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

APROBAT
prin Ordinul
Ministrului Finanțelor
nr. 72 din 30.06.2020
(*modificat prin Ordinul MF nr. 146 din 24.11.2020*)

FORMULARUL STANDARD AL DOCUMENTULUI UNIC DE ACHIZIȚII EUROPEAN

1. Documentul unic de achiziții european, (în continuare, DUAE) este o declarație pe proprie răspundere, prin care operatorul economic confirmă îndeplinirea criteriilor de calificare și selecție necesare în cadrul procedurilor de achiziție publică în Republica Moldova.
2. Formularul este completat, semnat electronic și transmis autorității contractante la depunerea ofertei.
3. Un DUAE depus de către operatorul economic în cadrul unei proceduri de achiziție publică anterioară poate fi reutilizat, cu condiția ca informațiile cuprinse în formular să fie corecte și valabile la data depunerii acestuia.
4. Ofertantul care prezintă în DUAE informații false sau documentele justificative prezentate nu confirmă informația indicată în documentul prezentat este exclus din procedura de achiziție publică și/sau poate răspunde conform legislației.
5. Formularul DUAE este constituit din 7 capitole, și anume:
1) Capitolul I. Informații privind procedura de achiziție publică și autoritatea/entitatea contractantă;
2) Capitolul II. Informații referitoare la operatorul economic;
3) Capitolul III. Motive de excludere din cadrul procedurii de achiziție publică;
4) Capitolul IV. Criteriile de calificare și selecție a operatorilor economici;
5) Capitolul V. Indicații generale pentru criteriile de selecție a operatorilor economici;
6) Capitolul VI. Preselecția candidaților pentru procedura de atribuire a contractului de achiziție publică;
7) Capitolul VII. Declarații finale.
6. Prezentarea formularului DUAE la depunerea ofertei care nu este conform cu cerințele stabilite în Documentația de atribuire duce la respingerea ofertei.

Capitolul I. Informații privind procedura de achiziție publică și autoritatea/entitatea contractantă

Compartimentul se completează doar de către autoritatea/entitatea contractantă.

Cod poziție	Conținutul cerinței	Răspuns
1	2	3
A. Informații despre publicare		
1A.1	Numărul anunțului/invitației publicate în Buletinul achizițiilor publice, și după caz numărul anunțului publicat în Jurnalul Oficial al Uniunii Europene	***Echipament de comunicații electronice (cu excepția echipamentului telefonic). Nr. ocds-b3wdp1-MD-1741001150278 (21374006)***
B. Identitatea autorității/entității contractante		
1B.1	Denumirea autorității/entității contractante	**Agenţia Servicii Publice**
1B.2	Număr unic de identificare (IDNO) a autorității/entității contractante	**1002600024700**

Capitolul II. Informații referitoare la operatorul economic

Compartimentul se completează doar de către operatorii economici.

Cod poziție	Conținutul cerințelor	Răspuns

1	2	3
A. Informații privind operatorul economic		
2A.1	Denumirea operatorul economic	Î.M. „Orange Moldova” S.A.
2A.2	Țara	Republica Moldova
2A.3	Cod poștal	MD-2071
2A.4	Oraș/Localitate	mun. Chișinău
2A.5	Adresa juridică	mun. Chișinău, str. Alba Iulia 75
2A.6	Pagina web	www.orange.md
2A.7	Persoana sau persoanele de contact	Ion Cozma
2A.7.1	*Telefon*	069198955
2A.7.2	*Adresa de e-mail*	*corporate@orange.md*
2A.8	Număr unic de identificare (IDNO/IDNP)	1003600106115
2A.9	Numărul cod TVA	7800044
2A.10	Forma organizatorico-juridică a activității de antreprenoriat	Societate pe acțiuni
2A.11	Informația cu privire la numele acționarilor/asociaților/beneficiarului efectiv	
2A.11.1	Numele acționarilor / asociaților	Orange Participations S.A. MMT-BIS S.A. Corporația Financiara Internațională
2A.11.2	Numele beneficiarului efectiv *[**beneficiar efectiv** – persoană fizică ce deține sau controlează în ultimă instanță o persoană fizică sau juridică ori beneficiar al unei societăți de investiții sau administrator al societății de investiții, ori persoană în al cărei nume se desfășoară o activitate sau se realizează o tranzacție și/sau care deține, direct sau indirect, dreptul de proprietate sau controlul asupra a cel puțin 25% din acțiuni sau din dreptul de vot al persoanei juridice ori asupra bunurilor aflate în administrare fiduciară]*	**Olga Surugiu** - Administrator **Nazaroi Ion** - Preşedinte al Consiliului societăţii **Climoc Liudmila** -Membru al Consiliului societăţii **Deloison Gilles –** Membru al Consiliului societăţii **Ribas Christine** - Membru al Consiliului societăţii **FANGILLE Barbara Marie** - Membru al Consiliului societăţii **Luginbühl Christian Urs** Membru al Consiliului societăţii **Culpin Jean-Marie** - Membru al Consiliului societăţii **„Orange” S.A.** Societatea-mamă
2A.11.3	Cetățenia beneficiarului efectiv *(legătură juridico-politică permanentă a persoanei fizice definite conform poziției 2A.11.2)*	**Olga Surugiu** – R.Moldova **Climoc Liudmila** - R.Moldova **Nazaroi Ion** - R.Moldova **Deloison Gilles** - Franța **Ribas Christine** - Franța **FANGILLE Barbara Marie** - Luxembourg **Luginbühl Christian Urs** - Elveția **Culpin Jean-Marie** - Franța **„Orange” S.A.** - Franța
2A.12	Operatorul economic este: • întreprindere mică • întreprindere mijlocie	☐Da ☒Nu ☐Da ☒Nu ☒Da ☐Nu

	• și altele	
2A.13	În cazul în care achiziția este rezervată: operatorul economic este un atelier protejat sau o întreprindere socială, sau va asigura executarea contractului în contextul programelor de angajare protejată?	☐Da ☒Nu
2A.13.1	*Dacă da, care este procentul corespunzător de lucrători cu dizabilități sau defavorizați?*	Nu se aplică
2A.13.2	*Specificați cărei sau căror categorii de lucrători cu dizabilități sau defavorizați le aparțin angajații în cauză?*	Nu se aplică
2A.14	Operatorul economic participă la procedura de achiziții publice împreună cu alți operatori economici?	☐Da ☒Nu
2A.14.1	*Dacă Da, precizați rolul operatorului economic în cadrul grupului (lider, responsabil cu îndeplinirea unor sarcini specifice, etc).*	Nu se aplică
2A.14.2	*Numiți operatorii economici care participă la procedura respectivă de achiziție publică.*	Nu se aplică
2A.14.3	*Specificați denumirea grupului participant.*	Nu se aplică
Notă. Dacă ați răspuns Da la întrebarea 2A.14, asigurați-vă ca operatorii economici menționați să prezinte un formular DUAE separat.		
B. Informații privind reprezentanții operatorului economic		
Indicați numele persoanei (persoanelor) împuternicită (împuternicite) să îl reprezinte pe operatorul economic în scopurile prezentei proceduri de achiziție publică.		
2B.1	Nume și prenume	Rodica Platon
2B.2	Poziție/acționând în calitate de..	Sales Suport Expert
2B.3	Țară	Republica Moldova
2B.4	Telefon	069197962
2B.5	Adresa de e-mail	rodica.platon@orange.com
C. Informații privind utilizarea capacităților altor entități		
2C.1	Operatorul economic utilizează capacitățile altor entități pentru a satisface criteriile de selecție prevăzute în capitolul IV, precum și (dacă este cazul) criteriile și regulile menționate în capitolul V de mai jos?	☐Da ☒Nu
Notă. Dacă ați răspuns Da la întrebarea 2C.1, prezentați un formular DUAE separat care să cuprindă informațiile solicitate în secțiunile A și B din capitolul respectiv și din capitolul III pentru fiecare dintre entitățile în cauză, completat și semnat în mod corespunzător de entitățile în cauză. Atragem atenția asupra faptului că trebuie incluși, de asemenea, tehnicienii sau organismele tehnice implicate, indiferent dacă fac sau nu parte din întreprinderea operatorului economic, în special cei care răspund de controlul calității și, în cazul contractelor de achiziții publice de lucrări, tehnicienii sau organismele tehnice la care poate face apel operatorul economic în vederea executării lucrărilor. În măsura în care este relevant pentru capacitatea (capacitățile) specifică (specifice) utilizată (utilizate) de operatorul economic, includeți informațiile prevăzute în capitolele IV și V pentru fiecare dintre entitățile în cauză.		
D. Informații privind subcontractanții pe ale căror capacități operatorul economic se bazează		
2D.1	Operatorul economic intenționează să subcontracteze vreo parte din contract cu alți operatori economici?	☐Da ☒Nu
2D.1.1	*Dacă Da, enumerați subcontractanții propuși.*	Nu se aplică

Capitolul III. Motive de excludere din cadrul procedurii de achiziție publică

Compartimentul se completează de către operatorii economici.

Cod poziție	Conținutul cerințelor	Răspuns

A. Motive referitoare la condamnări prin hotărârea definitivă a unei instanțe judecătorești		
1	**2**	**3**
3A.1	**Participare la o organizație criminală.** Operatorul economic însuși sau orice persoană care este membru al organismului de administrare, de conducere sau de supraveghere al acestuia sau care are putere de reprezentare, de decizie sau de control în cadrul acestuia a făcut obiectul unei condamnări pronunțate printr-o hotărâre definitivă pentru participare la o organizație criminală, printr-o condamnare pronunțată cu cel mult cinci ani în urmă sau în care continuă să se aplice o perioadă de excludere prevăzută în mod direct în condamnare?	☐ Da ☒Nu
3A.2	**Corupție.** Operatorul economic însuși sau orice persoană care este membru al organismului de administrare, de conducere sau de supraveghere al acestuia sau care are putere de reprezentare, de decizie sau de control în cadrul acestuia a făcut obiectul unei condamnări pentru corupție pronunțate printr-o hotărâre definitivă, printr-o condamnare pronunțată cu cel mult cinci ani în urmă sau în care continuă să se aplice o perioadă de excludere prevăzută în mod direct în condamnare?	☐Da ☒Nu
3A.3	**Fraude.** Operatorul economic însuși sau orice persoană care este membru al organismului de administrare, de conducere sau de supraveghere al acestuia sau care are putere de reprezentare, de decizie sau de control în cadrul acestuia a făcut obiectul unei condamnări pentru fraudă pronunțate printr-o hotărâre definitivă, printr-o condamnare pronunțată cu cel mult cinci ani în urmă sau în care continuă să se aplice o perioadă de excludere prevăzută în mod direct în condamnare?	☐Da ☒Nu
3A.4	**Infracțiuni teroriste sau infracțiuni legate de activitățile teroriste.** Operatorul economic însuși sau orice persoană care este membru al organismului de administrare, de conducere sau de supraveghere al acestuia sau care are putere de reprezentare, de decizie sau de control în cadrul acestuia a făcut obiectul unei condamnări pentru infracțiuni teroriste sau infracțiuni legate de activități teroriste, pronunțate printr-o hotărâre definitivă, printr-o condamnare pronunțată cu cel mult cinci ani în urmă sau în care continuă să se aplice o perioadă de excludere prevăzută în mod direct în condamnare?	☐Da ☒Nu
3A.5	**Spălare de bani sau finanțarea terorismului.** Operatorul economic însuși sau orice persoană care este membru al organismului de administrare, de conducere sau de supraveghere al acestuia sau care are putere de reprezentare, de decizie sau de control în cadrul acestuia a făcut obiectul unei condamnări pentru infracțiuni teroriste sau infracțiuni legate de activități teroriste, pronunțate printr-o hotărâre definitivă, printr-o condamnare pronunțată cu cel mult cinci ani în urmă sau în care	☐Da ☒Nu

	continuă să se aplice o perioadă de excludere prevăzută în mod direct în condamnare?	
3A.6	**Exploatarea prin muncă a copiilor și alte forme de trafic de persoane.** Operatorul economic însuși sau orice persoană care este membru al organismului de administrare, de conducere sau de supraveghere al acestuia sau care are putere de reprezentare, de decizie sau de control în cadrul acestuia a făcut obiectul unei condamnări pronunțate printr-o hotărâre definitivă pentru exploatare prin muncă a copiilor și alte forme de trafic de persoane, printr-o condamnare pronunțată cu cel mult cinci ani în urmă sau în care continuă să se aplice o perioadă de excludere prevăzută în mod direct în condamnare?	☐Da ☒Nu
3A.7	În cazul că răspunsul este Da pentru cel puțin una din întrebările 3A.1 – 3A.6, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?	Nu se aplică Se va prezenta Cazier Judiciar la necesitate
3A.7.1	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
B.	**Motive privind plata impozitelor sau/și a contribuțiilor de asigurări sociale**	
	Plata impozitelor	
3B.1	Operatorul economic și-a onorat obligațiile cu privire la plata impozitelor, taxelor și contribuțiilor sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în țara în care este stabilit?	☒Da ☐Nu
3B.1.1	*Dacă Nu, în ce mod a fost stabilită obligația cu privire la plata impozitelor, taxelor și contribuțiilor sociale?*	Nu se aplică
3B.1.2	*În cazul în care, încălcarea cu referire la obligațiile privind plata impozitelor, taxelor și contribuțiilor sociale a fost stabilită printr-o hotărâre judecătorească sau administrativă, această decizie este definitivă?*	☐Da ☒Nu
3B.1.3	*În cazul în care, încălcarea cu referire la obligațiile privind plata impozitelor, taxelor și contribuțiilor sociale a fost stabilită printr-o hotărâre judecătorească sau administrativă, precizați data și numărul deciziei.*	Nu se aplică
3B.2	Operatorul economic beneficiază, în condițiile legii, de eșalonarea obligațiilor de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale ori de alte facilități în vederea plății acestora, inclusiv a majorărilor de întârziere (penalităților) și/sau a amenzilor? Notă: *Se completează doar în cazul în care ați răspuns Nu, la întrebarea din 3B.1.*	Nu se aplică
3B.2.1	*Dacă Da, operatorul economic este în măsură să furnizeze actul privind eșalonarea obligațiilor de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale ori de alte facilități în vederea plății acestora?*	Nu se aplică
3B.3	Operatorul economic este în măsură să furnizeze un certificat cu privire la plata impozitelor sau să furnizeze informații privind onorarea obligațiilor fiscale?	☒Da ☐Nu

3B.4	Informațiile privind lipsa/existența restanțelor față de bugetul public național sunt disponibile gratuit pentru autorități, prin accesarea unei baze de date naționale? Dacă da, specificați informația care ar permite verificarea.	Adresa de internet: https://date.gov.md/open/company-details
C. Includerea în lista de interdicție a operatorilor economici		
3C.1	Operatorul economic este înscris în lista de interdicție a operatorilor economici?	☐Da ☒Nu
3C.1.1	*În cazul că răspunsul este Da pentru întrebarea 3C.1, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3C.1.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
D. Motive legate de insolvabilitate, conflicte de interese sau abateri profesionale		
	Obligațiile aplicabile în domeniul mediului, muncii și asigurărilor sociale	
3D.1	Operatorul economic a încălcat obligațiile în domeniul mediului în ultimii 3 ani?	☐Da ☒Nu
3D.1.1	*În cazul că răspunsul este Da pentru întrebarea 3D.1, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.1.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
3D.2	Operatorul economic a încălcat obligațiile în domeniul social în ultimii 3 ani?	☐Da ☒Nu
3D.2.1	*În cazul că răspunsul este Da pentru întrebarea 3D.2, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.2.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
3D.3	Operatorul economic a încălcat obligațiile în domeniul muncii în ultimii 3 ani?	☐Da ☒Nu
3D.3.1	*În cazul că răspunsul este Da pentru întrebarea 3D.3, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.3.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
	Insolvabilitatea	
3D.4	Operatorul economic este în situație de insolvabilitate sau de lichidare a activității antreprenoriale ca urmare a unei hotărârii judecătorești?	☐Da ☒Nu
3D.4.1	*În cazul că răspunsul este Da pentru întrebarea 3D.4, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.4.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
	Active administrate de lichidator	
3D.5	Activele operatorului economic sunt administrate de un lichidator sau de o instanță?	☐Da ☐Nu
3D.5.1	*În cazul că răspunsul este Da pentru întrebarea 3D.5, puteți*	Nu se aplică

	furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?	
3D.5.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
	Activitățile economice sunt suspendate	
3D.6	Activitățile economice ale operatorului economic sunt suspendate?	☐Da ☒Nu
3D.6.1	*În cazul că răspunsul este Da pentru întrebarea 3D.6, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.6.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
	Acorduri cu alți operatori economici care vizează denaturarea concurenței	
3D.7	Operatorul economic, în ultimii 3 ani, a încheiat acorduri cu alți operatori economici care au ca obiect denaturarea concurenței, fapt constatat prin decizie a organului abilitat în acest sens?	☐Da ☒Nu
3D.7.1	*În cazul că răspunsul este Da pentru întrebarea 3D.7, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.7.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
	Conflict de interese	
3D.8	Operatorul economic se află într-o situație de conflict de interese care nu poate fi remediată?	☐Da ☒Nu
3D.8.1	*În cazul că răspunsul este Da pentru întrebarea 3D.8, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.8.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
	Etica profesională	
3D.9	Operatorul economic a fost condamnat, în ultimii 3 ani, prin hotărâre definitivă a unei instanțe judecătorești, pentru o faptă care a adus atingere eticii profesionale sau pentru comiterea unei greșeli în materie profesională?	☐Da ☒Nu
3D.9.1	*În cazul că răspunsul este Da pentru întrebarea 3D.9, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.9.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică
	Integritatea	
3D.10	Operatorul economic, în ultimii 3 ani, se face vinovat de o abatere profesională, care îi pune la îndoială integritatea?	☐Da ☒Nu
3D.10.1	*În cazul că răspunsul este Da pentru întrebarea 3D.10, puteți furniza dovezi care să arate că măsurile luate sunt suficiente pentru a demonstra fiabilitatea, în pofida existenței unui motiv de excludere?*	Nu se aplică
3D.10.2	*Dacă Da, descrieți aceste măsuri.*	Nu se aplică

Capitolul IV. Criteriile de calificare și selecție a operatorilor economici

Compartimentul se completează de către autoritatea/entitatea (coloana nr.2) contractantă și operatorii economici (coloana nr.3).

Cod poziție	Conținutul cerințelor	Răspuns
1	**2**	**3**
A. Capacitatea de exercitare a activității profesionale		
4A.1	Operatorul economic este în măsură să furnizeze documentul/documentele prin care se va demonstra înregistrarea acestuia? ***Dovada înregistrării operatorului economic - copia extrasului din Registrul de stat al persoanelor juridice, semnată electronic de către operatorul economic.***	☒Da ☐Nu
4A.1.1	*Dacă Da, indicați actele de înregistrare a activității antreprenoriale și genul (genurile) de activitate determinate de legislație, aferent obiectului procedurii de atribuire a contractului, în baza căreia întreprinderea are dreptul să execute viitorul contract de achiziție publică.*	*Certificat de înregistrare nr. 0067000 eliberat la 24.07.2007, Extras din registrul de stat al persoanelor juridice nr. 597339 din 27.03.2025.* *Genul principal de activitate: Conform extrasului anexat.*
4A.1.2	*Actele de înregistrare a activității antreprenoriale, sunt disponibile gratuit pentru autorități dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea.*	*Adresa de internet:* Nu exista *Autoritatea sau organismul emitent(ă):* Nu exista *Referința exactă a documentației:* Nu exista
4A.2	Activitatea antreprenorială deține o certificare și/sau o autorizare echivalentă aferent obiectului procedurii de atribuire a contractului, în cadrul unui sistem național? ***Nu se solicită***	☒Da ☐Nu
4A.2.1	*Dacă Da, operatorul economic este în măsură să furnizeze documentul/documentele prin care se va demonstra certificarea și/sau autorizarea activității acestuia?*	☒Da ☐Nu
4A.2.3	*Actele privind certificarea sau autorizarea sunt disponibile gratuit pentru autorități, dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea.*	*Adresa de internet:* Nu exista *Autoritatea sau organismul emitent(ă):* Fortinet *Referința exactă a documentației:* Fortinet. *Cetificat ISO 9001, ISO 27001.* https://date.gov.md/open/company-details
4A.3	Genurile de activitate, și/sau certificarea, și/sau autorizarea privind activitatea de întreprinzător, acoperă criteriile de selecție impuse de autoritatea/entitatea contractantă în anunțul/invitația de participare?	☒Da ☐Nu

	Nu se solicită.	
B. Capacitatea economică și financiară		
	Declarații bancare	
4B.1	Operatorul economic este în măsură să furnizeze declarații bancare sau, după caz, dovezi privind asigurarea riscului profesional în conformitate cu cerințele din documentația de atribuire? ***Nu se solicită.***	☒Da ☐Nu
4B.1.1	*Informația menționată la punctul 4B.1 este disponibilă gratuit pentru autorități, dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea ei.*	*Adresa de internet:* Nu exista *Autoritatea sau organismul emitent(ă):* Nu exista *Referința exactă a documentației:* Nu exista
	Cifra de afaceri anuală (volumul vânzărilor)	
4B.2	Operatorul economic este în măsură să demonstreze o cifră de afaceri anuală, după cum urmează: Valoare _____ Perioada _____ *Notă. Se completează de către autoritatea contractantă valoarea și perioada* ***Nu se solicită.***	☒Da ☐Nu
4B.2.1	*Specificați care este cifra de afaceri anuală, conform datelor din raportul financiar.*	*3,434,619,697.00 MDL, 2023*
	Cifra de afaceri medie anuală	
4B.3	Operatorul economic este în măsură să demonstreze o cifră medie anuală de afaceri, după cum urmează: Valoare _____ Perioada _____ ***Nu se solicită***	☒Da ☐Nu
4B.3.1	*Specificați cifra de afaceri, conform datelor din raportul financiar.*	*3,434,619,697.00 MDL, 2023* *3,161,577,176.00 MDL, 2022* *3,050,691,749.00 MDL, 2021* *3,215,629,540.67 MDL Medie*
	Raport financiar	
4B.4	Operatorul economic este în măsură să furnizeze raportul financiar înregistrat, extrase din raportul financiar? ***Nu se solicită***	☒Da ☐Nu
4B.5	Informațiile privind situația economică și financiară sunt disponibile gratuit pentru autorități, dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea.	Adresa de internet: https://depozitar.statistica.md/ Autoritatea sau

		organismul emitent(ă): *aprobat de Biroul National de Statistica*
		Referința exactă a documentației: Nu exista
C. Capacitatea tehnică și/sau profesională		
4C.1	Operatorul economic este în măsură să furnizeze documentele solicitate de către autoritatea/entitatea contractantă în anunțul de participare, care demonstrează capacitatea tehnică și/sau profesională pentru executarea viitorului contract.	☒Da ☐Nu
4C.1.1	*Informațiile privind capacitatea tehnică și/sau profesională sunt disponibile gratuit pentru autorități, dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea.*	*Adresa de internet: Nu exista*
		Autoritatea sau organismul emitent(ă): Nu exista
		Referința exactă a documentației: Nu exista
	Instalații tehnice și măsuri de asigurare a calității	
4C.2	Operatorul economic este în măsură să furnizeze detalii referitoare la tehnicieni sau organismele tehnice, specificate în anunțul de participare/documentația de atribuire, pe care autoritatea/entitatea contractantă le poate solicita, în special cele responsabile de controlul calității în legătură cu acest exercițiu de achiziție publică? ***Nu se solicită.***	☒Da ☐Nu
4C.3	Operatorul economic este în măsură să furnizeze o informație cu privire la sistemele de management și de trasabilitate utilizate în cadrul lanțului de aprovizionare? ***Nu se solicită.***	☒Da ☐Nu
4C.3.1	*Informațiile sunt disponibile gratuit pentru autorități, dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea.*	*Adresa de internet: Nu exista*
		Autoritatea sau organismul emitent(ă): Î.M. „Orange Moldova” S.A.
		Referința exactă a documentației: Declarație
	Utilaje, instalații și echipament tehnic	
4C.4	Operatorul economic dispune de utilaje și echipament necesar pentru îndeplinirea corespunzătoare a contractului de achiziție publică? ***Nu se solicită***	☒Da ☐Nu
4C.5	Operatorul economic este în măsură să furnizeze o informație cu privire la dotările specifice, utilajul și echipamentul necesar pentru îndeplinirea contractului, conform cerințelor stabilite în anunțul de participare și documentația de atribuire?	☒Da ☐Nu

	Pregătirea profesională și calificarea personalului	
4C.6	Operatorul economic are în cadrul întreprinderii personal calificat conform cerințelor stabilite în anunțul de participare sau în documentația de atribuire? ***Nu se solicită***	☒Da ☐Nu
4C.7	Operatorul economic este în măsură să furnizeze o informație privind personalul de specialitate propus pentru executarea contractului, conform cerințelor stabilite în anunțul de participare și documentația de atribuire?	☒Da ☐Nu
4C.8	Indicați efectivele medii anuale de personal angajat din ultimii trei ani de activitate. ***Nu se solicită.***	Anul 2021 Angajați 865 Anul 2022 Angajați 679 Anul 2023 Angajați 663
	Numărul membrilor personalului de conducere	
4C.9	Indicați numărul membrilor personalului de conducere ale operatorului economic pe parcursul ultimilor trei ani. ***Nu se solicită.***	Anul 2021 Persoane 9 Anul 2022 Persoane 9 Anul 2023 Persoane 9
	Mostre, descrieri, fotografii	
4C.10	Operatorul economic este în măsură să furnizeze eșantioane (mostre), descrieri și/sau fotografii ale produselor/serviciilor care urmează să fie furnizate/prestate, conform cerințelor stabilite în documentația de atribuire? ***Mostre, descrieri și/sau fotografii (art. 22 alin. (1) lit. e) din Legea 131/2015 privind achizițiile publice) - Prezentarea copiei pașaportului tehnic(fișa tehnică) semnată electronic de către operatorul economic*** ***și/sau prezentarea link-urilor de pe site-urile producătorilor***	☒Da ☐Nu
	Pentru contractele de achiziție publică de lucrări	
4C.11	În perioada de referință, operatorul economic a îndeplinit lucrări specifice sau similare obiectului de achiziție indicat în anunțul de participare și în documentația de atribuire?	☒Da ☐Nu
4C.11.1	*Dacă Da, enumerați-le specificând descrierea lucrărilor, valoarea lor, data de începere, data procesului verbal de recepție la terminarea lucrărilor, beneficiarul și altă informație relevantă.*	*Nu se aplica*
	Pentru contractele de achiziție publică de bunuri	
4C.12	În perioada de referință, operatorul economic a efectuat livrări specifice obiectului de achiziție indicat în anunțul de participare și în documentația de atribuire? ***Experiență specifică în livrarea bunurilor similare (art. 22 alin. (1) lit. a) din Legea 131/2015 privind achizițiile publice).***	☒Da ☐Nu
4C.12.1	*Dacă Da, enumerați-le specificând descrierea livrărilor, valoarea lor, data de începere, data furnizării, beneficiarul*	*Referința exactă a documentației:*

	și altă informație relevantă. ***Declarație privind lista principalelor livrări/prestări efectuate în ultimii trei ani de activitate, completată conform Anexei nr. 12 la Documentația standard aprobată prin Ordinul Ministrului Finanțelor nr. 115 din 15.09.2021.*** ***Livrarea bunurilor se confirmă prin prezentarea unor certificate / documente (facturi fiscale) emise sau contrasemnate de către beneficiarii de bunuri, copiile semnate electronic de către operatorul economic.***	Contracte similare: ***„ICT Solutii SRL”*** *Contract Nr. 9988/1. Echipament IT/Software/Retea IP/Securitate Inf., 2023. Valoarea totală a bunurilor 300,000.00 EUR inclusiv TVA.* ***„IP STISC”****, Contract Nr. 102. Echipament IT/Software/Retea IP/Securitate Inf., 2022. Valoarea totală a bunurilor 5,745,000.00 MDL inclusiv TVA.* ***BC ”MAIB” S.A.*** *Contract unic fără număr. Echipament IT/Software/Retea IP/Securitate Inf., 2022. Valoarea totală a bunurilor 130,000.00 EUR inclusiv TVA.* ***B.C. Victoriabank S.A.*** *Contract unic CC-5577. Echipament IT/Software/Retea IP/Securitate Inf., 2021. Valoarea totală a bunurilor 360,000.00 USD inclusiv TVA.* ***Chemonics International INC****, Contract Nr PO-2023-263-02. Echipament IT/Securitate, 2024 Valoarea totală a bunurilor 176,784.10 EUR fara TVA.* ***„IP AGE”****, Contract Nr. MD-EGA-304698-GO-RFQ. Echipament IT/Software/Retea IP/Securitate Inf., 2024 Valoarea totală a bunurilor 87,307.00 EUR fara TVA.*
	Pentru contractele de achiziție publică de servicii	
4C.13	În perioada de referință, operatorul economic a prestat servicii similare cu obiectul de achiziție indicat în anunțul de participare și în documentația de atribuire?	☒Da ☐Nu

	Nu se solicită	
4C.13.1	*Dacă Da, enumerați-le specificând descrierea serviciilor, valoarea lor, durata de execuție, data începerii, beneficiarul și altă informație relevantă.*	*Referința exactă a documentației:* *Nu se aplica*
4C.14	În cazul că răspunsul este Da pentru una din întrebările 4C.11 – 4C.13, puteți furniza dovezi prin care se va demonstra îndeplinirea lucrărilor, livrarea bunurilor, prestarea serviciilor similare conform cerințelor documentației de atribuire? ***Nu se solicită***	☒Da ☐Nu
D. Standarde de asigurare a calității		
4D.1	Operatorul economic este în măsură să furnizeze certificate emise de organisme independente prin care se atestă faptul că operatorul economic respectă standardele de asigurare a calității conform cerințelor stabilite în anunțul de participare și în documentația atribuire? ***Nu se solicită***	☒Da ☐Nu
4D.2	Informațiile privind standardele de asigurare a calității, sunt disponibile gratuit pentru autorități, dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea.	Adresa de internet: https://www.orange.md/ro/util/iso Autoritatea sau organismul emitent(ă): "SCAR CERT" SRL Referința exactă a documentației: Certificate ISO 9001 ISO 27001
E. Standarde de protecție a mediului		
4E.1	Operatorul economic este în măsură să furnizeze certificate emise de organisme independente prin care se atestă faptul că operatorul economic respectă standardele de protecție a mediului, conform cerințelor stabilite în anunțul de participare și în documentația de atribuire? ***Demonstrarea conformării reglementărilor Legii nr. 209/2016 privind deșeurile***	☒Da ☐Nu
4E.2	Informațiile privind standardele de protecția mediului, sunt disponibile gratuit pentru autorități, dintr-o bază de date națională? Dacă da, specificați informația care ar permite verificarea. ***Prezentarea numărului de înregistrare din „Lista producătorilor de produse supuse reglementărilor de responsabilitate extinsă a producătorului", în conformitate cu Regulamentul privind deșeurile de echipamente electrice și electronice, aprobat prin Hotărârea Guvernului nr. 212 din 07.03.2018 (https://siamd.gov.md/portal/deee.html) – copia, semnată electronic de către operatorul economic.***	Adresa de internet: https://siamd.gov.md/portal/deee.html https://www.moldcontrol.md/ro/membri Autoritatea sau organismul emitent(ă): "SIAMD" Referința exactă a documentației: Registrul Sistemul

		informațional automatizat Managementul deșeurilor / Moldcontrol. nr. MD2022-5-EEE-001 Nr. MD2022-2-BA-002
F. Permiterea controalelor		
4F.1	Operatorul economic permite efectuarea verificărilor de către autoritatea/entitatea contractantă referitor la capacitățile economice și financiare, de producție sau tehnice privind executarea viitorului contract de achiziție publică? ***Nu se solicită.***	☒Da ☐Nu

Capitolul V. Indicații generale pentru criteriile de calificare și selecție

Compartimentul se completează de către autoritatea/entitatea contractantă (coloana nr.2) și operatorii economici (coloana nr.3).

Cod poziție	Conținutul cerințelor	Răspuns
1	**2**	3
A. Îndeplinirea tuturor criteriilor de selecție impuse		
5A.1	Operatorul economic este în măsură să furnizeze în Sistemul informaţional automatizat „Registrul de stat al achiziţiilor publice” sau prin mijloace electronice, sau dacă e cazul, pe suport de hârtie autorității contractante: formularele, certificatele, avizele și alte documente indicate de către autoritatea/entitatea contractantă în anunțul de participare și în documentația de atribuire? Termen **3 zile lucrătoare** de la solicitare. *Notă. Numărul de zile se indică de către autoritatea contractantă ţinând cont de cantitatea şi caracterul documentelor solicitate.*	☒Da ☐Nu
5A.2	Informațiile care să îi permită autorității/entității contractante să obțină documentele indicate în anunțul de participare și în documentația de atribuire, sunt disponibile gratuit și direct prin accesarea unei baze de date naționale în orice stat? Dacă da, specificați informația care ar permite verificarea.	Adresa de internet: *Nu exista* *Autoritatea sau organismul emitent(ă): Î.M. „Orange Moldova” S.A.* Referința exactă a documentației: *Acte/clarificări la solicitare*

Capitolul VI. Preselecția candidaților pentru procedura de atribuire a contractului de achiziție publică

Compartimentul se solicită de către autoritatea contractantă doar în cadrul procedurilor de achiziție publică: licitația restrânsă, negociere, dialog competitiv și parteneriatul pentru inovare.

Cod poziție	Conținutul cerințelor	Răspuns
1	**2**	**3**
A.	**Îndeplinirea tuturor criteriilor de selecție impuse**	

6A.1	Operatorul economic/candidatul îndeplinește criteriile de selecție stabilite de către autoritatea contractantă în anunțul de participare și în documentația de atribuire.	☒Da ☐Nu
6A.2	Operatorul economic/candidatul dispune și este în măsură să furnizeze în Sistemul informațional automatizat „Registrul de stat al achizițiilor publice” sau prin mijloace electronice, sau dacă e cazul, pe suport de hârtie autorității contractante certificate sau alte forme de documente justificative, după cum este cerut în anunțul de participare și în documentația de atribuire.	☒Da ☐Nu

Capitolul VII. Declarații finale

Operatorul economic declară că informațiile prezentate în capitolele II – V (după caz II-VI) sunt exacte și corect furnizate, cunoscând pe deplin consecințele cazurilor grave de declarații false.
Operatorul economic declară în mod oficial, că poate să furnizeze la solicitarea autorității/entității contractante fără întârziere, certificatele și documentele justificative solicitate, cu excepția cazului în care autoritatea/entitatea contractantă are posibilitatea de a obține documentele justificative în cauză direct prin accesarea unei baze de date relevante, care este disponibilă gratuit, cu condiția că operatorul economic să fi furnizat informațiile necesare (adresa de internet, autoritatea sau organismul emitent(ă), referința exactă a documentației) care să îi permită autorității contractante sau entității contractante să facă acest lucru și se consimte accesul la informațiile menționate, în cazul în care acest lucru este necesar.

Operatorul economic declară în mod oficial că este de acord ca **Agenţia Servicii Publice** astfel cum este descrisă în capitolul I secțiunea A să obțină acces la documentele justificative privind informațiile pe care le-a furnizat în acest DUAE în scopul desfășurării procedurii de achiziție: **licitaţie deschisă – Echipament de comunicații electronice (cu excepția echipamentului telefonic).**

Nume: **Anatolie BULGARU**
Poziția: Șef Diviziunea Suport și Elaborare Servicii IoT și ICT
Î.M. „Orange Moldova” S.A.
Data: 07.04.2025
Locul: Chișinău Republica Moldova

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

Anexa nr. 22
la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor
nr. 115 din 15.09.2021

Specificații tehnice

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1741001150278 (21374006) din **03 martie 2025**

Obiectul achiziției: Echipament de comunicații electronice (cu excepția echipamentului telefonic)

Denumirea bunurilor/ serviciilor	Denumirea modelului serviciului	Țara de origine	Producă torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standa rde de referin ță
1	2	3	4	5	6	7
Lotul nr.1 - Paravan de protecție tip 1						
1.1. Paravan de protecție tip 1	FortiGate-80F 8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports	SUA	FortiNet	H1.1 Cerințe Hardware **Paravan de protecție tip 1** FortiGate 80F, 8 x GE RJ45 ports, 2 x GE RJ45/SFP shared media WAN ports FG-80F sau echivalent; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; Toate componentele trebuie să fie actuale și să nu fie promovate ca EOS (End of Support = Sfârșit de mentenanță) / OL (End of Life = Sfârșit de viață); H1.1.01 Max. 1RU rack-mount 19” cu adâncimea max. de 300mm (echipamentul trebuie să fie completat cu KIT de montare) sau de tip desktop cu adâncimea max. de 300mm. H1.1.02 Echipamentul trebuie să permită redundanță energetică prin PSU(power supply unit) dublă(două surse) . H1.1.03 Echipamentul trebuie să fie compatibil cu rețeaua de curent electric AC100-240V, 50/60Hz H1.1.04 Echipamentul trebuie să fie optimizat pentru utilizare în medii silențioase (Fanless sau cu un sistem de răcire silențios, <30 dB) H1.1.05 Echipamentul trebuie să fie dotat cu min. 2 porturi WAN 1 Gb Ethernet SFP și min. 6 porturi LAN 1 Gb Ethernet RJ45 integrate. H1.1.06 Port serial de consolă RJ45 și USB. C1.1 Cerințe funcționale **Paravan de protecție tip 1** C1.1.01 Echipamentul trebuie să fie funcțional și să includă suport complet (actualizări software, baze de date IPS/Antivirus, licențe de securitate) pentru cel puțin 3 ani, fără limitări de licență.	**Paravan de protecție tip 1:** Part number: FG-80F Description: FortiGate-80F 8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports. Cantitate: 115 H1.1 Cerințe Hardware **Paravan de protecție tip 1** FortiGate 80F, 8 x GE RJ45 ports, 2 x GE RJ45/SFP shared media WAN ports FG-80F; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; Toate componentele sunt actuale și nu sunt promovate ca EOS (End of Support = Sfârșit de mentenanță) / OL (End of Life = Sfârșit de viață); H1.1.01 Max. 1RU rack-mount 19” cu adâncimea max. de 300mm (echipamentul trebuie să fie completat cu KIT de montare) sau de tip desktop cu adâncimea max. de 300mm. H1.1.02 Echipamentul permite redundanță energetică prin PSU(power supply unit) dublă(două surse) . H1.1.03 Echipamentul este compatibil cu rețeaua de curent electric AC100-240V, 50/60Hz H1.1.04 Echipamentul este optimizat pentru utilizare în medii silențioase (Fanless sau cu un sistem de răcire silențios, <30 dB) H1.1.05 Echipamentul este să fie dotat cu min. 2 porturi WAN 1 Gb Ethernet SFP și min. 6 porturi LAN 1 Gb Ethernet RJ45 integrate. H1.1.06 Port serial de consolă RJ45 și USB. C1.1 Cerințe funcționale **Paravan de protecție tip 1** C1.1.01 Echipamentul este funcțional și include suport complet (actualizări software, baze de date	**ISO 9001, 27001**

				C1.1.02	Paravanul de protecție trebuie să permită min. detectarea și filtrarea traficului: • detectarea și filtrarea aplicațiilor și actualizarea periodică a bazei de date; • stabilirea regulilor de firewall după criterii geografice (GeoIP); • să permită blocarea traficului din spre/către rețelele Botnet și actualizarea periodică a bazei de date (IPS); • Detectarea fișierelor infectate (Antivirus).		IPS/Antivirus, licențe de securitate) pentru cel puțin 3 ani, fără limitări de licență.		
				C1.1.03	Paravanul de protecție trebuie să asigure cerințele minime pentru asigurarea monitorizării componentelor hardware: • Suport SNMP v2/v3; • Suport Syslog; • Suport Netflow; • Monitorizarea grafica prin interfața de management in timp real si istoric.		C1.1.02	Paravanul de protecție permite min. detectarea și filtrarea traficului: • detectarea și filtrarea aplicațiilor și actualizarea periodică a bazei de date; • stabilirea regulilor de firewall după criterii geografice (GeoIP); • permite blocarea traficului din spre/către rețelele Botnet și actualizarea periodică a bazei de date (IPS); • Detectarea fișierelor infectate (Antivirus).		
				C1.1.04	Echipamentul trebuie să susțină configurarea atât prin CLI (SSH), grafic (WEB) cât și prin intermediul unui manager centralizat (aplicație web).		C1.1.03	Paravanul de protecție asigura cerințele minime pentru asigurarea monitorizării componentelor hardware: • Suport SNMP v2/v3; • Suport Syslog; • Suport Netflow; • Monitorizarea grafica prin interfața de management in timp real si istoric.		
				C1.1.05	Echipamentul trebuie să susțină Site to Site VPN constituit din minim: • Tunelare GRE și L2TP; • Criptare IPsec în mod transport și tunel.		C1.1.04	Echipamentul susține configurarea atât prin CLI (SSH), grafic (WEB) cât și prin intermediul unui manager centralizat (aplicație web).		
				C1.1.06	Echipamentul trebuie să suporte protocoalele caracteristice unui router: OSPF v2,v3, rutare statica,VRF, NAT,PAT,QoS,Vlan tagging 802.1q.		C1.1.05	Echipamentul susține Site to Site VPN constituit din minim: • Tunelare GRE și L2TP; • Criptare IPsec în mod transport și tunel.		
				C1.1.07	Performanța Firewall min. 9 Gb/s (trafic IPv4, pachete de 512 bytes).		C1.1.06	Echipamentul suporta protocoalele caracteristice unui router: OSPF v2,v3, rutare statica,VRF, NAT,PAT,QoS,Vlan tagging 802.1q.		
				C1.1.08	Performanta IPS min. 1.4 Gb/s.		C1.1.07	Performanța Firewall min. 9 Gb/s (trafic IPv4, pachete de 512 bytes).		
				C1.1.09	Performanța Firewall + Application Control + IPS min. 1 Gb/s.		C1.1.08	Performanta IPS min. 1.4 Gb/s.		
				C1.1.10	Sesiuni simultane min. 1 milion.		C1.1.09	Performanța Firewall + Application Control + IPS min. 1 Gb/s.		
				C1.1.11	Sesiuni noi min. 40 mii/sec.		C1.1.10	Sesiuni simultane min. 1 milion.		
				C1.1.12	Performanța SSL VPN min. 900 Mb/s.		C1.1.11	Sesiuni noi min. 40 mii/sec.		
				C1.1.13	Performanța IPSec VPN min. 6 Gb/s (pachete de 512 bytes, TCP).		C1.1.12	Performanța SSL VPN min. 900 Mb/s.		
				S1.1 Cerințe suport/mentenanță **Paravan de protecție tip 1**			C1.1.13	Performanța IPSec VPN min. 6 Gb/s (pachete de 512 bytes, TCP).		
							S1.1 Cerințe suport/mentenanță **Paravan de protecție tip 1**			

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>
<table>
<tr><td>S1.1.01.</td><td>Termen de garanție: min. 36 luni (3 ani) integral, cu suport de la producător, inclusiv înlocuirea echipamentelor defecte în baza rapoartelor de defecțiune a furnizorilor și/sau a producătorului. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare.
Cerințe SLA:
• Acces 24/7 la suport tehnic prin telefon, chat și email.
• Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport.
• Timp de răspuns garantat:
➢ Incidente critice: max. 1 oră.
➢ Incidente majore: max. 4 ore.
➢ Incidente minore: max. 24 ore.
• Acces la actualizările firmware pe toată durata suportului și mentenanței.
• RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.
• Acces la Fortinet Knowledge Base și documentația tehnică.</td></tr>
</table>
</td>
<td>
<table>
<tr><td>S1.1.01.</td><td>Termen de garanție: min. 36 luni (3 ani) integral, cu suport de la producător, inclusiv înlocuirea echipamentelor defecte în baza rapoartelor de defecțiune a furnizorilor și/sau a producătorului. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare.
Cerințe SLA:
• Acces 24/7 la suport tehnic prin telefon, chat și email.
• Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport.
• Timp de răspuns garantat:
➢ Incidente critice: max. 1 oră.
➢ Incidente majore: max. 4 ore.
➢ Incidente minore: max. 24 ore.
• Acces la actualizările firmware pe toată durata suportului și mentenanței.
• RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.
• Acces la Fortinet Knowledge Base și documentația tehnică.</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>1.2. Licență tip 1</td>
<td>FortiGate-80F 3 Year Advanced Threat Protection Bundle and FortiCare Premium (FC-10-0080F-928-02-36)</td>
<td>SUA</td>
<td>FortiNet</td>
<td>
<table>
<tr><td colspan="2">C1.2 Cerințe funcționale Licență tip 1
FortiGate-80F 3 Year Advanced Threat Protection Bundle and FortiCare Premium (FC-10-0080F-928-02-36) sau echivalent.</td></tr>
<tr><td>C1.2.01</td><td>Complet compatibil cu Paravan de protecție tip 1</td></tr>
<tr><td>C1.2.02</td><td>Protecție împotriva amenințărilor avansate (ATP - Advanced Threat Protection):
• Antivirus și protecție împotriva malware-ului.
• Soluție anti-botnet.</td></tr>
<tr><td>C1.2.03</td><td>Protecție avansată IPS (Intrusion Prevention System):
• Actualizare zilnică a semnăturilor IPS pentru protejarea împotriva exploit-urilor și vulnerabilităților critice.
• Protecție împotriva atacurilor zero-day prin semnături IPS și analiză comportamentală.
• Reguli personalizabile de IPS pentru protecția serviciilor critice.</td></tr>
<tr><td>C1.2.04</td><td>Filtrare aplicații și control granular (Application Control):
• Detectarea și controlul a peste 3.000 de aplicații (social media, VPN-uri ascunse, aplicații cloud etc.).
• Posibilitatea de blocare a aplicațiilor nedorite pe categorii și reguli personalizate.
• Integrare cu FortiGuard Threat Intelligence pentru actualizări automate ale bazei de date.</td></tr>
</table>
</td>
<td>
Licență tip 1:
Part number: FC-10-0080F-928-02-36
Description: FortiGate-80F 3 Year Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium).
Cantitate: 115

<table>
<tr><td colspan="2">C1.2 Cerințe funcționale Licență tip 1
FortiGate-80F 3 Year Advanced Threat Protection Bundle and FortiCare Premium (FC-10-0080F-928-02-36).</td></tr>
<tr><td>C1.2.01</td><td>Complet compatibil cu Paravan de protecție tip 1</td></tr>
<tr><td>C1.2.02</td><td>Protecție împotriva amenințărilor avansate (ATP - Advanced Threat Protection):
• Antivirus și protecție împotriva malware-ului.
• Soluție anti-botnet.</td></tr>
<tr><td>C1.2.03</td><td>Protecție avansată IPS (Intrusion Prevention System):
• Actualizare zilnică a semnăturilor IPS pentru protejarea împotriva exploit-urilor și vulnerabilităților critice.
• Protecție împotriva atacurilor zero-day prin semnături IPS și analiză comportamentală.
• Reguli personalizabile de IPS pentru protecția serviciilor critice.</td></tr>
<tr><td>C1.2.04</td><td>Filtrare aplicații și control granular (Application Control):</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>
<table>
<tr><td>C1.2.05</td><td>Sandboxing avansat pentru detecția malware-ului (FortiSandbox Cloud Integration):
• Analiza fișierelor necunoscute într-un sandbox cloud securizat.
• Detectarea atacurilor avansate de tip ransomware, malware polimorf și atacuri zero-day.
• Integrare cu FortiGate pentru blocarea automată a fișierelor dăunătoare.</td></tr>
<tr><td colspan="2">S1.2 Cerințe subscripție și suport Licență tip 1</td></tr>
<tr><td>S1.2.01</td><td>Subscripție și suport de la producător min. 36 luni(3 ani) integral
Cerințe SLA:
• Acces 24/7 la suport tehnic prin telefon, chat și email.
• Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport.
• Timp de răspuns garantat:
➢ Incidente critice: max. 1 oră.
➢ Incidente majore: max. 4 ore.
➢ Incidente minore: max. 24 ore.
• Acces la actualizările firmware pe toată durata active a subscripției și suportului.
• Acces la Fortinet Knowledge Base și documentația tehnică.</td></tr>
</table>
</td>
<td>
<table>
<tr><td></td><td>• Detectarea și controlul a peste 3.000 de aplicații (social media, VPN-uri ascunse, aplicații cloud etc.).
• Posibilitatea de blocare a aplicațiilor nedorite pe categorii și reguli personalizate.
• Integrare cu FortiGuard Threat Intelligence pentru actualizări automate ale bazei de date.</td></tr>
<tr><td>C1.2.05</td><td>Sandboxing avansat pentru detecția malware-ului (FortiSandbox Cloud Integration):
• Analiza fișierelor necunoscute într-un sandbox cloud securizat.
• Detectarea atacurilor avansate de tip ransomware, malware polimorf și atacuri zero-day.
• Integrare cu FortiGate pentru blocarea automată a fișierelor dăunătoare.</td></tr>
<tr><td colspan="2">S1.2 Cerințe subscripție și suport Licență tip 1</td></tr>
<tr><td>S1.2.01</td><td>Subscripție și suport de la producător min. 36 luni (3 ani) integral
Cerințe SLA:
• Acces 24/7 la suport tehnic prin telefon, chat și email.
• Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport.
• Timp de răspuns garantat:
➢ Incidente critice: max. 1 oră.
➢ Incidente majore: max. 4 ore.
➢ Incidente minore: max. 24 ore.
• Acces la actualizările firmware pe toată durata active a subscripției și suportului.
• Acces la Fortinet Knowledge Base și documentația tehnică.</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>1.3. Sursă de alimentare tip 1</td>
<td>SP-FG60E-PDC-5 - AC power adaptor Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 70/71F, 80E/81E, 80/81F, and 90/91G and FDC-100G power cable SP-FG60CPCOR-XX sold separately</td>
<td>SUA</td>
<td>FortiNet</td>
<td>
<table>
<tr><td colspan="2">H1.3 Cerințe Hardware Sursă de alimentare tip 1
Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 80E/81E and 80F/81F SP-FG60E-PDC-5 sau echivalent;
Echipamente și accesorii – Noi, ne recondiționate;
Toate cerințele sunt minime și obligatorii;
Toate componentele trebuie să fie actuale și să nu fie promovate ca EOS (End of Support = Sfârșit de mentenanță) / EOL (End of Life = Sfârșit de viață);</td></tr>
<tr><td>H1.3.01</td><td>Temperatura de operare – interval acceptat de la 0 până la +40 grade Celsius.</td></tr>
<tr><td>H1.3.02</td><td>Umiditatea relativa –interval acceptat de la 5 până la 95% fără condensare.</td></tr>
<tr><td>H1.3.03</td><td>Protecții electrice și fiabilitate:
• Protecție la supratensiune și supracurent.
• Protecție la scurtcircuit și supratemperatură.
• MTBF (Mean Time Between Failures): Minim 100.000 ore.</td></tr>
</table>
</td>
<td>
Sursă de alimentare tip 1:
Part number: SP-FG60E-PDC-5
Description: AC power adaptor Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 70/71F, 80E/81E, 80/81F, and 90/91G and FDC-100G power cable SP-FG60CPCOR-XX sold separately
Cantitate: 12

<table>
<tr><td colspan="2">H1.3 Cerințe Hardware Sursă de alimentare tip 1
Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 80E/81E and 80F/81F SP-FG60E-PDC-5;
Echipamente și accesorii – Noi, ne recondiționate;
Toate cerințele sunt minime și obligatorii;
Toate componentele sunt actuale și nu sunt promovate ca EOS (End of Support = Sfârșit de mentenanță) / EOL (End of Life = Sfârșit de viață);</td></tr>
<tr><td>H1.3.01</td><td>Temperatura de operare – interval acceptat de la 0 până la +40 grade Celsius.</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

				H1.3.04 Tip conector: Jack cilindric (2.1mm/5.5mm) – confirmat pentru compatibilitate cu dispozitivele Fortinet. C1.3 Cerințe funcționale **Sursă de alimentare tip 1** C1.3.01 Compatibil cu Paravan de protecție tip 1: • Sursa de alimentare trebuie să fie complet compatibilă cu echipamentele Fortinet: FG/FWF 60E/61E, 60F/61F, 80E/81E și 80F/81F • Nu sunt acceptate adaptoare cu conectori suplimentari sau neoriginali. C1.3.02 Putere min. 36W C1.3.03 Tensiunea și frecvența de intrare 100 - 240V, 50 - 60Hz C1.3.04 Tensiunea și intensitatea de ieșire 12V, 3A. S1.3 Cerințe suport/mentenanță **Sursă de alimentare tip 1** S1.3.01 Termen de garanție: min. 24 luni(2 ani) integral, cu suport de la producător, inclusiv înlocuirea echipamentelor defecte în baza rapoartelor de defecțiune a furnizorilor și/sau a producătorului. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare. Opțiune de înlocuire rapidă: În cazul defectării unui adaptor în perioada de garanție, furnizorul trebuie să asigure un dispozitiv de înlocuire provizoriu în maxim 5 zile lucrătoare.	H1.3.02 Umiditatea relativa –interval acceptat de la 5 până la 95% fără condensare. H1.3.03 Protecții electrice și fiabilitate: • Protecție la supratensiune și supracurent. • Protecție la scurtcircuit și supratemperatură. • MTBF (Mean Time Between Failures): Minim 100.000 ore. H1.3.04 Tip conector: Jack cilindric (2.1mm/5.5mm) – confirmat pentru compatibilitate cu dispozitivele Fortinet. C1.3 Cerințe funcționale **Sursă de alimentare tip 1** C1.3.01 Compatibil cu Paravan de protecție tip 1: • Sursa de alimentare trebuie să fie complet compatibilă cu echipamentele Fortinet: FG/FWF 60E/61E, 60F/61F, 80E/81E și 80F/81F • Nu sunt acceptate adaptoare cu conectori suplimentari sau neoriginali. C1.3.02 Putere min. 36W C1.3.03 Tensiunea și frecvența de intrare 100 - 240V, 50 - 60Hz C1.3.04 Tensiunea și intensitatea de ieșire 12V, 3A. S1.3 Cerințe suport/mentenanță **Sursă de alimentare tip 1** S1.3.01 Termen de garanție: min. 24 luni (2 ani) integral, cu suport de la producător, inclusiv înlocuirea echipamentelor defecte în baza rapoartelor de defecțiune a furnizorilor și/sau a producătorului. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare. Opțiune de înlocuire rapidă: În cazul defectării unui adaptor în perioada de garanție, furnizorul va asigura un dispozitiv de înlocuire provizoriu în maxim 5 zile lucrătoare.	
Lotul nr. 2 - Licență tip 2						
2.1. Licență tip 2	FMG-VM-100-UG - FortiManager - VM License Upgrade license for adding 100 Fortinet devices/Virtual Domains	SUA	FortiNet	C2.1 Cerințe funcționale **Licență tip 2** FortiManager VM Perpetual License/Upgrade license for adding 100 Fortinet devices FMG-VM-100-UG sau echivalent. C2.1.01 Complet compatibil cu Paravan de protecție tip 1 C2.1.02 Cerințe generale • Licența trebuie să fie perpetuă (fără termen de expirare) și să permită gestionarea a minimum 100 de dispozitive Fortinet. • Licența trebuie să fie compatibilă pentru a fi utilizată în medii on-premises sau cloud. • Toate funcționalitățile incluse în licență trebuie să fie active fără restricții sau limitări.	**Licență tip 2:** Part number: FMG-VM-100-UG Description: FortiManager - VM License Upgrade license for adding 100 Fortinet devices/Virtual Domains; allows for total of 5 GB/Day of Logs. Cantitate: 1 C2.1 Cerințe funcționale **Licență tip 2** FortiManager VM Perpetual License/Upgrade license for adding 100 Fortinet devices FMG-VM-100-UG. C2.1.01 Complet compatibil cu Paravan de protecție tip 1 C2.1.02 Cerințe generale	

				C2.1.03	Administrare centralizată pentru dispozitive Fortinet • Suport pentru FortiGate, FortiSwitch, FortiAP, FortiClient EMS și alte soluții Fortinet. • Administrare bazată pe politici de securitate pentru grupuri de dispozitive. • Configurare automată și management al versiunilor firmware pentru toate dispozitivele administrate. • Interfață web intuitivă cu suport pentru CLI (Command Line Interface).		• Licența este perpetuă (fără termen de expirare) și să permită gestionarea a minimum 100 de dispozitive Fortinet. • Licența este compatibilă pentru a fi utilizată în medii on-premises sau cloud. • Toate funcționalitățile incluse în licență sunt active fără restricții sau limitări.	
				C2.1.04	Gestionarea actualizărilor și a politicilor • Centralizare și distribuție automată a configurațiilor și actualizărilor pentru toate dispozitivele. • Control versiunilor firmware cu posibilitatea de rollback. • Implementare automată a regulilor firewall și a politicilor de securitate. • Sincronizare automată cu FortiGuard pentru actualizări ale semnăturilor IPS, antivirus, filtrare web și controlul aplicațiilor.	C2.1.03	Administrare centralizată pentru dispozitive Fortinet • Suport pentru FortiGate, FortiSwitch, FortiAP, FortiClient EMS și alte soluții Fortinet. • Administrare bazată pe politici de securitate pentru grupuri de dispozitive. • Configurare automată și management al versiunilor firmware pentru toate dispozitivele administrate. • Interfață web intuitivă cu suport pentru CLI (Command Line Interface).	
				C2.1.05	Funcționalități avansate de securitate • Detectarea și prevenirea configurațiilor greșite care pot expune dispozitivele la riscuri de securitate. • Autentificare multi-factor (MFA) pentru acces securizat la interfața de administrare. • Audit și jurnalizare a tuturor acțiunilor administratorilor. • Role-Based Access Control (RBAC) pentru gestionarea privilegiilor utilizatorilor.	C2.1.04	Gestionarea actualizărilor și a politicilor • Centralizare și distribuție automată a configurațiilor și actualizărilor pentru toate dispozitivele. • Control versiunilor firmware cu posibilitatea de rollback. • Implementare automată a regulilor firewall și a politicilor de securitate. • Sincronizare automată cu FortiGuard pentru actualizări ale semnăturilor IPS, antivirus, filtrare web și controlul aplicațiilor.	
				C2.1.06	Suport pentru automatizare și integrare • API REST pentru integrare cu alte sisteme de securitate și monitorizare. • Automatizarea proceselor prin FortiManager Automation Stitches. • Integrare cu SIEM-uri externe(de ex. IBM QRadar gestionat de ASP) pentru analiza avansată a logurilor.	C2.1.05	Funcționalități avansate de securitate • Detectarea și prevenirea configurațiilor greșite care pot expune dispozitivele la riscuri de securitate. • Autentificare multi-factor (MFA) pentru acces securizat la interfața de administrare. • Audit și jurnalizare a tuturor acțiunilor administratorilor. • Role-Based Access Control (RBAC) pentru gestionarea privilegiilor utilizatorilor.	
				C2.1.07	Cerințe de securitate: • Criptare AES-256 pentru toate datele și configurațiile stocate. • Protocol de comunicare securizat (TLS 1.2/1.3) pentru schimbul de date între FortiManager și dispozitivele administrate. • Protecție împotriva atacurilor de tip brute-force și DDoS asupra interfeței de management.	C2.1.06	Suport pentru automatizare și integrare • API REST pentru integrare cu alte sisteme de securitate și monitorizare. • Automatizarea proceselor prin FortiManager Automation Stitches. • Integrare cu SIEM-uri externe(de ex. IBM QRadar gestionat de ASP) pentru analiza avansată a logurilor.	
						C2.1.07	Cerințe de securitate:	

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>
<table>
<tr><td></td><td>• Autentificare bazată pe certificate digitale pentru dispozitivele conectate.
• Jurnalizare și audit complet al activităților utilizatorilor și modificărilor de configurație.</td></tr>
<tr><td colspan="2">S2.1 Cerințe subscripție Licență tip 2</td></tr>
<tr><td>S2.1.01</td><td>Subscripție de la producător – perpetual (fără termen de expirare).
Cerințe SLA:
• Acces 24/7 la suport tehnic prin telefon, chat și email.
• Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport.
• Timp de răspuns garantat:
➢ Incidente critice: max. 1 oră.
➢ Incidente majore: max. 4 ore.
➢ Incidente minore: max. 24 ore.
• Acces la actualizările firmware pe toată durata activă a suportului.
• Acces la Fortinet Knowledge Base și documentația tehnică.</td></tr>
</table>
</td>
<td>
<table>
<tr><td></td><td>• Criptare AES-256 pentru toate datele și configurațiile stocate.
• Protocol de comunicare securizat (TLS 1.2/1.3) pentru schimbul de date între FortiManager și dispozitivele administrate.
• Protecție împotriva atacurilor de tip brute-force și DDoS asupra interfeței de management.
• Autentificare bazată pe certificate digitale pentru dispozitivele conectate.
• Jurnalizare și audit complet al activităților utilizatorilor și modificărilor de configurație.</td></tr>
<tr><td colspan="2">S2.1 Cerințe subscripție Licență tip 2</td></tr>
<tr><td>S2.1.01</td><td>Subscripție de la producător – perpetual (fără termen de expirare).
Cerințe SLA:
• Acces 24/7 la suport tehnic prin telefon, chat și email.
• Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport.
• Timp de răspuns garantat:
➢ Incidente critice: max. 1 oră.
➢ Incidente majore: max. 4 ore.
➢ Incidente minore: max. 24 ore.
• Acces la actualizările firmware pe toată durata activă a suportului.
• Acces la Fortinet Knowledge Base și documentația tehnică.</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>2.2. Suport tip 1</td>
<td>FC2-10-M3004-248-02-12 - FortiManager - VM FortiCare Premium Support 1 Year FortiCare Premium Support (1 - 110 devices/Virtual Domains)</td>
<td>SUA</td>
<td>FortiNet</td>
<td>
<table>
<tr><td colspan="2">C2.2 Cerințe funcționale Suport tip 1
FortiManager - VM 1 Year FortiCare Premium FC2-10-M3004-248-02-12 sau echivalent.</td></tr>
<tr><td>C2.2.01</td><td>Complet compatibil cu Licența tip 2</td></tr>
<tr><td>C2.2.02</td><td>Acces la actualizări și patch-uri software pentru FortiManager pe întreaga perioadă contractuală.</td></tr>
<tr><td>C2.2.03</td><td>Acces la baza de cunoștințe și documentația oficială Fortinet.</td></tr>
<tr><td>C2.2.04</td><td>Asistență pentru depanarea problemelor și optimizarea configurațiilor.</td></tr>
<tr><td>C2.2.05</td><td>Acces la servicii de evaluare a vulnerabilităților și recomandări pentru îmbunătățirea securității.</td></tr>
<tr><td colspan="2">S2.2 Cerințe subscripție și suport Suport tip 1</td></tr>
</table>
</td>
<td>
Suport tip 1:
Part number: FC2-10-M3004-248-02-12
Description: FortiManager - VM FortiCare Premium Support 1 Year FortiCare Premium Support (1 - 110 devices/Virtual Domains)
Cantitate: 1

<table>
<tr><td colspan="2">C2.2 Cerințe funcționale Suport tip 1
FortiManager - VM 1 Year FortiCare Premium FC2-10-M3004-248-02-12.</td></tr>
<tr><td>C2.2.01</td><td>Complet compatibil cu Licența tip 2</td></tr>
<tr><td>C2.2.02</td><td>Acces la actualizări și patch-uri software pentru FortiManager pe întreaga perioadă contractuală.</td></tr>
<tr><td>C2.2.03</td><td>Acces la baza de cunoștințe și documentația oficială Fortinet.</td></tr>
<tr><td>C2.2.04</td><td>Asistență pentru depanarea problemelor și optimizarea configurațiilor.</td></tr>
<tr><td>C2.2.05</td><td>Acces la servicii de evaluare a vulnerabilităților și recomandări pentru îmbunătățirea securității.</td></tr>
<tr><td colspan="2">S2.2 Cerințe subscripție și suport Suport tip 1</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

				S2.2.01	Suport de la producător min. 12 luni Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat: ➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței. • Acces la Fortinet Knowledge Base și documentația tehnică.	S2.2.01	Suport de la producător min. 12 luni Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat: ➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței. • Acces la Fortinet Knowledge Base și documentația tehnică.	
Lotul nr. 3 - Switch tip 1								
	FortiSwitch-124F-FPOE	SUA	FortiNet	H3 Cerințe Hardware **Switch tip 1** Aruba 6000 24G Class4 PoE 4SFP 370W (R8N87A) sau echivalent; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; Toate componentele trebuie să fie actuale și să nu fie promovate ca EOS (End of Support = Sfârșit de mentenanță) /EOL (End of Life = Sfârșit de viață); H3.01 — 1U rack-mount 19” cu adâncimea maximă de 350mm, echipamentul trebuie să fie livrat cu KIT de montare inclus H3.02 — Echipamentele trebuie să fie compatibile cu rețeaua de curent electric AC100-240V, 50/60Hz H3.03 — Echipamentele trebuie să fie dotate cu bloc de alimentare intern H3.04 — Direcționarea fluxului de aer: față-spate sau lateral H3.05 — Porturi necesare: • min. 24 porturi 10/100/1000 Gigabit Ethernet RJ45 PoE+ (IEEE 802.3at) • min. 4 porturi 1Gb Ethernet (SFP) uplink • min. 1 port serial pentru consolă (RJ45 sau micro USB) compatibil cu management prin CLI H3.06 — Capacitatea PoE min. 350W conform IEEE 802.3at (PoE+) H3.07 — Capacitate de switching de cel puțin 56 Gbps H3.08 — Capacitate de forwarding (throughput) de min. 41 Mpps H3.09 — Latența maximă <1.7µs (LIFO-64-bytes packets) H3.10 — Min. 4GB RAM H3.11 — Memorie internă (flash) min. 16GB H3.12 — Echipamentele trebuie să fie destinate categoriei Acces Layer Switch	Hardware **Switch tip 1:** Part number: FS-124F-FPOE + FC-10-S124F-247-02-36+ Lifetime Warranty (în conformitate cu punctul 6 din documentul disponibil la: https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf). Description: FortiSwitch-124F-FPOE Layer 2 FortiGate switch controller compatible PoE+ switch with 24x 1G RJ45 with PoE+ and 4x 10G/1G SFP+/SFP ports and 1x RJ45 console port. Max 370W PoE output limit with smart fan/temperature control. + FC-10-S124F-247-02-36 FortiSwitch-124F-FPOE 3 years FortiCare Premium Support + Lifetime Warranty (în conformitate cu punctul 6 din documentul disponibil la: https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf). Cantitate: 12 H3 Cerințe Hardware **Switch tip 1** FortiSwitch-124F-FPOE Layer 2 FortiGate switch controller compatible PoE+ switch with 24x 1G RJ45 with PoE+ and 4x 10G/1G SFP+/SFP ports and 1x RJ45 console port. Max 370W PoE output limit with smart fan/temperature controlv; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; Toate componentele sunt actuale și nu sunt promovate ca EOS (End of Support = Sfârșit de mentenanță) /EOL (End of Life = Sfârșit de viață); H3.01 — 1U rack-mount 19” cu adâncimea maximă de 350mm, echipamentul trebuie să fie livrat cu KIT de montare inclus H3.02 — Echipamentele sunt compatibile cu rețeaua de curent electric AC100-240V, 50/60Hz		

				C3	Cerințe funcționale **Switch tip 1**	H3.03	Echipamentele sunt dotate cu bloc de alimentare intern		
				C3.01	Echipamentele trebuie să susțină min. 4094 VLAN ID-uri	H3.04	Direcționarea fluxului de aer: față-spate sau lateral		
				C3.02	Echipamentele trebuie să susțină protocolul IEEE 802.1Q VLAN pentru encapsulare	H3.05	Porturi necesare: • min. 24 porturi 10/100/1000 Gigabit Ethernet RJ45 PoE+ (IEEE 802.3at) • min. 4 porturi 1Gb Ethernet (SFP) uplink • min. 1 port serial pentru consolă (RJ45 sau micro USB) compatibil cu management prin CLI		
				C3.03	Echipamentele trebuie să susțină Jumbo Frames de min. 9000 bytes	H3.06	Capacitatea PoE min. 350W conform IEEE 802.3at (PoE+)		
				C3.04	Echipamentele trebuie să susțină min. 6000 MAC adrese	H3.07	Capacitate de switching de cel puțin 56 Gbps		
				C3.05	Echipamentele trebuie să susțină autentificarea minimum prin Radius sau TACACS, Secure Shell (SSH v2)	H3.08	Capacitate de forwarding (throughput) de min. 41 Mpps		
				C3.06	Echipamentele trebuie să susțină minim următoarele protocoale: - „Rapid Per-VLAN Spanning Tree (RPVST+) - Port Security - Access lists (ACL) - Quality of Service (QoS) - BPDU protection - Broadcast storm control - DHCP Snooping - Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s - Port-based network access control IEEE 802.1x - Link Aggregation Control Protocol (LACP) IEEE 802.3ad	H3.09	Latența maximă <1.7µs (LIFO-64-bytes packets)		
				C3.07	Echipamentele trebuie să susțină configurarea minim prin CLI, SNMPv2c, SNMPv3	H3.10	Min. 4GB RAM		
				S3	Cerințe suport/mentenanță **Switch tip 1**	H3.11	Memorie internă (flash) min. 16GB		
				S3.01	Termen de garanție: min. 36 luni(3 ani) integral cu întreținere la centrul de deservire autorizat de producător în Republica Moldova. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat: ➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței. • RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.	H3.12	Echipamentele trebuie să fie destinate categoriei Acces Layer Switch		
						C3	Cerințe funcționale **Switch tip 1**		
						C3.01	Echipamentele susțin min. 4094 VLAN ID-uri		
						C3.02	Echipamentele susțin protocolul IEEE 802.1Q VLAN pentru encapsulare		
						C3.03	Echipamentele susțin Jumbo Frames de min. 9000 bytes		
						C3.04	Echipamentele susțin min. 6000 MAC adrese		
						C3.05	Echipamentele susțin autentificarea minimum prin Radius sau TACACS, Secure Shell (SSH v2)		
						C3.06	Echipamentele susțin minim următoarele protocoale: - „Rapid Per-VLAN Spanning Tree (RPVST+) - Port Security - Access lists (ACL) - Quality of Service (QoS) - BPDU protection - Broadcast storm control - DHCP Snooping - Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s - Port-based network access control IEEE 802.1x - Link Aggregation Control Protocol (LACP) IEEE 802.3ad		
						C3.07	Echipamentele susțin configurarea minim prin CLI, SNMPv2c, SNMPv3		
						S3	Cerințe suport/mentenanță **Switch tip 1**		

					S3.01	Termen de garanție: min. 36 luni (3 ani) integral cu întreținere la centrul de deservire autorizat de producător în Republica Moldova. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/ Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat: ➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței. • RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.	
Lotul nr. 5 - Switch tip 2						
		SUA	FortiNet	H5 Cerințe Hardware **Switch tip 2** Aruba 6000 48G 4SFP (R8N86A) sau echivalent; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; T oate componentele trebuie să fie actuale și să nu fie promovate ca EOS (End of Support = Sfârșit de mentenanță) / EOL (End of Life = Sfârșit de viață); H5.01 — 1U rack-mount 19” cu adâncimea maximă de 350mm, echipamentul trebuie să fie livrat cu KIT de montare inclus H5.02 — Echipamentele trebuie să fie compatibile cu rețeaua de curent electric AC100-240V, 50/60Hz H5.03 — Echipamentele trebuie să fie dotate cu bloc de alimentare intern H5.04 — Direcționarea fluxului de aer: față-spate sau lateral H5.05 — Porturi necesare: • min. 48 porturi 10/100/1000 Gigabit Ethernet RJ45 • min. 4 porturi 1G Ethernet (SFP) uplink • min. 1 port serial pentru consola (RJ45 sau micro USB) compatibil cu management prin CLI H5.06 — Capacitate de switching de cel puțin 96 Gbps H5.07 — Capacitate de forwarding (throughput) de min. 72 Mpps H5.08 — Latența 1Gb <2.0µs (LIFO-64-bytes packets) H5.09 — Min. 4GB RAM H5.10 — Memorie internă (flash) min. 16GB	Hardware **Switch tip 2:** Part number: FS-148F + FC-10-148FN-247-02-36 + Lifetime Warranty (în conformitate cu punctul 6 din documentul disponibil la: https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf). Description: FortiSwitch-148F Layer 2 FortiGate switch controller compatible switch with 48x 1G RJ45 and 4x 10G/1G SFP+/SFP ports and 1x RJ45 console port + FortiSwitch-148F 3 Years FortiCare Premium Support + Lifetime Warranty (în conformitate cu punctul 6 din documentul disponibil la: https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf). Cantitate: 50 H5 Cerințe Hardware **Switch tip 2** FortiSwitch-148F Layer 2 FortiGate switch controller compatible switch with 48x 1G RJ45 and 4x 10G/1G SFP+/SFP ports and 1x RJ45 console port; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; Toate componentele sunt actuale și nu sunt promovate ca EOS (End of Support = Sfârșit de mentenanță) / EOL (End of Life = Sfârșit de viață); H5.01 — 1U rack-mount 19” cu adâncimea maximă de 350mm, echipamentul trebuie să fie livrat cu KIT de montare inclus H5.02 — Echipamentele sunt compatibile cu rețeaua de curent electric AC100-240V, 50/60Hz	

				H5.11	Echipamentele trebuie să fie destinate categoriei Acces Layer Switch	H5.03	Echipamentele sunt dotate cu bloc de alimentare intern		
				C5	Cerințe funcționale **Switch tip 2**	H5.04	Direcționarea fluxului de aer: față-spate sau lateral		
				C5.01	Echipamentele trebuie să susțină min. 4094 VLAN ID-uri	H5.05	Porturi necesare: • min. 48 porturi 10/100/1000 Gigabit Ethernet RJ45 • min. 4 porturi 1G Ethernet (SFP) uplink • min. 1 port serial pentru consola (RJ45 sau micro USB) compatibil cu management prin CLI		
				C5.02	Echipamentele trebuie să susțină protocolul IEEE 802.1Q VLAN pentru encapsulare	H5.06	Capacitate de switching de cel puțin 96 Gbps		
				C5.03	Echipamentele trebuie să susțină Jumbo Frames de min. 9000 bytes	H5.07	Capacitate de forwarding (throughput) de min. 72 Mpps		
				C5.04	Echipamentele trebuie să susțină min. 6000 MAC adrese	H5.08	Latența 1Gb <2.0µs (LIFO-64-bytes packets)		
				C5.05	Echipamentele trebuie să susțină autentificarea minimum prin Radius sau TACACS, Secure Shell (SSH v2)	H5.09	Min. 4GB RAM		
				C5.06	Echipamentele trebuie să susțină următoarele protocoale: - „Rapid Per-VLAN Spanning Tree (RPVST+) - Port Security - Access lists (ACL) - Quality of Service (QoS) - BPDU protection - Broadcast storm control - DHCP Snooping - Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s - Port-based network access control IEEE 802.1x - Link Aggregation Control Protocol (LACP) IEEE 802.3ad	H5.10	Memorie internă (flash) min. 16GB		
				C5.07	Echipamentele trebuie să susțină configurarea minimum prin CLI, SNMPv2c, SNMPv3	H5.11	Echipamentele trebuie să fie destinate categoriei Acces Layer Switch		
				S5	Cerințe suport/mentenanță **Switch tip 2**	C5	Cerințe funcționale **Switch tip 2**		
				S5.01	Termen de garanție: min. 36 luni(3 ani) integral cu întreținere la centrul de deservire autorizat de producător în Republica Moldova. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat: ➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței.	C5.01	Echipamentele susțin min. 4094 VLAN ID-uri		
						C5.02	Echipamentele susțin protocolul IEEE 802.1Q VLAN pentru encapsulare		
						C5.03	Echipamentele susțin Jumbo Frames de min. 9000 bytes		
						C5.04	Echipamentele susțin min. 6000 MAC adrese		
						C5.05	Echipamentele susțin autentificarea minimum prin Radius sau TACACS, Secure Shell (SSH v2)		
						C5.06	Echipamentele susțin următoarele protocoale: - „Rapid Per-VLAN Spanning Tree (RPVST+) - Port Security - Access lists (ACL) - Quality of Service (QoS) - BPDU protection - Broadcast storm control - DHCP Snooping - Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s - Port-based network access control IEEE 802.1x - Link Aggregation Control Protocol (LACP) IEEE 802.3ad		
						C5.07	Echipamentele susțin configurarea minimum prin CLI, SNMPv2c, SNMPv3		
						S5	Cerințe suport/mentenanță **Switch tip 2**		
						S5.01	Termen de garanție: min. 36 luni(3 ani) integral cu întreținere la centrul de deservire autorizat de producător în Republica Moldova. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare		

				RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.	Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat: ➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței. RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.	
Lotul nr. 6 - Switch tip 3						
		SUA	FortiNet	H6 Cerințe Hardware **Switch tip 3** Aruba 6000 24G 4SFP (R8N88A) sau echivalent; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; Toate componentele trebuie să fie actuale și să nu fie promovate ca EOS (End of Support = Sfârșit de mentenanță) / EOL (End of Life = Sfârșit de viață); H6.01 – 1U rack-mount 19” cu adâncimea maximă de 350mm, echipamentul trebuie să fie livrat cu KIT de montare inclus H6.02 – Echipamentele trebuie să fie compatibile cu rețeaua de curent electric AC100-240V, 50/60Hz H6.03 – Echipamentele trebuie să fie dotate cu bloc de alimentare intern H6.04 – Direcționarea fluxului de aer: față-spate sau lateral H6.05 – Porturi necesare: • min. 24 porturi 10/100/1000 Gigabit Ethernet RJ45 • min. 4 porturi 1G Ethernet (SFP) uplink • min. 1 port serial pentru consola (RJ45 sau micro USB) compatibil cu management prin CLI H6.06 – Capacitate de switching de cel puțin 56 Gbps H6.07 – Capacitate de forwarding (throughput) de min. 41 Mpps H6.08 – Latența 1Gb <1.7µs (LIFO-64-bytes packets) H6.09 – Min. 4GB RAM H6.10 – Memorie internă (flash) min. 16GB H6.11 – Echipamentele trebuie să fie destinate categoriei Acces Layer Switch C6 Cerințe funcționale **Switch tip 3** C6.01 – Echipamentele trebuie să susțină min. 4094 VLAN ID-uri	Hardware **Switch tip 3:** Part number: FS-124F+ FC-10-S124N-247-02-36 + Lifetime Warranty (în conformitate cu punctul 6 din documentul disponibil la: https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf). Description FortiSwitch-124F Layer 2 FortiGate switch controller compatible switch with 24x 1G RJ45 and 4x 10G/1G SFP+/SFP ports and 1x RJ45 console port. Fanless + FortiSwitch-124F 3 Years FortiCare Premium Support + Lifetime Warranty (în conformitate cu punctul 6 din documentul disponibil la: https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf). Cantitate: 60 H6 Cerințe Hardware **Switch tip 3** FortiSwitch-124F Layer 2 FortiGate switch controller compatible switch with 24x 1G RJ45 and 4x 10G/1G SFP+/SFP ports and 1x RJ45 console port. Fanless; Echipamente și accesorii – Noi, ne recondiționate; Toate cerințele sunt minime și obligatorii; Toate componentele sunt actuale și nu sunt promovate ca EOS (End of Support = Sfârșit de mentenanță) / EOL (End of Life = Sfârșit de viață); H6.01 – 1U rack-mount 19” cu adâncimea maximă de 350mm, echipamentul trebuie să fie livrat cu KIT de montare inclus H6.02 – Echipamentele trebuie să fie compatibile cu rețeaua de curent electric AC100-240V, 50/60Hz H6.03 – Echipamentele trebuie să fie dotate cu bloc de alimentare intern H6.04 – Direcționarea fluxului de aer: față-spate sau lateral H6.05 – Porturi necesare:	

				C6.02	Echipamentele trebuie să susțină protocolul IEEE 802.1Q VLAN pentru encapsulare		• min. 24 porturi 10/100/1000 Gigabit Ethernet RJ45 • min. 4 porturi 1G Ethernet (SFP) uplink • min. 1 port serial pentru consola (RJ45 sau micro USB) compatibil cu management prin CLI		
				C6.03	Echipamentele trebuie să susțină Jumbo Frames de min. 9000 bytes		H6.06	Capacitate de switching de cel puțin 56 Gbps	
				C6.04	Echipamentele trebuie să susțină min. 6000 MAC adrese		H6.07	Capacitate de forwarding (throughput) de min. 41 Mpps	
				C6.05	Echipamentele trebuie să susțină autentificarea minimum prin Radius sau TACACS, Secure Shell (SSH v2)		H6.08	Latența 1Gb <1.7µs (LIFO-64-bytes packets)	
				C6.06	Echipamentele trebuie să susțină următoarele protocoale: - „Rapid Per-VLAN Spanning Tree (RPVST+) - Port Security - Access lists (ACL) - Quality of Service (QoS) - BPDU protection - Broadcast storm control - DHCP Snooping - Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s - Port-based network access control IEEE 802.1x - Link Aggregation Control Protocol (LACP) IEEE 802.3ad		H6.09	Min. 4GB RAM	
				C6.07	Echipamentele trebuie să susțină configurarea minimum prin CLI, SNMPv2c, SNMPv3		H6.10	Memorie internă (flash) min. 16GB	
				S6	Cerințe suport/mentenanță **Switch tip 3**		H6.11	Echipamentele trebuie să fie destinate categoriei Acces Layer Switch	
				S6.01	Termen de garanție: min. 36 luni(3 ani) integral cu întreținere la centrul de deservire autorizat de producător în Republica Moldova. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat: ➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței. RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.		C6	Cerințe funcționale **Switch tip 3**	
							C6.01	Echipamentele susțin min. 4094 VLAN ID-uri	
							C6.02	Echipamentele susțin protocolul IEEE 802.1Q VLAN pentru encapsulare	
							C6.03	Echipamentele susțin Jumbo Frames de min. 9000 bytes	
							C6.04	Echipamentele susțin min. 6000 MAC adrese	
							C6.05	Echipamentele susțin autentificarea minimum prin Radius sau TACACS, Secure Shell (SSH v2)	
							C6.06	Echipamentele susțin următoarele protocoale: - „Rapid Per-VLAN Spanning Tree (RPVST+) - Port Security - Access lists (ACL) - Quality of Service (QoS) - BPDU protection - Broadcast storm control - DHCP Snooping - Multiple Spanning Tree Protocol (MSTP) IEEE 802.1s - Port-based network access control IEEE 802.1x - Link Aggregation Control Protocol (LACP) IEEE 802.3ad	
							C6.07	Echipamentele susțin configurarea minimum prin CLI, SNMPv2c, SNMPv3	
							S6	Cerințe suport/mentenanță **Switch tip 3**	
							S6.01	Termen de garanție: min. 36 luni(3 ani) integral cu întreținere la centrul de deservire autorizat de producător în Republica Moldova. Soluționarea cazurilor de garanție în termen până la 30 zile lucrătoare Cerințe SLA: • Acces 24/7 la suport tehnic prin telefon, chat și email. • Acces la portalul Furnizorului/Producătorului pentru gestionarea solicitărilor de suport. • Timp de răspuns garantat:	

						➢ Incidente critice: max. 1 oră. ➢ Incidente majore: max. 4 ore. ➢ Incidente minore: max. 24 ore. • Acces la actualizările firmware pe toată durata suportului și mentenanței. RMA (return merchandise authorization) avansat (Advanced Hardware Replacement) – înlocuirea rapidă a echipamentului în caz de defect hardware.	

Data completării 07.04.2025

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

Anexa nr. 23
la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor
nr. 115 din 15.09.2021

Specificații de preț

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1741001150278 (21374006) din **03 martie 2025**

Obiectul achiziției: Echipament de comunicații electronice (cu excepția echipamentului telefonic)

Cod CPV	Denumirea bunurilor/serviciilor	Unitatea de măsură	Canti -tatea	Preț unitar, MDL (fără TVA)	Preț unitar, MDL (cu TVA)	Suma, MDL fără TVA	Suma, MDL cu TVA	Termenul de livrare/ prestare	Clasificație bugetară (IBAN)
1	2	3	4	5	6	7	8	9	10
32500000-8	**Lotul nr. 1 - Paravan de protecție tip 1**								
	1.1. Paravan de protecție tip 1	Buc.	115	27,150.95	32,581.14	3,122,359.25	3,746,831.10	*Bunurile vor fi livrate în termen de până la 120 de zile calendaristice din data semnării contractului.*	MD97VI0000022242125555MDL
	1.2. Licență tip 1	Buc.	115	34,346.82	41,216.18	3,949,884.30	4,739,861.16		
	1.3. Sursă de alimentare tip 1	Buc.	12	7,907.91	9,489.49	94,894.92	113,873.90		
					Total lot nr. 1	**7,167,138.47**	**8,600,566.16**		
							Lotul nr. 2 - Licență tip 2		
	2.1. Licență tip 2	Buc.	1	176,762.63	212,115.16	176,762.63	212,115.16		
	2.2. Suport tip 1	Buc.	1	42,266.19	50,719.43	42,266.19	50,719.43		
					Total lot nr. 2	**262,834.58**	**262,834.58**		
	Lotul nr. 3 - Switch tip 1	Buc.	12	18,263.12	21,915.74	219,157.44	262,988.93		
					Total lot nr. 3	**219,157.44**	**262,988.93**		
	Lotul nr. 5 - Switch tip 2	Buc.	50	16,922.32	20,306.78	846,116.00	1,015,339.20		
					Total lot nr. 5	**846,116.00**	**1,015,339.20**		
	Lotul nr. 6 - Switch tip 3	Buc.	60	10,018.68	12,022.42	601,120.80	721,344.96		
					Total lot nr. 6	**601,120.80**	**721,344.96**		

Data completării 07.04.2025

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

Anexa nr. 7
la Documentația standard
aprobată prin Ordinul Ministrului Finanțelor
nr. 115 din 15.09.2021

CERERE DE PARTICIPARE

Către: **Agenția Servicii Publice**,
Republica Moldova, MD-2012, mun. Chișinău, str. Pușkin, 42.

Stimați domni,

Ca urmare a anunțului/invitației de participare/de preselecție apărut în Buletinul achizițiilor publice, nr. **ocds-b3wdp1-MD-1741001150278** din „03" Martie 2025, privind aplicarea procedurii pentru atribuirea contractului **„Echipament de comunicații electronice (cu excepția echipamentului telefonic)"**, noi **Î.M. „Orange Moldova" S.A.**, am luat cunoștință de condițiile și de cerințele expuse în documentația de atribuire și exprimăm prin prezenta interesul de a participa, în calitate de ofertant/candidat, neavând obiecții la documentația de atribuire.

Data completării 07.04.2025

Cu stimă,

Anatolie Bulgaru
Șef Diviziunea Suport și Elaborare Servicii IoT și ICT
Î.M. „Orange Moldova" S.A.

Anexa nr. 8
la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor
nr. 115 din 15.09.2021

DECLARAŢIE
privind valabilitatea ofertei

Către: **Agenţia Servicii Publice**,
Republica Moldova, MD-2012, mun. Chișinău, str. Puşkin, 42.

Stimați domni,

Ne angajăm să menținem oferta valabilă, privind achiziționarea **„Echipament de comunicații electronice (cu excepția echipamentului telefonic)", ocds-b3wdp1-MD-1741001150278 din „03" Martie 2025** prin procedura de achiziție **Licitație deschisă**, pentru o durată de **90 zile,** (**nouăzeci zile**), respectiv până la data de **08.07.2025**, și ea va rămâne obligatorie pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

Data completării 07.04.2025

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

DISTRIBUITOR AUTORIZAT FORTINET,
Netsafe Distribution SRL

Catre: I.P. Agenția Servicii Publice 07.04.2025

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

Fortinet Product License Agreement / EULA and Warranty Terms

Product License Agreement

The parties to this agreement are you and/or the entity on whose behalf you are acting (the "End User") and Fortinet, Inc. ("Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT" OR "EULA"). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY END USER OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET'S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. THE INDIVIDUAL ENTERING INTO THIS AGREEMENT REPRESENTS THAT SUCH INDIVIDUAL IS AUTHORIZED TO BIND THE END USER TO THE TERMS HEREIN. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE SVP LEGAL OR ABOVE OF FORTINET. IF END USER DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF END USER DOES NOT AGREE TO THE TERMS OF THIS AGREEMENT, END USER MUST IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER END USER'S RECEIPT OF THE PRODUCT, NOTIFY FORTINET LEGAL LEGAL@FORTINET.COM OF REQUESTED EULA CHANGES.

1. License Grant.

This is a license agreement between End User and Fortinet, not a sales agreement. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to the End User with, or incorporated into, Fortinet hardware and any stand-alone software provided to End User by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 16 below. Software as used herein also refers to any accompanying documentation, any updates and enhancements of the software or firmware provided to End User by Fortinet, at its option. Fortinet grants to End User a (a) non-transferable (except as provided in section 5 ("Transfer") and section 16 ("Open Source Software") below), (b) non-exclusive, (c) revocable (in the event of End User's failure to comply with these terms, in the event of termination, or in the event Fortinet is not properly paid for the applicable Product) license to use the Software in accordance with the terms set forth in this Agreement. Such use shall be solely for End User's internal business purposes unless agreed by Fortinet in writing. End User's use shall be subject to any further restrictions in Fortinet Documentation (including license metrics, term limitations, or restrictions). End User agrees that, except for the limited, specific license rights granted in this section 1, End User receives no license rights to the Software. "Documentation" means all Fortinet operating manuals, Fortinet user manuals, Fortinet product descriptions, Fortinet product specifications, and Fortinet technical manuals, and other Fortinet technical information relating to the Products.

2. Limitation on Use.

End User is prohibited, directly or indirectly, from and may not attempt to: (a) modify, translate, reverse engineer, decompile, decrypt, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner (except as expressly permitted for Channel Partners); (c) transfer, assign, or sublicense rights to any other person or entity (except as provided in section 5): (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers; (e) disclose the results of any benchmarking or performance measurements from use of the Software; (f) interfere with a platform for use of the Software; (g) use the Software on a device not owned and controlled by End User; (h) share non-public features or content of the software with any third party; (i) access the software in order to build a competitive product or service, to build a product using similar ideas, features, functions, or graphics of the software, or to copy any ideas, features, functions, or graphics of the software; or, (j) as otherwise prohibited by the Documentation.

3. Proprietary Rights.

All proprietary rights (including copyrights, trade secret, patent, and other intellectual property rights), title, and interest in and to the Software and any Product, and any copy thereof, remain with Fortinet. End User acknowledges that no title to the Software or other intellectual property rights in the Software or other Products is transferred to End User and End User will not acquire any rights to the Software or other Products except for the specific limited license as expressly set forth in section 1 ("License Grant") above. End User expressly agrees and acknowledges that Fortinet owns, retains, and shall retain all intellectual property rights in and to, and End User has no intellectual property rights in and to, the Products and the Software other than the License Grant. End User agrees to keep confidential all Fortinet confidential information disclosed hereunder, not disclose such confidential information to third parties, and only to use such information for the purposes for which Fortinet disclosed it.

4. Term and Termination.

The term of the license is as set forth in the ordering documents, the Fortinet Documentation, or per Fortinet practices or policies (such as with evaluation or beta licenses or subscription or other term licenses. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately with or without notice if End User breaches or fails to comply with any of the terms and conditions of this Agreement or for other reasons as stated in Fortinet's Documentation. End User agrees that, upon such termination, End User will cease using the Software and any Product and either destroy all copies of the Fortinet Software and Documentation or return all materials to Fortinet.

5. Transfer.

Authorized resellers and authorized distributors of Fortinet ("Channel Partners") may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one End User on a permanent basis, provided that: (i) the Channel Partner ensures that its customer (the end user) receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, Channel Partner hereby agrees to enforce the terms in this Agreement against such end user, (ii) Channel Partner at all times will comply with all applicable United States export control laws and regulations, and (iii) Channel Partner agrees to refund any fees paid to Channel Partner by a third party who purchased Product(s) from Channel Partner but does not

agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement (collectively, (i)-(iii) are the "Transfer Requirements"). Further, if End User attempts to transfer without being a Channel Partner authorized to do so, End User shall adhere to the Transfer Requirements. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet Channel Partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way. Fortinet's license, warranty, and support are only available for Products that End User purchased directly from Fortinet or from a Channel Partner. Products not purchased directly from Fortinet or from a Channel Partner may be blocked from registration.

6. Limited Warranty.

The warranty is only valid for Products that are properly registered on Fortinet's Support Website, https://support.fortinet.com, or such other website as provided by Fortinet. The warranty periods discussed below will start on the earlier of three events to occur: (i) registration of the Product, (ii) initial connection with Fortinet, or (iii) 60 days from the date of Fortinet's shipment (US/Canada) or 90 days from the date of shipment (outside of the US/Canada) ("Warranty Start Date"). It is the Fortinet Channel Partner's responsibility to make clear to the End User the date the product was originally shipped from Fortinet, and it is the End User's responsibility to understand the original ship date from the party from which the End User purchased the Product. All warranty claims must be submitted in writing to Fortinet before the expiration of the Hardware Warranty Period or Software Warranty Period as defined below, as applicable, or such claims are waived in full. Fortinet provides no warranty for beta, donation, or evaluation Products.

(A) Hardware. Fortinet warrants that the hardware portion of the Products ("Hardware") will be free from material defects in workmanship as compared to the Functional Specifications for three hundred sixty-five (365) days from the Warranty Start Date ("Hardware Warranty Period").

(B) Software. Fortinet warrants that the Software as initially shipped by Fortinet will substantially conform to Fortinet's then-current Functional Specifications for the Software, for a period of ninety (90) days from the Warranty Start Date ("Software Warranty Period"), except for FortiToken, which shall be warranted for three hundred sixty-five (365) days from the Warranty Start Date.

(C) Limited Lifetime Warranty for Certain Products. In addition, the following Products have a longer warranty than set forth above, and these Products have a warranty that lasts for five (5) years following the Product announced end-of-life date for the Hardware: (1) FortiAP and (2) FortiSwitch (except for the FortiSwitch-5000 series, which has only a three hundred sixty five (365) day warranty from the Warranty Start Date).

Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware or replacement Software for the non-conforming Software at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement for Hardware will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new nor of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The warranty period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware; and for Software, the warranty period for the repaired or replacement Software shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware or non-conforming Software, the price paid by the original purchaser for the defective Hardware or non-conforming Software will be refunded by Fortinet upon return to Fortinet of the defective Hardware or non-conforming Software (and all copies thereof). All Hardware (or parts thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. The Software license automatically terminates when a refund is given. As used herein, the term "Functional Specifications" means solely those specifications authorized and published by Fortinet in its product datasheets, subject to the terms and limitations specified in those datasheets. In the event no such specifications are provided to End User with the Software or Hardware, there shall be no warranty on such Software or Hardware.

7. Disclaimer of Other Warranties and Restrictions.

END USER ACKNOWLEDGES THAT SOFTWARE AND/OR HARDWARE IS NEVER ERROR-FREE. EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE OR WARRANTY OF NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. END USER HEREBY ACKNOWLEDGES AND AGREES THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE, AND FORTINET DISCLAIMS LIABILITY REGARDING END USER'S WEB BROWSER'S REQUIREMENTS OR ANY THIRD PARTY DEVICE OR APPLIANCE USED TO OPERATE THE SOFTWARE.

The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, configured, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee; (e) includes Non-General Availability Software Versions; or (f) is procured from a third party other than a Channel Partner. In the case of beta, testing, evaluation, donation or free Software or Product and Non-General Availability Software Versions, the End User acknowledges and agrees that such Software or Product could cause system failures, data loss and other issues, and the End User agrees that such Software or Product is provided "as-is" without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever for any system failures or data loss. For clarity, notwithstanding anything to the contrary, all sales are final and no provision in this EULA entitles End User to return Products, other than as expressly set forth herein.

8. Governing Law.

Any disputes arising from or relating to this Agreement, including Fortinet's limited warranty or the breach thereof, shall be governed by the laws of the state of California, without regard to conflict of laws principles. Any disputes arising from or relating to this Agreement or the breach hereof that cannot

be amicably settled by and between the parties shall be referred to and finally resolved by arbitration. The place of arbitration shall be Santa Clara County, California, pursuant to the Streamlined Arbitration Rules and Procedures of Judicial Arbitration and Mediation Services (JAMS), or its successor, before a sole, neutral arbitrator and shall be conducted in English. The parties specifically consent and agree that the federal courts located in the Northern District of California will have jurisdiction over enforcement of any arbitration decisions. For any dispute not referred to arbitration, the parties submit to the exclusive jurisdiction of federal courts (if applicable) or state courts (if federal courts are not applicable) located in Santa Clara County, California, and the parties agree to litigate any such disputes there.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, OTHER THAN AS EXPRESSLY SET FORTH IN THIS SECTION, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, INTEREST, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE), EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR BREACH OF WARRANTY, INCLUDING BREACH OF THE LIMITED WARRANTY UNDER SECTION 6, IS, AT FORTINET'S SOLE AND ABSOLUTE DISCRETION: REPAIR, REPLACEMENT, OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE. IN NO EVENT SHALL ANY END USER REMEDIES UNDER THIS EULA OR ANY SUPPORT AGREEMENT EXCEED THE AMOUNT PAID TO FORTINET FOR THE SPECIFIC APPLICABLE DEFECTIVE OR NON-CONFORMING PRODUCT AT ISSUE. IN NO EVENT SHALL ANY AGGREGATED END USER REMEDIES EXCEED THE TOTAL AMOUNT PAID FOR THE PRODUCTS BY THE END USER.

10. Compliance with Laws, Including Import/Export Laws and Foreign Corrupt Practices Act (FCPA).

End User is advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws; diversion contrary to United States law and regulation is prohibited. Both parties (Fortinet and the End User) agree to comply with all applicable laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see https://www.bis.doc.gov. Fortinet assumes no responsibility or liability for End User's failure to obtain any necessary import and export approvals and licenses, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. End User represents that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against End User or otherwise suspended, revoked, or denied End User's export privileges. End User agrees not to use or transfer the Products for any use relating to nuclear, chemical, or biological weapons or to missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, End User agrees not to directly or indirectly export, import, or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission, or use. Furthermore, End User hereby agrees that, for any orders that End User places with Fortinet whereby any legal or regulatory requirements may apply to Fortinet such as requirements related to the International Traffic in Arms Regulations, or Buy American Act, or the Trade Agreements Act: End User is responsible to ensure the purchase order submitted to Fortinet by End User and/or any Channel Partners clearly states the specific requirement in writing, or otherwise Fortinet is not bound by any such requirements. End User represents that End User understands, and End User hereby agrees (x) to comply with, all applicable laws including but not limited to the U.S. Foreign Corrupt Practices Act, and (y) that its employees have not accepted, and will not accept, anything of value, including money, meals, entertainment, paid-for travel, beta, testing, evaluation, donation or free Products and/or related services, or anything else of value, in exchange for maintaining current business or for new business opportunities with Fortinet. End User represents and warrants to Fortinet that End User and its employees, consultants, agents and representatives will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. End User agrees that it and its personnel will be responsible to comply in full with all laws and policies applicable to any and all dealings with Fortinet and Fortinet's Channel Partners.

11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

12. Tax Liability.

End User agrees to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

13. General Provisions.

Except as specifically permitted and required in section 5 ("Transfer") above, End User agrees not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement may be amended or updated by Fortinet as expressly provided in Section 1 above or by a writing that explicitly refers to this Agreement signed on behalf of both parties, and in the case of Fortinet, by its SVP Legal or above. For clarity, except for Fortinet's SVP Legal or above, no one (such as Sales representatives, Sales Engineers, and the like) can bind Fortinet, and any statements by such personnel are non-binding and should not be relied upon. End User acknowledges that End User has read this Agreement, understands it, and agrees to be bound by its terms and conditions. Notwithstanding anything to the contrary, this EULA constitutes the entire agreement between Fortinet and the End User with respect to the subject matter herein, and supersedes any and all prior representations or conflicting provisions related to Fortinet's product license or warranty terms, such as limitations of liability,

warranties, representations on product capabilities or otherwise in any and all communication with the End User or purported End User agreements, whether entered into now or in the future. In the event of a conflict between this EULA and another agreement, this EULA shall prevail with respect to the subject matter herein unless the conflicting agreement expressly states that it replaces this EULA, expressly referring to this EULA, and is agreed to in writing by authorized representatives of the parties (which, in the case of Fortinet, is Fortinet's SVP Legal or above).

14. No Waiver and Severability.

Failure by Fortinet to enforce any provision of this Agreement will not be deemed a waiver of future enforcement of that or any other provision. The exercise by either party of any remedy under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise. If for any reason a court of competent jurisdiction or an agreed-upon arbitrator finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement shall be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect.

15. Privacy.

End User agrees to Fortinet's collection, use, disclosure, protection and transfer of its information, as set forth in the Fortinet privacy policy on the Fortinet web site (http://www.fortinet.com/about-us/privacy.html), including (a) Fortinet's use of the End User's information to send information regarding Fortinet products and services; and (b) Fortinet's disclosure of End User's information to provide assistance to law enforcement, governmental agencies and other authorities or to allow Fortinet to protect its customers' and/or end users' rights. End User will comply with the Fortinet Data Terms (https://www.fortinet.com/corporate/about-us/legal/data-terms). Fortinet's Data Protection Addendum, which is hereby incorporated by reference (https://trust.fortinet.com/product/default/data-protection-addendum),
will apply to personal data within its scope. End User will not provide Fortinet with "protected health information" that is subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) unless (i) the relevant Fortinet Product is eligible for coverage under Fortinet's business associate agreement ("BAA") and End User has entered into the BAA with Fortinet or (ii) End User's configuration and use of the Product are exempt from HIPAA BAA requirements under applicable guidance from the U.S. Department of Health and Human Services.

16. Open Source Software.

Fortinet's Products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on a CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify any Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send a written request, along with a check in the amount of US $25.00, to General Public License Source Code Request, Fortinet, Inc., 909 Kifer Rd, Sunnyvale, CA 94086 USA. To receive the modified software modules, End User must also include the following information: (a) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, whether expressed or implied. In no event will the copyright holder for the open source software be liable to End User for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may obtained by contacting Fortinet's Legal Department at legal@fortinet.com.

GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc, https://fsf.org/

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.
In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.
If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, see <https://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Moe Ghoul>, 1 April 1989 Moe Ghoul, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. https://fsf.org/

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, see <https://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Moe Ghoul>, 1 April 1990 Moe Ghoul, President of Vice

That's all there is to it!

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/Software/Retea IP/Securitate Inf.	„ICT Solutii SRL”	contractant unic	300,000.00 EUR inclusiv TVA	Livrare unica anul 2023
2	Echipament IT/Retea IP/Securitate Inf.	„IP STISC”	contractant unic	5,745,000.00 MDL inclusiv TVA	Livrare unica anul 2022
3	Echipament IT/Retea IP/Securitate Inf.	BC ”MAIB” S.A.	contractant unic	130,000.00 EUR inclusiv TVA	Livrare unica anul 2022
4	Echipament IT/Retea IP/Securitate Inf.	B.C. Victoriabank S.A.	contractant unic	360,000.00 USD inclusiv TVA	Livrare unica anul 2021
5	Echipament IT/Retea IP/Securitate Inf.	Chemonics International INC	contractant unic	176,784.10 EUR fara TVA	Livrare unica anul 2024
6	Echipament IT/Retea IP/Securitate Inf.	„IP AGE”	contractant unic	87,307.00 EUR fara TVA	Livrare unica anul 2024

Data completării 07.04.2025

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

WHITE PAPER

Fortinet Security Fabric Enables Digital Innovation

Broad, Integrated, and Automated

Executive Summary

Organizations are rapidly adopting digital innovation (DI) initiatives to accelerate their businesses, reduce costs, improve efficiency, and provide better customer experiences. Common initiatives involve moving applications and workflows to the cloud, deploying Internet-of-Things (IoT) devices on the corporate network, and expanding the organization's footprint to new branch locations.

With this evolving infrastructure also come security risks. Organizations must cope with growing attack surfaces, advanced threats, increased infrastructure complexity, and an expanding regulatory landscape. To accomplish their desired DI outcomes while effectively managing risks and minimizing complexities, organizations need to adopt a cybersecurity platform that provides visibility across their environment and a means to manage both security and network operations easily.

The Fortinet Security Fabric solves these challenges with broad, integrated, and automated solutions that enable security-driven networking, zero-trust network access, dynamic cloud security, and artificial intelligence (AI)-driven security operations. Fortinet offerings are enhanced with an ecosystem of seamless integrated third-party products that minimize the gaps in enterprise security architectures, while maximizing security return on investment (ROI).

84% of security executives believe the risk of cyberattacks will increase[1]

77% of security professionals state that their organization has moved applications or infrastructure to the cloud despite known security concerns.[3]

Digital Innovation Is Transforming All Industries

Across economic sectors worldwide, DI is seen as an imperative to business growth and improved customer experience. CIOs are generally positive regarding their DI initiatives, with 61% stating that they have significant cloud, IoT, and mobile operations already in place.[2]

From the perspective of cloud service provider IT and cybersecurity leaders, DI translates into a variety of changes to their network environments. Users are increasingly mobile, and they are accessing the network from locations and endpoints that are not always under corporate IT control. They are also connecting directly to public clouds to use key business applications, such as Office 365. Outnumbering the human-controlled endpoints are IoT devices, which are widely distributed, often in remote and unsupervised locations. Finally, cloud service provider business footprints are diffusing into numerous and far-flung branches, most of which connect directly to cloud and cellular services, bypassing corporate data centers.

All these changes render obsolete the concept of a defensible network perimeter, requiring cloud service providers to adopt a new multilayer defense-in-depth strategy.

Migration of applications and workloads to the cloud

Almost every business has started to move some workloads and applications to the cloud—or at least plans to do so. These decisions are often driven by the desire to reduce costs and to improve operational efficiency and scalability by taking advantage of the flexibility that the cloud provides.

Cloud service providers offer a wide range of possible deployment models. Businesses can take advantage of Software-as-a-Service (SaaS) applications and services such as Salesforce or Box. Alternatively, applications designed and deployed in on-premises environments can be lifted to Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) deployments such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure, and IBM Cloud.

Wary of cloud service provider lock-in and aiming to deploy each application and workload in the cloud for which it is best suited, many organizations have adopted a multi-cloud infrastructure. The downside of such freedom of choice is the need to learn the idiosyncrasies of each cloud environment. In addition, they must use different tools to manage the environment and its security provisions, which obfuscates visibility and necessitates the use of multiple management consoles for policy management, reporting, and more.

Profusion of endpoints across multiple environments

Endpoints are arguably the most vulnerable nodes in the cloud service provider's network. The larger providers have thousands of employees, each using multiple work and personal devices to access network resources. Ensuring cyber hygiene and up-to-date endpoint security on all these devices is a formidable task. Even more daunting is the proliferation of IoT devices. By the end of 2019, the number of active devices exceeded 26.66 billion, and, during 2020, experts estimate that this number will reach 31 billion.[5]

IoT devices are present in numerous business contexts. They provide personalized experiences to retail and hospitality customers, track inventory in manufacturing and logistics, and monitor devices on factory floors or in power plants.

Often ruggedized and power-efficient, IoT devices focus on performance, often at the expense of security features and secure communication protocols. And unlike most network-attached devices, IoT equipment is commonly deployed in remote locations, out of doors, or in unstaffed or infrequently staffed facilities (such as power stations). From these insecure locations, the equipment frequently transmits critical, sensitive data to on-premises data centers and to cloud services.

Expanded business presence across distributed markets and geographies

As companies expand their global footprint by opening new facilities, branch offices, and other satellite locations, they experience increasing wide-area network (WAN) bandwidth constraints. Although SaaS applications, video, and Voice over IP (VoIP) boost productivity and enable new services, they also contribute to an exponential growth in WAN traffic volume.

Highly reliable multiprotocol label switching (MPLS) has been the WAN connectivity technology of choice for many years. However, with MPLS it is difficult to optimize WAN bandwidth use and to vary quality-of-service levels as needed for different applications. As a result, branch expansion and service enhancements can quickly lead to exploding WAN costs.

Consequently, organizations are turning to software-defined WAN (SD-WAN), which makes efficient use of MPLS, internet connections, and even telecommunications links. Plus, SD-WAN dynamically routes each kind of traffic over the optimal link.

Four Considerations for Security Architecture Design

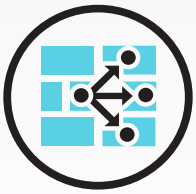
As organizations proceed enthusiastically with DI initiatives, the implications for network security are often overlooked or minimized. In fact, almost 80% of organizations are adding new digital innovations faster than they can secure them against cyber threats.[9]

IT leaders face four key challenges in designing secure architectures for their digitally innovating businesses:

Cloud environments are dynamic: 74% of companies have moved an application to the cloud and then brought it back on-premises.[4]

84% of enterprises have a multi-cloud strategy. 81% point to security as a major cloud challenge.[6]

From 2017 to 2019, there was a 73% increase in the number of organizations experiencing data breaches due to unsecured IoT devices or applications.[7]



SD-WAN provides better performance and security at a lower cost than MPLS.[8]

Expanding attack surface

Sensitive data can potentially reside anywhere—and it can travel over numerous connections outside enterprise control. Applications in the cloud are exposed to the internet so that every new cloud instance creates a new facet of the enterprise attack surface. IoT devices extend the attack surface to remote, unstaffed locations. In these dark parts of the attack surface, intrusions can fester unnoticed for weeks and months, wreaking havoc on the rest of the enterprise. Mobile devices and user-owned endpoints bring unpredictability to the attack surface, as users roam between corporate locations, through public spaces, and across international borders. In fact, extensive cloud migration, extensive use of mobile platforms, and extensive use of IoT devices are factors amplifying the per-record cost of a data breach by hundreds of thousands of dollars.[10]

This expanded, dynamic attack surface dissolves the once well-defined network perimeter and the security protections associated with it. It is much easier for attackers to infiltrate the network, and once inside, they often find few obstacles to moving freely and undetected to their targets. Therefore, security in DI enterprises must be multilayered—with controls on every network segment—based on the assumption that the perimeter will be breached sooner or later. And access to network resources must be based on least privilege and continuously verified trust.

Advanced threat landscape

The cyber-threat landscape is rapidly growing as bad actors attempt to circumvent and defeat traditional cybersecurity defenses. Up to 40% of new malware detected on any given day is zero day or previously unknown.[15] Whether this is driven by increased use of polymorphic malware or the availability of malware toolkits, the growth of zero-day malware makes traditional, signature-based malware detection algorithms less effective. In addition, bad actors continue to utilize social engineering by exploiting static trust methods used in traditional security approaches. Studies reveal that 85% of organizations experienced phishing or social engineering attacks this past year.[16]

As cyber threats become more sophisticated, data incidents and breaches are more difficult to detect and remediate. Between 2018 and 2019, the time to identify and contain a data breach grew from 266 to 279 days.[17] Beyond the ability to detect and prevent an attempted attack, organizations must also be capable of rapidly identifying and remediating a successful attack. Over 88% of organizations have reported experiencing at least one incident in the last year, demonstrating that all organizations are at risk of an attack and that cyber resiliency is critical.[18]

Greater ecosystem complexity

According to almost half of CIOs, increased complexity is the biggest challenge of an expanding attack surface.[19] This increased complexity is due to the fact that many organizations rely upon an array of nonintegrated point products for security. In fact, the average enterprise uses upwards of 75 distinct security solutions.[20]

This lack of security integration means that these organizations are unable to take advantage of automation in their security deployment. In fact, 30% of CIOs point to the number of manual processes as a top security issue in their organization.[21] Without security automation, CIOs require more skilled cybersecurity professionals to monitor and secure their network.

61% of CISOs state that they have significant cloud, IoT, and mobile operations already in place.[11]

Up to 40% of new malware detected on any given day is zero day or previously unknown.[12]

DI initiatives mean that enterprise security teams must deploy protections for 17 different types of endpoints.[13]

One-third of enterprises suffered a breach of business-critical data in the last year, which could lead to regulatory penalties.[14]

However, many organizations are unable to acquire the cybersecurity talent that they require. Estimates indicate that over 4 million cybersecurity positions are currently left unfilled, and the number is steadily growing.[22] This lack of access to necessary talent is putting organizations at risk, with 67% of CIOs saying that the cybersecurity skills shortage inhibits their ability to keep up with the pace of change.[23]

Attackers understand these challenges well, and use it to their advantage.

Fortinet Security Fabric

- Broad
- Automated
- Integrated

FORTINET FABRIC-READY

Increasing regulatory demands

The European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are two of the most well-known of the data protection regulations. However, they are far from the only ones. Every U.S. state currently has a data breach notification law, and many of them are enacting additional consumer privacy protections. Driven by political and social pressure, regulations are expected to expand in coming years, and penalties for noncompliance are becoming larger and more common.

Organizations must also comply with industry standards, and many struggle to do so. Indeed, less than 37% of organizations pass their interim Payment Card Industry Data Security Standard (PCI DSS) compliance audit.[24] As PCI DSS is superseded by the PCI Software Security Framework (PCI SSF), these organizations are likely to face even greater obstacles to remain compliant.

The need to achieve and maintain regulatory compliance has significant impacts on an organization's ability to achieve security transformation objectives. For example, of the 71% of organizations that have moved cloud-based applications back to on-premises data centers, 21% did so to maintain regulatory compliance.[25]

The Fortinet Security Fabric

The Fortinet Security Fabric addresses the security challenges mentioned above by providing broad visibility and control of an organization's entire digital attack surface to minimize risk, an integrated solution that reduces the complexity of supporting multiple point products, and automated workflow to increase the speed of operation.

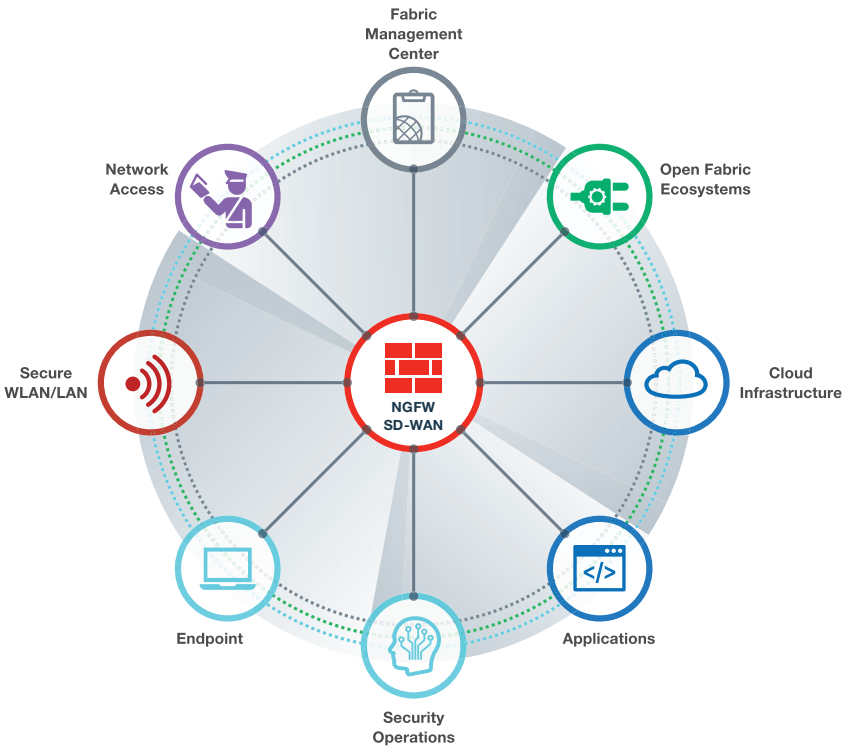


Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly together, across all environments and supported by a single source of threat intelligence, under a single console. This eliminates security gaps in the network and hastens responses to attacks and breaches.

Broad attack surface visibility

With organizational perimeters expanding as a result of DI transformations, the attack surface also expands. The Fortinet Security Fabric addresses the challenge of an expanding attack surface by providing an organization with end-to-end security and visibility across their network infrastructure. With the broadest range of high-performance, security-driven networking solutions for data centers, branch offices and small business, and all major cloud providers, the Fortinet Security Fabric flexes to protect every segment of the network.

All components are configured, managed, and monitored from a single centralized management system. In addition to eliminating the silos associated with point product security infrastructures, the single interface for all security components reduces the training burden on lean staffs. The management system also facilitates zero-touch deployment of remote components, saving truck rolls and further reducing operating costs.

Integrated security architecture

With all components driven by the same FortiOS network operating system, the Fortinet Security Fabric enables consistent configuration and policy management and effortless, real-time communication across the security infrastructure. This minimizes threat detection and mitigation times, reduces security risks resulting from configuration errors and manual data compilation, and facilitates timely and accurate compliance audit response.

In addition to integrating Fortinet products and solutions, the Security Fabric includes prebuilt application programming interface (API) connections for more than 70 Fabric-Ready Partners that ensure deep integration across all of the Security Fabric elements.

For security products that are not part of the Fabric-Ready Partner ecosystem, representational state transfer (REST) APIs and development operations (DevOps) scripts make it easy and fast for customers to add them to the Security Fabric.

Automated operations, orchestration, and response

In addition to seamless integration, the Fortinet Security Fabric is leading the industry in applying machine-learning (ML) technologies to keep up with the rapidly evolving cyber-threat landscape. The Fortinet Security Fabric includes advanced security orchestration, automation, and response (SOAR) capabilities, as well as proactive threat detection, threat correlation, intelligence-sharing alerts, and threat research and analysis.

Almost half of CISOs point to security integration and improved analytics as a major priority for their cybersecurity technology strategy.[26]

FortiGate NGFWs provide the highest price-performance ratio in third-party evaluations while scanning encrypted traffic. They achieve 5.7 Gbps SSL performance while blocking 100% of evasions.[27]

Driving down breach detection and response time can result in a 25% reduction in the overall costs of a data breach. [28]

Expediting incident response activities also requires ensuring that security staff is not distracted by other concerns, such as collecting data for and generating reports for regulatory compliance or the C-suite. Here, the Fortinet Security Fabric offers automated log aggregation, data correlation, and generation of reports using built-in templates.

Security Fabric Solutions

The Fortinet Security Fabric delivers solutions in five key areas: zero-trust access, security-driven networking, dynamic cloud security, AI-driven security operations, and the alliance ecosystem. Each of these includes best-in-class, award-winning solutions that have been evaluated and recommended by leading third-party tests, such as NSS Labs, and recognized by leading analysts, such as Gartner.[29,30]

Figure 2: Conceptual framework for the Fortinet Security Fabric.

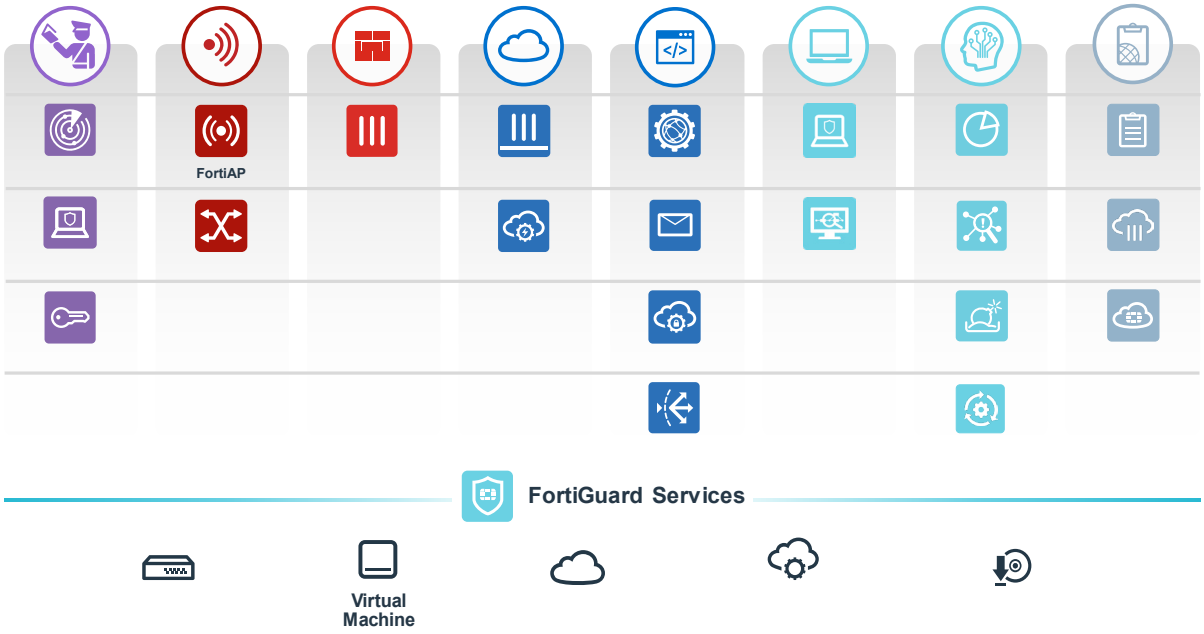


Figure 3: Key offerings in each of the Security Fabric solution areas.

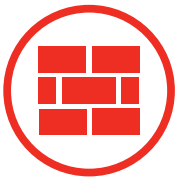
Zero-trust network access

As cyber threats become more sophisticated, a perimeter-focused security model is no longer sufficient. Credential theft and malware enable external threats to gain access to legitimate accounts within the corporate network. The Fortinet Security Fabric enables businesses to implement a zero-trust network access policy throughout their entire corporate WAN.

The first step in enforcing zero-trust access on a network is discovery of the devices connected to the network. **FortiNAC** network access control (NAC) solutions provide automated detection of devices connecting to the corporate WAN. Connected devices are subjected to security scanning, and an organization's security team can define device-specific policies to enforce. Once a device has been approved to access the network, it is monitored continuously to detect any behavioral anomalies that could indicate an infection or use by a malicious actor.

Able to identify the devices connected to its network, organizations can then implement zero-trust access to determine who is using these devices. FortiAuthenticator user identity management server offers built-in authentication and role-based access control (RBAC), allowing organizations to implement least privilege and separation of duties on their networks. FortiToken two-factor authentication tokens strengthen user authentication by enabling multi-factor authentication. This ensures that compromised user credentials do not provide an attacker with authenticated access to a user's account.

When devices are connected to the corporate network, device monitoring and policy enforcement can be performed over the network. However, enterprise use of mobile devices is growing rapidly, so enterprise devices may be used offline or on other networks. Installation of **FortiClient** Fabric Agent provides visibility into endpoints and implements dynamic access control both on and off of the corporate network.



Security-driven networking

As enterprise networks and attack surfaces expand with DI, the need to secure these networks grows. Security-driven networking tightly integrates an organization's network infrastructure and security architecture, enabling the network to scale and change without compromising security. Such integration reduces complexity by minimizing the number of disparate point products. It also makes it easy to leverage performance improvements, since networking and security appliances are optimized to work together.

Security-driven networking comes to the forefront in **FortiGate** next-generation firewalls (NGFWs); they are an organization's first line of defense against advanced threats. They are much more than firewalls, however. Because almost one-third of data breaches involve phishing attacks[31]—which rely upon malicious links or attachments to infect endpoints or steal user credentials—FortiGate NGFWs include a secure web gateway (SWG), which identifies and blocks attempted connections to malicious or suspicious URLs.

FortiGate NGFWs also perform secure sockets layer (SSL)/transport layer security (TLS) packet decryption and inspection. This is a critical requirement today, with an estimated 75% of enterprise network traffic protected with SSL/TLS, and about 82% of malicious traffic using encryption.[32,33] in response, **FortiGate NGFWs** use purpose-built security processors (SPUs) to minimize the performance impact of SSL/TLS traffic inspection. Integration of high-performance encrypted traffic inspection into an organization's NGFW also enables the business to avoid the overhead associated with acquiring and deploying standalone appliances throughout their network infrastructure.

If threats go undetected at the network perimeter, it is essential to prevent them from moving laterally throughout the network. Intent-based segmentation allows organizations to painlessly accomplish this by enabling segmentation of the network based upon business needs. Suspicious or malicious internal connections are blocked by default, and if a zero-day threat is identified after infection, threat intelligence is communicated through the Security Fabric to ensure that no secondary infections occur.

For this to work, an organization requires security integration across their entire enterprise network, including branch locations. **Fortinet Secure SD-WAN** provides optimized network performance and security integration for branch locations. FortiGate NGFWs integrated into SD-WAN appliances perform traffic inspection at each branch location. This improves network performance by enabling direct-to-internet connectivity for SaaS applications and services and enables WAN cost reductions.

Within a branch location, **Fortinet Secure SD-Branch** enables extension of an organization's visibility and centralized security management down to the switching layer. Fortinet Secure SD-Branch consists of FortiNAC solutions, FortiSwitch secured access switches, and **FortiAP** wireless access points monitored and controlled from a FortiGate NGFW. By integrating security across the corporate WANs, businesses simplify operations by eliminating redundancy and enable rapid, coordinated response to advanced threats.

Dynamic cloud security

As organizations transition to the cloud, expanding the organization's security deployment to cloud-based resources is essential. The Fortinet Security Fabric integrates a range of cloud-native solutions to provide security for any application and deployment environment.

Fortinet security solutions offer network security, visibility, and control in both public and private cloud deployments. FortiGate NGFWs are available in a VM form factor. This allows them to provide cloud-native security automation, VPN connectivity, network segmentation, intrusion prevention, and an SWG.

Beyond protecting against malicious content, organizations also must ensure that their cloud deployments are properly configured. Security misconfigurations are a major issue in the public cloud, with 99% of issues going unreported.[34] **FortiCWP** cloud security analytics provides visibility and control in public cloud infrastructure, including monitoring of configurations, data security, and compliance as well as integrated threat management.

Once the cloud infrastructure itself is secured, it is necessary to protect the applications running on it. A common use of public cloud deployments is hosting web applications and web APIs. **FortiWeb** provides these with cloud-native security. FortiWeb web application firewalls (WAFs) protect web applications from both known and unknown threats using a combination of signature detection, ML, and AI. In addition, as most web applications use APIs to link to web services and integrate with other tools, it is critical to secure those web APIs using schema validation and OpenAPI security to protect against potentially malicious bot activities such as scraping and analytics.

Organizations are also increasingly moving to cloud-based email solutions like Google G Suite and Microsoft Office 365. Since phishing attacks are a leading cause of security incidents and data breaches, securing cloud-based email is essential. Available as physical and virtual appliances or as a hosted service, **FortiMail** messaging security solutions protect both on-premises and cloud-based email deployments, including blocking traditional and advanced email threats and providing backup functionality to avoid the loss of sensitive information.

Beyond web applications and email, many organizations are reliant upon SaaS applications such as Google G Suite, Box, Microsoft Office 365, Dropbox, and Salesforce. **FortiCASB** cloud access security brokers (CASBs) manage the risks of security misconfiguration, provide centralized visibility and administrative control, deliver data security in SaaS applications, and ensure that SaaS application configurations maintain regulatory compliance.

AI-driven security operations

The increased volume and sophistication of malicious attacks render traditional cybersecurity solutions insufficient. Signature-based malware detection solutions are capable of detecting only half of malware attacks.[35] The use of AI and ML capabilities is essential to detecting and preventing these attacks.

FortiGuard AI enables organizations to keep ahead of cyber criminals. FortiGuard Labs collects threat data from millions of sensors worldwide and partners with over 200 global organizations. Using 5 billion-plus nodes, FortiGuard AI identifies unique features for both known and unknown threats. The volumes handled by FortiGuard Labs are immense: The team processes over 100 billion web queries every day and blocks over 3,600 malicious URL requests each second.

As threats grow in sophistication, 100% prevention is no longer possible. Advanced threat detection capabilities are essential to helping organizations avoid breaches. AI and ML capabilities integrated into **FortiDeceptor, FortiSandbox,** and **FortiInsight** help organizations to identify unknown adversaries and malware and to uncover and respond to insider threats.

As cyber threats accelerate, organizations must take advantage of strategic automation to more quickly contain and remediate threats. Using **FortiSIEM** and **FortiAnalyzer,** an organization can achieve global visibility of their network infrastructure and access AI-driven security analytics. Based on the collected data, security analysts can determine the nature and severity of threats, with support from **FortiAI** virtual analyst. But it does not stop at threat detection and prevention; **FortiSOAR** employs orchestration and automation to remediate threat intrusions that help overstretched security operations center (SOC) teams to scale and focus on threat hunting and other mission-critical tasks.

Endpoints also require AI-driven resources throughout their incident response process. **FortiEDR** endpoint detection and response (EDR) and FortiClient deliver advanced endpoint protection that includes vulnerability scanning, patching, and virtual patching and exploit prevention in both online and air-gapped environments. Additionally, if an endpoint becomes infected, FortiEDR threat detection and post-infection protection prevents malware from communicating with command and control servers or moving laterally through the network. Finally, FortiEDR offers risk-based threat response and online remediation with support for automated remediation recipes.

Fabric management center

The Fortinet Security Fabric is designed to simplify management of an organization's entire security architecture. The Fabric accomplishes this by integrating all deployed security point products, enabling them to be centrally monitored and managed.

The **FortiManager** centralized management platform and **FortiAnalyzer** centralized logging and reporting combine to provide single-pane-of-glass visibility and management of an organization's entire network infrastructure. This includes single console management, analytics, and workflow automation.

These capabilities are supported by a number of API-based integrations with Fortinet Fabric-Ready Partners. Twelve Fabric Connectors provide deep integration with third-party solutions, and API-based integration is available for over 135 Fabric-Ready Partners. For non-partner solutions, the Fortinet Security Fabric includes a REST API and DevOps scripts to enable easy integration.

As many organizations are moving operations to the cloud, a single-point-of-access and single-sign-on (SSO) solution is needed to reduce the complexity of multi-cloud deployments. **FortiCloud** provides SSO and portals to 15 Fortinet SaaS and Metal-as-a-Service (MaaS) solutions as well as a **FortiCare** services portal. With support for all major public cloud providers, the Fortinet Security Fabric simplifies any multi-cloud deployment.

By combining FortiManager, FortiAnalyzer, and FortiCloud, an organization can completely integrate their on-premises and cloud deployments. This integration enables the use of automation and orchestration to simplify security management. Additionally, by leveraging Fabric Connectors and APIs, security teams can receive real-time network health information, automate network log management, and simplify compliance reporting, all from a single pane of glass.

Manage the Risks, Pursue the Opportunities

DI enables organizations to achieve new levels of efficiency and cost savings for itself and improved experiences for its customers. However, DI initiatives also expand and change the organization's attack surface, opening up new attack vectors for cyber threats to exploit.

For organizations leading the charge in DI, acknowledging, accepting, and properly managing risks is of paramount importance. The Fortinet Security Fabric is the foundation for this. It unifies security solutions behind a single pane of glass, makes the growing digital attack surface visible, integrates AI-driven breach prevention, and automates operations, orchestration, and response. In sum, it enables organizations to create new value with DI without compromising security for business agility, performance, and simplicity.

[1] Nick Lansing, "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources," Forbes and Fortinet, 2019.

[2] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[3] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, 2019.

[4] Ibid.

[5] Gilad David Maayan, "The IoT Rundown For 2020: Stats, Risks, and Solutions," Security Today, January 13, 2020.

[6] "2019 State of the Cloud Report," Flexera, 2019.

[7] Larry Ponemon, "Third-party IoT risk: companies don't know what they don't know," ponemonsullivanreport.com, accessed February 4, 2020.

[8] Nirav Shah, "SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019," Fortinet, September 9, 2019.

[9] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, 2019.

[10] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

[11] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[12] According to internal data from FortiGuard Labs.

[13] "6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders," Fortinet, September 8, 2019.

[14] According to data from internal Fortinet research.

[15] According to internal data from FortiGuard Labs.

[16] Kelly Bissell, et al.,"The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, 2019.

[17] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

[18] Based off of internal Fortinet research.

[19] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[20] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO, March 14, 2016.

[21] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[22] ""Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)^2 Cybersecurity Workforce Study, 2019," (ISC)^2, 2019.

[23] "CIO Survey 2019: A Changing Perspective," Harvey Nash and KPMG, 2019.

[24] "2019 Payment Security Report," Verizon, 2019.

[25] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, 2019.

[26] "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources," Forbes and Fortinet, 2019.

[27] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October 14, 2019.

[28] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

[29] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October 14, 2019.

[30] "Gartner Magic Quadrant Reports," Fortinet, accessed January 22, 2020.

[31] "2019 Data Breach Investigations Report," Verizon, 2019.

[32] Alex Samonte, "TLS 1.3: What This Means For You," Fortinet, March 15, 2019.

[33] Robert Lemos, "Attackers Are Messing with Encryption Traffic to Evade Detection," Dark Reading, May 15, 2019.

[34] Charlie Osborne, "99 percent of all misconfigurations in the public cloud go unreported," ZDNet, September 24, 2019.

[35] Robert Lemos, "Only Half of Malware Caught by Signature AV," Dark Reading, December 11, 2019.

FORTINET

www.fortinet.com

March 10, 2021 6:00 PM

wp-fortinet-security-fabric-enables-digital-innovation

570099-A-0-EN

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

AGENȚIA SERVICII PUBLICE

Departamentul înregistrare și licențiere a unităților de drept

EXTRAS

din Registrul de stat al persoanelor juridice

Nr. **597339** data **27.03.2025**

Denumirea completă: **Întreprinderea Mixtă "ORANGE MOLDOVA" S.A.**
Denumirea prescurtată: **Î.M. "ORANGE MOLDOVA" S.A.**
Forma juridică de organizare: **Societate pe acțiuni**
Numărul de identificare de stat și codul fiscal (IDNO): **1003600106115**
Data înregistrării de stat: **18.03.1998**
Modul de constituire: **nou creată.**
Sediul: **MD-2071, str. Alba-Iulia, 75, mun. Chișinău, Republica Moldova.**
Obiectul principal de activitate:

1. Comerț cu ridicata al calculatoarelor, echipamentelor periferice și software-lui
2. Comerț cu ridicata de componente și echipamente electronice și de telecomunicații
3. Comerț cu amănuntul al calculatoarelor, unităților periferice și software-lui în magazine specializate
4. Comerț cu amănuntul al echipamentului pentru telecomunicații în magazine specializate
5. Comerț cu amănuntul al echipamentelor audio/video în magazine specializate
6. Comerț cu amănuntul prin intermediul caselor de comenzi sau prin Internet
7. Activități de editare a altor produse software
8. Activități de comunicații electronice prin rețele cu cablu
9. Activități de comunicații electronice prin rețele fără cablu (exclusiv prin satelit)
10. Alte activități de comunicații electronice
11. Activități de realizare a soft-ului la comandă (software orientat client)
12. Activități de consultanță în tehnologia informației
13. Activități de management (gestiune și exploatare) a mijloacelor de calcul
14. Alte activități de servicii privind tehnologia informației
15. Prelucrarea datelor, administrarea paginilor web și activități conexe
16. Activități ale agenților și broker-ilor de asigurări
17. Activități de contabilitate și audit financiar; consultanță în domeniul fiscal
18. Activități de consultanță pentru afaceri și management
19. Alte servicii de furnizare a forței de muncă
20. Repararea calculatoarelor și a echipamentelor periferice
21. Repararea echipamentelor de comunicații

Capitalul social: **179499609** lei,

Administrator: **SURUGIU OLGA, IDNP 0981202021274,**
în funcție pînă la data de 31.03.2028

Beneficiar efectiv: Societate cotată pe o piață reglementată care face obiectul cerințelor de divulgare a informațiilor în conformitate cu standardele internaționale echivalente care asigură transparența corespunzătoare informațiilor privind exercitarea dreptului de proprietate asupra unei cote părți din numărul de acțiuni ori din drepturile de vot sau prin participația în capitalul social al persoanei juridice respective, sau prin exercitarea controlului prin alte mijloace.

Prezentul extras este eliberat în temeiul art.34 al Legii nr.220-XVI din 19 octombrie 2007 privind înregistrarea de stat a persoanelor juridice și a întreprinzătorilor individuali și confirmă datele din Registrul de stat la data de: **27.03.2025**.

Registrator în domeniul înregistrării de stat **Dragomir Ala**

EB 0527920

IDNO 1002600024700 REPUBLICA MOLDOVA CHIȘINĂU 004

Date cu caracter personal

Date publice / Date despre persoana juridică

Criterii de accesare:

- **IDNO:** 1003600106115

Date de bază

- **IDNO/Cod Fiscal:** 1003600106115
- **Denumire:** Întreprinderea Mixtă ORANGE MOLDOVA S.A.
- **Data înregistrării:** 18.03.1998
- **Forma juridică:** Societate pe acţiuni de tip închis
- **Lichidată:** Nu
- **Adresa juridică:** mun. Chişinău, sec. Buiucani, str. Alba-Iulia, 75
- **Conducători:**
  - SURUGIU OLGA [Administrator]

Restanțe față de bugetul de stat

Nr.	Tipul bugetului	Suma (MDL)
1	Bugetul de stat și local	0,00
2	Bugetul de stat	0,00
3	Bugetele unităților administrativ-teritoriale	0,19
4	Bugetul asigurărilor sociale de stat	399,17
5	Fondurile asigurărilor obligatorii de asistență medicală	0,00
6	Fondul de susținere a populației	0,00

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

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: Lenovo, HP, Dell, Fortinet, Cisco, Trellix, 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 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 minim 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, schimbare echipament cu produse Fortinet existente în stoc, suport tehnic etc.

Termenul de prestare a serviciilor

Serviciile vor fi prestate pentru toata perioada de garanție a echipamentelor, licențelor, produselor.

Termenul de prestare a serviciilor poate fi prelungit ulterior la solicitarea Beneficiarului.

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:

Fluxul de lucru în perioada de exploatare operațională

NIVEL	DESCRIERE
Critice – 24/7, timp de reacție 15 minute, timp de răspuns garantat 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.
Majore – 24/7, timp de reacție 15 minute, timp de răspuns garantat 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.
Minore – 24/7, timp de reacție 15 minute, timp de răspuns garantat 12 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.

Nota: Suport tehnic va fi asigurat 24 de ore pe zi, 7 zile pe săptămână, 365 de zile pe an.

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 4:15 prin metodele definite şi în dependență de tipul incidentului începe procedura de depanare, în acest caz timpul de reacție este de 15 minute.
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 15 minute 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 5:00, în acest caz timpul de răspuns este o (1) oră.
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 15 minute a fost confirmată recepționarea cererii de suport, specialiştii se deplasează la locul incidentului. Timpul de înlăturare a

problemei va fi în maxim 24 ore 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 9X5. 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” Tel. +33 4 89 87 05 55 https://support.fortinet.com/WebChatOnline.aspx Clientul poate utiliza şi Service Desk al companiei Orange Moldova: Tel. +373 22 977 700 Fax. +373 22 977 710
- Lista de persoane responsabile pe tip de incident şi telefoane de contact: Ion Cozma email: ion.cozma@orange.com Tel. +37369198955 Anatolie Bulgaru Email: anatolie.bulgaru@orange.com Tel. +37369198955 Robert Gutuleac email: robert.gutuleac@netsafe.md Tel. +373 (68) 115511 Netsafe Distribution Suport Tehnic: http://support.netsafe.ro/
- FortiCare Support: Technical Assistance Center interfața pentru cererile de suport şi/sau interfața la sistemul automatizat de înregistrare a cererilor de suport “service desk”: https://customersso1.fortinet.com/saml-idp/jrx0g5n1etn0aoy9/login/?SAMLRequest=hZLJTsMwElZfJfl9azdqtZUKFaISS0QKBy7IOJPWKLGDZwzl7XFS1ks52Rr9M%2F83ywxFU7d86Winb%2BHFAVKwXs3ZYzmRaTWqxuFofFKGw2okwpPx2P8G3ZMOs2xQsuAeLCqj5yyLEhasER2sNZLQ5ENJNgiTYZgMNumEZylPplE2nTywYOVdlBbUZ%2B6lWuRxLB2SaXw9NGlUGesVQJE0Tdwhhqps42e7T7YjnQLpRJj3aVybrdlxC86NldD3MGeVqBE6llwgqlf4juTWkJGmPlW6VHo7Z85qbgQq5Fo0gJwkL5ZXl9z3wp8OluQXm00e5jfFhgVLRLAd9JnR6DxqAfZVSbi7vfxpA13bevi%2FHRTFzYE1Erjbs2Df1Bp5P%2FrjGO0nM1vMOjXvJ2x%2F5R9PF1%2FEbPEvXwMkSkGiR5zFv%2BwO3i2%2F9vXXq9zUSr53l28EHbfvlqoMq17KncYWpKoU%2BMNZ1rV5O7MgyC%2BlrPP7iRcH17%2FXuPgA&RelayState=UmV0dXJuVXJsPUwzUnBZMnRsZEM5cGJtUmxlQzVoYzNCNCZoa2V5PQ%3D%3D
- 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 Distribuitor: 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.

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 engleză sau limba rusă.

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 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. Executorul va livra alt echipament existent pe perioada soluționării problemei.

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, produsele este definit ca Moderat Critice.

Acoperire	Timp de Răspuns
Luni – Duminica, 24X7	o (1) oră

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 1 ora lucrătoare (intervalul de timp 24/24, iar suport tehnic 24 de ore pe zi, 7 zile pe săptămână, 365 de zile pe an. 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. 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: - diagnosticarea componentelor, schimbarea sau repararea componentelor; - serviciu avansat de înlocuire pentru defecțiuni hardware; - actualizări firmware și generale (web/online); - acces la asistență prin portal web, chat online și telefon; - acces rapid și ușor în scris la solicitările de asistență tehnică; - înlăturarea problemei nu va depăşi 30 zile lucrătoare; - update-uri automate de semnături de securitate pentru îndeplinirea tuturor funcționalităților solicitate, inclusiv protecție avansată malware, FortiGuard IPS; - acces continuu la portalul de suport; remedierea defecțiunilor, în speță de nivel hardware, se vor executa în sediul Beneficiarului de către personalul calificat din contul Orange Moldova, utilizând componentele livrate de producătorul echipamentului; - lucrările de deservire şi reparație a echipamentului se va executa în sediul Beneficiarului de către personalul calificat din contul Orange Moldova, utilizând componentele noi livrate de producătorul echipamentului; toate serviciile legate de înlăturarea defecțiunilor sau problemelor (inclusiv corespondența cu producătorul, transportarea, vămuirea pieselor de schimb și celor defectate, etc.) vor fi efectuate de către Prestator din contul său. Garanția include costul pieselor şi al manoperei. În cazul unor defecțiuni mai grave, echipamentele se vor transporta la sediul Prestatorului de către acesta; la solicitarea Beneficiarului lucrările de diagnosticare, deservire / reparație se va executa de către personalul Prestatorului şi în afară zilelor de lucru (în zilele de odihnă).

FORTINET
Training Institute

FORTINET
CERTIFIED
PROFESSIONAL
Security
Operations

This certifies that

Cozma Ion

has achieved

Fortinet Certified Professional Security Operations

Date of achievement: October 11, 2024
Valid until: October 11, 2026
Certification validation number: 6348820708CI

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/admin/tool/certificate/index.php

FORTINET
Training Institute

FORTINET
CERTIFIED
ASSOCIATE
Cybersecurity

This certifies that

Vlad MALAI

has achieved

Fortinet Certified Associate in Cybersecurity

Date of achievement: November 3, 2023
Valid until: November 3, 2025
Certification validation number: 2090105850VM

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/admin/tool/certificate/index.php

FORTINET
Training Institute

FORTINET
CERTIFIED
FUNDAMENTALS
Cybersecurity

This certifies that

Vlad MALAI

has achieved

Fortinet Certified Fundamentals in Cybersecurity

Date of achievement: November 1, 2023

Valid until: November 1, 2025

Certification validation number: 3818029707VM

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/admin/tool/certificate/index.php

FORTINET
Training Institute

FORTINET
CERTIFIED
PROFESSIONAL
Network
Security

This certifies that

Vlad MALAI

has achieved

Fortinet Certified Professional Network Security

Date of achievement: October 2, 2024
Valid until: October 2, 2026
Certification validation number: 0139142541VM

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/admin/tool/certificate/index.php

FORTINET

NSE Certification Program

This certifies that
Daniel Gribinet
has achieved
NSE 4 Network Security Professional

Date of achievement: June 5, 2023

Valid until: June 5, 2025

Certification Validation number: ADX2BwAhoZ

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET
Training Institute

FORTINET
CERTIFIED
PROFESSIONAL
Network
Security

This certifies that

Cozma Ion

has achieved

Fortinet Certified Professional Network Security

Date of achievement: October 11, 2024

Valid until: October 11, 2026

Certification validation number: 7986633482CI

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/admin/tool/certificate/index.php

Certificate of Authorized Reseller

Date: 7 April, 2025

Agentia Servicii Publice
MD-2012, MOLDOVA, mun.Chisinau, str. Puskin, 42
Reference: 32500000-8 - Echipament de telecomunicatii

Fortinet, Inc. (hereinafter “Fortinet”) is a US public company, domiciled at 909 Kifer Road Sunnyvale, California 94086, United States, which is especially dedicated to the design and manufacture of network security components and devices and operates through a channel of independent distributors and resellers (referred to as "FortiPartner/s"). For more details about the company you can visit: http://www.fortinet.com.

Fortinet hereby confirms that IM Orange Moldova SA, having its registered place of business at: str. Alba Iulia 75, Chisinau, MD 2075, Moldova, Republic of, as of date of this letter is an authorized FortiPartner to sell Fortinet products with the following designations and solely in the following territory:

- Level of Engagement: Regional
- Business Model: Integrator, MSSP
- Territory: MD

Provided the FortiPartner identified above has purchased applicable support services from Fortinet and the applicable support services have been effectively registered and contracted with Fortinet, Fortinet agrees and undertakes that Fortinet would provide support for the applicable Fortinet products according to the terms of the support agreement,available at https://support.fortinet.com. Fortinet Products are shipped subject to the terms of its then-current End User License Agreement, available at http://www.fortinet.com/doc/legal/EULA.pdf, which sets forth Fortinet's warranty.

This certificate is subject to the FortiPartner maintaining its FortiPartner Agreement and strictly adhering to Fortinet’s FortiPartner guidelines. Fortinet’s partner program and its guidelines are available for review at http://www.fortinet.com/partners/partner_program/fpp.html. Not withstanding anything to the contrary herein, authorized FortiPartners do not represent Fortinet and can not make statements that are binding on behalf of Fortinet.

Please note that this Certificate of Authorized Reseller shall not be used for U.S. State or U.S. local government entity (SLED) opportunities. Please contact your Fortinet representative if a SLED opportunity is sought.

Fortinet, Inc.
Thomas Schmidt
Senior Vice President, Legal & Compliance
Manufacturer Confirmation
2025
Status as Fortinet Reseller
Fortinet, Inc.
Kifer Road
Sunnyvale, California 94086
United States of America
duly incorporated under the laws of the State of Delaware

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

Întreprinderea mixtă "Orange Moldova" S.A.
GM 27.12.2023
Ieşire nr 11300

PROCURĂ

mun. Chişinău

Întreprinderea Mixtă „ORANGE MOLDOVA" S.A. (Societatea), persoană juridică a Republicii Moldova, IDNO 1003600106115, sediu: MD-2071, mun. Chişinău, str. Alba Iulia, nr. 75, reprezentată prin Directorul General Dna **Olga SURUGIU**, împuternicește pe Dl **Anatolie BULGARU**, cod personal 0972805016066, ca în timpul absenței Directorului Vânzări corporative şi servicii post-vânzări sau a altei imposibilități de exercitare de către acesta a atribuţiilor sale de serviciu, să reprezinte Societatea în relaţiile cu utilizatorii finali, persoane juridice, solicitanți ai serviciilor şi produselor de comunicații electronice şi accesorii comercializate de Î.M. „Orange Moldova" S.A., să semneze contracte şi anexe la acestea pentru prestarea serviciilor Virtual PBX/Business PBX, serviciilor M2M şi echipamente aferente prestării acestor servicii, serviciilor Microsoft Cloud, serviciilor Protecție DDoS, serviciilor Cert Pro, serviciilor Business Internet Security, serviciilor Software Antivirus, serviciilor si produselor care pot fi clasificate ca IoT si ICT (Internet of Things/ Information and Communications Technology), contracte de vânzare-cumpărare de echipamente aferente tehnologiilor de informare si comunicare „ICT", contracte de vânzare-cumpărare software (licențe, aplicații, software elaborat la comandă), contracte de vânzare-cumpărare a serviciilor de expertiză în domeniul Securității Informaționale, serviciilor Microsoft Cloud, contracte de elaborarea software la comandă, contracte de confidențialitate (Non Disclosure Agreement), inclusiv să modifice, prelungească şi înceteze astfel de contracte, să semneze Ofertele comerciale adresate acestor persoane în numele Societății şi să îndeplinească alte acțiuni şi formalități pentru îndeplinirea acestei împuterniciri.

Dl **Anatolie BULGARU** poate angaja Societatea şi semna / încheia actele juridice menționate mai sus în limitele şi în conformitate cu Ofertele comerciale publice ale Societății, precum şi Ofertele comerciale speciale aprobate în conformitate cu documentele interne ale Societății.

Prezenta procură este valabilă de la 01 ianuarie 2024 până la 31 decembrie 2026 şi este emisă fără dreptul de transmitere unei alte persoane.

Director General **Olga SURUGIU**

Întreprinderea mixtă "Orange Moldova" S.A. mun. Chişinău, Republica Moldova IDNO 1003600106115