Izmjena postupka

OSNOVNI PODACI

Opis predmeta javne nabavke:

Nabavka licenci

Vrsta predmeta:

Usluge

Vrsta postupka:

Otvoreni postupak

PODACI O NARUČIOCU

Naziv:

MINISTARSTVO UNUTRAŠNJIH POSLOVA

PIB:

02016010

Uslovi prije izmjena

Opis	Tip uslova	Važi za sve partije
U postupku javne nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja ili potvrde nadležnog organa izdatog na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište	Obavezni uslovi	Da
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje, o kojima evidenciju vodi organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište.	Obavezni uslovi	Da
Ispunjenost uslova za učešće u postupku javne nabavke dokazuje se Izjavom privrednog subjekta. Obrazac 1	ESPD	Da
Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosi od 2% procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 15 dana nakon isteka važenja ponude.Garancija ponude će se aktivirati ako ponuđač: 1) odustane od ponude u roku važenja ponude i/ili 2) odbije da zaključi ugovor o javnoj nabavci ili okvirni sporazum.	Garancija ponude	Da
Rok važenja ponude: 60 (šezdeset) dana od dana otvaranja ponuda.	Rok važenja ponude	Da
Mjesto izvršenja ugovora je zgrada Ministarstva unutrašnjih poslova u Podgorici, prostorije Službe za informacione tehnologije. .	Mjesto izvršenja ugovora	Da
Rok plaćanja: u roku od 30 (trideset) dana od dana dostavljanja fakture, nakon isporučene robe.	Rok plaćanja	Da

Način plaćanja: virmanski.	Način plaćanja	Da
Način sprovođenja kontrole kvaliteta: Kontrolu kvaliteta sprovodiće službenici Službe za informacione tehnologije.	Način sprovođenja kontrole kvaliteta	Da
Ukoliko se zahtijevaju posebni uslovi okoline ponuđač je dužan da specificira detaljno uslove okoline neophodne za ispravno funkcionisanje proizvoda.	Drugi uslovi	Da
Proizvod mora biti nov i nekorišćen.	Drugi uslovi	Da
Isporuka se može vršiti sukcesivno ali u okviru maksimalnog roka izvršenja ugovora	Drugi uslovi	Da
Ponuđač je u obavezi da za naručioca kod proizvođača otvori servisni nalog a sve u cilju upravljanja kupljenim proizvodom ili izvrši prebacivanje prava na već postojeći nalog naručioca .	Drugi uslovi	Da
Ukoliko se zahtjevaju posebni podaci potrebni za predmetnu nabavku, aktivaciju ili preusmjeravanje prava, naručilac se obavezuje da će iste dostaviti u neposrednoj komunikaciji sa izabranim ponuđačem.	Drugi uslovi	Da

Uslovi nakon izmjena

Opis	Tip uslova	Važi za sve partije
U postupku javne nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja ili potvrde nadležnog organa izdatog na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište	Obavezni uslovi	Da

U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje, o kojima evidenciju vodi organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište.	Obavezni uslovi	Da
Ispunjenost uslova za učešće u postupku javne nabavke dokazuje se Izjavom privrednog subjekta. Obrazac 1	ESPD	Da
Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosi od 2% procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 15 dana nakon isteka važenja ponude.Garancija ponude će se aktivirati ako ponuđač: 1) odustane od ponude u roku važenja ponude i/ili 2) odbije da zaključi ugovor o javnoj nabavci ili okvirni sporazum.	Garancija ponude	Da
Rok važenja ponude: 60 (šezdeset) dana od dana otvaranja ponuda.	Rok važenja ponude	Da
Mjesto izvršenja ugovora je zgrada Ministarstva unutrašnjih poslova u Podgorici, prostorije Službe za informacione tehnologije. .	Mjesto izvršenja ugovora	Da
Rok plaćanja: u roku od 30 (trideset) dana od dana dostavljanja fakture, nakon isporučene robe.	Rok plaćanja	Da
Način plaćanja: virmanski.	Način plaćanja	Da
Način sprovođenja kontrole kvaliteta: Kontrolu kvaliteta sprovodiće službenici Službe za informacione tehnologije.	Način sprovođenja kontrole kvaliteta	Da
Ukoliko se zahtijevaju posebni uslovi okoline ponuđač je dužan da specificira detaljno uslove okoline neophodne za ispravno funkcionisanje proizvoda.	Drugi uslovi	Da
Proizvod mora biti nov i nekorišćen.	Drugi uslovi	Da
Isporuka se može vršiti sukcesivno ali u okviru maksimalnog roka izvršenja ugovora	Drugi uslovi	Da
Ponuđač je u obavezi da za naručioca kod proizvođača otvori servisni nalog a sve u cilju upravljanja kupljenim proizvodom ili izvrši prebacivanje prava na već postojeći nalog naručioca .	Drugi uslovi	Da

Ukoliko se zahtjevaju posebni podaci potrebni za predmetnu nabavku, aktivaciju ili preusmjeravanje prava, naručilac se obavezuje da će iste dostaviti u neposrednoj komunikaciji sa izabranim ponuđačem.	Drugi uslovi	Da

Kriterijumi prije izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja	Važi za sve partije
Cijena	-	-	Da
Za partiju 1: parametar kvalitet vrednovaće se na sljedeći način: Maksimalan broj bodova po ovom parametru je 20, u okviru kojeg će se bodovati sljedeće: 1. Najkraći ponuđeni rok izvršenja ugovora ..... 20 bodova; Maksimalan broj bodova, po parametru Najkraći ponuđeni rok izvršenja ugovora dodjeljuje se ponuđaču koji je ponudio najkraći rok izvršenja ugovora, dok se bodovi ostalim ponuđačima, po ovom parametru, dodijeljuju proporcionalno, u odnosu na najkraći ponuđeni rok izvršenja ugovora, po formuli: Najkraći ponuđeni rok izvršenja ugovora Broj bodova = ---------- x 20 Ponuđeni rok izvršenja ugovora Ponuđači su dužni da u dijelu, kriterijum za vrednovanje ponuda, precizno naznače koliki rok izvršenja ugovora nude u danima, u odnosu na zahtijevani maksimum 60 dana od dana obostranog potpisivanja ugovora. Kao osnov za vrednovanje navedenog parametra, uzima se kraći ponuđeni rok izvršenja ugovora u odnosu na zahtijevani - maksimum 60 dana od dana potpisivanja ugovora.	Eksplicitna numerička vrijednost	Relativno	Ne

Za partiju 2: □ parametar kvalitet vrednovaće se na sljedeći način: Maksimalan broj bodova po ovom parametru je 20, u okviru kojeg će se bodovati sljedeće: 1. Najkraći ponuđeni rok izvršenja ugovora ..... 20 bodova; Maksimalan broj bodova, po parametru Najkraći ponuđeni rok izvršenja ugovora dodjeljuje se ponuđaču koji je ponudio najkraći rok izvršenja ugovora, dok se bodovi ostalim ponuđačima, po ovom parametru, dodijeljuju proporcionalno, u odnosu na najkraći ponuđeni rok izvršenja ugovora, po formuli: Najkraći ponuđeni rok izvršenja ugovora Broj bodova = ---------- x 20 Ponuđeni rok izvršenja ugovora Ponuđači su dužni da u dijelu, kriterijum za vrednovanje ponuda, precizno naznače koliki rok izvršenja ugovora nude u danima, u odnosu na zahtijevani maksimum 60 dana od dana obostranog potpisivanja ugovora. Kao osnov za vrednovanje navedenog parametra, uzima se kraći ponuđeni rok izvršenja ugovora u odnosu na zahtijevani - maksimum 60 dana od dana potpisivanja ugovora.	Eksplicitna numerička vrijednost	Relativno	Ne

Za partiju 3: parametar kvalitet vrednovaće se na sljedeći način: Maksimalan broj bodova po ovom parametru je 20, u okviru kojeg će se bodovati sljedeće: 1. Najkraći ponuđeni rok izvršenja ugovora ..... 20 bodova; Maksimalan broj bodova, po parametru Najkraći ponuđeni rok izvršenja ugovora dodjeljuje se ponuđaču koji je ponudio najkraći rok izvršenja ugovora, dok se bodovi ostalim ponuđačima, po ovom parametru, dodijeljuju proporcionalno, u odnosu na najkraći ponuđeni rok izvršenja ugovora, po formuli: Najkraći ponuđeni rok izvršenja ugovora Broj bodova = ---------- x 20 Ponuđeni rok izvršenja ugovora Ponuđači su dužni da u dijelu, kriterijum za vrednovanje ponuda, precizno naznače koliki rok izvršenja ugovora nude u danima, u odnosu na zahtijevani maksimum 60 dana od dana obostranog potpisivanja ugovora. Kao osnov za vrednovanje navedenog parametra, uzima se kraći ponuđeni rok izvršenja ugovora u odnosu na zahtijevani - maksimum 60 dana od dana potpisivanja ugovora.	Eksplicitna numerička vrijednost	Relativno	Ne

Kriterijumi nakon izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja	Važi za sve partije
Cijena	-	-	Da

Za partiju 1: □ parametar kvalitet vrednovaće se na sljedeći način: Maksimalan broj bodova po ovom parametru je 20, u okviru kojeg će se bodovati sljedeće: 1. Najkraći ponuđeni rok izvršenja ugovora ..... 20 bodova; Maksimalan broj bodova, po parametru Najkraći ponuđeni rok izvršenja ugovora dodjeljuje se ponuđaču koji je ponudio najkraći rok izvršenja ugovora, dok se bodovi ostalim ponuđačima, po ovom parametru, dodijeljuju proporcionalno, u odnosu na najkraći ponuđeni rok izvršenja ugovora, po formuli: Najkraći ponuđeni rok izvršenja ugovora Broj bodova = ---------- x 20 Ponuđeni rok izvršenja ugovora Ponuđači su dužni da u dijelu, kriterijum za vrednovanje ponuda, precizno naznače koliki rok izvršenja ugovora nude u danima, u odnosu na zahtijevani maksimum 60 dana od dana obostranog potpisivanja ugovora. Kao osnov za vrednovanje navedenog parametra, uzima se kraći ponuđeni rok izvršenja ugovora u odnosu na zahtijevani - maksimum 60 dana od dana potpisivanja ugovora.	Eksplicitna numerička vrijednost	Relativno	Ne

Za partiju 2: parametar kvalitet vrednovaće se na sljedeći način: Maksimalan broj bodova po ovom parametru je 20, u okviru kojeg će se bodovati sljedeće: 1. Najkraći ponuđeni rok izvršenja ugovora ..... 20 bodova; Maksimalan broj bodova, po parametru Najkraći ponuđeni rok izvršenja ugovora dodjeljuje se ponuđaču koji je ponudio najkraći rok izvršenja ugovora, dok se bodovi ostalim ponuđačima, po ovom parametru, dodijeljuju proporcionalno, u odnosu na najkraći ponuđeni rok izvršenja ugovora, po formuli: Najkraći ponuđeni rok izvršenja ugovora Broj bodova = ---------- x 20 Ponuđeni rok izvršenja ugovora Ponuđači su dužni da u dijelu, kriterijum za vrednovanje ponuda, precizno naznače koliki rok izvršenja ugovora nude u danima, u odnosu na zahtijevani maksimum 60 dana od dana obostranog potpisivanja ugovora. Kao osnov za vrednovanje navedenog parametra, uzima se kraći ponuđeni rok izvršenja ugovora u odnosu na zahtijevani - maksimum 60 dana od dana potpisivanja ugovora.	Eksplicitna numerička vrijednost	Relativno	Ne

Za partiju 3: □ parametar kvalitet vrednovaće se na sljedeći način: Maksimalan broj bodova po ovom parametru je 20, u okviru kojeg će se bodovati sljedeće: 1. Najkraći ponuđeni rok izvršenja ugovora ..... 20 bodova; Maksimalan broj bodova, po parametru Najkraći ponuđeni rok izvršenja ugovora dodjeljuje se ponuđaču koji je ponudio najkraći rok izvršenja ugovora, dok se bodovi ostalim ponuđačima, po ovom parametru, dodijeljuju proporcionalno, u odnosu na najkraći ponuđeni rok izvršenja ugovora, po formuli: Najkraći ponuđeni rok izvršenja ugovora Broj bodova = ---------- x 20 Ponuđeni rok izvršenja ugovora Ponuđači su dužni da u dijelu, kriterijum za vrednovanje ponuda, precizno naznače koliki rok izvršenja ugovora nude u danima, u odnosu na zahtijevani maksimum 60 dana od dana obostranog potpisivanja ugovora. Kao osnov za vrednovanje navedenog parametra, uzima se kraći ponuđeni rok izvršenja ugovora u odnosu na zahtijevani - maksimum 60 dana od dana potpisivanja ugovora.	Eksplicitna numerička vrijednost	Relativno	Ne

Tehnička specifikacija prije izmjena

Redni broj partije	Opis	Procijenjena vrijednost bez PDV	Redni broj predmeta nabavke	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina	Jedinica mjere
1	Nabavka licenci/softwerskog paketa	36500.00	1	UEM (Unified Endpoint Management) rješenje u on-premise modelu sa licencom/ma za 2 Tehničara (administracija Sistema), uspostavljanje redudantnog-failover sistema i Secyre Gateway Server.Rješenje mora da omogući centralizovano	1. Obuhvaćeni uređaji Uređaji koje rješenje mora podržavati: Windows 10/11 desktop i laptop uređaje Android mobilni uređaji iOS / iPadOS macOS 2. Funkcionalni zahtjevi 2.1. Upravljanje uređajima	1.00	Komada

				upravljanje desktop i mobilnim uređajima za potrebe organizacije.Rješenje mora podržavati minimalno 250 uređaja uz mogućnost skaliranja Ili ekvivalentno proizvodu ManageEngine Endpoint Central - Security edition	Ponuđeno rješenje mora imati mogućnosti: Centralizovana konzola (web-based) Automatski i ručni enrolment Remote wipe, remote lock, restart Konfiguracija Wi-Fi, VPN, APN, certifikata Upravljanje politikama lozinki i enkripcije Inventar uređaja (HW/SW) Upravljanje desktop OS-om (Windows i macOS – ako vendor podržava) 2.2. Upravljanje aplikacijama Silent instalacija i deinstalacija aplikacija Upravljanje verzijama aplikacija Blokiranje neodobrenih aplikacija Privatni katalog aplikacija (enterprise store) Distribucija aplikacija na Windows (MSI, EXE, PowerShell) 2.3. KIOSK MODE Rješenje mora obavezno podržavati kiosk mod sa sljedećim minimalnim mogućnostima: A) Single-App Kiosk Uređaj zaključan u jednu aplikaciju Zabranjeno napuštanje aplikacije Automatsko pokretanje aplikacije nakon restarta Onemogućavanje statusne trake, postavki, notifikacija Podržano i za Android i iOS Daljinsko		

aktiviranje/deaktiviranj
e
B) Multi-App Kiosk
Uređaj ograničen
samo na unaprijed
definisan skup
aplikacija
Blokada svih drugih
aplikacija i funkcija
Mogućnost
ograničavanja
browsera (dozvoljene
domene)
Kontrola fizičkih
dugmadi, USB-a,
Bluetooth-a i drugih
funkcija sistema
Podržano i za Android,
iOS, i Windows
(Assigned Access)
C) Dodatne
funkcionalnosti
Custom launcher
(Android)
Automatski reboot ako
aplikacija prestane
raditi
Ograničavanje
screenshotova
Onemogućavanje
sistemskih dijaloga
2.4. Secure Gateway
Server
Rješenje mora
uključivati ili omogućiti
integraciju Secure
Gateway komponente
(edge/proxy server)
koja:
Prima saobraćaj
agenata uređaja van
mreže naručioca i
prosljeđuje ga prema
glavnom UEM serveru.
Može se postaviti u
DMZ zoni radi
sigurnosti.
Koristi TLS/HTTPS
komunikaciju i
autentikaciju agenata.
Podržava skalabilnost
za trenutnih 250
uređaja i pruža moguć

						nost povećanja kapaciteta. Omogućava logovanje i auditing saobraćaja. Podržava visoku dostupnost. Administratorski portal i API za upravljanje, uključujući sertifikate i ACL pravila. 2.5. Sigurnosni zahtjevi DLP – Data Loss Prevention Enkripcija podataka (BitLocker, FileVault, Android/iOS native) Siguran web browser / filtriranje sadržaja Patch Management za Windows i macOS Endpoint privilege management Kontrola fizičkih dugmadi, USB-a, Bluetooth-a i drugih funkcija sistema Detekcija neusklađenih uređaja i automatska remedijacija TLS enkripcija komunikacije RBAC – role-based access control Audit log svi administratorskih i korisničkih aktivnosti 2.6. Dodatno-Sigurnosni zahtjevi Ransomware zaštita Malware zaštita 2.7. Integracije Integracija s Active Directory / LDAP PKI integracija (SCEP / CA) API (REST) za integraciju s drugim sistemima Integracija s SIEM sistemima (Splunk ,ELK, Graylog, …) 2.8. Izvještavanje		

					Automatsko generisanje PDF/CSV izvještaja Izvještaji o inventaru, sigurnosti, neusklađenim uređajima Notifikacije putem e-maila Dashboard s KPI (ključnim indikatorima sistema) 3. Tehnički zahtjevi za on-premise instalaciju 3.1. Operativni sistem servera Podržavati barem jedan od sljedećih OS-ova: Windows Server 2019/2022 Linux (RHEL, CentOS, Ubuntu) 3.2. Baza podataka Mora podržavati barem jednu DB platformu: MS SQL Server PostgreSQL MySQL 4. Podrška i servis minimalno 3 godine podrške i održavanja - uključena u ponudu minimalno 3 godine uključena nadogradnja (updates + security patches) SLA vrijeme odgovora: Standardni: 24h Instalacija i podešavanje Sistema. Obuka za administratore (min. 6h) – online ili onsite. 5. Skalabilnost Rješenje mora omogućavati skaliranje do 500+ uređaja bez promjene arhitekture.		
			2	Windows Server 2022 RDS (Remote Desktop	Korisnčki/User CAL	10.00	Komada

				Services) User CAL			
2	Zanavljenje/Priduženje Licenci	31000.00	1	Paket/Licenca (5 godina) Fortigate 100F	1. FG-10-F100F-950-02-36 FortiGate-100F 3 Year, Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service…etc) and FortiCare Premium.	2.00	Komada
			2	Paket/Licenca (5 godina) Fortigate 101F	1. FG-101F-BDL-809-36 FortiGate-101F + 3 Year Enterprise Protection (EP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service,DLP, ZTNA …etc), FortiCare Premium +HW.	2.00	Komada
3	Nabavka licenci/softwerskog paketa/hardverskih komponenti sistema za kontrolu i sigurnost digitalnog saobraćaja	56000.00	1	Sistem za kontrolu i filtriranje pristupa internetu, filtriranje sadržaja ili ekvivalentno modelu : HW FortiProxy-400G + sa uključenim SKU-ovima FC1-10-XY40G-514-02-36 i FC-10-XY40G-247-02-36	Sistem / Hardver Model: -Fizički Uređaj 1U Deployment: -Inline, Forward Proxy, Explicit Proxy, WCCP/PBR, Routed Proxy Podrška IP: -IPv4 i IPv6 Licence korisnika: -Min. 500 korisnika (SWG bundle) Performanse: -Throughput do 40 Gbps, do 8 miliona simultanih sesija, SSL/HTTPS inspekcija -Uređaj mora omogućiti kreiranje najmanje 10 logički nezavisnih jedinica, pri čemu svaka jedinica mora imati sopstveno stanje, konfiguraciju i mogućnost samostalnog upravljanja ili kontrole,	1.00	Komada

					nezavisno od ostalih jedinica. Memory: -Min. 16 GB Management: - HTTP/S, SSH, CLI, SNMP, Console RJ45 Network Interfaces: - Min. 4x GE RJ45 Storage : - Min. 4 TB (2 TB x2) Hard Disk Power Supply 220V : - Dual- redudantno HA: - Active-Active / Active-Passive sa sinhronizacijom sesija T. Protection / SWG Trajanje licence 5Y: - 5 godina trajanja licence u okviru kojih je omogućeno redovno ažuriranje, unapređenje definicija Web i Video Filtering - Dinamička kategorizacija, blokiranje malicioznih domena i URL-ova, crne i bele liste DNS Filtering - Blokiranje sumnjivih i malicioznih domena Kontrola aplikacija - Granularna kontrola, podrška za 3000+ aplikacija IPS (Intrusion Prevention) - Zaštita od mrežnih napada i ranjivosti Antivirus (AV) - Skeniranje fajlova, zaštita od virusa, ransomware i malvera Botnet zaštita - Blokiranje IP/domen botneta i C2 komunikacije Sandboxing - Cloud sandboxing za napredne i zero-day pretnje Content Disarm &		

Reconstruct - Sanitizacija i rekonstrukcija sadržaja pre isporuke korisniku
Autentifikacija
Metode: - Radius, SAML, LDAP, NTLM, Kerberos, OTP
Ugrađena autentifikacija - Da. Bez potrebe za dodatnim uređajem
Napredno keširanje
Web/Video caching - Keširanje sadržaja za ubrzanje pristupa i optimizaciju propusnog opsega
Reverse caching: - Obrnuto keširanje web sadržaja
Traffic shaping & QoS - Prioritetizacija aplikacija, podrška za dinamički adaptivni streaming (HTTP, RTP, RTMPT)
WAN optimizacija
Protokoli - HTTP, MAPI, CIFS, FTP, TCP
Tunneling - Sigurno tunelovanje preko WAN-a
WAN peers - Podrška za WAN Optimization peers
Management & Reporting
View - Mogća Integracija za monitoring i vizualizaciju saobraćaja
Analyzer - Integracija za centralizovano izveštavanje i analizu
Syslog - Podrška za Syslog server
RBAC - Granularna kontrola pristupa zasnovana na ulogama
Logging & Reporting -

					Praćenje, izveštavanje, testiranje politika Podrška / Servis 3 godine trajanja licenci Premium nivo: - Da. Podrška (24x7), tehnička pomoć, web i telefonska podrška Zamjena hardverskih delova: - RMA i zamjena kritičnih komponenti u slučaju kvara Firmware & Update - Redovno ažuriranje softvera, antivirusnih definicija, sigurnosnih potpisa		
				2	Sistem za kontrolu , filtriranje, zaštitu i enkripciju elektronske pošte sa 3 godine preimum-Pro podrškom i 3 godišnjom licencom antispam i antivirus servisa —dodatnih, “enterprise-level” sigurnosnih i zaštitnih funkcionalnosti ili ekvivalentno modelu : FortiMail 400F SKU:FML-400F-BDL-641-36	1. System / Deployment Hardware Specifications 10/100/1000 Interfaces (Copper, RJ45) : 4 Storage : 2× 1 TB RAID Storage Management: Hardware 0, 1, 5, 10, Hot Spare Memory: 8 GB Form Factor: Rack Mount, 1U System Specifications Protected Email Domains: Min. 70 Recipient-Based Policies (per Domain / per System): 400 / 1500 Server Mode local mailboxes: Min. 400 Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System): 50 / 200 Email Routing (per	1.00	Komada

hour): 250 K
Antispam + Virus Outbreak (per hour): 200 K
Email Routing (per hour): 83 K
Antispam + Virus Outbreak (per hour): 72 K
Power Source: 100–240 V AC, 50–60 Hz
Power Supply: Dual - redudant
Certification: VBSpam and VB100; NIST CMVP test (FIPS140 3).

• Deployment i operativnie opcije
o On-premise
o Transparent i server mode
• Inbound i outbound inspekcija emaila
• SMTP autentikacija (LDAP, RADIUS, POP3, IMAP)
• LDAP-based email routing
• Inspekcija po korisniku na osnovu LDAP atributa (po domen politici)
• Geografski IP-based policy
• Webmail interfejs za server mode i karantin
• Mail queue management
• Podrška za više jezika
• SMTP RFC kompatibilnost
• Modern HTML5 GUI
• Kompatibilnost sa cloud servisima: Microsoft 365, Google Workspace, AWS, Azure
• DNS-based Authentication of

Named Entities (DANE) podrška (ako proizvođač podržava)
2. Antispam
• Antispam servis
o Sender i domain reputation
o Spam i attachment signatures
o Heuristička i ponašajna analiza
o Outbreak protection
• URL category filtering: spam, malware, phishing, pornografski/adult sadržaj, newly registered domains
• Greylisting za IPv4, IPv6 i email accounts
• Lokalna reputacija pošiljalaca
• Integracija sa trećim spam URIs i RBL/SURBL listama
• Newsletter/greymail detekcija
• PDF i Office dokument skeniranje i analiza
• Blok/safe liste na globalnom, domen i korisničkom nivou
• Podrška za SPF, DKIM, DMARC
• Fleksibilne akcije i notifikacije
• Sistemski i per-user self-service karantin
3. Targeted Attack Protection
• Content disarm i reconstruction: neutralizacija makroa i aktivnog sadržaja u Office/PDF dokumentima
• Neutralizacija hyperlinkova u email HTML sadržaju (ako podržava proizvođač)
• Business Email Compromise (BEC)

					zaštita o Anti-spoof protection o Impersonation i cousin domain detection • URL click protection (preusmeravanje/skeniranje linkova) • Integracija sa browser isolation platformom ili sličnom funkcionalnošću (ako podržava proizvođač) 4. API Integration • Microsoft 365 i Google Workspace integracija o Post-delivery threat scanning (ako podržava) o Scheduled i real-time scanning o Internal mail scanning 5. Content Detection • Antivirus / malware detection (heuristika, signature-based, greyware) • Virus outbreak protection (global threat intelligence, ako proizvođač podržava) • Aktivni sadržaj (PDF & Office dokumenti) • Rescan poruka na karantinu • Custom file hash i MIME/type detekcija • DLP / Data-loss prevention (osnovna detekcija fajlova, PII, finansijski podaci, osetljivi sadržaji) • Decryption za arhive, PDF i Office dokumente sa poznatim password listama (ako podržava proizvođač) • PDF / Office skeniranje i analiza slika		

						• Dynamic image analysis (prepoznavanje nedozvoljenog sadržaja, ako podržava proizvođač) 6. Encryption • TLS server-to-server sa opcijama za ciphersuite • S/MIME • Clientless email enkripcija (portal-based ili built-in funkcionalnost) • Outlook plugin ili dodatak za enkripciju (ako podržava proizvođač) 7. Management, Logging, Reporting • Per-domain i role-based administracija • Aktivnost i promena konfiguracija logging • Built-in reporting i detaljno praćenje poruka • Centralizovani karantin za velike deployment-e • Centralizovano logovanje (ako podržava proizvođač) • SNMP, eksterni syslog • Open REST API za konfiguraciju i management • Lokalni ili eksterni storage serveri (uključujući iSCSI) 8. High Availability (HA) • Active-Passive i Active-Active konfiguracije • Sinhronizacija karantina i mail queue • Failover i redundantne interfejse 9. Advanced / Email Server funkcionalnosti		

					• Policy-based email archiving (uključujući Exchange journal, ako podržava) • POP3/IMAP pristup, webmail interfejs • Osnovne kalendarske funkcije i undo send • SAML 2.0 SSO i ADFS integracija (webmail/karantin) 10. Support • Profesionalna tehnička podrška; trajanje podrške 3 godine • Uključena RMA podrška • Licenca za Antispam i antivirus servise —dodatne, “enterprise-level” sigurnosne i zaštitne funkcionalnosti; trajanje licence 3 godine.		

Tehnička specifikacija nakon izmjena

Redni broj partije	Opis	Procijenjena vrijednost bez PDV	Redni broj predmeta nabavke	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina	Jedinica mjere
1	Nabavka licenci/softwerskog paketa	36500.00	1	UEM (Unified Endpoint Management) rješenje u on-premise modelu sa licencom/ma za 2 Tehničara (administracija Sistema), uspostavljanje redudantnog-failover sistema i Secyre Gateway Server.Rješenje mora da omogući centralizovano upravljanje desktop i mobilnim uređajima za	1. Obuhvaćeni uređaji Uređaji koje rješenje mora podržavati: Windows 10/11 desktop i laptop uređaje Android mobilni uređaji iOS / iPadOS macOS 2. Funkcionalni zahtjevi 2.1. Upravljanje uređajima Ponuđeno rješenje mora imati	1.00	Komada

				potrebe organizacije.Rješenje mora podržavati minimalno 250 uređaja uz mogućnost skaliranja Ili ekvivalentno proizvodu ManageEngine Endpoint Central - Security edition	mogućnosti: Centralizovana konzola (web-based) Automatski i ručni enrolment Remote wipe, remote lock, restart Konfiguracija Wi-Fi, VPN, APN, certifikata Upravljanje politikama lozinki i enkripcije Inventar uređaja (HW/SW) Upravljanje desktop OS-om (Windows i macOS – ako vendor podržava) 2.2. Upravljanje aplikacijama Silent instalacija i deinstalacija aplikacija Upravljanje verzijama aplikacija Blokiranje neodobrenih aplikacija Privatni katalog aplikacija (enterprise store) Distribucija aplikacija na Windows (MSI, EXE, PowerShell) 2.3. KIOSK MODE Rješenje mora obavezno podržavati kiosk mod sa sljedećim minimalnim mogućnostima: A) Single-App Kiosk Uređaj zaključan u jednu aplikaciju Zabranjeno napuštanje aplikacije Automatsko pokretanje aplikacije nakon restarta Onemogućavanje statusne trake, postavki, notifikacija Podržano i za Android i iOS Daljinsko aktiviranje/deaktiviranj e		

B) Multi-App Kiosk
Uređaj ograničen samo na unaprijed definisan skup aplikacija
Blokada svih drugih aplikacija i funkcija
Mogućnost ograničavanja browsera (dozvoljene domene)
Kontrola fizičkih dugmadi, USB-a, Bluetooth-a i drugih funkcija sistema
Podržano i za Android, iOS, i Windows (Assigned Access)
C) Dodatne funkcionalnosti
Custom launcher (Android)
Automatski reboot ako aplikacija prestane raditi
Ograničavanje screenshotova
Onemogućavanje sistemskih dijaloga
2.4. Secure Gateway Server
Rješenje mora uključivati ili omogućiti integraciju Secure Gateway komponente (edge/proxy server) koja:
Prima saobraćaj agenata uređaja van mreže naručioca i prosljeđuje ga prema glavnom UEM serveru.
Može se postaviti u DMZ zoni radi sigurnosti.
Koristi TLS/HTTPS komunikaciju i autentikaciju agenata.
Podržava skalabilnost za trenutnih 250 uređaja i pruža moguć nost povećanja kapaciteta.

					Omogućava logovanje i auditing saobraćaja. Podržava visoku dostupnost. Administratorski portal i API za upravljanje, uključujući sertifikate i ACL pravila. 2.5. Sigurnosni zahtjevi DLP – Data Loss Prevention Enkripcija podataka (BitLocker, FileVault, Android/iOS native) Siguran web browser / filtriranje sadržaja Patch Management za Windows i macOS Endpoint privilege management Kontrola fizičkih dugmadi, USB-a, Bluetooth-a i drugih funkcija sistema Detekcija neusklađenih uređaja i automatska remedijacija TLS enkripcija komunikacije RBAC – role-based access control Audit log svi administratorskih i korisničkih aktivnosti 2.6. Dodatno-Sigurnosni zahtjevi Ransomware zaštita Malware zaštita 2.7. Integracije Integracija s Active Directory / LDAP PKI integracija (SCEP / CA) API (REST) za integraciju s drugim sistemima Integracija s SIEM sistemima (Splunk ,ELK, Graylog, …) 2.8. Izvještavanje Automatsko generisanje PDF/CSV		

					izvještaja Izvještaji o inventaru, sigurnosti, neusklađenim uređajima Notifikacije putem e-maila Dashboard s KPI (ključnim indikatorima sistema) 3. Tehnički zahtjevi za on-premise instalaciju 3.1. Operativni sistem servera Podržavati barem jedan od sljedećih OS-ova: Windows Server 2019/2022 Linux (RHEL, CentOS, Ubuntu) 3.2. Baza podataka Mora podržavati barem jednu DB platformu: MS SQL Server PostgreSQL MySQL 4. Podrška i servis minimalno 3 godine podrške i održavanja - uključena u ponudu minimalno 3 godine uključena nadogradnja (updates + security patches) SLA vrijeme odgovora: Standardni: 24h Instalacija i podešavanje Sistema. Obuka za administratore (min. 6h) – online ili onsite. 5. Skalabilnost Rješenje mora omogućavati skaliranje do 500+ uređaja bez promjene arhitekture.		
			2	Windows Server 2022 RDS (Remote Desktop Services) User CAL	Korisnčki/User CAL	10.00	Komada

2	Zanavljenje/Priduženje Licenci	31000.00	1	Paket/Licenca (3 godina) Fortigate 100F	1. FG-10-F100F-950-02-36 FortiGate-100F 3 Year, Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service…etc) and FortiCare Premium.	2.00	Komada
			2	Paket/Licenca (3 godina) Fortigate 101F	1. FG-101F-BDL-809-36 FortiGate-101F + 3 Year Enterprise Protection (EP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service,DLP, ZTNA …etc), FortiCare Premium +HW.	2.00	Komada
3	Nabavka licenci/softwerskog paketa/hardverskih komponenti sistema za kontrolu i sigurnost digitalnog saobraćaja	56000.00	1	Sistem za kontrolu i filtriranje pristupa internetu, filtriranje sadržaja ili ekvivalentno modelu : HW FortiProxy-400G + sa uključenim SKU-ovima FC1-10-XY40G-514-02-36 i FC-10-XY40G-247-02-36	Sistem / Hardver Model: -Fizički Uređaj 1U Deployment: -Inline, Forward Proxy, Explicit Proxy, WCCP/PBR, Routed Proxy Podrška IP: -IPv4 i IPv6 Licence korisnika: -Min. 500 korisnika (SWG bundle) Performanse: -Throughput do 40 Gbps, do 8 miliona simultanih sesija, SSL/HTTPS inspekcija -Uređaj mora omogućiti kreiranje najmanje 10 logički nezavisnih jedinica, pri čemu svaka jedinica mora imati sopstveno stanje, konfiguraciju i mogućnost samostalnog upravljanja ili kontrole, nezavisno od ostalih	1.00	Komada

					jedinica. Memory: -Min. 16 GB Management: - HTTP/S, SSH, CLI, SNMP, Console RJ45 Network Interfaces: - Min. 4x GE RJ45 Storage : - Min. 4 TB (2 TB x2) Hard Disk Power Supply 220V : - Dual- redudantno HA: - Active-Active / Active-Passive sa sinhronizacijom sesija T. Protection / SWG Trajanje licence 5Y: - 5 godina trajanja licence u okviru kojih je omogućeno redovno ažuriranje, unapređenje definicija Web i Video Filtering - Dinamička kategorizacija, blokiranje malicioznih domena i URL-ova, crne i bele liste DNS Filtering - Blokiranje sumnjivih i malicioznih domena Kontrola aplikacija - Granularna kontrola, podrška za 3000+ aplikacija IPS (Intrusion Prevention) - Zaštita od mrežnih napada i ranjivosti Antivirus (AV) - Skeniranje fajlova, zaštita od virusa, ransomware i malvera Botnet zaštita - Blokiranje IP/domen botneta i C2 komunikacije Sandboxing - Cloud sandboxing za napredne i zero-day pretnje Content Disarm & Reconstruct -		

Sanitizacija i rekonstrukcija sadržaja pre isporuke korisniku
Autentifikacija
Metode: - Radius, SAML, LDAP, NTLM, Kerberos, OTP
Ugrađena autentifikacija - Da. Bez potrebe za dodatnim uređajem
Napredno keširanje
Web/Video caching - Keširanje sadržaja za ubrzanje pristupa i optimizaciju propusnog opsega
Reverse caching: - Obrnuto keširanje web sadržaja
Traffic shaping & QoS - Prioritetizacija aplikacija, podrška za dinamički adaptivni streaming (HTTP, RTP, RTMPT)
WAN optimizacija
Protokoli - HTTP, MAPI, CIFS, FTP, TCP
Tunneling - Sigurno tunelovanje preko WAN-a
WAN peers - Podrška za WAN Optimization peers
Management & Reporting
View - Mogća Integracija za monitoring i vizualizaciju saobraćaja
Analyzer - Integracija za centralizovano izveštavanje i analizu
Syslog - Podrška za Syslog server
RBAC - Granularna kontrola pristupa zasnovana na ulogama
Logging & Reporting - Praćenje, izveštavanje,

						testiranje politika Podrška / Servis 3 godine trajanja licenci Premium nivo: - Da. Podrška (24x7), tehnička pomoć, web i telefonska podrška Zamjena hardverskih delova: - RMA i zamjena kritičnih komponenti u slučaju kvara Firmware & Update - Redovno ažuriranje softvera, antivirusnih definicija, sigurnosnih potpisa		
				2	Sistem za kontrolu , filtriranje, zaštitu i enkripciju elektronske pošte sa 3 godine preimum-Pro podrškom i 3 godišnjom licencom antispam i antivirus servisa —dodatnih, “enterprise-level” sigurnosnih i zaštitnih funkcionalnosti ili ekvivalentno modelu : FortiMail 400F SKU:FML-400F-BDL-641-36	1. System / Deployment Hardware Specifications 10/100/1000 Interfaces (Copper, RJ45) : 4 Storage : 2× 1 TB RAID Storage Management: Hardware 0, 1, 5, 10, Hot Spare Memory: 8 GB Form Factor: Rack Mount, 1U System Specifications Protected Email Domains: Min. 70 Recipient-Based Policies (per Domain / per System): 400 / 1500 Server Mode local mailboxes: Min. 400 Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System): 50 / 200 Email Routing (per hour): 250 K	1.00	Komada

Antispam + Virus Outbreak (per hour): 200 K
Email Routing (per hour): 83 K
Antispam + Virus Outbreak (per hour): 72 K
Power Source: 100–240 V AC, 50–60 Hz
Power Supply: Dual - redudant
Certification: VBSpam and VB100; NIST CMVP test (FIPS140 3).

• Deployment i operativnie opcije
o On-premise
o Transparent i server mode
• Inbound i outbound inspekcija emaila
• SMTP autentikacija (LDAP, RADIUS, POP3, IMAP)
• LDAP-based email routing
• Inspekcija po korisniku na osnovu LDAP atributa (po domen politici)
• Geografski IP-based policy
• Webmail interfejs za server mode i karantin
• Mail queue management
• Podrška za više jezika
• SMTP RFC kompatibilnost
• Modern HTML5 GUI
• Kompatibilnost sa cloud servisima: Microsoft 365, Google Workspace, AWS, Azure
• DNS-based Authentication of Named Entities

(DANE) podrška (ako proizvođač podržava)
2. Antispam
• Antispam servis
o Sender i domain reputation
o Spam i attachment signatures
o Heuristička i ponašajna analiza
o Outbreak protection
• URL category filtering: spam, malware, phishing, pornografski/adult sadržaj, newly registered domains
• Greylisting za IPv4, IPv6 i email accounts
• Lokalna reputacija pošiljalaca
• Integracija sa trećim spam URIs i RBL/SURBL listama
• Newsletter/greymail detekcija
• PDF i Office dokument skeniranje i analiza
• Blok/safe liste na globalnom, domen i korisničkom nivou
• Podrška za SPF, DKIM, DMARC
• Fleksibilne akcije i notifikacije
• Sistemski i per-user self-service karantin
3. Targeted Attack Protection
• Content disarm i reconstruction: neutralizacija makroa i aktivnog sadržaja u Office/PDF dokumentima
• Neutralizacija hyperlinkova u email HTML sadržaju (ako podržava proizvođač)
• Business Email Compromise (BEC) zaštita

o Anti-spoof protection
o Impersonation i cousin domain detection
• URL click protection (preusmeravanje/skeniranje linkova)
• Integracija sa browser isolation platformom ili sličnom funkcionalnošću (ako podržava proizvođač)
4. API Integration
• Microsoft 365 i Google Workspace integracija
o Post-delivery threat scanning (ako podržava)
o Scheduled i real-time scanning
o Internal mail scanning
5. Content Detection
• Antivirus / malware detection (heuristika, signature-based, greyware)
• Virus outbreak protection (global threat intelligence, ako proizvođač podržava)
• Aktivni sadržaj (PDF & Office dokumenti)
• Rescan poruka na karantinu
• Custom file hash i MIME/type detekcija
• DLP / Data-loss prevention (osnovna detekcija fajlova, PII, finansijski podaci, osetljivi sadržaji)
• Decryption za arhive, PDF i Office dokumente sa poznatim password listama (ako podržava proizvođač)
• PDF / Office skeniranje i analiza slika
• Dynamic image

analysis (prepoznavanje nedozvoljenog sadržaja, ako podržava proizvođač)
6. Encryption
• TLS server-to-server sa opcijama za ciphersuite
• S/MIME
• Clientless email enkripcija (portal-based ili built-in funkcionalnost)
• Outlook plugin ili dodatak za enkripciju (ako podržava proizvođač)
7. Management, Logging, Reporting
• Per-domain i role-based administracija
• Aktivnost i promena konfiguracija logging
• Built-in reporting i detaljno praćenje poruka
• Centralizovani karantin za velike deployment-e
• Centralizovano logovanje (ako podržava proizvođač)
• SNMP, eksterni syslog
• Open REST API za konfiguraciju i management
• Lokalni ili eksterni storage serveri (uključujući iSCSI)
8. High Availability (HA)
• Active-Passive i Active-Active konfiguracije
• Sinhronizacija karantina i mail queue
• Failover i redundantne interfejse
9. Advanced / Email Server funkcionalnosti
• Policy-based email

					archiving (uključujući Exchange journal, ako podržava) • POP3/IMAP pristup, webmail interfejs • Osnovne kalendarske funkcije i undo send • SAML 2.0 SSO i ADFS integracija (webmail/karantin) 10. Support • Profesionalna tehnička podrška; trajanje podrške 3 godine • Uključena RMA podrška • Licenca za Antispam i antivirus servise —dodatne, “enterprise-level” sigurnosne i zaštitne funkcionalnosti; trajanje licence 3 godine.		

Izvještaj generisan 03.12.2025 10:40