Anexa nr. 22
la Documentația standard
nr. 115 din 15.09.2021
nr. ocds-b3wdp1-MD-1777362717526

Specificaţii tehnice

Numărul procedurii de achiziție ocds-b3wdp1-MD-1777362717526 din 28.04.2026
Obiectul achiziției: Echipamente de tip NGFW cu servicii de instalare, configurare, migrare și integrare.

Denumirea bunurilor/ serviciilor	**Denumirea modelului bunului/serviciului**	**Ţara de origine**	**Producătorul**	**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
Firewall (paravan de protecție)						
Echipamente de tip NGFW	FortiGate-701G	SUA China	Fortinet DO Network Limited	**Caracteristici fizice și de instalare:** a) Echipamentul trebuie să fie prevăzut cu șasiu pentru montare în rack standard 19”, livrat împreună cu toate accesoriile necesare pentru instalare în dulap de telecomunicații; b) Echipamentul trebuie să fie dotat cu minimum două surse de alimentare AC 220V redundante; c) Echipamentul trebuie să asigure fluxul de aer orientat din față spre spate (front-to-back); d) Echipamentul trebuie să fie livrat cu următoarele module optice și cabluri: 4 × SFP+ 10G AOC 5 m și 4 × SFP28 25G AOC 5 m. **Interfețe integrate:** a) Minimum 8 porturi Ethernet 1G; b) Minimum 4 porturi SFP+ 10G; c) Minimum 4 porturi SFP28 10/25G; d) Minimum 1 port de consolă RJ45; e) Minimum 1 port de management RJ45; f) Minimum 1 port dedicat pentru High Availability (HA).	FG-701G-BDL-950-36 FortiGate-701G Hardware plus 3 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) **Caracteristici fizice și de instalare:** a) Echipamentul este prevăzut cu șasiu pentru montare în rack standard 19” și este dotat cu toate accesoriile necesare pentru instalarea în dulap de telecomunicații.; b) Echipamentul este dotat cu două surse de alimentare AC 220V redundante; c) Echipamentul asigură fluxul de aer orientat lateral și din față spre spate (side and front-to-back).; d) Echipamentul este dotat cu următoarele module optice și cabluri: 4 × SFP+ 10G AOC 5 m și 4 × SFP28 25G AOC 5 m. **Interfețe integrate:** a) 8 porturi Ethernet 1/2.5/5G RJ45; b) 4 porturi SFP+ 10G; c) 4 porturi SFP28 10/25G; d) 1 port de consolă RJ45; e) 1 port de management RJ45; f) 1 port dedicat pentru High Availability (HA).	

				Performanță: a) Soluția propusă trebuie să asigure o capacitate de filtrare a traficului de minimum 140 Gbps; b) Soluția propusă trebuie să asigure o capacitate de tunelare IPSec (VPN) de minimum 50 Gbps; c) Soluția propusă trebuie să suporte cel puțin 2000 de conexiuni VPN simultane de tip Site-to-Site IPSec; d) Soluția propusă trebuie să suporte cel puțin 2000 de conexiuni VPN simultane de tip Remote Access SSL-VPN; e) Soluția propusă trebuie să asigure o capacitate de inspectare a traficului SSL de minimum 13 Gbps; f) Soluția propusă trebuie să asigure o capacitate de inspectare a traficului cu funcționalitatea IPS activată de minimum 36 Gbps; g) Soluția propusă trebuie să suporte până la 15 milioane de sesiuni TCP simultane; h) Soluția propusă trebuie să suporte cel puțin 700.000 de sesiuni noi pe secundă. **Funcționalități:** a) Detectarea și filtrarea traficului pe baza conținutului acestuia; b) Detectarea și atenuarea atacurilor de tip DDoS, pe baza politicilor definite; c) Definirea și aplicarea regulilor de QoS și traffic shaping pentru gestionarea traficului de rețea; d) Definirea și aplicarea politicilor de filtrare web (Web Inspection / Web Filtering); e) Aplicarea politicilor de securitate pentru antispam, antivirus și filtrare web; f) Definirea regulilor de firewall pe baza criteriilor GeoIP; g) Identificarea și controlul aplicațiilor prin mecanisme de Application Control; h) Blocarea traficului către și dinspre adrese BotNet, pe baza listelor actualizate periodic.	**Performanță:** a) Soluția propusă asigură o capacitate de filtrare a traficului de 145 Gbps; b) Soluția propusă asigură o capacitate de tunelare IPSec (VPN) de 55 Gbps; c) Soluția propusă suportă 2000 de conexiuni VPN simultane de tip Site-to-Site IPSec; d) Soluția propusă suportă 10000 de conexiuni VPN simultane de tip Remote Access SSL-VPN; e) Soluția propusă asigură o capacitate de inspectare a traficului SSL de 14 Gbps; f) Soluția propusă asigură o capacitate de inspectare a traficului cu funcționalitatea IPS activată de 38 Gbps; g) Soluția propusă suportă 28 milioane de sesiuni TCP simultane; h) Soluția propusă suportă 700000 de sesiuni noi pe secundă. **Funcționalități:** a) Detectarea și filtrarea traficului pe baza conținutului acestuia; b) Detectarea și atenuarea atacurilor de tip DDoS, pe baza politicilor definite; c) Definirea și aplicarea regulilor de QoS și traffic shaping pentru gestionarea traficului de rețea; d) Definirea și aplicarea politicilor de filtrare web (Web Inspection / Web Filtering); e) Aplicarea politicilor de securitate pentru antispam, antivirus și filtrare web; f) Definirea regulilor de firewall pe baza criteriilor GeoIP; g) Identificarea și controlul aplicațiilor prin mecanisme de Application Control; h) Blocarea traficului către și dinspre adrese BotNet, pe baza listelor actualizate periodic. **Segmentare:** Soluția permite segmentarea logică a sistemului prin alocarea resurselor dedicate, astfel încât fiecare unitate logică dispune de următoarele funcționalități: a) administrarea tabelei de rutare; b) NAT; c) firewall;	

				Segmentare: Soluția trebuie să permită segmentarea logică a sistemului prin alocarea resurselor dedicate, astfel încât fiecare unitate logică să dispună cel puțin de următoarele funcționalități: a) administrarea tabelei de rutare; b) NAT; c) firewall; d) instanțe VPN; e) politici de securitate (Application Control, Web Filtering etc.); f) interfețe fizice și logice dedicate. **Disponibilitate înaltă (High Availability):** Soluția trebuie să îndeplinească cerințele minime pentru asigurarea disponibilității înalte: a) funcționare în mod Active-Active și Active-Passive; b) stateful failover pentru firewall și VPN; c) detectarea și notificarea defectării echipamentelor; d) monitorizarea conexiunilor de rețea; e) mecanisme de link failover. **Monitorizare și management** a) Soluția trebuie să includă funcționalități de monitorizare a componentelor hardware: b) monitorizare grafică în timp real și istorică a parametrilor sistemului; c) suport pentru transmiterea logurilor prin Syslog; d) suport pentru SNMP v1/v2c/v3; e) notificări prin e-mail în cazul apariției alertelor; f) suport pentru exportul statisticilor de trafic prin sFlow și NetFlow. **Endpoint Control** Soluția trebuie să permită integrarea cu un software de securitate instalat pe stațiile utilizatorilor, oferind: a) blocarea traficului generat de aplicațiile instalate pe stații; b) restricționarea și filtrarea accesului web;	d) instanțe VPN; e) politici de securitate (Application Control, Web Filtering etc.); f) interfețe fizice și logice dedicate. **Disponibilitate înaltă (High Availability):** Soluția îndeplinește cerințele minime pentru asigurarea disponibilității înalte: a) funcționare în mod Active-Active și Active-Passive; b) stateful failover pentru firewall și VPN; c) detectarea și notificarea defectării echipamentelor; d) monitorizarea conexiunilor de rețea; e) mecanisme de link failover. **Monitorizare și management:** Soluția include funcționalități de monitorizare a componentelor hardware: a) monitorizare grafică în timp real și istorică a parametrilor sistemului; b) suport pentru transmiterea logurilor prin Syslog; c) suport pentru SNMP v1/v2c/v3; d) notificări prin e-mail în cazul apariției alertelor; e) suport pentru exportul statisticilor de trafic prin sFlow și NetFlow. **Endpoint Control:** Soluția permite integrarea cu FortiClient instalat pe stațiile utilizatorilor, oferind: a) blocarea traficului generat de aplicațiile instalate pe stații; b) restricționarea și filtrarea accesului web; c) scanarea stațiilor pentru identificarea vulnerabilităților; d) scanare antivirus; e) configurarea automată a tunelurilor VPN. **Prevenirea scurgerilor de date (DLP):** Soluția include funcționalități de Data Leak Prevention, care permit: a) blocarea și arhivarea comunicațiilor în cazul detectării tentativelor de scurgere de informații	

				c) scanarea stațiilor pentru identificarea vulnerabilităților; d) scanare antivirus; e) configurarea automată a tunelurilor VPN. **Prevenirea scurgerilor de date (DLP)** Soluția trebuie să includă funcționalități Data Leak Prevention, care să permită: a) blocarea și arhivarea comunicațiilor în cazul detectării tentativelor de scurgere de informații prin protocoalele e-mail, HTTP, FTP, inclusiv variantele criptate SSL; b) blocarea transferului de fișiere în funcție de tipul și dimensiunea acestora. **Autentificare și controlul accesului** Soluția trebuie să ofere mecanisme avansate de autentificare a utilizatorilor, inclusiv: a) definirea locală a utilizatorilor; b) integrarea cu Windows Active Directory (SSO); c) integrarea cu RADIUS, LDAP și TACACS+; d) autentificare în doi factori (2FA) utilizând coduri OTP transmise prin e-mail sau SMS; e) autentificare bazată pe certificate digitale PKI X.509; f) restricționarea accesului în rețea pentru utilizatorii care nu au instalat clientul software de securitate pe stație. **Garanție și suport pentru hardware și software - minimum 36 de luni, asigurate de producător, cu disponibilitate 24/7.**	prin protocoalele e-mail, HTTP, FTP, inclusiv variantele criptate SSL; b) blocarea transferului de fișiere în funcție de tipul și dimensiunea acestora. **Autentificare și controlul accesului:** Soluția oferă mecanisme avansate de autentificare a utilizatorilor, inclusiv: a) definirea locală a utilizatorilor; b) integrarea cu Windows Active Directory (SSO); c) integrarea cu RADIUS, LDAP și TACACS+; d) autentificare în doi factori (2FA) utilizând coduri OTP transmise prin e-mail sau SMS; e) autentificare bazată pe certificate digitale PKI X.509; f) restricționarea accesului în rețea pentru utilizatorii care nu au instalat FortiClient pe stație. **Garanție și suport pentru hardware și software - 36 de luni, asigurat de producător, cu disponibilitate 24/7.**	
Servicii de instalare, configurare, migrare și integrare	Servicii de instalare, configurare, migrare și integrare	Republica Moldova	IT-LAB GRUP SRL	**Ofertantul trebuie să asigure executarea următoarelor lucrări:** a) Elaborarea și convenirea cu Beneficiarul a documentației de proiectare, inclusiv High-Level Design (HLD) și Low-Level Design (LLD); b) Elaborarea politicilor de securitate a rețelei (niveluri de acces la rețea, liste de control al accesului – ACL, securitatea porturilor, VPN, precum și mecanisme de notificare și escaladare a incidentelor de securitate);	**Asigurăm executarea următoarelor lucrări:** a) Elaborarea și convenirea cu Beneficiarul a documentației de proiectare, inclusiv High-Level Design (HLD) și Low-Level Design (LLD); b) Elaborarea politicilor de securitate a rețelei (niveluri de acces la rețea, liste de control al accesului – ACL, securitatea porturilor, VPN, precum și mecanisme de notificare și escaladare a incidentelor de securitate); c) Coordonarea planului de implementare și a tuturor etapelor de migrare către noua infrastructură;	

				c) Coordonarea planului de implementare și a tuturor etapelor de migrare către noua infrastructură; d) Instalarea și configurarea echipamentelor de tip paravan de protecție (firewall). **Ofertantul trebuie să asigure:** e) Livrarea, instalarea și configurarea echipamentelor propuse, precum și integrarea acestora în infrastructura de rețea existentă; f) Configurarea echipamentelor de tip paravan de protecție în regim de funcționare cluster/stack pentru asigurarea redundanței; g) Migrarea configurațiilor de pe echipamentele existente FortiGate 201E, inclusiv: routing, L2TP/IPsec, DMZ, Data Center, OSPF, reguli firewall, VLAN, VDOM, conexiuni site-to-site IPsec, precum și politici NGFW/IPS/Antivirus; h) Configurarea politicilor și regulilor de securitate; i) Segmentarea rețelei pe zone de securitate; j) Configurarea accesului VPN de tip Remote Access pentru minimum 500 utilizatori. **Toate lucrările trebuie realizate fără perturbarea funcționării infrastructurilor existente.**	d) Instalarea și configurarea echipamentelor de tip paravan de protecție (firewall). **Asigurăm:** e) Livrarea, instalarea și configurarea echipamentelor propuse, precum și integrarea acestora în infrastructura de rețea existentă; f) Configurarea echipamentelor de tip paravan de protecție în regim de funcționare cluster/stack pentru asigurarea redundanței; g) Migrarea configurațiilor de pe echipamentele existente FortiGate 201E, inclusiv: routing, L2TP/IPsec, DMZ, Data Center, OSPF, reguli firewall, VLAN, VDOM, conexiuni site-to-site IPsec, precum și politici NGFW/IPS/Antivirus; h) Configurarea politicilor și regulilor de securitate; i) Segmentarea rețelei pe zone de securitate; j) Configurarea accesului VPN de tip Remote Access pentru minimum 500 utilizatori. **Toate lucrările vor fi realizate fără perturbarea funcționării infrastructurilor existente.**	
TOTAL						

Digitally signed by Cioban Alexei
Date: 2026.05.19 18:47:06 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

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

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