) |

Table 8

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| General requirements | * Router with network shielding functions * The maximum performance of the router is not lower than 7600 packets per second * Router performance of at least 20 Gbps (for IMIX traffic) * Router performance of at least 40 Gbit/s (for 1518-byte packets) * The maximum performance of the router in the mode of inter-network shielding is not lower than 8100 packets per second * The performance of the router in the mode of inter-network shielding is at least 20 Gbit/s (for IMIX traffic) * The performance of the router in the mode of inter-network shielding is at least 40 Gbit/s (for packets of 1518 bytes) * The performance of the IPS intrusion detection and prevention system is at least 10 Gbps (if activated by a separate license) * Productivity of the intelligent application recognition system at least 18 Gbps (DPI) (if activated by a separate license) * Performance in "Next Generation Firewall" mode at least 7 Gbps (stateful firewall, logging, DPI, UserFW, IPS, URL-filtering) * IPsec VPN performance with a packet length of 1400 bytes at least 10 Gbps * IPsec VPN performance of at least 5 Gbps (for IMIX traffic) * Work under the control of a modular operating system, which allows starting, stopping, restarting individual software processes without affecting other running processes |
| Architecture and form factor | * The possibility of installing two routers in a 1RU 19" mounting structure that meets the ANSI/EIA-310 standard * Mounting height no more than 1 UA (44.45 mm) |
| Requirement for physical interfaces | * At least 8 Ethernet 1000/10GBaseX-X SFP/SFP+ ports * At least 10 Ethernet 1000/10Gbase-X SFP/SFP+ ports * At least 2 dedicated Ethernet 1000/10Gbase-X SFP/SFP+ ports to form a cluster * At least 1 Ethernet 1000Base-T RJ45 port for out-of-band management * At least 2 USB ports for configuration download and software upgrade operations |
| Physical parameters | * Availability of alternating current power supply with 50Hz/220V parameters * The delivery set consists of a power supply unit with a power cable, a console cable, a set for mounting two routers in a rack |
| Software requirements | * Supports the function of configuring software probes in the form of ICMPs, UDP/TCP, HTTP protocol packets to determine the availability of network nodes and parameters of communication channels * Taking into account statistical information about data flows processed by the router. The information should include the addresses of the sender and the recipient, the start and end time of the data exchange, the identifiers of the transport layer protocols * Support for "transparent" operating mode and router mode * The possibility of activating the UTM functionality with a separate license without the need to replace the software. Functionality of UTM, including antivirus check, web filtering using a cloud service, content filtering, antispam * The Web Filtering functionality should support retrieving the resource category from the cloud service being checked, as well as manually creating URL blacklists and whitelists |
| Requirements for the functionality of the physical level | * Supports channel reservation mechanism between devices. At the same time, both separate physical communication lines and logical channels consisting of several physical communication lines can act as channels |
| Requirements for level 2 functionality | * Q-in-Q support |
| Requirements for level 3 functionality | * Support for Static Routing (RFC 1812) * Bidirectional Forwarding Detection (BFD) protocol support * Support for routing protocols RIP v1/v2, OSPF, BGPv4, MP-BGP, IS-IS * Support for ICMPv6, OSPFv3, RIPng, DHCPv6, IPv6, BGP extension for IPv6 * RSVP, RSVP-TE protocol support * LDP protocol support * Support for MPLS Layer 3 VPN functionality * Support for MPLS Layer 2 VPN functionality * Support for VPLS functionality * Support for NG-MVPN functionality * MPLS Fast Reroute support * Support for OSPF-Traffic Engineering, IS-IS-Traffic Engineering extensions * Support for selection function in the device context of logical devices – virtual routers * At least 2000000 IPv4 routes in the routing table * At least 2000000 IPv6 routes in the routing table |
| High availability | * Ability to implement active-active device reservation * Configuration synchronization between cluster devices * Synchronization of firewall and VPN connection information between cluster devices * Detection of failure of the cluster or the communication line between the cluster devices * Support for In Service Software Upgrade when working in cluster mode * Monitoring the status of interfaces, internal nodes, external IP addresses and making a decision to switch the cluster in case of their failure/unavailability * BGP Graceful protocol restart function * IS-IS Graceful protocol restart function * OSPF Graceful protocol restart function * VRRP protocol support |
| Multicast transmission (Multicast) | * Support for multicast protocols:   + Internet Group Management Protocol (IGMP v1/2/3)   + PIM-SM/DM/SSM   + Session Description Protocol (SDP)   + Session Announcement Protocol (SAP)   + Distance Vector Multicast Routing Protocol (DVMRP)   + Multicast Source Discovery Protocol (MSDP)   + Support IP MPLS Multicast VPN, NG-MVPN |
| Quality of Service (QoS) | * RFC2474 IPv4 Diffserv standard support * Support for queue management mechanisms:   + Weighted Random Early Drop (WRED)   + Class-based queue management with prioritization   + Queue management based on VLAN, data-link connection identifier (DLCI), interface |
| Informational security | * Functionality of the inter-network screen of the statefull class * Ability to activate built-in anti-virus protection, antispam, Web filtering, intrusion detection and prevention systems * Support for Network Access Control technology to control user access to network resources * When activated by a separate license, support for the function of defining applications that exchange data based on application signatures, including defining applications that work on non-standard TCP/UDP ports, writing own signatures, defining nested applications. * At the same time, on the basis of the received data, the following functions should be supported: blocking of selected applications, collection of application data exchange statistics, application of QoS mechanisms * Support for creating address books and address sets for use in security policies * Support for content filtering technology * Support for at least 2000 simultaneous IPSec VPN tunnels * At least 175,000 sessions per second * At least 5,000,000 simultaneous sessions * At least 2,000 demilitarized zones (DMZs) * At least 60,000 security policies * Support for NAT with Port Address Translation (PAT), static NAT, destination NAT with PAT, Persistent NAT, NAT64 * Support for the following Application Layer Gateways protocols: DNS, DDNS, FTP/IPv6 FTP, H.323, Avaya H.323, MS-RPC, Sun-RPC, PPTP, Real-Time Streaming Protocol (RTSP) including interleave mode, Remote shell, SCCP, SCCP v20, SIP, SMTP, IKE/ESP, SQL, TALK, PTSP, TFTP, MGCP * Access control lists (ACL) support * Support for applying different security policies to different MS Active Directory users or user groups. Integration with MS Active Directory should be carried out without the use of additional software agents. * Support for the SSL Forward Proxy functionality – decryption of SSL traffic on the fly for the purpose of inspection and application of security policies. * Support for sending files for scanning to a zero-day virus detection service, which includes scanning by no less than six antivirus engines, static analysis with the parsing of program instructions, and dynamic analysis with the launch of the scanned file in a virtual environment with analysis of its activity. (subject to the appropriate license) * Support for checking sender/recipient IP addresses, domains and recipient URLs against a database of malicious and suspicious resources to block protected users from accessing them. The reputation of the resource must be maintained. (subject to the appropriate license) * Support for loading own dynamic lists of resource addresses, access to which can be allowed or prohibited. Lists should be loaded dynamically without the need to enter them into the device configuration. * Simple Certificate Enrolment Protocol support |
| Management | * Support for HTTP/HTTPs management * SSH protocol support * SNMP v1/v2c/v3 protocol support * SMTP protocol support for sending emails to a local or remote SMTP server * OSPF RMON support * IEEE 802.3ah Link Fault Management (LFM) standard support * Support for RADIUS, LDAP, TACACS+, SecurID protocols * Support for storing on the device the backup configuration of the device * Support for returning the device to its previous configuration * Support for automatic return of the device to the previous working configuration * At least 49 functions of automatic saving of previous configurations * The number of saved configurations is not limited by the operating system |
| Other | * Support for returning the device to the previous software version * Checking the consistency of the configuration before use * Ability to configure the device through the web interface * Support for NTP, DNS, Syslog protocols * Support for DHCP server, DHCP Relay, DHCP client functionality |

Table 9

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| General requirements | * The network security and SD-WAN routing device must be a device that performs intelligent traffic routing (SD-WAN), network traffic inspection and corporate infrastructure protection in accordance with the following requirements * If, according to the functionality of the device or according to the architectural approach, the implementation of technical requirements requires additional systems, devices or licenses, then all this should be included in the delivery set, taking into account the requirements for the term and functionality of technical support * All necessary licenses to provide the functionality and quantitative performance indicators specified in these requirements must be included in the proposed solution * The equipment should not have end-of-sale and end-of-life (EOS/EOL) announcements from the manufacturer * NGFW must have a valid expert opinion of the State Service for Special Communications and Information Protection of Ukraine on compliance with the requirements of the legislation in the field of information protection or pass the appropriate state examination at the time of submission of the tender offer by the Participant * All functional requirements and quantitative performance indicators must be supported in the manufacturer's documentation |
| Architecture and form factor | * Software and hardware complex for installation in a standard 19" mounting cabinet |
| Interfaces and interface modules | * Not less than 16 \* GE RJ45 * Not less than 8 \* GE SFP * Not less than 8 \* 10GE SFP+ * At least 1 \* GE RJ45 management port (OOB MGMT) * At least 1 \* RJ45 console port * At least 1 \* USB port |
| Power supply | * 2 power supplies (100-240V AC, 50-60 Hz) that support "hot" replacement |
| Internal storage | * Internal storage (SSD) with a total volume of at least 480 GB for local storage of configuration files, software, etc. |
| Routing and SD-WAN | * Static Routing and Policy Based Routing (PBR) * Dynamic routing protocols: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4 * Simultaneous use of physical and logical interfaces with various types of connections (MPLS, broadband Internet, LTE, etc.) for effective traffic routing * Evaluation of the quality of SD-WAN communication channels by sending packets or requests to certain nodes in the network or by passive methods * Monitoring the characteristics of communication channels in real time (packet loss, jitter, latency) and their graphic display (gui real-time monitor) * SLA control for user applications (applications) based on the characteristics of communication channels (packet loss, jitter, latency) in real time * Determination of various algorithms/strategies for the selection of communication channels for routing application and service traffic based on SLA compliance criteria, best values ​​of communication channel characteristics, etc. * Determination of application and service traffic routing rules through SD-WAN channels, taking into account algorithms/strategies and SLA * Automatic load balancing, switching and reservation of communication channels for user applications and services when the characteristics of network connections (loss, jitter, latency) change in real time * Dynamic correction of packet loss or recovery of packets with errors caused by adverse conditions of WAN channels during operation via VPN - Forward Error Correction and Packet duplication * Balancing packets of one session through several IPSec VPN tunnels |
| Performance of security services | * Number of concurrent TCP sessions: no less than 100,000,000 * Number of new TCP sessions/second: not less than 8,000,000 * Packet throughput per second: no less than 100,000,000 * Bandwidth Enterprise Testing Conditions / Enterprise traffic mix / APPMIX (with FW+App Control+IPS+Malware Protection services included): not less than 7 Gbps * Throughput during inspection of SSL/TLS traffic using IPS: at least 14 Gbps |
| VPN performance | * IPSec VPN bandwidth: at least 55 Gbps * Number of simultaneous SSL VPN connections to the gateway: at least 5,000 * Number of simultaneous client-gateway IPSec VPN connections: not less than 2,000 * Number of simultaneous gateway-gateway IPSec VPN connections: no less than 2,000 |
| Virtualization | * Virtual FW, (Virtual Systems/Security contexts/Virtual Domains) which are independent devices with their own security policies, interfaces, administrators, etc.: not less than 10 |
| High availability | * Active-Active * Active-Standby |
| L2 functionality and network services | * Port aggregation (802.3ad) * VLAN (802.1Q and Trunking) * Built-in DHCP, NTP, DNS server |
| NAT | * Static NAT * Dynamic NAT * PAT |
| Multicast | * Sparse and dense mode * PIM support |
| Security services | * Stateful Firewall * Application identification and control (AC/AVC) * Protection against threats based on signature analysis (IPS) * Protection against malware (Antivirus/AMP) * Web and DNS filtering * Inspection/scanning of SSL/TLS traffic for threats * Protection against unknown threats (0-day) * Data Leakage Prevention (DLP) * Protection against DOS attacks * IPSec VPN, SSL VPN |
| Stateful Firewall | * Operating modes:   + NAT/router   + transparent mode (bridge)   + Support for VoIP traffic: deep inspection and protection against SIP protocol attacks   + Performing the role of a proxy for analysis, inspection and ensuring the correct operation of sessions of various protocols (session helpers, application layer gateway) |
| Application identification and control (AC/AVC) | * Inspection and application of actions to network traffic based on signature analysis and a certain category of applications (application control/application visibility control) * Configuration of AC/AVC sensors with the required set of signatures corresponding to the user's environment * Configuration of exceptions in actions with certain applications (exemption/override) * Creating custom application signatures |
| Protection against threats based on signature analysis (IPS) | * Inspection and application of actions to network traffic based on signature analysis and detection of known attacks (intrusion prevention system) * Configuration of IPS sensors with the required set of signatures corresponding to the user's environment * Configuration of exceptions in actions with certain signatures (exemption/override) * Creation of custom IPS-signatures |
| Protection against malware (Antivirus/AMP) | * Anti-Virus / Anti-malware protection * Detection and blocking of unwanted programs or files (grayware) * Detect and block files based on configured file size thresholds for different protocols * Protection against malware for mobile devices |
| Web and DNS filtering | * Inspection of URL requests and the possibility of blocking them based on the relationship to a certain category (Web filtering) * Inspection of DNS requests and the possibility of blocking them based on the relationship to a certain category (DNS filtering) * Detection and blocking of access to Botnet networks * Blocking certain dangerous elements of websites (Java Applet, ActiveX scripts, etc.) * Static blacklists and whitelists |
| SSL/TLS inspection | * Interception, decryption and inspection of HTTPS, FTPS sessions, etc * Configuration of exceptions from SSL/TLS inspection of certain IP addresses, URLs, etc. (exemption/override) * Inspection of the SSL/TLS certificate for compliance with a certain web resource to which the connection is made and the validity period (SSL/TLS certificate inspection) * Full content inspection of encrypted sessions (full SSL/TLS inspection) * Inspection of SSL/TLS traffic should include the following inspections: IPS, AC/AVC, AV/AMP, Web filtering, DLP |
| Protection against unknown threats (0-day) | * Integration with the protection system against complex zero-day attacks (in the form of a cloud service from the manufacturer - cloud sandbox) * Sending files from user traffic for analysis in the cloud sandbox to detect unknown "0-day" threats * Licensing in the delivery set should allow inspecting at least 20,000 files per day (24 hours) in the cloud sandbox |
| Data Loss Prevention | * Prevent leakage of sensitive data by inspecting traffic (by file name, file type, file size, regular expressions) * Preventing leakage of confidential data by checking traffic with predetermined information (credit card numbers, SIN numbers, etc.) * DLP functionality should prevent leakage through the following protocols: HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP, etc. |
| Protection against DOS attacks | * Ability to recognize and block DoS attacks:   + TCP Syn flood   + TCP/UDP/SCTP port scan   + ICMP sweep   + TCP/UDP/SCTP/ICMP session flooding |
| IPSec VPN, SSL VPN | * Encryption algorithms: 3DES, AES128, AES192, AES256 * Hashing algorithms: MD5, SHA256, SHA384, SHA512 * Diffie-Hellman Group: 1, 2, 5, 14 * Support for Hub & Spoke topology, mesh topology, DMVPN/ADVPN or similar |
| QoS | * Traffic Shaping * Traffic Policing |
| Authentication, authorization and accounting (AAA) | * Local user database * Support for LDAP, RADIUS, TACACS+ protocols * Support for two-factor authentication based on software tokens * At least 2 software tokens for installation on mobile devices (smartphones) * Single Sign-On: integration with Windows AD * PKI and certificates: X.509, SCEP support, creation of Certificate Signing Request (CSR), automatic renewal of certificates before expiration, OCSP support |
| Management, reporting, integration | * Graphical web interface (Web GUI) * Command Line Interface (CLI) * Support for a centralized management system * Support of a centralized system for collecting log files, analyzing them and creating reports * Administrator role access (RBAC) * REST API support * Keeping event logs (logging) * Functionality of recording packets from network interfaces for their further analysis (packet capture) * Functionality of backup and recovery of configuration files * SNMP v1, v2, v3 * sFlow v5 / Netflow v9 or similar, syslog |
| Technical service support | * The proposed solution must be provided with technical service support for a period of at least 1 year with a 24\*7 service level * Permanent access to the manufacturer's technical support center via the website, by e-mail or by phone 24\*7 * Permanent authorized access to the manufacturer's website 24\*7 * Obtaining up-to-date reputation bases, signatures and all necessary updates for security services * Receiving major and intermediate software releases * Ability to register service cases 24\*7   Delivery and replacement of spare parts in the Next Business Day mode in Kyiv (replacement equipment is delivered the next day after confirmation of the replacement by the manufacturer's support service) |

Table 10

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| General requirements | * The network security and SD-WAN routing device must be a device that performs intelligent traffic routing (SD-WAN), network traffic inspection and corporate infrastructure protection in accordance with the following requirements * If, according to the functionality of the device or according to the architectural approach, the implementation of technical requirements requires additional systems, devices or licenses, then all this should be included in the delivery set, taking into account the requirements for the term and functionality of technical support * All necessary licenses to provide the functionality and quantitative performance indicators specified in these requirements must be included in the proposed solution * The equipment should not have end-of-sale and end-of-life (EOS/EOL) announcements from the manufacturer * NGFW must have a valid expert opinion of the State Service for Special Communications and Information Protection of Ukraine on compliance with the requirements of the legislation in the field of information protection or pass the appropriate state examination at the time of submission of the tender offer by the Participant * All functional requirements and quantitative performance indicators must be supported in the manufacturer's documentation |
| Architecture and form factor | * Software and hardware complex (PAK) for installation in a standard 19" mounting cabinet |
| Interfaces and interface modules | * No less than 8 \* GE RJ45 * Not less than 8 \* GE SFP * Not less than 2 \* 10GE SFP+ * At least 1 \* GE RJ45 management port (OOB MGMT) * At least 1 \* RJ45 console port * At least 1 \* USB port * At least 2 \* 10GE SFP+ interface modules (optics, type SR) |
| Power supply | * 2 power supplies (100-240V AC, 50-60 Hz) that support "hot" replacement |
| Internal storage | * Internal storage (SSD) with a total volume of at least 480 GB for local storage of configuration files, software, etc. |
| Routing and SD-WAN | * Static routing and policy-based routing (PBR) * Dynamic routing protocols: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4 * Simultaneous use of physical and logical interfaces with various types of connections (MPLS, broadband Internet, LTE, etc.) for effective traffic routing * Evaluation of the quality of SD-WAN communication channels by sending packets or requests to certain nodes in the network or by passive methods * Monitoring the characteristics of communication channels in real time (packet loss, jitter, latency) and their graphic display (gui real-time monitor) * SLA control for user applications (applications) based on the characteristics of communication channels (packet loss, jitter, latency) in real time * Determination of various algorithms/strategies for the selection of communication channels for routing application and service traffic based on SLA compliance criteria, best values ​​of communication channel characteristics, etc. * Determination of application and service traffic routing rules through SD-WAN channels, taking into account algorithms/strategies and SLA * Automatic load balancing, switching and reservation of communication channels for user applications and services when the characteristics of network connections (loss, jitter, latency) change in real time * Dynamic correction of packet loss or recovery of packets with errors caused by adverse conditions of WAN channels during operation via VPN - Forward Error Correction and Packet duplication * Balancing packets of one session through several IPSec VPN tunnels |
| Productivity of security services | * Number of simultaneous TCP sessions: not less than 8,000,000 * Number of new TCP sessions/second: not less than 450,000 * Bandwidth on packets of 450 bytes or Enterprise Testing Conditions / Enterprise traffic mix / APPMIX (with FW+App Control+IPS+Malware Protection services included): not less than 7 Gbit/c * Throughput during inspection of SSL/TLS traffic using IPS: not less than 7 Gbps |
| VPN performance | * IPSec VPN bandwidth: at least 20 Gbps * Number of simultaneous SSL VPN connections to the gateway: no less than 2,000 * Number of simultaneous client-gateway IPSec VPN connections: not less than 2,000 * Number of simultaneous gateway-gateway IPSec VPN connections: no less than 2,000 |
| Virtualization | * Virtual FW, (Virtual Systems/Security contexts/Virtual Domains) which are independent devices with their own security policies, interfaces, administrators, etc.: not less than 10 |
| High availability | * Active-Active * Active-Standby |
| L2 functionality and network services | * Port aggregation (802.3ad) * VLAN (802.1Q and Trunking) * Built-in DHCP, NTP, DNS server |
| NAT | * Static NAT * Dynamic NAT * PAT |
| Multicast | * Sparse and dense mode * PIM support |
| Security services | * Stateful Firewall * Application identification and control (AC/AVC) * Protection against threats based on signature analysis (IPS) * Protection against malware (Antivirus/AMP) * Web and DNS filtering * Inspection/scanning of SSL/TLS traffic for threats * Protection against unknown threats (0-day) * Data Leakage Prevention (DLP) * Protection against DOS attacks * IPSec VPN, SSL VPN |
| Stateful Firewall | * Operating modes:   + NAT/router   + transparent mode (bridge)   + Support for VoIP traffic: deep inspection and protection against SIP protocol attacks   + Performing the role of a proxy for analysis, inspection and ensuring the correct operation of sessions of various protocols (session helpers, application layer gateway) |
| Application identification and control (AC/AVC) | * Inspection and application of actions to network traffic based on signature analysis and a certain category of applications (application control/application visibility control) * Configuration of AC/AVC sensors with the required set of signatures corresponding to the user's environment * Configuration of exceptions in actions with certain applications (exemption/override) * Creating custom application signatures |
| Security against threats based on signature analysis (IPS) | * Inspection and application of actions to network traffic based on signature analysis and detection of known attacks (intrusion prevention system) * Configuration of IPS sensors with the required set of signatures corresponding to the user's environment * Configuration of exceptions in actions with certain signatures (exemption/override) * Creation of custom IPS-signatures |
| Protection against malware (Antivirus/AMP) | * Anti-Virus / Anti-malware protection * Detection and blocking of unwanted programs or files (grayware) * Detect and block files based on configured file size thresholds for different protocols * Protection against malware for mobile devices |
| Web and DNS filtering | * Inspection of URL requests and the possibility of blocking them based on the relationship to a certain category (Web filtering) * Inspection of DNS requests and the possibility of blocking them based on the relationship to a certain category (DNS filtering) * Detection and blocking of access to Botnet networks * Blocking certain dangerous elements of websites (Java Applet, ActiveX scripts, etc.) * Static blacklists and whitelists |
| SSL/TLS inspection | * Interception, decryption and inspection of HTTPS, FTPS sessions, etc * Configuration of exceptions from SSL/TLS inspection of certain IP addresses, URLs, etc. (exemption/override) * Inspection of the SSL/TLS certificate for compliance with a certain web resource to which the connection is made and the validity period (SSL/TLS certificate inspection) * Full content inspection of encrypted sessions (full SSL/TLS inspection) * Inspection of SSL/TLS traffic should include the following inspections: IPS, AC/AVC, AV/AMP, Web filtering, DLP |
| Protection against unknown threats (0-day) | * Integration with the protection system against complex zero-day attacks (in the form of a cloud service from the manufacturer - cloud sandbox) * Sending files from user traffic for analysis in the cloud sandbox to detect unknown "0-day" threats * Licensing in the delivery set should allow inspecting at least 20,000 files per day (24 hours) in the cloud sandbox |
| Data Loss Prevention | * Prevent leakage of confidential data by inspecting traffic (by file name, file type, file size, regular expressions) * Preventing leakage of confidential data by checking traffic with predetermined information (credit card numbers, SIN numbers, etc.) * DLP functionality should prevent leakage through the following protocols: HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP, etc. |
| Protection against DOS attacks | * Ability to recognize and block DoS attacks:   + TCP Syn flood   + TCP/UDP/SCTP port scan   + ICMP sweep   + TCP/UDP/SCTP/ICMP session flooding |
| IPSec VPN, SSL VPN | * Encryption algorithms: 3DES, AES128, AES192, AES256 * Hashing algorithms: MD5, SHA256, SHA384, SHA512 * Diffie-Hellman Group: 1, 2, 5, 14 * Support for Hub & Spoke topology, mesh topology, DMVPN/ADVPN or similar |
| QoS | * Traffic Shaping * Traffic Policing |
| Authentication, Authorization and Accounting (AAA) | * Local user database * Support for LDAP, RADIUS, TACACS+ protocols * Support for two-factor authentication based on software tokens * At least 2 software tokens for installation on mobile devices (smartphones) * Single Sign-On: integration with Windows AD * PKI and certificates: X.509, SCEP support, creation of Certificate Signing Request (CSR), automatic renewal of certificates before expiration, OCSP support |
| Management, reporting, integration | * Graphical web interface (Web GUI) * Command Line Interface (CLI) * Support for a centralized management system * Support of a centralized system for collecting log files, analyzing them and creating reports * Administrator role access (RBAC) * REST API support * Keeping event logs (logging) * Functionality of recording packets from network interfaces for their further analysis (packet capture) * Functionality of backup and recovery of configuration files * SNMP v1, v2, v3 * sFlow v5 / Netflow v9 or similar, syslog |
| Technical service support | * The proposed solution must be provided with technical service support for a period of at least 1 year with a 24\*7 service level * Permanent access to the manufacturer's technical support center via the website, by e-mail or by phone 24\*7 * Permanent authorized access to the manufacturer's website 24\*7 * Obtaining up-to-date reputation bases, signatures and all necessary updates for security services * Receiving major and intermediate software releases * Ability to register service cases 24\*7 * Delivery and replacement of spare parts in the Next Business Day mode in Kyiv (replacement equipment is delivered the next day after confirmation of the replacement by the manufacturer's support service) |
| Compatibility | * Compatibility with FortiGate-601E devices |

Table 11

|  |  |
| --- | --- |
| **Name** | **Requirements** |
| Form factor | * External - for installation in a standard 19" mounting cabinet height no more than 1 RU |
| Power supply | * At least 1 power supply unit included |
| Network and other interfaces | * No less than 48 x 10/100/1000 RJ45 * No less than 4 x GE SFP+ * At least 1 x Console (RJ45) |
| Switching performance | * Bandwidth of the switching matrix (duplex): not less than 175 Gbps * Bandwidth of packets per second (duplex): not less than 260 Mpps |
| System characteristics | * Number of MACs: not less than 32,000 * Number of VLANs: not less than 4,000 * ACL: not less than 700 |
| Layer 2 OSI functions | * IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) * IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) * STP Root Guard, STP BPDU Guard, Edge Port/Port Fast * Jumbo Frames * IEEE 802.1Q VLAN Tagging * IEEE 802.3ad Link Aggregation with LACP * IEEE 802.3x Flow Control * Storm Control * IGMP Snooping |
| Security features | * DHCP-Snooping * Port Mirroring * sFlow/NetFlow * IEEE 802.1x authentication * ACL * Dynamic ARP Inspection * DHCP-Snooping * Determination of the operating systems of devices connected to the switch |
| Layer 3 OSI functions | * Static routing * Bidirectional Forwarding Detection (BFD) * Equal-cost multi-path (ECMP) * Support of dynamic routing protocols (in case of additional licensing) - RIPv2, OSPFv2, VRRP |
| High Availability | * Cross Stack Link Aggregation / Multi-Chassis Link Aggregation * Traffic balancing between interfaces |
| Management, diagnostics | * Web GUI, CLI * HTTPS, SSH, SNMP v2/v3 * Centralized management with the ability to automatically quarantine compromised hosts directly on the switch * Centralized cloud management * Support for HTTP REST APIs for configuration and monitoring |
| Guarantee | * The equipment must be guaranteed by the manufacturer for at least 12 months |
| Compatibility | * Compatibility with FortiSwitch-148F devices |

**3. ADDITIONAL REQUIREMENTS**

3.1. All the main components of the equipment must be original, replacement of components with non-original ones is prohibited.

3.2. Warranty for all equipment must be not less than 36 (thirty six) months for all equipment components. The equipment manufacturer must have authorized service centres on the territory of Ukraine, as well as ability to open service requests 24/7 via server manufacturer hotline and by e-mail;

3.3 Delivery of the equipment must be done within 2 months from the date of signing the Contract.

3.4 All necessary technical documentation must be given by the Contractor at the day of delivery.

**4. EXPERIENCE AND QUALIFICATION REQUIREMENTS**

* Officially registered company (for Ukrainian companies – company should be registered in the territory controlled by the government of Ukraine).
* At least 1 year of experience in supply of similar products
* At least 2 (two) positive recommendation letters from previous clients as per supplying of similar to this Specification equipment from past 2 years will be an asset.

**5. EVALUATION METHOD**

The Contract will be awarded to the technically compliant offer with the lowest prices.

Shorter equipment delivery time will be considered as an asset.

**6. PRICE OFFER AND PAYMENT SCHEDULE**

• The contract value must remain fixed for the duration of the contract.

• Applicants must include all costs associated with the work in their price quotation (such as the supply of all materials and equipment, transportation and unloading costs, staff salaries, office expenses, installation of equipment and software etc.).

• Payments should be arranged as follows:

Payment for goods/services shall be made through bank transfer to the Contractor’s account during 30 (thirty) days from the date of delivery and acceptance of equipment by UNDP;

Partial delivery is not allowed.

Taking into account that purchase of services will be carried out within the project of international technical assistance, price offers/invoices for payment must be presented without VAT. For mitigation of currency rate fluctuation, it is recommended to quote in USD.

Bidders can submit price offers for only one of the lots or for several lots.

Bidders must submit their price offers in the following format:

Lot 1 – Network cables:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Equipment name and specification requirements** | **Quantity of units (pcs)** | **Unit price, without VAT, USD** | **Total cost, without VAT, USD** |
| 1 | Network cable 0.5 m. length  *Indicate Brand, Model and parameters* | 15 |  |  |
| 2 | Network cable 1 m. length  *Indicate Brand, Model and parameters* | 20 |  |  |
| 3 | Network cable 2 m. length  *Indicate Brand, Model and parameters* | 20 |  |  |
| 4 | Network cable 3 m. length  *Indicate Brand, Model and parameters* | 20 |  |  |
| 5 | Network cable 4 m. length  *Indicate Brand, Model and parameters* | 20 |  |  |
| 6 | Network cable 5 m. length  *Indicate Brand, Model and parameters* | 20 |  |  |
|  | **Delivery** |  |  |  |
| **TOTAL without VAT, USD** | | | |  |
| **Equipment delivery time (working days from contract signature date)** | | | |  |

Lot 2 – USB cables and adaptors:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Equipment name and specification requirements** | **Quantity of units (pcs)** | **Unit price, without VAT, USD** | **Total cost, without VAT, USD** |
| 1 | USB/COM adapter  *Indicate Brand, Model and parameters* | 4 |  |  |
| 2 | USB 3.0 extender 1.5 m length  *Indicate Brand, Model and parameters* | 4 |  |  |
| 3 | USB 3.0 extender 2 m length  *Indicate Brand, Model and parameters* | 4 |  |  |
| 4 | Power extender with USB ports  *Indicate Brand, Model and parameters* | 2 |  |  |
| 5 | USB hub  *Indicate Brand, Model and parameters* | 3 |  |  |
| 6 | Network adapter USB/RJ-45  *Indicate Brand, Model and parameters* | 2 |  |  |
|  | **Delivery** |  |  |  |
| **TOTAL without VAT, USD** | | | |  |
| **Equipment delivery time (working days from contract signature date)** | | | |  |

Lot 3 – External hard drive:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Equipment name and specification requirements** | **Quantity of units (pcs)** | **Unit price, without VAT, USD** | **Total cost, without VAT, USD** |
| 1 | External hard drive *Indicate Brand, Model and parameters* | 2 |  |  |
|  | **Delivery** |  |  |  |
| **TOTAL without VAT, USD** | | | |  |
| **Equipment delivery time (working days from contract signature date)** | | | |  |

Lot 4 – Router:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Equipment name and specification requirements** | **Quantity of units (pcs)** | **Unit price, without VAT, USD** | **Total cost, without VAT, USD** |
| 1 | Router  *Indicate Brand, Model and parameters* | 2 |  |  |
|  | **Delivery** |  |  |  |
| **TOTAL without VAT, USD** | | | |  |
| **Equipment delivery time (working days from contract signature date)** | | | |  |

Lot 5 – Networking equipment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Equipment name and specification requirements** | **Quantity of units (pcs)** | **Unit price, without VAT, USD** | **Total cost, without VAT, USD** |
| 1 | Router/Firewall  *Indicate Brand, Model and parameters* | 2 |  |  |
| 2 | Network screen  *Indicate Brand, Model and parameters* | 2 |  |  |
| 3 | Switch  *Indicate Brand, Model and parameters* | 4 |  |  |
|  | **Delivery** |  |  |  |
| **TOTAL without VAT, USD** | | | |  |
| **Equipment delivery time (working days from contract signature date)** | | | |  |