CAIET DE SARCINI

Privind achiziționarea echipamentului specializat pentru asigurarea securității resurselor informaționale ale CCI

1. Informație generală

Denumirea organizației: Camera de Comerț și Industrie a Republicii Moldova (CCI a RM);

Adresa: bd. Ștefan cel Mare și Sfânt 151, MD-2004, Chișinău, Republica Moldova;

Numărul de telefon: +373 69448826;

Adresa de e-mail a organizației: camera@chamber.md;

Pagina web a organizației: www.chamber.md.

Informație despre achiziția echipamentului specializat: Achiziția este efectuată în cadrul Acordului de Grant nr. 81302064 din 27.11.2023 în cadrul proiectului „***Transformarea digitală a întreprinderilor mici și mijlocii din țările Parteneriatului Estic***” finanțat de Ministerul German pentru Cooperare Economică și Dezvoltare (BMZ), proiectul este implementat de Agenția de Cooperare Internațională a Germaniei (GIZ).

2. Dosarul de aplicare va conține:

1. **Oferta financiară** va include următoarele acte:

- prețul unitar în MDL și prețul total cu TVA inclus,
- certificat de atribuire a contului bancar;

- garanția de bună execuție prezentată prin scrisoare de confirmare din partea companiei;
- termenul de valabilitate a ofertelor - 90 de zile.

2. Oferta tehnică se va prezenta astfel încât să se asigure posibilitatea verificării corespondentei ofertei tehnice cu specificațiile tehnice prevăzute în Caietul de sarcini, care sunt sunt minimali și obligatorii.

Ofertanții vor prezenta următorul set de documente:
- datele de contact ale ofertantului (numele, prenumele conducătorului, adresa, telefon de contact, e-mail);
- profilul companiei, cu descrierea și calificarea în domeniu, demonstrarea experienței operatorului economic pentru ultimii 3 ani privind livrarea bunurilor în domeniul de activitate aferent obiectului contractului ce urmează a fi atribuit, referințe de vânzare NGFW – minim 3 contracte, extras din Registrul de Stat al persoanelor juridice;
- descrierea bunurilor propuse (poate fi indicat și un link cu imaginea produsului oferit și alte detalii);
- fotografii/desene tehnice/imagini;
- act ce atestă dreptul de a livra bunurile;
- certificatele de origine a bunurilor oferite;
- certificate de calificare/instruiri în domeniul instalării produsului ofertat a minim 2 specialiști (fără asociere cu o alta companie);
- autorizarea de la producător pentru licitația la care participă.

Oferta financiară și oferta tehnică vor fi semnate electronic sau olograf de către persoana autorizată.

Descrierea specificațiilor tehnice:

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
1	**Echipament firewall de generație**	1	Bucată	**Specificațiile tehnice pentru echipamentul firewall de generație următoare (NGFW)**

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
	următoare (NGFW)			Se dorește achiziționarea unei soluții de firewall cu inspecție la Layer 7 ce va conține minim modulele de securitate așa ca: Prevenirea Amenințărilor Avansate (ATP), Filtrarea URL-urilor, Sandbox, DNS Security, SD-WAN, agent de Vpn pentru utilizatori, inclusiv dispozitive mobile Android si iOS. Firewall-ul trebuie sa acopere specificatiile tehnice minime mentionate mai jos: **<u>Cerințe și caracteristici generale:</u>** - NGFW-ul trebuie să ofere vizibilitate și capacitatea de a identifica și restricționa aplicațiile, indiferent de port, protocol, tehnici evazive sau criptare (TLS/SSL) sau folosind porturi non-standard într-o singură regulă de politică de Securitate; - NGFW-ul trebuie să suporte separarea printr-un management plane (care se ocupă de GUI-ul firewall-ului și de configurația firewall-ului) și a unui data plane (care se ocupă de traficul care trece prin firewall); - NGFW-ul trebuie să suporte si sa aibă o bază de date de peste 4000 de aplicații cu filtre dinamice bazate pe următoarele criterii de filtrare: categorie, subcategorie, caracteristică comportamentală, tehnologie de bază sau factor de risc; - NGFW-ul trebuie să ofere posibilitatea de a solicita re-categorizarea URL-ului din interiorul firewall-ului prin intermediul WebGUI; - NGFW-ul trebuie să ofere posibilitatea de a importa fluxuri de date de tip threat feeds în firewall;

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				- NGFW-ul trebuie să utilizeze o singură interfață de management de tip WebGUI încorporată atât pentru amenințări, configurare firewall, politici IPS, precum și pentru logare și raportare; - NGFW-ul trebuie să identifice tot payload-ul din aplicație (de exemplu, fișiere și patern-uri de date) pentru a bloca fișierele rău intenționate sau malițioase și pentru a împiedica încercările de exfiltrare ale datelor; - NGFW-ul trebuie să accepte aplicarea de profile de securitate ce include IPS, Anti-Malware, Filtrarea conținutului, Filtrarea URL într-o singură regulă de politică de Securitate; - Suport pentru semnăturile IPS pentru detectarea Post Quantum Cyphers (PQC) - acești algoritmi criptografici pot fi utilizați de actori rău intenționați pentru a extrage date din rețelele securizate sau pentru a introduce malware fără a fi detectați; - NGFW-ul trebuie să accepte marcarea și reclasificarea QoS pe baza IP-ului sursă/destinație, port, protocol și aplicație; - Administratorul trebuie să aibă capacitatea de a gestiona firewall-urile local printr-un WebGui nativ și încorporat și să aibă suport pentru o platformă externă opțională de management central; - NGFW-ul trebuie să susțină capacitatea de a crea politici de securitate pentru a preveni furtul de credențiale și pentru a preveni scurgerea credențialelor corporative către site-uri web terțe și pentru a preveni re-utilizarea credențialelor furate prin

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				activarea autentificării multifactoriale (MFA) la nivelul rețelei pentru orice aplicație, fără nicio modificare a aplicației.; - NGFW-ul trebuie să suporte capacitatea de a impune autentificarea cu mai mulți factori pentru aplicațiile interne; - NGFW trebuie să suporte protecția de securitate la nivel de protocol DNS, cum ar fi: detectarea DNS callback domain (malware și domenii C2, domenii botnet, domenii Fast-flux, DGA aleatorii, DGA de tip dicționar), domenii DNS cu risc ridicat (grayware, domenii noi înregistrate, domenii parcate, cele de tip proxy avoidance, dns dinamic, detectarea predictivă, domenii "îmbătrânite" strategic), atacuri de tip DNS Record Attacks (domain squatting, dangling DNS, zone DNS compromise, DNS Wildcard, CNAME cloacking), atacuri la nivel de protocol DNS (DNS Rebinding, NXNSAttacks), detectarea tunelării la nivel de protocol DNS, ultra-slow DNS Tunneling și DNS infiltration, suport pentru DNS Sinkholing pentru a identifica stațiile infectate într-o retea; - Semnăturile și conținutul de filtrare antivirus și cele pentru URL filtering trebuie să fie native pentru producătorul producătorului echipamentului NGFW - adică nu este folosită nicio terță parte pentru semnăturile de filtrare AV sau URL; - NGFW-ul trebuie să suporte analiza de tip NFGW Zero-Day Malware și trebuie să accepte următoarele protocoale: HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP și SMB; - NGFW-ul trebuie să poată accepta decriptarea următoarelor protocoale: SSL, SSH și trebuie să inspecteze și să aplice politici traficului criptat TLS/SSL, atât pentru

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				traficul de intrare (inbound), cât și de ieșire (outbound), inclusiv pentru traficul care utilizează TLS 1.3 și HTTP/2; - NGFW-ul trebuie să ofere o vizibilitate bogată asupra traficului TLS, cum ar fi cantitatea de trafic criptat, versiunile TLS/SSL, suitele de criptare și multe altele, fără decriptare și trebuie să permită controlul asupra utilizării protocoalelor TLS vechi, a cifrurilor nesigure și a certificatelor configurate greșit pentru a atenua riscurile; - NGFW-ul trebuie să conțină o soluție avansată de analiză a malware-ului (malware sandboxing) și trebuie să aibă în mod implicit suport și pentru scanarea executabilelor MacOS și Linux; - Soluția avansată de analiză a malware (malware sandboxing) trebuie să fie aprobată de FedRamp; - NGFW-ul trebuie să se integreze cu ușurință cu o gamă largă de soluții pentru a valorifica informațiile de tip utilizator și trebuie să poată obține identități de utilizator de la cel puțin urmatoarele: LDAP, portal captiv, VPN, NAC-uri (XML sau API), Syslog, terminal services, header de tip XFF, monitorizarea serverelor și client probing; - NGFW-ul trebuie să accepte integrarea cu surse de tip Directory de la Microsoft AD, Azure AD, Okta, Google, PingID pentru crearea de politici de securitate bazate pe utilizatori și grupuri; - NGFW-ul trebuie să accepte următoarele IdP-uri pentru autentificarea în cloud (SAML): Azure, PingID, Okta, Google, alți IdP-uri SAML 2.0;

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				- NGFW-ul trebuie să sprijine identitatea și autentificarea atât cu furnizorii de identitate din rețeaua locală, cât și cu furnizorii de identitate din cloud, precum și să impună controale bazate pe utilizatori atât în infrastructura locală, cât și în infrastructura cloud; - NGFW-ul trebuie să ofere access la API-uri complet deschis și nelimitat, fără un paywall (abonament) pentru a accesa setul de instrumente de tip Dev toolkit, Tool-uri, Scripturi și sample-uri; - NGFW-ul trebuie să respecte CIPA pentru Google Safe Search și YouTube pentru funcționare la cel mai înalt nivel de Securitate; - NGFW-ul trebuie să accepte capacitatea de a crea rapoarte standard și personalizate, inclusiv rapoarte de utilizare direct din WebGUI-ul echipamentului NGFW; - NGFW-ul trebuie să accepte capacitatea de a regrupa în mod dinamic și automat utilizatorii pe baza evenimentelor de securitate legate de acel utilizator, fără a fi necesar un răspuns manual; - NGFW-ul trebuie să suporte capacitatea de a identifica Domain Generating Algorithms în traficul DNS pentru a proteja împotriva exfiltrării datelor; - NGFW-ul trebuie să suporte etichetarea obiectele pentru a permite aplicarea dinamică a politicilor de securitate, indiferent de orice modificare a IP-ului, a zonei sau a direcției traficului din care provine, fără a fi nevoie de reconfigurarea politicilor; - NGFW-ul trebuie să fie capabil pentru utilizarea unor algoritmi de învățare automată (Machine Learning algorithms) pentru protecție avansată direct din NGFW,

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				fără conexiuni externe necesare pentru a asigura prevenirea atacurilor de tip signatureless attack prevention și identificarea și oprirea încercărilor de phishing nemaivăzute până acum; - NGFW-ul trebuie să poată permite activarea oricărei noi subscripții de securitate fără a afecta performanța traficului care circulă prin acesta (adică minim de control al aplicațiilor, IPS, antivirus, antispyware, sandboxing, filtrare web, securitate DNS, blocarea fișierelor, VPN SSL și IPSec și cu logarea activată); - NGFW-ul trebuie să suporte recomandări automate de politici de securitate care economisesc timp și reduc șansele de eroare umană și care sunt personalizate pentru implementarea fiecărui client pentru a consolida postura de Securitate; - NFGW-ul trebuie să sprijine adoptarea de funcționalități și caracteristici ale firewall-ului și a serviciilor de securitate de la achiziție la activare la configurare până la conformitatea cu cele mai bune practici și să maximizeze rentabilitatea investiției în securitate și trebuie să sprijine urmărirea progresului și să primească recomandări personalizate pentru configurațiile critice ale politicilor pentru a aborda și măsura progresul implementării celor mai bune practice; - NGFW-ul trebuie să sprijine rezolvarea proactivă a întreruperilor firewall-ului prin detectarea și prevenirea problemelor firewall-ului, inclusiv problemele hardware și software ale sistemului, utilizarea resurselor, logare, protecția zonelor de securitate și limite de configurare dinamică ale configurației;

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				- NGFW-ul trebuie să suporte o funcționalitate care, atunci când ceva necesită atenție legat de securitate și probleme de sistem, să poată fi trimisă o notificare de alertă prin e-mail; - NGFW-ul trebuie să accepte funcționalități de tip SD-WAN integrate în firewall și trebuie să ofere direcționarea traficului și cea mai bună experiență pentru utilizatorul final, reducând latența, jitter-ul și pachet loss; - NGFW-ul trebuie să accepte accesul de la distanță VPN (SSL VPN, IPsec VPN, clientless VPN), trebuie să suporte prevenirea amenințărilor aduse de device-urile mobile și aplicarea politicilor bazate pe aplicații, utilizatori, conținut, tipul de dispozitiv și starea dispozitivului; - NGFW-ul trebuie să accepte BYOD cu VPN la nivel de aplicație pentru confidențialitatea utilizatorilor pe Android și iOS; - NGFW-ul trebuie să accepte fallback automat SSL VPN de la IPSec VPN; - NGFW-ul trebuie să accepte conexiuni VPN de pe următoarele platforme: Microsoft Windows și Windows UWP, Apple macOS, Apple iOS și iPad OS, Google Chrome OS, Android OS, Linux OS (RedHat, CentOS, Ubuntu) și dispozitive IoT; - NGFW-ul trebuie să accepte scalarea pe orizontală a numărului de utilizatori VPN, în cazul în care este necesar, utilizând dispozitive NGFW suplimentare într-o configurație fără disponibilitate ridicată (adică autonomă); - NGFW-ul trebuie sa fie asigurat cu o alimentare redundantă.

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				Performante generale: **Performance** • Threat prevention throughput 1 Gbps; • IPsec VPN throughput 1.6 Gbps; • Connections per second 37,500; • Firewall throughput 2.2 Gbps; • Max sessions (IPv4 or IPv6) 200,000. **Policies** • Security rules 2,000; • Security rule schedules 256; • NAT rules 3,000; • Decryption rules 300; • App override rules 300; • Tunnel content inspection rules 300; • SD-WAN rules 250; • Policy based forwarding rules 300; • Captive portal rules 300; • DoS protection rules 300 **Security Zones** • Max security zones 50. **Objects (addresses and services)** • Address objects 10,000; • Address groups 250; • Members per address group 2,500; • Service objects 1,500; • Service groups 500; • Members per service group 500;

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				• FQDN address objects 2,000; • Max DAG IP addresses 50,000; • Tags per IP address 64. **Security Profiles** • Security profiles 100. **SSL Decryption** • Max SSL inbound certificates 75; • SSL certificate cache (forward proxy) 1,000; • Max concurrent decryption sessions 25,600; • SSL Port Mirror Yes. **URL Filtering** • Total entries for allow list, block list and custom categories 25,000; • Max custom categories 2,849; • Max custom categories (virtual system specific) 500; • Management plane dynamic cache size 600,000. **Interfaces** • I/O: 1G SFP/RJ45 combo (2), RJ45 (4), RJ45/PoE (4); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2), Micro USB console port (1). **Storage Capacity** • 128 GB eMMC **Virtual Routers** • Virtual routers 3. **Routing** • IPv4 forwarding table size 5,000; • IPv6 forwarding table size 5,000; • System total forwarding table size 5,000;

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				• Max routing peers (protocol dependent) 1,000; • Static entries - DNS proxy 1,024. **L2 Forwarding** • ARP table size per device 3000; • IPv6 neighbor table size 3000; • MAC table size per device 3000; • Max ARP entries per broadcast domain 3000; • Max MAC entries per broadcast domain 3000. **NAT** • Total NAT rule capacity 3,000; • Max NAT rules (static) 3,000; • Max NAT rules (DIP) 2,000; • Max NAT rules (DIPP) 1,000; • Max translated IPs (DIP) 128,000; • Max translated IPs (DIPP) 1,000. **Address Assignment** • DHCP servers 5; • DHCP relays 500; • Max number of assigned addresses 64,000. **High Availability** • Devices supported 2; • Max virtual addresses 48. **QoS** • Number of QoS policies 1,000; • Physical interfaces supporting QoS 8; • Clear text nodes per physical interface 31. **IPSec VPN** • Max IKE Peers 2,800;

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				• Site to site (with proxy id) 2,800; • SD-WAN IPsec tunnels 2,800.
	Alte acte pentru prezentare			- Copia certificatului în calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013. - Copia Certificatului ISO 27001:2018, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT si de securitate, inclusiv teste de penetrare – certificat confirmat cu aplicarea semnăturii electronice.
	Garanție			**2 ani,** conform specificațiilor tehnice (scrisoare oficială pentru confirmarea garanției, garanție oficială, indicată pe site-ul oficial al producătorului). Produsele defecte, înlocuite în termenul de garanție vor beneficia de același termen de garanție care va curge de la data înlocuirii celui defect. Furnizorul se obligă să asigure servicii sigure și permanente și/sau înlocuirea echipamentelor defecte în perioada de garanție. Service-ul si suportul in perioada de garanție va fi efectuat de către personal abilitat/certificat sa acționeze asupra echipamentelor, pentru a nu se pierde garanția acordat.
	Termenul de livrare			Maxim pana la **90 zile** de la data intrării în vigoare a contractului. Costul livrării va fi inclus în prețul total – livrarea se va realiza la sediul CCI a RM conform adresei indicate. Ofertantul câștigător va asigura transportul echipamentului la adresa stabilită de către CCI a RM.

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
				La livrare echipamentele vor fi însoțite de factura, declarații/certificat de conformitate, certificat de garanție/calitate, documentația tehnica, carnete service, proces verbal de recepție si punere in funcțiune etc. Dacă produsul livrat nu este conform specificațiilor minime indicate, autoritatea contractantă poate să îl refuze, iar furnizorul va trebui să îl înlocuiască, pentru a satisface cerințele specificațiilor tehnice din caietul de sarcini şi din contract, fără a percepe un cost suplimentar. Produsele vor fi recepționate de persoanele desemnate de către CCI a RM. În cadrul recepției cantitative şi calitative, achizitorul are dreptul, prin reprezentanții săi, de a inspecta şi/sau testa produsele pentru a verifica conformitatea lor cu specificațiile din documentația de atribuire şi din ofertă. Recepția cantitativă va fi efectuată în momentul livrării şi va consta în: - verificarea denumirii comerciale a produsului, - verificarea cantității livrate. Recepția calitativă constă în inspecția şi testarea produselor livrate şi se materializează printr-un proces-verbal de recepție si punere în funcțiune. Livrarea produselor se considera încheiată in momentul în care sunt îndeplinite prevederilor clauzelor de recepție la nivel calitativ si de performanta ofertat, si beneficiarul a semnat si stampilat procesul verbal.

Nr d/o	Denumirea bunurilor solicitate	Cantitatea	Unitatea de măsură	Specificarea tehnică deplină solicitată, standarde de referință
	Instalare, configurare și mentenanță			Lucrările de instalare, configurare, punerea în funcțiune si training trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comerciala. Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului.

4. Termenul limită de depunere a ofertelor

Dosarele de aplicare vor fi depuse până la data de 26 ianuarie, ora 17:00 la adresa de e-mail valentina.ichim@chamber.md, cu mențiunea „Echipament IT – CCI a RM”. Ofertele incomplete sau transmise după termenul indicat mai sus nu vor fi acceptate.

5. Criteriile de selectare a ofertantului

Evaluarea ofertelor se va face pe baza unui raport de 40 % pentru oferta tehnică și 60 % pentru oferta financiară:

- dosar complet ce corespunde caietului de sarcini;
- corespunderea bunului propus parametrilor tehnici indicați în caietul de sarcini.

6. Achitarea

Achitarea se va efectua în MDL prin transfer în contul bancar indicat de ofertant în factura de plată.

Suma va fi achitată integral în maxim 10 zile după livrarea bunului.

Plata produselor efectiv livrate se va realiza în baza procesului verbal asumat de ambele părți si factura cu evidențierea tuturor informațiilor minime definite prin legislația.