**Anexa nr. 22**
**la Documentația standard, aprobată prin**
**Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021**

## Specificaţii tehnice

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

| |
|---|
| **Numărul procedurii de achiziție:** *ocds-b3wdp1-MD-1696424091739 (21097019) din 04.10.2023* |
| **Obiectul achiziției:** *Echipament Fortinet Fortigate 201F sau echivalentul* |

| Denumirea bunurilor/serviciilor | Denumirea modelului bunului | Țara 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 |
| **Echipament Fortinet Fortigate 201F sau echivalentul** | FG-201F-BDL-950-12 | SUA | Fortinet | Tip: Echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificată, inclusiv 12 luni de suport și subscriere de la producător.<br>Cantitatea și cerințe de licențiere:<br>- Este responsabilitatea Ofertantului de a determina modelul de licențiere și cantitatea licențelor.<br>- 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).<br>**Cerințe tehnice:**<br>**Soluția propusă trebuie sa fie o soluție inovatoare, care va asigura următoarele cerințe minime:**<br>**1. Specificații hardware:**<br>• Interfețe GbE RJ-45: 16<br>• Interfețe management/HA/DMZ GbE RJ-45: 1/2/1<br>• Interfete WAN Gbe RJ-45: 2 | Tip: FG-201F– este un echipament integrat de protecție a rețelei ce funcționează ca o soluție de securitate unificată, inclusiv cu 12 luni de suport și subscriere de la producător.<br>Cantitatea și cerințe de licențiere:<br>- Ofertantului va determina modelul de licențiere și cantitatea licențelor.<br>- Toate licențele livrate includ 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).<br>**Cerințe tehnice:**<br>**Soluția propusă este o soluție inovatoare, care va asigura următoarele cerințe minime:**<br>**1. Specificații hardware:**<br>• Interfețe GbE RJ-45: 16<br>• Interfețe management/HA/DMZ GbE RJ-45: 1/2/1<br>• Interfete WAN Gbe RJ-45: 2<br>• Interfete combo RJ45/SFP Gbe: 4 | n/a |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Interfete combo RJ45/SFP Gbe: 4<br>• Sloturi GE SFP: 8<br>• Sloturi 10GE SFP+: 2<br>• Porturi consola RJ-45: 1<br>• Porturi USB: 1<br>• Dimensiune: 1U<br>• Alimentare redundantă<br>• Stocare interna SSD: 1x 480 GB SSD.<br>2. **Caracteristici:**<br>• Trafic firewall (1518/512/64 byte pachete UDP): 27/27/11 Gbps<br>• Latenta Firewall: 4.78 µs<br>• Trafic Firewall măsurat în pachete per secunda: 15 Mpps<br>• Trafic IPSec VPN (512 byte packets): 13 Gbps<br>• Trafic IPS: 5 Gbps<br>• Trafic NGFW: 3.5 Gbps<br>• Performanta SSL Inspection (IPS, HTTP): 3 Gbps<br>• Număr de tunele IPSec VPN site-to-site: 2.000<br>• Număr de clienți IPSec VPN: 16.000<br>• Trafic SSL-VPN: 4 Gbps<br>• Număr de clienți concurenți SSL-VPN: 500<br>• Număr de sesiuni concurente TCP: 3.000.000<br>• Număr de sesiuni noi pe secundă TCP: 280.000<br>• Număr de politici de securitate: 10.000<br>• Număr de instanțe virtuale: 10<br>• Număr de AP-uri administrate (total/tunnel mode): 256/128<br>• Trafic CAPWAP: 20 Gbps<br>• Număr de token-uri OTP administrate: 5.000.<br>**3**. **Funcționalități generale:**<br>• Filtru de SPAM și viruși; Echipament integrat de securitate cu funcționalități simultane de:<br>- Firewall de tip stateful | • Sloturi GE SFP: 8<br>• Sloturi 10GE SFP+: 2<br>• Porturi consola RJ-45: 1<br>• Porturi USB: 1<br>• Dimensiune: 1U<br>• Alimentare redundantă<br>• Stocare interna SSD: 1x 480 GB SSD.<br>2. **Caracteristici:**<br>• Trafic firewall (1518/512/64 byte pachete UDP): 27/27/11 Gbps<br>• Latenta Firewall: 4.78 µs<br>• Trafic Firewall măsurat în pachete per secunda: 15 Mpps<br>• Trafic IPSec VPN (512 byte packets): 13 Gbps<br>• Trafic IPS: 5 Gbps<br>• Trafic NGFW: 3.5 Gbps<br>• Performanta SSL Inspection (IPS, HTTP): 3 Gbps<br>• Număr de tunele IPSec VPN site-to-site: 2.000<br>• Număr de clienți IPSec VPN: 16.000<br>• Trafic SSL-VPN: 4 Gbps<br>• Număr de clienți concurenți SSL-VPN: 500<br>• Număr de sesiuni concurente TCP: 3.000.000<br>• Număr de sesiuni noi pe secundă TCP: 280.000<br>• Număr de politici de securitate: 10.000<br>• Număr de instanțe virtuale: 10<br>• Număr de AP-uri administrate (total/tunnel mode): 256/128<br>• Trafic CAPWAP: 20 Gbps<br>• Număr de token-uri OTP administrate: 5.000.<br>**3**. **Funcționalități generale:**<br>• Filtru de SPAM și viruși; Echipament integrat de securitate cu funcționalități simultane de:<br>- Firewall de tip stateful | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | - Router cu suport pentru protocoale de rutare dinamice<br>- Posibilitate de instalare în mod bridge Ethernet<br>- Protecție Antivirus<br>- Criptare de date: IPSec VPN si SSL VPN<br>- Suport pentru QoS si Traffic Shaping<br>- Detecția si prevenirea intruziunilor – IDS/IPS<br>- Scanare si filtrare WEB – Web Inspection/Filter<br>- Blocarea si controlul traficului din rețea generat de aplicații<br>- Protecție Antispam<br>- Protecție împotriva scurgerii de informații confidențiale<br>- Update-uri automate și în timp real<br>- Suport pentru IPv6 UTM<br>- Funcționalitate de proxy SSL – posibilitatea inspecției traficului criptat<br>- Wireless controller<br>• Toate funcționalitățile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum și platforma hardware aparțin aceluiași producător<br>• Echipamentul firewall trebuie sa asigure management pentru Switch/ Acces Point<br>• Certificări pentru producător și produs: ICSA Labs pentru Firewall, IPSec, SSL VPN, IPS, Antivirus<br>• Conformitate cu: CE, CB.<br>**Funcționalități securitate:**<br>**4. Funcționalități firewall:**<br>• Funcționalități NAT, PAT și Transparent Bridge<br>• Opțiune de a aplica NAT per politica<br>• Suport VLAN Tagging 802.1Q<br>• Autentificarea utilizatorilor pe grupuri<br>• Suport VoIP SIP/H.323/SCCP Traversal NAT<br>• Funcționalitate proxy explicit HTTP/HTTPS și FTP | - Router cu suport pentru protocoale de rutare dinamice<br>- Posibilitate de instalare în mod bridge Ethernet<br>- Protecție Antivirus<br>- Criptare de date: IPSec VPN si SSL VPN<br>- Suport pentru QoS si Traffic Shaping<br>- Detecția si prevenirea intruziunilor – IDS/IPS<br>- Scanare si filtrare WEB – Web Inspection/Filter<br>- Blocarea si controlul traficului din rețea generat de aplicații<br>- Protecție Antispam<br>- Protecție împotriva scurgerii de informații confidențiale<br>- Update-uri automate și în timp real<br>- Suport pentru IPv6 UTM<br>- Funcționalitate de proxy SSL – posibilitatea inspecției traficului criptat<br>- Wireless controller<br>• Toate funcționalitățile de securitate (antivirus, IPS, antispam, Web filtering), tehnologiile incluse, sistemul de operare precum și platforma hardware aparțin aceluiași producător<br>• Echipamentul firewall trebuie sa asigure management pentru Switch/ Acces Point<br>• Certificări pentru producător și produs: ICSA Labs pentru Firewall, IPSec, SSL VPN, IPS, Antivirus<br>• Conformitate cu: CE, CB.<br>**Funcționalități securitate:**<br>**4. Funcționalități firewall:**<br>• Funcționalități NAT, PAT și Transparent Bridge<br>• Opțiune de a aplica NAT per politica<br>• Suport VLAN Tagging 802.1Q<br>• Autentificarea utilizatorilor pe grupuri<br>• Suport VoIP SIP/H.323/SCCP Traversal NAT | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru funcționalitatea proxy explicit<br>• Suport WINS<br>• Suport securitate VoIP ALG (SIP Firewall/RTP Pinholing)<br>• Suport pentru TCP MSS clamping<br>• Suport pentru rescrierea câmpului Class of Service<br>• Suport IPv6 (NAT/mod Transparent)<br>• Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de stație folosit – funcționalitate de tip BYOD (bring your own device)<br>• Opțiune "Scheduling" pentru politicile de firewall<br>• Posibilitate de blocare a traficului după tara de origine a sursei sau destinației (Geo IP)<br>• Mecanism de calcul și afișare al reputației utilizatorilor din rețea pe baza de scor dedus în mod configurabil din activitatea detectata prin mecanismele de inspecție de blocarea a atacurilor, blocare malware, filtrare web, firewall și inspecție a traficului de aplicații.<br>**5. Funcționalități VPN:**<br>• Suport PPTP, L2TP, IPSec, L2TP over IPSec, SSL-VPN<br>• Criptare DES, 3DES, AES 128, AES 192, AES 256<br>• Autentificare MD5, SHA-1, SHA-256, SHA-384, SHA-512<br>• Suport pentru PPTP și L2TP VPN Client Pass Through<br>• Funcționalitate "Hub and Spoke" IPSec VPN<br>• Autentificare IKE prin certificate X.509 - suport pentru RSA și ECDSA<br>• Suport IPSec Xauth NAT Traversal<br>• Suport configurare IPSec automata<br>• Funcționalitate IKE Dead Peer Detection<br>• Suport pentru RSA SecureID | • Funcționalitate proxy explicit HTTP/HTTPS și FTP<br>• Suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru funcționalitatea proxy explicit<br>• Suport WINS<br>• Suport securitate VoIP ALG (SIP Firewall/RTP Pinholing)<br>• Suport pentru TCP MSS clamping<br>• Suport pentru rescrierea câmpului Class of Service<br>• Suport IPv6 (NAT/mod Transparent)<br>• Politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare de stație folosit – funcționalitate de tip BYOD (bring your own device)<br>• Opțiune "Scheduling" pentru politicile de firewall<br>• Posibilitate de blocare a traficului după tara de origine a sursei sau destinației (Geo IP)<br>• Mecanism de calcul și afișare al reputației utilizatorilor din rețea pe baza de scor dedus în mod configurabil din activitatea detectata prin mecanismele de inspecție de blocarea a atacurilor, blocare malware, filtrare web, firewall și inspecție a traficului de aplicații.<br>**5. Funcționalități VPN:**<br>• Suport PPTP, L2TP, IPSec, L2TP over IPSec, SSL-VPN<br>• Criptare DES, 3DES, AES 128, AES 192, AES 256<br>• Autentificare MD5, SHA-1, SHA-256, SHA-384, SHA-512<br>• Suport pentru PPTP și L2TP VPN Client Pass Through<br>• Funcționalitate "Hub and Spoke" IPSec VPN<br>• Autentificare IKE prin certificate X.509 - suport pentru RSA și ECDSA<br>• Suport IPSec Xauth NAT Traversal | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Suport Single-Sign-On pentru book-mark-uri portal SSL-VPN<br>• Funcționalitate Two-Factor Authentication pentru SSL-VPN<br>• Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN)<br>• Suport tunele SSL în mod tunel și în mod portal<br>• Suport pentru validarea clienților SSL VPN prin verificarea aplicațiilor instalate pe stație înainte de conectare - compatibilitate cu sistemele de operare Windows<br>• Suport pentru limitarea aplicațiilor utilizabile pe stațiile clienților SSL VPN după conectare - compatibilitate cu sistemele de operare Windows<br>• Suport pentru izolarea datelor utilizate în cadrul sesiunii SSL VPN de restul aplicațiilor ce rulează pe stațiile utilizatorilor și ștergerea acestora după terminarea sesiunii SSL VPN - compatibilitate cu sistemele de operare Windows<br>• Suport pentru autentificarea utilizatorilor de tip Single Sign On prin portalul SSL VPN<br>• Funcționalități monitorizare tunele VPN.<br>**6. Funcționalități Antivirus:**<br>• Filtru de SPAM și viruși; Protecție anti-malware (virus, troian, worm, spyware, grayware)<br>• Protocoale suportate: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S IMAP/IMAPS, MAPI, FTP<br>• Suport scanare antivirus Proxy-Based și Flow-Based<br>• Opțiune pentru detecția malware prin sandboxing de tip Cloud-Based al fișierelor suspecte, oferita de producător<br>• Update-uri automate de semnături malware<br>• Protecție împotriva rețelelor botnet și site-urilor de tip phishing pe baza de reputație a | • Suport configurare IPSec automata<br>• Funcționalitate IKE Dead Peer Detection<br>• Suport pentru RSA SecureID<br>• Suport Single-Sign-On pentru book-mark-uri portal SSL-VPN<br>• Funcționalitate Two-Factor Authentication pentru SSL-VPN<br>• Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN)<br>• Suport tunele SSL în mod tunel și în mod portal<br>• Suport pentru validarea clienților SSL VPN prin verificarea aplicațiilor instalate pe stație înainte de conectare - compatibilitate cu sistemele de operare Windows<br>• Suport pentru limitarea aplicațiilor utilizabile pe stațiile clienților SSL VPN după conectare - compatibilitate cu sistemele de operare Windows<br>• Suport pentru izolarea datelor utilizate în cadrul sesiunii SSL VPN de restul aplicațiilor ce rulează pe stațiile utilizatorilor și ștergerea acestora după terminarea sesiunii SSL VPN - compatibilitate cu sistemele de operare Windows<br>• Suport pentru autentificarea utilizatorilor de tip Single Sign On prin portalul SSL VPN<br>• Funcționalități monitorizare tunele VPN.<br>**6. Funcționalități Antivirus:**<br>• Filtru de SPAM și viruși; Protecție anti-malware (virus, troian, worm, spyware, grayware)<br>• Protocoale suportate: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S IMAP/IMAPS, MAPI, FTP<br>• Suport scanare antivirus Proxy-Based și Flow-Based<br>• Opțiune pentru detecția malware prin sandboxing de tip Cloud-Based al fișierelor suspecte, oferita de producător<br>• Update-uri automate de semnături malware | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | adreselor IP și a URL-urilor accesate de utilizatori.<br>**7. Funcționalități filtrare trafic WEB:**<br>• Filtrare pentru protocoalele HTTP si HTTPS<br>• Filtrare după categorii site-uri/URL-uri<br>• Funcționalitate de contorizare a timpului de acces sau a volumului de trafic pentru utilizatori – definire de cote de utilizare<br>• Blocare a conexiunilor în funcție de URL/cuvânt cheie sau expresie în conținutul paginilor web<br>• Blocare a conexiunilor în funcție de URL-ul din header-ul Referer al cererii HTTP<br>• Filtrare pentru Java Applet, Cookies, scripturi Active X<br>• Posibilitate de activare forțată a opțiunii „Safe Search" pentru motoare de căutare web<br>• Posibilitatea de modificare a header-elor HTTP din cererile generate de utilizatori<br>• Funcționalitate de monitorizare a activității web a utilizatorilor<br>• Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor în cadrul unui browser web, privind paginile web blocate.<br>**8. Funcționalități sistem de control al aplicațiilor:**<br>• Identificarea și controlul a peste 3000 de aplicații<br>• Opțiune de Traffic-Shaping per aplicație<br>• Control specific pentru aplicațiile de tip IM/P2P<br>• Clasificare granulara a aplicațiilor după criterii multiple precum: Categorii de aplicații, Popularitate, Tehnologie și Risc<br>• Monitorizare aplicațiilor cu rata cea mai mare de consum de banda<br>• Monitorizarea aplicațiilor pe baza IP/Utilizator<br>• Suport pentru decriptarea și inspectarea sesiunilor SSH | • Protecție împotriva rețelelor botnet și site-urilor de tip phishing pe baza de reputație a adreselor IP și a URL-urilor accesate de utilizatori.<br>**7. Funcționalități filtrare trafic WEB:**<br>• Filtrare pentru protocoalele HTTP si HTTPS<br>• Filtrare după categorii site-uri/URL-uri<br>• Funcționalitate de contorizare a timpului de acces sau a volumului de trafic pentru utilizatori – definire de cote de utilizare<br>• Blocare a conexiunilor în funcție de URL/cuvânt cheie sau expresie în conținutul paginilor web<br>• Blocare a conexiunilor în funcție de URL-ul din header-ul Referer al cererii HTTP<br>• Filtrare pentru Java Applet, Cookies, scripturi Active X<br>• Posibilitate de activare forțată a opțiunii „Safe Search" pentru motoare de căutare web<br>• Posibilitatea de modificare a header-elor HTTP din cererile generate de utilizatori<br>• Funcționalitate de monitorizare a activității web a utilizatorilor<br>• Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor în cadrul unui browser web, privind paginile web blocate.<br>**8. Funcționalități sistem de control al aplicațiilor:**<br>• Identificarea și controlul a peste 3000 de aplicații<br>• Opțiune de Traffic-Shaping per aplicație<br>• Control specific pentru aplicațiile de tip IM/P2P<br>• Clasificare granulara a aplicațiilor după criterii multiple precum: Categorii de aplicații, Popularitate, Tehnologie și Risc<br>• Monitorizare aplicațiilor cu rata cea mai mare de consum de banda<br>• Monitorizarea aplicațiilor pe baza IP/Utilizator | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Suport pentru blocarea aplicațiilor utilizate în cadrul rețelelor de tip Botnet<br>• Posibilitate de definire a semnăturilor de aplicație personalizate<br>• Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor în cadrul unui browser web, privind traficul de aplicații blocat.<br>**9. Funcționalități sistem de prevenire a intruziunilor/atacurilor (IPS):**<br>• Protecție pentru peste 10.000 de semnături de atac<br>• Suport pentru inspecția traficului de aplicație criptat prin protocolul SSL<br>• Protecție pentru atacuri de tip brute force<br>• Detectarea anomaliilor de protocol<br>• Suport pentru semnături configurabile<br>• Update-uri automate pentru semnături<br>• Suport pentru IPv4 și IPv6 DoS/DDoS.<br>**10. Funcționalități Antispam:**<br>• Scanare pentru SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI<br>• Suport RBL/ORDBL<br>• Inspecție header MIME<br>• Filtrare după cuvinte cheie/expresie<br>• Filtrare după Black/White List pentru adrese IP și e-mail<br>• Update-uri automate și în timp real.<br>**11. Funcționalitate Data Leak Prevention:**<br>• In caz de scurgere de informații trebuie sa permită blocarea și arhivarea conversației pe protocoale de email, HTTP, FTP și variantele criptate SSL;<br>• Blocare după tip și dimensiune fișier<br>• DLP fingerprint și arhivare.<br>**12. Funcționalități sistem de verificare a stațiilor (Endpoint Control):**<br>• Integrare cu o aplicație software pentru securitate ce rulează pe stații care sa permită:<br>- Blocarea traficului de aplicații instalate pe stații<br>- Restricționarea/filtrarea accesului web<br>- Scanarea pentru vulnerabilități a stațiilor | • Suport pentru decriptarea și inspectarea sesiunilor SSH<br>• Suport pentru blocarea aplicațiilor utilizate în cadrul rețelelor de tip Botnet<br>• Posibilitate de definire a semnăturilor de aplicație personalizate<br>• Posibilitate de înștiințare a utilizatorilor, prin afișarea informațiilor în cadrul unui browser web, privind traficul de aplicații blocat.<br>**9. Funcționalități sistem de prevenire a intruziunilor/atacurilor (IPS):**<br>• Protecție pentru peste 10.000 de semnături de atac<br>• Suport pentru inspecția traficului de aplicație criptat prin protocolul SSL<br>• Protecție pentru atacuri de tip brute force<br>• Detectarea anomaliilor de protocol<br>• Suport pentru semnături configurabile<br>• Update-uri automate pentru semnături<br>• Suport pentru IPv4 și IPv6 DoS/DDoS.<br>**10. Funcționalități Antispam:**<br>• Scanare pentru SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI<br>• Suport RBL/ORDBL<br>• Inspecție header MIME<br>• Filtrare după cuvinte cheie/expresie<br>• Filtrare după Black/White List pentru adrese IP și e-mail<br>• Update-uri automate și în timp real.<br>**11. Funcționalitate Data Leak Prevention:**<br>• In caz de scurgere de informații trebuie sa permită blocarea și arhivarea conversației pe protocoale de email, HTTP, FTP și variantele criptate SSL;<br>• Blocare după tip și dimensiune fișier<br>• DLP fingerprint și arhivare.<br>**12. Funcționalități sistem de verificare a stațiilor (Endpoint Control):**<br>• Integrare cu o aplicație software pentru securitate ce rulează pe stații care sa permită: | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | - Scanare Antivirus<br>- Configurarea automata pentru tunele VPN.<br>**Funcționalități rețea:**<br>**13. Funcționalități rețea și rutare:**<br>• SD-WAN-control inteligent al interfeței WAN, prin direcționarea traficului prin aceasta având link-uri configurate care pot susține peste 5000 de aplicații și utilizatori/grupuri de utilizatori. Suport pentru legături WAN multiple cu balansare a traficului după metodele:<br>- Weighted round robin a sesiunilor, împărțire proporțională a volumului de trafic, prin limitarea per interfață a benzii maxime utilizabile, după calitatea conexiunii ISP (jitter sau latenta).<br>• Suport PPPoE și DHCP Client/Server<br>• Rute statice<br>• Rutare dinamica IPv4: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS<br>• Rutare dinamica IPv6: RIPng, OSPF v3, BGP 4+<br>• Gruparea interfețelor în zone de securitate<br>• Rutare intre zonele de securitate<br>• Policy-based routing<br>• Suport VRRP și Link Failure Control<br>• Suport VLAN Tagging (802.1q)<br>• Rutare intre VLAN-uri<br>• Suport pentru IPv6 (Firewall, DNS, SIP)<br>• Posibilitate mapare (Binding) adrese IP – adrese MAC<br>• Suport One-to-One NAT<br>• Tunelare IP în IP<br>• Suport NAT64, DNS64, NAT46, NAT66<br>• Suport LLDP.<br>**14. Funcționalitate Wireless Controller:**<br>• Modul wireless controller pentru thin-AP-uri integrat cu următoarele funcționalități:<br>- Detecție și suprimare a AP-urilor neînregistrate în controller; | - Blocarea traficului de aplicații instalate pe stații<br>- Restricționarea/filtrarea accesului web<br>- Scanarea pentru vulnerabilități a stațiilor<br>- Scanare Antivirus<br>- Configurarea automata pentru tunele VPN.<br>**Funcționalități rețea:**<br>**13. Funcționalități rețea și rutare:**<br>• SD-WAN-control inteligent al interfeței WAN, prin direcționarea traficului prin aceasta având link-uri configurate care pot susține peste 5000 de aplicații și utilizatori/grupuri de utilizatori. Suport pentru legături WAN multiple cu balansare a traficului după metodele:<br>- Weighted round robin a sesiunilor, împărțire proporțională a volumului de trafic, prin limitarea per interfață a benzii maxime utilizabile, după calitatea conexiunii ISP (jitter sau latenta).<br>• Suport PPPoE și DHCP Client/Server<br>• Rute statice<br>• Rutare dinamica IPv4: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS<br>• Rutare dinamica IPv6: RIPng, OSPF v3, BGP 4+<br>• Gruparea interfețelor în zone de securitate<br>• Rutare intre zonele de securitate<br>• Policy-based routing<br>• Suport VRRP și Link Failure Control<br>• Suport VLAN Tagging (802.1q)<br>• Rutare intre VLAN-uri<br>• Suport pentru IPv6 (Firewall, DNS, SIP)<br>• Posibilitate mapare (Binding) adrese IP – adrese MAC<br>• Suport One-to-One NAT<br>• Tunelare IP în IP<br>• Suport NAT64, DNS64, NAT46, NAT66<br>• Suport LLDP.<br>**14. Funcționalitate Wireless Controller:** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | - Selecție automata a canalului pentru AP în funcție de interferentele din mediu;<br>- Suport pentru SSID-uri multiple;<br>- Autentificare WEP, WPA, WPA2, WPA2 Enterprise, 802.1x<br>- Suport Captive Portal;<br>- Funcționalitate de gestionare a conturilor de tip guest prin intermediul unei interfețe web diferita de interfața pentru administrare globala;<br>- Suport pentru Wireless Mesh si roaming;<br>- Distribuire automata a clienților wireless per AP sau banda de frecvente pentru a obține performante optime.<br>- Rutare dinamica a traficului generat de utilizatorii wireless prin VLAN-uri folosind autentificare prin RADIUS<br>- Autentificare suplimentara a clienților wireless prin RADIUS pe baza adresei MAC<br>- Suport pentru RADIUS Accounting<br>- Posibilitatea gestionarii AP-urilor remote de către controller dar cu rutarea traficului printr-un gateway local<br>- Wireless IDS<br>- Monitorizarea activa a utilizării spectrului de frecvente radio.<br>**15. Funcționalități Traffic Shaping:**<br>• Limitare/garantare/prioritizare a benzii de trafic prin politici<br>• Traffic Shaping per aplicație și adresa IP<br>• Suport pentru DSCP<br>• Limitare a cotei de trafic (per adresa IP)<br>• Suport pentru ToS.<br>**16. Funcționalități High Availability - HA:**<br>• Funcționare Active-Active, Active-Passive<br>• Funcționalitate Stateful Failover (Firewall si VPN)<br>• Detectare și notificare pentru echipament nefuncțional<br>• Monitorizarea conexiunii la rețea<br>• Funcționalitate Link Failover. | • Modul wireless controller pentru thin-AP-uri integrat cu următoarele funcționalități:<br>- Detecție și suprimare a AP-urilor neînregistrate în controller;<br>- Selecție automata a canalului pentru AP în funcție de interferentele din mediu;<br>- Suport pentru SSID-uri multiple;<br>- Autentificare WEP, WPA, WPA2, WPA2 Enterprise, 802.1x<br>- Suport Captive Portal;<br>- Funcționalitate de gestionare a conturilor de tip guest prin intermediul unei interfețe web diferita de interfața pentru administrare globala;<br>- Suport pentru Wireless Mesh si roaming;<br>- Distribuire automata a clienților wireless per AP sau banda de frecvente pentru a obține performante optime.<br>- Rutare dinamica a traficului generat de utilizatorii wireless prin VLAN-uri folosind autentificare prin RADIUS<br>- Autentificare suplimentara a clienților wireless prin RADIUS pe baza adresei MAC<br>- Suport pentru RADIUS Accounting<br>- Posibilitatea gestionarii AP-urilor remote de către controller dar cu rutarea traficului printr-un gateway local<br>- Wireless IDS<br>- Monitorizarea activa a utilizării spectrului de frecvente radio.<br>**15. Funcționalități Traffic Shaping:**<br>• Limitare/garantare/prioritizare a benzii de trafic prin politici<br>• Traffic Shaping per aplicație și adresa IP<br>• Suport pentru DSCP<br>• Limitare a cotei de trafic (per adresa IP)<br>• Suport pentru ToS.<br>**16. Funcționalități High Availability - HA:**<br>• Funcționare Active-Active, Active-Passive | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **Funcționalități de administrare, logare, autentificare a utilizatorilor:**<br>**17. Funcționalități de administrare:**<br>• Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI)<br>• Posibilitatea de administrare dintr-un portal cloud-based oferit de producător<br>• Utilizatori/Administratori cu drepturi configurabile<br>• Funcționalitate de export/import a configurației<br>• Politica de control a parolelor.<br>**18. Funcționalități de logare și monitorizare:**<br>• Opțiune de păstrare a log-urilor pe memoria internă.<br>**19. Funcționalități de autentificare a utilizatorilor:**<br>• Definire locala a utilizatorilor<br>• Integrare cu Windows Active Directory (AD) pentru Single Sign On<br>• Integrare cu Citrix pentru autentificare SSO a utilizatorilor<br>• Integrare cu RADIUS/LDAP/TACACS+/POP3<br>• Suport Xauth pentru IPSec VPN<br>• Suport pentru autentificarea grupurilor de utilizatori prin LDAP<br>• Suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS<br>• Suport pentru autentificare prin certificate digitale PKI X.509<br>• Posibilitatea limitării accesului utilizatorilor în rețea ce nu au instalat un client software de stație (client endpoint).<br>**20. Condiții de alimentare:**<br>• Alimentare curent alternativ 100-240V, 50-60 Hz<br>• Consum maxim de putere: 121.94 W. | • Funcționalitate Stateful Failover (Firewall si VPN)<br>• Detectare și notificare pentru echipament nefuncțional<br>• Monitorizarea conexiunii la rețea<br>• Funcționalitate Link Failover.<br>**Funcționalități de administrare, logare, autentificare a utilizatorilor:**<br>**17. Funcționalități de administrare:**<br>• Administrare prin WEB UI, Secure Command Shell (SSH) si Command Line Interface (CLI)<br>• Posibilitatea de administrare dintr-un portal cloud-based oferit de producător<br>• Utilizatori/Administratori cu drepturi configurabile<br>• Funcționalitate de export/import a configurației<br>• Politica de control a parolelor.<br>**18. Funcționalități de logare și monitorizare:**<br>• Opțiune de păstrare a log-urilor pe memoria internă.<br>**19. Funcționalități de autentificare a utilizatorilor:**<br>• Definire locala a utilizatorilor<br>• Integrare cu Windows Active Directory (AD) pentru Single Sign On<br>• Integrare cu Citrix pentru autentificare SSO a utilizatorilor<br>• Integrare cu RADIUS/LDAP/TACACS+/POP3<br>• Suport Xauth pentru IPSec VPN<br>• Suport pentru autentificarea grupurilor de utilizatori prin LDAP<br>• Suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS<br>• Suport pentru autentificare prin certificate digitale PKI X.509 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **21. Condiții de mediu:**<br>• Temperatura de operare: 0 – 40 grade Celsius<br>• Umiditate: 10–90 %, fără condens.<br>**22. Garanție si suport:**<br>• Solutia va beneficia de minimum un an ce va include:<br>• Înlocuirea echipamentului în caz de defecțiune hardware<br>• Suport tehnic din partea producătorului 7 zile pe săptămâna, 24 de ore pe zi, în regim Next Business Day<br>• Update firmware versiuni minore și majore<br>• Soluția va beneficia de update-uri automate de semnături de securitate pentru îndeplinirea funcționalităților de Antivirus, Web Filtering, Antispam, Application Control și IPS timp de minimum trei ani.<br>**<u>Alte cerințe obligatorii:</u> Costul ofertei trebuie să includă activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției.**<br>**În echipament trebuie sa fie prezent un controler Wi-Fi integrat și compatibil cu următoarele echipamente, care fac parte din rețeaua Wi-Fi a agenției: 1. FortiAP14C; 2. FortiAP21D; 3. FortiAP24D** | • Posibilitatea limitării accesului utilizatorilor în rețea ce nu au instalat un client software de stație (client endpoint).<br>**20. Condiții de alimentare:**<br>• Alimentare curent alternativ 100-240V, 50-60 Hz<br>• Consum maxim de putere: 121.94 W.<br>**21. Condiții de mediu:**<br>• Temperatura de operare: 0 – 40 grade Celsius<br>• Umiditate: 10–90 %, fără condens.<br>**22. Garanție si suport:**<br>• Solutia va beneficia de minimum un an ce va include:<br>• Înlocuirea echipamentului în caz de defecțiune hardware<br>• Suport tehnic din partea producătorului 7 zile pe săptămâna, 24 de ore pe zi, în regim Next Business Day<br>• Update firmware versiuni minore și majore<br>• Soluția va beneficia de update-uri automate de semnături de securitate pentru îndeplinirea funcționalităților de Antivirus, Web Filtering, Antispam, Application Control și IPS timp de minimum trei ani.<br>**<u>Alte cerințe obligatorii:</u> Costul ofertei include activitățile de instalare, configurare (inclusiv configurarea politicilor inițiale), punerea în funcțiune a soluției.**<br>**În echipament va fi prezent un controler Wi-Fi integrat și compatibil cu următoarele echipamente, care fac parte din rețeaua Wi-Fi a agenției: 1. FortiAP14C; 2. FortiAP21D; 3. FortiAP24D** | |

Nume: **Anatolie BULGARU**
Poziția: Șef Diviziunea Suport și Elaborare Servicii IoT și ICT.
Data: 12.10.2023
Locul: Chișinău Republica Moldova

**Anexa nr. 23**
**la Documentația standard, aprobată prin**
**Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021**

## Specificații de preț

*[Acest tabel va fi completat de către ofertant în coloanele 5,6,7,8 și 11 la necesitate, iar de către autoritatea contractantă – în coloanele 1,2,3,4,9,10]*

**Numărul procedurii de achiziție:** *ocds-b3wdp1-MD-1696424091739 (21097019) din 04.10.2023*

**Obiectul achiziției:** *Echipament Fortinet Fortigate 201F sau echivalentul*

| Cod CPV | Denumirea bunurilor | Unitatea de măsură | Canti-tatea | Preț unitar, lei fără TVA | Preț unitar, lei cu TVA | Suma, lei fără TVA | Suma, lei cu TVA | Termenul de livrare/prestare | Clasificație bugetară (IBAN) |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **32420000-3** | **Echipament Fortinet Fortigate 201F** | **Buc.** | **1** | 196,063.92 | 235,276.70 | 196,063.92 | 235,276.70 | În termen de 60 zile din data intrării în vigoare a contractului (data înregistrării contractului la una din Trezoreriile Regionale ale Ministerului Finanțelor | 314110 |
| | **TOTAL** | | | | | **196,063.92** | **235,276.70** | | |

Nume: **Anatolie BULGARU**
Poziția: Șef Diviziunea Suport și Elaborare Servicii IoT și ICT.
Data: 12.10.2023
Locul: Chișinău Republica Moldova

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

# AGENŢIA SERVICII PUBLICE

Departamentul înregistrare şi licenţiere a unităţilor de drept

## EXTRAS

**din Registrul de stat al persoanelor juridice**

Nr. **526338** data **13.07.2023**

Denumirea completă: **Întreprinderea Mixtă "ORANGE MOLDOVA" S.A.**
Denumirea prescurtată: **Î.M. "ORANGE MOLDOVA" S.A.**
Forma juridică de organizare: **Societate pe acţiuni de tip închis,**
Numărul de identificare de stat şi codul fiscal (IDNO): **1003600106115**
Data înregistrării de stat: **18.03.1998**
Modul de constituire: **nou creată.**
Succesiunea în drept: Întreprinderea Mixtă "ORANGE MOLDOVA" S.A., IDNO 1003600106115 din 18.03.1998, este succesoarea tuturor drepturilor şi obligaţiunilor Societăţii cu Răspundere Limitată "SUN COMMUNICATIONS", (IDNO 1003600061928) ca urmare a reorganizării acesteia prin fuziune (absorbţie) în conformitate cu Contractul de fuziune din 25.04.2023 şi Actul de transmitere (primire-predare) din 25.04.2023.
Sediul: **MD-2071, str. Alba-Iulia, 75, mun. Chişinău, Republica Moldova.** tel.

Obiectul principal de activitate:
**1. Telecomunicaţii**
**2. Repararea aparatelor de radio şi televiziune**

Capitalul social: **179499609** lei,

Administrator: **SURUGIU OLGA, IDNP 0981202021274, în funcţie pînă la data de 31.03.2025**

Prezentul extras este eliberat în temeiul art.34 al Legii nr.220-XVI din 19 octombrie 2007 privind înregistrarea de stat a persoanelor juridice şi a întreprinzătorilor individuali şi confirmă datele din Registrul de stat la data de: **13.07.2023**.

**Registrator în domeniul înregistrării de stat** **Novac Stela**

INSTITUŢIA PUBLICĂ "AGENŢIA SERVICII PUBLICE" IDNO 1002600024700 REPUBLICA MOLDOVA CHIŞINĂU 158

EB 0435055

Date cu caracter personal

REPUBLICA MOLDOVA

# CERTIFICAT DE ÎNREGISTRARE

**ÎNTREPRINDEREA MIXTĂ "ORANGE MOLDOVA" S.A.**
ESTE ÎNREGISTRATĂ LA CAMERA ÎNREGISTRĂRII DE STAT

*Numărul de identificare de stat - codul fiscal*
**1003600106115**

*Data înregistrării* **18.03.1998**

*Data eliberării* **24.04.2007**

**Bolboceanu Adela, registrator de stat**
*Funcția, numele, prenumele persoanei care a eliberat certificatul*

*semnătura*

MINISTERUL DEZVOLTĂRII INFORMAȚIONALE AL REPUBLICII MOLDOVA
CAMERA ÎNREGISTRĂRII DE STAT
1004600077777
109

MD 0067000

maib

**Dnei Olga Surugiu**
**Director General Î.M. "ORANGE MOLDOVA" S.A.**

C180/E01851
13 septembrie 2023

CERTIFICAT

Prin prezenta, BC "MAIB" S.A. confirmă datele bancare pentru Î.M. "ORANGE MOLDOVA" S.A.:

| | |
|---|---|
| Beneficiar: | Î.M. "ORANGE MOLDOVA" S.A.<br>IDNO 1003600106115 |
| IBAN: | IBAN MD64AG000000225110801767 |
| Banca Beneficiară: | BC "MAIB" S.A.<br>Sucursala Petru Movila |
| BIC: | AGRNMD2X |

Certificatul este eliberat la solicitarea titularului de cont, pentru a fi prezentat la cerere.

Prezentul certificat este eliberat în scop informativ şi nu prezintă careva obligaţiuni financiare din partea Băncii.

**Vladimir Bîrsan,**
Șef al Departamentului Clienți Corporativi


Ex. Svetlana Veleşcu
Tel: 022 303 369

1313 | /373/ 22 450 603
aib@maib.md
maib.md

BC "MAIB" SA
Str. Constantin Tănase 9/1, mun. Chișinău, Republica Moldova
Numărul înregistrării de stat - 1 002 600 003 778
Mărimea capitalului social - 207 526 800 lei
Președinte al Comitetului de Conducere - Giorgi Shagidze

Anexa nr. 2
la Regulamentul cu privire la achizițiile
publice de valoare mică

# DECLARAŢIE DE ELIGIBILITATE

Către: **Agenția de Stat pentru Proprietatea Intelectuală (AGEPI)**

**Stimaţi domni**,

Subsemnatul, reprezentant împuternicit al Î.M. Orange Moldova S.A., în calitate de ofertant, declar pe propria răspundere, sub sancțiunea excluderii din procedură și sub sancțiunile aplicate faptei de fals în acte publice, că nu mă aflu în una dintre situațiile prevăzute la art. 19 din Legea nr. 131/2015 privind achizițiile publice.

Mă oblig, la solicitarea autorității/entității contractante, în scopul verificării și confirmării declarației, să prezint orice document doveditor de care dispun.

Nume: **Anatolie BULGARU**
Poziția: Șef Diviziunea Suport și Elaborare Servicii IoT și ICT.
Data: 12.10.2023
Locul: Chișinău Republica Moldova

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

FORTINET

FAST.SECURE.GLOBAL.

CONTRACT DE DISTRIBUȚIE

Prezentul Contract de Distribuție („Contractul") este încheiat în 28 noiembrie 2018 („Data intrării în vigoare") între **Fortinet, Inc.,** cu sediul în 899 Kifer Road, Sunnyvale, CA 94086, SUA și **Fortinet Singapore Private Limited**, cu sediul în 8 Temasek Boulevard no.12-01 Suntec Tower 3, 038988 (fiecare denumită în continuare „Fortinet") și **S.C. Netsafe Distribution SRL**, o corporație cu sediul în Str. Grădina Botanică 14/3, MD Chișinău, Republica Moldova („Distribuitor").

PREAMBUL

AVÂND ÎN VEDERE că Fortinet este furnizor de produse și servicii de securitate a rețelei și alte produse și servicii care sunt descrise în acest Contract; și

AVÂND ÎN VEDERE că Distribuitorul dorește să fie numit un comerciant neexclusiv și distribuitor al unora sau toate Produsele, în teritoriul specificat în acest Contract și Fortinet dorește să facă această numire în termenii din acest Contract;

PRIN URMARE, Fortinet și Distribuitorul sunt de acord, având în vedere înțelegerile reciproce conținute în acest Contract și pentru buna și valoroasa considerație, a căror primire și suficiență sunt recunoscute, să încheie acest Contract în următoarele condiții:

1. DEFINIȚII

Următoarele definiții se vor aplica la termenii cu majuscule din acest Contract. Toți ceilalți termeni cu majuscule sunt definiți în corpul acestui Contract. Termenii „zile" și „luni" se referă la zilele calendaristice și lunile în Teritoriu, în loc de zile lucrătoare și luni lucrătoare, cu excepția cazului în care sunt menționate expres altfel.

1.1. „Codul de conduită" înseamnă Codul de Conduită în afaceri și Etică al Fortinet, așa cum este publicat pe site-ul Fortinet, care poate fi actualizat la alegerea Fortinet.

1.2. „Informații confidențiale" înseamnă orice informații confidențiale divulgate de o Parte celeilalte Părți, inclusiv (fără limitare): (i) produse sau servicii confidențiale, design, tehnologie, idei și algoritmi (de reținut design, tehnologie, idei și algoritmi în Produsele și Serviciile Fortinet și Software și componente legate de aceste produse și servicii, vor fi considerate „Informațiile confidențiale" ale Fortinet); (ii) secrete comerciale; (iii) informațiile și planurile tehnice, comerciale sau financiare ale oricăreia din Părțile la acest contract; și (iv) termenii acestui Contract; și (v) orice articol marcat drept confidențial de către Partea divulgatoare. Cu excepția celor de mai sus, Informațiile confidențiale nu vor include informațiile pe care Partea primitoare le poate dovedi: (a) sunt sau au devenit de domeniul public sau cunoscute sau disponibile publicului nu din vina Părții primitoare; (b)

*DISTRIBUITOR AUTORIZAT FORTINET,*
**Netsafe Distribution SRL**

10.10.2023

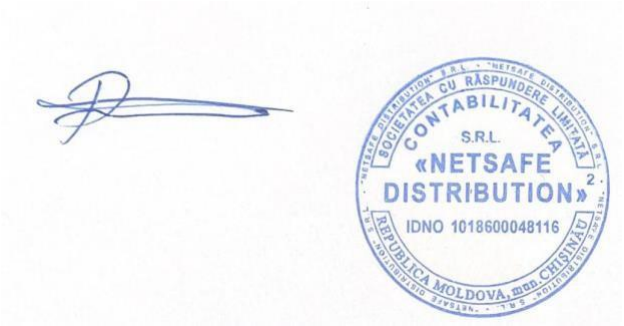
Catre: Agenţia de Stat pentru Proprietatea Intelectuală “AGEPI”

**AUTORIZARE**

Noi, Netsafe Distribution SRL, cu sediul in Chisinau, Str. Gradina Botanica 14/3, Moldova, ca distribuitori autorizati de produse FORTINET si servicii atasate acestora, confirmam prin prezenta ca Î.M. “Orange Moldova” S.A.- str. Alba Iulia nr. 75, Chishinau, Republica Moldova este partener autorizat Fortinet.
Î.M. “Orange Moldova” S.A. in calitate de centru de service local in Moldova poate oferi produsele si serviciile Fortinet.

.

Distribuitor autorizat Fortinet,
Netsafe Distribution SRL
Administrator: Guțuleac Robert



**Către:** Agenția de Stat pentru Proprietatea Intelectuală (AGEPI)
**Achiziție cu costuri mici:** Privind achiziționarea Echipament Fortinet Fortigate 201F sau echivalentul

12 octombrie 2023

**DECLARAȚIE**

privind includerea în Lista producătorilor de produse supuse reglementărilor de responsabilitate extinsă a producătorilor

Prin prezenta Declarație, compania ”Orange MOLDOVA” S.A. declară pe proprie răspundere că:

în temeiul art. 12 alin. (15) Legea nr. 209 din 29 iulie 2016 privind deșeurile (Monitorul Oficial al Republicii Moldova, 2016, nr. 459-471, art. 916), este inclusă în Lista producătorilor de produse supuse reglementărilor de responsabilitate extinsă a producătorilor, în condițiile pct. 111 din Regulamentul privind deșeurile de echipamente electrice și electronice, aprobat prin HG nr. 212 din 07.03.2018.

Numărul de Înregistrare: MD2022-5-EEE-001

şi în temeiul art. 49 alin. (13) Legea nr. 209/2016 privind deșeurile (Monitorul Oficial al Republicii Moldova, 2016, nr. 459-471, art. 916), este inclusă în Lista producătorilor de produse supuse reglementărilor de responsabilitate extinsă a producătorilor, în condițiile pct. 42 din Regulamentului privind gestionarea bateriilor și acumulatorilor și deșeurilor de baterii și acumulatori, aprobat prin HG nr. 586 din 31.07.2020.

Numărul de Înregistrare: MD2022-2-BA-002

Data completării 12.10.2023
Anatolie BULGARU
Șef Diviziunea Suport și Elaborare Servicii IoT și ICT
Î.M. „Orange Moldova” S.A.

Despre SIAMD
Cadrul legal
Lista producătorilor
Ambalaje
Baterii și acumulatoare
Echipamente electrice și electronice
Uleiuri
Vehicule

# Lista producătorilor de deșeuri electrice și electrocasnice

Export pagină curentă

orange

| Nr. în Listă | Data fondării | Persoana juridică | IDNO | Data înregistrării | Identificarea | Adresa juridică |
|---|---|---|---|---|---|---|
| MD2022-5-EEE-001 | 1998-03-18 | ORANGE MOLDOVA SA | 1003600106115 | 2022-05-10 | Producător | mun. Chișinău, str. Alba-Iulia 75 |

Despre SIAMD
Cadrul legal
Lista producătorilor
Ambalaje
Baterii și acumulatoare
Echipamente electrice și electronice
Uleiuri
Vehicule
Asistență

## Lista producătorilor de deșeuri de baterii și acumulatori

Export pagină curentă

orange

| Nr. în Listă | Data fondării | Persoana juridică | IDNO | Data înregistrării | Identificarea | Adresa juridică |
|---|---|---|---|---|---|---|
| MD2022-2-BA-002 | 1998-03-18 | ORANGE MOLDOVA SA | 1003600106115 | 2022-02-15 | Producător | mun. Chișinău, str. Alba-Iulia 75 |

**Declarație privind deservirea echipamentelor în perioada de garanție**

**Către:** Agenția de Stat pentru Proprietatea Intelectuală (AGEPI)
**Licitație deschisă:** ocds-b3wdp1-MD-1696424091739

11 octombrie 2023

Stimată autoritate contractantă,

Prin prezenta declarație, compania Orange Moldova S.A., în calitate de centru de service local, confirmă deservirea echipamentelor ofertate prin **Achiziția cu costuri mici nr. ocds-b3wdp1-MD-1696424091739** din 4 octombrie 2023, achiziționarea: **Echipament Fortinet Fortigate 201F sau echivalentul**, în perioada de garanție care constituie minim 12 luni, ne obligăm să asigurăm:

- Posibilitatea contactării imediate a Ofertantului (Prestatorului) la linia „hot-line" disponibil 24x7, în scopul raportării unei defecțiuni sau probleme.
- În perioada de garanție, v-om asigura constatarea (diagnosticarea) unei defecțiuni în maxim 4 ore lucrătoare şi remedierea defecțiunii în maxim 7 zile lucrătoare de la data reclamării acesteia de către Cumpărător (în perioada 08:00 – 18:00, zile lucrătoare).
- Constatarea şi remedierea defecțiunii se va face la sediul Cumpărătorului, iar în cazul unor defecțiuni mai grave, echipamentele se vor transporta la centrul de deservire autorizat de către Producător de către Vânzător.
- La solicitarea Cumpărătorului, lucrările de remediere a defecțiunilor vor fi executate şi în afara orelor de lucru, sau în zilele nelucrătoare.

Data completării 12.10.2023
Cu stimă
Anatolie BULGARU
Șef Diviziunea Suport și Elaborare Servicii IoT și ICT
Î.M. „Orange Moldova" S.A.

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

# Fluxul de lucru în perioada de exploatare operațională

I.M. Orange Moldova S.A.
IDNO 1003600106115
Str. Alba Iulia 75, MD-2071 Chisinau
Republica Moldova
Capital social 179499609 lei
Administrator Olga Surugiu
www.orange.md

# Fluxul de lucru în perioada de exploatare operațională

## Table of contents

# Fluxul de lucru în perioada de exploatare operațională

## Despre companie

Una din activitățile de bază a companiei Orange Moldova este prestarea unei game largi de servicii în domeniul IT/ domeniul Securității Cibernetice, asistență acordată clienților pentru dezvoltarea, modernizarea  şi suportul infrastructurii sale IT.

Compania Orange Moldova utilizează în activitatea sa cele mai noi tehnologii în domeniile de soluții aplicative de nivelul întreprinderii, centre de date, soluții de stocare, automatizare, telecomunicații şi transport de date. Experiența echipei tehnice din cadrul companiei Orange Moldova permite prestarea serviciilor de cea mai înaltă calitate şi aliniată la cele mai bune practice internaționale.

Orange Moldova este partenerul celor mai renumiți Vendori – producători:Fortinet, Lenovo, HP, Cisco, McAfee, Microsoft, Oracle, VmWare, Huawei etc. Acest lucru se datorează inclusiv faptului că Orange Moldova nu doar implementează soluții/ bunuri pentru clientii săi dar şi utilizează soluțiile şi bunurile în scopul propriul uz, ceea ce oferă un avantaj considerabil față de alți parteneri din Republica Moldova.

Echipa tehnică şi de suport include specialişti  de cea mai înaltă calificare şi cu experiență vastă de integrare şi suport a sistemelor informatice complexe.

Echipa tehnică şi de suport oferă servicii de mentenanță şi suport la nivel național.

Orange Moldova este parte a Grupului Orange, unul dintre liderii mondiali în servicii de telecomunicații, cu sediul în Paris, Franța. Grupul Orange conduce un număr de aproximativ 20 000 de persoane angajate şi care îşi desfășoară activitatea în Franța, Belgia, Marea Britanie, Elveția, Austria, Polonia, Slovacia, România, Moldova, Spania;  în Africa, Orientul mijlociu și în Caraibe.

Orange este parte a grupului France Telecom, una dintre cele mai mari companii de comunicații din lume, cu peste 163 milioane de utilizatori pe cinci continente. Este inclusiv un furnizor de frunte a sistemelor informatice şi a serviciilor şi soluțiilor cuprinse în ele.

# Fluxul de lucru în perioada de exploatare operațională

Grupul Orange prezintă rezultate record în ultima perioadă. Companie a înregistrat vânzări de 43,513 miliarde Euro.

# Fluxul de lucru în perioada de exploatare operațională

## Descrierea

Pentru toate echipamentele incluse în lista de echipamente deservite de centru autorizat local Lenovo pe durata garanției echipamentelor în caz şi în perioada ulterioară, compania Orange Moldova va presta serviciile în conformitate cu nivele de deservire (Service Level Agreement - SLA) în descrierea serviciilor.

## Punctul unic de contact

Pe durata prestării serviciilor Orange Moldova va desemna 2 (două) persoane responsabile certificate pentru controlul activităților de zi cu zi pentru îndeplinirea cererilor de suport. Acestea persoane vor acționa ca punct unic de contact în caz de escaladări.

## Termenul de prestare a serviciilor

Serviciile vor fi prestate pentru toata perioada de garanție a echipamentelor.
Termenul de prestare a serviciilor poate fi prelungit ulterior la solicitarea Beneficiarului – Agenția de Stat pentru Proprietatea Intelectuală (AGEPI).

Serviciile vor fi prestate pentru toata perioada contractată, dacă este indicată într-un contract de prelungire a garanției sau contract de prestare a serviciilor de mentenanță.

## Nivelul de deservire (SLA)

Orange Moldova va asigura nivele de deservire în conformitate cu Descrierea Serviciilor.

Nivele de deservire solicitate pot fi clasificate pe 2 (două) nivele de descriere:

| NIVEL | DESCRIERE |
|---|---|
| Critice – 24/7, timp de reacție 1 oră, timp de răspuns 4 ore | Sisteme care necesită o reacție rapidă în cazul unui incident, şi cu demararea procedurilor de remediere imediată sau într-un timp scurt. Pentru aceste sisteme este caracteristic graficul de lucru 24 din 24 inclusiv zilele de sărbători naționale/ internaționale. |
| Moderat Critice – 9X5, timp de reacție 1 oră, timp de răspuns 24 ore | Sisteme care necesită o reacție rapidă din partea echipei de asistență tehnică doar în timpul zilei lucrătoare, nu afectează funcționalitățile principale ale sistemului informatic, şi demararea remedierii incidentului poate fi începută mai târziu.<br>. |

# Fluxul de lucru în perioada de exploatare operațională

## Termenii şi indicatorii care definesc Nivele de Deservire (SLA)

**Cerere de suport** este solicitarea asistenței tehnice sau raportarea unui incident prin metodele definite în metodele de comunicare definite către serviciul “hot-line”.

**Timp de reacție** indicatorul care defineşte timpul maxim de confirmare a cererii de suport. Pentru măsurarea acestui indicator se vor folosi datele din sistemul de înregistrare a cererilor de suport.

Exemplu. Incidentul a fost raportat la orele 4:00, organizația de suport confirmă recepționarea cererii de suport până la orale 5:00 prin metodele definite şi în dependență de tipul incidentului începe procedura de depanare, în acest caz timpul de reacție este de o (1) oră.

**Timp de răspuns** este indicatorul care defineşte timpul minim pentru prezentarea unui scenariu de remediere a incidentului. Se va face o diferențiere între timpul de reacție din cauza că depanarea unui subsistem poate necesita prezența la sediul beneficiarului sau în centrul de date.

Exemplu. Incidentul a fost raportat la orele 4:00, timp de o (1) oră a fost confirmată recepționarea cererii de suport, specialiştii se deplasează la locul incidentului. Timpul de începere a procedurii de depanare şi prezența a specialiştilor la locul incidentului este 8:00, în acest caz timpul de răspuns este 4 ore.

**Timp de soluționare** indicatorul care defineşte timpul maxim de înlăturare a problemei.

Exemplu. Incidentul a fost raportat în data de 1.09.2021 la orele 4:00, timp de o (1) oră a fost confirmată recepționarea cererii de suport, specialiştii se deplasează la locul incidentului. Timpul de înlăturare a problemei va fi în maxim 7 zile lucrătoare de la data reclamării acesteia.

**Acoperire** este indicatorul care defineşte disponibilitatea specialiştilor furnizorului de servicii pentru soluționarea incidentelor.

Exemplu. Specialiştii furnizorului de servicii sunt disponibili pentru recepționarea şi soluționarea cererilor de suport de Luni până Vineri în timpul orelor de lucru 8:00 – 18:00, în acest caz acoperirea este Luni-Vineri 8X5. În cazul când se solicită disponibilitatea specialiştilor în regim de 24 ore pe zi, inclusiv zilele de sărbători naționale/ internaționale acoperirea este de 24X7.

## Organizarea şi asigurarea suportului

Pentru comunicarea cu furnizorul de servicii şi înregistrarea cererilor de suport în contractul de deservire vor fi indicate:

| |
|---|
| - Numărul unic de telefon şi fax a serviciului “hot-line”<br>Tel. +33 4 89 87 05 55<br>https://support.fortinet.com/webchatonline.aspx<br>Clientul poate utiliza şi Service Desk al companiei Orange Moldova:<br>Tel. +373 22 977 700<br>Fax. +373 22 977 710 |
| |
| - Lista de persoane responsabile pe tip de incident şi telefoane de contact:<br><br>Ion Cozma<br>email: ion.cozma@orange.com<br>Tel. +37369198955<br><br>Anatolie Bulgaru<br>Email: anatolie.bulgaru@orange.com<br>Tel. +37369198955<br><br>Robert Gutuleac<br>email: robert.gutuleac@netsafe.md<br>Tel. +373 (68) 115511<br><br>Netsafe Distribution<br>Suport tehnic: http://support.netsafe.ro/ |
| |
| - FortiCare Support: technical Assstance Center interfața pentru cererile de suport suport şi/sau interfața la sistemul automatizat de înregistrare a cererilor de suport “service desk”: https://Fortinet SSO |
| |

- Lista persoanelor pentru escaladare incidentelor

Ion Cozma
email: ion.cozma@orange.com
Tel. +37369198955

Anatolie Bulgaru
Email: anatolie.bulgaru@orange.com
Tel. +37369198955

Service Desk al companiei Orange Moldova:
Tel. +373 22 977 700
Fax. +373 22 977 710

- Lista de contacte pentru adresările directe la producător:
Robert Gutuleac
email: robert.gutuleac@netsafe.md
Tel. +373 (68) 115511

Netsafe Distribution
Suport tehnic: http://support.netsafe.ro/

Important: Pentru a deschide cererea de suport va fi necesar următoarea informație:

- Product Serial Number
- Persoana responsabilă din partea Beneficiarului pentru asigurarea accesului fizic şi logic la sistemele afectate: telefon şi email
- Adresa locației echipamentului
- Descrierea problemei – simptome, caracterul problemei

## Timp de reacție

Din momentul când a fost comunicată cererea de suport, Executorul va începe activitatea de depanare a cauzei incidentului nu mai mult decât peste o oră, cu excepția cazului în care Beneficiarul va fixa alt timp de intervenție.

# Fluxul de lucru în perioada de exploatare operațională

## Locul prestării serviciilor

Serviciile vor fi prestate la locul instalării echipamentelor sau la distanță. Pentru aceasta Beneficiarul va asigura accesul fizic şi logic la locul instalării echipamentelor.

## Limba de comunicare

Limba de comunicare cu serviciul “hot-line” poate fi la alegerea Beneficiarului – limba de stat, limba rusă, sau limba engleză.

## Procedurile de suport

I. Înregistrea cererilor de suport – în caz de necesitate, Beneficiarul se va adresa către serviciul “hot-line” sau va accesa FortiCare Support Portal. Serviciul “hot-line” comunică Beneficiarului un număr unic, acordat cererii de suport.

Obligator se va comunica următoarele informații:

- Descrierea problemei – simptome, caracterul problemei
- Timpul apariției problemei
- Persoana responsabilă din partea Beneficiarului pentru asigurarea accesului fizic şi logic la sistemele afectate
- Persoana responsabilă din partea serviciului de suport

II. Procesul de depanare – în acelaşi timp cu înregistrarea cererii de suport Executorul va începe activitatea de determinare şi înlăturare a cauzei cheie. Procesul de depanare va fi demarat nu mai târziu decât SLA-ul agreat.
Specialiştii Executorului se pot adresa Clientului pentru a concretiza informația primită, pentru a primi date suplimentare despre defecțiune, sau pot interveni on-site.

III. Escaladare – în caz de necesitate Executorul va escalada incidentul la producător.

IV. Raport de progres – la cererea Beneficiarului Executorul se obligă să informeze Beneficiarul despre starea cereri de suport. Executorul se obligă să informeze Beneficiarul despre orice întârzieri în efectuarea procedurilor de remediere a incidentului, despre cauzele apariției acestora şi măsurile întreprinse pentru a le înlătura. La fel progresul şi starea incidentelor se va monitoriza prin intermediul sistemului Service Desk disponibil Beneficiarului.

V. Raport periodic – Dacă este indicat în contract, executorul se obligă să raporteze Beneficiarului lunar despre orice incidente înregistrate, starea lor, cauzele apariției, metodele de soluționare, la fel ca şi orice altă informație creată sau obținută în rezultatul furnizări serviciilor de suport.

## Descrierea serviciilor

Orange Moldova are toate competențele necesare pentru alte a presta următoarele servicii pe deplin şi la cea mai înaltă calitate.

## Acoperire şi Timp de Răspuns

Nivelul de deservire pentru toate echipamentele este definit ca Moderat Critice.

| Acoperire | Timp de Răspuns |
|---|---|
| Luni – Vineri, 9X5 | Next Day |

În cazul în care în anumite cazuri Beneficiarul va solicita ca anumite echipamente să fie deservite conform unui nivel înalt de deservire din cauza diferitor factori – importanța unui loc de muncă anumit, perioadă de timp critică etc, menționăm că în aceste cazuri echipa tehnică va ridica nivelul de deservire automat a resurselor echipelor de intervenție.

## Timp de soluționare

În perioada de garanție se va asigura constatarea (diagnosticarea) unei defecțiuni în

maxim 4 ore lucrătoare (în zilele de lucru, intervalul de timp 08:00 – 18:00, iar în cazul în care la necesitatea Cumpărătorului executarea lucrărilor de diagnosticare se efectuează în orele /zilele nelucrătoare, termenul de diagnosticare poate fi extins până la 5 zile lucrătoare) și înlăturarea problemei în maxim 7 zile lucrătoare de la data reclamării acesteia de către Cumpărător (în perioada 08:00 – 17:00, zile lucrătoare). Înlăturarea problemei presupune repararea sau substituirea componentelor defectate, instalarea, configurarea şi testarea funcționării adecvate a lor. La solicitarea Cumpărătorului, lucrările de remediere a defecțiunilor vor fi executate și în afara orelor de lucru, sau în zilele nelucrătoare. Constatarea şi remedierea defecțiunii se va face la sediul Cumpărătorului de către personalul calificat din contul Vânzătorului, utilizând componentele livrate de producătorul echipamentului, iar în cazul unor defecțiuni mai grave, echipamentele se vor transporta la centrul de deservire autorizat de către Vânzător. În cazul unor defecțiuni mai grave, Bunurile se vor transporta de către Vânzător la centrul de deservire autorizat de către Producător. Toate serviciile legate de înlăturarea defecțiunilor (pieselor defecte) sau problemelor (inclusiv corespondența cu producătorul, transportarea, vămuirea pieselor de schimb și celor defectate, etc.) vor fi efectuate de către Vânzător din contul său. De asemenea, toate serviciile legate de returnarea (transportarea, împachetarea, vămuirea, etc.) echipamentelor/pieselor defectate către Producător vor fi efectuate de către Vânzător din contul Vânzătorului. Garanția include costul pieselor şi al manoperei. Lucrările de suport vor include următoarele: i) diagnosticarea componentelor; ii) schimbarea sau repararea componentelor în caz de defectare; iii) efectuarea lucrărilor de suport și upgrade a softului firmware.

*Anexa nr. 14*
*la Documentația standard*
*aprobată prin Ordinul Ministrului Finanțelor*
*nr. 115 din 15.09.2021*

**DECLARAŢIE**
**privind personalul de specialitate propus pentru implementarea contractului**

| Nr. d/o | Funcţia | Studii de specialitate | Experienţa de muncă în domeniul solicitat | Experienţă de muncă în organizaţie | Numărul şi denumirea bunurilor/serviciilor similare livrate/prestate în calitate de conducător | Numărul certificatului de atestare și data eliberării |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | Inginer Cert NSE 4 | Diploma de licenţă Universitatea Tehnică din Moldova, Licențiat în Ingineria Computațională<br><br>Certificat FORTINET „NSE 4 Network Security Professional” – 2023 | 9 ani | 2 ani | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. |
| 2 | Inginer Cert NSE 1-3 | Diploma de licenţă Universitatea Tehnică din Moldova, Facultatea Radioelectronica si Telecomunicatii. Specialitatea Sisteme Optoelectronice<br><br>Certificat FORTINET „NSE 1 Network Security Associate” – 2023<br>Certificat FORTINET „NSE 2 Network Security Associate” – 2023<br>Certificat FORTINET „NSE 2 Network Security Associate” – 2023<br>Certificat FORTINET „NSE 3 Network Security Associate” – 2023 | 2 ani | 5 ani | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. |
| 3 | Inginer Cert NSE 2-3 | Diploma de licenţă Universitatea Tehnică din Moldova, Licențiat în Inginerie și Management în Construcția de Mașini<br><br>Certificat FORTINET „NSE 2 Network Security Associate” – 2022<br>Certificat FORTINET „NSE 3 Network Security Associate” – 2022<br>Certificat Huawei „Transmission&Access Pre-sales Specialist” - 2022 | 6 ani | 6 ani | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | Inginer<br>Cert NSE 4-7 | Universitatea Româno-Americană din București - Informatica Manageriala, Cibernetica, Statistica si Informatica Economica<br><br>Certificat FORTINET „NSE 4 Network Security Professional” – 2021<br>Certificat FORTINET „NSE 5 Network Security Analyst” – 2021<br>Certificat FORTINET „NSE 7 Network Security Architect” – 2021<br>Certificat FORTINET „NSE 5 FortiAnalyzer” – 2019<br>Certificat FORTINET „NSE 5 FortiManager” – 2020<br>Certificat FORTINET „NSE 5 FortiAuthenticator” – 2021 | 6 ani | 2 ani | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. |
| 5 | Inginer Infrastructura | Diploma de licenţă Universitatea Tehnică din Moldova, Facultatea Inginerie în Telecomunicaţii<br><br>Certificat HUAWEI „Data Center Facility” | 19 ani | 14 ani | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. |
| 6 | Inginer Expert Solutii ICT | Diploma de licenţă Universitatea Tehnică din Moldova, Facultatea Inginerie în Tehnologii Informationale<br><br>Certificat HUAWEI „Datacom”<br>Certificat HUAWEI „HUAWEI Certified Specialist Associate Sales-IP Network” | 8 ani | 1 an | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. | Conform documentelor suport anexate prezentei documentatii: CV si recomandari aferente. |

Nume: Anatolie BULGARU
Poziția: Șef Diviziunea Suport și Elaborare Servicii IoT și ICT.
Data: 12.10.2023
Locul: Chișinău Republica Moldova

*Anexa nr. 12*
*la Documentația standard*
*aprobată prin Ordinul Ministrului Finanţelor*
*nr. 115 din 15.09.2021*

**DECLARAȚIE**
**privind lista principalelor livrari/prestări efectuate în ultimii 3 ani de activitate**

| Nr d/o | Obiectul contractului | Denumirea/numele beneficiarului/ Adresa | Calitatea Furnizorului /Prestatorului*) | Preţul contractului/ valoarea bunurilor/serviciilor livrate/prestate | Perioada de livrare/prestare (luni) |
|---|---|---|---|---|---|
| **1** | Echipament IT/Retea IP/Securitate Inf. | B.C. Victoriabank S.A. | contractant unic | 360,000.00 USD inclusiv TVA. | Livrare unica anul 2021 |
| **2** | Echipament IT/Retea IP/Securitate Inf. | BC ”MAIB” S.A. | contractant unic | 130,000.00 EUR inclusiv TVA. | Livrare unica anul 2022 |
| **3** | Echipament IT/Retea IP/Securitate Inf. | Noction S.R.L. | contractant unic | 20,000.00 USD inclusiv TVA | Livrare unica anul 2022 |
| **4** | Echipament IT/Retea IP/Securitate Inf. | IP STISC | contractant unic | 5,745,000.00 MDL inclusiv TVA | Livrare unica anul 2022 |
| **5** | Echipament IT/Retea IP/Securitate Inf. | IT-Lab Grup SRL | contractant unic | 6,300.00 EUR inclusiv TVA. | Livrare unica anul 2022 |
| **6** | Echipament IT/Retea IP/Securitate Inf. | Health Forever International SRL | contractant unic | 27,000.00 EUR inclusiv TVA | Livrare unica anul 2023 |
| **7** | Echipament IT/Retea IP/Securitate Inf. | ICT Solutii SRL | contractant unic | 300,000.00 EUR inclusiv TVA. | Livrare unica anul 2023 |

Data completării 12.10.2023

Cu stimă,
Anatolie Bulgaru
Șef Diviziunea Suport și Elaborare Servicii IoT și ICT
Î.M. „Orange Moldova” S.A.