Izmjena postupka

OSNOVNI PODACI

Opis predmeta javne nabavke:

Nabavka kompjuterske opreme

Vrsta predmeta:

Robe

Vrsta postupka:

Otvoreni postupak

PODACI O NARUČIOCU

Naziv:

PORESKA UPRAVA

PIB:

11069169

Uslovi prije izmjena

Opis	Tip uslova	Važi za sve partije
U postupku javne nabavke može da učestvuje samo privredni subjekat koji 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. Ispunjenost navedenog uslova dokazuje se 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. Ispunjenost navedenog uslova dokazuje se na osnovu uvjerenja ili potvrde organa uprave nadležnog za poslove naplate poreza, odnosno nadležnog organa države u kojoj privredni subjekat ima sjedište.	Obavezni uslovi	Da
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je upisan u Centralni registar privrednih subjekata ili drugi odgovarajući registar u državi u kojoj privredni subjekat ima sjedište što se dokazuje dostavljanjem dokaza o registraciji u Centralnom registru privrednih subjekata ili drugom odgovarajućem registru, sa podacima o ovlašćenom licu privrednog subjekta	Uslovi za obavljanje djelatnosti	Da

Izjava privrednog subjekta dostaviti u skladu sa Pravilnikom o obrascu izjave privrednog subjekta ("Službeni list Crne Gore, broj 114/24" od 29.11.2024.) i Zakonom o javnim nabavkama (Sl. list CG br. 74/19 od 30.12.2019. godine, 03/23 od 10.01.2023. godine, 11/23 od 27.01.2023. godine i 84/24 od 06.09.2024. godine). Izjavu privrednog subjekta potpisuje ovlašćeno lice privrednog subjekta elektronskim potpisom. U obrascu 1 izjave privrednog subjekta koji je sastavni dio Pravilnika o obrascu izjave privrednog subjekta nalazi se uputstvo za popunjavanje izjave i izjavu privrednog subjekta treba popuniti u skladu sa uputstvom za popunjavanje izjave.	ESPD	Da
Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2 % procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i osam dana nakon isteka važenja ponude. Ako ponuđač ne može da garanciju ponude podnese u elektronskom obliku, dužan je da putem ESJN dostavi kopiju garancije ponude, a da original garancije ponude dostavi, odnosno uruči naručiocu neposredno ili putem pošte preporučenom pošiljkom najkasnije prije isteka roka za podnošenje ponuda. Original garancije ponude u pisanom obliku dostavlja se u koverti, na kojoj se navodi: naziv i sjedište naručioca, broj tenderske dokumentacije za koju se podnosi garancija, naziv, sjedište i adresa ponuđača i naznake "garancija ponude" i "ne otvaraj prije roka za otvaranje ponuda".	Garancija ponude	Da
Rok važenja ponude je 60 dana od dana otvaranja ponuda.	Rok važenja ponude	Da
Rok plaćanja: 30 dana od dana ispostavljanja fakture	Rok plaćanja	Da
Način plaćanja: Virmanski	Način plaćanja	Da
Rok izvršenja ugovora: Period izvršenja ugovora je maksimum 90 kalendarskih dana od dana zaključenja ugovora. Najkraće ponuđeni rok za izvršenje ugovora je 15 kalendarskih dana.	Rok izvršenja ugovora	Da
Mjesto izvršenje ugovora: Podgorica	Mjesto izvršenja ugovora	Da

PARTIJA 2: Za STAVKU 1 minimum 3 godine garancije, potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku. Za STAVKU 2 minimum 3 godine garancije, potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku. Za STAVKU 3 Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak). Za STAVKU 4 Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak). Za STAVKU 5 Garancija: minimum 24 mjeseca (potrebno je dostaviti potvrdu proizvođača ili kancelarije proizvođača o trajanju garantnog roka).	Garantni rok	Ne
Ponuđač je duzan da dostavi pisano ovlašćenje (autorizacija) proizvođača ili distributera (zastupnika) proizvođača čiju opremu nudi, u kojem je navedeno da je ponuđač ovlašćen da nudi opremu u predmetnom postupku javne nabavke. U slučaju dostavljanja ovlašćenja od distributera (zastupnika) neophodno je dostaviti i dokaz od proizvođača da je on ovlašćeni zastupnik za konkretan postupak.	Drugi uslovi	Ne
U skladu sa članom 110 Zakona o javnim nabavkama Naručilac će isključiti privrednog subjekta iz postupka javne nabavke, koji u periodu od tri prethodne godine do isteka roka za podnošenje prijava, odnosno ponuda ima sa tim ili drugim naručiocem raskinut ugovor o javnoj nabavci, ugovor o javno-privatnom partnerstvu ili ugovor o koncesiji ili kojem je aktivirano sredstvo finansijskog obezbjeđenja ugovora, naplaćena šteta ili druga sankcija u skladu sa zakonom, zbog značajnih i trajnih nedostataka tokom sprovođenja ključnih zahtjeva iz prethodnog ugovora o javnoj nabavci, ugovora o javno-privatnom partnerstvu ili ugovora o koncesiji;	Posebni osnovi za isključenje iz postupka javne nabavke	Ne
Za PARTIJU 1: Za STAVKU 1 1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu. Za STAVKU 2 1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu.	Garantni rok	Ne

Ispunjenost uslova stručne i tehničke sposobnosti dokazuje se na osnovu dokaza o stručnim i kadrovskim kapacitetima angažovane radne snage dokazom o angažovanju minimum 2 (dva) stručna lica sa završenim fakultetom tehničkih ili prirodnih nauka (elektronika, energetika, telekomunikacije, informacione tehnologije ili računarstvo) minimum VII stepen (240 ECTS kredita) što se dokazuje dokazima o stručnoj spremi sertifikovanih stručnih lica (diploma, uvjerenje, svjedočanstvo ili drugi odgovarajući akt nadležnog organa ili organizacije), koja imaju odgovarajuće sertifikate koji su potrebni za izvršenje predmeta nabavke u skladu sa zakonom - mrežne opreme Firewall što se dokazuje dokazom o angažovanju sertifikovanih tehničkih lica sa odgovarajućim sertifikatima koji su potrebni za izvršenje predmeta nabavke u skladu sa zakonom - mrežne opreme Firewall i način angažovanja radne snage za navedena sertifikovana tehnička lica (prijava na osiguranje zaposlenog ili ugovor o radu ili sporazum o preuzimanju zaposlenog ili ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom). Komisija će prilikom provjere izjave privrednog subjekta zatražiti navedene dokaze.	Stručna i tehnička sposobnost	Ne
• Ponuđač je u svojoj ponudi dužan da dostavi Dokaz izdat od strane proizvođača, ovlašćenog distributera, zastupnika ili predstavnika proizvođača hardvera i softwera da je Ponuđač ovlašćeni partner za prodaju , implementaciju i održavanje na teritoriji Crne Gore. U slučaju dostavljanja ovlašćenja od distributera (zastupnika) neophodno je dostaviti i dokaz od proizvođača da je on ovlašćeni zastupnik za konkretnu nabavku.	Drugi uslovi	Ne

Uslovi nakon izmjena

Opis	Tip uslova	Važi za sve partije
U postupku javne nabavke može da učestvuje samo privredni subjekat koji 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. Ispunjenost navedenog uslova dokazuje se 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. Ispunjenost navedenog uslova dokazuje se na osnovu uvjerenja ili potvrde organa uprave nadležnog za poslove naplate poreza, odnosno nadležnog organa države u kojoj privredni subjekat ima sjedište.	Obavezni uslovi	Da
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je upisan u Centralni registar privrednih subjekata ili drugi odgovarajući registar u državi u kojoj privredni subjekat ima sjedište što se dokazuje dostavljanjem dokaza o registraciji u Centralnom registru privrednih subjekata ili drugom odgovarajućem registru, sa podacima o ovlašćenom licu privrednog subjekta	Uslovi za obavljanje djelatnosti	Da

Izjava privrednog subjekta dostaviti u skladu sa Pravilnikom o obrascu izjave privrednog subjekta ("Službeni list Crne Gore, broj 114/24" od 29.11.2024.) i Zakonom o javnim nabavkama (Sl. list CG br. 74/19 od 30.12.2019. godine, 03/23 od 10.01.2023. godine, 11/23 od 27.01.2023. godine i 84/24 od 06.09.2024. godine). Izjavu privrednog subjekta potpisuje ovlašćeno lice privrednog subjekta elektronskim potpisom. U obrascu 1 izjave privrednog subjekta koji je sastavni dio Pravilnika o obrascu izjave privrednog subjekta nalazi se uputstvo za popunjavanje izjave i izjavu privrednog subjekta treba popuniti u skladu sa uputstvom za popunjavanje izjave.	ESPD	Da
Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2 % procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i osam dana nakon isteka važenja ponude. Ako ponuđač ne može da garanciju ponude podnese u elektronskom obliku, dužan je da putem ESJN dostavi kopiju garancije ponude, a da original garancije ponude dostavi, odnosno uruči naručiocu neposredno ili putem pošte preporučenom pošiljkom najkasnije prije isteka roka za podnošenje ponuda. Original garancije ponude u pisanom obliku dostavlja se u koverti, na kojoj se navodi: naziv i sjedište naručioca, broj tenderske dokumentacije za koju se podnosi garancija, naziv, sjedište i adresa ponuđača i naznake "garancija ponude" i "ne otvaraj prije roka za otvaranje ponuda".	Garancija ponude	Da
Rok važenja ponude je 60 dana od dana otvaranja ponuda.	Rok važenja ponude	Da
Rok plaćanja: 30 dana od dana ispostavljanja fakture	Rok plaćanja	Da
Način plaćanja: Virmanski	Način plaćanja	Da
Mjesto izvršenje ugovora: Podgorica	Mjesto izvršenja ugovora	Da

PARTIJA 2: Za STAVKU 1 minimum 3 godine garancije, potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku. Za STAVKU 2 minimum 3 godine garancije, potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku. Za STAVKU 3 Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak). Za STAVKU 4 Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak). Za STAVKU 5 Garancija: minimum 24 mjeseca (potrebno je dostaviti potvrdu proizvođača ili kancelarije proizvođača o trajanju garantnog roka).	Garantni rok	Ne
Ponuđač je duzan da dostavi pisano ovlašćenje (autorizacija) proizvođača ili distributera (zastupnika) proizvođača čiju opremu nudi, u kojem je navedeno da je ponuđač ovlašćen da nudi opremu u predmetnom postupku javne nabavke. U slučaju dostavljanja ovlašćenja od distributera (zastupnika) neophodno je dostaviti i dokaz od proizvođača da je on ovlašćeni zastupnik za konkretan postupak.	Drugi uslovi	Ne
U skladu sa članom 110 Zakona o javnim nabavkama Naručilac će isključiti privrednog subjekta iz postupka javne nabavke, koji u periodu od tri prethodne godine do isteka roka za podnošenje prijava, odnosno ponuda ima sa tim ili drugim naručiocem raskinut ugovor o javnoj nabavci, ugovor o javno-privatnom partnerstvu ili ugovor o koncesiji ili kojem je aktivirano sredstvo finansijskog obezbjeđenja ugovora, naplaćena šteta ili druga sankcija u skladu sa zakonom, zbog značajnih i trajnih nedostataka tokom sprovođenja ključnih zahtjeva iz prethodnog ugovora o javnoj nabavci, ugovora o javno-privatnom partnerstvu ili ugovora o koncesiji;	Posebni osnovi za isključenje iz postupka javne nabavke	Ne
Za PARTIJU 1: Za STAVKU 1 1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu. Za STAVKU 2 1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu.	Garantni rok	Ne

Ispunjenost uslova stručne i tehničke sposobnosti dokazuje se na osnovu dokaza o stručnim i kadrovskim kapacitetima angažovane radne snage dokazom o angažovanju minimum 1 (jednog) stručnog lica sa završenim fakultetom tehničkih ili prirodnih nauka (elektronika, energetika, telekomunikacije, informacione tehnologije ili računarstvo) minimum VI stepen (180 ECTS kredita) što se dokazuje dokazima o stručnoj spremi stručnog lica (diploma, uvjerenje, svjedočanstvo ili drugi odgovarajući akt nadležnog organa ili organizacije), koje ima odgovarajuće sertifikate koji su potrebni za izvršenje predmeta nabavke u skladu sa zakonom - mrežne opreme Firewall što se dokazuje dokazom o angažovanju sertifikovanog tehničkog lica sa odgovarajućim sertifikatima koji su potrebni za izvršenje predmeta nabavke u skladu sa zakonom - mrežne opreme Firewall i načinom angažovanja radne snage za navedeno sertifikovano tehničko lice što se dokazuje sa: (prijava na osiguranje zaposlenog ili ugovor o radu ili sporazum o preuzimanju zaposlenog ili ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom). Komisija će prilikom provjere izjave privrednog subjekta zatražiti navedene dokaze.	Stručna i tehnička sposobnost	Ne
• Ponuđač je u svojoj ponudi dužan da dostavi Dokaz izdat od strane proizvođača, ovlašćenog distributera, zastupnika ili predstavnika proizvođača hardvera i softwera da je Ponuđač ovlašćeni partner za prodaju , implementaciju i odražavanje na teritoriji Crne Gore. U slučaju dostavljanja ovlašćenja od distributera (zastupnika) neophodno je dostaviti i dokaz od proizvođača da je on ovlašćeni zastupnik za konkretnu nabavku.	Drugi uslovi	Ne

Kriterijumi prije izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja	Važi za sve partije
Cijena	-	-	Da
Period izvršenja ugovora je maksimum 90 kalendarskih dana od dana zaključenja ugovora. Najkraće ponuđeni rok za izvršenje ugovora je 15 kalendarskih dana.	Eksplicitna numerička vrijednost	Relativno	Da

Kriterijumi nakon izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja	Važi za sve partije
Cijena	-	-	Da
Period izvršenja ugovora je maksimum 90 kalendarskih dana od dana zaključenja ugovora. Najkraće ponuđeni rok za izvršenje ugovora je 15 kalendarskih dana.	Eksplicitna numerička vrijednost	Relativno	Da

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, isporuka, implementacija i konfiguracija firewall rješenja sa migracijom sa postojećeg firewall/a i pružanje stručnih konsultanskih usluga	41322.31	1	Mrežni sigurnosni uređaj (Firewall) Tip1 Primarna lokacija	• Broj Gigabit Ethernet RJ45 LAN portova: minimum 8; • Broj Gigabit Ethernet RJ45 MGMT (Management) portova: minimum 1; • Broj Gigabit Ethernet RJ45 HA (High Availability) portova: minimum 1; • Broj 5/2.5/GE RJ45 LAN portova: minimum 8; • Broj Ten Gigabit Ethernet SFP+ slotova: minimum 8; • Broj Gigabit Ethernet SFP slotova: minimum 4; • Broj USB portova: minimum 1; • Broj konzolnih portova: minimum 1; • Uređaj mora biti veličine maksimalno 1RU i opremljen za montažu u standardni 19-inčni rek orman • Mora posjedovati redundantna napajanja sa podržanim naizmjeničnim naponom u opsegu od	2.00	komada

						100V do 240V • Uređaj mora imati minium 39 Gbps firewall protok; • Uređaj mora imati minimum 9 Gbps IPS propusnost; • Uređaj mora imati protok za funkcionalnosti Firewall, IPS i kontrola aplikacija od minimum 7 Gbps; • Uređaj mora imati protok SSL inspekcije od minimumu 7 Gbps • Uređaj mora imati IPsec VPN protok od minimum 36 Gbps • Uređaj mora podržavati minimum 11 miliona konkurentnih konekcija • Uređaj mora podržavati minimum 400k novih konekcija u sekundi • Uređaj mora podržavati minimum 499 istovremenih SSL VPN korisnika (ukoliko su potrebne licence, iste moraju biti uključene za navedeni kapacitet) • Uređaj mora imati mogućnost segregacije uređaja na najmanje 10 virtualnih uređaja, koji imaju zaseban menadžment, portove, polise • Broj Firewall polisa: minimum 10k; • Uređaj mora podržavati IPV6 • Konfiguracije visoke raspoloživosti: Active/Active, Active/Passive, Clustering; • Uređaj mora podržavati kreiranje		

					firewall pravila po username-u i grupi korisnika • Uređaj mora podržavati kontrolu saobraćaja po aplikaciji • Uređaj mora podržavati ograničenje bandwidth-a po aplikaciji • Uređaj mora imati inegrisanu funkcionalnost usmjeravanja saobraćaja kroz različite mrežne interfejse, u zavisnosti od tipa aplikacije koja genereši saobraćaj (SD-WAN) • Uređaj mora podržavati automatski izbor najboljeg linka (između redundantnih IPsec VPN liknova) za pojedinačne aplikacije i servise, u zavisnosti od vrijednosti kašnjenja paketa ili broja izgubljenih paketa na linku • Uređaj mora podržavati L3 i transparentni način rada • Uređaj mora podržavati eksplicitni proxy način rada, • Uređaj mora podržavati slanje logova preko syslog-a • Uređaj mora podržavati Captive Portal funkcionalnost za autentifikaciju korisnika • Uređaj mora imati mogućnost provjere file-ova u cloud sandbox-u • Uređaj mora imati mogućnost detefkcije		

malware-a za mobilne uređaje
• Uređaj mora imati integrisan wireless controller ili uključivati zasebno rješenje
• Uređaj mora podržavati kontrolu minimum 128 access point-a
• Licence koje moraju biti uključene uz uređaja i to na 12 mjeseci:

Opis licence:
Napredna zaštita: Rješenje mora obezbjeđivati višeslojnu zaštitu saobraćaja kroz kombinaciju sistema za prevenciju upada (IPS), antivirusne i anti-malware zaštite, detekcije botnet i command-and-control (C2) komunikacije, kontrole zlonamjernih URL-ova, kao i naprednih mehanizama za identifikaciju sumnjivih i nepoznatih datoteka. Sistem mora podržavati sandbox analizu i dodatne mehanizme za otkrivanje sofisticiranih i zero-day prijetnji, uključujući zaštitu zasnovanu na globalnoj threat intelligence mreži proizvođača.
Kontrola i filtriranje: Rješenje mora omogućiti web filtriranje (URL filtering), DNS filtriranje i kontrolu aplikacija (Application Control).
Dodatna sigurnost:

						Uređaj mora podržavati anti-spam zaštitu i mehanizme za sprječavanje curenja podataka (Data Loss Prevention – DLP). Mrežne funkcionalnosti: Uređaj mora podržavati VPN konekcije (IPsec i SSL), imati integrisanu SD-WAN funkcionalnost i omogućavati implementaciju Zero Trust pristupa (ZTNA ili ekvivalent). Zaštita proširene mrežne površine: Rješenje treba da podržava detekciju i procjenu rizika uređaja povezanih na mrežu, uključujući IoT i druge neklasične krajnje tačke, uz mogućnost sigurnosnog rangiranja, identifikacije ranjivosti i dodatne korelacije sigurnosnih događaja. Tehnička podrška: Ponuđač mora obezbijediti 24/7 tehničku podršku proizvođača, pravo na softverske nadogradnje i sigurnosne zakrpe, zamjenu neispravnog uređaja u garantnom roku (RMA), kao i pristup online portalima za podršku i tehničku dokumentaciju. Sigurnosne pretplate: Rješenje mora uključivati aktivne sigurnosne servise koji obezbjeđuju kontinuirano ažuriranje		

					sigurnosnih baza i prijetnji, globalni threat intelligence u realnom vremenu, automatizovanu detekciju i odgovor na incidente, kao i centralizovano izvještavanje i analitiku. Period važenja: Sve licence i pretplate moraju važiti minimalno 12 mjeseci od dana aktivacije. Opšti tehnički zahtjevi: Uređaj mora biti nov i nekorišten, podržavati rad u produkcionim mrežama srednjih i većih organizacija, te imati odgovarajuće performanse za obradu mrežnog saobraćaja bez degradacije sigurnosnih funkcija. • 8 x 10 GE SFP+ transceiver module, short range 300m, LC connector • 2 x 10 GE SFP+ passive direct attach cable 1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu		
				2	Mrežni sigurnosni uređaj (Firewall) Tip2 DR lokacija	• Broj Gigabit Ethernet RJ45 LAN portova: minimum 8; • Broj Gigabit Ethernet RJ45 MGMT (Management) portova: minimum 1; • Broj Gigabit Ethernet	2.00	komada

						RJ45 HA (High Availability) portova: minimum 1; • Broj 5/2.5/GE RJ45 LAN portova: minimum 8; • Broj Ten Gigabit Ethernet SFP+ slotova: minimum 8; • Broj Gigabit Ethernet SFP slotova: minimum 4; • Broj USB portova: minimum 1; • Broj konzolnih portova: minimum 1; • Uređaj mora biti veličine maksimalno 1RU i opremljen za montažu u standardni 19-inčni rek orman • Mora posjedovati redundantna napajanja sa podržanim naizmjeničnim naponom u opsegu od 100V do 240V • Uređaj mora imati minium 39 Gbps firewall protok; • Uređaj mora imati minimum 9 Gbps IPS propusnost; • Uređaj mora imati protok za funkcionalnosti Firewall, IPS i kontrola aplikacija od minimum 7 Gbps; • Uređaj mora imati protok SSL inspekcije od minimumu 7 Gbps • Uređaj mora imati IPsec VPN protok od minimum 36 Gbps • Uređaj mora podržavati minimum 11 miliona konkurentnih konekcija • Uređaj mora podržavati minimum 400k novih konekcija u sekundi		

						• Uređaj mora podržavati minimum 499 istovremenih SSL VPN korisnika (ukoliko su potrebne licence, iste moraju biti uključene za navedeni kapacitet) • Uređaj mora imati mogućnost segregacije uređaja na najmanje 10 virtualnih uređaja, koji imaju zaseban menadžment, portove, polise • Broj Firewall polisa: minimum 10k; • Uređaj mora podržavati IPV6 • Konfiguracije visoke raspoloživosti: Active/Active, Active/Passive, Clustering; • Uređaj mora podržavati kreiranje firewall pravila po username-u i grupi korisnika • Uređaj mora podržavati kontrolu saobraćaja po aplikaciji • Uređaj mora podržavati ograničenje bandwidth-a po aplikaciji • Uređaj mora imati inegrisanu funkcionalnost usmjeravanja saobraćaja kroz različite mrežne interfejse, u zavisnosti od tipa aplikacije koja genereši saobraćaj (SD-WAN) • Uređaj mora podržavati automatski izbor najboljeg linka (između redundantnih IPsec VPN liknova) za pojedinačne aplikacije i		

						servise, u zavisnosti od vrijednosti kašnjenja paketa ili broja izgubljenih paketa na linku • Uređaj mora podržavati L3 i transparentni način rada • Uređaj mora podržavati eksplicitni proxy način rada, • Uređaj mora podržavati slanje logova preko syslog-a • Uređaj mora podržavati Captive Portal funkcionalnost za autentifikaciju korisnika • Uređaj mora imati mogućnost provjere file-ova u cloud sandbox-u • Uređaj mora imati mogućnost detefkcije malware-a za mobilne uređaje • Uređaj mora imati integrisan wireless controller ili uključivati zasebno rješenje • Uređaj mora podržavati kontrolu minimum 128 access point-a • Licence koje moraju biti uključene uz uređaja i to na 12 mjeseci: Opis licence: Predmet nabavke obuhvata aktivaciju licence za tehničku podršku proizvođača koja omogućava kontinuirano održavanje, nadogradnju i podršku za mrežni sigurnosni uređaj. Minimalni zahtjevi za		

tehničku podršku:
Dostupnost tehničke podrške 24 sata dnevno, 7 dana u sedmici (24/7)
Pristup zvaničnoj tehničkoj podršci proizvođača (putem web portala, e-maila i telefona)
Pravo na preuzimanje i instalaciju:
softverskih nadogradnji sigurnosnih zakrpa novih verzija firmware-a
Mogućnost otvaranja i praćenja tehničkih slučajeva (ticketing sistem)
Definisani vremenski okviri odziva u skladu sa nivoom prioriteta incidenta
Hardverska podrška:
Zamjena neispravnog uređaja u garantnom roku (RMA)
Napredna zamjena hardvera u najkraćem mogućem roku u slučaju kvara
Pristup logističkoj podršci proizvođača
Dodatne usluge:
Pristup tehničkoj dokumentaciji, bazama znanja i preporukama proizvođača
Mogućnost eskalacije problema prema višim nivoima tehničke podrške
Preporuke za optimizaciju i održavanje sistema
Period važenja:
Licenca mora važiti minimalno 12 mjeseci od dana aktivacije.
Opšti zahtjevi:
Licenca mora biti validna te mora biti u

						potpunosti kompatibilna sa ponuđenim mrežnim sigurnosnim uređajem. • 4 x 10 GE SFP+ transceiver module, short range 300m, LC connector • 2 x 10 GE SFP+ passive direct attach cable 1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu		
				3	Softversko rješenje za centralizovano logovanje, analitiku i izvještavanje za Centralni Firewall (stavka br. 1)	Rješenje koje omogućava čuvanje logova, analitiku i izvještavanje za firewall rješenje opisano u stavci 1, sa sljedećim minimalnim funkcionalnostima i zahtjevima: Rješenje mora omogućiti centralizovano prikupljanje, skladištenje, korelaciju i analizu sigurnosnih i sistemskih logova, kao i grafičko i automatizovano izvještavanje u svrhu sigurnosnog nadzora i revizijskih dokaza. Rješenje mora biti isporučeno kao virtuelni uređaj (VM) i mora podržavati proširenje kapaciteta kroz dodatne licence (sklabilni licencni model). Virtuelno rješenje mora biti podržano na najmanje jednoj od	1.00	komad

sljedećih platformi: VMware ESXi, Microsoft Hyper-V, KVM, Open Source Xen / Citrix XenServer, Nutanix AHV, Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI).
Napomena: Ponuđač mora u ponudi navesti izabranu platformu.
Rješenje mora biti licencirano za obradu minimalno 5 GB logova dnevno (GB/dan), uz mogućnost povećanja kapaciteta kupovinom dodatnih licenci (skalabilni model kapaciteta).
Rješenje mora podržavati centralizovano prikupljanje više tipova logova, uključujući najmanje:
Logove mrežnih aktivnosti / saobraćaja
Sistemske logove
Logove virusa / malvera
Logove napada / IPS događaja
Logove filtriranja web sadržaja
Logove e-mail sigurnosti (gdje je primjenjivo)
Rješenje mora omogućiti:
Prikupljanje logova u realnom vremenu
Pregled i pretragu historijskih logova
Rješenje mora omogućiti vizualizaciju logova, korelaciju događaja i analitiku za

						predmetno firewall rješenje. Rješenje mora podržavati agregaciju događaja i normalizaciju logova (prepoznavanje tipa događaja i konzistentan prikaz). Rješenje mora omogućiti filtriranje i pretragu najmanje po uređaju, vremenu i tipu događaja. Prikupljeni logovi moraju biti dostupni u čitljivom (normalizovanom) formatu, uz mogućnost pristupa sirovim (neobrađenim) logovima. Rješenje mora podržavati automatsko obogaćivanje podataka vizuelnim indikatorima (npr. aplikacija, geolokacija) radi lakše analize. Rješenje mora omogućiti korelaciju korisničkog identiteta sa aktivnostima/događajima (gdje je primjenjivo i gdje postoje izvori identiteta). Rješenje mora podržavati: Generisanje grafičkih izvještaja Automatizovano (planirano) izvještavanje Predefinisane šablone izvještaja sa detaljnim informacijama i grafičkim prikazima Izvoz izvještaja u PDF formatu Kreiranje prilagođenih izvještaja (baziranih na šablonima ili		

					skupovima podataka) Jednostavan mehanizam uvoza/izvoza izvještaja Rješenje mora obezbijediti konzolu za upravljanje događajima i detekciju abnormalnog ponašanja u intuitivnom i preglednom formatu. Sistem za alarme mora podržavati kompleksna pravila okidanja, kao što su: nivo ozbiljnosti, specifičan događaj, akcija, odredište ili pragovi (threshold uslovi). Alarmiranje mora biti dostupno najmanje putem: E-maila SNMP-a Syslog-a Rješenje mora podržavati enkriptovanu komunikaciju za prenos logova ka i od sigurnosnih uređaja (npr. TLS/HTTPS ili ekvivalent). Rješenje mora imati web-bazirano grafičko upravljačko sučelje dostupno putem HTTPS protokola, optimizovano za PC i tablet uređaje. Grafički interfejs mora obezbijediti sve funkcije potrebne za administraciju i SOC (Security Operations Center) operacije. Rješenje mora podržavati CLI (command-line interface) za konfiguraciju, monitoring i		

						troubleshooting. Administratorski nalozi moraju podržavati RBAC (role-based access control). Rješenje mora omogućiti razdvajanje na nezavisne administrativne domene (npr. po organizacionim jedinicama). Rješenje mora podržavati prosljeđivanje logova ka eksternim sistemima (npr. SIEM / syslog), gdje je potrebno. Rješenje mora podržavati rad kao: kompletan analitički engine i/ili kolektor u distribuiranom okruženju Rješenje mora obezbijediti jednostavnu i dokumentovanu API integraciju, uključujući podršku za JSON API i XML API, za integraciju sa sistemima trećih strana. Modul za procjenu sigurnosnog stanja (Security Posture Assessment Module) Rješenje mora uključivati servis/modul za kontinuiranu procjenu sigurnosnog stanja i napadne površine, zasnovan na stvarnoj konfiguraciji i ponašanju sistema, koji minimalno obuhvata: Automatsku procjenu napadne površine analizom konfiguracija,		

					politika i detektovanih događaja Dodjelu sigurnosnog rejtinga/ocjene koji kvantifikuje trenutno sigurnosno stanje Identifikaciju slabosti, rizičnih konfiguracija i odstupanja od sigurnosnih najboljih praksi Procjenu usklađenosti sa relevantnim sigurnosnim okvirima i standardima (npr. interne politike, industrijski standardi) Preporuke za unapređenje sigurnosnog stanja na osnovu realnih operativnih podataka Praćenje trenda sigurnosne ocjene kroz vrijeme radi mjerenja efikasnosti implementiranih mjera Modul mora biti integrisan u upravljačko okruženje i podržavati grafičko i PDF izvještavanje Licence i podrška Nabavka uključuje licencu za minimalno 5 GB logova dnevno za period od najmanje pet (1) godina. Licenca mora uključivati sve gore navedene funkcionalnosti. Ponuđač mora obezbijediti: tehničku podršku minimalnog nivoa 8x5 (ili bolje) pravo na nadogradnje (firmware/operativni sistem) i sigurnosne zakrpe u trajanju od najmanje jedne godine		
					LICENCE ZA	1.00	komad	

				4	LICENCE ZA DVOFAKTORSKU AUTENTIKACIJU (2FA) Primarna lokacija	DVOFAKTORSKU AUTENTIKACIJU (2FA) za Mrežni sigurnosni uređaj (Firewall) Tip1 Nabavka softverskih licenci za generisanje jednokratnih lozinki (OTP – One-Time Password) za potrebe dvofaktorske autentikacije korisnika. Opis licence: Predmet nabavke obuhvata isporuku softverskih autentikacionih tokena koji omogućavaju generisanje jednokratnih lozinki putem mobilnih uređaja, u cilju povećanja sigurnosti pristupa informacionim sistemima. Licence moraju biti kompatibilne sa mobilnim operativnim sistemima, uključujući najmanje: iOS, Android ,druge ekvivalentne mobilne platforme Obim i tip licence: Ukupan broj licenci: 100 korisničkih licenci (tokena) Tip licence: trajna (perpetual) Način isporuke: elektronski licencni certifikat Funkcionalni zahtjevi: Rješenje mora omogućiti: Generisanje vremenski ograničenih jednokratnih lozinki (OTP) Implementaciju dvofaktorske autentikacije (2FA)		

Integraciju sa sistemima za udaljeni pristup (VPN, web aplikacije i sl.)
Sigurnu aktivaciju tokena putem jedinstvenog aktivacionog koda ili QR koda
Korišćenje jednog tokena po korisničkom nalogu
Ograničenja licence:
Svaka licenca (token) je vezana za jedan korisnički uređaj
Prenos licence između uređaja nije dozvoljen
U slučaju promjene ili gubitka uređaja, potrebno je izvršiti deaktivaciju postojećeg i izdavanje novog tokena od strane administratora
Administracija i upravljanje:
Rješenje mora omogućiti centralizovano upravljanje, uključujući:
Dodjelu i aktivaciju tokena korisnicima
Deaktivaciju i brisanje tokena
Ponovnu dodjelu tokena u slučaju potrebe
Evidenciju i praćenje autentikacionih aktivnosti
Namjena:
Licence su namijenjene za implementaciju dodatnog sigurnosnog sloja pri autentikaciji korisnika i zaštitu pristupa informacionim resursima od neovlaštenog pristupa.

SET OD 100kom

				5	Implementacija	Opis usluga migracije i implementacije firewall infrastrukture Predmet ove nabavke obuhvata pružanje sveobuhvatnih konsultantskih, projektnih i implementacionih usluga u cilju migracije postojećeg firewall okruženja na novo, savremeno firewall rješenje zasnovano na visoko dostupnoj (HA – High Availability) klaster arhitekturi, uz unapređenje bezbjednosnih funkcionalnosti i optimizaciju postojećih sigurnosnih politika. Postojeće okruženje na primarnoj lokaciji sastoji se od dva FortiGate 500E uređaja u HA konfiguraciji, kao i dva Cisco ASA uređaja takođe implementirana u režimu visoke dostupnosti. Na rezervnoj (DR) lokaciji implementiran je jedan FortiGate 500E uređaj koji obezbjeđuje osnovne sigurnosne funkcionalnosti u slučaju prekida rada primarne lokacije. Cilj projekta je uspostavljanje novog firewall sistema na obje lokacije, pri čemu će na primarnoj lokaciji novo rješenje biti implementirano u klaster (HA) konfiguraciji sa logičkom podjelom na dvije odvojene virtuelne firewall	1.00	komad

instance. Jedna virtuelna instanca biće namijenjena migraciji i preuzimanju funkcionalnosti postojećeg FortiGate okruženja, dok će druga instanca biti predviđena za migraciju funkcionalnosti Cisco ASA sistema. Ove dvije logičke cjeline moraju biti međusobno izolovane u smislu sigurnosnih politika, upravljanja i obrade saobraćaja, uz istovremeno omogućavanje centralizovanog nadzora i upravljanja. Na DR lokaciji planirana je implementacija novog firewall rješenja u HA konfiguraciji, uz migraciju postojećeg FortiGate sistema, bez potrebe za dodatnom virtuelizacijom ili logičkom segmentacijom, imajući u vidu ulogu ove lokacije kao rezervnog sistema. Ponuđač je dužan da izvrši detaljnu analizu postojećeg stanja, uključujući sve relevantne konfiguracione elemente kao što su sigurnosne politike, NAT pravila, VPN konfiguracije, mrežna segmentacija, routing i svi zavisni servisi. Na osnovu sprovedene analize, izabrani ponuđač je obavezan da izradi detaljan dizajn ciljne arhitekture

						i plan migracije koji će osigurati minimalan uticaj na produkciono okruženje i kontinuitet poslovanja. Migracija konfiguracije mora obuhvatiti prenos i prilagođavanje svih relevantnih sigurnosnih pravila, NAT politika, VPN konekcija i mrežnih parametara sa postojećih sistema na novo rješenje. Poseban zahtjev odnosi se na transformaciju postojećeg SSL VPN pristupa u IPsec VPN rješenje, uz obaveznu implementaciju dvofaktorske autentikacije (2FA). Nova VPN arhitektura mora biti usklađena sa savremenim bezbjednosnim standardima i, gdje je primjenjivo, integrisana sa postojećim sistemima za upravljanje identitetima (npr. Active Directory, LDAP ili RADIUS). U okviru implementacije, ponuđač je obavezan da izvrši instalaciju i konfiguraciju firewall klastera na obje lokacije, uključujući uspostavljanje visoke dostupnosti, konfiguraciju virtuelnih firewall instanci na primarnoj lokaciji, kao i integraciju sa postojećim infrastrukturnim sistemima kao što su sistemi za autentikaciju, DNS, sistemi za nadzor i		

upravljanje bezbjednošću. Posebna pažnja mora biti posvećena testiranju i validaciji implementiranog rješenja. Ovo uključuje funkcionalno testiranje svih servisa (javno i interno) dostupnih kritičnih za funkcionisanje Poreske uprave, provjeru sigurnosnih politika, validaciju VPN konekcija (uključujući IPsec i 2FA), kao i testiranje scenarija otkaza i preuzimanja (failover) u okviru HA konfiguracije. Ponuđač je takođe obavezan da obezbijedi kontinuiranu konsultantsku podršku tokom svih faza projekta, uključujući planiranje, implementaciju i završnu fazu migracije (cutover), kao i podršku u periodu stabilizacije sistema nakon migracije. Važno je naglasiti da se za migraciju Cisco ASA firewall sistema zahtijevaju isključivo konsultantske usluge. To podrazumijeva da ponuđač nije odgovoran za direktnu implementaciju konfiguracije, već za izradu preporuka, validaciju pristupa, asistenciju tokom migracije i verifikaciju konačne konfiguracije. Svi radovi moraju biti planirani i izvedeni na način koji minimizuje prekid rada

produkcionog sistema. Maksimalno dozvoljeno vrijeme prekida rada tokom migracije produkcionog firewall sistema ne smije biti duže od dva (2) sata, te ponuđač mora predvidjeti odgovarajuće mehanizme i procedure kako bi se ovaj zahtjev ispunio. Po završetku projekta, ponuđač je dužan da isporuči kompletnu tehničku dokumentaciju, uključujući opis postojeće i nove arhitekture (as-is i to-be stanje), mapiranje konfiguracija, finalne konfiguracione postavke, kao i preporuke za dalje unapređenje i održavanje sistema.

U okviru predmetne nabavke, ponuđač je dužan da izvrši implementaciju i konfiguraciju sistema za centralizovano logovanje, analitiku i izvještavanje, u skladu sa definisanim tehničkim zahtjevima. Implementacija mora obuhvatiti inicijalnu instalaciju sistema u predviđenom okruženju, njegovu integraciju sa svim relevantnim firewall instancama (uključujući virtuelne firewall-e na primarnoj lokaciji i firewall sistem na DR lokaciji), kao i uspostavljanje centralizovanog

						prikupljanja i skladištenja logova. Ponuđač je obavezan da izvrši konfiguraciju logovanja za sve relevantne tipove događaja, uključujući sigurnosne, sistemske i mrežne logove, kao i da obezbijedi njihovu normalizaciju, korelaciju i dostupnost za dalju analizu. Takođe, potrebno je konfigurisati mehanizme za pretragu i filtriranje logova, kao i kreiranje prilagođenih i predefinisanih izvještaja, uključujući automatizovano generisanje i distribuciju izvještaja u skladu sa zahtjevima naručioca. Rješenje mora biti integrisano sa postojećim sigurnosnim i infrastrukturnim sistemima gdje je primjenjivo, te mora omogućiti jednostavno upravljanje, vizualizaciju događaja i efikasno otkrivanje sigurnosnih incidenata. Ponuđač je dužan da izvrši inicijalno podešavanje sistema za alarmiranje, uključujući definisanje pravila i notifikacija za kritične događaje. Nakon implementacije, ponuđač mora izvršiti testiranje funkcionalnosti sistema, validaciju prikupljanja i obrade logova, kao i obuku relevantnog osoblja		

					naručioca za korišćenje i administraciju sistema. Takođe, obavezno je dostavljanje odgovarajuće tehničke dokumentacije koja obuhvata konfiguraciju sistema, opis integracije i preporuke za dalje korišćenje i optimizaciju.		
2	Nabavka računara i ostale ICT opreme	99173.54	1	All in one	Procesor minimum 10 jezgara (6 P-jezgara + 4 E-jezgara), 16 niti, bazna frekvencija P-jezgra 2.5GHz / Ejezgra 1.8GHz, maksimalna frekvencija P-core 5.2GHz / Ecore 4.0GHz, 24 MB cache Memorija minimum 16GB DDR5, 2 memorijska slota SSD minimum 512 GB SSD M.2 2280 PCIe Gen4 Operativni sistem Windows 11 Professional ili ekvivalentno (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o fabricki preinstaliranom operativnom sistemu) Displej 27" FHD (1920 x 1080), IPS, Anti-Glare, 300 nita, 100Hz, maksimalni ugao gledanja 89 stepeni, kontrast minimum 1300:1 Kamera minimum 5MP sa mehanickim zatvaracem kamere radi privatnosti Integrisani zvucnici minimum 2 x 3W Tastatura sa YU setom karaktera i mis istog	53.00	komada

proizvodjaca kao i racunar
Postolje podrzava tilt podesavanje od -5° do +15°
Integrisani portovi pozadi minimum 1x USB-A 10Gbps, 2x USB-A , 1x HDMI-in 1.4, 1x HDMI-out 2.1, 1x Ethernet (RJ-45), sa strane: 1x headphone / microphone combo jack (3.5mm) , 1x USB-C 10Gbps - data transfer i 15W punjenje
Sigurnost minimum Pokretanje bez tastature i miša, Kontrola sekvence pokretanja, BIOS koji se sam oporavlja - hardverski integrisan mehanizam ugrađen u računarske sisteme koji omogućava automatski oporavak BIOS firmware-a iz hardverski zaštićene kopije (bez potrebe za pristupom mreži) u slučaju neuspjelog ažuriranja, oštećenja ili maliciozne izmjene. Bezbjednosni standard UEFI firmvera koji osigurava da se uređaj pokreće isključivo pomoću softvera kojem proizvođač originalne opreme vjeruje, sprečavajući učitavanje neovlašćenih operativnih sistema i malicioznog koda tokom procesa podizanja sistema.
Napajanje maksimum 90W
minimum 3 godine garancije, potrebno je

					dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku		
				2	Laptop tip 1	Procesor minimum up to 2.5 GHz LP E-core Max Turbo frequency, up to 4.2 GHz E-core Max Turbo frequency, up to 4.9 GHz P-core Max Turbo frequency,18 MB L3 cache, 4 P-cores, 2 LP E-cores and 8 E-cores,14 niti, 13 NPU TOPS Memorija minimum 16GB DDR5, minimum 2 memorijska slota SSD minimum 512GB M.2 Operativni sistem Windows 11 Professional ili ekvivalentno (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o fabricki preinstaliranom operativnom sistemu) Displej 16" diagonal, rezolucija minimum 1920 x 1200, IPS, anti-glare, 300 nita Tastatura sa YU setom karaktera i pozadinskim osvjetljenjem Kamera minimum 5MP IR kamera Integrisani portovi minimum 1 x HDMI 2.1; 1 x stereo headphone/microphone combo jack; 1 x RJ-45; 2x USB Type-A 5Gbps (powered); 2x USB Type-C 20Gbps (USB Power Delivery, DisplayPort, omogućeno punjenje	10.00	komada

						eksternih uređaja čak i kada je laptop u režimu spavanja ili potpuno isključen) Sigurnost minimum citac otiska prsta, Koristeći bezbjednosni kontroler (čip na matičnoj ploči), sistem treba da bude opremljen rješenjem, omogućavajući zaposlenima da brzo i bezbjedno oporave operativni sistem na najnoviju ispravnu verziju slike pomoću ugrađenog modula za skladištenje. Računari će podržavati modernu bezbjednosnu tehnologiju QR koda bez lozinki koje se koriste za kontrolu pristupa BIOS-u za daljinsko upravljanje i/ili lokalno upravljanje za osoblje za podršku na terenu. Baterija minimum 56Wh ,punjenje do 50% za 30 minuta Tezina maksimum 1.75 kg Torba istog proizvodjaca kao i laptop minimum 3 godine, potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku		
				3	MFP A4	Tehnologija štampe: laser Funkcije: štampanje, kopiranje, skeniranje, faks Brzina štampe A4: minimum 40 ppm u režimu velike brzine Dupleks štampa:	30.00	komada

					automatska , 31 ipm ili vise Mjesečni ciklus A4: minimum 100,000 strana Jezici štampe: PCL 6, PCL 5, PostScript level 3 emulation Povezivanje: 2 x USB 2.0 Host; 1 x USB 2.0 Device; 1x Gigabit Ethernet; 1 x Fax Procesor minimum 800 MHz Memorija minimum 2 GB Storage minimum 16 GB eMMC Control panel minimum 4.3” Color Touch Control Panel Ulaz papira: ulaz 1: 100 lista, ulaz 2: 250 lista, moguće dodavanje trećeg ulaza papira za 550 lista, ADF od minimum 50 lista. Izlaz papira: minimum 150 lista Skener: Flatbed i ADF (duplex skeniranje iz ADF) Brzina skeniranja: minimum crnobijelo: 29 ppm/46 ipm (jednostrano/duplex), kolor: 20 ppm/35 ipm (jednostrano/duplex) Sigurnost minimum funkcija koja provjerava integritet BIOS-a - ako detektuje napad ili oštećenje, sistem se samostalno oporavlja (self-healing) učitavanjem čiste kopije BIOS-a (Hardverski izolovana). Konstantno nadgledanje uređaja u realnom vremenu radi prepoznavanja pokušaja neovlašćenog pristupa		

						ili malicioznih aktivnosti. Napredna mrežna zaštita koja analizira odlazni saobraćaj i blokira sumnjive zahtjeve pre nego što uređaj bude kompromitovan. Onemogućavanje USB portova (USB port disablement): Opcija fizičkog ili softverskog blokiranja USB ulaza kako bi se spriječilo curenje podataka ili unošenje virusa putem eksternih diskova. Mogućnost korišćenja tonera kapaciteta minimum 10.000 kopija. Potrošni materijal mora biti jednodijelan. Uređaj ne smije posjedovati zaseban, odvojen drum unit kao poseban potrošni dio koji se mijenja nezavisno od kasete sa tonerom Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak)		
				4	Skeneri	ADF skener Standardne funkcije digitalnog slanja Skeniranje na računar; Skeniranje na USB disk; Skeniranje u e-poštu; Skeniranje u mrežnu mapu; Skeniranje u SharePoint; Skeniranje u prečicu; Skeniranje u oblak Radni ciklus (dnevni) Preporučeni dnevni	26.00	komada

radni ciklus: 7500 stranica
Brzina skeniranja ADF-a Do 75 str./min / 150 slika u minuti
Veličina skeniranja (ADF), maksimalna 216 x 3100 mm
Minimalna veličina skeniranja (ADF) 50,8 x 50,8 mm
Kapacitet ADF-a 80 listova
Dvostrano skeniranje ADF-a Da
Format datoteke skeniranja Za tekst i slike: PDF, PDF/A, šifrirani PDF, JPEG, PNG, BMP, TIFF, Word, Excel, PowerPoint, tekst (.txt), obogaćeni tekst (.rtf) i pretraživi PDF
Načini unosa skeniranja Dva načina skeniranja (jednostrano/dupleks) sa 10,9 cm (4,3 inča) ekranom u boji osjetljivim na dodir na prednjoj ploči ili preko aplikacije u Windows OS-u, u Mac OS-u i aplikacije trećih strana putem TWAIN, ISIS i WIA
Detekcija višestrukog uvlačenja papira Da
Postavke dpi izlazne rezolucije 75; 150; 200; 240; 300; 400; 500; 600; 1200 ppi
Izvor svjetlosti (skeniranje) LED
Napredne funkcije skenera Automatska ekspozicija, Automatski prag, Automatsko otkrivanje boje, Automatsko otkrivanje veličine, Ispravljanje sadržaja,

					Poboljšanje sadržaja, Automatsko uvlačenje papira, Senzor za detekciju višestrukog uvlačenja papira, Automatska orijentacija, Brisanje ivica, Brisanje prazne stranice, Spajanje stranica, Popunjavanje rupa, Digitalni pečati, Snimanje metapodataka, PDF dozvole, Odvajanje dokumenata (Prazna stranica, Barkod, Zonski barkod, Zonski OCR) Brzina procesora minimum 666 MHz Memorija minimum 1 GB Povezivost, standardna Ethernet 10/100/1000 Base-T, USB 3.0, Wi-Fi 802.11 b/g/n, Wi-Fi Direct Bežične mogućnosti Da,minimum Wi-Fi 802.11 b/g/n, Wi-Fi Direct Mrežni protokoli, podržani minimum ARP; ICMP; IGMP; UDP; TCP; DHCP; APIPA; DNS; mDNS; LLMNR; WSD; WS-Scan; SNTP; SMB; SNMP; FTP; SFTP; SMTP; HTTP serverski dio; HTTPS Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak)		
			5	Produzni kabl sa prenaponskom	Raspon ulaznog napona (Vac) 200 ~	15.00	komada

				zastitom	250 Dužina kabla za napajanje (m) 1.8 Prekidač za uključivanje/isključivanje Da Zaštita od preopterećenja Prekidač strujnog kruga Zaštita od preopterećenja strujom (A) 10 Tip utičnice Schuko x 8 USB priključak(i) za punjenje USB-A x 2 USB-A izlaz za punjenje 5 V / 2,4 A Zaštita od prenapona i filtriranje Suzbijanje prenapona (džuli) 1050 Maksimalni prenapon (V) 6000 Maksimalna udarna struja (A) 22500 Neutralni vodič prema uzemljenju (NG): 7500 Neutralni vod prema uzemljenju (NG): 1200 Vrijeme odziva (ns); < 1 LED indikatori Zaštićeno od prenapona, uzemljeno Otpornost kućišta na vatru Da Montaža na zid: Da Sigurnosni prekidač: Da Garancija: minimum 24 mjeseca (potrebno je dostaviti potvrdu proizvođača ili kancelarije proizvođača o trajanju garantnog roka)		

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, isporuka, implementacija i konfiguracija firewall rješenja sa migracijom sa postojećeg firewall/a i pružanje stručnih konsultanskih usluga	41322.31	1	Mrežni sigurnosni uređaj (Firewall) Tip1 Primarna lokacija	• Broj Gigabit Ethernet RJ45 LAN portova: minimum 8; • Broj Gigabit Ethernet RJ45 MGMT (Management) portova: minimum 1; • Broj Gigabit Ethernet RJ45 HA (High Availability) portova: minimum 1; • Broj 5/2.5/GE RJ45 LAN portova: minimum 8; • Broj Ten Gigabit Ethernet SFP+ slotova: minimum 8; • Broj Gigabit Ethernet SFP slotova: minimum 4; • Broj USB portova: minimum 1; • Broj konzolnih portova: minimum 1; • Uređaj mora biti veličine maksimalno 1RU i opremljen za montažu u standardni 19-inčni rek orman • Mora posjedovati redundantna napajanja sa podržanim naizmjeničnim naponom u opsegu od 100V do 240V • Uređaj mora imati minium 39 Gbps firewall protok; • Uređaj mora imati minimum 9 Gbps IPS propusnost; • Uređaj mora imati protok za funkcionalnosti Firewall, IPS i kontrola aplikacija od minimum	2.00	komada

						7 Gbps; • Uređaj mora imati protok SSL inspekcije od minimumu 7 Gbps • Uređaj mora imati IPsec VPN protok od minimum 36 Gbps • Uređaj mora podržavati minimum 11 miliona konkurentnih konekcija • Uređaj mora podržavati minimum 400k novih konekcija u sekundi • Uređaj mora podržavati minimum 499 istovremenih SSL VPN korisnika (ukoliko su potrebne licence, iste moraju biti uključene za navedeni kapacitet) • Uređaj mora imati mogućnost segregacije uređaja na najmanje 10 virtualnih uređaja, koji imaju zaseban menadžment, portove, polise • Broj Firewall polisa: minimum 10k; • Uređaj mora podržavati IPV6 • Konfiguracije visoke raspoloživosti: Active/Active, Active/Passive, Clustering; • Uređaj mora podržavati kreiranje firewall pravila po username-u i grupi korisnika • Uređaj mora podržavati kontrolu saobraćaja po aplikaciji • Uređaj mora podržavati ograničenje bandwidth-a po aplikaciji • Uređaj mora imati		

						inegrisanu funkcionalnost usmjeravanja saobraćaja kroz različite mrežne interfejse, u zavisnosti od tipa aplikacije koja genereši saobraćaj (SD-WAN) • Uređaj mora podržavati automatski izbor najboljeg linka (između redundantnih IPsec VPN liknova) za pojedinačne aplikacije i servise, u zavisnosti od vrijednosti kašnjenja paketa ili broja izgubljenih paketa na linku • Uređaj mora podržavati L3 i transparentni način rada • Uređaj mora podržavati eksplicitni proxy način rada, • Uređaj mora podržavati slanje logova preko syslog-a • Uređaj mora podržavati Captive Portal funkcionalnost za autentifikaciju korisnika • Uređaj mora imati mogućnost provjere file-ova u cloud sandbox-u • Uređaj mora imati mogućnost detefkcije malware-a za mobilne uređaje • Uređaj mora imati integrisan wireless controller ili uključivati zasebno rješenje • Uređaj mora podržavati kontrolu minimum 128 access point-a • Licence koje moraju biti uključene uz		

uređaja i to na 12 mjeseci:

Opis licence:
Napredna zaštita:
Rješenje mora obezbjeđivati višeslojnu zaštitu saobraćaja kroz kombinaciju sistema za prevenciju upada (IPS), antivirusne i anti-malware zaštite, detekcije botnet i command-and-control (C2) komunikacije, kontrole zlonamjernih URL-ova, kao i naprednih mehanizama za identifikaciju sumnjivih i nepoznatih datoteka. Sistem mora podržavati sandbox analizu i dodatne mehanizme za otkrivanje sofisticiranih i zero-day prijetnji, uključujući zaštitu zasnovanu na globalnoj threat intelligence mreži proizvođača.
Kontrola i filtriranje:
Rješenje mora omogućiti web filtriranje (URL filtering), DNS filtriranje i kontrolu aplikacija (Application Control).
Dodatna sigurnost:
Uređaj mora podržavati anti-spam zaštitu i mehanizme za sprječavanje curenja podataka (Data Loss Prevention – DLP).
Mrežne funkcionalnosti:
Uređaj mora podržavati VPN konekcije (IPsec i SSL), imati integrisanu

					SD-WAN funkcionalnost i omogućavati implementaciju Zero Trust pristupa (ZTNA ili ekvivalent). Zaštita proširene mrežne površine: Rješenje treba da podržava detekciju i procjenu rizika uređaja povezanih na mrežu, uključujući IoT i druge neklasične krajnje tačke, uz mogućnost sigurnosnog rangiranja, identifikacije ranjivosti i dodatne korelacije sigurnosnih događaja. Tehnička podrška: Ponuđač mora obezbijediti 24/7 tehničku podršku proizvođača, pravo na softverske nadogradnje i sigurnosne zakrpe, zamjenu neispravnog uređaja u garantnom roku (RMA), kao i pristup online portalima za podršku i tehničku dokumentaciju. Sigurnosne pretplate: Rješenje mora uključivati aktivne sigurnosne servise koji obezbjeđuju kontinuirano ažuriranje sigurnosnih baza i prijetnji, globalni threat intelligence u realnom vremenu, automatizovanu detekciju i odgovor na incidente, kao i centralizovano izvještavanje i analitiku. Period važenja: Sve licence i pretplate		

					moraju važiti minimalno 12 mjeseci od dana aktivacije. Opšti tehnički zahtjevi: Uređaj mora biti nov i nekorišten, podržavati rad u produkcionim mrežama srednjih i većih organizacija, te imati odgovarajuće performanse za obradu mrežnog saobraćaja bez degradacije sigurnosnih funkcija. • 8 x 10 GE SFP+ transceiver module, short range 300m, LC connector • 2 x 10 GE SFP+ passive direct attach cable 1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu		
				2	Mrežni sigurnosni uređaj (Firewall) Tip2 DR lokacija	• Broj Gigabit Ethernet RJ45 LAN portova: minimum 8; • Broj Gigabit Ethernet RJ45 MGMT (Management) portova: minimum 1; • Broj Gigabit Ethernet RJ45 HA (High Availability) portova: minimum 1; • Broj 5/2.5/GE RJ45 LAN portova: minimum 8; • Broj Ten Gigabit Ethernet SFP+ slotova: minimum 8; • Broj Gigabit Ethernet SFP slotova: minimum	2.00	komada

4;
• Broj USB portova: minimum 1;
• Broj konzolnih portova: minimum 1;
• Uređaj mora biti veličine maksimalno 1RU i opremljen za montažu u standardni 19-inčni rek orman
• Mora posjedovati redundantna napajanja sa podržanim naizmjeničnim naponom u opsegu od 100V do 240V
• Uređaj mora imati minium 39 Gbps firewall protok;
• Uređaj mora imati minimum 9 Gbps IPS propusnost;
• Uređaj mora imati protok za funkcionalnosti Firewall, IPS i kontrola aplikacija od minimum 7 Gbps;
• Uređaj mora imati protok SSL inspekcije od minimumu 7 Gbps
• Uređaj mora imati IPsec VPN protok od minimum 36 Gbps
• Uređaj mora podržavati minimum 11 miliona konkurentnih konekcija
• Uređaj mora podržavati minimum 400k novih konekcija u sekundi
• Uređaj mora podržavati minimum 499 istovremenih SSL VPN korisnika (ukoliko su potrebne licence, iste moraju biti uključene za navedeni kapacitet)
• Uređaj mora imati mogućnost segregacije uređaja na najmanje

10 virtualnih uređaja, koji imaju zaseban menadžment, portove, polise
• Broj Firewall polisa: minimum 10k;
• Uređaj mora podržavati IPV6
• Konfiguracije visoke raspoloživosti: Active/Active, Active/Passive, Clustering;
• Uređaj mora podržavati kreiranje firewall pravila po username-u i grupi korisnika
• Uređaj mora podržavati kontrolu saobraćaja po aplikaciji
• Uređaj mora podržavati ograničenje bandwidth-a po aplikaciji
• Uređaj mora imati inegrisanu funkcionalnost usmjeravanja saobraćaja kroz različite mrežne interfejse, u zavisnosti od tipa aplikacije koja genereši saobraćaj (SD-WAN)
• Uređaj mora podržavati automatski izbor najboljeg linka (između redundantnih IPsec VPN liknova) za pojedinačne aplikacije i servise, u zavisnosti od vrijednosti kašnjenja paketa ili broja izgubljenih paketa na linku
• Uređaj mora podržavati L3 i transparentni način rada
• Uređaj mora podržavati eksplicitni

proxy način rada,
• Uređaj mora podržavati slanje logova preko syslog-a
• Uređaj mora podržavati Captive Portal funkcionalnost za autentifikaciju korisnika
• Uređaj mora imati mogućnost provjere file-ova u cloud sandbox-u
• Uređaj mora imati mogućnost detefkcije malware-a za mobilne uređaje
• Uređaj mora imati integrisan wireless controller ili uključivati zasebno rješenje
• Uređaj mora podržavati kontrolu minimum 128 access point-a
• Licence koje moraju biti uključene uz uređaja i to na 12 mjeseci:

Opis licence:
Predmet nabavke obuhvata aktivaciju licence za tehničku podršku proizvođača koja omogućava kontinuirano održavanje, nadogradnju i podršku za mrežni sigurnosni uređaj.
Minimalni zahtjevi za tehničku podršku:
Dostupnost tehničke podrške 24 sata dnevno, 7 dana u sedmici (24/7)
Pristup zvaničnoj tehničkoj podršci proizvođača (putem web portala, e-maila i telefona)
Pravo na preuzimanje i

instalaciju:
softverskih nadogradnji sigurnosnih zakrpa novih verzija firmware-a
Mogućnost otvaranja i praćenja tehničkih slučajeva (ticketing sistem)
Definisani vremenski okviri odziva u skladu sa nivoom prioriteta incidenta
Hardverska podrška:
Zamjena neispravnog uređaja u garantnom roku (RMA)
Napredna zamjena hardvera u najkraćem mogućem roku u slučaju kvara
Pristup logističkoj podršci proizvođača
Dodatne usluge:
Pristup tehničkoj dokumentaciji, bazama znanja i preporukama proizvođača
Mogućnost eskalacije problema prema višim nivoima tehničke podrške
Preporuke za optimizaciju i održavanje sistema
Period važenja:
Licenca mora važiti minimalno 12 mjeseci od dana aktivacije.
Opšti zahtjevi:
Licenca mora biti validna te mora biti u potpunosti kompatibilna sa ponuđenim mrežnim sigurnosnim uređajem.
• 4 x 10 GE SFP+ transceiver module, short range 300m, LC connector
• 2 x 10 GE SFP+ passive direct attach cable

					1 godina garancije, sa mogućnošću besplatnog upgrade firmware-a kao i otvaranja zahtjeva za tehničkom podrškom u definisanom periodu i zamjena neispravnog uređaja u definisanom periodu		
				3	Softversko rješenje za centralizovano logovanje, analitiku i izvještavanje za Centralni Firewall (stavka br. 1)	Rješenje koje omogućava čuvanje logova, analitiku i izvještavanje za firewall rješenje opisano u stavci 1, sa sljedećim minimalnim funkcionalnostima i zahtjevima: Rješenje mora omogućiti centralizovano prikupljanje, skladištenje, korelaciju i analizu sigurnosnih i sistemskih logova, kao i grafičko i automatizovano izvještavanje u svrhu sigurnosnog nadzora i revizijskih dokaza. Rješenje mora biti isporučeno kao virtuelni uređaj (VM) i mora podržavati proširenje kapaciteta kroz dodatne licence (sklabilni licencni model). Virtuelno rješenje mora biti podržano na najmanje jednoj od sljedećih platformi: VMware ESXi, Microsoft Hyper-V, KVM, Open Source Xen / Citrix XenServer, Nutanix AHV, Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud	1.00	komad

					Infrastructure (OCI). Napomena: Ponuđač mora u ponudi navesti izabranu platformu. Rješenje mora biti licencirano za obradu minimalno 5 GB logova dnevno (GB/dan), uz mogućnost povećanja kapaciteta kupovinom dodatnih licenci (skalabilni model kapaciteta). Rješenje mora podržavati centralizovano prikupljanje više tipova logova, uključujući najmanje: Logove mrežnih aktivnosti / saobraćaja Sistemske logove Logove virusa / malvera Logove napada / IPS događaja Logove filtriranja web sadržaja Logove e-mail sigurnosti (gdje je primjenjivo) Rješenje mora omogućiti: Prikupljanje logova u realnom vremenu Pregled i pretragu historijskih logova Rješenje mora omogućiti vizualizaciju logova, korelaciju događaja i analitiku za predmetno firewall rješenje. Rješenje mora podržavati agregaciju događaja i normalizaciju logova (prepoznavanje tipa događaja i konzistentan prikaz). Rješenje mora		

						omogućiti filtriranje i pretragu najmanje po uređaju, vremenu i tipu događaja. Prikupljeni logovi moraju biti dostupni u čitljivom (normalizovanom) formatu, uz mogućnost pristupa sirovim (neobrađenim) logovima. Rješenje mora podržavati automatsko obogaćivanje podataka vizuelnim indikatorima (npr. aplikacija, geolokacija) radi lakše analize. Rješenje mora omogućiti korelaciju korisničkog identiteta sa aktivnostima/događajima (gdje je primjenjivo i gdje postoje izvori identiteta). Rješenje mora podržavati: Generisanje grafičkih izvještaja Automatizovano (planirano) izvještavanje Predefinisane šablone izvještaja sa detaljnim informacijama i grafičkim prikazima Izvoz izvještaja u PDF formatu Kreiranje prilagođenih izvještaja (baziranih na šablonima ili skupovima podataka) Jednostavan mehanizam uvoza/izvoza izvještaja Rješenje mora obezbijediti konzolu za upravljanje događajima i detekciju abnormalnog ponašanja u		

						intuitivnom i preglednom formatu. Sistem za alarme mora podržavati kompleksna pravila okidanja, kao što su: nivo ozbiljnosti, specifičan događaj, akcija, odredište ili pragovi (threshold uslovi). Alarmiranje mora biti dostupno najmanje putem: E-maila SNMP-a Syslog-a Rješenje mora podržavati enkriptovanu komunikaciju za prenos logova ka i od sigurnosnih uređaja (npr. TLS/HTTPS ili ekvivalent). Rješenje mora imati web-bazirano grafičko upravljačko sučelje dostupno putem HTTPS protokola, optimizovano za PC i tablet uređaje. Grafički interfejs mora obezbijediti sve funkcije potrebne za administraciju i SOC (Security Operations Center) operacije. Rješenje mora podržavati CLI (command-line interface) za konfiguraciju, monitoring i troubleshooting. Administratorski nalozi moraju podržavati RBAC (role-based access control). Rješenje mora omogućiti razdvajanje na nezavisne administrativne domene (npr. po		

					organizacionim jedinicama). Rješenje mora podržavati prosljeđivanje logova ka eksternim sistemima (npr. SIEM / syslog), gdje je potrebno. Rješenje mora podržavati rad kao: kompletan analitički engine i/ili kolektor u distribuiranom okruženju Rješenje mora obezbijediti jednostavnu i dokumentovanu API integraciju, uključujući podršku za JSON API i XML API, za integraciju sa sistemima trećih strana. Modul za procjenu sigurnosnog stanja (Security Posture Assessment Module) Rješenje mora uključivati servis/modul za kontinuiranu procjenu sigurnosnog stanja i napadne površine, zasnovan na stvarnoj konfiguraciji i ponašanju sistema, koji minimalno obuhvata: Automatsku procjenu napadne površine analizom konfiguracija, politika i detektovanih događaja Dodjelu sigurnosnog rejtinga/ocjene koji kvantifikuje trenutno sigurnosno stanje Identifikaciju slabosti, rizičnih konfiguracija i odstupanja od sigurnosnih najboljih		

						praksi Procjenu usklađenosti sa relevantnim sigurnosnim okvirima i standardima (npr. interne politike, industrijski standardi) Preporuke za unapređenje sigurnosnog stanja na osnovu realnih operativnih podataka Praćenje trenda sigurnosne ocjene kroz vrijeme radi mjerenja efikasnosti implementiranih mjera Modul mora biti integrisan u upravljačko okruženje i podržavati grafičko i PDF izvještavanje Licence i podrška Nabavka uključuje licencu za minimalno 5 GB logova dnevno za period od najmanje pet (1) godina. Licenca mora uključivati sve gore navedene funkcionalnosti. Ponuđač mora obezbijediti: tehničku podršku minimalnog nivoa 8x5 (ili bolje) pravo na nadogradnje (firmware/operativni sistem) i sigurnosne zakrpe u trajanju od najmanje jedne godine		
				4	LICENCE ZA DVOFAKTORSKU AUTENTIKACIJU (2FA) Primarna lokacija	LICENCE ZA DVOFAKTORSKU AUTENTIKACIJU (2FA) za Mrežni sigurnosni uređaj (Firewall) Tip1 Nabavka softverskih licenci za generisanje jednokratnih lozinki (OTP – One-Time	1.00	komad

					Password) za potrebe dvofaktorske autentikacije korisnika. Opis licence: Predmet nabavke obuhvata isporuku softverskih autentikacionih tokena koji omogućavaju generisanje jednokratnih lozinki putem mobilnih uređaja, u cilju povećanja sigurnosti pristupa informacionim sistemima. Licence moraju biti kompatibilne sa mobilnim operativnim sistemima, uključujući najmanje: iOS, Android ,druge ekvivalentne mobilne platforme Obim i tip licence: Ukupan broj licenci: 100 korisničkih licenci (tokena) Tip licence: trajna (perpetual) Način isporuke: elektronski licencni certifikat Funkcionalni zahtjevi: Rješenje mora omogućiti: Generisanje vremenski ograničenih jednokratnih lozinki (OTP) Implementaciju dvofaktorske autentikacije (2FA) Integraciju sa sistemima za udaljeni pristup (VPN, web aplikacije i sl.) Sigurnu aktivaciju tokena putem jedinstvenog aktivacionog koda ili QR koda Korišćenje jednog			

						tokena po korisničkom nalogu Ograničenja licence: Svaka licenca (token) je vezana za jedan korisnički uređaj Prenos licence između uređaja nije dozvoljen U slučaju promjene ili gubitka uređaja, potrebno je izvršiti deaktivaciju postojećeg i izdavanje novog tokena od strane administratora Administracija i upravljanje: Rješenje mora omogućiti centralizovano upravljanje, uključujući: Dodjelu i aktivaciju tokena korisnicima Deaktivaciju i brisanje tokena Ponovnu dodjelu tokena u slučaju potrebe Evidenciju i praćenje autentikacionih aktivnosti Namjena: Licence su namijenjene za implementaciju dodatnog sigurnosnog sloja pri autentikaciji korisnika i zaštitu pristupa informacionim resursima od neovlaštenog pristupa. SET OD 100kom		
				5	Implementacija	Opis usluga migracije i implementacije firewall infrastrukture Predmet ove nabavke obuhvata pružanje sveobuhvatnih konsultantskih, projektnih i implementacionih	1.00	komad

usluga u cilju migracije postojećeg firewall okruženja na novo, savremeno firewall rješenje zasnovano na visoko dostupnoj (HA – High Availability) klaster arhitekturi, uz unapređenje bezbjednosnih funkcionalnosti i optimizaciju postojećih sigurnosnih politika.
Postojeće okruženje na primarnoj lokaciji sastoji se od dva FortiGate 500E uređaja u HA konfiguraciji, kao i dva Cisco ASA uređaja takođe implementirana u režimu visoke dostupnosti. Na rezervnoj (DR) lokaciji implementiran je jedan FortiGate 500E uređaj koji obezbjeđuje osnovne sigurnosne funkcionalnosti u slučaju prekida rada primarne lokacije.
Cilj projekta je uspostavljanje novog firewall sistema na obje lokacije, pri čemu će na primarnoj lokaciji novo rješenje biti implementirano u klaster (HA) konfiguraciji sa logičkom podjelom na dvije odvojene virtuelne firewall instance. Jedna virtuelna instanca biće namijenjena migraciji i preuzimanju funkcionalnosti postojećeg FortiGate okruženja, dok će druga instanca biti predviđena za migraciju

						funkcionalnosti Cisco ASA sistema. Ove dvije logičke cjeline moraju biti međusobno izolovane u smislu sigurnosnih politika, upravljanja i obrade saobraćaja, uz istovremeno omogućavanje centralizovanog nadzora i upravljanja. Na DR lokaciji planirana je implementacija novog firewall rješenja u HA konfiguraciji, uz migraciju postojećeg FortiGate sistema, bez potrebe za dodatnom virtuelizacijom ili logičkom segmentacijom, imajući u vidu ulogu ove lokacije kao rezervnog sistema. Ponuđač je dužan da izvrši detaljnu analizu postojećeg stanja, uključujući sve relevantne konfiguracione elemente kao što su sigurnosne politike, NAT pravila, VPN konfiguracije, mrežna segmentacija, routing i svi zavisni servisi. Na osnovu sprovedene analize, izabrani ponuđač je obavezan da izradi detaljan dizajn ciljne arhitekture i plan migracije koji će osigurati minimalan uticaj na produkciono okruženje i kontinuitet poslovanja. Migracija konfiguracije mora obuhvatiti prenos i prilagođavanje svih relevantnih sigurnosnih pravila, NAT politika,		

						VPN konekcija i mrežnih parametara sa postojećih sistema na novo rješenje. Poseban zahtjev odnosi se na transformaciju postojećeg SSL VPN pristupa u IPsec VPN rješenje, uz obaveznu implementaciju dvofaktorske autentikacije (2FA). Nova VPN arhitektura mora biti usklađena sa savremenim bezbjednosnim standardima i, gdje je primjenjivo, integrisana sa postojećim sistemima za upravljanje identitetima (npr. Active Directory, LDAP ili RADIUS). U okviru implementacije, ponuđač je obavezan da izvrši instalaciju i konfiguraciju firewall klastera na obje lokacije, uključujući uspostavljanje visoke dostupnosti, konfiguraciju virtuelnih firewall instanci na primarnoj lokaciji, kao i integraciju sa postojećim infrastrukturnim sistemima kao što su sistemi za autentikaciju, DNS, sistemi za nadzor i upravljanje bezbjednošću. Posebna pažnja mora biti posvećena testiranju i validaciji implementiranog rješenja. Ovo uključuje funkcionalno testiranje svih servisa (javno i interno) dostupnih		

						kritičnih za funkcionisanje Poreske uprave, provjeru sigurnosnih politika, validaciju VPN konekcija (uključujući IPsec i 2FA), kao i testiranje scenarija otkaza i preuzimanja (failover) u okviru HA konfiguracije. Ponuđač je takođe obavezan da obezbijedi kontinuiranu konsultantsku podršku tokom svih faza projekta, uključujući planiranje, implementaciju i završnu fazu migracije (cutover), kao i podršku u periodu stabilizacije sistema nakon migracije. Važno je naglasiti da se za migraciju Cisco ASA firewall sistema zahtijevaju isključivo konsultantske usluge. To podrazumijeva da ponuđač nije odgovoran za direktnu implementaciju konfiguracije, već za izradu preporuka, validaciju pristupa, asistenciju tokom migracije i verifikaciju konačne konfiguracije. Svi radovi moraju biti planirani i izvedeni na način koji minimizuje prekid rada produkcionog sistema. Maksimalno dozvoljeno vrijeme prekida rada tokom migracije produkcionog firewall sistema ne smije biti duže od dva (2) sata, te ponuđač mora predvidjeti odgovarajuće		

mehanizme i procedure kako bi se ovaj zahtjev ispunio. Po završetku projekta, ponuđač je dužan da isporuči kompletnu tehničku dokumentaciju, uključujući opis postojeće i nove arhitekture (as-is i to-be stanje), mapiranje konfiguracija, finalne konfiguracione postavke, kao i preporuke za dalje unapređenje i održavanje sistema.

U okviru predmetne nabavke, ponuđač je dužan da izvrši implementaciju i konfiguraciju sistema za centralizovano logovanje, analitiku i izvještavanje, u skladu sa definisanim tehničkim zahtjevima. Implementacija mora obuhvatiti inicijalnu instalaciju sistema u predviđenom okruženju, njegovu integraciju sa svim relevantnim firewall instancama (uključujući virtuelne firewall-e na primarnoj lokaciji i firewall sistem na DR lokaciji), kao i uspostavljanje centralizovanog prikupljanja i skladištenja logova. Ponuđač je obavezan da izvrši konfiguraciju logovanja za sve relevantne tipove događaja, uključujući sigurnosne, sistemske i mrežne logove, kao i da obezbijedi njihovu

						normalizaciju, korelaciju i dostupnost za dalju analizu. Takođe, potrebno je konfigurisati mehanizme za pretragu i filtriranje logova, kao i kreiranje prilagođenih i predefinisanih izvještaja, uključujući automatizovano generisanje i distribuciju izvještaja u skladu sa zahtjevima naručioca. Rješenje mora biti integrisano sa postojećim sigurnosnim i infrastrukturnim sistemima gdje je primjenjivo, te mora omogućiti jednostavno upravljanje, vizualizaciju događaja i efikasno otkrivanje sigurnosnih incidenata. Ponuđač je dužan da izvrši inicijalno podešavanje sistema za alarmiranje, uključujući definisanje pravila i notifikacija za kritične događaje. Nakon implementacije, ponuđač mora izvršiti testiranje funkcionalnosti sistema, validaciju prikupljanja i obrade logova, kao i obuku relevantnog osoblja naručioca za korišćenje i administraciju sistema. Takođe, obavezno je dostavljanje odgovarajuće tehničke dokumentacije koja obuhvata konfiguraciju sistema, opis integracije i preporuke		

					za dalje korišćenje i optimizaciju.		
2	Nabavka računara i ostale ICT opreme	99173.54	1	All in one	Procesor minimum 10 jezgara (6 P-jezgara + 4 E-jezgara), 16 niti, bazna frekvencija P-jezgra 2.5GHz / Ejezgra 1.8GHz, maksimalna frekvencija P-core 5.2GHz / Ecore 4.0GHz, 24 MB cache Memorija minimum 16GB DDR5, 2 memorijska slota SSD minimum 512 GB SSD M.2 2280 PCIe Gen4 Operativni sistem Windows 11 Professional ili ekvivalentno (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o fabricki preinstaliranom operativnom sistemu) Displej 27" FHD (1920 x 1080), IPS, Anti-Glare, 300 nita, 100Hz, maksimalni ugao gledanja 89 stepeni, kontrast minimum 1300:1 Kamera minimum 5MP sa mehanickim zatvaracem kamere radi privatnosti Integrisani zvucnici minimum 2 x 3W Tastatura sa YU setom karaktera i mis istog proizvodjaca kao i racunar Postolje podrzava tilt podesavanje od -5° do +15° Integrisani portovi pozadi minimum 1x USB-A 10Gbps, 2x USB-A , 1x HDMI-in	53.00	komada

					1.4, 1x HDMI-out 2.1, 1x Ethernet (RJ-45), sa strane: 1x headphone / microphone combo jack (3.5mm) , 1x USB-C 10Gbps - data transfer i 15W punjenje Sigurnost minimum Pokretanje bez tastature i miša, Kontrola sekvence pokretanja, BIOS koji se sam oporavlja - hardverski integrisan mehanizam ugrađen u računarske sisteme koji omogućava automatski oporavak BIOS firmware-a iz hardverski zaštićene kopije (bez potrebe za pristupom mreži) u slučaju neuspjelog ažuriranja, oštećenja ili maliciozne izmjene. Bezbjednosni standard UEFI firmvera koji osigurava da se uređaj pokreće isključivo pomoću softvera kojem proizvođač originalne opreme vjeruje, sprečavajući učitavanje neovlašćenih operativnih sistema i malicioznog koda tokom procesa podizanja sistema. Napajanje maksimum 90W minimum 3 godine garancije, potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku		
			2	Laptop tip 1	Procesor minimum up to 2.5 GHz LP E-core Max Turbo frequency,	10.00	komada

						up to 4.2 GHz E-core Max Turbo frequency, up to 4.9 GHz P-core Max Turbo frequency,18 MB L3 cache, 4 P-cores, 2 LP E-cores and 8 E-cores,14 niti, 13 NPU TOPS Memorija minimum 16GB DDR5, minimum 2 memorijska slota SSD minimum 512GB M.2 Operativni sistem Windows 11 Professional ili ekvivalentno (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o fabricki preinstaliranom operativnom sistemu) Displej 16" diagonal, rezolucija minimum 1920 x 1200, IPS, anti-glare, 300 nita Tastatura sa YU setom karaktera i pozadinskim osvjetljenjem Kamera minimum 5MP IR kamera Integrisani portovi minimum 1 x HDMI 2.1; 1 x stereo headphone/microphone combo jack; 1 x RJ-45; 2x USB Type-A 5Gbps (powered); 2x USB Type-C 20Gbps (USB Power Delivery, DisplayPort, omogućeno punjenje eksternih uređaja čak i kada je laptop u režimu spavanja ili potpuno isključen) Sigurnost minimum citac otiska prsta, Koristeći bezbjednosni kontroler (čip na			

					matičnoj ploči), sistem treba da bude opremljen rješenjem, omogućavajući zaposlenima da brzo i bezbjedno oporave operativni sistem na najnoviju ispravnu verziju slike pomoću ugrađenog modula za skladištenje. Računari će podržavati modernu bezbjednosnu tehnologiju QR koda bez lozinki koje se koriste za kontrolu pristupa BIOS-u za daljinsko upravljanje i/ili lokalno upravljanje za osoblje za podršku na terenu. Baterija minimum 56Wh ,punjenje do 50% za 30 minuta Tezina maksimum 1.75 kg Torba istog proizvodjaca kao i laptop minimum 3 godine, potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o garantnom roku		
				3	MFP A4	Tehnologija štampe: laser Funkcije: štampanje, kopiranje, skeniranje, faks Brzina štampe A4: minimum 40 ppm u režimu velike brzine Dupleks štampa: automatska , 31 ipm ili vise Mjesečni ciklus A4: minimum 100,000 strana Jezici štampe: PCL 6, PCL 5, PostScript level 3 emulation	30.00	komada

						Povezivanje: 2 x USB 2.0 Host; 1 x USB 2.0 Device; 1x Gigabit Ethernet; 1 x Fax Procesor minimum 800 MHz Memorija minimum 2 GB Storage minimum 16 GB eMMC Control panel minimum 4.3” Color Touch Control Panel Ulaz papira: ulaz 1: 100 lista, ulaz 2: 250 lista, moguće dodavanje trećeg ulaza papira za 550 lista, ADF od minimum 50 lista. Izlaz papira: minimum 150 lista Skener: Flatbed i ADF (duplex skeniranje iz ADF) Brzina skeniranja: minimum crnobijelo: 29 ppm/46 ipm (jednostrano/duplex), kolor: 20 ppm/35 ipm (jednostrano/duplex) Sigurnost minimum funkcija koja provjerava integritet BIOS-a - ako detektuje napad ili oštećenje, sistem se samostalno oporavlja (self-healing) učitavanjem čiste kopije BIOS-a (Hardverski izolovana). Konstantno nadgledanje uređaja u realnom vremenu radi prepoznavanja pokušaja neovlašćenog pristupa ili malicioznih aktivnosti. Napredna mrežna zaštita koja analizira odlazni saobraćaj i blokira sumnjive zahtjeve pre nego što uređaj bude kompromitovan.		

						Onemogućavanje USB portova (USB port disablement): Opcija fizičkog ili softverskog blokiranja USB ulaza kako bi se spriječilo curenje podataka ili unošenje virusa putem eksternih diskova. Mogućnost korišćenja tonera kapaciteta minimum 10.000 kopija. Potrošni materijal mora biti jednodijelan. Uređaj ne smije posjedovati zaseban, odvojen drum unit kao poseban potrošni dio koji se mijenja nezavisno od kasete sa tonerom Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak)		
				4	Skeneri	ADF skener Standardne funkcije digitalnog slanja Skeniranje na računar; Skeniranje na USB disk; Skeniranje u e-poštu; Skeniranje u mrežnu mapu; Skeniranje u SharePoint; Skeniranje u prečicu; Skeniranje u oblak Radni ciklus (dnevni) Preporučeni dnevni radni ciklus: 7500 stranica Brzina skeniranja ADF-a Do 75 str./min / 150 slika u minuti Veličina skeniranja (ADF), maksimalna 216 x 3100 mm	26.00	komada

Minimalna veličina skeniranja (ADF) 50,8 x 50,8 mm
Kapacitet ADF-a 80 listova
Dvostrano skeniranje ADF-a Da
Format datoteke skeniranja Za tekst i slike: PDF, PDF/A, šifrirani PDF, JPEG, PNG, BMP, TIFF, Word, Excel, PowerPoint, tekst (.txt), obogaćeni tekst (.rtf) i pretraživi PDF
Načini unosa skeniranja Dva načina skeniranja (jednostrano/dupleks)
sa 10,9 cm (4,3 inča) ekranom u boji osjetljivim na dodir na prednjoj ploči ili preko aplikacije u Windows OS-u, u Mac OS-u i aplikacije trećih strana putem TWAIN, ISIS i WIA
Detekcija višestrukog uvlačenja papira Da
Postavke dpi izlazne rezolucije 75; 150; 200; 240; 300; 400; 500; 600; 1200 ppi
Izvor svjetlosti (skeniranje) LED
Napredne funkcije skenera Automatska ekspozicija, Automatski prag, Automatsko otkrivanje boje, Automatsko otkrivanje veličine, Ispravljanje sadržaja, Poboljšanje sadržaja, Automatsko uvlačenje papira, Senzor za detekciju višestrukog uvlačenja papira, Automatska orijentacija, Brisanje ivica, Brisanje prazne

						stranice, Spajanje stranica, Popunjavanje rupa, Digitalni pečati, Snimanje metapodataka, PDF dozvole, Odvajanje dokumenata (Prazna stranica, Barkod, Zonski barkod, Zonski OCR) Brzina procesora minimum 666 MHz Memorija minimum 1 GB Povezivost, standardna Ethernet 10/100/1000 Base-T, USB 3.0, Wi-Fi 802.11 b/g/n, Wi-Fi Direct Bežične mogućnosti Da,minimum Wi-Fi 802.11 b/g/n, Wi-Fi Direct Mrežni protokoli, podržani minimum ARP; ICMP; IGMP; UDP; TCP; DHCP; APIPA; DNS; mDNS; LLMNR; WSD; WS-Scan; SNTP; SMB; SNMP; FTP; SFTP; SMTP; HTTP serverski dio; HTTPS Garancija: minimum 3 godine (potrebno je dostaviti potvrdu proizvodjaca ili kancelarije proizvodjaca o trajanju garantnog roka za ponudjeni uredjaj i konkretan postupak)		
				5	Produzni kabl sa prenaponskom zastitom	Raspon ulaznog napona (Vac) 200 ~ 250 Dužina kabla za napajanje (m) 1.8 Prekidač za uključivanje/isključivanje Da Zaštita od preopterećenja	15.00	komada

					Prekidač strujnog kruga Zaštita od preopterećenja strujom (A) 10 Tip utičnice Schuko x 8 USB priključak(i) za punjenje USB-A x 2 USB-A izlaz za punjenje 5 V / 2,4 A Zaštita od prenapona i filtriranje Suzbijanje prenapona (džuli) 1050 Maksimalni prenapon (V) 6000 Maksimalna udarna struja (A) 22500 Neutralni vodič prema uzemljenju (NG): 7500 Neutralni vod prema uzemljenju (NG): 1200 Vrijeme odziva (ns); < 1 LED indikatori Zaštićeno od prenapona, uzemljeno Otpornost kućišta na vatru Da Montaža na zid: Da Sigurnosni prekidač: Da Garancija: minimum 24 mjeseca (potrebno je dostaviti potvrdu proizvođača ili kancelarije proizvođača o trajanju garantnog roka)		