ANUNȚ DE PARTICIPARE INCLUSIV PENTRU PROCEDURILE DE PRESELECȚIE/PROCEDURILE NEGOCIATE

privind achiziționarea: ***Echipamente de rețea de tip Next Generation Firewall (NGFW)***

prin procedura de achiziție ***Cererea ofertelor de pret***

****Procedura a fost inclusă în planul de achiziții publice a autorității contractante (Da/Nu): Da***
Link-ul către planul de achiziții publice publicat:

https://cnas.gov.md/ro/transparenta/achizitii-publice/planuri-de-achizitii-publice

1. **Denumirea autorității contractante:** *Casa Națională de Asigurări Sociale*
2. **IDNO:** *1004600030235*
3. **Adresa:** *mun. Chișinău, str. Gh. Tudor,3*
4. **Numărul de telefon/fax:** *022-257-681; 022-257-840; 022-257-752 .*
5. **Adresa de e-mail şi pagina web oficială ale autorității contractante:** achizitiicnas@cnas.gov.md , www.cnas.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 sunt anexate în cadrul procedurii în M-Tender 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:**

Codul CPV: *32420000-3 echipamente de rețea*

Specificația tehnică

Denumire bunurilor solicitate	Specificarea tehnică deplină solicitată, Standarde de referinţă	Cantitatea	Valoarea estimată fără TVA lei MLD	Pasul minim de licitare (electronică) lei MLD
1.	***Echipamente de rețea de tip Next Generation Firewall (NGFW)*** Cerințe tehnice 1. Protecția rețelei cu controlul stării sesiunilor; 2. Recunoașterea și blocarea aplicațiilor de rețea la nivelul 7 al modelului OSI în funcție de traficul care trece prin firewall, inclusiv individual pentru toate aplicațiile care folosesc porturi comune, inclusiv 80 și 443, precum și pentru aplicațiile care utilizează porturi TCP/UDP dinamice; 3. Firewall-ul NGFW propus trebuie să fie certificat minim conform standardelor ISO 27001, ISO 27017, ISO 27018, ISO 27701, Germany C5, Common Criteria, FIPS 140-2, CMVP. 4. Firewall-ul NGFW propus nu trebuie să necesite o	**10 bucăți**	**387 000,00**	**3 800,00**

repornire pentru a verifica și instala actualizările de securitate.

5. Firewall-ul NGFW propus trebuie să poată identifica aplicațiile indiferent de portul utilizat, criptarea SSL/SSH sau metodele de ocolire folosite.
6. Firewall-ul NGFW propus trebuie să clasifice aplicațiile neidentificate pentru gestionarea politicii, analiza criminalistică a amenințărilor sau dezvoltarea tehnologiilor de identificare a aplicațiilor.
7. Firewall-ul NGFW propus trebuie să fie o soluție dezvoltată inițial pentru asigurarea securității (nu un management de aplicații cu un firewall de bază care verifică starea).
8. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas.
9. Firewall-ul NGFW propus trebuie să fie un dispozitiv dezvoltat inițial cu o arhitectură de procesare paralelă a traficului pe un singur pas.
10. Firewall-ul NGFW propus trebuie să poată să delimiteze diferite părți ale unei aplicații, cum ar fi permiterea chat-ului pe Facebook, dar blocarea posibilității de a trimite fișiere.
11. Firewall-ul NGFW propus trebuie să controleze accesul și să aplice politici pentru site-uri web și aplicații, inclusiv pentru aplicațiile SaaS.
12. Firewall-ul NGFW propus trebuie să utilizeze un sistem de operare unificat în toate formatele.
13. Firewall-ul NGFW propus trebuie să sprijine crearea politicii de securitate pentru prevenirea furtului de credențiale.
14. Firewall-ul NGFW propus trebuie să sprijine aplicarea autentificării multi-factor pentru aplicațiile interne.
15. Firewall-ul NGFW propus trebuie să permită vizibilitatea și controlul aplicațiilor care folosesc porturi non-standard, într-o politică unică de securitate.
16. Firewall-ul NGFW propus trebuie să poată oferi algoritmi de învățare automată pentru protecție avansată direct din NGFW, fără a necesita conexiuni externe.
17. Recunoașterea în traficul inspectat la Layer-7 al modelului OSI a semnăturilor stocate pe MFE pentru următoarele categorii de aplicații:

17.1 . Aplicații corporative:

17.1.1. Servicii de autentificare, inclusiv Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS;

17.1.2. Sisteme de gestionare a bazelor de date (SGBD), inclusiv Microsoft SQL, Oracle, DB2, Postgres, Sybase;

17.1.3. Servicii de fișiere, inclusiv Microsoft SMB.

17.1.4. ERP, CRM, inclusiv SAP, 1C;

17.1.5. Sisteme de management al documentelor electronice și schimb de mesaje, inclusiv EMC

	Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus; 17.1.6. Protocoale de schimb de e-mail: SMTP, POP3, IMAP; 17.1.7. Protocoale VoIP și conferințe audio-video, inclusiv SIP, H.323, H.245, H.225, Webex; 17.1.8. Servicii de actualizare software, inclusiv Microsoft Update, software antivirus (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple; 17.1.9. Servicii de backup, inclusiv Symantec Backup Exec; 17.1.10. Servicii de virtualizare și acces la terminale, inclusiv VMware, Citrix, Microsoft RDP; 17.1.11. Alte protocoale și tehnologii utilizate pentru crearea aplicațiilor distribuite, inclusiv CORBA, SOAP; 17.1.12. Protocoale de acces de la distanță, inclusiv Telnet, SSH, VNC, Radmin; 17.1.13. Protocoale de rețea, inclusiv protocoale de rutare dinamică și SSL, IPsec VPN; 17.2. Aplicații Internet: 17.2.1. E-mail, inclusiv Gmail, Yandex.Mail, Mail.ru, Hotmail; 17.2.2. Rețele sociale, inclusiv Facebook, Google+, LinkedIn, ВКонтакте, Odnoklassniki, „Moy Mir”; 17.2.3. Servicii de mesagerie instantanee, inclusiv Jabber, IRC, MSN, servicii similare în cadrul rețelelor sociale enumerate mai sus; 17.2.4. Servicii de conferință audio-video 17.2.5. Servicii de schimb de fișiere prin HTTP(S) și peer-to-peer, inclusiv Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, WebDav; 17.2.6. Streaming audio-video (indiferent de site-ul web), inclusiv YouTube, Vimeo, audio și video prin HTTP; 17.2.7. Servicii de publicare a desktop-ului și oferirea de acces de la distanță, inclusiv TeamViewer, LogMeIn; 17.2.8. Proxy externe și anonimizatoare, inclusiv Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy; 17.2.9. Servicii de construire a VPN-urilor private și tuneluri deasupra altor aplicații, inclusiv FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS; 18. Oferirea de instrumente integrate în MFE pentru crearea semnăturilor proprii de aplicații bazate pe expresii regulate folosind decodoare pentru HTTP(S), FTP, SMB, SMTP, RPC și altele, precum și pe mască pentru conținutul pachetelor TCP/UDP; 19. Recunoașterea aplicațiilor transmise prin protocolul HTTP/2; 20. Recunoașterea aplicațiilor de rețea prin traficul criptat SSL (suport pentru chei RSA de până la 2048 de biți) și SSHv2 care trece prin firewall (decriptarea SSL, SSHv2) – atât pentru conexiunile intrante, cât și			

	pentru cele ieșite, transparent pentru utilizatori în domeniu, cu posibilitatea de a controla funcțiile individuale ale aplicațiilor, inclusiv trimiterea de mesaje pe rețelele sociale, schimbul de fișiere, streaming audio și video; 21. Inspecția tunelurilor: 21.1. Generic Routing Encapsulation (GRE) (RFC 2784); 21.2. Trafic IPSec necriptat [NULL Encryption Algorithm pentru IPSec (RFC 2410)]; 21.3. Mod de transport AH IPSec. 22. Recunoașterea secvențială a diferitelor aplicații utilizate într-o singură sesiune; 23. Recunoașterea utilizatorilor care folosesc aplicații de rețea prin integrarea cu serviciile corporative de autentificare a utilizatorilor, cum ar fi Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; posibilitatea integrării cu alte servicii de autentificare (de exemplu, controlerele de rețea wireless) printr-o API XML deschisă; posibilitatea de a utiliza autentificarea forțată a utilizatorilor folosind o pagină WEB – „Captive portal”; suport pentru Kerberos, Tacacs+, SAML v.2, suport pentru roaming-ul L3 al utilizatorilor prin sondaje WMI și NetBios; 24. Inspecția în timp real a conținutului traficului transmis prin firewall pe baza semnăturilor și comportamentului, protecția împotriva vulnerabilităților, atacurilor de rețea și a malware-ului, recunoașterea tipurilor de fișiere pe baza semnăturilor acestora, detectarea virușilor transmiși prin web, e-mail, FTP, SMB, spyware, viermi de rețea, blocarea transmiterii unor conținuturi specifice folosind expresii regulate, inclusiv pentru aplicațiile care utilizează criptare SSL și SSHv2; 25. Crearea de reguli pentru traficul care trece prin firewall într-o politică unificată de securitate, utilizând următorii parametri pentru fiecare conexiune: 25.1. Adresa IP a expeditorului, 25.2. Adresa IP a destinatarului, 25.3. Serviciile L4 utilizate: porturi pentru protocoalele TCP și UDP, 25.4. Numele utilizatorilor sau grupurilor de utilizatori din Active Directory, 25.5. Aplicațiile la nivelul 7 al modelului OSI, 25.6. URL categorii. 26. Crearea de reguli într-o politică unificată de securitate, utilizând ca parametri informațiile despre adresele IP ale expeditorului, destinatarului, serviciile utilizate (porturi TCP/UDP), numele utilizatorilor, grupurilor de utilizatori și aplicațiile utilizate de aceștia sau anumite categorii de aplicații. În politicile create, trebuie să existe posibilitatea implementării următoarelor acțiuni:			

	• Permisiune sau interdicție; • Permisiunea unui anumit aplicații sau categorii de aplicații de a utiliza doar porturi TCP/UDP standard sau strict definite. Aceste porturi nu trebuie să fie folosite de alte aplicații fără o politică care să permită explicit astfel de interacțiuni; • Permisiune, dar cu scanare pentru viruși și alte amenințări; • Permisiune sau interdicție pe bază de orar, utilizator sau grup de utilizatori; • Decriptare și verificare. Dacă nu s-a putut decripta (în cazul unui algoritm criptografic nestandard, certificat expirat etc.) – interzicere; • Ne-decriptarea anumitor categorii de URL și site-uri web de încredere; • Aplicarea marcajului DSCP și limitarea traficului folosind politici QoS bazate pe aplicații, adrese IP, utilizatori și grupuri de utilizatori; • Implementarea hardware a QoS pentru traficul real-time, identificat la nivelul aplicațiilor; • Aplicarea redirecționării traficului pe bază de politici (Policy Based Forwarding); • Permisiunea anumitor funcții ale aplicației; • Oricare combinație dintre acțiunile de mai sus. 27. Protecție antivirus, protecție împotriva software-ului spyware, protecție împotriva vulnerabilităților și atacurilor de rețea (sistem de detecție și prevenire a intruziunilor), filtrare URL utilizând o bază dinamică de reputație, care susține categorizarea diferitelor secțiuni ale aceluiași site web, inclusiv susținerea categoriilor pentru site-uri web în limba rusă, blocarea transferului de fișiere pe baza tipurilor definite de semnături; 28. Posibilitatea de a verifica suplimentar traficul pentru amenințări necunoscute prin analiza acestuia utilizând tehnologia învățării automate prin servicii cloud; 29. Detectarea și filtrarea solicitărilor către resursele din rețea în funcție de categoria acestora, de exemplu, site-uri malware, rețele sociale, resurse publicitare etc.; 30. Suport pentru acțiuni: permisiune, notificare, blocare, solicitarea confirmării utilizatorului, solicitarea parolei utilizatorului; 31. Filtrarea URL trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 32. Analiza SNI în TLS Hello simultan cu URL-ul în cererea HTTP pentru a contracara tehnicile de ocolire de tip SNIcat; 33. Analiza cererilor DNS suspecte, domeniilor DGA și localizarea stațiilor infectate utilizând tehnologia DNS sinkhole (modificarea răspunsului serverului DNS); 34. Detectarea tehnicilor de ocolire a protecției prin cereri DNS care încearcă să folosească domenii generate automat (DGA), inclusiv analiza frecvenței n-			

	gramelor, analiza entropiei, frecvența cererilor, tunelarea în DNS, canale de transfer de date prin cereri DNS, inclusiv tuneluri DNS ultra-lente; 35. Blocarea domeniilor DGA, domeniilor DGA create pe baza unui dicționar, tehnici de ocolire DNS-rebinding, FastFlux, interogări către înregistrări DNS suspendate, atacuri NSNX, atacuri cu domenii recent înregistrate; 36. Analiza cererilor DNS suspecte trebuie realizată cu tehnologia de învățare automată pentru a reduce timpul de reacție la amenințări; 37. Protecție împotriva tehnicilor de evitare (evasions), de exemplu MPTCP; 38. Oferirea unui serviciu de scanare a fișierelor potențial dăunătoare necunoscute în sandbox cu sisteme de operare Microsoft Windows, Linux prin metoda de emulare a rulării și vizualizare a documentelor; 39. Sandbox-ul trebuie să verifice fișierele executabile suspecte (inclusiv EXE, DLL, SCR, BAT, etc.), fișiere ELF, documente în formatele PDF, MS Office 2007, 2010, 2016 și mai sus, Java și Flash, Android APK, Mach-O, DMG și PKG, arhive RAR, ZIP, 7Zip; 40. Firewall-ul trebuie să trimită spre verificare în sandbox fișierele suspecte transmise prin aplicațiile HTTP, SMTP, POP3, IMAP, SMB, FTP, precum și implementările acestora prin SSL, dacă există; 41. Sandbox-ul trebuie să genereze și să trimită către firewall un raport despre verificarea fișierului; 42. Sandbox-ul trebuie să genereze semnături pentru blocarea atacurilor de tip zero-day pentru utilizarea pe toate firewall-urile companiei în aplicațiile enumerate, în decurs de 5 minute de la primirea fișierului pentru verificare; 43. Firewall-ul trebuie să primească semnăturile fișierelor din sandbox și să aibă un motor de blocare bazat pe noile semnături obținute de la sandbox-ul cloud sau local; 44. Sandbox-ul furnizorului cloud trebuie să aibă posibilitatea de a schimba semnături între toți clienții furnizorului; 45. Firewall-ul trebuie să primească din sandbox indicatori de compromitere: IP, URL, DNS, care sunt utilizate de codul malițios și să blocheze conexiunile pe baza listei de indicatori malițioși. 46. Sandbox-ul trebuie să verifice linkurile HTTP:// și HTTPS:// din e-mailuri prin protocoalele SMTP/POP3. 47. Sandbox-ul trebuie să verifice fișierele din aplicațiile criptate SSL, cel puțin în protocolul HTTPS. 48. Suport obligatoriu pentru învățarea automată în timpul inspectării amenințărilor de tip zero-day pentru a reduce întârzierea în inspecția fișierelor suspecte; 49. Sandbox-ul trebuie să asigure analiza comportamentului fișierelor și linkurilor suspecte în cloud privat sau extern (sandbox), să detecteze noi			

	malware și să genereze automat semnături antivirus în decurs de 5 minute și să actualizeze baza de reputație URL în decurs de 30 de minute, care se vor instala pe toate dispozitivele Clientului cu abonamentele corespunzătoare; 50. Posibilitatea integrării cu subsistemul de detectare a amenințărilor zero-day, implementat pe un dispozitiv hardware dedicat aceluiași furnizor, plasat pe obiectul central al Clientului (cloud privat), care permite generarea automată a semnăturii antivirus local, pe dispozitivul hardware dedicat în centrul de date (DC) al Clientului în decurs de 5 minute; 51. Sandbox-ul local dedicat trebuie să aibă un API pentru primirea fișierelor spre verificare atât de la firewall-uri, cât și de la servicii terțe; 52. Sandbox-ul trebuie să genereze rapoarte despre verificările efectuate și să permită vizualizarea acestora în format PDF; 53. Sandbox-ul cloud trebuie să utilizeze tehnologia Bare Metal Analysis fără a utiliza emularea sistemului de operare; 54. Firewall-ul trebuie să aibă capacitatea de a trimite fișiere diferite în sandbox-uri diferite, de exemplu, fișierele EXE în sandbox-ul cloud, iar fișierele DOC în sandbox-ul local; 55. Sandbox-ul cloud trebuie să accepte fișiere PE pentru verificare, chiar și în absența unui abonament; 56. Suport pentru următorii furnizori de autentificare multi-factor (Multi-Factor Authentication - MFA) (direct, fără utilizarea produselor intermediare):Duo, • Okta, • RSA SecureID, • PingID; 57. Protecție împotriva furtului de loginuri și parole ale utilizatorilor prin integrarea cu Active Directory (AD), monitorizarea transmiterii conturilor de utilizator către zone de securitate neîncredere, autentificarea forțată a utilizatorilor prin autentificare cu doi factori (MFA); 58. Funcționalitate de control granular al accesului utilizatorilor de la distanță în mediul de lucru corporativ, cu posibilitatea de verificare a existenței anumitor software-uri pe stația de lucru a utilizatorului și accesul prin dispozitive mobile; 59. Funcționalitate de protecție împotriva atacurilor DoS; 60. Posibilitatea de a activa 100% din semnăturile IPS, antivirus, filtrarea URL-urilor, controlul aplicațiilor și Threat Intelligence fără a degrada performanța; 61. Funcționalitate de blocare a scanării porturilor ICMP/TCP/UDP; 62. Detectarea obiectelor din fișierele transmise prin rețea care conțin informații importante și blocarea transmiterii acestor fișiere; 63. Detectarea prezenței datelor filtrabile în fișierele transmise prin rețea, incluzând, dar fără a se limita la:			

	Adobe PDF, HTML, Microsoft Office (Excel, Word, PowerPoint). Rich Text Format; 64. Prezența șabloanelor de date preconfigurate, cum ar fi numerele de carduri de credit. 65. Suport pentru crearea de șabloane proprii de date pe baza expresiilor regulate. 66. Posibilitatea de integrare cu subsistemul de management centralizat, logare, raportare și actualizare a software-ului pentru firewall-uri de același furnizor. 67. Cerințe pentru sistemul de management centralizat: • Funcționalități avansate de vizualizare a activității aplicațiilor rețelei, amenințărilor rețelei detectate și blocate, utilizarea aplicațiilor de către utilizatori. Permite filtrarea informațiilor pe aplicații, amenințări, utilizatori, adrese IP, porturi TCP/UDP, zone de securitate, tipuri de amenințări etc.; • Corelarea automată a jurnalelor de diferite tipuri, generate în cadrul aceleași sesiuni (filtrarea traficului prin firewall, protecția împotriva amenințărilor, controlul transferului de fișiere, filtrarea URL); • Posibilitatea de corelare automată a evenimentelor de securitate folosind obiecte de corelare actualizabile care folosesc informații de la protecția antivirus, protecția împotriva software-ului spyware, protecția împotriva vulnerabilităților și atacurilor, amenințările de tip zero-day; • Funcționalități de generare automată a rapoartelor și de generare a rapoartelor pe bază de program, cu opțiuni de personalizare manuală a rapoartelor. Rapoartele trebuie să fie vizibile prin interfața grafică (GUI) și să poată fi exportate în formate PDF și CSV. • Posibilitatea de a configura funcționalitățile SD-WAN prin consola de management centralizat. • Sistemul trebuie să poată exporta logurile către soluții externe prin syslog, utilizând formate standardizate precum CEF sau LEEF; • Trebuie să existe mecanisme de inițializare automată pentru echipamente noi, inclusiv în locații la distanță, fără intervenție manuală; • Trebuie să fie posibilă actualizarea centralizată a software-ului pentru echipamentele administrate, într-un mod simplificat; • Soluția trebuie să ofere interfețe moderne de integrare (REST API) compatibile cu XML și JSON, pentru interoperabilitate cu alte sisteme. • Fiecare administrator trebuie să poată face modificări izolate, cu salvare separată, pentru a evita suprascrierea neintenționată; • Sistemul trebuie să permită definirea de roluri și permisiuni personalizate pentru utilizatori, cu acces diferențiat la funcționalități. • Platforma trebuie să permită organizarea			

	echipamentelor și configurațiilor prin grupuri, ierarhii și etichete; • Sistemul trebuie să suporte funcționare în mod redundant (high availability) și echilibrare a sarcinii (load balancing); 68. Posibilitatea de a detecta și analiza traficul dispozitivelor IoT folosind algoritmi de învățare automată. 69. Funcționalitatea de a trimite traficul SSL decriptat către dispozitive externe. 70. Funcționalitatea de a captura traficul de la dispozitive externe și de a-l cripta într-un tunel SSL pentru transmiterea prin Internet. 71. Prezența unui raport separat pentru aplicațiile de tip SaaS. 72. Funcționalitatea IPSec VPN. 73. Integrarea cu sistemele externe SIEM/SIM prin protocolul Syslog, cu configurare flexibilă a formatului jurnalelor. 74. Suport pentru rutare statică și protocoale de rutare dinamică BGP, OSPF, RIP. 75. Suport pentru diverse moduri de lucru ale interfețelor rețelei (monitorizare trafic mirroring, mod transparent, Layer 2 și Layer 3). 76. Suport pentru IPv6, inclusiv identificarea aplicațiilor și utilizatorilor. 77. Suport pentru multicast, incluzând PIM-SM, PIM-SSM, IGMP v1, v2, v3. 78. Suport pentru rutarea între VLAN-uri. 79. Suport pentru NAT, DHCP și DHCP relay. 80. Suport pentru etichetarea cadrelor prin 802.1Q (minim 4094 VLAN-uri). 81. Suport pentru agregarea interfețelor prin 802.3ad (suport LACP). 82. Suport pentru pachete mari (Jumbo frames). 83. Managementul rolurilor administratorilor locali: • Posibilitatea de a restricționa vizualizarea și gestionarea la nivelul dispozitivului și al sistemelor virtuale (contexte); • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la orice secțiune a interfeței web; • Posibilitatea de a acorda acces în modul de editare sau doar pentru citire, sau de a restricționa accesul la CLI-ul firewall-ului. 84. Firewall-ul hardware trebuie să dispună de o platformă hardware specializată, care să permită administrarea dispozitivului fără întreruperi, chiar și în condiții de încărcare maximă. Trebuie să fie asigurate resurse de procesare dedicate, separate pentru analiza traficului monitorizat și pentru activitățile de management. Administrarea fiecărui dispozitiv în parte trebuie să se			

	realizeze prin protocoalele HTTPS și SSH, fără a necesita instalarea vreunui software suplimentar de administrare pe stația de lucru a administratorului. Interfața de administrare a firewall-urilor (web și CLI) trebuie să fie unificată cu subsistemul de management centralizat, jurnalizare, raportare și actualizare a software-ului. Cerințe de performanță ale firewall-ului: Performance: • Threat prevention throughput 1.2 Gbps; • IPsec VPN throughput 800 Mbps; • Connections per second 1100; • Firewall throughput 1.4 Gbps; Policies: • Security rules min 500; • Security rule schedules min 256; • NAT rules min 400; • Tunnel content inspection rules 100; • SD-WAN rules min 100; • Policy based forwarding rules min 100; • DoS protection rules min 100. Security Zones: • security zones 25. Security Profiles: • Security profiles min 75. URL Filtering: • Total entries for allow list, block list and custom categories 25,000; Interfaces: • I/O: 1G RJ45 (7); • Management I/O: 10/100/1000 out-of-band management port (1), RJ45 console port (1), USB port (2). Storage Capacity: • 128 GB Virtual Routers: • Virtual routers 3. Routing: • IPv4 forwarding table size min 5,000; • IPv6 forwarding table size min 2500; • System total forwarding table size min 5,000; L2 Forwarding: • ARP table size per device 1500; • IPv6 neighbor table size 1500; • MAC table size per device 1500; Address Assignment: • DHCP servers 3; • DHCP relays 500; •			

	IPSec VPN: • Suport Site to site over gre IPSec tunnels • SD-WAN IPsec tunnels 85. Alte cerințe obligatorii: - Garanție, Mentenanta si Suport HW+SW incluse – 12 luni; - Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului; - Ofertantul va indica în ofertă costul serviciilor pentru efectuarea instalării și configurării a echipamentului ofertat, va asigura integrarea echipamentului ofertat cu dispozitivele existente pe baza platformei existente in cadrul instituției prin realizarea configurărilor necesare, cu setarea tuturor parametrilor aplicabili în corespundere cu cerințele înaintate pe infrastructura Beneficiarului. - Prezentarea a certificatelor a minim 1 specialist pe produsul ofertat din partea ofertantului (fără asociere cu o alta companie); - Ofertantul va prezenta copia Certificatului ISO 27001:2018, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT - Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware si software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea si managementul infrastructurii IT si de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa; - Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013; - Referințe de vânzare NGFW – minim 3 contracte; - Termen de livrare: maxim pana la 90 zile de la data intrării în vigoare a contractului			
Valoarea estimativă		**387 000,00**		

Anexa nr. 1

Cerințe suplimentare se vor include ca parte componentă a contractului:

1. Echipamentul propus trebuie să fie furnizat de producători recunoscuți mondiali (BRAND NAME).

2. Furnizorul va asigura instalarea și configurarea echipamentului prin specialiștii certificați menționați în ofertă, în ferestre de mentenanță agreate, fără întreruperea serviciilor critice.
3. Garanția echipamentelor livrate cade în răspunderea vânzătorului pe toată perioada de garanție definită în ofertă.
4. În cazul apariției unor defecțiuni în perioada de garanție, furnizorul are obligația de a efectua reparațiile necesare sau de a asigura înlocuirea elementelor defecte cu piese de rezervă conforme, pe propria cheltuială. Deservirea în cazul unor neajunsuri sau defectări tehnice a utilajului are loc conform programului de lucru de către furnizor la Aparatul Central CNAS. Recepționarea și livrarea utilajului reparat în baza garanției se efectuează la sediul Aparatului Central CNAS.
5. Bunurile vor fi livrate cu transportul Vânzătorului și descărcate în depozitul aparatului central CNAS mun. Chișinău, str. Gheorghe Tudor 3.
6. Bunurile livrate urmează să fie însoțite de certificatul de origine și certificatul de atestare a calității echipamentului.
7. Bunurile livrate trebuie să fie noi, nefolosite și ne-recondiționate (non-refurbished) și să nu fie fabricate cu mai mult de 12 luni înainte de data livrării.

9. În cazul procedurilor de preselecţie se indică numărul minim al candidaţilor şi, dacă este cazul, numărul maxim al acestora. *Nu se aplică*

10. În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):

1). Pentru fiecare lot în parte

11. Admiterea sau interzicerea ofertelor alternative: *Nu se admite*

12. Termenii și condițiile de livrare/prestare/executare solicitați: *Timp de 90 zile din data înaintării comunicării către Vânzător privind transmiterea dării de seamă la Agenția Achiziții Publice, cu livrare și descărcare a bunurilor la depozitul CNAS din str. Gheorghe Tudor nr. 3 mun. Chișinău, cu recepționarea de către persoana responsabilă desemnată din cadrul CNAS.*

13. Termenul de valabilitate a contractului : *31.12.2026*

14. 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*

15. 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*

16. 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	Criteriile de calificare și de selecție (Descrierea criteriului/cerinței)	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	Prezentarea Cererii de participare conform ***Anexei nr.7*** din Ordinul MF 115/2021**.**	Cerere de participare confirmată prin semnătura electronică	***Obligatoriu***
2	Prezentarea Declarației privind valabilitatea ofertei conform ***Anexei nr.8*** din Ordinul MF 115/2021	Declarația privind valabilitatea ofertei confirmată prin semnătura electronică	***Obligatoriu***
3	Prezentarea Specificații de preț conform ***Anexei nr.23*** din Ordinul MF 115/2021	Specificații de preț, confirmat prin semnătura electronică	***Obligatoriu***

4	Prezentarea Specificații tehnice conform ***Anexei nr.22*** din Ordinul MF 115/2021	Specificații tehnice, confirmată prin semnătura electronică .	***Obligatoriu***
5	Prezentarea Formularul standard al Documentului Unic de Achiziții European completat	Formularul standard al Documentului Unic de Achiziții European confirmat prin semnătura electronică	***Obligatoriu***
6	Vor fi excluși operatorii economici care nu și-au îndeplinit obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în ţara în care este stabilit.	Accesarea informației privind îndeplinirea obligațiilor de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale de către candidatul sau ofertantul la procedura de atribuire a contractului de achiziții publice se va efectua nemijlocit de către autoritatea contractantă prin accesarea de către autoritățile contractante de pe platforma de interoperabilitate (MConnect), precum și de pe Portalul guvernamental de date, accesând următorul link: https://date.gov.md/open/company-details ..	***Obligatoriu***
7	Vor fi excluși operatorii economici care nu dispun de capacitatea de exercitare a activităţii profesionale	- operatorul economic participant la licitație trebuie să dețină un centru de deservire de garanție a bunurilor livrate sau contract cu un asemeni centru de deservire valabil la data deschiderii ofertei. - Producător de calculatoare trebuie să fie recunoscut mondial (BRAND NAME). - Ofertantul va prezenta copia Certificatului ISO 27001:2018, in domeniul serviciilor privind asigurarea securității informației, design-ul acestuia, implementarea, monitorizarea si managementul infrastructurii IT - Ofertantul va prezenta Certificatului ISO 9001:2015, pentru Servicii de comercializare și implementare suport tehnic în garanție și post garanție pentru sisteme informaționale, echipamente hardware si software și Servicii privind asigurarea securității informației, designul, implementarea, monitorizarea si managementul infrastructurii IT si de Securitate – certificat confirmat cu aplicarea semnăturii electronice; - Ofertantul va prezenta Autorizarea de la producător pentru licitația la care participa; - Prezentarea a certificatelor a minim 1 specialist pe produsul ofertat din partea ofertantului (fără asociere cu o alta companie); - Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013;	***Obligatoriu***
8	Vor fi excluși operatorii economici care nu dispun de standarde de asigurare a calităţii	Declarație pe proprie răspundere referitor la - Garanția echipamentelor livrate cade în răspunderea vânzătorului pe toată perioada de garanție și constituie 12 luni. - Producătorul trebuie să ofere suport prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului - În caz de defecție a echipamentului furnizorul trebuie să asigure repararea elementelor defectate sau să dețină rezerve necesare pentru substituire lor în baza garanției. Deservirea în cazul unor neajunsuri sau defectări tehnice a utilajului are loc conform programului de lucru de către furnizor la Aparatul Central CNAS. Recepționarea și livrarea utilajului reparat în baza garanției se efectuează la sediul Aparatului Central CNAS. - Bunurile livrate urmează să nu fie mai vechi de un an de la data livrării și să fie noi (non refurbished).	***Obligatoriu***

9	Va fi exclus orice operator economic care nu deține numărul de înregistrare a producătorului în Lista producătorilor	Declarație pe propria răspundere privind numărul de înregistrare a producătorului de echipamente electrice și electronice în Lista producătorilor de produse supuse reglementărilor de responsabilitate extinsă a producătorilor (HG 212/2018) - confirmată prin semnătura electronică a Participantului	***Obligatoriu***
10	Va fi exclus din procedura de atribuire a contractului de achiziţii publice orice ofertant sau candidat despre care are cunoştinţă că, în ultimii 5 ani, a fost condamnat, prin hotărârea definitivă a unei instanţe judecătoreşti, pentru participare la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, pentru fraudă şi/sau pentru spălare de bani, pentru infracţiuni de terorism sau infracţiuni legate de activităţi teroriste, finanţarea terorismului, exploatarea prin muncă a copiilor şi alte forme de trafic de persoane.	La depunerea ofertei prin declararea în DUAE/la evaluare la solicitarea AC	***Obligatoriu*** *Lipsa condamnării pe parcursul a ultimilor 5 ani.*
11	Va fi exclus orice operator economic care se află în proces de insolvabilitate ca urmare a hotărârii judecătoreşti.	La depunerea ofertei prin declararea în DUAE	***Obligatoriu*** *Nu se află în proces de insolvabilitate*
12	DECLARAŢIE privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani	Declarație în conformitate cu **Anexa nr. 2** autentificată prin aplicarea semnăturii electronice a Participantului – depunere obligatorie după desemnare în calitate de ofertant/ofertant asociat desemnat câștigător;	***Da*** *– depunere obligatorie după desemnare în calitate de câștigător*

Anexa nr. 2

APROBAT
prin Ordinul
Ministrului Finanțelor
nr. 145 din 24 noiembrie 2020

DECLARAŢIE
privind confirmarea identității beneficiarilor efectivi și neîncadrarea acestora în situația condamnării pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.

Subsemnatul, _____ reprezentant împuternicit al _____ *(denumirea operatorului economic)* în calitate de ofertant/ofertant asociat desemnat câștigător în cadrul procedurii de achiziție publică nr. _____ din data __/__/___, declar pe propria răspundere, sub sancţiunile aplicabile faptei de fals în acte publice, că beneficiarul/beneficiarii efectivi ai operatorului economic în ultimii 5 ani nu au fost condamnați prin hotărâre judecătorească definitivă pentru participarea la activităţi ale unei organizaţii sau grupări criminale, pentru corupţie, fraudă şi/sau spălare de bani.

Numele și prenumele beneficiarului efectiv	IDNP al beneficiarului efectiv

Data completării: _____
Semnat: _____
Nume/prenume: _____
Funcţia: _____
Denumirea operatorului economic _____
IDNO al operatorului economic _____

17. Garanția pentru ofertă, nu se aplică;
18. Garanția de bună execuție a contractului, nu se aplică;
19. Motivul recurgerii la procedura accelerată (în cazul licitației deschise, restrânse și al procedurii negociate), după caz . *Nu se aplică*
20. Tehnici și instrumente specifice de atribuire (dacă este cazul specificați dacă se va utiliza acordul-cadru, sistemul dinamic de achiziție sau licitația electronică): licitația electronică, 3 runde , pasul minim pentru întreaga ofertă 3 800,00 lei.
21. Condiții speciale de care depinde îndeplinirea contractului (indicați după caz**) nu sunt.**
22. Ofertele se prezintă în valuta: - lei moldovenești.
23. Criteriul de evaluare aplicat pentru adjudecarea contractului: *Cel mai mic preț fără TVA pentru întreaga ofertă.*
24. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum și ponderile lor: *Nu se aplică*

Nr. d/o	Denumirea factorului de evaluare	Ponderea%
	Nu se aplică	

25. Termenul limită de depunere/deschidere a ofertelor:
Conform informației în SI "RSAP"
26. Adresa la care trebuie transmise ofertele sau cererile de participare:
Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SI RSAP.
27. Termenul de valabilitate a ofertelor: *60 zile*
28. Locul deschiderii ofertelor: *SI RSAP M-Tender.*
***Ofertele întârziate vor fi respinse*.**
29. Persoanele autorizate să asiste la deschiderea ofertelor:
Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SI RSAP.
30. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:
Limba de stat .
31. Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: *Nu se aplică*
32. 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
33. Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul): *Nu se aplică*
34. În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare: *Nu se aplică*
35. Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunț: *Nu se aplică*
36. Data transmiterii spre publicare a anunțului de participare:
Conform informației în SI RSAP.
37. 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	Se acceptă

participare	
sistemul de comenzi electronice	Nu se acceptă
facturarea electronică	Nu se acceptă
plățile electronice	Se acceptă

38. 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*

39. Alte informații relevante: _____

Președinta grupului de lucru: Digitally signed by Moraru Maia
Date: 2026.07.15 15:40:40 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Maia Moraru

L.Ș.