Formularul ofertei pentru bunuri şi servicii

Data depunerii ofertei: **01.10.2025**

Procedura de achiziţie Nr.: **ocds-b3wdp1-MD-1758554929432 (21479101)**

Anunţ de participare Nr.: **42 (patruzeci şi doi)**

Către: ***Întreprinderea de Stat „Poşta Moldovei”***

Î.M. ORANGE Moldova S.A. **declară că:**

a) Au fost examinate şi nu există rezervări fată de documentele de atribuire, inclusiv modificările nr.

-

(introduceţi numărul şi data fiecărei modificări, dacă au avut loc)

b) ***Î.M. ORANGE Moldova S.A.*** se angajează să presteze, în conformitate cu documentele de atribuire şi condiţiile stipulate în specificaţiile tehnice şi preţ, următoarele:

Echipament Firewall

c) Suma totală a ofertei fără TVA constituie:

448,332.66 lei (patru sute patruzeci şi opt de mii trei sute treizeci şi doi lei, 66 bani)

(introduceţi preţul pe loturi (unde e cazul) şi totalul ofertei în cuvinte şi cifre, indicând sumele şi valutele respective)

d) Suma totală a ofertei cu TVA constituie:

537,999.19 lei (cinci sute treizeci şi şapte de mii nouă sute nouăzeci şi nouă, 19 bani)

(introduceţi preţul pe loturi (unde e cazul) şi totalul ofertei în cuvinte şi cifre, indicând sumele şi valutele respective)

e) Prezenta ofertă va rămâne valabilă pentru perioada de timp de ***60*** zile, începând cu data-limită pentru depunere a ofertei, în conformitate cu **Anexa nr. 22 *„Specificaţii tehnice”* şi Anexa nr. 23 *„Specificaţii de preţ”***, astfel va rămâne obligatorie şi va putea fi acceptată în orice moment până la expirarea acestei perioade;

f) Compania semnatară, afiliaţii sau sucursalele sale, inclusiv fiecare partener sau subcontractor ce fac parte din contract, nu au fost declarate neeligibile în baza prevederilor legislaţiei în vigoare sau a regulamentelor cu incidenţă în domeniul achiziţiilor publice.

Data completării 01.10.2025

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

Specificații tehnice

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1758554929432 (21479101) din 22 septembrie 2025

Obiectul achiziției: Echipament Firewall

Denumirea serviciilor / bunurilor	Denumirea modelului/ serviciilor/ bunurilor	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Echipament Firewall						
Echipament Firewall	Fortigate FG-400F	SUA	Fortinet	**1. Cerințe generale** **1.1.** Echipamentul ofertat trebuie să fie **nou, calitativ**, produs de **producători renumiți, recunoscuți internațional** în domeniul TI; **1.2.** Configurația echipamentului trebuie să fie compusă din componente **reciproc compatibile**, care să asigure funcționarea optimă a sistemului în ansamblu; **1.3.** În cazul existenței **certificatelor de compatibilitate și atestare a calității**, o copie sau referința web trebuie inclusă în ofertă; **1.4.** Ofertantul va prezenta **caracteristicile tehnice oficiale** (fișă/broșură/catalog/pagină web) pentru identificarea parametrilor produsului ofertat. **2. Caracteristici minime HARDWARE** **2.1. Chassis** • 1U **2.2. Configurație HA**	<table><tr><th>Part number</th><th>Descriere</th><th>Cantitate</th></tr><tr><td>FG-200G-BDL-950-12</td><td>FortiGate-200G 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)</td><td>2</td></tr></table> 1. Cerințe generale 1.1. Echipamentul ofertat este nou, calitativ, produs de producători renumiți, recunoscuți internațional în domeniul TI; 1.2. Configurația echipamentului este compusă din componente reciproc compatibile, care asigură funcționarea optimă a sistemului în ansamblu; 1.3. În cazul existenței certificatelor de compatibilitate și atestare a calității, o	NA

Denumirea serviciilor / bunurilor	Denumirea modelului/ serviciilor/ bunurilor	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				• Active-Active • Active-Pasive • Clustering **2.3. Interfețe** • 2 × GE RJ45 MGMT/HA Ports • 8 × GE RJ45 Ports • 8 × 5/2.5/GE SFP Slots • 8 × 10GE SFP+/SFP Slots • 4 × GE SFP Slots • 2 × 10GE SFP+ transceiver module, short range (pentru sisteme cu SFP+ și SFP/SFP+ Slots) • 2 × 10GE SFP+ transceiver module, certificat pentru HPE Aruba 5412Rzl2 **2.4. Alimentare** • 2 × surse de alimentare redundante (PSU) • 2 × cabluri de alimentare • Conectare PDU **2.5. Performanță (conform specificațiilor producătorului)** • IPS Throughput: până la 9 Gbps • NGFW Throughput: până la 7 Gbps • Firewall Latency (64 byte, UDP): 4.36 µs • Firewall Throughput (Packet per Second): 39.75 Mpps • Concurrent Sessions (TCP): 11 milioane • Firewall Policies: 10 000 • IPsec VPN Throughput (512 byte): 36 Gbps	copie sau referința web este inclusă în ofertă; 1.4. Orange Moldova a prezentat caracteristicile tehnice oficiale prin anexare la oferta a fișei/broșurei si link catre pagină web (https://www.fortinet.com/resources/data-sheets/fortigate-200g-series) pentru identificarea parametrilor produsului ofertat. 2. Caracteristici HARDWARE 2.1. Chassis • 1U 2.2. Configurație HA • Active-Active • Active-Pasive • Clustering 2.3. Interfețe • 2 × GE RJ45 MGMT/HA Ports • 8 × GE RJ45 Ports • 8 × 5/2.5/GE SFP Slots • 8 × 10GE SFP+/SFP Slots • 4 × GE SFP Slots • 2 × 10GE SFP+ transceiver module, short range (pentru sisteme cu SFP+ și SFP/SFP+ Slots) • 2 × 10GE SFP+ transceiver module, certificat pentru HPE Aruba 5412Rzl2 2.4. Alimentare • 2 × surse de alimentare redundante (PSU) • 2 × cabluri de alimentare • Conectare PDU	

Denumirea serviciilor / bunurilor	Denumirea modelului/ serviciilor/ bunurilor	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				• SSL-VPN Throughput: 3 Gbps SSL Inspection Throughput: 7 Gbps **3. Funcţionalităţi de securitate** **3.1.** Firewall stateful **3.2.** Router cu suport pentru protocoale dinamice (RIP, OSPF, BGP, Multicast PIM-DM/PIM-SM, IGMP v1/v2/v3, IS-IS) **3.3.** Gruparea interfeţelor în zone de securitate şi rutare între acestea **3.4.** Policy-based routing **3.5.** NAT, PAT şi Transparent Bridge (inclusiv NAT per politică) **3.6.** VLAN Tagging 802.1Q **3.7.** Criptare: IPSec VPN, SSL VPN **3.8.** QoS şi Traffic Shaping **3.9.** IDS/IPS (detecţie şi prevenire intruziuni) **3.10.** Protecţie Anti-Malware **3.11.** Filtrare URL, DNS şi Video **3.12.** Control şi identificare aplicaţii + traffic shaping per aplicaţie **3.13.** Clasificare granulară a aplicaţiilor (categorie, popularitate, tehnologie, risc) **3.14.** Detectare anomalii de protocol **3.15.** Protecţie IPv4/IPv6 DDoS **3.16.** Scheduling pentru politici de firewall **3.17.** Actualizări automate de semnături de securitate **Notă:** Toate funcţionalităţile de securitate, sistemul de operare şi platforma hardware trebuie să aparţină **aceluiaşi producător**. **4. Funcţionalităţi de administrare şi autentificare**	2.5. Performanţă (conform specificaţiilor producătorului) • IPS Throughput: până la 9 Gbps • NGFW Throughput: până la 7 Gbps • Firewall Latency (64 byte, UDP): 4.36 µs • Firewall Throughput (Packet per Second): 39.75 Mpps • Concurrent Sessions (TCP): 11 milioane • Firewall Policies: 10 000 • IPsec VPN Throughput (512 byte): 36 Gbps • SSL-VPN Throughput: 3 Gbps SSL Inspection Throughput: 7 Gbps 3. Funcţionalităţi de securitate 3.1. Firewall stateful 3.2. Router cu suport pentru protocoale dinamice (RIP, OSPF, BGP, Multicast PIM-DM/PIM-SM, IGMP v1/v2/v3, IS-IS) 3.3. Gruparea interfeţelor în zone de securitate şi rutare între acestea 3.4. Policy-based routing 3.5. NAT, PAT şi Transparent Bridge (inclusiv NAT per politică) 3.6. VLAN Tagging 802.1Q 3.7. Criptare: IPSec VPN, SSL VPN 3.8. QoS şi Traffic Shaping 3.9. IDS/IPS (detecţie şi prevenire intruziuni) 3.10. Protecţie Anti-Malware 3.11. Filtrare URL, DNS şi Video	

Denumirea serviciilor / bunurilor	Denumirea modelului/ serviciilor/ bunurilor	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
				4.1. Administrare: Web UI, SSH, CLI **4.2.** Utilizatori/administratori cu drepturi configurabile **4.3.** Export/import configurație **4.4.** Monitorizare grafică (real-time și istorică) **4.5.** Suport syslog și SNMP v1/v2c/v3 **4.6.** Notificare prin e-mail pentru alerte **4.7.** Definire locală utilizatori **4.8.** Integrare cu Windows AD **4.9.** Suport Xauth pentru IPSec VPN Autentificare utilizatori prin LDAP, certificate digitale PKI X.509 și autentificare doi factori **5. Eficiență energetică** Certificat **Green-e® Energy** sau echivalent. **6. Garanție și suport** **6.1. Minim 12 luni** garanție și suport, incluzând: • Înlocuirea echipamentului în caz de defecțiune hardware • Diagnosticare și suport pentru probleme tehnice • Asigurarea pieselor de schimb • Suport tehnic producător 24/7/365 • Actualizări firmware (majore și minore) Actualizări automate de semnături de securitate	3.12. Control și identificare aplicații + traffic shaping per aplicație 3.13. Clasificare granulară a aplicațiilor (categorie, popularitate, tehnologie, risc) 3.14. Detectare anomalii de protocol 3.15. Protecție IPv4/IPv6 DDoS 3.16. Scheduling pentru politici de firewall 3.17. Actualizări automate de semnături de securitate Notă: Toate funcționalitățile de securitate, sistemul de operare și platforma hardware trebuie să aparțină aceluiași producător. 4. Funcționalități de administrare și autentificare 4.1. Administrare: Web UI, SSH, CLI 4.2. Utilizatori/administratori cu drepturi configurabile 4.3. Export/import configurație 4.4. Monitorizare grafică (real-time și istorică) 4.5. Suport syslog și SNMP v1/v2c/v3 4.6. Notificare prin e-mail pentru alerte 4.7. Definire locală utilizatori 4.8. Integrare cu Windows AD 4.9. Suport Xauth pentru IPSec VPN Autentificare utilizatori prin LDAP, certificate digitale PKI X.509 și autentificare doi factori 5. Eficiență energetică	

Denumirea serviciilor / bunurilor	Denumirea modelului/ serviciilor/ bunurilor	Țara de origine	Producă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
					Certificat Green-e® Energy sau echivalent. 6. Garanție și suport 6.1. 12 luni garanție și suport, incluzând: • Înlocuirea echipamentului în caz de defecțiune hardware • Diagnosticare și suport pentru probleme tehnice • Asigurarea pieselor de schimb • Suport tehnic producător 24/7/365 • Actualizări firmware (majore și minore) • Actualizări automate de semnături de securitate	

Data completării 01.10.2025
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 Finanțelor
nr. 115 din 15.09.2021

Specificații de preț

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1758554929432 (21479101) din 22 septembrie 2025									
Obiectul achiziției: Echipament Firewall									
Cod CPV	**Denumirea bunurilor/serviciilor**	**Cantitatea și U/M**	**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**
32420000-3	**Echipament Firewall**								
	Echipament Firewall FortiGate-200G 1 Year Unified Threat Protection (UTP) 2 buc	2 buc	2	224,166.33	268,999.60	448,332.66	537,999.19	*Livrarea se va efectua din contul operatorului economic, la adresa mun. Chișinău, str. Piața Gării, nr. 3, în termen de 30 zile lucrătoare din data semnării contractului.*	MD36ML00000000225183434
	TOTAL					448,332.66	537,999.19		

Data completării 01.10.2025
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

I.P. "AGENȚIA SERVICII PUBLICE"
Departamentul înregistrare a unităților de drept (DÎUD)

Extras
din Registrul de stat al persoanelor juridice
nr. **188046** din **26.09.2025**

Denumirea completă: **Întreprinderea Mixtă "ORANGE MOLDOVA" S.A.**
Denumirea prescurtată: **Î.M. "ORANGE MOLDOVA" S.A.**
Forma juridică de organizare: **Societate pe acţiuni.**
Numărul de identificare de stat și codul fiscal: **1003600106115**
Data înregistrării de stat: **18.03.1998**
Sediu: **MD-2071, strada Alba-Iulia 75, mun. Chişinău, Republica Moldova**
Genurile de activitate:

1. **Comerţ cu ridicata al calculatoarelor, echipamentelor periferice şi software-lui;**
2. **Comerţ cu ridicata de componente şi echipamente electronice şi de telecomunicaţii;**
3. **Comerţ cu amănuntul al calculatoarelor, unităţilor periferice şi software-lui în magazine specializate;**
4. **Comerţ cu amănuntul al echipamentului pentru telecomunicaţii în magazine specializate;**
5. **Comerţ cu amănuntul al echipamentelor audio/video în magazine specializate;**
6. **Comerţ cu amănuntul prin intermediul caselor de comenzi sau prin Internet;**
7. **Activităţi de editare a altor produse software;**
8. **Activităţi de comunicaţii electronice prin reţele cu cablu;**
9. **Activităţi de comunicaţii electronice prin reţele fără cablu (exclusiv prin satelit);**
10. **Alte activităţi de comunicaţii electronice;**
11. **Activităţi de realizare a soft-ului la comandă (software orientat client);**
12. **Activităţi de consultanţă în tehnologia informaţiei;**
13. **Activităţi de management (gestiune şi exploatare) a mijloacelor de calcul;**
14. **Alte activităţi de servicii privind tehnologia informaţiei;**
15. **Prelucrarea datelor, administrarea paginilor web şi activităţi conexe;**
16. **Activităţi ale agenţilor şi broker-ilor de asigurări;**
17. **Activităţi de contabilitate şi audit financiar; consultanţă în domeniul fiscal;**
18. **Activităţi de consultanţă pentru afaceri şi management;**
19. **Alte servicii de furnizare a forţei de muncă;**
20. **Repararea calculatoarelor şi a echipamentelor periferice;**
21. **Repararea echipamentelor de comunicaţii;**

Capitalul social: **179499609 Lei**
Administrator (Director general): **SURUGIU OLGA, în funcţie până la data de 31.03.2028.**

Prezentul extras este eliberat în temeiul art. 34 al Legii nr.220/2007 privind înregistrarea de stat a persoanelor juridice şi a întreprinzătorilor individuali şi confirmă datele din Registrul de stat la data de 26.09.2025

Specialist coordonator
Diana Nasian-Nicolaev
tel. 022-20-7826

INSTITUTIA PUBLICA AGENTIA SERVICII PUBLICE
IDNO 1002600024700
REPUBLICA MOLDOVA
CHIȘINĂU

EB 0588476

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

Modificat

SERVICIUL FISCAL DE STAT
ГОСУДАРСТВЕННАЯ НАЛОГОВАЯ СЛУЖБА

CERTIFICAT

Aprobat de către Inspectoratul Fiscal Principal de Stat
prin ordinul nr. 04 din 06.01.2004

DE ÎNREGISTRARE A SUBIECTULUI IMPUNERII CU TVA

7800044

SUBIECTUL IMPUNERII ÎNREGISTRAT Зарегистрированный субъект налогообложения	
Denumirea Наименование	ÎM "Orange Moldova" SA
Data înregistrării Дата регистрации	01.04.1998
Adresa juridică Юридический адрес	mun. Chișinău str. Alba Iulia, 75
Codul fiscal Фискальный код	1003600106115
Numărul de înregistrare ca subiect impozabil cu TVA Номер регистрации в качестве субъекта налогообложения НДС	7800044

Tipul activității economice desfășurate în conformitate cu clasificatorul activităților Тип осуществляемой деятельности согласно статистическому классификатору деятельности	6420

PRIMA PERIOADĂ FISCALĂ ПЕРВЫЙ НАЛОГОВЫЙ ПЕРИОД	
din от 01.04.1998	**pînă la** до 01.08.1998

PERIOADĂ FISCALĂ ULTERIOARĂ ПОСЛЕДУЮЩИЙ НАЛОГОВЫЙ ПЕРИОД	
din от	**pînă la** до

Șeful DAGII

LOC PENTRU ŞTAMPILĂ
МЕСТО ДЛЯ ПЕЧАТИ

Z. Morari

DATA ANULĂRII ÎNREGISTRĂRII ДАТА АННУЛИРОВАНИЯ РЕГИСТРАЦИИ	

LOC PENTRU ŞTAMPILĂ
МЕСТО ДЛЯ ПЕЧАТИ

I.S. F.E.P. «Tipografia Centrală»

Dlui Alexandru Simonov
Head of Treasury I.M. ORANGE MOLDOVA S.A.

08 decembrie 2023
C180/E02366

CERTIFICAT

Prin prezenta, BC "MAIB" S.A. vă informează că sucursala "Petru Movilă" și-a sistat activitatea, astfel pentru efectuarea operațiunilor bancate urmează să utilizați următoarele date bancare:

Beneficiar:	I.M. ORANGE MOLDOVA S.A.
Cod Fiscal:	1003600106115
Banca Beneficiară:	BC MAIB S.A. Sucursala MAIB PARK
BIC:	AGRNMD2X522
IBAN:	MD64AG000000225110801767
Număr cont:	225110801767
Valuta cont:	Leu moldovenesc

Certificatul este eliberat la solicitarea Î.M. "ORANGE MOLDOVA" S.A. pentru a fi prezentat la cerere.

Cu respect,

Vladimir Bîrsan,
Șef al Departamentului Clienți Corporativi

Ex: Svetlana Velescu
Tel. 0699 35 371

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

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

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

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

Nr d/o	Obiectul contractului	Denumirea/numele beneficiarului/ Adresa	Calitatea Furnizorului /Prestatorului*)	Preţul contractului/ valoarea bunurilor/serviciilor livrate/prestate	Perioada de livrare/prestare (luni)
1	Echipament IT/Retea IP/Securitate Inf.	B.C. Victoriabank S.A.	contractant unic	360,000.00 USD inclusiv TVA.	Livrare unica anul 2021
2	Echipament IT/Retea IP/Securitate Inf.	BC ”MAIB” S.A.	contractant unic	130,000.00 EUR inclusiv TVA.	Livrare unica anul 2022
3	Echipament IT/Retea IP/Securitate Inf.	Noction S.R.L.	contractant unic	20,000.00 USD inclusiv TVA	Livrare unica anul 2022
4	Echipament IT/Retea IP/Securitate Inf.	IP STISC	contractant unic	5,745,000.00 MDL inclusiv TVA	Livrare unica anul 2022
5	Echipament IT/Retea IP/Securitate Inf.	IT-Lab Grup SRL	contractant unic	6,300.00 EUR inclusiv TVA.	Livrare unica anul 2022
6	Echipament IT/Retea IP/Securitate Inf.	Health Forever International SRL	contractant unic	27,000.00 EUR inclusiv TVA	Livrare unica anul 2023
7	Echipament IT/Retea IP/Securitate Inf.	ICT Solutii SRL	contractant unic	300,000.00 EUR inclusiv TVA.	Livrare unica anul 2023
8	Solutie IT/ Securitate Inf.	BIROUL DE CREDIT S.R.L	contractant unic	21,000.00 MDL inclusiv TVA.	Livrare unica anul 2023
9	Solutie IT/ Securitate Inf.	S.A. FEE - NORD	contractant unic	69,000.00 MDL inclusiv TVA.	Livrare unica anul 2023
10	Solutie IT/ Securitate Inf.	Agenţia de Stat pentru Proprietatea Intelectuală (AGEPI)	contractant unic	116,000.00 MDL inclusiv TVA.	Livrare unica anul 2024

Data completării 01.10.2025

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

Anexa nr. 3

Denumirea operatorului economic: **Î.M. „Orange Moldova" S.A.**
Titlul achiziției: **Echipament Firewall**
Nr. procedurii de achiziție: *ocds-b3wdp1-MD-1758554929432 (21479101)*

DECLARAȚIE
pe proprie răspundere privind îndeplinirea criteriilor de calificare şi selecție

Subsemnatul, **Anatolie Bulgaru** reprezentantul legal al **Î.M. „Orange Moldova" S.A.** în calitate de ofertant, la achiziția **Echipament Firewall** organizată de către **Î.S."Poșta Moldovei",** declar pe propria răspundere, sub sancțiunea excluderii din procedura de achiziție și a sancțiunilor aplicate faptei de fals în acte publice, că în conformitate cu situațiile prevăzute la:

1. Art. 67, alin. (3) și (4) al Legii nr. 74 din 2020 privind achizițiile în sectoarele energeticii, apei, transporturilor și serviciilor poștale:

1.1. În ultimii 5 ani, nu am fost condamnați, prin hotărâre definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, pentru finanțarea terorismului, exploatarea prin muncă a copiilor și pentru alte forme de trafic de persoane.

1.2. Nicio persoană ce este membru al organismului de administrare, de conducere sau de control al respectivului ofertant/candidat sau are putere de reprezentare, de decizie sau de control în cadrul acestuia nu a fost condamnată printr-o hotărâre definitivă a unei instanțe de judecată pentru infracțiunile prevăzute la **pct. 1.1.**;

2. Art. 68 al Legii, alin. (1) nr. 74 din 2020 privind achizițiile în sectoarele energeticii, apei, transporturilor și serviciilor poștale:

2.1. Nu ne aflăm în oricare dintre situațiile prevăzute la art. 19 al Legii 131 din 2015 privind achizițiile publice:

2.1.1. În ultimii 5 ani, nu am fost condamnați, prin hotărârea definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, finanțarea terorismului, exploatarea prin muncă a copiilor și alte forme de trafic de persoane;

2.1.2. Nicio persoană ce este membru al organismului de administrare, de conducere sau de control al respectivului ofertant/candidat sau are putere de reprezentare, de decizie sau de control în cadrul acestuia nu a fost condamnată printr-o hotărâre definitivă a unei instanțe de judecată pentru infracțiunile prevăzute la **pct. 2.1.1.**;

2.1.3. Nu ne aflăm în proces de insolvabilitate ca urmare a hotărârii judecătorești;

2.1.4. Ne-am îndeplinit obligațiile de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în țara în care suntem stabiliți;

2.1.5. Nu am fost condamnați, în ultimii 3 ani, prin hotărârea definitivă a unei instanțe judecătorești, pentru o faptă care a adus atingere eticii profesionale sau pentru comiterea unei greșeli în materie profesională;

2.1.6. Nu am prezentat / nu prezentăm informații false sau am prezentat / prezentăm informațiile solicitate de către autoritatea contractantă în scopul demonstrării îndeplinirii criteriilor de calificare și selecție;

2.1.7. Nu am încălcat obligațiile aplicabile în domeniul mediului, muncii și asigurărilor sociale;

2.1.8. Nu ne facem vinovați de o abatere profesională, care ne pune la îndoială integritatea;

2.1.9. Nu am încheiat cu alți operatori economici acorduri care vizează denaturarea concurenței;

2.1.10. Nu ne aflăm într-o situaţie de conflict de interese care nu poate fi remediată în mod efectiv prin măsurile prevăzute la art. 79 al legii nr. 131 din 2015 privind achiziţiile publice;

2.1.11. Nu suntem incluşi în Lista de interdicţie a operatorilor economici;

2.1.12. Respectăm regimul de compatibilităţi prevăzut la art. 16 alin. (6) al legii nr. 131 din 2015 privind achiziţiile publice *„Persoanele fizice şi juridice care sunt înregistrate, au reşedinţa sau desfăşoară activitatea economică principală în jurisdicţii ori regiuni autonome ce nu implementează standarde internaţionale de transparenţă, precum şi persoanele juridice în componenţa cărora figurează, direct sau indirect, una sau mai multe persoane (fondatori, asociaţi, acţionari, administratori, beneficiari efectivi) care sunt înregistrate, au reşedinţa sau desfăşoară activitatea economică principală în astfel de jurisdicţii ori regiuni autonome. Metodologia de stabilire a jurisdicţiilor care nu implementează standarde internaţionale de transparenţă, precum şi lista jurisdicţiilor respective, în sensul prezentei legi, se aprobă de către Guvern, la propunerea Serviciului Prevenirea şi Combaterea Spălării Banilor, după consultarea Băncii Naţionale a Moldovei şi a Comisiei Naţionale a Pieţei Financiare.”.*

3. Art. 70 alin. (1) lit. c) a Legii nr. 74 din 2020 privind achiziţiile în sectoarele energeticii, apei, transporturilor şi serviciilor poştale:

3.1. Îndeplinim criteriile de selecţie stabilite de entitatea contractantă în conformitate cu prevederile legii nr. 74 din 2020 privind achiziţiile în sectoarele energeticii, apei, transporturilor şi serviciilor poştale:

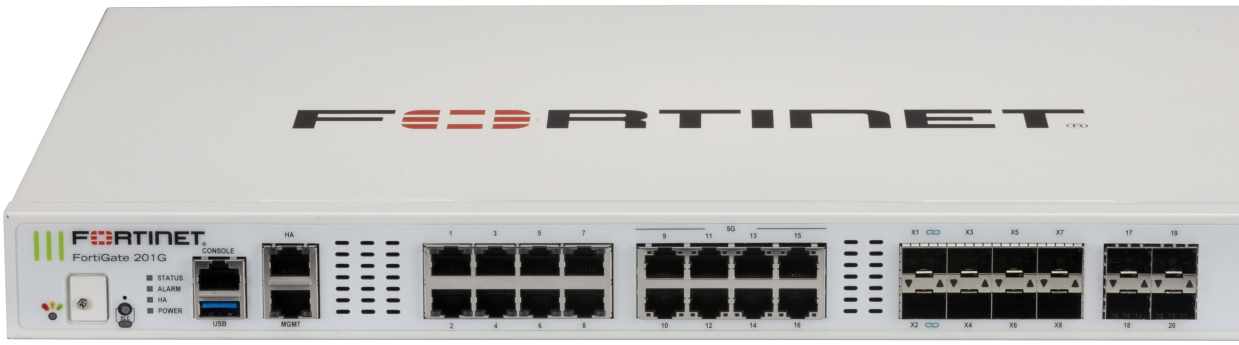
3.1.1. Suntem de acord cu termenul de plată propus de către **Î.S. „Poşta Moldovei”** de nu mai puţin de 30 de zile din data prezentării facturilor fiscale şi a actelor de predare-primire;

Data completării 01.10.2025
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

FortiGate 200G Series



Highlights

Gartner® Magic Quadrant™ Leaders for both Network Firewalls and WAN Edge Infrastructure

Secure Networking with FortiOS for converged networking and security

State-of-the-art unparalleled performance with Fortinet's patented SPU and vSPU processors

Enterprise security with consolidated AI/ML-powered FortiGuard services

Deep visibility into applications, users, and devices beyond traditional firewall techniques

Artificial Intelligence, Machine Learning Security with Deep Visibility

The FortiGate 200G series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) to deliver threat protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 200G Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

Universal zero-trust network access (ZTNA) automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast threat protection and SSL inspection provides security at the edge you can see without impacting performance.

IPS	NGFW	Threat Protection	Interfaces
9 Gbps	7 Gbps	6 Gbps	Multiple GE RJ45, 5GE RJ45, 10GE SFP+ Slots, GE SFP Slots

Use Cases

Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-Powered Security Services, natively integrated with your NGFW, secures web, content, and devices and protects networks from ransomware, malware, zero days, and sophisticated AI-powered cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU technology provides industry-leading high-performance protection

Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for hybrid working models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security from the branch to the data center and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services, detects and prevents known, zero-day, and unknown attacks

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Real-Time Network Security Operating System

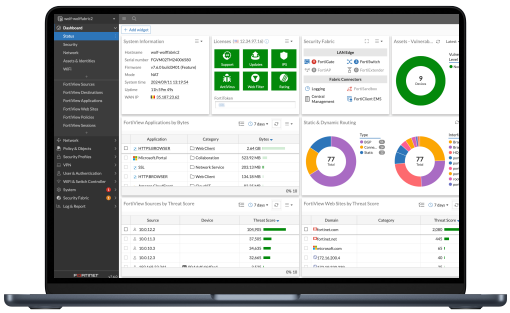
FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integrating generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

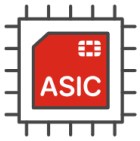
Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status

Fortinet ASICs: Unrivaled Security, Unprecedented Performance



Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

Network processor NP7Lite

Fortinet's new, breakthrough SPU NP7Lite network processor works in line with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content processor CP10

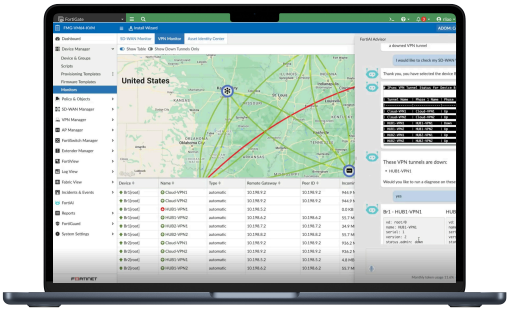
Content processors act as co-processors to offload resource-intensive processing of security functions. The tenth generation of the Fortinet Content Processor, the CP10, accelerates resource-intensive security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload

FortiManager

Centralized management at scale for distributed enterprises

FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.



GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.

FortiConverter Service

Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

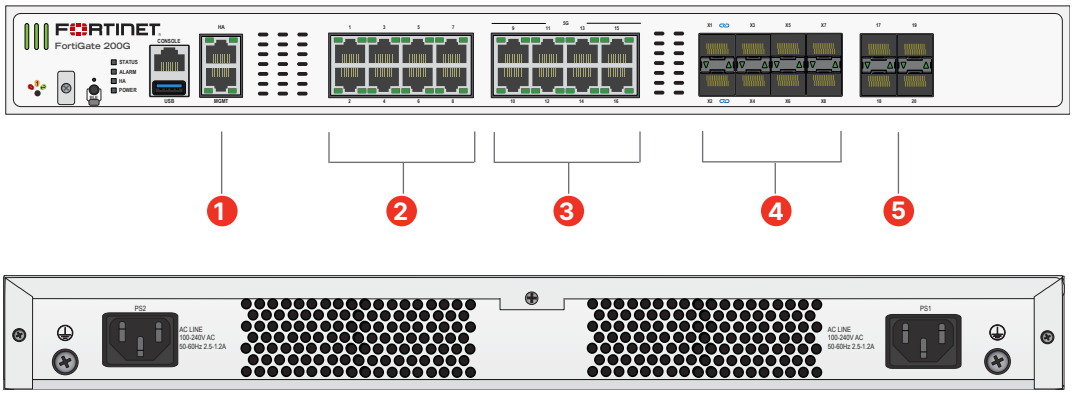
FortiCare Services

Expertise at your service

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

Hardware

FortiGate 200G Series



Interfaces

1. 2 x GE RJ45 MGMT/HA Ports
2. 8 x GE RJ45 Ports
3. 8 × 5/2.5/GE RJ45 Ports
4. 8 × 10 GE SFP+/SFP FortiLink Slots
5. 4 x GE SFP Slots

Hardware Features

NP7Lite (SP5) | CP10 | TPM | 1RU | DUAL AC | 10/5/GE | 480GB

Trusted Platform Module (TPM)

The FortiGate 200G series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 200G series offers dual built-in non-hot swappable power supplies.

Access layer security

FortiLink protocol enables you to converge security and network access by integrating the FortiSwitch into the FortiGate as a logical extension of the firewall. These FortiLink-enabled ports can be reconfigured as regular ports as needed.

Signed Firmware Hardware Switch

The signed firmware switch is a physical security switch. It is by default set to the highest security level. The highest security level ensures that only an appropriately validated FortiOS firmware can be loaded on the FortiGate. This feature adds an additional physical layer of security to the FortiGate, acting as a key deterrent to and reducing risk of compromise.

Specifications

	FORTIGATE 200G	FORTIGATE 201G
Interfaces and Modules		
GE RJ45 Ports	8	
GE RJ45 Management / HA	1 / 1	
5/2.5/GE RJ45 Ports	8	
GE SFP Slots	4	
10/GE SFP/+ FortiLink Slots (default)	8	
USB Port	1	
Console Port	1	
Onboard Storage	0	1× 480 GB SSD
Trusted Platform Module (TPM)	✓	
Bluetooth Low Energy (BLE)	✓	
Signed Firmware Hardware Switch	✓	
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	9 Gbps	
NGFW Throughput [2, 4]	7 Gbps	
Threat Protection Throughput [2, 5]	6 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	39 / 39 / 26.5 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	39 / 39 / 26.5 Gbps	
Firewall Latency (64 byte, UDP)	4.36 µs	
Firewall Throughput (Packet per Second)	39.75 Mpps	
Concurrent Sessions (TCP)	11 Million	
New Sessions/Second (TCP)	400 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	36 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	16 000	
SSL-VPN Throughput [6]	3 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	7 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	7100	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	900 000	
Application Control Throughput (HTTP 64K) [2]	27.8 Gbps	
CAPWAP Throughput (HTTP 64K)	37.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 25	
Maximum Number of FortiSwitches Supported	64	
Maximum Number of FortiAPs (Total / Tunnel)	256 / 128	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 200G	FORTIGATE 201G
Dimensions and Power		
Height x Width x Length (inches)	1.75 × 17.0 × 15.0	
Height x Width x Length (mm)	44.45 × 432 × 380	
Weight	14.11 lbs (6.4 kg)	14.33 lbs (6.5 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Consumption (Average / Maximum)	145 W / 175 W	145 W / 176 W
AC Power Input	100–240V AC, 50/60Hz	
AC Current (Maximum)	2A @100VAC, 1.2A @240VAC	
Heat Dissipation	597.12 BTU/h	600.54 BTU/h
Power Supply Efficiency Rating	80Plus Compliant	
Redundant Power Supplies	✓ (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Operating Environment and Certifications		
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	5% to 90% non-condensing	
Noise Level	LPA 48 dBA / LWA 55 dBA	
Forced Airflow	Side and Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certification	USGv6/IPv6	

Note: All performance values are "up to" and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

[6] Uses RSA-2048 certificate.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		----------included with FortiCare Subscription----------		
	Inline CASB [3]		----------included with FortiCare Subscription----------		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	Models up to FG/FWF-60F series			
	SD-WAN Underlay and Application Monitoring Service	FG-70F series and above			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE expansion for SD-WAN (SD-WAN SPA Connector license plus FortiSASE starter kit for n* users) [2]	Selected models only[2]			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)	Desktop models only			
NOC and SOC Services	FortiConverter Service for one time configuration conversion	•	•		
	Managed FortiGate Service—available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management	•			
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiGuard SOCaaS—24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service	•			
Hardware and Software Support	FortiCare Essentials	Desktop models only			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		----------included with FortiCare Subscription----------		

1. Full features available when running FortiOS 7.4.1.

2. See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.

FortiGuard Bundles

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

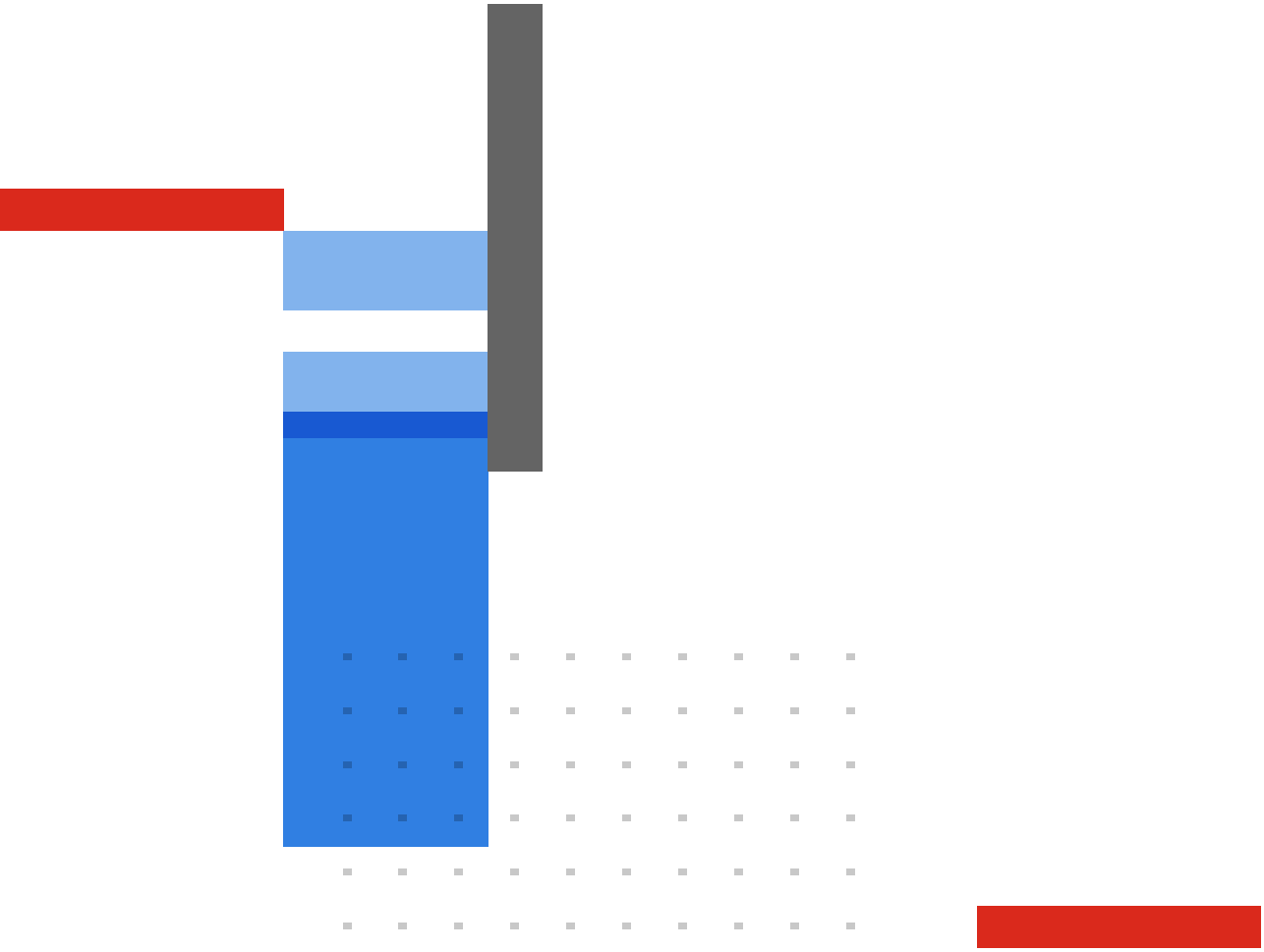
Ordering Information

Product	SKU	Description
FortiGate 200G	FG-200G	10x GE RJ45 (including 1x MGMT port, 1x HA port, 8x switch ports), 4x GE SFP slots, 8× 5GE RJ45, 8× 10GE SFP+ slots, NP7Lite and CP10 hardware accelerated.
FortiGate 201G	FG-201G	10x GE RJ45 (including 1x MGMT port, 1x HA port, 8x switch ports), 4x GE SFP slots, 8× 5GE RJ45, 8× 10GE SFP+ slots, NP7Lite and CP10 hardware accelerated, 480GB onboard SSD storage.
Transceivers		
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 80km Extreme Long Range	FN-TRAN-SFP+ZR	10GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, (connects to FN-TRAN-SFP+BD27, ordered separately)	FN-TRAN-SFP+BD33	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
25 GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range, compatible with 10 GE SFP/SFP+ slots.
Cables		
10 GE SFP+ Passive Direct Attach Cable 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you 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 illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

April 30, 2025

FG-200G-DAT-R08-20250430

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