ANUNȚ DE PARTICIPARE

privind achiziționarea: Paravan de protecție în rețea (Firewall)
(se indică obiectul achiziției)

prin procedura de achiziție: Cererea ofertelor de prețuri
(tipul procedurii de achiziție)

1. **Denumirea autorității contractante:** Biroul Național de Statistică
2. **IDNO:** 1006601000200
3. **Adresa:** Mun. Chișinău, str. Grenoble 106
4. **Numărul de telefon/fax:** 022 403 125, 022 403 127
5. **Adresa de e-mail și de Internet a autorității contractante:** moldstat@statistica.gov.md, www.statistica.gov.md
6. **Adresa de e-mail sau de Internet de la care se va putea obține accesul la documentația de atribuire:** Documentația de atribuire este anexată în cadrul procedurii în SIA RSAP
7. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** Nu se aplică
8. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea următoarelor bunuri:**

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	Cantitatea	Specificarea tehnică deplină solicitată, standarde de referință	Valoarea estimată (fără TVA)
	LOTUL I. Paravan de protecție în rețea (Firewall)				
1.	3240000-3	Paravan de protecție în rețea (Firewall)	1 unitate	Conform Anexei 1	269 800,00
	Valoarea estimativă totală a achiziției, fără TVA				**269 800,00**

9. **În cazul în care contractul este împărțit pe loturi, un operator economic poate depune oferta (se va selecta):** Pentru mai multe loturi
10. **Admiterea sau interzicerea ofertelor alternative:** Nu se admite
(indicați se admite sau nu se admite)
11. **Termenii și condițiile de livrare solicitați:** Timp de 30 (treizeci) zile calendaristice din data semnării și înregistrării contractului, cu livrarea la adresa Beneficiarului: mun. Chișinău, str. Grenoble, 106.
12. **Termenul de valabilitate a contractului:** 31.12.2021

13.Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): Nu se aplică

14.Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz): Nu se aplică

(se menționează respectivele acte cu putere de lege și acte administrative)

15.Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1.	DUAE	Semnat electronic de către operatorul economic	Obligatoriu
2.	Oferta	Formularul F 3.1, semnat electronic de către operatorul economic	Obligatoriu
3.	Extras de la Camera Înregistrării de Stat	Semnat electronic de către operatorul economic	Obligatoriu
4.	Certificat de atribuire a contului bancar	Copie, semnată electronic de către operatorul economic	Obligatoriu
5.	Certificat privind lipsa sau existența restanțelor față de bugetul public național	Copie, semnată electronic de către operatorul economic	Obligatoriu
6.	Raport financiar pentru anul 2020	Copie, semnată electronic de către operatorul economic până la termenul limită de depunere a ofertei	Obligatoriu
7.	Formularul informativ despre ofertant	Formularul F 3.3, semnat electronic de către operatorul economic	Obligatoriu
8.	Specificații tehnice	Original, semnat electronic de către operatorul economic, în conformitate cu formularul F 4.1	Obligatoriu
9.	Specificații de preț	Original, semnat electronic de către operatorul economic, în conformitate cu formularul F 4.2	Obligatoriu

10.	Garanția pentru ofertă – 1%	Original, scrisoare de garanție bancară formularul F.3.2, semnat electronic de către operatorul economic	Obligatoriu
11.	Garanția de bună execuție, în mărime de 3% din valoarea contractului	La încheierea contractului, original, semnat electronic de către operatorul economic	Obligatoriu
12.	Declarația privind conduita etică și neimplicarea în practici frauduloase și de corupere	Original, semnat electronic de către operatorul economic, în conformitate cu formularul F 3.4	Obligatoriu
13.	Minim ani de experiență specifică în livrarea bunurilor	3 ani	Obligatoriu
14.	Declarație privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activități ale unei organizații sau grupări criminale, pentru corupție, fraudă și/sau spălare de bani	Declarație, semnată electronic de către operatorul economic	Obligatoriu

16.Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrînse și a procedurii negociate), după caz: Nu se aplică

17.Tehnici și instrumente specifice de atribuire (dacă este cazul, specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică): Nu se aplică

18.Condiții speciale de care depinde îndeplinirea contractului (indicați după caz): Nu se aplică

19.Criteriul de evaluare aplicat pentru adjudecarea contractului: Cel mai mic preț

20.Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor:

21.Termenul limită de depunere/deschidere a ofertelor:

- **până la:** [0:00] Informația o găsiți pe SIA RSAP
- **pe:** Informația o găsiți pe SIA RSAP
- Ofertele prezentate cu întîrziere vor fi respinse

22.Adresa la care trebuie transmise ofertele sau cererile de participare: Ofertele sau cererile de participare vor fi depuse electronic, prin intermediul SIA RSAP

23.Termenul de valabilitate a ofertelor: 60 zile calendaristice

24.Locul deschiderii ofertelor: SIA RSAP
(SIA RSAP sau adresa deschiderii)

25. **Persoanele autorizate să asiste la deschiderea ofertelor:** Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului cînd ofertele au fost depuse prin SIA RSAP

26. **Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:** Limba română

27. **Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene:** Nu
(se specifică denumirea proiectului și/sau programului)

28. **Denumirea și adresa organismului competent de soluționare a contestațiilor:**

- Agenția Națională pentru Soluționarea Contestațiilor
- Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt, nr.124 (et.4), MD 2001, tel/fax/email: 022 820 652, 022 820 651, contestatii@ansc.md

29. **Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respectiv (dacă este cazul):** Nu se aplică

30. **În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare:** Nu se aplică

31. **Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț:** Nu a fost publicat un anunț de intenție

32. **Data transmiterii spre publicare a anunțului de participare:** Conform SIA RSAP

33. **În cadrul procedurii de achiziție publică se va utiliza/accepta:**

Denumirea instrumentului electronic	Se va utiliza/accepta sau nu
Depunerea electronică a ofertelor sau a cererilor de participare	Se acceptă
Sistemul de comenzi electronice	Nu se acceptă
Facturarea electronică	Se acceptă
Plățile electronice	Se acceptă

34. **Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene):** Nu se aplică
(se specifică da sau nu)

Conducătorul Grupului de lucru:

Oleg CARA
Director general

Anexa 1

CERINȚE

Soluția integrată "Paravan de protective" trebuie sa fie de tip HW, un echipament și soft integrat de protecție a rețelei Biroului Național de Statistică, ce va funcționa ca o soluție de securitate unificată, constituită din 2 unități centrale.

1. Paravan de protecție pentru oficiul central

Cantitate	**(2) Două unități** pentru asigurarea disponibilității înalte (prin tehnologia high-availability cluster)
Specificații minime hardware	• Interfețe GbE RJ-45: minimum 16 • Interfețe GbE SFP: minimum 8 • Interfețe GbE SFP +: minimum 2 • Porturi pentru consola RJ-45: minimum 1 • Porturi USB: minimum 1 • Posibilitate de instalare în dulap de echipamente (IT rack) • Dimensiune: maximum 1U (one rack unit)

Caracteristici de performanță	• Trafic firewall (minimum):
	  • Pachete UDP de 1518 byte – 27 Gbps
	  • Pachete UDP de 512 byte – 27 Gbps
	  • Pachete UDP de 64 byte – 11 Gbps
	• Latență Firewall: maximum 4,78 µs
	• Trafic Firewall măsurat în pachete per secundă: minimum 16,5 million pps
	• Trafic IPSec VPN: minimum 13 Gbps
	• Trafic NGFW: minimum 3,5 Gbps
	• Trafic IPS: minimum 5 Gbps
	• Trafic Protecția importiva amenințărilor: minimum 3 Gbps
	• Performanța SSL Inspection: minimum 4 Gbps
	• Număr de tunele IPSec VPN site-to-site: minimum 2.000
	• Număr de clienți IPSec VPN: minimum 16.000
	• Trafic SSL-VPN: minimum 2 Gbps
	• Număr de clienți concomitenți SSL-VPN: minimum 500
	• Număr de sesiuni concurente TCP: minimum 3.000.000
	• Număr de sesiuni noi pe secundă TCP: minimum 280.000
	• Număr de politici de securitate: minimum 10.000
	• Număr de instanțe virtuale: minimum10
	• Număr de AP-uri administrate în modul tunel: 128
	• Trafic CAPWAP (HTTP): minimum 20 Gbps
	• Număr de token-uri OTP administrate: minimum 5.000

Funcționalități generale	Echipament integrat de securitate cu funcționalități simultane de: • Router cu suport pentru protocoale de rutare dinamice • Posibilitate de instalare în mod bridge Ethernet • Protecție tip Antivirus • Criptare de date: IPSec VPN si SSL VPN • Suport pentru QoS și Traffic Shaping • Detecția și prevenirea intruziunilor – IDS/IPS • Scanare și filtrare WEB – Web Inspection/Filter • Blocarea și controlul traficului din rețea generat de aplicații

- Protecție Antispam
- Update-uri automate şi în timp real
- Suport pentru IPv6 UTM
- Funcționalitate de proxy SSL – posibilitatea inspecției traficului criptat
- Wireless controller
- SD-WAN
- Conectori SDN
- Suport extins pentru antivirus (Virus outbreak services)
- Toate funcționalitățile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum și platforma hardware aparțin aceluiaşi producător
- Certificări pentru producator şi produs: ICSA Labs pentru Firewall, IPSec, SSL VPN, IPS, Antivirus sau echivalent
- Conformitate cu: CE, CB

Funcționalități securitate

Funcționalități firewall

- Funcționalități NAT, PAT şi Transparent Bridge
- Opțiune de a aplica NAT per politică
- Suport VLAN Tagging 802.1Q
- Autentificarea utilizatorilor pe grupuri
- Suport VoIP SIP/H.323/SCCP Traversal NAT
- Funcționalitate proxy explicit HTTP/HTTPS şi FTP
- Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru funcționalitatea proxy explicit
- Suport WINS
- Suport securitate VoIP ALG (SIP Firewall/RTP Pinholing)
- Suport pentru TCP MSS clamping
- Suport pentru rescrierea câmpului Class of Service
- Suport IPv6 (NAT/mod Transparent)
- Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de stație folosit – funcționalitate de tip BYOD (bring your own device)
- Opțiune "Scheduling" pentru politicile de firewall
- Posibilitate de blocare a traficului după țara de origine a sursei sau destinației (Geo IP)

Funcționalități VPN

- Suport PPTP, L2TP, IPSec, L2TP over IPSec, SSL-VPN
- Criptare DES, 3DES, AES 128, AES 192, AES 256
- Autentificare MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Suport pentru PPTP si L2TP VPN Client Pass Through
- Funcționalitate "Hub and Spoke" IPSec VPN
- Autentificare IKE prin certificate X.509 - suport pentru RSA şi ECDSA
- Suport IPSec Xauth NAT Traversal
- Suport configurare IPSec automată
- Funcționalitate IKE Dead Peer Detection
- Suport pentru RSA SecureID
- Suport Single-Sign-On pentru pentru book-mark-uri portal SSL-VPN
- Funcționalitate Two-Factor Authentication pentru SSL-VPN
- Suport pentru autentificare de grupuri de utilizatori prin LDAP

	(SSL-VPN) • Suport tunele SSL în mod tunel şi în mod portal • Suport pentru validarea clienţilor SSL VPN prin verificarea aplicaţiilor instalate pe staţie înainte de conectare - comaptibilitate cu sistemele de operare Windows • Suport pentru autentificarea utilizatorilor de tip Single Sign On prin portalul SSL VPN • Funcţionalităţi monitorizare tunele VPN • Producătorul are în portofoliu client de VPN IPSec şi SSL propriu, care are şi funcţionalităţi de: antivirus, filtrare web şi optimizare de bandă, filtrare a traficului de aplicaţii, scanare de vulnerabilităţi
Funcţionalităţi Antivirus	• Protecţie anti-malware (virus, troian, worm, spyware, grayware) • Protocoale suportate: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP • Suport scanare antivirus Proxy-Based şi Flow-Based • Suport pentru detecţia malware prin sandboxing de tip Cloud-Based al fişierelor suspecte • Suport pentru carantină a fişierelor infectate • Protecţie împotriva reţelelor botnet şi site-urilor de tip phishing pe bază de reputaţie a adreselor IP si a URL-urilor accesate de utilizatori
Funcţionalităţi filtrare trafic WEB	• Filtrare pentru protocoalele HTTP şi HTTPS • Blocare a conexiunilor în funcţie de URL/cuvânt cheie sau expresie în conţinutul paginilor web • Blocare a conexiunilor în funcţie de URL-ul din header-ul Referer al cererii HTTP • Filtrare pentru Java Applet, Cookies, scripturi Active X • Posibilitate de activare forţată a opţiunii „Safe Search" pentru motoare de căutare web • Posibilitatea de modificare a header-elor HTTP din cererile generate de utilizatori • Funcţionalitate de monitorizare a activităţii web a utilizatorilor • Posibilitate de înştiinţare a utilizatorilor, prin afisarea informaţiilor în cadrul unui browser web, privind paginile web blocate
Funcţionalităţi sistem de control al aplicaţiilor	• Identificarea şi controlul a cel puţin 4000 de aplicaţii bine cunoscute • Opţiune de Traffic-Shaping per aplicaţie • Clasificare granulară a aplicaţiilor după criterii multiple precum: Categorii de aplicaţii, Popularitate, Tehnologie şi Risc • Monitorizarea aplicaţiilor cu rata cea mai mare de consum de bandă • Monitorizarea aplicaţiilor pe baza IP/Utilizator • Suport pentru decriptarea şi inspectarea sesiunilor SSH • Suport pentru blocarea aplicaţiilor utilizate în cadrul reţelelor de tip Botnet • Posibilitate de definire a semnăturilor de aplicaţie personalizate • Posibilitate de înştiinţare a utilizatorilor, prin afişarea

	informațiilor în cadrul unui browser web, privind traficul de aplicații blocat
Funcționalități sistem de prevenire a intruziunilor/atacurilor (IPS)	• Protecție pentru cel puțin 10.000 de semnături de atac • Suport pentru inspecția traficului de aplicație criptat prin protocolul SSL • Protecție pentru atacuri de tip brute force • Detectarea anomaliilor de protocol • Suport pentru semnături configurabile • Update-uri automate pentru semnături • Suport pentru IPv4 si IPv6 DDoS
Funcționalități Antispam	• Scanare pentru SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI • Suport RBL/ORDBL • Filtrare după cuvinte cheie/expresie • Filtrare dupa Black/White List pentru adrese IP și e-mail
Funcționalități rețea	
Funcționalități rețelistică și rutare	• Suport pentru legături WAN multiple cu balansare a traficului după metodele: weighted round robin a sesiunilor, impartire proporțională a volumului de trafic, prin limitarea per interfață a benzii maxime utilizabile, după calitatea conexiunii ISP (jitter sau latență) • Suport PPPoE și DHCP Client/Server • Rute statice • Rutare dinamică IPv4: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS • Rutare dinamică IPv6: RIPng, OSPF v3, BGP 4+ • Gruparea interfețelor în zone de securitate • Policy-based routing • Suport VRRP și Link Failure Control • Suport VLAN Tagging (802.1q) • Suport pentru IPv6 (Firewall, DNS, SIP) • Suport One-to-One NAT • Suport pentru mecanismul GTSM(IETF RFC 3682) • Suport NAT64, DNS64, NAT46, NAT66 • Suport LLDP • EMAC VLAN
Funcționalitate Wireless Controller	Modul wireless controller pentru thin-AP-uri integrat cu următoarele funcționalități: • Detecție și suprimare a AP-urilor neînregistrate în controller; • Selecție automată a canalului pentru AP în funcție de interferențele din mediu; • Suport pentru SSID-uri multiple; • Autentificare WEP, WPA, WPA2, WPA2 Enterprise, 802.1x • Suport Captive Portal; • Suport pentru Wireless Mesh și roaming; • Distribuire automată a clienților wireless per AP sau bandă de frecvențe pentru a obține performanțe optime. • Rutare dinamică a traficului generat de utilizatorii wireless prin

	VLAN-uri folosind autentificare prin RADIUS • Autentificare suplimentară a clienților wireless prin RADIUS pe baza adresei MAC • Suport pentru RADIUS Accounting • Posibilitatea gestionării AP-urilor remote de către controller dar cu rutarea traficului printr-un gateway local • Wireless IDS
Funcționalități Traffic Shaping	• Limitare/garantare/prioritizare a benzii de trafic prin politici • Traffic Shaping per aplicație și adresa IP • Suport pentru DSCP • Limitare a cotei de trafic (per adresă IP) • Suport pentru ToS
Suport instanțe virtuale	• Firewall/rutare per instanță virtuală • VRF • Administrare separată per instanță virtuală • Interfețe VLAN separate per instanță virtuală • Politici de securitate per instanță virtuală
Suport pentru centre de date – data center	• Balansare de trafic pentru servere pe protocoalele HTTP, HTTPS, SMTPS, IMAPS, POP3S, SSL, TCP, UDP, IP • Balansare de trafic prin metode de tip: round-robin, weighted, first alive, least RTT, least session, HTTP host (din header-ul HTTP) • Persistența sesiunilor prin metode de tip: HTTP cookie, SSL session ID • Health monitoring pentru servere fizice • Multiplexare TCP pentru sesiunile balansate • Offloading pentru SSL (preia operațiunile de criptare/decriptare de la server-ul intern pentru HTTPS și execută aceste operații direct pe echipament) • Suport WCCP • Suport ICAP
Funcționalități High Availability - HA	• Funcționare Active-Active, Active-Passive • Funcționalitate Stateful Failover (Firewall și VPN) • Detectare și notificare pentru echipament nefuncțional • Monitorizarea conexiunii la rețea • Funcționalitate Link Failover

Funcționalități de administrare, logare, autentificare a utilizatorilor

Funcționalități de administrare	• Administrare prin WEB UI, Secure Command Shell (SSH) și Command Line Interface (CLI), conexiune USB • Posibilitatea de administrare dintr-un portal cloud-based oferit de producător • Utilizatori/Administratori cu drepturi configurabile • Funcționalitate de export/import a configurației • Politică de control a parolelor
Funcționalități de	• Monitorizare grafică în timp real și istorică

logare și monitorizare	• Opțiune de păstrare a log-urilor pe memoria internă • Suport syslog • Suport SNMP v1/v2c/v3 • Notificare prin e-mail pentru alerte • Suport sFlow și Netflow
Funcționalități de autentificare a utilizatorilor	• Definire locală a utilizatorilor • Integrare cu Windows Active Directory (AD) pentru Single Sign On • Integrare cu Citrix pentru autentificare SSO a utilizatorilor • Integrare cu RADIUS/LDAP/TACACS+/POP3 • Suport Xauth pentru IPSec VPN • Suport pentru autentificarea grupurilor de utilizatori prin LDAP • Suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software, ce pot fi trimise utilizatorilor prin Email sau SMS • Suport pentru autentificare prin certificate digitale PKI X.509 • Posibilitatea limitării accesului utilizatorilor în rețea ce nu au instalat un client software de stație (client endpoint)
Condiții de alimentare	• Alimentare curent alternativ 100-240V, 50-60 Hz • Putere consumată: maxim 120 W
Condiții de mediu	• Temperatură de operare: 0 – 40 grade Celsius • Umiditate: 20 – 90 %, fara condens
Garanție și suport	**Soluția va beneficia de minimum 1 an de suport, ce va include:** • Suport tehnic din partea producătorului 7 zile pe saptamana, 24 de ore pe zi • Înlocuirea echipamentului în caz de defecțiune hardware fără costuri suplimentare pentru beneficiar • Update firmware versiuni minore și majore • Update-uri automate de semnături pentru: controlul aplicației, IPS și anti-virus • Acces la următoarele servicii: sandbox în cloud, web filter și anti-spam