ROMÂNIA
MINISTERUL APĂRĂRII NAȚIONALE
COMANDAMENTUL APĂRĂRII CIBERNETICE
Anexa nr. 2 Nr. ZA-500 din 06.03.2026
București –

NECLASIFICAT
Exemplarul unic
Dosar nr. ___
Termen de păstrare: 5 ani

Specificația tehnică revizuită în urma consultării pieței pentru produsul
"Complet de monitorizare și protecție pentru aplicații de tip Web"

BUCUREȘTI
2026

CUPRINS

1. SCOP

Prezenta specificaţie stabileşte cerinţele tehnice pentru achiziţionarea unui *Complet de monitorizare şi protecţie pentru aplicaţii Web* ce are ca scop principal securizarea aplicaţiilor web prin monitorizarea, filtrarea şi blocarea traficului web.

2. CERINŢE

Ofertantul va furniza o soluţie de tip appliance, soluţie care trebuie să ofere protecţie împotriva atacurilor web precum cele definite în OWASP Top 10 şi nu numai, respectând totodată cerinţele definite mai jos.

2.1 Cerinţe privind configuraţia produsului ofertat

Nr. cerinţă	CERINŢA
C1.	Completul ofertat trebuie să fie compus dintr-o soluţie de tip „*Appliance*" dedicat care are instalat un software adecvat al aceluiaşi producător, care să permită toate funcţionalităţile descrise în acest document şi licenţe / subscripţii valabile pentru minim 5 ani.

2.2 Cerinţe de performanţă şi specifice produsului

Nr. cerinţă	CERINŢA
C1.	Soluţia trebuie să poată fi instalată în reţea în următoarele moduri: • Reverse proxy • Inline transparent • Proxy în mod transparent • Offline sniffing • Web Cache Communication Protocol (WCCP) client
C2.	Soluţia trebuie să aibă următoarea capacitate de procesare: • Trafic procesat în timp real HTTP : 10 Gbps • Trafic procesat în timp real HTTPS : 10 Gbps • Latenţă trafic: <5 ms • Trafic procesat în timp real: 10Gbps • Tranzacţii HTTP/Sec: minim 100.000 • Tranzacţii HTTPS/Sec: minim 100.000
C3.	Echipamentul hardware trebuie să poată fi instalat într-un rack de 19", să aibă înălţimea maximă de 2U şi să conţină minim următoarele componente: • Interfeţe de reţea 10G SFP+: 10, dintre care minim 2 cu posibilitate de tip hardware bypass; • Interfeţe de retea 10/100/1000 Ethernet RJ-45 cu posibilitate de tip hardware bypass: 8; • Interfeţe de reţea SFP GbE: 4; • Porturi USB: 2; • Capacitate de stocare: 2x 960 GB SSD.
C4.	Soluţia trebuie să aibă o sursă de alimentare redundantă de tip hot-swap.
C5.	Soluţia trebuie să poată funcţiona în următoarele condiţii: • Condiţii alimentare: 100–240 VAC, 60–50 Hz; • Putere medie consumată: 200 W; • Temperatura mediului de operare: 0 – 40 grade Celsius; • Umiditatea mediului de operare: 5 - 90% fără condens.

C6.	Soluția trebuie să aibă următoarele opțiuni pentru autentificarea utilizatorilor: • Operațiunea de autentificare a utilizatorilor trebuie să poată verifica credențialele prin verificare locală sau externă prin protocoalele RADIUS (inclusiv autentificare prin doi factori), LDAP și suport SAML; • Suport pentru Single Sign On a utilizatorilor pe aplicațiile Microsoft protejate (Outlook Web Access, Sharepoint); • Posibilitatea de autentificare activă sau pasivă; • Autentificare prin Single Sign-On (SSO); • Autentificare adițională a clienților prin certificate digitale X.509 (pentru aplicații HTTPS) – validare locală a certificatului (folosind un certificat importat al CA-ului semnatar) și posibilitate de trimitere a informațiilor legate de acesta către aplicația protejată; • Posibilitate de a verifica validitatea certificatelor digitale X.509 ale clienților prin verificarea de fișiere CRL (retrase prin HTTP, SCEP); • Posibilitate de a verifica validitatea certificatelor digitale X.509 ale clienților prin verificarea de CRL-uri prin protocolul HTTP; • Posibilitate de definire de domenii de administrare separate;
C7.	Soluția trebuie să protejeze aplicațiile web împotriva atacurilor de tip: Browser Exploits, Brute Force Login, Buffer Overflows, Command Injection, Cookie Tampering/Poisoning, Cross Site Request Forgery, Cross Site Scripting, Denial Of Service, Directory Traversal, Forms Tampering, Hidden Field Manipulation, HTTP Header overflow, Outbound Data Leakage, Local file Inclusion, Man in the Middle attacks, Remote File Inclusion, Session Hijacking, Site Reconnaissance, SQL Injection, XML Intrusion Prevention și a altor tipuri de atacuri specifice aplicațiilor și serverelor de tip web.
C8.	Soluția trebuie să ofere următoarele opțiuni de procesare a traficului: • Load balancing la nivel de aplicație prin algoritmii: round-robin, weighted round-robin, least connections, round-robin cu persistența sesiunii HTTP; • Rutare dupa conținut HTTP după combinație între cookie, URL accesat și headerul Host din cerere; • Health checking a serverelor aplicațiilor protejate prin protocoalele TCP, HTTP/HTTPS și ICMP pentru funcționalitatea load balancing; • SSL offloading pentru aplicațiile protejate ce folosesc protocolul HTTPS cu posibilitatea de configurare a nivelului de securitate SSL/TLS; • Suport pentru utilizarea Server Name Indication (SNI) în modul reverse proxy pentru SSL offloading; • Compresie și decompresie a traficului dintre client și aplicația protejată; • Caching pentru răspunsul serverelor de aplicație.
C9.	Soluția trebuie să aibă următoarele opțiuni de definire a politicilor și profilelor de securizare: • Definire în mod automat și dinamic a profilelor de securizare pentru aplicații în urma monitorizării traficului acestora; • Politici de securitate predefinite; • Opțiuni de partajare al accesului administrativ pentru configurația profilelor și politicilor de securizare pentru aplicațiile web protejate, prin utilizarea de domenii administrative; • Opțiune de creare sarcini de lucru pentru actualizarea politicilor de securitate și corectarea configurărilor folosind un asistent virtual bazat pe inteligență artificială.
C10.	Soluția trebuie să aibă suport pentru High Availability: • Clustering de tip Activ/Pasiv sau Activ/Activ; • Sincronizare de configurație între doua echipamente; • Posibilitatea de a funcționa ca și client WCCP.

C11.	Soluția trebuie să ofere următoarele opțiuni de protecție la nivel de aplicație: • Posibilitatea de a defini manual semnături de atac noi; • Blocare pe baza de reputație a surselor cu potențial malițios; • Protecție împotriva botnet, crawler, search engine; • Posibilitatea de a monitoriza și bloca traficul provenit dintr-o anumită regiune geografică sau țară; • Protecție împotriva scanării fișierelor de conținut malițios (scanare antivirus); • Protecție bazată pe modele ML cu scopul de a minimiza fals-pozitivele, identificarea și mangementul traficului, automatizare de descoperire API-uri, precum și detectare și blocare de atacuri „zero-day" • Protecție DoS pentru atacuri la nivel rețea și aplicație – limitare pentru numărul de cereri HTTP /secundă de la o singură sursa IP, limitare a numărului de conexiuni TCP concurente per adresa IP sursă ce folosesc același cookie HTTP, protecție pentru HTTP request flood făcut de o sursă IP pentru același URL, protecție împotriva cererilor HTTP generate de posibile scripturi (prin validarea browserului client), blocare a atacurilor de tip TCP SYN flood, limitare a numărului de conexiuni TCP concurente per adresa IP sursă; • Controlul accesului clienților de aplicație HTTP dupa blacklist-uri și whitelist-uri configurabile de adrese IP; • Suport pentru redirectarea cererilor HTTP și modificarea URL-ului și a headerelor Host si Referer din cereri; • Suport pentru modificarea răspunsurilor HTTP – headerul Location și întregul corp al răspunsului; • Posibilitatea de a impune clienților accesul într-o anumită ordine a paginilor aplicației HTTP protejate – cererile unui client ce nu respectă această ordine trebuie să poată fi blocate; • Protecție Anti Web Defacement – restaurarea conținutului original al unei aplicații web protejate în cazul modificării malițioase al acestuia; • Validarea compliantei RFC HTTP a traficului procesat; • Funcționalitate de scanare programabilă și raportare automată a vulnerabilităților aplicațiilor web protejate; • Control asupra parametrilor protocolului HTTP; • Posibiliatea de a include header pentru HTTP Strict Transport Security(HSTS) în răspunsul serverului de aplicație web către client; • Scanarea atașamentelor pentru aplicațiile ActiveSync/MAPI, OWA și FTP; • Suport pentru protocolul IPv6; • Alerte configurabile prin mesaje email, loguri Syslog; • Suport SNMP și WebSockets;
C12.	Soluția trebuie să fie conformă cu următoarele standarde: RCM, VCCI, CE, UL/CB/cUL.

2.3 Cerințe licențiere

Nr. cerință	CERINȚA
C13.	Licențele software trebuie să fie valabile pentru o perioadă de minim 60 de luni. În această perioadă, ofertantul trebuie să asigure accesul beneficiarului la toate actualizările software ale elementelor componente ale soluției.
C14.	Ofertantul trebuie să livreze și alte licențele necesare, respectiv pentru toate modulele și pachetele software adiționale, dacă este cazul, integrate sau nu, necesare pentru funcționarea soluției în acord cu cerințele din acest document.
C15.	Soluția nu trebuie să aibă licențiere pentru numărul aplicațiilor protejate.

C16.	După ieşirea din garanţie echipamentul trebuie sa functioneze. să permită atât administrarea cât şi fluxurile de date. chiar dacă semnăturile nu mai sunt actualizate la zi.

2.4 Cerinţe privind garanţia produsului

Nr. cerinţă	CERINŢA
C17.	Garanţia generală trebuie să fie de minim 60 luni pentru produsul ofertat, fără costuri suplimentare.
C18.	Nu se acceptă condiţionarea acordării garanţiei produsului de acordarea accesului ofertantului la produsul instalat în reţele private ale beneficiarului.
C19.	În cazul defectării în perioada de garanţie a unui mediu de stocare. ofertantul trebuie să îl înlocuiască fără a solicita beneficiarului restituirea celui defect. MApN rezervându-şi dreptul de a-l distruge în cazul în care consideră că este necesar.
C20.	Solutia va beneficia de minim 5 ani de suport ce va include: • Înlocuirea echipamentului în caz de defecţiune hardware: • Update firmware versiuni minore şi majore: • Update-uri automate de semnături de securitate pentru îndeplinirea tuturor funcţionalitatilor cerute mai sus.

2.5 Cerinţe privind recepţia produsului

Nr. cerinţă	CERINŢA
C21.	Recepţia produsului se va desfăşura în acord cu prevederilor contractuale şi va conţine o recepţie calitativă şi o recepţie cantitativă.
C22.	Recepţia cantitativă şi calitativă se va realiza la sediul beneficiarului. de către comisia de recepţie a acestuia.
C23.	Recepţia cantitativă şi calitativă se va realiza în termen de 10 zile de la data finalizării livrării produselor.
C24.	În cadrul activităţii de recepţie se vor parcurge următoarele etape: a) verificarea livrării cantitative a produsului: b) verificarea livrării documentelor prevăzute la pct. 4 din Caietul de sarcini: c) verificarea funcţionării produsului în acord cu prevederile cerinţelor tehnice prevăzute în anexa nr. 1 la caietul de sarcini. de către o comisie de recepţie formată din angajaţi ai beneficiarului.
C25.	La finalul activităţii de recepţie se va întocmi un proces verbal de recepţie cantitativă şi calitativă a activului fix. prin care se va finaliza activitatea de recepţie.
C26.	Dacă în cadrul recepţiei se constată că unele produse nu corespund cantitativ şi calitativ. beneficiarul are dreptul de a respinge produsele. iar Furnizorul are obligaţia să remedieze neconformităţile constatate în decurs de 5 (cinci) zile de la constatarea lor.
C27.	La finalul activităţii de recepţie se va întocmi un proces verbal de recepţie cantitativă şi calitativă a activului fix. prin care se va finaliza activitatea de recepţie.
C28.	Dacă în urma exploatării produsului. în termen de 90 de zile de la efectuarea recepţiei se constată că apar deficienţe care nu au putut fi descoperite la recepţie şi prin care nu sunt respectate cerinţele din caietul de sarcini. achizitorul poate solicita remedierea sau înlocuirea produsului. cu suportarea tuturor cheltuielilor de către ofertant.

2.6 Cerințe privind condițiile de livrare

Nr. cerință	CERINȚA
C29.	Termenul de livrare trebuie să fie de maxim 45 de zile de la data semnării contractului subsecvent de ambele părți. Termenul de livrare nu include timpul necesar desfășurării activității de recepție a produsului.
C30.	Livrarea produsului ofertat trebuie să se realizeze la sediul beneficiarului din str. Drumul Taberei 7-9, Sectoi 6, București.
C31.	La livrare, produsul trebuie însoțit de declarații de conformitate
C32.	La livrare, produsul trebuie etichetat de către furnizor clar și vizibil astfel încât acestea să poată fi identificate cu ușurință. Furnizorul are dreptul de a inscripționa suplimentar coletele livrate, pentru a asigura informațiile pe care le consideră necesar a fi cunoscute pe timpul transportului, depozitării și manipulării acestora.
C33.	Etichetele de marcare trebuie să conțină toate informațiile obligatorii prevăzute de reglementările în vigoare.
C34.	Etichetele de marcare trebuie să reziste la acțiunea intemperiilor și să nu permită deteriorarea accidentală pe timpul manipulării, transportului sau depozitării.
C35.	La livrare, produsul trebuie să fie ambalat astfel încât să permită depozitarea și transportul acestora în condiții de siguranță în spații închise. Toate materialele de ambalare, precum și toate materialele necesare protecției coletelor (folii de protecție, cutii etc.) rămân în proprietatea achizitorului.
C36.	Documentația de însoțire trebuie să cuprindă: • inventarul cantitativ-valoric, în limba română, care trebuie să coincidă cu prețul unitar al produsului ofertat cu TVA; • certificatul de conformitate emis de organul de calitate abilitat al ofertantului; • certificatul/certificatele de garanție; • documentația de exploatare, cunoaștere și întreținere, în format electronic; • documentele reprezentând licențele produselor software, în format electronic și tipărit, din care să reiasă obligatoriu perioada de valabilitate.

2.7 Alte cerințe

Nr. cerință	CERINȚA
C37.	Tehnica oferită trebuie să fie nouă, nefolosită și să încorporeze toate îmbunătățirile recente din documentația tehnică și de fabricație.
C38.	Tehnica propusă nu trebuie să includă produse EoL (*End of Life*) și/sau EoS (*End of Sale*) la data depunerii ofertei.
C39.	Specificațiile tehnice și de calitate ale produsului oferit trebuie, obligatoriu, susținute de documentații originale: prospecte, foi de catalog sau medii de stocare cu documentații în format electronic.
C40.	Ofertantul trebuie să precizeze detaliat în oferta tehnică modul de îndeplinire concretă a cerințelor tehnice hardware și software pentru toate componentele, indicând pagina și paragraful din documentația oficială detaliată a produsului emis de producătorul acestuia, unde se găsesc informațiile legate de îndeplinirea cerinței respective. Nu sunt luate în considerare ofertele care prezintă simpla confirmare a îndeplinirii cerinței, sau numai copierea acesteia, fără a fi detaliată modalitatea de îndeplinire.

Toate cerinţele definite în cadrul prezentei specificaţii tehnice sunt obligatorii. Nerespectarea lor va conduce la respingerea ofertei.