PREGLED POSTUPKA #86952

1 PODACI O NARUČIOCU

Naziv naručioca	AGENCIJA ZA CIVILNO VAZDUHOPLOVSTVO
PIB	02638649
E-mail	acv@caa.me
Telefon	+382 20 625 507
Internet adresa	www.caa.me
Fax	+382 20 625 517
Adresa	Josipa Broza Tita bb
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Nabavka softverskog rješenja za kontrolu pristupa internet sadržaju zaposlenih
Status	Čeka na objavu
Vrsta predmeta	Robe
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Sanja Poleksic
Kontakt	067/400-191
Datum objave	17.02.2025. 11:00
Napomena	-

3 FAZE U POSTUPKU

Nema faza u izabranom postupku

4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
Posebni oblici javne nabavke	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
Nabavka se sprovodi kao	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne

5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2025	**AGENCIJA ZA CIVILNO VAZDUHOPLOVSTVO** **Softversko rješenje za kontrolu pristupa internet sadržaju zaposlenih** 48000000 - Softverski paketi i informacioni sistemi	20.661,16 EUR	4.338,84 EUR	-	-	-	Jednostavna nabavka

17.02.2025 10:39:07

6 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Tip uslova / zahtjeva
Izjava ponuđača o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisana od strane ovlašćenog lica ponuđača, koja se sačinjava na Obrascu 2 iz Pravilnika o načinu sprovođenja jednostavnih nabavki	Obrazac 2
Podgorica, Agencija za civilno vazduhoplovstvo, ul. Josipa Broza Tita bb	Mjesto izvršenja ugovora
Rok plaćanja je 15 dana po ispostavljenoj fakturi za izvršene usluge za prethodni mjesec sa pozivom na broj ugovora po kojem se plaćanje vrši	Uslovi plaćanja
Virmanski	Način plaćanja
Rok izvršenja ugovora je 12 mjeseci od dana zaključivanja ugovora ili do dostizanja ugovorene vrijednosti nabavke, u zavisnosti od toga koji od dva navedena uslova bude ranije ispunjen	Rok izvršenja ugovora
Garantni rok: minimalno 12 mjeseci od dana isporuke licenci i implementacije predmeta nabavke i prijema od strane ovlašćenih lica naručioca: - Ponuđač je dužan da dostavi potvrdu proizvođača predmetnog rješenja, kojom potvrđuje da je ponuđen softver sa obezbijeđenom tehničkom podrškom od minimalno 12 mjeseci od strane proizvođača softvera ili njenog ovlašćenog predstavnika	Garantni rok
Ponuđač mora imati uspostavljen sistem upravljanja kvalitetom iz oblasti predmeta nabavke koju dokazuje sertifikatom ili drugom odgovarajućom potvrdom nadležnog organa ili organizacije o ispunjavanju uslova upravljanja kvalitetom iz oblasti predmeta nabavke: 1. Sertifikat o ispunjenosti standarda ISO 27001 za upravljanje IT sigurnošću 2. Sertifikat o ispunjenosti standarda ISO 9001 za upravljanje kvalitetom	Dokaz odnosno sertifikat, koje izdaju akreditovana sertifikaciona tijela o ispunjavanju uslova kvaliteta predmeta nabavke
Ponuđač je dužan da na realizaciji predmeta javne nabavke angažuje stručni tim koji će biti sastavljen od minimum sledećih lica: - Ponuđač je obavezan da ima minimum jedno sertifikovano tehničko lice koja će biti uključeno u implementaciju traženog security rješenja;	Stručna i tehnička sposobnost

Dokaz o angažovanju radne snage (kopija radne knjižice, prijava za osiguranje ili ugovor o radu) za implementaciju ponuđenog security rješenja – sertifikat od ponuđenog proizvođača softvera za tehničku obučenost za upravljanje i konfigurisanje ponuđenog rješenja	Stručna i tehnička sposobnost

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **20.661,16 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		Ponuđeno rješenje mora nuditi forward i reverse proxy funkcionalnost u svrhu upravljanja web i streaming sadržajima internih i vanjskih korisnika; Ponuđeno rješenje može biti u obliku hardverskog uređaja sa operativnim sistemom visokih performansi, posebno prilagođenim velikom broju konekcija i volumenu web prometa. Pored gore navedenog hardverskog uređaja, rješenje može biti dostupno i u obliku virtualnog uređaja za Vmware ESX okruženje. Sistem mora podržavati implementaciju i u oblaku, sa istim funkcionalnostima kao i lokalno. Ponuđeno rješenje se mora temeljiti na namjenskom operativnom sistemu visokih performansi koji nije temeljen na OS-u opšte namjene (Linux, Microsoft, itd.); Podržano više načina integracije u mrežnu infrastrukturu: eksplicitni proxy (postavke definisane na klijentu ručno ili kroz PAC/WPAD skriptu); transparentni proxy (bez definisanih proxy postavki na klijentu): podrška za Cisco WCCP, transparent bridging, default gateway uz IP forwarding, Policy-based routing (TCP port redirekcija). Ponuđeno rješenje mora podržavati IPv6 .	

		Potrebno je da ponuđeno rješenje podržava visoku raspoloživost (High availability) kroz active/passive clustering uz automatski failover korištenjem virtualnih IP adresa; Potrebno je da rješenje ima mogućnost korišćenja više linkova (gateway-a) prema internetu uz gateway load balancing i failover; Potrebno je da ponuđeno rješenje podržava link agregaciju više interface-ova koristeći standard 802.1AX Link Aggregation. Korišćenje višestrukih routing domena tj. različitih setova routing tablica ovisno o interface-u (fizičkom ili VLAN) mora biti podržano. 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 . Optimizacija protokola mora uključivati napredni caching HTTP i streaming sadržaja; Podrška za slijedeće autentikacijske mehanizme: Active Directory LDAP, Windows IWA odnosno SSO (NTLM), SAML, SunOne, eDirectory, Oracle COREid, Radius, lokalni password file; Podrška za korištenje višestrukih autentifikacijskih mehanizama i njihovo ulančavanje; Integracija sa Active Directory dostupna na 2 načina: spajanje direktno sa uređaja ili korišćenjem posredničkog servisa/agenta instaliranog na domain member serveru. Podrška za istovremeno korišćenje više Active Directory izvora, čak i ako nisu u trust odnosu tj. povezani na bilo koji način.	

		Mogućnost filtriranja prometa i kroz cloud servis, uz mogućnost sinkronizacije politike na uređaju i u cloud-u na jednoj točki administracije. Podrška za ICAP protokol i integracija sa antivirusnim rješenjima temeljenima na ICAP protokolu; Podrška za intrgraciju sa Zero Turst Network Access. Podrška i integracija sa Data-loss prevention (DLP) rješenjima temeljenima na ICAP protokolu. Filtriranje i sigurnost prometa Potrebno je da je podržana granularna politika pristupa prema odredišnim parametrima kao što su IP/Subnet, Port, URL, URL kategorija, pravi tip datoteke, extenzija datoteke, MIME tip, HTTP „Response Code“, HTTP „Response Header“, aplikacija, te kombinacije navedenog . Pravila pristupa moraju podržavati različite politike pristupa prema vremenskim intervalima (npr. dani u nedelji i slično). Rješenje mora podržavati mogućnost definisanje bandwidth ili vremenskih kvota po korisnicima (npr. ograničavanje vremena provedenog na internetu ili ograničavanje ukupnog volumena prometa u nekom vremenu). Integrirana podrška za URL filtriranje po kategorijama sadržaja na samom uređaju, uz podršku za dinamičku kategorizaciju web stranica u realnom vremenu; Rješenje mora podržavati kategorizaciju URL-ova, te mogućnost definisanja vlastitih kategorija. Rješenje mora podržavati detekciju "Botnet" mreža i prometa. Potrebno je da sistem omogućava primjenu istih pristupnih politika za korisnike unutra i izvan mreže korišćenjem agenta. sistem mora omogućiti i primjenu pristupnih politika zavisno i	

1	Nabavka i implementacija softvera za kontrolu pristupa internet sadrzaju zaposlenih u skladu sa tehničkom specifikacijom za 70 zaposlenih	o lokaciji klijenta (unutar ili izvan mreže organizacije). sistem mora omogućiti detekciju malicioznog koda u komprimiranim datotekama (.zip, .jar, .gzip, .tar, itd.). sistem mora podržavati kontrolu pristupa na mobilnim uređajima (iOS i Android). sistem mora podržavati sljedeće Internet preglednike: MS Edge, Chrome, Firefox i Safari). sistem mora imati mogućnost detekciju verzije Internet preglednika i blokiranja pristupa zastarjelim verzijama. Potrebno je da podržava dvosmjerno filtriranje i detekciju malicioznog sadržaja . Podrška za presretanje SSL prometa uz fleksibilnu i granularnu konfiguraciju uvjeta dekripcije SSL prometa; Granularno filtriranje Webex prometa: npr. korisnik može sudjelovati u Webex sjednici, ali ne može dijeliti datoteke ili vlastiti desktop. Ponuđeno rješenje mora imati mogućnost "izolacije" Internet odredišta, uklanjanjem svog koda te slanjem samo slike odredišta korisniku. Ponuđeno rješenje mora imati mogućnost blokiranja unosa pristupnih podataka na "izoliranim" Internet odredištima. Mogućnost kontrole i filtriranja web aplikacija prema nizu atributa same aplikacije, npr. radi li se o Enterprise-ready aplikaciji, podržava li SSO, podržava li multi-factor autentikaciju, podržava li SAML, podržava li SSL, da li ima password policy i podržava li kompleksne lozinke, radi li se o nativnoj mobilnoj aplikaciji, radi li se o aplikaciji za non-business korisnike, uključuje li aplikacija u datacentru kriptiranje sadržaja (data-at-rest), itd. Mogućnost filtriranja prometa prema ocijeni rizika, a koja je dobivena u realnom vremenu.	1,00 komplet

		Mogućnost filtriranja prometa prema geografskoj lokaciji Internet odredišta. Mora postojati mogućnost pregleda korištenih cloud servisa od strane korisnika. Reverzni proxy i Web Application Firewall Podrška za HTTP/HTTPS reverzni proxy uz mogućnost SSL rasterećenja backend servera; Podrška za kompleksna prepisivanja sadržaja (npr. URL and content rewriting) kod objave internih web aplikacija: kroz GUI ili ugrađeni skriptini jezik. Provjera saglasnosti protokola (protokol compliance checks) i Denial of Service zaštita. Opcionalno mogućnost aktiviranja Web Application Firewall (WAF) funkcionalnosti sa zaštitom od napada poput SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), buffer overflow, itd. Opcionalna WAF funkcionalnost mora koristiti napredno filtriranje temeljeno i na detekciji anomalija u prometu, a kako bi se izbjegle lažne detekcije povezane sa prepoznavanjem uzoraka teksta u prometu (pattern matching). Opcionalna WAF funkcionalnost ima mogućnost filtriranja prometa prema lokaciji odnosno zemlji koja je izvorište prometa (Geo lokacija). Upravljanje i izvještavanje Web i CLI interface za menadžment . SSHv2 i SSL/TLS administracija. Mogućnost centralizovanog upravljanja kroz zasebno softversko rješenje koje podržava centralizovani monitoring	

		svih rješenja u portfelju proizvođača. Eksport konfiguracije kroz tekstualni format tj. seriju naredbi koje je moguće upisati u CLI interface. Podrška za Safenet HSM-ove kod pohrane privatnih ključeva i certifikata (npr. kod objave SSL web site-a). Podrška za odvojene i zasebne politike za više organizacija na istom hardveru (tzv. multi-tenant policy) uz mogućnost definiranja zajedničke tj. krovne politike. Mogućnost definisanja zajedničke politike u scenariju kada se koriste uređaji i cloud servis za filtriranje istovremeno. Obavještavanje administratora korišćenjem SNMP i SMTP protokola. Određivanje statusa mrežne povezanosti eksternih servisa (npr., dostupnost DNS, LDAP, itd. kroz tzv. health check) i odaziva servisa te krojenja politike prema rezultatima provjere. Podrška za Syslog logovanje . Logovanje sljedećih korisničkih aktivnosti: HTTP, HTTPS, FTP, Telnet, SOCKS, P2P, TCP-Tunnel, ICP, IM, Windows Media, Real Media, QuickTime, DNS. Praćenje trenutnih realtime statistika prometa: HTTP/FTP/IM/Streaming aktivne sesije, broj korisnika, iskorištenje bandwidtha po protokolima, itd. Web aplikacija za napredno izvještavanje prema autenticiranom korisniku, mreži, sigurnosti, vrsti aplikacijskog protokola, itd. Integracija sa LDAP/AD-om kako bi se ostvarila mogućnost različitih prikaza za različite funkcije unutar organizacije, kao i mogućnost da svaki pojedini zaposleni vidi svoje podatke. Slanje odabranih izvještaja u vremenskim intervalima (eng. Scheduler).	

		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 izvještavanje. Delegacija 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). Web aplikacija za izvještavanje: moguće i kroz cloud servis, pri čemu uređaji i klijenti šalju logove na cloud reporting servis, a radi centralnog izvještavanja neovisno o lokaciji korisnika (unutar ili van LAN mreže). Content Analysis System Antivirusno skeniranje prometa korišćenjem barem 1 antivirusnog engine-a, uz opcionalno korištenje višestrukih engine-a paralelno. Antimalware zaštitu od virusa, spyware-a, trojana, rootkitova, botova (uključujući i skeniranje SSL prometa). Antimalware komponenta mora se integrirati sa proxy rješenjem putem ICAP protokola. Podrška za Secure ICAP (ICAPS) protokol. Dubinska provjera svog sadržaja na malware i cjelokupnog prometa, uključujući nekompresovane datoteke do 8GB veličine, te kompresiju do 99 nivoa. Opcija vlastitog Whitelistinga i blacklistinga za eliminiranje nepotrebne analize sigurnih datoteka. Integrisana usluga file reputacije tj. provjere hash-a datoteke i njezine rasprostranjenosti globalno uz određivanje ocjene rizičnosti	

		Statička analiza koda radi detekcije nepoznatog malware-a. Mogućnost prosljeđivanja sumnjivih datoteka u sandboxing rješenje radi dodatne analize. Mogućnost integracija sa više sandboxing rješenja različitih proizvođača. Inteligentni caching kako bi se izbjegla dvostruka provjera identičnog sadržaja. Feedback o novootkrivenim prijetnjama prema dinamičkoj bazi prijetnji proizvođača, radi detekcije na ostalim točkama i eventualnim drugim rješenjima. Rješenje mora imati mogućnosti integracije sa EDR i XDRpostojećim rješenjem	