NR. 46.049/06.11.2025

CAIET DE SARCINI

Achiziție

Firewall DMZ

1. Scopul documentului

Prezentul Caiet de Sarcini definește cerințele tehnice, funcționale, administrative și contractuale pentru achiziția a două (2) echipamente de tip Next-Generation Firewall (NGFW) și a licențelor aferente, destinate construcției unei zone tampon de tip DMZ (Demilitarized Zone) la interfața dintre rețeaua locală și Internet, consolidării infrastructurii de securitate cibernetică a rețelei existente. Achiziția vizează extinderea capacităților de protecție împotriva amenințărilor avansate, integrându-se în arhitectura actuală de securitate, fără a necesita modificări majore ale infrastructurii existente. Obiectivul principal este îmbunătățirea rezilienței rețelei prin implementarea unor soluții capabile de inspecție profundă a traficului, prevenire a intruziunilor și gestionare centralizată, conform standardelor actuale de securitate (ex. ISO 27001, GDPR).

Echipamentele și licențele / subscriptiile necesare asigurării pentru o perioadă de minim 3 ani a următoarelor funcționalități și capabilități avansate de securitate: protecție antivirus, detecția și controlul aplicațiilor (la nivelul OSI 7), prevenirea intruziunilor (IPS) si protectie malware.

Prin această achiziție ROMGAZ dorește îndeplinirea următoarelor obiective:

- ✓ *Întărirea arhitecturii de securitate existente*: Achiziția celor două echipamente suplimentare vizează consolidarea infrastructurii de securitate actuale, prin adăugarea de capabilități avansate de inspecție profundă a pachetelor și prevenire a intruziunilor.
- ✓ *Extinderea capacității de filtrare a traficului*: Noile echipamente vor completa soluțiile existente, oferind o capacitate sporită de procesare a traficului de rețea și implementarea unor politici granulare de control al accesului în cadrul infrastructurii curente.
- ✓ *Îmbunătățirea rezilienței la amenințări avansate*: Adăugarea acestor dispozitive în rețea va spori protecția împotriva amenințărilor cibernetice complexe, precum atacuri APT și exploit-uri zero-day, integrându-se perfect cu sistemele de securitate existente.
- ✓ *Optimizarea performanței în medii cu încărcare mare*: Echipamentele suplimentare vor susține infrastructura actuală prin gestionarea eficientă a fluxurilor de date cu latență scăzută, asigurând continuitatea operațiunilor în condiții de trafic intens.
- ✓ *Integrare avansată cu managementul centralizat*: Noile dispozitive vor fi integrate în platforma de administrare existentă, permițând corelarea datelor de securitate și automatizarea răspunsului la incidente pentru o gestionare mai eficientă a rețelei.
- ✓ *Asigurarea conformității și scalabilității*: Achiziția vizează extinderea capabilităților de conformitate cu standardele de securitate, prin implementarea de funcționalități

suplimentare de monitorizare și raportare, adaptate la nevoile în evoluție ale rețelei existente.

2. Descrierea obiectului achiziției

Achiziția include:

- ✓ Două (2) echipamente hardware de tip NGFW cu specificațiile minime de mai jos.
- ✓ Licențe software aferente pentru fiecare echipament, incluzând
  - o Prevenția Amenințăilor (Threat Prevention)
  - o Filtrare avansată a URL-urilor (Advanced URL Filtering)
  - o Securitate DNS (DNS Security)
  - o Analiză avansată a amenințărilor (Sandboxing/Threat Analysis
  - o Access securizat la distanță (Remote Access Security)

  pentru o perioadă minimă de 3 ani (cu opțiune de prelungire anuală).
- ✓ Servicii asociate: instalare, configurare inițială, training de bază și suport tehnic inițial.

Echipamentele vor fi utilizate ca dispozitive suplimentare în rețeaua existentă, pentru distribuirea sarcinii de securitate și creșterea scalabilității.

2.1 Scopul achiziției

Achiziția vizează:

- ✓ Întărirea arhitecturii de securitate existente prin adăugarea de capabilități avansate de inspecție profundă a pachetelor și prevenire a intruziunilor.
- ✓ Extinderea capacității de filtrare a traficului, oferind o procesare sporită a fluxurilor de date cu latență scăzută.
- ✓ Îmbunătățirea rezilienței la amenințări avansate (APT, zero-day exploits), integrându-se perfect cu sistemele de securitate curente.
- ✓ Optimizarea performanței în medii cu trafic intens, susținând continuitatea operațională.
- ✓ Integrare avansată cu managementul centralizat existent, pentru corelarea datelor și automatizarea răspunsului la incidente.
- ✓ Asigurarea conformității cu standardele de securitate și scalabilității rețelei.

3. Specificații tehnice și funcționale minim obligatorii

Soluția de securitate NGFW va asigura următoarele capabilități tehnice și funcționale minim obligatorii:

1. Soluția implementează simultan printr-un singur proces de inspecție a traficului mecanisme de protecție la nivel de retea (filtru de pachete), firewall de aplicatie, mecanisme anti-intruziune (IPS), filtrare anti malware, mecanisme de protectie impotriva exfiltrarii datelor (anti spyware), identificare de utilizator si de terminal, servicii de concentare VPN IPSec si SSL, decriptare SSL de tip inbound si outbound (forward proxy), decriptare SSH, inspectie tunele GRE, IPsec non-criptate.
2. Se va avea în vedere livrarea unei soluții redundante compusă din două seturi de echipamente care rulează în paralel, și asigură funcționalitatea și în cazul în care unul dintre echipamente este oprit.
3. Din punct de vedere hardware fiecare echipament in parte:
   - ✓ va fi de tip rack-mountable 1xRU (se vor livra toate accesoriile necesare montarii in rack 19");
   - ✓ va fi echipat cu surse de alimentare redundante (se vor livra cabluri pentru conectare la surse tip PDU C13 - C14);
   - ✓ va fi echipat cu minim 8 interfete retea 10/100/1000 Mbps RJ-45
   - ✓ va fi echipat cu minim 4 interfete retea 1G/2.5G/5G RJ-45 cu capabilitati PoE
   - ✓ va avea disponibile 6 sloturi de tip 1G SFP
   - ✓ va avea disponibile 4 sloturi de tip 1G/10G SFP/SFP+
   - ✓ va fi echipat cu minim o interfeta dedicate pentru HA;
   - ✓ va fi echipat cu port management „Out of Band" (OOB) de tip 1000BaseT;
   - ✓ va fi echipat cu port consola
   - ✓ echipamentele trebuie să fie noi, neutilizate.
4. Fiecare echipament in parte va fi echipat cu HDD/SSD local pentru stocarea loguri: minim 120 GB.

5. Echipamentul trebuie să suporte separarea unui management plane (care se ocupă de GUI-ul firewall-ului și de configurația firewall-ului) și a unui data plane (care se ocupă de traficul care trece prin firewall). Echipamentul trebuie să dețină în acest sens minim 2 core-uri de CPU dedicate pentru management plane.
6. Echipamentele și componentele propuse trebuie livrate împreună cu toate accesoriile necesare montării în rack-urile din centrele de date ale autorității contractante precum și a punerii în funcțiune. Instalarea echipamentelor și componentelor ofertate va fi efectuata în conformitate cu specificațiile producătorului.
7. Echipamentele suporta agregarea interfetelor utilizand protocolul LACP (802.3ad);
8. Interfetele pot fi configurate mod Layer3, Layer2, TAP, Virtual Wire (Transparent Mode);
9. Sunt suportate subintefete 802.1Q (VLAN tag 1-4093 / interfata);
10. Fiecare echipament in parte va rula un sistem de operare dedicat, dezvoltat de către producător. Nu este permisă folosirea unui sistem de operare comercial, pentru uz general.
11. Fiecare echipament in parte va asigura urmatorii parametrii de performanta:
    - ✓ Minim 100,000 sesiuni noi / secunda;
    - ✓ Minim 945,000 sesiuni concurente;
    - ✓ „Firewall Throughput"
        - o minim 8,5 Gbps utilizand un patern de trafic mix, avand jurnalizarea evenimentelor activata ("logging enabled") si identificarea aplicatiilor in traficul monitorizat;
    - ✓ „Threat Prevention throughput":
        - o minim 4,5 Gbps utilizand un patern de trafic mix pentru care se aplica inspectie IPS, antivirus, file blocking, anti-malware, filtrare aplicatie si cu „logging enabled";
    - ✓ "IPSec VPN Throughput"
        - o minim 4,1 Gbps utilizand tranzactii HTTP de 64 KB si cu "logging enabled"
12. Este obligatoriu ca stocarea datelor transmise în cloud (pentru analiză amenințări informatice, fișiere sau aplicații suspicioase, loguri necesare suportului extern pentru remedierea unor defecțiuni etc.) se va face pe teritoriul UE, cu respectarea prevederilor Regulamentului UE nr. 679, iar acest aspect trebuie certificat și/sau garantat explicit de către producătorul soluției.
13. Solutia asigura pe baza de subscriptie de tip „threat inteligence" , subscriptie valida pe durata periodei de garantie, informatii puse la dispozitie de catre producatorul sistemului NGFW urmatoarele capabilitati minime obligatorii:
    - ✓ Să asigure analiza in timp real a comunicațiilor spyware si de tip C2 (comandă și control) necunoscute, pe baza algoritmilor de tip Deep Learning implementati în cloud-ul producătorului. Solutia trebuie sa permita implementarea functionalitatii cel putin pentru trafic de tip HTTP, HTTP/2, TLS si aplicatii neidentificate de platforma in trafic TCP si UDP si sa permita blocarea comunicatiei malitioase analizate in cloud in timp real la nivelul echipamentului de tip next generation firewall
    - ✓ Componenta IPS asigura pe baza de semnaturi:
        - o actualizări automate ale semnăturilor de tip IPS;
        - o protectia împotriva atacurilor de tip DoS (Denial of Service);
        - o detectare anomalii utilizare protocoale de comunicații;
        - o detectarea si sa blocarea incercarilor de exploatare, tehnicilor evazive atat la nivel de retea cat si la nivel de aplicatie, inclusiv atacuri de tip port scan, buffer overflow, remote code execution si command injection;
        - o detectare atacuri de tip "port scan" si "host sweeping";
        - o asigură inspecția fișierelor arhivate fără parolă;
        - o suportă semnături definite de catre administratori.
    - ✓ Trebuie să conțină o soluție avansată de analiză a malware-ului fără sa fie bazat pe semnaturi (malware sandboxing) și trebuie să aibă în mod implicit suport și pentru scanarea executabilelor MacOS și Linux. În acest sens soluția trebuie sa ofere o analiza detaliată a fiecărui fișier analizat pe mai multe sisteme de operare, inclusiv cu
      informații legate de activitatea la nivel de host cat si la nivel de rețea cât și să ofere accesul la fișierul original inclusiv PCAP cu analiza dinamica a sesiunii dacă este considerat a fi malware pentru reverse engineering, cat și un raport de tip pdf detaliat cu analiza statica si dinamica.

14. Solutia asigura funcționalități pentru controlul aplicațiilor:
    - ✓ Identificare și control pentru cel puțin 5000 de aplicații uzuale (control la nivelul OSI layer 7, inclusiv pentru cele existente în cloud - de exemplu suita Microsoft 365 și altele)
    - ✓ utilizează tehnici multiple de identificare pentru a determina tipul de aplicațiilor care traversează echipamentele firewall, indiferent de port, protocol, tactici evazive sau criptare.
    - ✓ permite definirea unor politici de securitate pentru anumite aplicatii care sa permita activarea unora dintre funcționalitatile aplicației în timp ce blochează altele. De ex. se vor configura o politica care permit utilizarea aplicatiei WebEx dar nu permite transferul de fisiere, politica care permite „file downloading" dar nu „file uploading" sau „file sharing";
    - ✓ limitare de bandă („traffic shaping") per aplicație
    - ✓ analiza aplicațiilor care au ratele cele mai mari de consum de bandă
    - ✓ decriptare si inspectie a traficului criptat TLS1.2 / TLS1.3;
15. Solutia asigura minim urmatoarele funcționalități la nivel retea:
    - ✓ Suportă IPv4 și IPv6 pentru toate serviciile oferite;
    - ✓ NAT („Network Address Translation") / NAT 1 la 1 /PAT („Port Address Translation");
    - ✓ Rutare statica / rutare dinamică OSPF, BGP, Multicast;
    - ✓ Rutare bazată pe politici („policy-based routing");
    - ✓ Funcționalități management lărgime de bandă („traffic shaping"): asigură limitarea / garantarea lărgimii de bandă în funcție de politici / adrese IP / aplicații
16. Solutia permite definirea unor politici de securitate bazate pe identitatea utilizatorilor
17. Solutia permite programarea în timp (scheduling) a politicilor de firewall
18. Soluția trebuie să ofere funcționalitatea accesului de la distanță la resursele organizației pentru cel putin 1500 de utilizatorii finali pentru sisteme de tip Windows si MacOS.
19. Solutia trebuie sa poata stabili tuneluri VPN folosind atat protocoalele IPSec si SSL.
20. Funcționalitatea de acces la distanță VPN trebuie să fie integrată cu recunoașterea utilizatorului.
21. Adresele IP selectate trebuie să poată ocoli tunelul de acces la distanță VPN și să direcționeze traficul direct către destinația publica.
22. Solutia trebuie sa ofere functionalitatea de definire a tunelurilor de tip site-to-site VPN
23. Solutia trebuie sa ofere suport pentru Post Quantum Hybrid Key Exchange VPN pentru extinderea securității VPN prin functionalitatea de a crea chei hibride de tip PQC (Post Quantum Cryptographic) folosind suitele criptografice NIST round 3 si round 4 (RFC 9242 si RFC 9370). Acest lucru are rolul de a proteja împotriva atacurilor de tip "harvest now, decrypt later)

Astfel echipamentele și licențele / subscripțiile solicitate sunt următoarele:

Nr. crt.	Denumire produs	Cantitate
1	Echipament Firewall Next Generation	2
2	Servicii suport / garanție 36 luni	2
3	Subscriptie servicii licență Firewall Next Generation (ex. servicii de prevenire a amenințărilor și analiză a malware-ului soluții integrate de securitate și SD-WAN, servicii de filtrare după URL, etc) 36 luni	2

4. Cerințe pentru servicii asociate

4.1. Instalare și configurare

Serviciile includ instalarea, configurarea, punerea în funcțiune si instruire pentru echipamentul livrat cu licențele aferente, asigurând protecție completă împotriva amenințărilor cunoscute și necunoscute.
Activitățile de instalare, configurare vor cuprinde minim următoarele:

- ✓ Instalarea fizică, conectarea și configurarea inițială a echipamentului;
- ✓ Proiectarea (design) zonei DMZ
- ✓ Definirea interfețelor, zonelor de securitate, rutării și regulilor de acces;
- ✓ Activarea și configurarea funcțiilor avansate de securitate (IPS/IDS, Anti-Spyware, URL Filtering, File Blocking, DNS Security, Analiză malware);
- ✓ Integrarea cu infrastructura existentă (Active Directory, NTP, DNS, Syslog/SIEM);
- ✓ Testarea funcționalității și validarea politicilor de securitate;
- ✓ Documentarea zonei DMZ și a instanței instalate.

Instalarea și configurarea va fi realizată de tehnicieni certificați, în maxim 10 zile lucrătoare de la livrare, pe locație Sediul Central Romgaz. Include testare end-to-end și predarea documentație tehnice aferente echipamentelor

4.2. Servicii de instruire

Servicii de instruire oferit de partener autorizat în oferirea de cursuri pentru echipamentele furnizate. Cursul va fi realizat cu instructor specializat și va oferi cursanților minim următoarele deprinderi:

- ✓ Configurarea și gestionarea funcțiile esențiale ale firewall-urilor de ultimă generație;
- ✓ Configurarea și gestionarea politicilor de securitate și NAT pentru a permite traficul aprobat către și dinspre zone;
- ✓ Configurarea și gestionarea strategiile de prevenire a amenințărilor pentru a bloca traficul provenit de la adrese IP, domenii și URL-uri cunoscute și necunoscute;
- ✓ Monitorizarea traficul de rețea utilizând interfața web interactivă și rapoartele firewall-ului;

Training: Sesiune de 5 zile pentru 2 utilizatori (administratori), acoperind configurare, management și troubleshooting conform tematicii de mai sus.
Documentație: Manuale în limba engleză/română, scheme de integrare, rapoarte de conformitate.

5. Garanție

Durata minimă: 36 de luni de la data punerii în funcțiune, acoperind defecte de fabricație și uzură normală.
Condiții: RMA (Return Material Authorization) în maxim 48 de ore, înlocuire cu echipament echivalent sau superior.
Prelungire: Perioada de garanție se prelungește cu numărul de zile de nefuncționare cauzate de defecte.
Responsabilitate: Furnizorul asigură transportul și instalarea pieselor de schimb fără costuri suplimentare.

6. Suport tehnic și mentenanță

Nivel de suport: 8/5, cu răspuns inițial în maxim 1 oră (telefon/email), rezolvare în maxim 4 ore pentru probleme critice (downtime).
Tip suport: On-site pentru intervenții majore (next business day), remote pentru diagnostic.
Durata: Inclusă în licențe pentru 3 ani; opțiune de extindere.
Escalation: Procedură clară, cu SLA (Service Level Agreement): 99.9% uptime.
Actualizări: Gratuite pentru software și threat intelligence pe durata licenței.
Furnizorul va furniza un contract de suport detaliat.

7. Condiții de livrare și plată

7.1. Livrare

Termen: Maxim 30 de zile calendaristice de la semnarea contractului.
Locație: Sediul Central Romgaz.
Transport: Asumat de furnizor, cu asigurare împotriva pierderii/deteriorării.

7.2. Plată

Contractantul va emite factura pentru produsele livrate și serviciile prestate. Fiecare factura va avea menționat numărul contractului, datele de emitere și de scadența ale facturii respective, coduri CPV. Facturile vor fi transmise prin sistemul RO e-Factura.

Factura va fi emisă după semnarea de către Autoritatea/entitatea contractantă a procesului verbal de recepție calitativă, acceptat, după livrare, instalare și punere în funcțiune. Procesul verbal de recepție va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute mai jos:

a) certificatul de calitate și garanție;
b) declarația de conformitate;
c) avizul de expediție a produsului.

Plățile în favoarea Contractantului se vor efectua în termen de 30 de la data primirii facturii fiscale și a tuturor documentelor justificative.

ANEXA nr. ....1..... la Caietul de sarcini nr. ..46049/06.11.2025

Nr. 48247/18.11.2025

Cod CPV: 32420000-3

Serviciul Telecomunicații

1. **Documente obligatorii în faza de adjudecare şi ulterior, la livrarea produselor sau prestarea serviciilor/lucrărilor**
   Toate documentele vor fi prezentate în limba română. Documentele emise în altă limbă vor fi însoțite de traduceri autorizate.

1.1 ***Pentru produse/echipamente:***

- ✓ **Certificat de conformitate CE**
- ✓ **Declarația de conformitate** a producătorului/importatorului/comerciantului (privind îndeplinirea cerințelor de securitate şi sănătate);
- ✓ **Certificatul de garanție** emis de producător;

1.2 ***Pentru serviciile desfășurate pe amplasamente aparținând S.N.G.N. Romgaz S.A.***

- ✓ Lista cu persoanele care prestează serviciile (actualizată);

Notă:
Prezentele reglementări nu sunt limitative. Pe toată perioada derulării contractului, contractorul va respecta legislația din domeniul securității şi sănătății în muncă, în vigoare, aplicabilă activităților pe care le desfășoară.

ANEXA nr. 2. la Caietul de sarcini nr. 46.049/06.11.2025

Nr.47.675/14.11.2025

Către:
SERVICIUL TELECOMUNICAȚII

1. Documente obligatorii în faza de adjudecare

1.1 Nu este cazul

2. Documente obligatorii a fi prezentate de către ofertantul declarat câștigător, în termen de 10 zile lucrătoare de la data comunicării rezultatului procedurii

2.1 Nu este cazul

3. CERINȚE DE PROTECȚIA MEDIULUI ASOCIATE ASPECTELOR DE MEDIU POTENȚIALE

Entitatea contractantă va preciza în contract următoarele obligații în sarcina contractantului:

3.1 Să instruiască personalul propriu cu cerințele legale de mediu precum și cu cerințele din caietul de sarcini/contract, iar la începerea desfășurării contractului, să prezinte responsabilului cu urmărirea contractului dovada instruirii personalului propriu;
3.2 Să respecte legislația de mediu în vigoare, aplicabilă activității ce face obiectul achiziției, repectiv:
- OUG nr. 195/2005 privind protecția mediului, cu modificările și completările ulterioare;
- OUG nr. 92/2021 privind regimul deșeurilor, cu modificările și completările ulterioare;
- LEGE nr. 249/2015 privind modalitatea de gestionare a ambalajelor și a deșeurilor de ambalaje, modificată și completată prin OUG nr. 38/2016, LEGE nr. 87/2018 și OUG nr. 74/2018, LEGE nr. 31/2019, OUG nr. 50/2019, LEGE nr. 99/2021, OG nr. 1/2021 și OUG nr. 96/2023;
- OUG nr. 5/2015 privind deșeurile de echipamente electrice și electronice, modificată și completată prin OUG nr. 44/2019, OUG nr. 93/2020, OUG nr. 92/2021, LEGE nr. 127/2024 și OUG nr. 137/2024;
- HG nr. 322/2013 privind restricțiile de utilizare a anumitor substanțe periculoase în echipamentele electrice și electronice, modificată și completată prin HG nr. 897/2016 și HG nr. 234/2019;
- ORDIN nr. 556/2006 MMGA privind marcajul specific aplicat echipamentelor electrice și electronice introduse pe piață după data de 31 decembrie 2006;
- HG nr.661/2011 privind stabilirea unor măsuri pentru asigurarea aplicării la nivel național a prevederilor Regulamentului (CE) nr. 66/2010 al Parlamentului European și al Consiliului din 25 noiembrie 2009 privind eticheta UE ecologică;
- SR EN ISO 14024:2018 Etichete și declarații de mediu. Eco-etichetare de tipul I. Principii și proceduri;
- OUG nr. 68/2007 privind răspunderea de mediu cu referire la prevenirea și repararea prejudiciului asupra mediului, cu modificările și completările ulterioare.

3.3 Să livreze produse în conformitate cu prevederile legale, marcate CE (conformitate europeană) pe produse/ambalaje sau documente însoțitoare (în limba română), semnificând conformitatea produselor cu toate cerințele de siguranță, sănătate, mediu și protecție a consumatorului;
3.4 Să livreze produse în conformitate cu cerințele UE privind etichetarea echipamentelor, respectiv eticheta UE ecologică. Produsele care dețin o etichetă ecologică relevantă de tip I și care respectă cerințele enumerate sunt considerate conforme. Pentru categoria de echipamente care nu dețin etichetă ecologică de tip I, contractantul va prezenta alte mijloace doveditoare adecvate privind performanța de mediu a produselor, dintre care (fără a se limita la acestea):
   - Declarația UE de Conformitate (DoC) emisă de producător, care atestă conformitatea cu directivele aplicabile (inclusiv RoHS, EMC, LVD);

NOTĂ: La completare, se vor elimina din formular cerințele care nu corespund achiziției.

ANEXA nr. ..... la Caietul de sarcini nr. 46.049/06.11.2025

- Rapoarte de testare sau certificate emise de organisme acreditate privind conformitatea cu RoHS, consumul de energie, nivelul de zgomot sau alte caracteristici relevante;
- Fișe tehnice oficiale ale producătorului care includ parametri de consum energetic, informații privind materialele utilizate, durata de viață estimată, precum și recomandări privind gestionarea la sfârșitul ciclului de viață;
- Declarații de mediu ale producătorului (Environmental Product Declaration - EPD), dacă există;
- Certificări ale sistemului de management de mediu al producătorului (ex.: ISO 14001) sau standarde echivalente;
- Declarații sau rapoarte de conformitate privind substanțele periculoase (ex.: conform REACH și RoHS);
- Documente privind reciclabilitatea produsului și ambalajelor (ex.: procent de reciclabilitate, materiale utilizate, marcaje corespunzătoare). Prezentarea unuia sau mai multor documente dintre cele enumerate este obligatorie pentru demonstrarea conformității cu cerințele de mediu în lipsa unei etichete ecologice de tip I.

3.5 Repararea și întreținerea echipamentelor în perioada de garanție se va face în conformitate cu reglementările tehnice specifice, cu instrucțiunile de utilizare, verificare și întreținere ale producătorilor/furnizorilor și cu standardele europene de referință, astfel încât să se asigure permanent performanțele normate;

3.6 Certificatul de garanție trebuie să acopere reparațiile și înlocuirile. Garanția trebuie să asigure faptul că produsele sunt conforme cu specificațiile tehnice, incluzând și defectele bateriilor (dacă este cazul);

3.7 Se interzice prezentarea de către contractant/producător de date inexacte privind rezultatele procesului de evaluare a performanțelor echipamentelor livrate;

3.8 Să informeze entitatea contractantă cu privire la potențialele riscuri la utilizare, care pot apărea și să indice natura măsurilor ce se impun în vederea prevenirii manifestării acestora (dacă este cazul);

3.9 Să asigure nivelul de zgomot/vibrații emis de echipamente în limita pragul fonic maxim admis de prevederile legale în vigoare;

3.10 Să asigure mijloace de transport necesare furnizării echipamentelor, ce respectă standardele privind emisiile de eșapament, consum redus de combustibil, cu reviziile tehnice la zi, respectând totodată condițiile tehnice de livrare;

3.11 Să răspundă pentru desfășurarea în siguranță a tuturor serviciilor de transport, livrare, instalare;

3.12 Să livreze produsele în ambalaje ce permit refolosirea sau reciclarea, marcate corespunzător, prin intermediul simbolurilor;

3.13 Se interzice depozitarea necontrolată a deșeurilor generate din activitatea proprie;

3.14 Să colecteze selectiv deșeurile rezultate în urma prestării serviciilor de montare în recipiente etichetate, adecvate tipului de deșeu și să le depoziteze în locurile special amenajate în vederea valorificării/eliminării;

3.15 Să preia DEEE în sistem "unul la unul", la solicitarea expresă a entității contractante în mod gratuit (în baza unui proces-verbal de predare-primire), în aceleași condiții precum cele de livrare a produsului nou, dacă echipamentul este de tip echivalent și a îndeplinit aceleași funcții ca echipamentul nou furnizat și să informeze entitatea contractantă despre această posibilitate înainte de achiziționarea produselor (daca este cazul);

3.16 Să predea DEEE în cadrul sistemului de colectare, potrivit prevederilor legale;

3.17 Să furnizeze la cererea entității contractante orice documente/informații care au legătură cu contractul;

3.18 Să răspundă pentru prejudiciul cauzat mediului de serviciul prestat necorespunzător, în acest sens va suporta sancțiune aplicată de către autoritățile de mediu pentru motive imputabile;

3.19 Va respecta Declarația de politică referitoare la calitate, mediu si sănătate, securitate în muncă, disponibilă la adresa: https://www.romgaz.ro.

NOTĂ: La completare, se vor elimina din formular cerințele care nu corespund achiziției.

ANEXA nr. ..... la Caietul de sarcini nr. 46.049/06.11.2025

Notă: Cerințele de mediu sunt considerate indicative și nelimitative. Pe toată perioada derulării contractului, contractantul va respecta legislația de mediu în vigoare, aplicabilă activităților pe care le desfășoară. Dacă apar acte normative noi sau modificări/completări în cerințele legale de mediu aplicabile activităților desfășurate, contractantul va lua imediat toate măsurile necesare pentru conformare.

NOTĂ: La completare, se vor elimina din formular cerințele care nu corespund achiziției.

ROMGAZ	Cerinţe privind situaţiile de urgenţă la achiziţia de servicii de proiectare/execuţie lucrări	Cod: 02F-34-Act.3.2
		Pag. 1 / 1

ANEXA nr. ..... 3 ..... la C.S. 46049/06.11.2025
Solicitarea de cerinte nr. 46050/06.11.2025

Nr. 4962 / 14.11.2025

Către: Sediu - Serviciul Telecomunicatii

Cerinţe privind Situaţiile de Urgenţă la achiziţia de:

„ Firewall DMZ "

Cod CPV : 32420000-3 Echipament de retea

Conform procedurii operaţionale 02PO-03 Ediţia 3 Revizia 3

5.2.1 De la Serviciul SUIC se solicită completarea formularului 02F-34 pentru achiziţia de **servicii de proiectare/execuţie lucrări si achiziţia de mijloace tehnice de apărare împotriva incendiilor** (sisteme, instalaţii, echipamente, utilaje, stingătoare, dispozitive, accesorii, materiale, produse, substanţe şi autospeciale destinate prevenirii, limitării şi stingerii incendiilor).

Având în vedere aspectele enunţate mai sus nu este necesara solicitarea/emiterea cerinţelor privind Situaţiile de Urgenţă la achiziţia de **„ Firewall DMZ ".**

Data: 17.11.2025

11