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

Specificaţii tehnice

Numărul procedurii de achiziție ocds-b3wdp1-MD-1733490330936 din 06.12.2024
Obiectul achiziției: Echipament de securizare a rețelei de calculatoare interne a MAI

Denumirea bunurilor/serviciilor	**Denumirea modelului bunului/ serviciului**	**Ţara de origine**	**Produ-cătorul**	**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
Bunuri/servicii						
Lotul 1 Actualizarea infrastructurii IT în cadrul MAI						
Paravan de protecție tip 1 (instalare, configurare, migrare)	FortiGate 401F	SUA	Fortinet	Conform Specificațiilor tehnice Caietului de sarcini	FortiGate-401F Hardware plus 3 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) (FG-401F-BDL-950-36) 1.1 Carcasa rack-mount 1U 19" 1.2 Porturi: 16x 1GE RJ45; 8x 10G SFP+ 1.3 AC Power Input 100–240V AC, 50/60Hz, conector C14 1.4 Temperatura de operare de la 0°C până la 40°C 1.5 Blocuri de alimentare redundante AC 1+1(Hot Swappable) 1.6 Direcționarea fluxului de aer: față și lateral - spre spate 1.7 Echipamentul include 8x SFP+ 10G Active Optical Cable (AOC) 1.8 Echipamentul include toate cablurile si accesorile pentru conectare în rack 1.9 Porturi de consolă: 1xRJ45 1.10 Porturi de management: 1xRJ45 1.11Porturi HA: 1xRJ45 1.12 Soluția propusă este funcțională si sa corespunda tuturor cerințelor, fără careva limitări. 1.13 Soluția propusă permită detectarea și filtrarea traficului după conținut (content). 1.14 Soluția propusă permită detectarea și filtrarea atacurilor de tip DDoS prin definirea politicilor 1.15 Soluția propusă permită detectarea și filtrarea aplicațiilor. 1.16 Soluția propusă permită stabilirea regulilor de antispam, antivirus, web filtering. 1.17 Soluția propusă permită stabilirea regulilor de QoS și traffic shaping. 1.18 Soluția propusa permită stabilirea regulilor de firewall după criteriul de GeoIP.	

					1.19 Soluția propusa permită aplicarea regulilor de blocare a traficului de rețea având ca sursa sau destinație adresele BotNet, care se actualizează periodic. 1.20 Soluția propusa permită stabilirea regulilor de filtrare web – web inspection/Filter 1.21 Soluția propusă permită divizarea logica, prin atribuirea resurselor limita, ce va permite furnizarea pentru fiecare unitate logica cel puțin următoarea funcționalități: - Gestionarea Tabelei de Rutare - Gestionarea Tabelei de NAT - Gestionarea Tabelei Firewall - Gestionarea VPN Instance - Gestionarea Politicilor de securitate(Application,WebFilter,etc) - Gestionarea Interfețelor fizice si logice atribuite 1.22 Soluția propusa asigură cerințele minime pentru asigurarea disponibilității înalte: - Functionare Active-Active, Active-Passive - Functionalitate Stateful Failover (Firewall si VPN) - Detectare si notificare pentru echipament nefunctional - Monitorizarea conexiunii la retea - Functionalitate Link Failover 1.23 Soluția propusa asigură cerințele minime pentru asigurarea monitorizării componentelor hardware: - Monitorizare grafica in timp real si istorica - Suport syslog - Suport SNMP v1/v2c/v3 - Notificare prin e-mail pentru alerte - Suport sFlow si Netflow 1.24 Soluția propusă permită filtrarea traficului de 79 Gbps. 1.25 Soluția propusă are capacitatea de tunelare IPSec(VPN) de 55Gbps. 1.26 Soluția propusă suportă 2000 conexiunii VPN simultane de tip Site-to-Site Ipsec VPN 1.27 Soluția propusă suportă 5000 conexiunii VPN simultane de tip Remote Access SSL-VPN 1.28 Soluția propusă are capacitatea de inspectare a traficului SSL de 8Gbps. 1.29 Soluția propusă are capacitatea de inspectare a traficului prin activarea funcționalului de IPS de 12Gbps. 1.30 Soluția propusă are capacitatea de a stabili sesiuni simultane TCP până la 7.8 milioane. 1.31 Soluția propusă are capacitatea de a stabili sesiuni noi de 500000 pe secunda 1.32 Soluția propusă are funcționalite de verificare a stațiilor (Endpoint Control) prin integrare cu o aplicație software pentru securitate ce rulează pe stații care sa permită: - Blocarea traficului de aplicații instalate pe stații	

					- Restricționarea/filtrarea accesului web - Scanarea pentru vulnerabilități a stațiilor - Scanare Antivirus - Configurarea automata pentru tunele VPN 1.33 Soluția propusă are funcționalitate Data Leak Prevention: - In caz de scurgere de informații permită blocarea si arhivarea conversației pe protocoale de email, HTTP, FTP si variantele criptate SSL - Blocare după tip si dimensiune fișier - DLP fingerprint si arhivare 1.34Soluția propusă are funcționalități de autentificare a utilizatorilor: - Definire locala a utilizatorilor - Integrare cu Windows Active Directory (AD) pentru Single Sign On - Integrare cu RADIUS/LDAP/TACACS+ - Suport pentru autentificare prin doi factori folosind OTP generate de tokenuri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS - Suport pentru autentificare prin certificate digitale PKI X.509 - Posibilitatea limitării accesului utilizatorilor in rețea ce nu au instalat un client software de stație (client endpoint) 1.35 Soluția propusă include suport hardware și software din partea producătorului in regim 7/24 pentru 3 ani. 1.36 Soluția propusă include servicii de instalare, configurare, migrare, integrare conform caiet de sarcini.	
Paravan de protecție tip 2 (instalare, configurare, migrare)	FortiGate 201G	SUA	Fortinet		FortiGate-201G Hardware plus 3 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) (FG-201G-BDL-950-36) 2.1 Carcasa rack-mount 1U 19” 2.2 Porturi: 8x 1GE RJ45, 8x 10G SFP+ 2.3 AC Power Input 100–240V AC, 50/60Hz, conector C14 2.4 Temperatura de operare de la 0°C până la 40°C 2.5 Blocuri de alimentare redundante AC 1+1 2.6 Direcționarea fluxului de aer: față și lateral - spre spate 2.7 Echipamentul include 8x SFP+ 10G Active Optical Cable (AOC) 2.8 Echipamentul include toate cablurile si accesorile pentru conectare în rack 2.9 Porturi de consolă: 1xRJ45 2.10 Porturi de management: 1xRJ45 2.11 Porturi HA: 1xRJ45 2.12 Soluția propusă este funcțională si sa corespunda tuturor cerințelor, fără careva limitări. 2.13 Soluția propusă permită detectarea și filtrarea traficului după conținut (content). 2.14 Soluția propusă permită detectarea și filtrarea atacurilor de tip DDoS prin definirea politicilor 2.15 Soluția propusă permită detectarea și filtrarea aplicațiilor.	

					2.16 Soluția propusă permită stabilirea regulilor de antispam, antivirus, web filtering. 2.17 Soluția propusă permită stabilirea regulilor de QoS și traffic shaping. 2.18 Soluția propusa permită stabilirea regulilor de firewall după criteriul de GeoIP. 2.19 Soluția propusa permită aplicarea regulilor de blocare a traficului de rețea având ca sursa sau destinație adresele BotNet, care se actualizează periodic. 2.20 Soluția propusa permită stabilirea regulilor de filtrare web – web inspection/Filter 2.21 Soluția propusă permită divizarea logica, prin atribuirea resurselor limita, ce va permite furnizarea pentru fiecare unitate logica cel puțin următoarea funcționalități: - Gestionarea Tabelei de Rutare - Gestionarea Tabelei de NAT - Gestionarea Tabelei Firewall - Gestionarea VPN Instance - Gestionarea Politicilor de securitate(Application,WebFilter,etc) - Gestionarea Interfețelor fizice si logice atribuite 2.22 Soluția propusa asigură cerințele minime pentru asigurarea disponibilității înalte: - Functionare Active-Active, Active-Passive - Functionalitate Stateful Failover (Firewall si VPN) - Detectare si notificare pentru echipament nefunctional - Monitorizarea conexiunii la retea - Functionalitate Link Failover 2.23Soluția propusa asigură cerințele minime pentru asigurarea monitorizării componentelor hardware: - Monitorizare grafica in timp real si istorica - Suport syslog - Suport SNMP v1/v2c/v3 - Notificare prin e-mail pentru alerte - Suport sFlow si Netflow 2.24 Soluția propusă permită filtrarea traficului de 39 Gbps. 2.25 Soluția propusă are capacitatea de tunelare IPSec(VPN) de 36 Gbps. 2.26 Soluția propusă suportă 2000 conexiunii VPN simultane de tip Site-to-Site Ipsec VPN 2.27 Soluția propusă suportă 500 conexiunii VPN simultane de tip Remote Access SSL-VPN 2.28 Soluția propusă are capacitatea de inspectare a traficului SSL de 7Gbps. 2.29 Soluția propusă are capacitatea de inspectare a traficului prin activarea funcționalului de IPS de 9Gbps. 2.30 Soluția propusă are capacitatea de a stabili sesiuni simultane TCP până la 11 milioane. 2.31 Soluția propusă are capacitatea de a stabili sesiuni noi de 400000 pe secunda	

					2.32 Soluția propusă are funcționalite de verificare a stațiilor (Endpoint Control) prin integrare cu o aplicație software pentru securitate ce rulează pe stații care sa permită: - Blocarea traficului de aplicații instalate pe stații - Restricționarea/filtrarea accesului web - Scanarea pentru vulnerabilități a stațiilor - Scanare Antivirus - Configurarea automata pentru tunele VPN 2.33 Soluția propusă are funcționalitate Data Leak Prevention: - In caz de scurgere de informații permită blocarea si arhivarea conversației pe protocoale de email, HTTP, FTP si variantele criptate SSL - Blocare după tip si dimensiune fișier - DLP fingerprint si arhivare 2.34 Soluția propusă are funcționalități de autentificare a utilizatorilor: - Definire locala a utilizatorilor - Integrare cu Windows Active Directory (AD) pentru Single Sign On - Integrare cu RADIUS/LDAP/TACACS+ - Suport pentru autentificare prin doi factori folosind OTP generate de tokenuri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS - Suport pentru autentificare prin certificate digitale PKI X.509 - Posibilitatea limitării accesului utilizatorilor in rețea ce nu au instalat un client software de stație (client endpoint) 2.35 Soluția propusă include suport hardware și software din partea producătorului in regim 7/24 pentru 3 ani. 2.36 Soluția propusă include servicii de instalare, configurare, migrare, integrare conform caiet de sarcini.	
Sistem centralizat de monitorizare și de gestionare a echipamentelor de rețea (instalare, configurare, migrare)	FortiManager VM	SUA	Fortinet		FortiManager - VM License with FortiCare Premium Support (FMG-VM-10-UG with FC1-10-M3004-248-02-36) 3.1 Sistemul destinat monitorizării și gestionării urmatoarelor tipuri ale echipamentelor de rețea: paravane de protecție. 3.2 Sistemul capabil de agrega și stoca jurnalele de pe toate echipamentele de rețea, de a crea rapoarte, gestiona setările (folosind controlul accesului flexibil), licențe, actualizări și monitoriza starea hardware ‑ ului 3.3 Sistemul susține gestionarea politicilor și obiectelor comune prin grupuri de dispozitive ierarhice. La nivel de grup de dispozitive, este posibil crea politici partajate care sunt definite ca primul set de reguli și ultimul set de reguli - regulile pre și regulile pose-reguli, care urmează să fie evaluate cu potrivirea criterii 3.4 Sistemul susține administrarea bazată pe roluri, utilizată pentru a delega nivelul caracteristicilor accesului administrativ, inclusiv disponibilitatea modulelor numai de citire și ascundere din vedere pentru diferiți utilizatori 3.5 Sistemul susține următoarele moduri de implementare:	

					- Managementul configurațiilor pentru dispozitivele gestionate, fără colectarea jurnalelor. - Controlul atât funcțiilor de politică, cât și managementul jurnalelor pentru toate dispozitivele gestionate. - Colectarea și managementul jurnalelor din dispozitive gestionate 3.6 Sistemul susține autentificarea prin baza de date a sistemului, RADIUS, SAML, LDAP 3.7 Sistemul oferă următoarele modalități APIs de management: interfața grafică, Command - line interfața, XML ori alternative 3.9 Sistemul suportă regim HA, Active-Passive 3.10 Sistemul de protecție este realizat ca o aplicație virtuală și susține implementarea ca un dispozitiv virtual pe VMware ESXi; KVM și Microsoft Hyper - V 3.11 Sistemul include licența pentru gestionarea/monitorizarea concurentă a 10 de paravane de protecție 3.12 Sistemul are posibilitate de a gestiona/monitoriza 100 de paravane de protecție 3.13 Sistemul include suport tehnic din partea producătorului in regim 7/24 pentru timp de 3 ani 3.14 Soluția propusă include servicii de instalare, configurare, migrare, integrare conform caiet de sarcini.	
TOTAL						

Semnat:_____ Numele, Prenumele: Cioban Alexei În calitate de: Director

Digitally signed by Cioban Alexei
Date: 2024.12.26 22:59:10 EET
Reason: MoldSign Signature
Location: Moldova

MOLDOVA EUROPEANĂ

Ofertantul: IT-LAB GRUP SRL Adresa: mun. Chisinau; str-la Studentilor 2/4