REPUBLIKA HRVATSKA
MINISTARSTVO FINANCIJA

KLASA: 406-01/14-01/121
URBROJ: 513-03-04-14-3

Zagreb, 10. lipnja 2014.

DODATAK O IZMJENI DOKUMENTACIJE ZA BAGATELNI POSTUPAK NABAVE PROXY POSLUŽITELJ

Naručitelj Ministarstvo financija objavljuje dodatak o izmjeni Dokumentacije za bagatelni postupak nabave proxy poslužitelj KLASA: 406-01/14-01/121, URBROJ: 513-03-04-14-2 od 6. lipnja 2014., bagatelna nabava 9/14.

I. DOPUNA

Naručitelj u Dokumentaciji za bagatelni postupak nabave proxy poslužitelj dodaje u točki 3. PREDMET NABAVE; TEHNIČKA SPECIFIKACIJA; Tablica 1., redak pod redni broj 1. :

„Ponuđeno rješenje mora podržavati 1000 istovremenih korisnika.”

Izmijenjena Tablica 1., Dokumentacije za bagatelni postupak nabave proxy poslužitelj KLASA: 406-01/14-01/121, URBROJ: 513-03-04-14-2 od 6. lipnja 2014., bagatelna nabava 9/14 :

Tablica 1.

PROXY POSLUŽITELJ - TEHNIČKA SPECIFIKACIJA -		
Redni Broj	Opis minimalnih zahtjeva	Zadovoljava Da/Ne
1.	Ponuđeno rješenje mora podržavati 1000 istovremenih korisnika	
2.	Ponuđeno rješenje mora biti pozicionirano od strane tržišnih analitičara (kao Gartner) kao predvodnik	
3.	Ponuđeno rješenje mora biti dostupno u obliku *virtual appliance*-a za Vmware ESX okruženje	
4.	upravljanje i zaštita web prometa internih korisnika (prema internetu) tako i vanjskih korisnika	
5.	Ponuđeno rješenje mora nuditi forward i reverse proxy funkcionalnost u svrhu upravljanja web i streaming sadržajima internih i vanjskih korisnika;	
6.	Namjenski operativni sustav visokih performansi koji nije temeljen na OS-u opće namjene (Linux, Microsoft, itd.);	
7.	Podržano više načina integracije u mrežnu infrastrukturu: eksplicitni proxy (postavke definirane na klijentu ručno ili kroz PAC/WPAD skriptu); transparentni proxy (bez definiranih proxy postavki na klijentu): podrška za Cisco WCCP, transparent bridging, default gateway uz IP forwarding, Policy-based routing (TCP port redirekcija).	
8.	Podrška za IPv6	
9.	Mogućnost dobivanja visoke raspoloživosti (High availability) kroz active/passive clustering uz automatski failover korištenjem virtualnih IP adresa;	
10.	Mogućnost korištenja više linkova (gateway-a) prema internetu uz gateway load balancing i failover;	
11.	Proxy mora podržavati terminaciju, nadzor, kontrolu i optimizaciju barem sljedećih protokola: HTTP, HTTPS (SSL), FTP, Telnet, SOCKS, P2P, AOL IM, Yahoo IM, Microsoft IM, MMS, RTSP (streaming), QuickTime, Flash streaming (RTMP), TCP-Tunneling, DNS	
12.	Optimizacija protokola mora uključivati napredni caching HTTP i streaming sadržaja;	
13.	Podrška za slijedeće autentikacijske mehanizme: Active Directory LDAP, Windows IWA odnosno SSO (NTLM), SAML, SunOne, eDirectory, Netegrity Siteminder, Oblix, Radius, lokalni password file;	
14.	Podrška za korištenje višestrukih autentifikacijskih mehanizama i njihovo ulančavanje;	
15.	Mogućnost definiranja fleksibilne i granularne politike autentifikacije korisnika iz više LDAP i/ili Active Directory izvora ovisno o različitim parametrima klijenta (IP adresa, mreža, User-agent polje, proxy port, kombinacije navedenog itd.);	
16.	Mogućnost definiranja granularne politike pristupa prema odredišnim parametrima kao što su IP/Subnet, Port, URL, URL kategorija, extenzija datoteke, MIME tip, HTTP „Response Code", HTTP „Response Header" te kombinacije navedenog	
17.	Mogućnost definiranja politike pristupa po parametrima kao što su tip protokola (HTTP: FTP over HTTP, P2P over HTTP...), Protokol metode (HTTP: Connect, Get, Post; FTP: CWD, PASV, PASS...)	
18.	Mogućnost definiranja različitih politika pristupa prema vremenskim intervalima	
19.	Integrirana podrška za URL filtriranje po kategorijama sadržaja na samom uređaju, uz podršku za dinamičku kategorizaciju web stranica u realnom vremenu;	
20.	Mogućnost kategorizacije jednog URL-a u do 4 kategorije (npr. Social Networking, Games, Web Advertisements)	
21.	Rješenje mora uključivati detekciju zlonamjernog prometa u odlaznom toku (tzv. bot phone home), te praćenje/detekciju malnet/bot aktivnosti na internetu kroz dinamičku kategorizaciju sadržaja	
22.	Mogućnost primjene iste ili različite politike filtriranja URL sadržaja na klijente unutar i izvan mreže, koristeći posebni softver na klijentima	
23.	Softverski klijent treba imati: • mogućnost optimizacije i ubrzavanja aplikacijskih protokola, koristeći barem ove tehnike: byte caching, optimizacija TCP prometa, optimizacija CIFS (Windows Networking) prometa, CIFS caching, kompresija cjelokupnog mrežnog prometa. • mogućnost definiranja politike ovisno o lokaciji klijenta (unutar ili izvan mreže organizacije) • Real-time kategorizacija URL-ova i anti-phising zaštita na razini klijenta • Centralno upravljana politika pristupa web sadržaju - politika na klijentu (čak i kada je izvan lokalne mreže odnosno offline!) je sinkronizirana sa centralnom politikom na internet gateway-u. • Upravljanje i udaljena instalacija sa centralne konzole • Integracija sa postojećim rješenjem za siguran pristup internetu na internet gateway-u.	
24.	Mogućnost filtriranja prometa i kroz *cloud* servis, uz mogućnost sinkronizacije politike na uređaju i u cloud-u na jednoj točki administracije	
25.	Podrška za ICAP protokol i integracija s antivirusnim rješenjima temeljenima na ICAP protokolu;	
26.	Podrška i integracija sa Data-loss prevention (DLP) rješenjima temeljenima na ICAP protokolu;	
27.	Ugrađena mogućnost detekcije i filtriranja popularnih web aplikacija neovisno o URL-u (npr. Facebook, Google Talk, Dropbox, itd.)	
28.	Integrirana osnovna DLP funkcionalnost na samom uređaju: npr. mogućnost zabrane upload-a na webmail servise (npr. Gmail), zabrana slanja datoteka preko Facebook-a i sl.	
29.	Ažurna detekcija popularnih web servisa uz granularnu kontrolu akcija (npr. omogućavanje samo read-only rada u okviru Facebook-a i sličnih servisa)	
30.	Podrška za SSL intercepciju uz fleksibilnu i granularnu konfiguraciju uvjeta dekripcije SSL prometa;	

31.	Podrška za HTTPS reverzni proxy uz mogućnost SSL rasterećenja backend servera;	
32.	Reverzni proxy mora imati elemente zaštite web site-ova od vanjskih prijetnji (Web Application Firewall) poput SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), buffer overflow napadi uz provjeru sukladnosti protokola (protocol compliance checks) i Denial of Service zaštitu;	
33.	Upravljanje streaming sadržajem (RTSP, RTMP, MMS, QuickTime, Real Networks) uz tzv. stream splitting i caching;	
34.	Upravljanje bandwith-om s obzirom na smjer prometa (dolazni i odlazni) te stranu komunikacije (prema klijentu, prema serveru);	
35.	Prioritiziranje prometa.	
36.	Granularna kontrola Skype prometa prema autenticiranom korisniku;	
37.	Prepoznavanje i upravljanje (bandwidth management, blokiranje, itd.) pojedinim Peer-to-Peer protokolima;	
38.	Instant Messaging refleksija (na način da IM promet ne izlazi iz organizacije, a poruke se proslijeđuju primateljima);	
39.	Instant Messaging filtriranje sadržaja prema ključnim riječima, vrsti attachmenta, itd.	
40.	Mogućnost logiranja IM prometa (MSN, Yahoo, AOL);	
41.	Podrška za HTTP kompresiju kao i kompresiju na TCP nivou;	
42.	Mogućnost definiranja politike na temelju QOS TOS / DSCP vrijednosti;	
43.	Web i CLI interface za menadžment	
44.	Split-DNS podrška	
45.	SSHv2 i SSL/TLS administracija	
46.	Obavještavanje administratora korištenjem SNMP i SMTP protokola	
47.	Podrška za Syslog logiranje	
48.	Logiranje slijedećih korisničkih aktivnosti: HTTP, HTTPS, FTP, Telnet, SOCKS, P2P, TCP-Tunnel, ICP, IM, Windows Media, Real Media, QuickTime, DNS.	
49.	Praćenje trenutnih realtime statistika prometa: HTTP/FTP/IM/Streaming aktivne sesije, broj korisnika, iskorištenje bandwidtha po protokolima, itd.	
50.	Web aplikacija za napredno izvještavanje prema autenticiranom korisniku, mreži, sigurnosti, vrsti aplikacijskog protokola, itd.	
51.	Web aplikacija za napredno izvještavanje treba sadržavati • podesivu kontrolnu ploču • pred-definirane izvještaje te jednostavno kreiranje posebnih izvještaja ○ Spyware i Malware ○ Korištenje pojmova na tražilicama ○ URL filtering kategorije ○ Web sadržaj ○ Korisnici/Grupe i ostalo • Mogućnost integracije sa LDAP/AD-om kako bi se ostvarila mogućnost različitih prikaza za različite funkcije unutar organizacije, kao i mogućnost da svaki pojedini zaposlenik vidi svoje podatke • WEB API koji omogućuje dohvat podatka u aplikaciji u HTTP/XML, PDF i CSV formatima • Mogućnost forenzičke analize sve do razine sesije korištenjem drill-in metodologije ili detaljnih parametara • Audit log (audit trail) svih aktivnosti u sklopu aplikacije za izještavanje	
52.	Mogućnost delegacije prava formiranja politike URL filtriranja različitim osobama (lokalnim administratorima), pri čemu te osobe formiraju politiku za određenu grupu korisnika (iz LDAP-a, Active Directory-a ili jednostavno prema rangu IP adrese).	
53.	Mogućnost formulara za feedback: korisnik može poslati povratnu informaciju na e-mail administratora kroz konfigurabilni web formular koji se prikaže pri blokiranju određene stranice.	
54.	Instalacija, konfiguracija i integracija Proxy poslužitelja u postojeće računalno komunikacijsko okruženje prema poslovnim potrebama Naručitelja	
55.	Ponuditi jamstvo i održavanje za Proxy poslužitelj u trajanju od minimalno 3 godine na lokaciji Naručitelja. Obaveza Ponuditelja je osigurati ispravke pogrešaka u programskoj opremi i zakrpe (patch) kao i online, mail i telefonsku pomoć direktno od Ponuditelja u trajanju od 3 godine. Održavanje uključuje testiranje novih inačica programske opreme, te podrška, instalacija i implementacija na lokaciji Naručitelja. Sve nadogradnje i zakrpe koje se pojave u jamstvenom roku i vremenu održavanja također su uključeni u održavanje kao i njihova instalacija, implementacija i testiranje. Prelazak na drugu inačicu programske opreme besplatan je sve dok traje jamstveni rok.	
56.	Originalna programska (isporuka popravaka i nadogradnji koda) i sigurnosna (automatska nadogradnja sigurnosnih ažuriranja, pravila i potpisa) podrška proizvođača opreme za vrijeme trajanja jamstva	
57.	Naručitelj prijavljuje kvar u jamstvenom roku od 00-24h (365/7/24 podrška). Ponuditelj počinje otklanjati kvar izlaskom na lokaciju Naručitelja na način da otkloni kvar u roku do 24 sata od prijave kvara. Ukoliko Ponuditelj ne može otkloniti kvar na neispravnoj opremi može isporučiti zamjensku opremu istih ili boljih karakteristika koja time postaje vlasništvo Naručitelja.	
58.	Jamstvo 3 godine na lokaciji naručitelja od datuma potpisa Zapisnika o primopredaji (obrazac Naručitelja)	