Anexa nr.1
la Caietul de sarcini

Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7,
iar de către BNM – în coloanele 1, 5,]

Numărul procedurii de achiziţie nr. ocds-b3wdp1-MD-1654178592543 din 19 iunie 2022
Obiectul achiziţiei: **Soluții de securitate antispam, WAF și proxy**

Denumirea bunurilor	**Denumirea modelului**	**Ţara de origine**	**Producă-torul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5	6	7
Lot 1: Soluția antispam pentru email						
Soluție antispam pentru email	FC-10-0VM02-643-02-12; FWB-VM02	SUA	FortiNet	<u>Tip:</u> Soluție antispam pentru email, inclusiv 12 luni de suport și subscriere de la producător. <u>Cantitatea și cerințe de licențiere:</u> - Este responsabilitatea Ofertantului de a determina modelul de licențiere și cantitatea licențelor. - Toate licențele livrate vor include prețul pentru 12 luni de suport și subscriere furnizat de producătorul licențelor, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licențelor până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor).	FortiMail VM02; 1 an 24x7 Enterprise ATP Bundle FortiMail VM02 *Corespundere totala cu cerințele din caiet de sarcini. Vezi fisa tehnică atașată FortiMail pdf.*	n/a

Denumirea bunurilor	Denumirea modelului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				Cerințe tehnice: Soluția propusă trebuie sa fie o soluție inovatoare, care va asigura următoarele cerințe minime: 1. Cerințe pentru securitatea datelor corporative: • Filtru de SPAM și viruși; • Protecție spoofing, fishing și malware; • DoS protectie; • Filtru costumizabil mesaje de intrare/ieșire; • Recepționarea emailuri prin protocoalele SMTP, IMAP și POP; • Mecanism de partajare a informației (atașamentului sau /și conținutului email-ului) în mod protejat/criptat cu părți terțe prin intermediul unui URL către un portal specializat, pe care destinatarul de email se va putea autentifica/înregistra pentru a accesa email-ul securizat. 2. Cerințe pentru Managementul politicilor: • Filtrare după adrese IP și conținut; • Rutare email pe bază de politici; • Criptare conținut; • DNS Reverse blocare;		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă -torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				• Server to server TLS encryption cu control granular al suitei de criptare și aplicare opțională, inclusiv posibilitatea setării Implicit/Explicit TLS; • Blocare după character-set; • Filtrare după expeditor/destinatar; • Blocare URL pattern; • Suport RBL si DNSBL; • Textul pentru etichetarea mesajelor trebuie să fie configurabil. 3. <u>Cerințe pentru protecție viruși și SPAM:</u> • Analiză reputație IP; • SPF și DomKey verificare; • Algoritmi de scor Rules-based; • Despachetare arhive din atașamente; • Filtru după tipul de fișiere; • Toate mesajele și atașamentele primite trebuie scanate cu modulul antivirus; • Blocare sau plasare în carantină a mesajelor după categoria de atașamente; trebuie recunoscute cel puțin următoarele categorii: documente MS-Office, documente PDF, fișiere executabile, fișiere multimedia, scripturi Windows;		

Denumirea bunurilor	Denumirea modelului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				• Blocare mesaje sau carantină cu atașamente care conțin cuvinte cheie sau modele de text specifice. 4. <u>Cerințe pentru prevenirea scurgerilor de date și reputație:</u> • Prevenirea de pierdere de reputație și blacklisting; • Posibilitatea de a bloca, a pune în carantină sau a eticheta mesajele pentru anumite adrese de e-mail sau domenii ale destinatarului; • Blocare mesajele sau carantină după numele atașamentului sau modelul de nume; • Blocare sau plasare în carantină a mesajelor după tipul MIME de atașament. 5. <u>Cerințe End Users:</u> • Filtru User-based; • Suport pentru Block/White liste la nivel global, domen și utilizator. 6. <u>Cerințe de administrare a soluției:</u> • Interfața de administrare Web; • Posibilitatea de administrare a utilizatorilor; • Existența unui instrument de raportare complex, customizabil cu grafice și statistică; • Integrare LDAP;		

Denumirea bunurilor	Denumirea modelului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				• Suport pentru mai multe nume de domen; • Crearea conturilor cu rol de suport utilizatori și de administrator; • Performanță de procesare și capacitate inclusă (gratuită); • Statistica mesajelor într-o anumită perioadă de timp; • Integrare SNMP; • Integrare SIEM; • Integrare Office 365. 7. <u>Cerințe tehnice și de instalare a soluției:</u> • Suport la configurația High Availability; • Virtual appliance de tip on-premise; • Suport multiplatformă de virtualizare (VMware 7, Citrix XEN 8.x); • Logare a modificărilor configurației. 8. <u>Cerințe minime pentru perioada de suport și subscriere oferite de producător:</u> • 12 luni din data acceptanței soluției; • suport prin e-mail sau conectare de la distanță; • protecție avansată a amendărilor de securitate;		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				• actualizarea nomenclatoarelor SPAM și BD reputațiunile; • actualizarea la oră a sistemului antivirus și antimalware. Notă: După deschiderea ofertelor, pentru verificarea corespunderii soluției ofertate cu cerințele înaintate, la solicitare Ofertantul va pune la dispoziția Autorității contractante în decurs de 3 zile lucrătoare pentru testare versiunea trial a soluției ofertate. Alte cerințe obligatorii: Costul ofertei trebuie să includă activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției, precum și transferul de cunoștințe către administratorii Cumpărătorului, executate de Ofertant (Furnizor).		
Lot 2: Soluție virtuală de tip Web Application Firewall						
Soluție virtuală de tip Web Application Firewall	FWB-VM02; FC-10-VVM02-603-02-12	SUA	FortiNet	Tip: Soluție virtuală de tip Web Application Firewall, inclusiv 12 luni de suport și subscriere de la producător. Cerințe de licențiere: - Este responsabilitatea Ofertantului de a determina modelul de licențiere și cantitatea licențelor; - Modelul de licențiere propus trebuie să acopere 2 instanțe;	FortiWeb VM02; 1 an Advanced Bundle (24x7 FortiCare plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, and Credential	n/a

Denumirea bunurilor	Denumirea modelului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- Soluția livrată va include prețul pentru 12 luni de suport și subscriere de la producătorul soluției, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licenței până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). **<u>Cerințe generale:</u>** • Soluția trebuie să fie propusă ca un Appliance Virtual, compatibilă cu platformele virtuale VMware vSphere 7.0 și Citrix 8.1; • Soluția trebuie să fie în configurația de High-Availability (Active-Active); • Soluția trebuie să asigure minim o performanță de procesare (HTTP) de 100 Mbps; • Modelul de licențiere nu trebuie să limiteze numărul de aplicații protejate. • **<u>Cerințe față de funcționalitatea Application Delivery:</u>** - URL Rewriting; - HTTPS/SSL Offloading; - HTTP Compresion; - Caching; - Layer 7 load balancing. • **<u>Cerințe față de protecția Aplicațiilor:</u>**	Stuffing Defense Service) FortiWeb VM02 Pentru solutia data sunt ofertate cate 2 licente in conformitate cu cerintele din CS. Corespundere totala cu cerințele din caiet de sarcini. Vezi fisa tehnica atașată FortiWeb pdf.	

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- Cross Site Scripting; - Bot based; - DoS; - SQL Injection; - Session Hijacking; - Protecție împotriva OWASP top 10 atacuri; - Scanare fișiere (AV și sandbox). • **<u>Cerințe față de serviciile de Securitate:</u>** - Detecție malware; - Protecție brute-force; - Prevenție DoS; - Protecție XML și JSON REST API; - Mecanisme de protecție bazate pe Machine Learning; - Protecție împotriva scurgerii datelor; - L4 Stateful Network Firewall; - HTTP Header Security; - Known threat and zero-day attack protection; - Data leak prevention; - Web Defacement Protection; - Geo-IP și IP Reputation. • **<u>Cerințe față de mecanimsele de autentificare:</u>** - Suportul protocoalelor de autentificare SAML, LDAP, RADIUS;		

Denumirea bunurilor	Denumirea modelului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- Autentificarea pe bază de certificat; - Suport 2-factor authentification. • **<u>Cerințe față de Administrare și Raportare:</u>** - Interfață web de administrare; - Dashbord-uri informaționale; - Rapoarte și log-uri centralizate; - Syslog, snmp, email notificări; - Crearea conturilor de administrare pe bază de roluri; <u>Cerințe minime pentru perioada de suport și subscriere de la producător:</u> • 12 luni din data acceptanței soluției; • suport prin e-mail sau conectare de la distanță de la producător. <u>Notă:</u> După deschiderea ofertelor, pentru verificarea corespunderii soluției ofertate cu cerințele înaintate, la solicitare Ofertantul va pune la dispoziția Autorității contractante în decurs de 3 zile lucrătoare pentru testare versiunea trial a soluției ofertate. <u>Alte cerințe obligatorii:</u> Costul ofertei trebuie să includă activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				soluției, precum și transferul de cunoștințe către administratorii Cumpărătorului, executate de Ofertant (Furnizor).		
Lot 3: Soluție de protecţie a accesului la rețeaua Internet						
Soluție de protecţie a accesului la rețeaua Internet	LIC-FPRXY-VM02; FC1-10-XYVM2-515-02-12; FC1-10-XYVM2-160-02-12	SUA	FortiNet	Tip: Soluție de protecţie a accesului la rețeaua Internet - Internet Gateway (proxy), inclusiv 12 luni de suport și subscriere de la producător. Cerințe de licențiere: • Modelul de licențiere propus trebuie să acopere 400 utilizatori, inclusiv 1 instanță; • Soluția livrată va include prețul pentru 12 luni de suport și subscriere de la producătorul soluției, care va începe de la data acceptanței soluției, după instalare și testare a funcționalităților. În cazul activării licenței până la data acceptanței soluției, toate costurile de licențiere de la producător în perioada de până la acceptanță vor fi suportate de către Ofertant (Furnizor). Caracteristici tehnice și de compatibilitate cu infrastructura BNM: • Soluția trebuie să se poată instala în infrastructură în următoarele moduri:	FortiProxy VM02 virtual appliance designed for all supported platforms. 4x vCPU core, Unlimited RAM and 2TB Disk; SWG Protection including 24x7 FortiCare Support - Web & Video Filtering, DNS Filtering, Application Control, DLP, IPS, AV, Botnet (IP/Domain), Sandbox Cloud including Virus Outbreak and Content Disarm & Reconstruct. 100 User license with SWG Protection	n/a

Denumirea bunurilor	Denumirea modelului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				Transparent/WCCP Proxy, Explicit Proxy, Routed Proxy; • Suport la configurația High Availability; • Virtual appliance de tip on-premise; • Suport multiplatformă de virtualizare (VMware 7, Citrix XEN 8.x); • Soluția trebuie să poată acționa ca proxy explicit pentru următorul tip de trafic: HTTP și HTTPS, FTP și FTPS; • Soluția trebuie să permită următoarele moduri de autentificare: NTLM, RADIUS, Active Directory, LDAP, Kerberos, Local user accounts (utilizatori stocați în baza de date a proxy-ului), • Soluția trebuie să ofere un serviciu de găzduire web unde se poate găzdui scriptul de configurare proxy de tipul .pac; • Soluția trebuie să permită pe viitor posibilitatea de configurare în mod cluster a 2 instanțe cu disponibilitate ridicată și distribuire de sarcină automată între noduri (HA available as active-active and active-backup with session synchronization); • Soluția trebuie să fie capabilă să-și sincronizeze ceasul intern prin NTP;	FortiProxy VM02 4 licente a cate 100 utilizatori conform cerintelor; Content Analysis Service. 100 User license FortiProxy VM02, 4 licente cate 100 utilizatori conform cerintelor; Corespundere totala cu cerințele din caiet de sarcini. Vezi fisa tehnica atașată FortiProxy pdf.	

Denumirea bunurilor	Denumirea modelului	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				• Soluția trebuie să utilizeze DNS caching pentru a reduce încărcarea pe serverele de DNS; • Soluția trebuie să permită segregarea rolurilor pentru raportare, configurare, administrare politici și reguli; • Soluția trebuie să permită restricționarea accesului administrativ la o singură interfață de rețea; • Soluția trebuie să auditeze acțiunile administratorilor, păstrând cel puțin următoarele informații: • Timpul la care s-a produs modificarea • Cine a produs modificarea • Ce acțiune a fost luată • Pe ce obiect a fost luată acțiunea • Noua valoare a obiectului modificat; • Soluția trebuie să permită împingerea evenimentelor de audit automat pe o soluție SIEM; • Soluția trebuie să permită configurarea unei sarcini automate ce transferă backup-ul configurației pe un alt server; • Soluția trebuie să permite instalarea în mediu virtual. **<u>Cerințe Antimalware:</u>** • Soluția trebuie să folosească motoare de scanare antivirus;		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				• Soluția trebuie să folosească euristice în identificarea și blocarea conținutului malițios de următoarele tipuri: Fișiere executabile, JavaScript, Flash ActionScript, Java Applets, ActiveX, Windows DDL, Scripturi Visual Basic; • Integrare cu Sandbox Cloud (inclus în subscriere); • Soluția trebuie să-și facă update pentru motoarele de scanare antivirus cel puțin o dată pe zi; • Soluția trebuie să ofere protecție și împotriva atacurilor de tip Zero-Day; • Soluția trebuie să dețină un mecanism pentru protecția de scurgeri de date (DLP – Data Leak prevention) bazat pe filtre, care să permită blocarea sau jurnalizarea scurgerii informației sensibile după cuvinte cheie. • Soluția trebuie includă protecție IPS (Intrusion Prevention System) bazat pe semnături ale vulnerabilităților și exploite-urilor cunoscute. De asemenea trebuie să includă protecție la SQL injection, domain generation algorithm attacks, java and flash exploits. • Soluția trebuie să identifice și să blocheze transmisii după comportament:		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				- Furt de date: keylogger, backdoor, spyware - Compromitere sistem: exploatare vulnerabilități browser, execuție de cod prin exploatare vulnerabilități, software de tip troian - Activitate ascunsă: Rootkit, injectare de cod - Replicare virală: vierme de rețea, virus ce infectează fișiere - Amenințări web: corss site scripting, ActiveX vulnerabil • Scanarea antivirus trebuie să se facă prin captive portal și data trickling; • Soluția trebuie să își actualizeze automat semnăturile antivirus cel puțin zilnic. **<u>Cerințe față de filtrarea site-urilor:</u>** • Soluția trebuie să permită blocarea site-urilor web după: • Categorie de site (Ex: Social Networking, Streaming Media, etc.); • Categorie de risc (Ex: High Risk, Medium Risk,etc.); • Listă statică cu nume de site-uri web; • Listă statică cu IP-uri la care sunt găzduite site-uri; • Soluția trebuie să permită activarea acțiunii de coaching în locul blocării pentru a avertiza utilizatorii despre		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă -torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				riscul la care se supun dacă doresc să continue la site-ul dorit; • Soluția trebuie să permită suprascrierea locală a clasificării unui site din baza de date furnizată de producător. (Ex: Un site considerat de Social Networking să poată fi clasificat local de Business); • Soluția trebuie să permite copierea politicilor și regulilor pentru a ușura procesul de configurare; • Soluția trebuie să permită modificarea paginilor de notificare prezentate utilizatorilor; • Soluția trebuie să permită blocarea site-urilor după țara în care acestea sunt găzduite; • Soluția trebuie să verifice validitatea certificatelor SSL în cazul site-urilor securizate; • Soluția trebuie să ofere capabilități de inspecție a traficului SSL (man in the middle). **<u>Cerințe față de Control de aplicații:</u>** • Soluția trebuie să permită blocarea de aplicații ce sunt tunelate prin proxy; • Soluția trebuie să vină cu o bază de date de aplicații furnizată de producător și actualizată de acesta cel puțin o dată pe lună;		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă -torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				• Soluția trebuie să vină cu o bază de date de aplicații ce le împarte în categorii și nivel de risc. **<u>Cerințe față de control de conținut:</u>** • Soluția trebuie sa permită analiza real-time a conținutului grafic pentru a detecta conținut grafic malițios în cadrul paginilor-web (Content Analysis Service). **<u>Cerințe față de raportare:</u>** • Soluția trebuie să raporteze statistici despre: Trafic Instant Messaging, Trafic Web, Malware, Tipuri de fișiere, Certificatele digitale verificate, URL Filtering, Web Cache, Trafic pe internet/utilizator, Aplicații web folosite; • Rapoartele trebuie să poată fi exportate în cel puțin următorul format: PDF; • Rapoartele trebuie să poată fi automat transmise pe/prin e-mail; • Soluția trebuie să ofere statistici de performanță ale sistemului: CPU, Memorie, Lățime de bandă, Cereri/secundă, etc; • Soluția trebuie să permită investigarea logurilor de acces la internet.		

Denumirea bunurilor	Denumirea modelului	Ţara de origine	Producă -torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
				Cerințe minime pentru perioada de suport și subscriere de la producător: • 12 luni din data acceptanței soluției; • suport prin e-mail sau conectare de la distanță de la producător. Notă: După deschiderea ofertelor, pentru verificarea corespunderii soluției ofertate cu cerințele înaintate, la solicitare Ofertantul va pune la dispoziția Autorității contractante în decurs de 3 zile lucrătoare pentru testare versiunea trial a soluției ofertate. Alte cerințe obligatorii: În costul ofertei trebuie să fie incluse activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției, precum și transferul de cunoștințe către administratorii Cumpărătorului.		

Cu stimă,
Ofertant/candidat„S&T MOLD" S.R.L.
Chief Commercial Officer Andrei Cojocari
Data completării 16.06.2022

Semăntura autorizată _____

Digitally signed by Cojocari Andrei
Date: 2022.06.16 17:00:10 EEST
Reason: MoldSign Signature
Location: Moldova