S.C. COMPANIA DE APĂ ORADEA S.A.

Tel centrala: 004 0259 436 909
Tel secretariat: 004 0259 435 051
Fax : 004 0259 432 576
CUI: RO 54760
J 05 / 14 / 28. 05. 1991
Cont : RO41BRDE050SV03433450500
Capital social : 12.000.800 RON
E-mail: apaoradea@apaoradea.ro
Website: http://www.apaoradea.ro

ROMÂNIA, BIHOR, ORADEA 410202, STR. DUILIU ZAMFIRESCU NR. 3

Compartiment Achiziţii Publice
Nr. 37010 din 24.10.2018

INVITAȚIE DE PARTICIPARE LA ACHIZIȚIA DIRECTĂ

Obiectul achiziţiei directe:
„Furnizare, punere în funcțiune și testare echipament FortiGate 100D pentru legătura VPN cu sucursala Beiuș” din cadrul S.C. Compania de Apă Oradea S.A.

Cod CPV: 32420000-3 - Echipament de reţea

Valoarea estimată a achiziţiei: - 10.000,00 lei fără T.V.A.

Sursa de finanţare: Surse proprii

Modul de finalizare a achiziţiei directe : încheierea unui contract de furnizare.
Câştigătorul achiziţiei directe va introduce în catalogul electronic al achiziţiilor publice de pe SEAP oferta câştigătoare, pentru a putea finaliza achiziţia.

Modul de prezentare a propunerii financiare : Oferta financiară se va prezenta în lei fără T.V.A.

Durata contractului : Durata furnizării şi punerii în funcțiune va fi de maxim 10 zile (lucrătoare) la care se adaugă 7 zile calendaristice pentru testarea echipamentului.

Perioada minima pe parcursul căreia ofertantul trebuie să îşi menţină oferta: 60 zile (de la termenul limita de depunere a ofertelor).

Criteriul de atribuire: Preţul cel mai scăzut, dintre ofertele admisibile.

Persoană de contact: ing. Dorin ȚENȚ - **tel: 0728/116.421**.

Termenul de livrare: Specificaţi termenul de livrare, dar maxim 10 zile lucrătoare.

Termenul de garanţie: Specificaţi termenul de garanţie acordat echipamentului.

Oferta financiara va fi DDP – S.C. Compania de Apa Oradea S.A. – Sucursala Beiuș, str. Horia, nr.9.

Documentele de calificare solicitate:

- Declaraţie privind situaţia personala a ofertantului (conform formulare anexate 1÷3);
- Certificat constatator emis de Oficiul Registrului Comerţului, din care sa rezulte obiectul de activitate al ofertantului. Obiectul contractului trebuie să aibă corespondent în codul CAEN din certificatul constatator emis de ONRC;
- Prezentarea cel puţin a trei recomandări/copii contract/ proces verbal de punere în funcțiune /certificat constatator pentru contract similar, care să confirme prestarea de servicii similare (implementae de FireWall, securitate sau VPN în nume propriu) în ultimii trei ani, raportați la data limită de depunere a ofertelor. Implementarile care nu contin echipamente de firewall sau VPN nu vor fi luate in considerare;
- Ofertantii vor avea personal certificat pentru astfel de implementari, adica certificari pentru implementari echipamente de securitate;
- Acceptare model contract. Documentele de contract vor fi parafate pe fiecare pagina si semnate la final.

Modul de prezentare a propunerii tehnice:

Propunerea tehnica va respecta cerinţele caietului de sarcini de mai jos.

Propunerea tehnica va fi prezentata astfel încât să rezulte că: Ofertantul a înţeles corect cerinţele din Caietul de sarcini, şi oferta prezentată acoperă şi îndeplineşte întru totul aceste cerinţe. De asemenea propunerea trebuie să convingă achizitorul că în caz de atribuire ofertantul dispune de resurse materiale şi umane suficiente pentru a asigura serviciile oferite cu respectarea tuturor prevederilor legale naţionale in vigoare.

Specificatiile caietului de sarcini sunt minimale şi obligatorii.

Dacă propunerea tehnică nu satisface cerinţele caietului de sarcini, oferta va fi considerată neconformă, şi va fi descalificată.

Oferta va fi prezentata astfel :

a) Documente de calificare
b) Oferta tehnică
c) Oferta financiară.

CAIET DE SARCINI

Solutia actuala de VPN este efectuata cu un echipament Linksys RV042. Acest echipament nu se mai fabrica, este „end of sales", nu mai satisface cerintele actuale ale retelei intranet actuale a S.C. Compania de Apa Oradea S.A si nu este compliant GDPR. S-a ales varianta configurarii unui DMZ, iar acest echipament nu poate face VPN in acelasi timp intre 2 retele: serverele centrale (unde sunt instalate aplicatiile companiei) si DMZ (unde sunt serverul de mail si web al companiei).

Echipamentul este legatura securizata peste internet intre sediul central al companie si sucursala Beius si o defectiune a acestui echipament ar opri intreaga activitate o sucursalei Beius.

Acest echipament va fi dedicat pentru solutia de VPN intre sediul central al S.C. Companiea de Apa S.A. si sucursala Beius

Cerințe de implementare și testare a echipamentului VPN:

Echipamentul FortiGate 100D trebuie instalat si configurat la sucursala Beius. Echipamentul va face VPN cu sediul central de la Oradea, unde va putea sa aiba access controlat in toate retelele din sediul central (controlat pe baza de politici de securitate – servicii, protocoale, aplicatii ... etc). De asemenea conexiunea la internet, din sucursala Beius, se va face doar prin sediul central din Oradea pe baza unor politici de internet pe baza de useri (definiti si autentificati in Active Directory), protocoale (HTTP, HTTPS, IMAP, IMAPS, POP3, ... etc), aplicatii folosite (ex. block aplicatiile p2p, QUICK ... etc), servicii necesare , site-uri accesate (ex, block site-urile de socializare, terorism, droguri, sex ... etc). Aceste politici se vor stabili de comun acord cu angajatii companiei, in urma unui studiu de monitorizare a locatiei respective, de unde va rezulta folosirea actuala a internetului si ceea ce ar fi necesar sa foloseasca (ca trafic).

De asemenea prin acest echipament va trebui accesate controlat si camerele de supraveghere din locatia Beius (statia de epurare, sediu ... etc). Acest control va trebui stabilit de comun acord cu angajatii companiei cum se va face: pe baza de ip sursa, user .. etc.

Acest echipament va trebui sa faca de asemenea si legatura VPN cu statia de epurare de unde unii useri (definiti in Active Directory) vor putea accesa resursele (aplicatii, foldere, printere, ... etc) existente in cadrul retelei din sediul central.

Toate aceste tuneluri VPN se vor face pe baza protocolului Ipsec.

Echipamentul va trebui sa se poata accesa remote (de oriunde din internet), pe baza de software client si user si parola, tot printr-un tunel VPN. Trebuie sa fie accesat de cel putin 10 clienti remote.

Ofertanti vor trebui sa faca dovada a cel putin 3 implementari de firewall, securitate sau VPN in nume propriu. Implementarile care nu contin echipamente de firewall sau VPN nu vor fi luate in considerare. De asemenea ofertanti trebuie sa aiba personal certificat pentru astfel de implementari, adica certificari pentru implementari echipamente de securitate. Implementarea se va face on-site la sediul S.C. Compania de Apa S.A. din sucursala Beius.

Echipamentul se va considera pus in functiune si se va efactua plata atunci cand se vor semna procesele verbale de receptie si echipamentul a fost testat cel putin 7 zile calendaristice. Toate cerintele de mai sus sunt obligatorii nerespectarea lor duce la descalificare.

***Caracteristici minime pentru echipamentul VPN*:**

Firewall Throughput (1518/512/64 byte UDP)	2500 / 1000 / 200 Mbps
Firewall Latency	37 µs
Concurrent Sessions	2.5 Mil
New Sessions/Sec	22,000
Firewall Policies	10,000
IPSec VPN Throughput	450 Mbps
Max G/W to G/W IPSEC Tunnels	1,500
Max Client to G/W IPSEC Tunnels	5,000
SSL VPN Throughput	300 Mbps
Recommended SSL VPN Users	200
System Performance - Optimal Traffic Mix	
IPS Throughput	950 Mbps
System Performance - Enterprise Traffic Mix	
IPS Throughput	400 Mbps
NGFW Throughput	250 Mbps
Threat Protection Throughput	200 Mbps
Antivirus Throughput (Proxy- Based/ Flow-Based)	300 / 700 Mbps
Virtual Domains (Default/Max)	10 / 10
Interfaces (FE, GbE ports)	20x GbE Copper, 2x Shared Port Pairs
High Availability Configurations	Active / Active, Active / Passive, Clustering
Local Storage	16 GB
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6
Power Supplies	Single AC Power Supply
Form Factor	Rack Mount (1 RU)
De asemenea se va asigura, in caz de defectare, schimbarea echipamentului in maxim 3 zile calendaristice timp de un an de zile (serviciu mentenanta 24x7).	

Durata furnizării şi punerii în funcţiune va fi de maxim 10 zile (lucrătoare) la care se adaugă 7 zile calendaristice pentru testarea echipamentului.

Plata se va face într-o singura tranşă după semnarea proceselor verbale de: recepţie şi testare - cel puţin 7 zile calendaristice a echipamentului.

Mod de întocmire a ofertei financiare

Nr. crt.	Denumire serviciu	UM.	Cant.	Preţ unitar lei fără TVA
1	**Furnizare, punere în funcţiune şi testare echipament FortiGate 100D pentru legătura VPN cu sucursala Beiuş**	buc	1	

Toate documentele cuprinse în ofertă vor fi prezentate în limba română.

Ofertanţii sunt rugaţi să urmărească pe site-ul S.C. Compania de Apa Oradea S.A. eventualele răspunsuri la solicitările de clarificări postate în termen legal şi anexate prezentei invitatii.

Oferta va fi depusă la Secretariatul S.C. Compania de Apă Oradea S.A., str. Duiliu Zamfirescu nr. 3, în plic închis, cu menţiunea ofertă **„Furnizare, punere în funcţiune şi testare echipament FortiGate 100D pentru legătura VPN cu sucursala Beiuş”**din cadrul S.C. Compania de Apă Oradea S.A., până la data de **30.10.2018 ora 15^{30}**, având perioada de valabilitate 60 zile de la data limită de depunere a ofertelor.

Vă mulţumim pentru colaborare.

DIRECTOR GENERAL
ing. Ovidiu GAVRA

ŞEF COMP. ACHIZIŢII PUBLICE
ing. Vivianne SAVA

SV/VI