Anexa nr. 22
la Documentația standard nr._____
din "____" _____ 20___

Specificaţii tehnice

Numărul procedurii de achiziție ocds-b3wdp1-MD-1755590637678 din 19.08.2025
Obiectul achiziției: Echipament IT (Sistem de securitate).

Denumirea bunurilor/serviciilor		**Denumirea modelului bunului/ serviciului**	**Țara de origine**	**Produ-cătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referință**
1		2	3	4	5	6	7
Lot Echipament IT (Sistem de securitate).							
1.1 Next Generation Firewall (NGFW)	Cluster of 2x Next Generation Firewall (NGFW)	FortiGate-200G cu FortiGuard Enterprise Protection și FortiAnalyzer-VM	SUA TAIWAN	Fortinet, Inc	Cluster of 2x Next Generation Firewall (NGFW). Descrierea conform anexei	**Cluster de 2 noduri Next Generation Firewall (NGFW) include:** **- 2x FG-200G-BDL-809-36** FortiGate-200G Hardware plus 3 Year FortiCare Premium and FortiGuard Enterprise Protection **- 1x FAZ-VM-GB5** FortiAnalyzer-VM Upgrade license for adding 5 GB/Day of Logs. **- 1x FC2-10-LV0VM-248-02-36** FortiAnalyzer-VM FortiCare Premium Support 3 Year FortiCare Premium Support **- 8x SP-CABLE-ADASFP+** 10 GE SFP+ active direct attach cable, 10m **- 8x FN-TRAN-SFP+SR** 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm - **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Perioada de garanție și suport tehnic direct din partea producătorului:** 36 de luni - **Perioada a subscripțiilor:** 36 de luni	
1.2 Licente Sofware incluse aferente NGFW solicitat la p. 1.1	Licente Sofware incluse aferente NGFW solicitat la p. 1.1						

						- **Perioada de suport tehnic local din partea ofertantului:** 12 luni Specificarea tehnică deplină propusă , este prezentată în Tabelul №1 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.) Codurile produselor ale producătorului sunt prezentate in Tabelul №2 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.)	
2.1. Web Application Firewall (WAF) 2.2 Licente Sofware incluse aferente soluției Web Application Firewall (WAF) la p. 2.1	Soluție de tip Web Application Firewall (WAF) Licente Sofware incluse aferente soluției Web Application Firewall (WAF) la p. 2.1	FortiWeb Web Application Firewall cu AV, FortiWeb Security Service, IP Reputation, Credential Stuffing Defense Service și Threat Analytics	SUA	Fortinet, Inc	Soluție de tip Web Application Firewall (WAF). Descrierea conform anexei	- **1x FWB-VM02** FortiWeb-VM02 Web Application Firewall - virtual appliance, supports up to 2 x vCPU core - **1x FC-10-VVM02-581-02-36** FortiWeb-VM02 3 Year Advanced Bundle - Standard Bundle plus Credential Stuffing Defense Service and Threat Analytics - **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Perioada de garanție și suport tehnic direct din partea producătorului:** 36 de luni - **Perioada a subscripțiilor:** 36 de luni - **Perioada de suport tehnic local din partea ofertantului:** 12 luni Specificarea tehnică deplină propusă , este prezentată în Tabelul №1 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.) Codurile produselor ale producătorului sunt prezentate in Tabelul №2 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.)	
3.1 Soluție Mail Security Gateway 3.2 Licente Sofware incluse aferente soluției Mail Security Gateway la p. 3.1	Soluție Mail Security Gateway Licente Sofware incluse aferente soluției Mail Security Gateway la p. 3.1	FortiMail-VM virtual appliance cu FortiGuard Enterprise ATP Bundle	SUA	Fortinet, Inc	Soluție Mail Security Gateway Descrierea conform anexei	- **1x FML-VM02** FortiMail-VM02 FortiMail-VM virtual appliance, 2 x vCPU cores - **1x FC-10-0VM02-643-02-36** FortiMail-VM02 3 Year FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă;	

						- Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Perioada de garanție și suport tehnic direct din partea producătorului:** 36 de luni - **Perioada a subscripțiilor:** 36 de luni - **Perioada de suport tehnic local din partea ofertantului:** 12 luni Specificarea tehnică deplină propusă , este prezentată în Tabelul №1 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.) Codurile produselor ale producătorului sunt prezentate in Tabelul №2 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.)	
4.1 Soluție Zero Trust Network Access (ZTNA)	Soluție Zero Trust Network Access (ZTNA), min. 200 stații de lucru	FortiClient EPP/ATP Subscription pentru 200 endpoints, include VPN/ZTNA Agent, EPP/ATP on-prem EMS cu FortiCare Premium.	SUA	Fortinet, Inc	Soluție Zero Trust Network Access (ZTNA), min. 200 stații de lucru Descrierea conform anexei	- **8x FC1-10-EMS04-429-01-36** Endpoint-based Licenses - EPP/ATP (On Premise Deployments) 3 Year FortiClient EPP/ATP Subscription for 25 endpoints, Includes VPN/ZTNA Agent, EPP/ATP on-prem EMS with FortiCare Premium. **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Perioada de garanție și suport tehnic direct din partea producătorului:** 36 de luni - **Perioada a subscripțiilor:** 36 de luni - **Perioada de suport tehnic local din partea ofertantului:** 12 luni Specificarea tehnică deplină propusă , este prezentată în Tabelul №1 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.) Codurile produselor ale producătorului sunt prezentate in Tabelul №2 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.)	
4.2 Licente Sofware incluse aferente soluției Zero Trust Network Access (ZTNA) la p. 4.1	Licente Sofware incluse aferente soluției Zero Trust Network Access (ZTNA) la p. 4.1						
5.1 Soluție de gestiune a autorizării în rețeaua securizată	Soluție de gestiune a autorizării în rețeaua securizată. min 200 de utilizatori	FortiAuthenticator - VM Base License și FortiTokenMobile (Electronic License), suportă 200 utilizatori	SUA	Fortinet, Inc	Soluție de gestiune a autorizării în rețeaua securizată. min 200 de utilizatori. Descrierea conform anexei	- **1x FAC-VM-BASE** FortiAuthenticator - VM License VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine	
5.2 Licente Sofware incluse aferente soluției de gestiune a	Licente Sofware incluse aferente soluției de gestiune a autorizării						

autorizării în rețeaua securizată la p. 5.1	în rețeaua securizată la p. 5.1					(KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms - **1x FAC-VM-100-UG** FortiAuthenticator - VM License FortiAuthenticator-VM 100 users license upgrade - **1x FC1-10-0ACVM-248-02-36** FortiAuthenticator - VM License 3 Year FortiCare Premium Support (1 - 500 USERS) - **1x FTM-ELIC-200** FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 200 users. Electronic license certificate. License transfer between devices is not allowed. **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Perioada de garanție și suport tehnic direct din partea producătorului:** 36 de luni - **Perioada a subscripțiilor:** 36 de luni - **Perioada de suport tehnic local din partea ofertantului:** 12 luni Specificarea tehnică deplină propusă , este prezentată în Tabelul №1 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.) Codurile produselor ale producătorului sunt prezentate in Tabelul №2 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.)	
6.1 Soluție de Sandboxing	Soluție de Sandboxing	FortiSandbox VM00 Sandboxing Virtual Appliance cu Sandbox Threat Intelligence; Real-time Zero-Day Anti-Phishing Service	SUA	Fortinet, Inc	Soluție de Sandboxing Descrierea conform anexei	- **1x FSA-VM00** FortiSandbox VM00 Sandboxing Virtual Appliance. Available Universal VM expansion supports up to max 8 local and 200 cloud, with a total count not exceeding 200. No Universal VM count and Microsoft licenses included. - **3x FC-10-FSV00-500-02-12** FortiSandbox VM00 1 Year Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs. - **3x FC-10-FSV00-682-02-12** FortiSandbox VM00 1 Year Real-time Zero-Day Anti-Phishing Service - **3x FC-10-FSV00-248-02-12** FortiSandbox VM00 1 Year FortiCare Premium Support	
6.2. Licente Sofware incluse aferente soluției de Sandboxing	Licente Sofware incluse aferente soluției de Sandboxing						

						- **5x FSA-UPG-VM-WIN11-1** FortiSandbox Windows Licenses Expands FSA license of Windows 11 for FSA VM Appliance. Allows 1 VM clone on Local (including Custom) and Cloud. - **1x FSA-UPG-OFFICE2021-1** FortiSandbox Office Licenses Expands FSA (Appliance/VM) licenses of Microsoft Office 2021 by 1. **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - **Perioada de garanție și suport tehnic direct din partea producătorului:** 36 de luni - **Perioada a subscripțiilor:** 36 de luni - **Perioada de suport tehnic local din partea ofertantului:** 12 luni Specificarea tehnică deplină propusă , este prezentată în Tabelul №1 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.) Codurile produselor ale producătorului sunt prezentate in Tabelul №2 (Anexa nr. 1 la Anexa nr. 22 – Specificații tehnice.)	
TOTAL							

Semnat: Digitally signed by Cioban Alexei
Date: 2025.09.13 22:24:42 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Numele, Prenumele: Cioban Alexei

În calitate de: Director

Ofertantul: IT-LAB GRUP SRL

Adresa: mun. Chisinau; str-la Studentilor 2/4

Anexa nr. 1
la Anexa nr. 22 – Specificații tehnice

Tabel №1. Specificarea tehnică

Nr de ordine confrom anexei de specificatie	Specificarea tehnică deplină solicitată de către autoritatea contractantă		Specificarea tehnică deplină propusă de către ofertant
1.3. 1.3.1	**Soluție de tip Next Generation Firewall (NGFW)** **Cluster of 2x Next Generation Firewall (NGFW)**		**Soluție de tip Next Generation Firewall (NGFW)** **Cluster of 2 nodes FortiGate-200G cu FortiGuard Enterprise Protection si FortiAnalyzer-VM**
1.3.2.	Cerințe generale	Echipamentul furnizat în cadrul achiziției trebuie să fie nou, de înaltă calitate, fabricat de producători de renume, recunoscuți pe plan internațional în industria IT. Configurația acestuia trebuie să includă componente compatibile între ele, garantând funcționarea optimă și integrată a sistemului.	Echipamentul oferit în cadrul achiziției este nou, de înaltă calitate, fabricat de producător de renume (Fortinet), recunoscut pe plan internațional în industria IT. Configurația include componente compatibile între ele, garantând funcționarea optimă și integrată a sistemului
1.3.3	Performanță	- Threat protection Throughput (Full Protection): min. 6 Gbps - Max concurrent sessions: min. 1 M - New sessions per second: min. 140 000	Specificarea tehnică per node: - Threat protection Throughput (Full Protection): 6 Gbps - Max concurrent sessions: 11 M - New sessions per second: 400 000
1.3.4	Interfețe/Porturi	- min. 1 x Console Port - min. 1 x Port GE RJ45 MGMT dedicat - min. 1 x Port GE RJ45 HA dedicat - min. 8 x Porturi GE RJ45 - min. 8 x Porturi 10GE/GE SFP+/SFP	Specificarea tehnică per node: - 1 x Console Port - 1 x Port GE RJ45 MGMT dedicat - 1 x Port GE RJ45 HA dedicat - 8 x Porturi GE RJ45 - 8 x 5/2.5/GE RJ45 Ports - 4x GE SFP - 8 x Porturi 10GE/GE SFP+/SFP
1.3.5	Transceivers	- min. 4 x transceivere 10GBASE-SR SFP+, compatibile IEEE 802.3ae, distanță operare min. 100 m pe fibră multimode OM3/OM4, conector LC duplex; - min. 2 x AOC SFP+ active, lungime 1 m; - min. 2 x AOC SFP+ active, lungime 3 m; - Toate modulele și cablurile să fie noi, originale, testate din fabrică și certificate pentru compatibilitate cu echipamentele furnizate.	Specificarea tehnică per node: - 4 x FN-TRAN-SFP+SR 10 GE SFP+ transceiver module, short range 300m, LC connector, compatibile IEEE 802.3ae, fibră multimode OM3/OM4, 850nm, conector LC duplex; - 4 x SP-CABLE-ADASFP+ 10 GE SFP+ active direct attach cable, 10m - Toate modulele și cablurile sunt noi, originale, testate din fabrică și certificate pentru compatibilitate cu echipamentele furnizate.
1.3.6	High Availability Configurations	- Active-Active, Active-Passive, Clustering	Specificarea tehnică per node: - Active-Active, Active-Passive, Clustering
1.3.7	Routing protocols	- Static, OSPFv2/3, BGPv4	Specificarea tehnică per node: - Static, OSPFv2/3, BGPv4
1.3.8	VLAN Support (802.1Q)	- 4094 VLANs	Specificarea tehnică per node: - 4094 VLANs
1.3.9	Funcționalități (incuzînd licențele necesare)	- Firewall de tip stateful - Filtrare URL, DNS - Antivirus, antispam, botnet detection	Specificarea tehnică per node: - Firewall de tip stateful - Filtrare URL, DNS

		- Virtual patching, security rating - Router cu suport protocoalelor de rutare dinamice (RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS) - SD-WAN Application aware routing - VRF support - Virtual firewall with license included – min 10 - Gruparea interfețelor în zone de securitate - Rutare între zonele de securitate - Policy-based routing - Funcționalități NAT, PAT si Transparent Bridge - Opțiune de a aplica NAT per politică - Suport VLAN Tagging 802.1Q - Suport VoIP SIP/H.323/SCCP Traversal NAT - Criptare de date: IPSec VPN, SSL VPN, ZTNA - Suport ZTNA, reguli de firewall in baza tag-rilor ZTNA, criptare canalului ZTNA prin DTLS cu autentificare mutuala client din poziția 1.8 și NGFW in baza certificatelor digitale - Suport pentru QoS si Traffic Shaping - Detecția și prevenirea intruziunilor – IDS/IPS - Protecție Anti-Malware prin folosirea tehnologiei AI - Blocarea și controlul traficului din rețea generat de aplicații - Identificarea și controlul aplicațiilor - Opțiune de Traffic-Shaping per aplicație - Clasificare granulară a aplicațiilor după criterii multiple precum: Categorii de aplicații, Popularitate, Tehnologie și Risc - Monitorizarea aplicațiilor pe bază de IP/Utilizator, consum de bandă - Posibilitatea de definire a semnăturilor de aplicație personalizate - Protecție pentru atacuri de tip brute force - Detectarea anomaliilor de protocol - Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de stație folosit – funcționalitate de tip BYOD - Integrare cu soluția de tip Sandbox (solicitată la poziția 1.8) - Actualizări automate de semnături de securitate AV de la sandox pentru protecția eficienta de la zero day attacks - Actualizări automate de semnături de securitate pentru îndeplinirea tuturor funcționalităților solicitate	- Antivirus, antispam, botnet detection - Virtual patching, security rating - Router cu suport protocoalelor de rutare dinamice (RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS) - SD-WAN Application aware routing - VRF support - Virtual firewall with license included – 10 - Gruparea interfețelor în zone de securitate - Rutare între zonele de securitate - Policy-based routing - Funcționalități NAT, PAT si Transparent Bridge - Opțiune de a aplica NAT per politică - Suport VLAN Tagging 802.1Q - Suport VoIP SIP/H.323/SCCP Traversal NAT - Criptare de date: IPSec VPN, SSL VPN, ZTNA - Suport ZTNA, reguli de firewall in baza tag-rilor ZTNA, criptare canalului ZTNA prin DTLS cu autentificare mutuala client din FortiSandbox și NGFW in baza certificatelor digitale - Suport pentru QoS si Traffic Shaping - Detecția și prevenirea intruziunilor – IDS/IPS - Protecție Anti-Malware prin folosirea tehnologiei AI - Blocarea și controlul traficului din rețea generat de aplicații - Identificarea și controlul aplicațiilor - Opțiune de Traffic-Shaping per aplicație - Clasificare granulară a aplicațiilor după criterii multiple precum: Categorii de aplicații, Popularitate, Tehnologie și Risc - Monitorizarea aplicațiilor pe bază de IP/Utilizator, consum de bandă - Posibilitatea de definire a semnăturilor de aplicație personalizate - Protecție pentru atacuri de tip brute force - Detectarea anomaliilor de protocol - Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de stație folosit – funcționalitate de tip BYOD - Integrare cu soluția FortiSandbox - Actualizări automate de semnături de securitate AV de la sandox pentru protecția eficienta de la zero day attacks - Actualizări automate de semnături de securitate pentru îndeplinirea tuturor funcționalităților solicitate
1.3.10	Funcționalități de administrare, logare, autentificare a utilizatorilor	- Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI) - Utilizatori/Administratori cu drepturi configurabile - Funcționalitate de export/import a configurației - Monitorizare grafică în timp real și istorică - Suport syslog - Suport SNMP v1/v2c/v3 - Notificare prin e-mail pentru alerte - Definire locală a utilizatorilor - Integrare cu Windows Active Directory (AD)	Specificarea tehnică per cluster: - Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI) - Utilizatori/Administratori cu drepturi configurabile - Funcționalitate de export/import a configurației - Monitorizare grafică în timp real și istorică - Suport syslog - Suport SNMP v1/v2c/v3 - Notificare prin e-mail pentru alerte - Definire locală a utilizatorilor

		- Suport pentru autentificarea grupurilor de utilizatori prin LDAP - Suport pentru autentificare prin doi factori - Centralized Security Data Lake: Collects and consolidates logs and telemetry data - Advanced Analytics and Event Correlation - Unified Logging and Analytics Platform - Real-Time Threat Intelligence Integration - Automated Reporting and Customizable Dashboards - Log Forwarding Capabilities - Attack Surface Security Scoring and Compliance Monitoring Service	- Integrare cu Windows Active Directory (AD) - Suport pentru autentificarea grupurilor de utilizatori prin LDAP - Suport pentru autentificare prin doi factori - Centralized Security Data Lake: Collects and consolidates logs and telemetry data - Advanced Analytics and Event Correlation - Unified Logging and Analytics Platform - Real-Time Threat Intelligence Integration - Automated Reporting and Customizable Dashboards - Log Forwarding Capabilities - Attack Surface Security Scoring and Compliance Monitoring Service
1.3.11	Chassis	- Rackmount, 1U, metal, all mounting accessories included	Specificarea tehnică per node: - Rackmount, 1U, metal, all mounting accessories included
1.3.12	Power	- min. 2 x Redundant Power Supplies, with 2 Power cables, PDU connection - 100–240V AC, 50/60Hz	Specificarea tehnică per node: - 2 x Redundant Power Supplies, with 2 Power cables, PDU connection - 100–240V AC, 50/60Hz
1.3.13	Licensing	- Minimum 3 Years, including all security subscriptions and updates	- FortiAnalyzer-VM – perpetual license with 3 Year FortiCare Premium Support - FortiGate - FortiGuard Enterprise Protection - 3 years Subscription and FortiCare Support

1.3.14	Garanție și suport	- Perioada minimă de garanție: 36 luni, acordată de producător, care să includă:
		  - Înlocuirea echipamentului în caz de defect hardware;
		  - Diagnosticare și remediere defecțiuni;
		  - Furnizarea pieselor de schimb necesare;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de firmware/software, atât pentru versiuni minore, cât și majore;
		  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
		- **Suport tehnic local** din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de End-of-Support și End-of-Life a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- Garanția și suportul se acordă indiferent de păstrarea ambalajului original.
		- Cerințe privind instalarea și serviciile aferente**:**
		  - Implementarea completă a soluției;
		  - Migrarea regulilor de securitate existente către noul echipament;
		  - Integrarea echipamentelor noi cu infrastructura existentă;
		  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
		  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.
		- Cerințe privind acreditările furnizorului:
			- **Perioada de garanție:** 36 luni, acordată de producător, care să includă:
			  - Înlocuirea echipamentului în caz de defect hardware;
			  - Diagnosticare și remediere defecțiuni;
			  - Furnizarea pieselor de schimb necesare;
			  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
			  - Actualizări de firmware/software, atât pentru versiuni minore, cât și majore;
			  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
			- **Suport tehnic local** din partea IT-LAB GRUP SRL: 12 luni, disponibil 24x7x365, cu alocarea a 15 ore/lună;
			- Garanția și suportul se acordă indiferent de păstrarea ambalajului original.
			- **Instalarea și serviciile aferente:**
			  - Implementarea completă a soluției;
			  - Migrarea regulilor de securitate existente către noul echipament;
			  - Integrarea echipamentelor noi cu infrastructura existentă;
			  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
			  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.

		- Minimum două persoane tehnice, deținând certificări emise de producător (vendor), pentru echipamentele și soluțiile propuse; - Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.	
1.4. 1.4.1	**Soluție de tip Web Application Firewall (WAF)** **Web Application Firewall (WAF)**		**Soluție de tip Web Application Firewall (WAF)** **FortiWeb Web Application Firewall cu AV, FortiWeb Security Service, IP Reputation, Credential Stuffing Defense Service și Threat Analytics**
1.4.2	Tip	- Modelul de licențiere trebuie să fie de tip perpetual. - Virtual Machine (On-premises)	- Modelul de licențiere de tip perpetual. - Virtual Machine (On-premises)
1.4.3	Deployment Platform	- Microsoft Hyper-V - High availability support - Min. 10 domene Web	- Microsoft Hyper-V - High availability support - Minimum 16 domene Web
1.4.4	HTTP Throughput	- Min. 100 Mbps	- 100 Mbps
1.4.5	Web Security	- Protection against OWASP Top 10 vulnerabilities - Cross-Site Scripting (XSS) prevention - Session hijacking defense - Brute force attack mitigation - IP address reputation services - Geolocation-based IP blocking - WebSocket traffic security - HTTP protocol compliance and validation	- Protection against OWASP Top 10 vulnerabilities - Cross-Site Scripting (XSS) prevention - Session hijacking defense - Brute force attack mitigation - IP address reputation services - Geolocation-based IP blocking - WebSocket traffic security - HTTP protocol compliance and validation
1.4.6	Application Attack Protection	- SQL Injection prevention - Integration with third-party scanners for virtual patching - Session hijacking protection	- SQL Injection prevention - Integration with third-party scanners for virtual patching - Session hijacking protection
1.4.7	Security Services	- Malware detection - Virtual patching capabilities - Denial-of-Service (DoS) attack prevention - Advanced threat detection through correlation - Brute force attack defense - Credential stuffing - Defense against known and zero-day attacks - Web services signature validation - Advanced threat intelligence and analytics	- Malware detection - Virtual patching capabilities - Denial-of-Service (DoS) attack prevention - Advanced threat detection through correlation - Brute force attack defense - Credential stuffing - Defense against known and zero-day attacks - Web services signature validation - Advanced threat intelligence and analytics
1.4.8	Application Delivery	- HTTPS/SSL Offloading - Caching	- HTTPS/SSL Offloading - Caching
1.4.9	Authentication	- Support for LDAP, RADIUS, and SAML authentication protocols - SSL client certificate authentication - SAML authentication compatibility	- Support for LDAP, RADIUS, and SAML authentication protocols - SSL client certificate authentication - SAML authentication compatibility
1.4.10	API Protection	- RESTful API support - Web services signature verification - API Gateway functionality - Schema validation	- RESTful API support - Web services signature verification - API Gateway functionality - Schema validation

1.4.11	Management and Reporting	- Centralized management and reporting system - Real-time data dashboards - Role-based access control (RBAC) implementation - OWASP Top 10 threat categorization - Geolocation-based blocking with embedded analytics	- Centralized management and reporting system - Real-time data dashboards - Role-based access control (RBAC) implementation - OWASP Top 10 threat categorization - Geolocation-based blocking with embedded analytics
1.4.12	Licensing	- Minimum 3 Years, including all security subscriptions and updates	- FortiWeb-VM02 – perpetual license with 3 Years FortiCare Premium Support and FortiGuard Enterprise ATP Bundle Contract

1.4.13	Garanție și suport	- Perioada minimă de garanție: 36 luni, acordată de producător, care să includă:
		  - Diagnosticare și remediere defecțiuni;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de software, atât pentru versiuni minore, cât și majore;
		  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
		- Suport tehnic local din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de End-of-Support și End-of-Life a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- Cerințe privind instalarea și serviciile aferente**:**
		  - Implementarea completă a soluției;
		  - Migrarea regulilor de securitate existente către noul echipament;
		  - Integrarea echipamentelor noi cu infrastructura existentă;
		  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
		  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.
		- Cerințe privind acreditările furnizorului**:**
		  - Personal tehnic certificat pentru echipamentele și soluțiile propuse;
		Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.
			- **Perioada de garanție:** 36 luni, acordată de producător, care să includă:
			  - Diagnosticare și remediere defecțiuni;
			  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
			  - Actualizări de software, atât pentru versiuni minore, cât și majore;
			  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
			- **Suport tehnic local din partea IT-LAB GRUP SRL:** 12 luni, disponibil 24x7x365, cu alocarea a 15 ore/lună;
			- **Instalarea și serviciile aferente:**
			  - Implementarea completă a soluției;
			  - Migrarea regulilor de securitate existente către noul echipament;
			  - Integrarea echipamentelor noi cu infrastructura existentă;
			  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
			  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.

1.5. 1.5.1	**Soluție Mail Security Gateway** **Mail Security Gateway**		**Soluție Mail Security Gateway** **FortiMail-VM virtual appliance cu FortiGuard Enterprise ATP Bundle**
1.5.2	Tip	- Modelul de licențiere trebuie să fie de tip perpetual. - Virtual Machine (On-premises) - Working mode: Gateway	- Modelul de licențiere de tip perpetual. - Virtual Machine (On-premises) - Working mode: Gateway
1.5.3	Supported Hypervisors	- Microsoft Hyper-V - KVM QEMU	- Microsoft Hyper-V - KVM QEMU
1.5.4	Mailbox Compatibility	- Microsoft Exchange Server 2019 - Supports up to 500 mailboxes - Inbound/Outbound messages inspection and routing	- Microsoft Exchange Server 2019 - Supports more than 500 mailboxes - Inbound/Outbound messages inspection and routing
1.5.5	Performance (with Threat	- performanța de prelucrare a mesajelor e-mail min. 50 000 pe ora - Antispam and antiphishing capture rate: min 99.9 %	- performanța de prelucrare a mesajelor e-mail 67 000 pe ora - Antispam and antiphishing capture rate: 99.9 %

	Protection Enabled)		
1.5.6	User Interface	- Robust webmail interface for server-mode deployments and quarantine management - Comprehensive mail queue management system	- Robust webmail interface for server-mode deployments and quarantine management - Comprehensive mail queue management system

1.5.7	Antispam	- Sender and domain reputation analysis
		- Spam and attachment signature detection
		- Adaptive heuristic rules for dynamic threat response
		- Outbreak protection mechanisms
		- Filtering for spam, malware, and phishing URLs
		- Detection of newly registered domains
		- Greylisting for IPv4, IPv6, and email accounts
		- Local sender reputation tracking (based on IPv4, IPv6, and Endpoint ID)
		- Behavioral analysis for advanced threat detection
		- Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
		- Detection of newsletters (greymail) and suspicious newsletters
		- PDF scanning and image analysis
		- Global, domain, and user-level block/safe lists
		- Support for enterprise sender identity standards:
		  - Sender Policy Framework (SPF)
		  - DomainKeys Identified Mail (DKIM)
		  - Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
		- Multi-system and per-user self-service quarantine options
			- Sender and domain reputation analysis
			- Spam and attachment signature detection
			- Adaptive heuristic rules for dynamic threat response
			- Outbreak protection mechanisms
			- Filtering for spam, malware, and phishing URLs
			- Detection of newly registered domains
			- Greylisting for IPv4, IPv6, and email accounts
			- Local sender reputation tracking (based on IPv4, IPv6, and Endpoint ID)
			- Behavioral analysis for advanced threat detection
			- Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
			- Detection of newsletters (greymail) and suspicious newsletters
			- PDF scanning and image analysis
			- Global, domain, and user-level block/safe lists
			- Support for enterprise sender identity standards:
			  - Sender Policy Framework (SPF)
			  - DomainKeys Identified Mail (DKIM)
			  - Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
			- Multi-system and per-user self-service quarantine options

1.5.8	Targeted attack protection	- Content Disarm and Reconstruction (CDR) - Neutralization of Office and PDF documents (removal of macros, active content, and attachments) - Sanitization of email HTML content by removing hyperlinks or rewriting URLs - Protection against Business Email Compromise (BEC) - Multi-layered anti-spoofing measures - Manual and automated impersonation detection - Cousin domain detection - URL Click Protect for URL rewriting and real-time rescanning	- Content Disarm and Reconstruction (CDR) - Neutralization of Office and PDF documents (removal of macros, active content, and attachments) - Sanitization of email HTML content by removing hyperlinks or rewriting URLs - Protection against Business Email Compromise (BEC) - Multi-layered anti-spoofing measures - Manual and automated impersonation detection - Cousin domain detection - URL Click Protect for URL rewriting and real-time rescanning
1.5.9	Content detection	- CPRL signature verification - Heuristic-based behavioral analysis - Greyware identification - Global threat intelligence and data analytics - Active content detection in PDF and Office documents - Threat rescanning upon quarantine release - Custom file hash verification - MIME and file type identification - Advanced data-loss prevention with file fingerprinting and sensitive data detection - Automated fingerprinting for Windows fileshares and manual uploads	- CPRL signature verification - Heuristic-based behavioral analysis - Greyware identification - Global threat intelligence and data analytics - Active content detection in PDF and Office documents - Threat rescanning upon quarantine release - Custom file hash verification - MIME and file type identification - Advanced data-loss prevention with file fingerprinting and sensitive data detection - Automated fingerprinting for Windows fileshares and manual uploads - Detection of healthcare, financial, personally identifiable information (PII), and profanity - Decryption of archives, PDFs, and Office documents using built-in and admin-defined password lists

		- Detection of healthcare, financial, personally identifiable information (PII), and profanity - Decryption of archives, PDFs, and Office documents using built-in and admin-defined password lists - Word detection within email bodies - Dynamic Image Analysis Service	- Word detection within email bodies - Dynamic Image Analysis Service
1.5.10	Encryption	- Comprehensive encryption support - Server-to-server TLS with granular ciphersuite control and optional enforcement - S/MIME support - Clientless encryption to recipient desktops using Identity-Based Encryption (IBE) - Optional Outlook plugin for triggering IBE	- Comprehensive encryption support - Server-to-server TLS with granular ciphersuite control and optional enforcement - S/MIME support - Clientless encryption to recipient desktops using Identity-Based Encryption (IBE) - Optional Outlook plugin for triggering IBE
1.5.11	Management, logging, and reporting	- Basic and advanced management modes - Role-based administration accounts per domain - Detailed logging for activities, configuration changes, and incidents - Built-in reporting module - Comprehensive message tracking - Centralized quarantine for large-scale deployments - Centralized logging and reporting system - SNMP support with standard and private MIBs, including threshold-based traps - Support for local or external storage servers, including iSCSI devices - External Syslog integration - Open REST API for configuration and management	- Basic and advanced management modes - Role-based administration accounts per domain - Detailed logging for activities, configuration changes, and incidents - Built-in reporting module - Comprehensive message tracking - Centralized quarantine for large-scale deployments - Centralized logging and reporting system - SNMP support with standard and private MIBs, including threshold-based traps - Support for local or external storage servers, including iSCSI devices - External Syslog integration - Open REST API for configuration and management
1.5.12	High availability support	- Active-Passive mode - Active-Active configuration synchronization - Synchronization of quarantine and mail queues - Device failure detection and notifications - Support for link status monitoring, failover, and redundant interfaces	- Active-Passive mode - Active-Active configuration synchronization - Synchronization of quarantine and mail queues - Device failure detection and notifications - Support for link status monitoring, failover, and redundant interfaces
1.5.13	Licensing	- Minimum 3 Years, including all security subscriptions and updates	- FortiMail-VM02 – perpetual license with 3 Years FortiCare Premium Support and FortiGuard Enterprise ATP Bundle

1.5.14	Garanție și suport	- Perioada minimă de garanție: 36 luni, acordată de producător, care să includă:
		- Diagnosticare și remediere defecțiuni;
		- Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		- Actualizări de software, atât pentru versiuni minore, cât și majore;
		- Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
		- Suport tehnic local din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de End-of-Support și End-of-Life a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- Cerințe privind instalarea și serviciile aferente**:**
		- Implementarea completă a soluției;
		- Migrarea regulilor de securitate existente către noul echipament;
		- Integrarea echipamentelor noi cu infrastructura existentă;
			- **Perioada de garanție:** 36 luni, acordată de producător, care să includă:
			- Diagnosticare și remediere defecțiuni;
			- Suport tehnic non-stop (24x7x365) direct din partea producătorului;
			- Actualizări de software, atât pentru versiuni minore, cât și majore;
			- Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
			- **Suport tehnic local din partea IT-LAB GRUP SRL:** 12 luni, disponibil 24x7x365, cu alocarea a 15 ore/lună;
			- **Instalarea și serviciile aferente:**
			  - Implementarea completă a soluției;
			  - Migrarea regulilor de securitate existente către noul echipament;
			  - Integrarea echipamentelor noi cu infrastructura existentă;
			  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
			  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.

		- Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - Cerințe privind acreditările furnizorului**:** - Personal tehnic certificat pentru echipamentele și soluțiile propuse; Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.	
1.6.	**Soluție Zero Trust Network Access (ZTNA)**		**FortiClient EPP/ATP Subscription pentru 200 endpoints, include VPN/ZTNA Agent, EPP/ATP on-prem EMS cu FortiCare Premium.**
1.6.1	Tip	- Soluție pentru gestionarea securizată a accesului utilizatorilor la resursele interne, în conformitate cu conceptul ZTNA și cu implementarea protecției avansate la nivel de endpoint.	- Soluție pentru gestionarea securizată a accesului utilizatorilor la resursele interne, în conformitate cu conceptul ZTNA și cu implementarea protecției avansate la nivel de endpoint.
1.6.2	Cantitate	- min. 200 stații de lucru	- 200 stații de lucru
1.6.3	Cerințe generale:	- Soluția trebuie să ofere un instrument centralizat de administrare; - Clientul endpoint trebuie să fie compatibil cu sistemele de operare: Windows 10 și mai sus, OS X 10.14 și mai sus, Linux Ubuntu 22 și mai sus.	- Soluția oferă un instrument centralizat de administrare; - Clientul endpoint este compatibil cu sistemele de operare: Windows 10 și mai sus, OS X 10.14 și mai sus, Linux Ubuntu 22 și mai sus.
1.6.4	Funcționalități	- Remote Client deployment. - Endpoint onboarding, custom client installers, email invitations - Integration with Windows Active Directory - Real-time dashboard - Software inventory management - Vulnerability detection and remediation - Automatic group assignment - Remote triggers - Remote Logging and Reporting prin integrare cu soluția de gestiune, analiză și raportare pe baza jurnalelor de rețea (solicitată la poziția 1.3.10) - ZTNA Remote Access - IPSEC, SLL VPN Access - Split Tunnel on application basis - Removable media control - Application control, firewall - AI-driven antivirus - Automated quarantine - Ransomware protection - Patch Policy Enforcement: instalarea automata a patch-rilor pentru aplicațiile instalate in sistemul de operare a utilizatorului. Raportarea vulnerabilității aplicațiilor identificate cu oferirea CVE score-ului - Multifactor factor authentication, integrare cu soluția de gestiune a autorizării în rețeaua securizată (solicitată la poziția 1.7) - Integrarea cu soluția Sanbox (solicitată la poziția 1.8)	- Remote Client deployment. - Endpoint onboarding, custom client installers, email invitations - Integration with Windows Active Directory - Real-time dashboard - Software inventory management - Vulnerability detection and remediation - Automatic group assignment - Remote triggers - Remote Logging and Reporting prin integrare cu soluția de gestiune, analiză și raportare pe baza jurnalelor de rețea (solicitată la poziția 1.3.10) - ZTNA Remote Access - IPSEC, SLL VPN Access - Split Tunnel on application basis - Removable media control - Application control, firewall - AI-driven antivirus - Automated quarantine - Ransomware protection - Patch Policy Enforcement: instalarea automata a patch-rilor pentru aplicațiile instalate in sistemul de operare a utilizatorului. Raportarea vulnerabilității aplicațiilor identificate cu oferirea CVE score-ului - Multifactor factor authentication, integrare cu soluția de gestiune a autorizării în rețeaua securizată (FortiAuthenticator) - Integrarea cu soluția Sanbox (FortiSandbox)
1.6.5	Licensing	- Minimum 3 Years, including all security subscriptions and updates	- FortiClient EPP/ATP - 3 Years subscription with FortiCare Premium Support
1.6.6	Garanție și suport	- Perioada minimă de garanție: 36 luni, acordată de producător, care să includă:	- **Perioada de garanție:** 36 luni, acordată de producător, care să includă: - Diagnosticare și remediere defecțiuni;

		- Diagnosticare și remediere defecțiuni; - Suport tehnic non-stop (24x7x365) direct din partea producătorului; - Actualizări de software, atât pentru versiuni minore, cât și majore; - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate; - Suport tehnic local din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună; - Perioada de End-of-Support și End-of-Life a echipamentului nu trebuie să fie mai devreme de anul 2030; - Cerințe privind instalarea și serviciile aferente**:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - Cerințe privind acreditările furnizorului**:** - Personal tehnic certificat pentru echipamentele și soluțiile propuse; Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.	- Suport tehnic non-stop (24x7x365) direct din partea producătorului; - Actualizări de software, atât pentru versiuni minore, cât și majore; - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate; - **Suport tehnic local din partea IT-LAB GRUP SRL:** 12 luni, disponibil 24x7x365, cu alocarea a 15 ore/lună; - **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.
1.7	**Soluție de gestiune a autorizării în rețeaua securizată**		**FortiAuthenticator - VM Base License (with 100 extra users license upgrade) și FortiTokenMobile (Electronic License), suportă 200 utilizatori**
1.7.1	Tip	- Soluție pentru gestionarea autorizării în cadrul rețelei securizate, bazată pe identificarea utilizatorilor și pe permisiunile de acces furnizate de sisteme terțe (Identity-Based Policies).	- Soluție pentru gestionarea autorizării în cadrul rețelei securizate, bazată pe identificarea utilizatorilor și pe permisiunile de acces furnizate de sisteme terțe (Identity-Based Policies).
1.7.2	Cantitate	- 200 de utilizatori	- 200 de utilizatori
1.7.3	Cerințe generale	- Soluția trebuie să asigure integrarea cu echipamentele de tip firewall din poziția 1.3 în vederea permiterii accesului în rețeaua securizată. - Soluția trebuie să asigure integrarea cu soluția de gestiune, analiză și raportare pe baza jurnalelor de rețea (solicitată la poziția 1.3.10) - Soluția trebuie să ofere un instrument centralizat de administrare. - Soluția trebuie să fie oferită ca Appliance Virtual. - Compatibilitate cu platforma de virtualizare: Microsoft Hyper-V. - Soluția trebuie să conțină cel putin 200 licențe de software de tip One-time password application pentru iOS, Android	- Soluția asigură integrarea cu echipamentele de tip firewall din poziția 1.3 în vederea permiterii accesului în rețeaua securizată. - Soluția asigură integrarea cu soluția de gestiune, analiză și raportare pe baza jurnalelor de rețea (solicitată la poziția 1.3.10) - Soluția oferă un instrument centralizat de administrare. - Soluția este oferită ca Appliance Virtual. - Compatibilitate cu platforma de virtualizare: Microsoft Hyper-V. - Soluția conține 200 licențe de software de tip One-time password application pentru iOS, Android
1.7.4	Funcționalități	- Enables identity and role-based security policies in the secured enterprise network without the need for additional authentication through integration with Active Directory - Integration with LDAP and Active Directory for group membership - Enablement of identity and role-based security - Support of 802.1x, RADIUS, TACACS+, SAML IdP - Support of Single Sign-On (SSO)	- Enables identity and role-based security policies in the secured enterprise network without the need for additional authentication through integration with Active Directory - Integration with LDAP and Active Directory for group membership - Enablement of identity and role-based security - Support of 802.1x, RADIUS, TACACS+, SAML IdP - Support of Single Sign-On (SSO) - Support wide range of multi-factor authentification metods: One Time Password (OTP) tokens, e-mail and SMS OTP, digital certificates. - Support of Facial/PIN/Fingerpring security in Mobile OTP application

		- Support wide range of multi-factor authentification metods: One Time Password (OTP) tokens, e-mail and SMS OTP, digital certificates. - Support of Facial/PIN/Fingerpring security in Mobile OTP applicationSupport of RFC6238, RFC4226 specifications in Mobile OTP application	- Support of RFC6238, RFC4226 specifications in Mobile OTP application
1.7.5	Licensing	- Minimum 3 Years, including all security subscriptions and updates	- FortiAuthenticator VM Base License 100 extra users license upgrade – perpetual license for 200 users with 3 Years FortiCare Premium Support - FortiTokenMobile - perpetual license for 200 users

1.7.6	Garanție și suport	- Perioada minimă de garanție: 36 luni, acordată de producător, care să includă:
		  - Diagnosticare și remediere defecțiuni;
		  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
		  - Actualizări de software, atât pentru versiuni minore, cât și majore;
		  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
		- Suport tehnic local din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună;
		- Perioada de End-of-Support și End-of-Life a echipamentului nu trebuie să fie mai devreme de anul 2030;
		- Cerințe privind instalarea și serviciile aferente**:**
		  - Implementarea completă a soluției;
		  - Migrarea regulilor de securitate existente către noul echipament;
		  - Integrarea echipamentelor noi cu infrastructura existentă;
		  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
		  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.
		- Cerințe privind acreditările furnizorului**:**
		  - Personal tehnic certificat pentru echipamentele și soluțiile propuse;
		Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.
			- **Perioada de garanție:** 36 luni, acordată de producător, care să includă:
			  - Diagnosticare și remediere defecțiuni;
			  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
			  - Actualizări de software, atât pentru versiuni minore, cât și majore;
			  - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate;
			- **Suport tehnic local din partea IT-LAB GRUP SRL:** 12 luni, disponibil 24x7x365, cu alocarea a 15 ore/lună;
			- **Instalarea și serviciile aferente:**
			  - Implementarea completă a soluției;
			  - Migrarea regulilor de securitate existente către noul echipament;
			  - Integrarea echipamentelor noi cu infrastructura existentă;
			  - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției;
			  - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.

1.8.	**Soluție de Sandboxing**		**FortiSandbox VM00 Sandboxing Virtual Appliance cu Sandbox Threat Intelligence; Real-time Zero-Day Anti-Phishing Service**
1.8.1	Tip	- Soluție de tip Sandbox	- Soluție de tip Sandbox

1.8.2	Integrare	- Pentru analiza fișierelor și altor resurse, Soluția trebuie să fie capabila să se integreze și să accepte și analizeze informația cu echipamentele:
		  - Next-Generation Firewall (NGFW)
		  - Web Application Firewall (WAF)
		  - Mail Security Gateway
		  - Zero Trust Network Access (ZTNA) client
		  - Third-party integrations via APIs
			- Pentru analiza fișierelor și altor resurse, Soluția este capabila să se integreze și să accepte și analizeze informația cu echipamentele:
			  - Next-Generation Firewall (NGFW)
			  - Web Application Firewall (WAF)
			  - Mail Security Gateway
			  - Zero Trust Network Access (ZTNA) client
			  - Third-party integrations via APIs

1.8.3	Cerințe generale:	- Modelul de licențiere trebuie să fie de tip perpetual.	- Modelul de licențiere de tip perpetual.

		- Soluția trebuie să fie oferită ca Appliance Virtual. - Soluția trebuie să suporte min 5 mașini virtuale locale (nested VM) pentru simulare, să conțină 5 licențe pentru MS Windows 11 si 1 x licența MS Office (cu capabilitatea pentru 5 VM) - Compatibilitate cu platforma de virtualizare: Microsoft Hyper-V. - Soluția trebuie să suporte generarea rapoartelor detailate a amenințărilor identificate, cu posibilitatea de export in format STIX/TAXII pentru import-ul in sisteme SIEM compatibile - Soluția trebuie să ofere câteva nivele de scanare: statică (in baza de metadate: IP adresa sursă, domain, email), asistata AI (simulare in modele de AI) și in cele din urmă scanare dinamică (in sistemele de operare virtualizate in sandbox) - Pentru optimizarea performanței Soluția trebuie să suporte scanare paralelă, cu distribuția sarcinii intre diferite mașini virtuale. - Pentru optimizarea performantei Soluția trebuie să fie capabilă sa creeze înregistrări cache pentru resursele scanate ulterior (fișiere, link-ri, etc) și să ofere instant verdictul scanării in cazul in care aceeași resursa este solicitată de către Clienți mai mult decât 1 data. - Soluția trebuie să fie capabilă sa creeze semnături AV, care vor fi populate de NGFW din poziția 1.3 și de soluția din poziția 1.6 - Soluția trebuie să suporte neutralizarea URL-rilor malițioase si impunerea executării URL-rilor din email in sandox (CDR - content disarm and reconstruction)	- Soluția este oferită ca Appliance Virtual. - Soluția suportă 5 mașini virtuale locale (nested VM) pentru simulare, conține 5 licențe pentru MS Windows 11 si 1 x licența MS Office (cu capabilitatea pentru 5 VM) - Compatibilitate cu platforma de virtualizare: Microsoft Hyper-V. - Soluția suportă generarea rapoartelor detailate a amenințărilor identificate, cu posibilitatea de export in format STIX/TAXII pentru import-ul in sisteme SIEM compatibile - Soluția oferă câteva nivele de scanare: statică (in baza de metadate: IP adresa sursă, domain, email), asistata AI (simulare in modele de AI) și in cele din urmă scanare dinamică (in sistemele de operare virtualizate in sandbox) - Pentru optimizarea performanței Soluția suportă scanare paralelă, cu distribuția sarcinii intre diferite mașini virtuale. - Pentru optimizarea performantei Soluția este capabilă sa creeze înregistrări cache pentru resursele scanate ulterior (fișiere, link-ri, etc) și oferă instant verdictul scanării in cazul in care aceeași resursa este solicitată de către Clienți mai mult decât 1 data. - Soluția este capabilă sa creeze semnături AV, care vor fi populate de NGFW FortiGate-200G și de soluția FortiClient EPP. - Soluția suportă neutralizarea URL-rilor malițioase si impunerea executării URL-rilor din email in sandox (CDR - content disarm and reconstruction)
1.8.4	Funcționalități	- Zero-day threat detection and antiphising blocking in real-time mode - AI/ML analyze and detection - Inline blocking - Modes of working: File submission from NGFW/ESG/WAF/Endpoint, URL submission, sniffer, network share scanning (SMB, NFS, FTP, sFTP, OneDrive) - Antivirus, IPS, Web filtering - Sandboxing virtual mashines OS types: Windows 10/11, MacOS, Linux, Android - Possibility to create custom VMs - OCR scanning - URL, QR-code scanning - Supported file types: exe, documents, web, emails, Linux/Andoid/MacOS files, user-defined types - Advanced monitoring and reporting functionality - CLI, WEB management - Integration with external systems via ICAP, API	- Zero-day threat detection and antiphising blocking in real-time mode - AI/ML analyze and detection - Inline blocking - Modes of working: File submission from NGFW/ESG/WAF/Endpoint, URL submission, sniffer, network share scanning (SMB, NFS, FTP, sFTP, OneDrive) - Antivirus, IPS, Web filtering - Sandboxing virtual mashines OS types: Windows 10/11, MacOS, Linux, Android - Possibility to create custom VMs - OCR scanning - URL, QR-code scanning - Supported file types: exe, documents, web, emails, Linux/Andoid/MacOS files, user-defined types - Advanced monitoring and reporting functionality - CLI, WEB management - Integration with external systems via ICAP, API
1.8.5	Licensing	- Minimum 3 Years, including all security subscriptions and updates	- FortiSandbox VM00 – perpetual license with 3 Years FortiCare Premium Support - Threat Intelligence – 3 Year subscription and FortiCare Premium Support - Real-time Zero-Day Anti-Phishing Service – 3 Year subscription - FortiSandbox Windows Licenses - perpetual license - FortiSandbox Office Licenses - perpetual license

1.8.6	Garanție și suport	- Perioada minimă de garanție: 36 luni, acordată de producător, care să includă:
		  - Diagnosticare și remediere defecțiuni;
			- **Perioada de garanție:** 36 luni, acordată de producător, care să includă:
			  - Diagnosticare și remediere defecțiuni;
			  - Suport tehnic non-stop (24x7x365) direct din partea producătorului;
			  - Actualizări de software, atât pentru versiuni minore, cât și majore;

		- Suport tehnic non-stop (24x7x365) direct din partea producătorului; - Actualizări de software, atât pentru versiuni minore, cât și majore; - Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate; - Suport tehnic local din partea ofertantului: minim 12 luni, disponibil 24x7x365, cu alocarea a cel puțin 15 ore/lună; - Perioada de End-of-Support și End-of-Life a echipamentului nu trebuie să fie mai devreme de anul 2030; - Cerințe privind instalarea și serviciile aferente**:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului. - Cerințe privind acreditările furnizorului**:** - Personal tehnic certificat pentru echipamentele și soluțiile propuse; Formular de autorizare emis de producător (Manufacturer Authorization Form – MAF) valabil pentru teritoriul Republicii Moldova.	- Actualizări automate ale semnăturilor de securitate, necesare pentru îndeplinirea tuturor funcționalităților solicitate; - **Suport tehnic local din partea IT-LAB GRUP SRL:** 12 luni, disponibil 24x7x365, cu alocarea a 15 ore/lună; - **Instalarea și serviciile aferente:** - Implementarea completă a soluției; - Migrarea regulilor de securitate existente către noul echipament; - Integrarea echipamentelor noi cu infrastructura existentă; - Crearea regulilor de securitate necesare și punerea în funcțiune a soluției; - Transfer de cunoștințe (knowledge transfer) către echipa IT a beneficiarului.

Tabel №2. Codurile produselor (Part Number) ale producătorului

Denumirea bunurilor solicitat	Part number	Denumirea bunurilor oferit	Can-tea
1.1 Next Generation Firewall (NGFW)	FG-200G-BDL-809-36	FortiGate-200G Hardware plus 3 Year FortiCare Premium and FortiGuard Enterprise Protection	2
	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m, 0°C to 70°C, transceivers included, for systems with SFP+ and SFP/SFP+ slots	8
	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots	8
1.2 Licente Sofware incluse aferente NGFW solicitat la p. 1.1	FAZ-VM-GB5	FortiAnalyzer-VM Upgrade license for adding 5 GB/Day of Logs.	1
	FC2-10-LV0VM-248-02-36	FortiAnalyzer-VM FortiCare Premium Support 3 Year FortiCare Premium Support (for 1-11 GB/Day of Logs)	1
2.1 Web Application Firewall (WAF)	FWB-VM02	FortiWeb-VM02 Web Application Firewall - virtual appliance for all supported platforms. Supports up to 2 x vCPU core	1
2.2 Licente Sofware incluse aferente soluției Web Application Firewall (WAF) la p. 2.1	FC-10-VVM02-581-02-36	FortiWeb-VM02 3 Year Advanced Bundle - Standard Bundle plus Credential Stuffing Defense Service and Threat Analytics	1
3.1 Soluție Mail Security Gateway	FML-VM02	FortiMail-VM02 FortiMail-VM virtual appliance for all supported platforms. 2 x vCPU cores	1
3.2 Licente Sofware incluse aferente soluției Mail Security Gateway la p. 3.1	FC-10-0VM02-643-02-36	FortiMail-VM02 3 Year FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract	1
4.1 Soluție Zero Trust Network Access (ZTNA) 4.2 Licente Sofware incluse aferente soluției Zero Trust Network Access (ZTNA) la p. 4.1	FC1-10-EMS04-429-01-36	Endpoint-based Licenses - EPP/ATP (On Premise Deployments) 3 Year FortiClient EPP/ATP Subscription for 25 endpoints, Includes VPN/ZTNA Agent, EPP/ATP on-prem EMS with FortiCare Premium.	8
5.1 Soluție de gestiune a autorizării în rețeaua securizată	FAC-VM-BASE	FortiAuthenticator - VM License VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms	1
5.2 Licente Sofware incluse aferente soluției de gestiune a autorizării în rețeaua securizată la p. 5.1	FAC-VM-100-UG	FortiAuthenticator - VM License FortiAuthenticator-VM 100 users license upgrade	1
	FC1-10-0ACVM-248-02-36	FortiAuthenticator - VM License 3 Year FortiCare Premium Support (1 - 500 USERS)	1
	FTM-ELIC-200	FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 200 users. Electronic license certificate. License transfer between devices is not allowed.	1
6.1 Soluție de Sandboxing	FSA-VM00	FortiSandbox VM00 Sandboxing Virtual Appliance. Available Universal VM expansion supports up to max 8 local and 200 cloud, with a total count not exceeding 200. No Universal VM count and Microsoft licenses included.	1
6.2 Licente Sofware incluse aferente soluției de Sandboxing	FC-10-FSV00-500-02-12	FortiSandbox VM00 1 Year Sandbox Threat Intelligence (Antivirus, IPS, Web Filtering, File Query, Industrial Security, SandBox Engine) plus FortiCare Premium. Subscribes up to 8 VMs.	3
	FC-10-FSV00-682-02-12	FortiSandbox VM00 1 Year Real-time Zero-Day Anti-Phishing Service	3
	FC-10-FSV00-248-02-12	FortiSandbox VM00 1 Year FortiCare Premium Support	3
	FSA-UPG-VM-WIN11-1	FortiSandbox Windows Licenses Expands FSA license of Windows 11 for FSA VM Appliance. Allows 1 VM clone on Local (including Custom) and Cloud.	5
	FSA-UPG-OFFICE2021-1	FortiSandbox Office Licenses Expands FSA (Appliance/VM) licenses of Microsoft Office 2021 by 1.	1