



CONSILIUL NAȚIONAL DE SOLUȚIONARE A CONTESTAȚIILOR

C. N. S. C.

Str. Stavropoleos, nr. 6, ..., ..., România, CIF 20329980, CP 030084
Tel. +4 021 3104641 Fax. +4 021 3104642 +4 021 890 07 45 www.cnsc.ro

În conformitate cu prevederile art. 266 alin. (2) din OUG nr. 34/2006 privind atribuirea contractelor de achiziție publică, a contractelor de concesiune de lucrări publice și a contractelor de concesiune de servicii, aprobată prin Legea nr. 337/2006 cu modificările și completările ulterioare, Consiliul adoptă următoarea

DECIZIE

Nr. .../.../...

Data: ...

Prin contestația nr. ..., înregistrată la CNSC sub nr. ..., înaintată de SC ... SA, cu sediul în ..., str. ..., ..., înmatriculată la Oficiul Registrului Comerțului sub nr. ..., având CUI RO ..., reprezentată legal de ... – administrator, formulată împotriva adresei de comunicare a rezultatului procedurii nr. .../09.04.2015, transmisă de ..., cu sediul în ..., ..., ..., în calitate de autoritate contractantă, în cadrul procedurii de licitație deschisă, organizată în vederea atribuirii contractului de „sistem firewall de protecție a aplicațiilor web”, inițiată prin publicarea în SEAP a anunțului de participare nr. .../ 31.01.2015, s-a solicitat Consiliului, în principal, anularea adresei de comunicare a rezultatului procedurii nr. .../09.04.2015 și a raportului procedurii precum și obligarea autorității contractante la reevaluarea ofertei sale, iar, în subsidiar, anularea procedurii.

În baza legii și a documentelor depuse de părți,
CONSILIUL NAȚIONAL DE SOLUȚIONARE A CONTESTAȚIILOR

DECIDE

Respinge, ca nefondată, contestația formulată de SC ... SA, în contradictoriu cu

Dispune continuarea procedurii de achiziție publică.

Obligatorie.

Împotriva prezentei decizii se poate formula plângere, în termen de 10 zile de la comunicare.

MOTIVARE

În luarea deciziei, s-au avut în vedere următoarele:

Prin contestația ..., înregistrată la CNSC sub nr. ..., SC ... SA critică decizia ... de a-i respinge ca neconformă și inacceptabilă oferta depusă în cadrul procedurii anterior menționată, solicitând cele menționate în partea introductivă.

Contestatoarea arată că motivele invocate de autoritatea contractantă pentru respingerea, ca neconformă, a ofertei sale, au fost următoarele:

- nu satisface în mod corespunzător cerințele caietului de sarcini nr. 13, 23 și 30, fiind incidente dispozițiile art. 36 alin. (2) lit. a) din HG nr. 925/2006;

- prin răspunsurile la clarificările din adresa nr. 126/07.04.2015 a modificat conținutul propunerii tehnice, fiind incidente dispozițiile art. 79 alin. (2) din HG nr. 925/2006; și inacceptabilă fiind incidente dispozițiile art. 36 alin. (1) lit. c) din HG nr. 925/2006, fiind reținute următoarele aspecte:

1. soluția ofertată nu suportă integrare nativă cu RSA enVision – fiind încălcată cerința nr. 13 din caietul de sarcini;

2. echipamentul firewall FortiWeb-100D nu are interfețe de fibră optică de 10G - fiind încălcată cerința nr. 30 din caietul de sarcini;

3. switch-urile FortiSwitch 448B, astfel cum au fost ofertate, nu asigură redundanța la nivelul surselor de tensiune și ventilatoarelor - fiind încălcată cerința nr. 23 din caietul de sarcini;

4. în cadrul listei transmise prin adresa de răspuns nr. 112/26.03.2015, la solicitarea de detalieri a produselor ofertate, se regăsește, pentru soluția de management centralizat a echipamentelor (conform cerinței nr. 21 din caietul de sarcini), **o singură licență** FortiWeb Central Manager (Part No. FWB-CM-LIC-10), iar prin răspunsul nr. 1 din adresa nr. 126/07.04.2015, se face referire la **două licențe**, declarându-se că soluția bazată pe licențe software FortiWeb Central Manager (...) oferă o redundanță distribuită, datorită faptului că cele 2 licențe sunt instalate pe 2 echipamente FortiWeb diferite – ceea ce reprezintă o modificare a ofertei tehnice;

5. prin răspunsul nr. 3 din adresa nr. 126/07.04.2015, s-a precizat că SC ... SA va oferi, fără costuri suplimentare, o sursă de putere externă (cod produs FRPS-100), pentru a suplini

neîndeplinirea cerinței tehnice obligatorii nr. 23 din caietul de sarcini privind asigurarea redundanței la nivelul surselor de tensiune - ceea ce reprezintă o modificare a ofertei tehnice.

De asemenea, contestatoarea arată că motivul invocat de autoritatea contractantă pentru respingerea ca inacceptabilă a ofertei sale a constat în faptul că prin adresa de răspuns la clarificări nr. 112/26.03.2015 a fost precizat faptul că, referințele la gama de produse FortiManager (care nu au fost incluse în lista detaliată a componentelor hardware și software ale soluției ofertate) au fost făcute pentru situația în care ar exista o preferință către acest scenariu, ceea ce a fost interpretat ca fiind o ofertă alternativă.

În opinia contestatoarei, motivele invocate de autoritatea contractantă pentru respingerea ca neconformă a ofertei sale, sunt eronate, deoarece:

1. prin răspunsul la solicitarea de clarificări ce a vizat cerința nr. 13 din caietul de sarcini, a comunicat autorității contractante că, în condițiile în care nu există un conector nativ dezvoltat și pus la dispoziție de RSA, se poate face integrarea cu enVision prin exportul evenimentelor prin Syslog, metodă folosită și de alte WAF. Mai mult, în contextul în care a fost ofertată o soluție Web Application Firewall (WAF) și nu echipamente ce îndeplinesc funcția de WAF, și luând în considerare faptul că RSA enVision este anunțat „End of Primary Support (EOPS)” în decembrie 2015 și se recomandă upgrade-ul la „RSA Security Analytics 10.4 or later”, soluția ofertată, prin intermediul echipamentului FortiAnalyzer - parte integrantă a ofertei, asigură conectare nativă cu RSA Security Analytics.

2. cerința tehnică obligatorie nr. 30 din caietul de sarcini *limitează ofertarea de echipamente spre o anumită categorie de echipamente specifice unui singur producător, ceea ce încalcă principiile promovării concurenței, tratamentului egal și al nediscriminării.* În opinia contestatoarei, soluția și nu echipamentul trebuie să fie capabilă să asigure extinderea capacităților de bandă fără a fi necesară schimbarea echipamentului. Mai mult, soluția ofertată asigură toate opțiunile de upgradare ale sistemului furnizat, în conformitate cu cerința tehnică obligatorie nr. 30, ca un sistem unitar și integrat, suportând mai mult decât s-a solicitat, respectiv 4 x 10 Gbps la nivelul soluției.

3. având în vedere modul în care este formulată cerința nr. 23 din caietul de sarcini, atât echipamentul care asigură managementul centralizat (licența instalată pe echipamentul FortiWeb 1000D) cât și echipamentele firewall de aplicație (echipamentul FortiWeb 1000D) asigură redundanță la nivelul surselor de tensiune, ventilatoarelor și HDD-urilor. Având în vedere că oferta sa este bazată pe redundanță la nivel de soluție, au fost ofertate două echipamente firewall

Fortiweb 1000D, care sunt prevăzute cu surse de alimentare și ventilatoare redundante conectate în HA, la două switch-uri FortiSwitch prevăzute cu o singură sursă de putere respectiv un ventilator (per switch). Redundanța surselor de putere și a ventilatoarelor este îndeplinită la nivelul soluției în sensul în care un switch se va defecta (ventilator, sursa de putere etc.), soluția este funcțională datorită celui de-al doilea switch.

Cele două switch-uri funcționează ca un sistem unitar având două surse de putere și două ventilatoare fiind astfel îndeplinită cerința privind redundanța la nivelul surselor de alimentare și a ventilatoarelor. Mai mult, având în vedere designul soluției tehnice oferite, aceste două switch-uri sunt considerate, împreună cu echipamentele Fortiweb, elemente critice asigurând repararea sau înlocuirea echipamentelor critice în conformitate cu cerințele BNR.

4. în oferta tehnică, la pagina 14, capitolul „Managementul Soluției” se precizează că: *„Managementul echipamentelor FortiWeb 1000D se face prin intermediul FortiWeb Central Manager accesibil prin activarea unei licențe care permite managementul de până la 10 echipamente FortiWeb prin intermediul porturilor de management de pe un singur FortiWeb 1000D. Astfel nu sunt necesare appliance-uri separate sau instalarea în sistemul informatic a unui server de management dedicat.”*

În aceste condiții, în cazul în care echipamentul pe care este instalată licența FWB-CM-LIC-10, prin intermediul căreia se realizează managementul de până la 10 echipamente FortiWeb, se defectează, această licență se poate transfera pe echipamentul rămas în funcțiune, preluând această funcționalitate. Deci, licența fiind transmisibilă, soluția oferită poate fi administrată fără afectarea serviciului. În momentul în care echipamentul defect este reparat sau înlocuit, funcționalitățile asigurate de această licență realizează sincronizarea politicilor, dacă acestea au fost schimbate între timp.

Prin urmare, prin referința la două licențe FortiWeb Central Manager nu a fost modificată oferta tehnică.

5. soluția de conectare a sistemului Fortiweb la rețea bazată pe două echipamente FortiSwitch este redundantă la nivel de surse de putere dar ... a menționat că switch-urile au posibilitatea de a include **o componentă și nu un echipament**, așa cum susține autoritatea contractantă, care să mărească cerința pentru cea de-a doua sursă de putere. Redundanța ventilatoarelor și a surselor de putere este realizată la nivelul soluției nefiind necesară introducerea ulterioară în ofertă a unui echipament care să asigure îndeplinirea cerinței nr. 23 din caietul de sarcini. Totodată, în clarificări, autoritatea contractantă nu a solicitat detalierea tuturor componentelor sistemului unitar oferit.

De asemenea, în răspunsul nr. 3 din adresa nr. 126/07.04.2015, s-a precizat că respectivul reper, respectiv sursă de putere externă (cod produs FRPS-100), va fi disponibil împreună cu echipamentele FortiSwitch, fiind parte componentă din echipamentul FortiSwitch propus. Prin urmare, sursa de putere externă fiind o componentă a echipamentului FortiSwitch și nu un echipament de sine stătător, aceasta nu modifică propunerea tehnică, așa cum susține autoritatea contractantă.

6. În ceea ce privește motivul invocat de autoritatea contractantă pentru respingerea ca inacceptabilă a ofertei, ... precizează că nu ofertează echipamentul FortiManager, acesta fiind menționat cu titlu informativ și nu ca o alternativă. În răspunsul la care face referire autoritatea contractantă nu apare sintagma „se oferă” ci doar se menționează echipamentul respectiv cu titlu informativ pentru a se arăta capabilitățile și versatilitatea soluțiilor puse la dispoziție de către Fortinet. Prin urmare, nu a fost modificată oferta tehnică și nici nu a fost prezentată o ofertă alternativă.

Date fiind cele menționate anterior, contestatoarea apreciază că că motivele pentru care oferta sa a fost respinsă au fost rezultatul evaluării tehnice greșite, nefiind justificate în nici un fel de realitate, de conținutul ofertei tehnice sau al răspunsurilor la solicitările de clarificări. Evaluarea tehnică greșită a dus, în opinia sa, la încălcarea legislației în vigoare privind achizițiile publice, inclusiv a principiilor care stau la baza atribuirii contractului de achiziție publică, în condițiile în care respingerea ofertei sale conduce la *restrângerea concurenței și la favorizarea unui anumit operator economic*.

Totodată, contestatoarea solicită studierea dosarului cauzei și înțelege să se folosească de proba reprezentată de expertiză tehnică de specialitate informatică-securitate IT.

Prin adresa nr. ..., înregistrată la Consiliu cu nr. ..., ... a transmis punctul său de vedere cu privire la contestație, însoțit de copiile dosarului achiziției și ale ofertelor depuse de contestatoare și de către câștigătoarea procedurii.

Prin punctul de vedere transmis, autoritatea contractantă invocă neîndeplinirea de către contestatoare a obligației de transmitere, în original, a dovezii privind constituirea garanției de bună conduită, prevăzută la art. 271¹ alin. (2) din OUG nr. 34/2006, solicitând respingerea, în consecință, a contestației.

De asemenea, autoritatea contractantă solicită respingerea ca tardivă a criticii legată de faptul că „*cerința tehnică obligatorie nr. 30 din caietul de sarcini limitează ofertarea de echipamente spre o anumită categorie de echipamente specifice unui singur producător, ceea ce încalcă principiile promovării concurenței, tratamentului egal și al nediscriminării*”. În susținerea acestei excepții, autoritatea

contractantă invocă data depunerii contestației (respectiv 20.04.2015), prevederile art. 256² alin. (1) lit. a) din OUG 34/2006, precum și data luării la cunoștință de actele autorității contractante.

Totodată, este invocată excepția tardivității și în raport cu criticile legate de restrângerea concurenței. În acest sens, se arată că autoritatea contractantă nu se află în situația în care, prin decizia luată, să conducă la limitarea concurenței, nefiind în discuție momentul depunerii ofertelor, ci momentul stabilirii ofertei câștigătoare. Prin necontestarea în termenul legal a cerințelor din documentația de atribuire, documentația în cauză și-a consolidat forța obligatorie atât pentru autoritatea contractantă, cât mai ales pentru operatorii economici interesați în participarea la procedura de atribuire. Odată cu depunerea ofertelor pentru procedura în cauză, respectivii operatori economici au acceptat condițiile impuse de autoritatea contractantă. Prin urmare, autoritatea contractantă apreciază că, în situația în care existau neclarități sau obiecții privind limitarea concurenței asupra acestor documente, contestatoarea avea obligația să le clarifice sau să le conteste înainte de expirarea termenului legal, anterior menționat.

Pe fondul contestației, solicită respingerea acesteia ca nefondată și neîntemeiată din următoarele considerente:

Așa cum reiese din Secțiunea II: Obiectul Contractului, capitolul II. 1 Descriere, subcapitolul II. 1.5 Descrierea succintă a contractului sau a achiziției/achizițiilor) din fișa de date a achiziției, dar și din caietul de sarcini, BNR dorește achiziționarea unui „*Sistem firewall de protecție a aplicațiilor web*”, o soluție funcțională, formată din echipamente (Server management, Firewall principal/secundar) și din servicii (servicii de instalare, instruire, suport și mentenanță, acces la serviciul oferit de producător pentru actualizări ale versiunilor software instalate). Astfel, atât soluția ofertată cât și componentele ei, trebuie să îndeplinească în totalitate cerințele impuse prin caietul de sarcini (cerințele tehnice obligatorii de la 1 la 30 fac referire atât la soluție cât și la echipamentele componente ale soluției).

Din analiza ofertei tehnice a ... s-a constatat faptul că aceasta nu îndeplinește cerința obligatorie nr. 13 din caietul de sarcini, la pag. 20 din ofertă, contestatoarea susținând că „... Fortinet este partener RSA enVision pentru o serie de produse încă din 2010, dar **RSA nu a pus la dispoziție încă un conector nativ**. Totuși integrarea este ușoară, evenimentele fiind primite prin standardul syslog”.

Or, cerința respectivă a fost impusă tocmai de necesitatea ca soluția solicitată să permită integrarea **nativă**, în mod automat, cu sistemul *ilSecurity information and event management (SIEM)* utilizat în prezent de BNR. Soluția propusă de SC ... SA nu este conformă, implicând definirea **manuală** a regulilor de filtrare,

nivelurilor de severitate și orice alți parametri utilizați ca și filtre condiționale ale evenimentelor recepționate *via syslog* pentru identificarea atacurilor informatice. Totodată, autoritatea contractantă atrage atenția că, în anexa 3.1.4 prezentată de ofertant, soluția FortiWeb nu este listată.

Referitor la cerința obligatorie nr. 30 din caietul de sarcini, respectiv "*Echipamentul firewall de aplicație trebuie să asigure capabilități de extindere hardware, (...)*", autoritatea contractantă arată că, deși prezintă în oferta sa un echipament firewall FortiWeb-1000D care nu suportă tipurile de interfețe optice solicitate, SC ... SA face o interpretare proprie a acestei cerințe a caietului de sarcini, propunând o **soluție și nu un echipament**. Soluția propusă de contestatoare ar implica utilizarea unor echipamente suplimentare (*switch-uri ethernet*) pentru ca cerința prevăzută de caietul de sarcini să fie îndeplinită. Mai mult, dacă se acceptă interpretarea mai largă „**soluția** să asigure capabilități de extindere hardware ...”, atunci soluția trebuie să îndeplinească în totalitate cerințele minime obligatorii de redundanță. Or, din analiza celor susținute în contestație, SC ... SA alege să interpreteze cerința 23 din caietul de sarcini nu în sensul "soluției" mai sus evocate, ci al echipamentului firewall de aplicație FortiWeb 1000D.

Pe de altă parte, autoritatea contractantă arată că, din analiza anexei tehnice 3.1.2 (pag. 6) trimisă de ofertant, rezultă că există, în gama de produse ale fabricantului FortiNet, echipamente (sisteme WAF) care ar fi îndeplinit cerințele caietului de sarcini: FORTIWEB 3C>OODFsx/FORTIWEB 4000D, ceea ce înseamnă că, deși avea posibilitatea să ofere un echipament conform, contestatoarea a ales să ofereze sisteme WAF din gama "*entry level*" a producătorului FortiNet care, chiar dacă ar fi acceptate sub forma unei "*soluții WAF*" împreună cu *switch-urile ethernet*, nu ar îndeplini cerința minimă obligatorie nr. 23 din caietul de sarcini.

În ceea ce privește cerința obligatorie nr. 23 din caietul de sarcini, respectiv privind *asigurarea redundanței la nivelul surselor de tensiune și ventilatoarelor*, autoritatea contractantă arată că, din oferta contestatoarei reiese că, „*echipamentul FortiSwitch 448B constituie o componentă esențială a soluției oferite pentru a asigura o densitate crescută a porturilor și capacității solicitate de BNR*”. De asemenea, din răspunsul la solicitarea de clarificări ce a vizat acest aspect, (adresa nr. 126/07.04.2015) contestatoarea a prezentat soluția FortiWeb+FortiSwitch ca un *cluster funcționar*. Prin urmare, acesta reprezintă o componentă activă a sistemului WAF, atât pentru management cât și pentru firewall aplicație, deci toate componentele sistemului WAF, inclusiv switch-ul, trebuie să îndeplinească cerința

obligatorie pentru redundanță la nivelul surselor de alimentare și ventilatoare, condiție care, în realitate, nu este îndeplinită.

Autoritatea contractantă mai arată că, în urma verificării modului în care propunerea tehnică prezentată de către SC ... SA satisface cerințele din caietul de sarcini, prin adresa nr. .../2015 a solicitat contestatoarei lista detaliată a produselor oferite. Prin răspunsul nr. 112/26.03.2015, SC ... SA a menționat, pentru soluția de management centralizat al echipamentelor (conform cerinței nr.21 din caietul de sarcini), **o singură licență** FortiWeb Central Manager, ceea ce era în concordanță și cu oferta tehnică, unde, la pagina 14, capitolul "*Managementul soluției*" se precizează că: „*Managementul echipamentelor FortiWeb 1000D se face prin intermediul FortiWeb Central Manager accesibil prin activarea unei licențe...*”.

Cu toate acestea, prin adresa nr. 126/07.04.2015, răspunsul nr. 1, SC ... SA a modificat oferta tehnică prin suplimentarea licențelor cu o bucată, precizând că: “*(...) UCS a propus soluția bazată pe licențe software FortiWeb Central Manager din următoarele rațiuni: Oferă un cost eficient; Asigură aceleași funcționalități ca și în cazul utilizării unui echipament de management dedicat; Oferă o redundanță distribuită, datorită faptului că cele 2 licențe sunt instalate pe 2 echipamente FortiWeb diferite; Nu este necesar hardware suplimentar pentru instalarea softului de management;(...*”.

Fiind evident că sunt necesare două licențe și nu una, așa cum s-a oferit inițial, oferta depusă de SC ... SA a fost considerată neconformă, modificarea ofertei neputând fi încadrată la excepțiile prevăzute la art. 79 alin. (2) din HG nr. 925/2006.

Tot în legătură cu neconformitatea ofertei SC ... SA, autoritatea contractantă mai arată că ofertantul încearcă să reformuleze ceea ce a transmis în mod foarte clar în răspunsul nr. 3 din adresa nr. 126/07.04.2015 și anume: “*In cazul în care BNR dorește instalarea și celei de-a doua surse de power, FortiSwitch suportă instalarea unei surse de putere externe (cod produs FRPS-100), oferită fără costuri suplimentare.*”

Argumentele formulate de contestatoare conform cărora „în clarificări nu s-a solicitat detalierea tuturor componentelor sistemului unitar oferit (...)”, sunt, în opinia autorității contractante, doar încercări de inducere în eroare, întrucât cele arătate au făcut obiectul primei cereri de clarificare (scrisoarea nr.XXIII.3/2307/25.03.2015 cu următoarea formulare: „*(...) vă rugăm să ne transmiteți detalierea exactă (la nivel de part number producător și cantitate oferită) a echipamentelor și a licențelor, componente ale soluției oferite.*”

Astfel, se confirmă că sursa de putere externă (cod produs FRPS-100) nu se regăsește în lista produselor oferite inițial, fiind propusă ulterior, fără costuri suplimentare, lucru care întărește

temeiul legal al declarării ca neconformă a ofertei SC ... SA, ca urmare a modificărilor propunerii tehnice, modificări care, de asemenea, nu pot fi încadrate în excepțiile prevăzute de art. 79 alin. (2) din HG nr. 925/2006.

Potrivit autorității contractante, oferta contestatoarei a fost respinsă ca inacceptabilă, în considerarea faptului că, în cadrul adresei nr. 112/26.03.2015, prin care SC ... SA a răspuns la solicitările de clarificări ce au vizat îndeplinirea cerințelor minime obligatorii pentru soluția ofertată (1, 6, 21, 23), *apar referințe către o gama de produse (FortiManager) care nu sunt cuprinse în lista detaliată a componentelor hardware și software ale soluției propuse, iar din adresa nr. 126/07.04.2015 a contestatoarei, reiese că „(...)este menționată și soluția cu FortiManager (appliance sau virtualizat) în cazul în care există o preferință către acest scenariu”.*

Prin urmare, s-a apreciat că soluția cu FortiManager (appliance sau virtualizat) constituie o alternativă la prevederile caietului de sarcini, alternativă care nu poate fi luată în considerare deoarece în anunțul de participare nu este precizată în mod explicit posibilitatea depunerii unor oferte alternative.

Ca urmare a studiului dosarului achiziției la sediul Consiliului, SC ... SA a transmis „concluziile scrise” prin adresa nr. 172/30.04.2015, înregistrată la Consiliu cu nr. 7083/ 30.04.2015, în care precizează că își menține în totalitate criticile din cadrul contestației și face, totodată, o serie de precizări cu privire la susținerile din cadrul punctului de vedere al autorității contractante.

Astfel, referitor la susținerea autorității contractante conform căreia „(...)BNR dorește achiziționarea unui „Sistem firewall de protecție a aplicațiilor web”, o soluție funcțională, formată din echipamente (Server management, Firewall principal/secundar) și din servicii (servicii de instalare, instruire, suport și mentenanță, acces la serviciul oferit de producător pentru actualizări ale versiunilor software instalate)”, contestatoarea apreciază ca fiind evident faptul că obiectul contractului este achiziționarea unei soluții, ceea ce ea a și ofertat. Prin urmare, interpretarea conform căreia, „(...) atît soluția ofertată cât și componentele ei, trebuie să îndeplinească în totalitate cerințele impuse prin caietul de sarcini (cerințele tehnice obligatorii de la 1 la 30 fac referire atît la soluție cât și la echipamentele componente ale soluției)” încalcă principiile promovării concurenței, tratamentului egal și al nediscriminării prin orientarea către produsele unui anumit furnizor, în speță produsul Imperva Secure Sphere X2510, în condițiile în care pe piață există echipamente care, făcând parte dintr-o soluție integrată, oferă aceleași caracteristici la un preț mai mic și cu o flexibilitate superioară.

Contestatoarea afirmă că și-a construit oferta astfel încât să răspundă cerințelor de disponibilitate și redundanță, luând în calcul faptul că sunt posibile abordări echivalente, respectiv redundanță la nivel de soluție sau la nivel de echipamente, din punctul de vedere al dezideratelor de disponibilitate și redundanță expuse anterior.

În ceea ce privește lipsa conectorului nativ cu sistemul Security Information and Event Management (SIEM), ceea ce implică definirea manuală a regulilor de filtrare, nivelurilor de severitate și orice alți parametri utilizați ca filtre condiționale ale evenimentelor recepționate via Syslog, contestatoarea precizează că și în cazul unui conector nativ cu respectivul SIEM există necesitatea intervenției și/sau introducerii/modificării manuale a regulilor de filtrare nivelurilor de severitate și orice alți parametri utilizați ca filtre condiționale ale evenimentelor recepționate via Syslog. Astfel, respingerea ofertei pentru acest motiv este forțată, cu atât mai mult cu cât, RSA nVision este EOPS la finalul lui 2015 iar producătorul recomandă upgrade la versiunea următoare, versiune pentru care este oferit un conector nativ cu RSA nVision prin intermediul FortiAnalyzer.

Potrivit contestatoarei, aceasta nu a oferit un echipament „entry level” așa cum afirmă autoritatea contractantă, echipamentul FortiWeb 1000D încadrându-se în mod cert la o categorie superioară de echipamente. Pe de altă parte, din analiza ofertei câștigătoare rezultă că aceasta a oferit echipamentul Imperva Secure Sphere X2510, care este din categoria „entry level”, afirmație pe care contestatoarea o susține prin trimitere la site-ul producătorului: http://www.imperva.com/docs/DS_SecureSphere_Appliance.pdf. În plus, din analiza specificațiilor tehnice ale echipamentului în cauză, respectiv volumul maxim de trafic inspectat de 500Mbps, având în vedere cerința nr. 24 din caietul de sarcini, în care se solicită ca echipamentul firewall WEBX2510 oferit să asigure inspectarea și procesarea unui trafic de 500 Mbps, și coroborat cu răspunsul ofertantului câștigător potrivit căruia „echipamentele firewall WEB x 2510 oferite asigură inspectarea și procesarea unui trafic de 500 Mbps”, rezultă că, cel puțin din acest motiv, inclusiv oferta depusă de SC KAPSCH SRL trebuia respinsă ca neconformă. În plus, modul în care a fost întocmită oferta SC KAPSCH SRL nu permite creșterea volumului de trafic inspectat peste valoarea de 500 Mbps ceea ce intră în contradicție cu cerința privind existența modulelor de extensie de 10 Gb.

În opinia contestatoarei, afirmația autorității contractante referitoare la faptul că „(...) există, în gama de produse ale fabricantului FortiNet, echipamente (sisteme WAF) care ar fi îndeplinit cerințele caietului de sarcini: FORTIWEB 3C>OODFsx/FORTIWEB

4000D (...)” denotă faptul că autoritatea contractantă nu cunoaște specificațiile gamei de produse WAF ale Fortinet, sugerând în mod eronat ideea că oferta SC ... SA se bazează pe echipamente ieftine. În plus, chiar dacă ar fi oferat echipamentele respective, oferta ar fi fost, declarată neconformă deoarece cerința nr. 30 nu putea fi satisfăcută decât de echipamentele produse de Imperva (SecureSphere x 2510) și oferate de SC KAPSCH SRL.

Contestatoarea mai atrage atenția și asupra faptului că, prin respingerea în mod eronat a ofertei sale, autoritatea contractantă este în situația de a achiziționa un sistem firewall mai puțin performant și de 1,6 ori mai scump decât cel oferat de SC ... SA.

Având în vedere faptul că atașat contestației, SC ... SA a depus garanția de bună conduită nr. 00888-02-0135818 emisă de UniCredit Jiriac Bank la data de 17.04.2015, în original, la CNSC și nu la autoritatea contractantă, la data de 05.05.2015, la solicitarea acesteia a preluat acest document și l-a depus, prin adresa nr. 174/05.05.2015, la autoritatea contractantă, fiind înregistrat cu nr. 00013268/05.05.2015.

Față de susținerile contestatoarei și de documentele depuse la dosarul cauzei, Consiliul reține cele ce urmează:

În vederea atribuirii contractului de achiziție publică având ca obiect „sistem firewall de protecție a aplicațiilor web”, ..., în calitate de autoritate contractantă, a inițiat procedura de licitație deschisă online, prin publicarea în SEAP, a anunțului de participare nr. .../31.01.2015.

Ca urmare a finalizării evaluării ofertelor, autoritatea contractantă a întocmit raportul procedurii nr. ... 09.04.2015, iar prin adresa .../09.04.2015 a comunicat contestatoarei că oferta sa a fost respinsă ca **neconformă în baza art. 36 alin. (2) lit. a) din HG nr. 925/2006**, deoarece nu satisface în mod corespunzător cerințele nr. 13, 23 și 30 din caietul de sarcini **și în baza art. 79 alin. (2) din HG nr. 925/2006** pentru modificarea ofertei tehnice prin răspunsurile nr. 112/26.03.2015 și nr. 126/07.04.2015. De asemenea, i-a comunicat că oferta a fost respinsă și ca **inacceptabilă, în baza art. 36 alin. (1) lit. c) din HG nr. 925/2006**, motivat de faptul că a prezentat o ofertă alternativă.

Nemulțumită fiind de rezultatul procedurii, ... a investit Consiliul cu soluționarea prezentei contestații, însoțită de garanția de bună conduită nr. 00888-02-0135818 emisă de UniCredit Jiriac Bank la data de 17.04.2015, depusă în original la autoritatea contractantă cu nr. 00013268/05.05.2015, solicitând, în principal, anularea adresei de comunicare a rezultatului procedurii nr. XXIII.3/2798/09.04.2015 și a raportului procedurii precum și obligarea autorității contractante la reevaluarea ofertei sale și, în subsidiar, anularea procedurii.

Analizând prezenta contestație, Consiliul are în vedere următoarele cerințe din cadrul documentației de atribuire:

- cap. II.1.1) din fișa de date a achiziției: denumirea dată contractului
- sistem firewall de protecție a aplicațiilor web;
- cap. II.1.5) din fișa de date a achiziției: descrierea succintă a contractului: sistem firewall de protecție a aplicațiilor web: server management; firewall principal/secundar; servicii de instalare, instruire, suport și mentenanță; acces serviciu de update;
- cerința 13 din caietul de sarcini: Soluția ofertată trebuie să suporte integrarea nativă cu RSA enVision;
- cerința 23 din caietul de sarcini: Atât echipamentul care asigură managementul centralizat cât și echipamentele firewall de aplicație trebuie să asigure redundanță la nivelul surselor de tensiune, ventilatoarelor, HDD-urilor;
- cerința 30 din caietul de sarcini: Echipamentul firewall de aplicație trebuie să asigure capabilități de extindere hardware, existând posibilitatea instalării oricăror din următoarele tipuri de interfețe de rețea (suplimentar interfețelor de rețea implicite cerute), fără a fi necesară schimbare echipamentului:

- a. minim 4 interfețe electrice de 1G;
- b. minim 2 interfețe de fibră optică de 1G;
- c. minim 2 interfețe de fibră optică de 10 G.

Cu privire la modul de îndeplinire a acestor cerințe, Consiliul reține că, pe parcursul evaluării ofertelor, autoritatea contractantă a solicitat mai multe clarificări în vederea stabilirii conformității ofertei prezentate, potrivit prevederilor art. 35 și 78 din HG nr. 925/2006, la care aceasta a răspuns, susținând că soluția ofertată le îndeplinește, ca ansamblu și prezentând modalitățile concrete prin care sunt satisfăcute aceste cerințe.

În acest sens, Consiliul reține că SC ... SA susține că soluția ofertată nu suportă integrarea nativă cu RSA envision, ci sunt necesare elemente suplimentare, că echipamentele firewall de aplicație nu asigură redundanță la nivelul surselor de tensiune, ventilatoarelor, HDD-urilor, dar că soluția asigură redundanța printr-o altă modalitate, că echipamentul firewall de aplicație nu asigură capabilități de extindere hardware cu minim 2 interfețe de fibră optică de 10 G, dar că soluție asigură posibilitatea acestei interfațări.

În acest context, Consiliul reține că autoritatea contractantă a depus toate diligențele în vederea stabilirii caracterului admisibil sau nu al ofertei depuse de contestatoare și a concluzionat că oferta acesteia este neconformă, din motivele mai sus menționate.

De asemenea, Consiliul reține în soluționare, următoarele elemente:

- conform prevederilor art. 35 alin. (2) din OUG nr. 34/2006, cu modificările și completările ulterioare „specificatiile tehnice reprezintă cerințe, prescripții, caracteristici de natură tehnică ce permit fiecărui produs, serviciu sau lucrare să fie descris, în mod obiectiv, în așa manieră încât să corespundă necesității autorității contractante”, contestatoarea neprezentând dovezi concrete din care să rezulte că diferențele existente în propunerea sa tehnică față de prevederile caietului de sarcini, mai conduc la o soluție care satisface necesitățile autorității contractante;

- contestatoarea, deși a ales o soluție tehnică care nu respectă, în totalitate, prevederile caietului de sarcini, nu a depus minima diligență de a aduce la cunoștința și de a solicita acceptul autorității contractante pentru aceste abateri, în perioada anterioară depunerii ofertelor;

- deși obiectul contractului îl reprezintă „sistem firewall de protecție a aplicațiilor web”, ceea ce reprezintă o soluție unitară, anumite cerințe, care au fost formulate cu referire la echipamentele componente, nefiind contestate, trebuie respectate ca atare, atât de către ofertanți, în temeiul art. 170 din OUG nr. 34/2006, cu modificările și completările ulterioare, respectiv „Ofertantul elaborează oferta în conformitate cu prevederile din documentația de atribuire”, cât și de către autoritatea contractantă, în evaluarea ofertelor, cu respectarea, în raport cu ceilalți ofertanți și cu operatorii economici care nu au depus oferte deoarece soluțiile lor nu respectau chiar aceste cerințe, a principiului tratamentului egal și al transparenței, principii ce stau la baza atribuirii contractelor de achiziție publică, enunțate la art. 2 alin. (2) lit. b) și d) din același act normativ;

- nu pot fi considerate ca incidente prevederile art. 36 alin. (2) din OUG nr. 34/2006, cu modificările și completările ulterioare, deoarece, deși „autoritatea contractantă definește specificațiile tehnice din caietul de sarcini prin precizarea performanțelor și/sau cerințelor funcționale solicitate”, contestatoarea nu s-a raportat la standarde, omologări sau reglementări tehnice, ci a adoptat o soluție tehnică diferită.

Dispozițiile art. 34 și 72 alin. (1) din HG nr. 925/2006 stabilesc obligația de evaluare completă a ofertelor în sarcina autorității contractante, obligație pe care aceasta și-a îndeplinit-o pentru stabilirea corectă a rezultatului procedurii.

Prin urmare, Consiliul constată că evaluarea ofertei prezentate de contestatoare s-a făcut cu respectarea prevederilor art. 72 alin. (2) din HG nr. 925/2006, sub acest aspect.

Totodată, Consiliul consideră că nu se impune o expertiză tehnică de specialitate informatică-securitate IT (așa cum propune contestatoarea) pentru stabilirea conformității ofertei sale, în discuție nefiind funcționalitatea ofertei sale, ci respectarea de către propunerea sa tehnică a prevederilor caietului de sarcini.

Această apreciere a Consiliului este rezultatul faptului că s-a analizat efectiv modul în care contestatoarea a înțeles să-și întocmească oferta și să răspundă solicitărilor de clarificări întocmite cu respectarea prevederilor art. 78 din HG nr. 34/2006 și a principiilor care stau la baza achizițiilor publice stipulate la art. 2 alin. (2) din ordonanța de urgență.

În ceea ce privește criticile formulate de contestatoare prin "concluzii scrise", suplimentare celor din contestație, în referire la ofertantul declarat câștigător, Consiliu are în vedere prevederile art. 270 din OUG nr. 34/2006, potrivit cărora: *Contestația se formulează în scris și trebuie să conțină următoarele elemente: a) numele, domiciliul sau reședința contestatorului ori, pentru persoanele juridice, denumirea, sediul lor și codul unic de înregistrare. În cazul persoanelor juridice se vor indica și persoanele care le reprezintă și în ce calitate; b) denumirea și sediul autorității contractante; c) denumirea obiectului contractului de achiziție publică și procedura de atribuire aplicată; d) obiectul contestației; e) motivarea în fapt și în drept a cererii; f) mijloacele de probă pe care se sprijină contestația, în măsura în care este posibil; g) semnătura părții sau a reprezentantului persoanei juridice. (2) În situația în care Consiliul apreciază că în contestație nu sunt cuprinse toate informațiile prevăzute la alin. (1), va cere contestatorului ca, în termen de 5 zile de la înștiințarea prin care i se aduce la cunoștință această situație, acesta să completeze contestația. În cazul în care contestatorul nu se conformează obligației impuse de Consiliu, contestația va fi respinsă.*

Din conținutul normei expuse rezultă că persoana vătămată sesizează Consiliul, într-un termen anume dat, cu o contestație care trebuie să cuprindă obligatoriu motivarea în fapt și drept.

Nicăieri în cuprinsul cap. IX din ordonanță nu se amintește că persoana vătămată își poate completa voluntar motivarea contestației prin care s-a delimitat cadrul soluționării, astfel încât Consiliul să analizeze alte critici decât cele cu care a fost investit în termenul legal de contestare.

Prin urmare, criticile suplimentare celor din contestația formulată prin "concluzii scrise" vor fi respinse ca inadmisibile.

Luând în considerare aspectele de fapt și de drept evocate, în baza art. 278 alin. (5) din Ordonanța de urgență a Guvernului nr. 34/2006 privind atribuirea contractelor de achiziție publică, a contractelor de concesiune de lucrări publice și a contractelor de concesiune de servicii, cu modificările și completările ulterioare, Consiliul respinge, ca nefondată, contestația formulată de SC ... SA, în contradictoriu cu

În baza art. 278 alin. (6) din ordonanța de urgență, Consiliul dispune continuarea procedurii de achiziție publică.

La punerea în aplicare a dispozițiilor din prezenta decizie, părțile vor avea în vedere că aceasta este obligatorie, conform art. 280 alin. (3) din OUG nr. 34/2006, având dreptul de a o ataca cu plângere, în concordanță cu art. 281 din același act normativ.

PREȘEDINTE COMPLET

...

MEMBRU COMPLET

MEMBRU COMPLET

...

Redactată în 4 exemplare originale, conține 15 pagini.