1. Scop

Scopul prezentei achiziții constă în furnizarea, instalarea, configurarea și integrarea unei soluții de tip NGFW (Next Generation Firewall), destinată protecției infrastructurii informatice critice a Î.S. „Aeroportul Internațional Chișinău", precum și asigurării continuității operaționale, segmentării securizate a rețelei și controlului avansat al traficului.

Nr.	Denumirea echipamentului / serviciului	Cantitatea (buc.)
1.	Echipament de tip NGFW	2
2.	Servicii de instalare, configurare, migrare și integrare	1

2. Caracteristici tehnice

N/o	Denumi-rea bunurilor	Unita-tea de măsură	Cantitatea	Specificarea tehnică deplină solicitată de către autoritatea contractantă
1.	**Firewall (paravan de protecție)**			
1.1	Echipament de tip NGFW	bucată	2	**Caracteristici fizice și de instalare:** a) Echipamentul trebuie să fie prevăzut cu șasiu pentru montare în rack standard 19", livrat împreună cu toate accesoriile necesare pentru instalare în dulap de telecomunicații; b) Echipamentul trebuie să fie dotat cu minimum două surse de alimentare AC 220V redundante; c) Echipamentul trebuie să asigure fluxul de aer orientat din față spre spate (front-to-back); d) Echipamentul trebuie să fie livrat cu următoarele module optice și cabluri: 4 × SFP+ 10G AOC 5 m și 4 × SFP28 25G AOC 5 m. **Interfețe integrate:** a) Minimum 8 porturi Ethernet 1G; b) Minimum 4 porturi SFP+ 10G; c) Minimum 4 porturi SFP28 10/25G; d) Minimum 1 port de consolă RJ45; e) Minimum 1 port de management RJ45; f) Minimum 1 port dedicat pentru High Availability (HA). **Performanță:** a) Soluția propusă trebuie să asigure o capacitate de filtrare a traficului de minimum 140 Gbps; b) Soluția propusă trebuie să asigure o capacitate de tunelare IPSec (VPN) de minimum 50 Gbps; c) Soluția propusă trebuie să suporte cel puțin 2000 de conexiuni VPN simultane de tip Site-to-Site IPSec; d) Soluția propusă trebuie să suporte cel puțin 2000 de conexiuni VPN simultane de tip Remote Access SSL-VPN; e) Soluția propusă trebuie să asigure o capacitate de inspectare a traficului SSL de minimum 13 Gbps; f) Soluția propusă trebuie să asigure o capacitate de inspectare a traficului cu funcționalitatea IPS activată de minimum 36 Gbps; g) Soluția propusă trebuie să suporte până la 15 milioane de sesiuni TCP simultane; h) Soluția propusă trebuie să suporte cel puțin 700.000 de sesiuni noi pe secundă.

N/o	Denumi-rea bunurilor	Unita-tea de măsură	Cantitatea	Specificarea tehnică deplină solicitată de către autoritatea contractantă
				Funcționalități: a) Detectarea și filtrarea traficului pe baza conținutului acestuia; b) Detectarea și atenuarea atacurilor de tip DDoS, pe baza politicilor definite; c) Definirea și aplicarea regulilor de QoS și traffic shaping pentru gestionarea traficului de rețea; d) Definirea și aplicarea politicilor de filtrare web (Web Inspection / Web Filtering); e) Aplicarea politicilor de securitate pentru antispam, antivirus și filtrare web; f) Definirea regulilor de firewall pe baza criteriilor GeoIP; g) Identificarea și controlul aplicațiilor prin mecanisme de Application Control; h) Blocarea traficului către și dinspre adrese BotNet, pe baza listelor actualizate periodic. **Segmentare:** Soluția trebuie să permită segmentarea logică a sistemului prin alocarea resurselor dedicate, astfel încât fiecare unitate logică să dispună cel puțin de următoarele funcționalități: a) administrarea tabelei de rutare; b) NAT; c) firewall; d) instanțe VPN; e) politici de securitate (Application Control, Web Filtering etc.); f) interfețe fizice și logice dedicate. **Disponibilitate înaltă (High Availability):** Soluția trebuie să îndeplinească cerințele minime pentru asigurarea disponibilității înalte: a) funcționare în mod Active-Active și Active-Passive; b) stateful failover pentru firewall și VPN; c) detectarea și notificarea defectării echipamentelor; d) monitorizarea conexiunilor de rețea; e) mecanisme de link failover. **Monitorizare și management** a) Soluția trebuie să includă funcționalități de monitorizare a componentelor hardware: b) monitorizare grafică în timp real și istorică a parametrilor sistemului; c) suport pentru transmiterea logurilor prin Syslog; d) suport pentru SNMP v1/v2c/v3; e) notificări prin e-mail în cazul apariției alertelor; f) suport pentru exportul statisticilor de trafic prin sFlow și NetFlow. **Endpoint Control** Soluția trebuie să permită integrarea cu un software de securitate instalat pe stațiile utilizatorilor, oferind: a) blocarea traficului generat de aplicațiile instalate pe stații;

N/o	Denumi-rea bunurilor	Unita-tea de măsură	Cantitatea	Specificarea tehnică deplină solicitată de către autoritatea contractantă
				b) restricționarea și filtrarea accesului web; c) scanarea stațiilor pentru identificarea vulnerabilităților; d) scanare antivirus; e) configurarea automată a tunelurilor VPN. **Prevenirea scurgerilor de date (DLP)** Soluția trebuie să includă funcționalități Data Leak Prevention, care să permită: a) blocarea și arhivarea comunicațiilor în cazul detectării tentativelor de scurgere de informații prin protocoalele e-mail, HTTP, FTP, inclusiv variantele criptate SSL; b) blocarea transferului de fișiere în funcție de tipul și dimensiunea acestora. **Autentificare și controlul accesului** Soluția trebuie să ofere mecanisme avansate de autentificare a utilizatorilor, inclusiv: a) definirea locală a utilizatorilor; b) integrarea cu Windows Active Directory (SSO); c) integrarea cu RADIUS, LDAP și TACACS+; d) autentificare în doi factori (2FA) utilizând coduri OTP transmise prin e-mail sau SMS; e) autentificare bazată pe certificate digitale PKI X.509; f) restricționarea accesului în rețea pentru utilizatorii care nu au instalat clientul software de securitate pe stație. **Garanție și suport pentru hardware și software - minimum 36 de luni, asigurate de producător, cu disponibilitate 24/7.**
1.2	Servicii de instalare, configurare, migrare și integrare	serv	1	**Ofertantul trebuie să asigure executarea următoarelor lucrări:** a) Elaborarea și convenirea cu Beneficiarul a documentației de proiectare, inclusiv High-Level Design (HLD) și Low-Level Design (LLD); b) Elaborarea politicilor de securitate a rețelei (niveluri de acces la rețea, liste de control al accesului – ACL, securitatea porturilor, VPN, precum și mecanisme de notificare și escaladare a incidentelor de securitate); c) Coordonarea planului de implementare și a tuturor etapelor de migrare către noua infrastructură; d) Instalarea și configurarea echipamentelor de tip paravan de protecție (firewall). **Ofertantul trebuie să asigure:** e) Livrarea, instalarea și configurarea echipamentelor propuse, precum și integrarea acestora în infrastructura de rețea existentă; f) Configurarea echipamentelor de tip paravan de protecție în regim de funcționare cluster/stack pentru asigurarea redundanței; g) Migrarea configurațiilor de pe echipamentele existente FortiGate 201E, inclusiv: routing, L2TP/IPsec, DMZ, Data Center, OSPF, reguli

N/o	Denumi-rea bunurilor	Unita-tea de măsură	Cantitatea	Specificarea tehnică deplină solicitată de către autoritatea contractantă
				firewall, VLAN, VDOM, conexiuni site-to-site IPsec, precum şi politici NGFW/IPS/Antivirus; h) Configurarea politicilor şi regulilor de securitate; i) Segmentarea reţelei pe zone de securitate; j) Configurarea accesului VPN de tip Remote Access pentru minimum 500 utilizatori. **Toate lucrările trebuie realizate fără perturbarea funcționării infrastructurilor existente.**

3. Cerințe față de ofertant

a) Ofertantul trebuie să demonstreze disponibilitatea personalului calificat necesar pentru îndeplinirea corespunzătoare a obiectului contractului. Echipa de proiect trebuie să includă cel puțin un inginer certificat la nivel Associate, Professional sau Expert Certified Engineer de catre producatorul echipamentului oferit. Specialiștii trebuie să fie angajați ai operatorului economic participant. Certificatul trebuie să fie valabil la momentul depunerii ofertei și pe întreaga perioadă de implementare a proiectului.

b) Ofertantul trebuie să demonstreze experiență relevantă, prin prezentarea a cel puțin trei contracte executate în ultimii 3 ani, similare ca obiect cu cel al prezentei achiziții, fiecare având o valoare cel puțin egală sau mai mare decât valoarea ofertei prezentate în cadrul procedurii de achiziție.

c) Ofertantul trebuie să dețină statut de partener oficial al producătorului pentru echipamentele propuse, pe teritoriul Republicii Moldova, fapt confirmat prin documente oficiale care atestă dreptul de comercializare, livrare și suport pentru bunurile solicitate.