Javno naročilo	
Naročnik	**NIJZ** **Trubarjeva cesta 2** **1000 LJUBLJANA**
Oznaka	**60K220621**
Ime posla	**Nadgradnja opreme IT sistemske infrastrukture eZdravja**

Posamezna oprema strojne opreme naj vsebuje najmanj:

Skladno s 7. alinejo, 2. odstavka, 6. člena **Uredbe o zelenem javnem naročanju (ZeJN)**, mora strežniška oprema izpolnjevati najnovejše standarde za energijsko učinkovitost, veljavne na dan objave obvestila o javnem naročilu ali na dan povabila k oddaji ponudbe, ali enakovredne standarde.

Način dokazovanja
Ponudnik mora ponudbi priložiti:
- potrdilo Energy Star ali
- potrdilo, da ima blago znak za okolje tipa I, ali
- tehnično dokumentacijo proizvajalca, iz katere izhaja, da so zahteve izpolnjene.

Splošno

Nacionalni inštitut za javno zdravje (NIJZ), ob zavedanju dinamičnega in konkurenčnega trga na področju predmetnega naročila, stalno izvaja raziskavo tržišča. Prav tako skrbno spremlja tudi dobre prakse v evropskem prostoru. Oprema, ki je vgrajena v varno zdravstveno omrežje eZdravja (zNET), je funkcionalno preverjena.

Javni razpis je namenjen nakupu in zamenjavi obstoječe IT infrastrukture »Prenova in dograditev primarne in sekundarne lokacije« (mrežna oprema, varnostna opreme, strežniška oprema in programske licence), ki ni oziroma ne bo več pod veljavnim vzdrževanjem proizvajalca in vključuje predviden obseg:

- **Lot 1:** prenova in dograditev mrežne ter varnostne infrastrukture (stikala, VPN koncentrator in požarna pregrada)
- **Lot 2:** prenova in dograditev data center infrastrukture (strežniško ohišje, strežniške rezine, nadgradnja diskovnega sistema HPE 3PAR 8200)
- **Lot 3:** nadgradnja ter nakup programske licence (Cisco, Oracle in centralni zbiralnik logov in korelacijo dogodkov)

Oprema je potrebna za prenovo in dograditev IT infrastrukture na primarni in sekundarni lokaciji NIJZ. Ponudbo je potrebno ponuditi kot celoto (Lot 1, Lot 2 in Lot 3).

Natančen pogodbeni obseg dobav in storitev, vključno z vsemi tehničnimi podatki, zahtevami in pogoji, je podan v dokumentaciji v zvezi z oddajo javnega naročila, prijavi/ponudbi izvajalca in končnem ponudbenem predračunu, ki so sestavni del javnega naročila.

Vsa ponujena oprema mora biti nova in nabavljena preko uradnega distribucijskega kanala v Sloveniji, namenjena slovenskemu trgu - torej takšna, da jo bo mogoče brez modifikacij uporabljati v Sloveniji ter ji v Sloveniji zagotavljati celostno podporo. Zahtevana je garancija in

podpora proizvajalca celotne opreme za obdobje 36 mesecev z odpravo napake. Podpora mora biti vidna v sistemu proizvajalca.

Za ponujeno opremo mora veljati poseben garancijski pogoj, v katerih se ponudnik opreme obvezuje za čas pogodbe:

- sprejeti prijavo okvare v režimu 24x7
- odpraviti prijavljeno okvaro na nedelujoči opremi najkasneje v roku naslednjega delovnega dne oziroma jo zamenjati z enako opremo ali njenim funkcionalnim ekvivalentom od trenutka predaje nedelujoče opreme v popravilo ponudniku (osebna dostava ali po pošti) na lokaciji ponudnikovega servisa.

Za ponujeno opremo se ponudnik opreme obvezuje naročniku, v obdobju 36 mesecev od prevzema opreme, brezplačno zagotavljati vse nove verzije programske opreme v okviru iste funkcionalnosti.
Obdobje zagotavljanja rezervnih delov za ponujeno opremo je 36 mesecev od prevzema opreme.

Za vso ponujeno opremo mora ponudnik predložiti izjavo:
Izjava proizvajalca opreme (MAF »Manufacturer's Authorisation«), s katero izjavlja da ima ponudnik ustrezne kompetence za prodajo, implementacijo in vzdrževanje ponujene opreme.

Predračun, dobavni roki, rok za izvedbo, garancijski rok in licenčna podpora.

1 Predračun zajema dobavo, zagon in osnovna nastavitev opreme in nadgradnje na najnovejšo priporočeno različico operacijskega sistema. Specifikacija storitev je natančno opisana v poglavju »storitve«.
2 Dobavni rok za vso opremo je **največ 120 dni** od podpisa pogodbe; zagon in konfiguracija opreme bo izvedena naknadno, po izvršeni dobavi opreme, v dogovoru med naročnikom in izbranim ponudnikom.
3 Rok za izvedbo »storitev« je **5 delovnih dni po dobavi opreme.**
4 Splošno določen garancijski rok za strojno in programsko opremo je 36 mesecev.
V primeru potrebe po licenčni podpori naj bo 36 mesecev.

Tehnične zahteve za Lot 1, Lot 2 in Lot 3

LOT 1: prenova in dograditev mrežne ter varnostne infrastrukture (stikala, VPN koncentrator in požarna pregrada)

Obstoječa naročnikova mrežna in varnostna oprema (stikala, VPN koncentrator) v okviru zNet omrežja temelji na opremi proizvajalca Cisco Systems, za katero ima naročnik zagotovljene strokovnjake. Zaradi navedenega želimo zagotoviti kompatibilnosti z obstoječo komunikacijsko opremo, pričakujemo vsaj:

- združljivost na funkcionalnem in protokolnem tehničnem nivoju z opremo obstoječega komunikacijskega omrežja zNET;
- zanesljivo obratovanje v obstoječem sistemu oziroma omrežju.

Vsa ponujena mrežna oprema mora biti od istega proizvajalca. Naročnik sprejme popolnoma enakovredno mrežno opremo pri tem, da bo ponudnik v tem primeru moral zagotoviti brezplačno usposabljanje in izobraževanje strokovnjakov (za 4 osebe), ki skrbijo za nemoteno delovanje omrežja, za pridobitev ekvivalentnih znanj, kot so navedena v razpisni dokumentaciji. Ta usposabljanja in izobraževanja strokovnjakov (vključujoč uradno certifikacijo) morajo vsebovati pridobitev znanja za:

- povezavo enakovredne opreme z obstoječo Cisco Systems opremo,
- konfiguracija te opreme v zNET okolju s Cisco Systems opremo v skladu z zahtevami naročnika, vzdrževanje enakovredne opreme.

Obstoječa naročnikova varnostna oprema (požarna pregrada) v okviru zNet omrežja temelji na opremi proizvajalca CheckPoint, za katero ima naročnik zagotovljene strokovnjake. Zaradi navedenega želimo zagotoviti kompatibilnosti z obstoječo varnostno opremo.

Vsa ponujena varnostna oprema mora biti od istega proizvajalca. Naročnik sprejme popolnoma enakovredno varnostno opremo (požarna pregrada) pri tem, da bo ponudnik v tem primeru moral zagotoviti brezplačno usposabljanje in izobraževanje strokovnjakov (za 4 osebe), ki skrbijo za nemoteno delovanje, za pridobitev ekvivalentnih znanj, kot so navedena v razpisni dokumentaciji. Ta usposabljanja in izobraževanja strokovnjakov (vključujoč uradno certifikacijo) morajo vsebovati pridobitev znanja za:

- povezavo enakovredne opreme z obstoječo CheckPoint opremo,
- konfiguracija te opreme v zNET okolju s CheckPoint opremo v skladu z zahtevami naročnika, vzdrževanje enakovredne opreme.

V Lot 1 je potrebno vključiti garancijo in podporo proizvajalca za čas trajanja pogodbe (tovarniška podpora za nadgradnjo in odpravo napak) za vso ponujeno strojno in programsko opremo.

Lot 1: prenova in dograditev mrežne ter varnostne infrastrukture	**Količina**
1. Centralno stikalo	**2**
S stikali se bo zagotovila povezljivost med različnimi segmenti celotnega omrežja. Priložiti je treba vse potrebne licence za spodnje zahteve: ***Zahtevani vmesniki in zmogljivost:*** • vsaj 24 fiksnih vmesniških rež, ki omogočajo vgradnjo: o 1Gb/s Ethernet SFP, o 10Gb/s Ethernet SFP+, • možnost uporabe na vsaj 8 vmesniških režah: o 25Gb/s Ethernet SFP28, • možnost nadgradnje najmanj 2 vmesniških rež na, o 40Gb/s QSFP+, • namenski RJ-45 vmesnik za upravljanje stikala, • konzolni vmesnik, • USB vmesnik, • Zmogljivost najmanj 64'000 IPv4 in 32'000 IPv6 smeri, • Najmanj 4000 Vlan-ov, • Prepustnost 960 Gbps in 720 Mpps, ***Splošne zahteve:*** • možnost vgradnje v 19'' omaro, • višina 1 RU (rack unit), • zračno hlajenje z zajemom zraka s strani vmesnikov, • podpora za IEEE 802.1p, • podpora za IGMP, QoS,	

• podpora za IPv6, • avtentikacija administrativnih uporabnikov po protokolih TACACS+ in RADIUS, • podpora za 802.1q (VLAN), • podpora zasebnim VLAN-om (»private VLAN«, podpora več VLAN-om znotraj istega omrežnega segmenta), • podpora dinamičnemu dodeljevanju VLAN pri avtentikaciji 802.1x, • zmožnost odpravljanja zank in zagotavljanja redundance na drugi ravni ISO/OSI: podpora za protokole »Spanning-tree, STP« (IEEE 802.1D), »Multiple STP« (IEEE 802.1s) in »Rapid STP« (IEEE 802.1w), • podpora za protokol STP za vsak VLAN posebej, • podpora za povezovanje fizičnih omrežnih vmesnikov v en logični vmesnik – "link aggregation" po protokolu IEEE 802.3ad (LACP), • možnost preverjanja izvora paketov ARP in preprečevanja pošiljanja paketov z napačno vsebino glede na povezavo naslovov IP-MAC ("ARP inspecition"), • podpora paketom MTU dolžine 9000 zlogov (Jumbo frames), • Visoka razpoložljivost s skladanjem dveh stikal v virtualno šasijo ali VSS, Nonstop Forwarding (NSF), Graceful Insertion and Removal (GIR), Fast Software Upgrade (FSU), • možnost združevanja povezav na različnih stikalih, • podpora za protokol Link Layer Discovery Protokol (LLDP) IEEE 802.1AB, • vgrajen dodatni redundantni napajalnik, • možnost zamenjave napajalnika med delovanjem, • redundatni ventilatorji z možnost zamenjave med delovanjem, • Avtomatizacija upravljanja s protokoli YANG in RESTCONF/NETCONF, • Možnost uporabe IEEE 802.1ae MAC Security (MACsec 256 bit) na vseh vmesnikih, • Usmerjevalni in stikalni protokoli: BGP, EIGRP, IS-IS, MSDP, OSPF, PBR, PIM, SSM, VRF in PVLAN, • Podpora naprednih protokolov: VRF, BGP EVPN z VXLAN, LISP in SGT (Security group tags), ***Zahteve za nadzor in upravljanje:*** • možnost upravljanja po protokolu SSH, Web, SNMP in serijskem vmesniku, • možnost nalaganja oziroma shranjevanja konfiguracije naprave z uporabo FTP ali TFTP strežnika, • možnost nalaganja oziroma shranjevanja konfiguracije naprave z uporabo vgrajenega vmesnika USB, • možnost aktiviranja prejšnje konfiguracije, • Omrežna vidljivost: Telemetry, sampled NetFlow, SPAN, RSPAN;	
2. Pristopno stikalo	**4**
Tehnična specifikacija za pristopna stikala. Priložiti je treba vse potrebne licence za spodnje zahteve: ***Zahtevani vmesniki in zmogljivost:*** • vsaj 24 vmesnikov ethernet 10/100/1000 (Base-T, RJ45),	

• vsaj 8 vmesnike 10Gb/s Ethernet SFP+, • zmogljivost stikala po prepustnosti najmanj 200 Gbps oz. 680 Gbps v skladu, • zmogljivost stikala po številu paketov najmanj 150 Mpps. • namenska vmesnika za povezovanje v sklad, • namenski RJ-45 vmesnik za upravljanje stikala, • konzolni vmesnik, • USB vmesnik, • Zmogljivost najmanj 20'000 IPv4 in 10'000 IPv6 smeri, • Najmanj 4000 Vlan-ov, • Podpora najmanj 10 virtualnih instanc (VRF). ***Splošne zahteve:*** • možnost vgradnje v 19'' omaro, • višina 1 RU (rack unit), • povezana dva stikala v sklad z možnostjo dodajanjem do skupaj osem stikal, o dodani podatkovni povezovalni (stack) kabli, • podpora za IEEE 802.1p, • podpora za IGMP, QoS, • podpora za IPv6, • avtentikacija administrativnih uporabnikov po protokolih TACACS+ in RADIUS, • podpora za 802.1q (VLAN), • podpora zasebnim VLAN-om (»private VLAN«, podpora več VLAN-om znotraj istega omrežnega segmenta), • podpora dinamičnemu dodeljevanju VLAN pri avtentikaciji 802.1x, • zmožnost odpravljanja zank in zagotavljanja redundance na drugi ravni ISO/OSI: podpora za protokole »Spanning-tree, STP« (IEEE 802.1D), »Multiple STP« (IEEE 802.1s) in »Rapid STP« (IEEE 802.1w), • podpora za protokol STP za vsak VLAN posebej, • podpora za povezovanje fizičnih omrežnih vmesnikov v en logični vmesnik – "link aggregation" po protokolu IEEE 802.3ad (LACP), • zaščita proti priklopom nepooblaščenih strežnikov DHCP (DHCP Snooping) • možnost preverjanja izvora paketov ARP in preprečevanja pošiljanja paketov z napačno vsebino glede na povezavo naslovov IP-MAC ("ARP inspecition"), • podpora paketom MTU dolžine 9000 zlogov (Jumbo frames), • možnost združevanja povezav na različnih stikalih, • podpora za protokol Link Layer Discovery Protokol (LLDP) IEEE 802.1AB, • možnost odkrivanja sosednjih naprav po protokolu CDP (neighbor learning) • vgrajen dodatni redundantni napajalnik, • možnost zamenjave oz. vgradnje napajalnika med delovanjem, • redundantni ventilatorji z možnost zamenjave med delovanjem, • Avtomatizacija upravljanja s protokoli YANG in RESTCONF/NETCONF, • Možnost uporabe IEEE 802.1ae MAC Security (MACsec 128 bit) na vseh vmesnikih, • Usmerjevalni in stikalni protokoli: EIGRP, BGP, OSPF, PBR, PIM, VRRP in PVLAN,	

• zaščita vrat pred broadcast, multicast in unicast preobremenitvijo (storm control) ***Zahteve za nadzor in upravljanje:*** • možnost upravljanja po protokolu SSH, Web, SNMP in serijskem vmesniku, • možnost nalaganja oziroma shranjevanja konfiguracije naprave z uporabo FTP ali TFTP strežnika, • možnost nalaganja oziroma shranjevanja konfiguracije naprave z uporabo vgrajenega vmesnika USB, • možnost aktiviranja prejšnje konfiguracije, • Omrežna vidljivost: Telemetry, sampled NetFlow, SPAN, RSPAN;	
3. Vgradni modul za obstoječo mrežno opremo - C9500-16X	**2**
Zahtevani vmesniki in zmogljivost: • vsaj 8 vmesnikov 10Gb/s Ethernet SFP+	
4. VPN koncentrator	**2**
Tehnična specifikacija za VPN koncentrator. Priložiti je treba vse potrebne licence za spodnje zahteve: ***Zahtevani vmesniki in zmogljivosti***: • zmogljivost požarne pregrade po prepustnosti vsaj 6 Gbps, • zmogljivost požarne pregrade po prepustnosti pri povezovanju z več protokoli hkrati vsaj 3 Gbps, • vsaj 1.5 milijona sočasnih povezav, • vsaj 28000 novih povezav na sekundo, • vsaj 2 virtualnih požarnih pregrad z možnostjo razširitve na 25, • TLS prepustnost vsaj 460 Mbps, • IPsec VPN prepustnost vsaj 700Mbps, • možnost uravnoteženja VPN povezav, • vsaj 3.500 možnih povezav VPN, • visoka razpoložljivost active/standby in active/active • vsaj 12x 1 Gbps ethernet vmesnikov (RJ45), • vsaj 4x 10 Gbps ethernet vmesnikov (SFP), • vsaj 1x 10/100/1000 Mbps ethernet vmesnik za namen upravljanja požarne pregrade, • konzolni vmesnik za konfiguracijo naprave, • vsaj 100 GB prostora za shranjevanje datotek, • USB vmesnik za možnost nadgradnje operacijskega sistema ali nameščanje sistemskih popravkov, • Ventilatorji: Zajem hladnega zraka s sprednje strani. ***Splošne zahteve:*** • možnost vgradnje v 19'' omaro, • višina usmerjevalnika 1RU,	

• podpora za povezovanje fizičnih omrežnih vmesnikov v en logični vmesnik – "link aggregation" po protokolu IEEE 802.3ad (LACP),
• translacija naslovov IP (Network Address Translation - NAT),
• Dynamic Host Configuratin Protocol (DHCP), kjer je usmerjevalnik strežnik, odjemalec ali posrednik (relay),
• filtriranje prometa IP z uporabo Access Control List (ACLs),
• kakovost storitev (QoS) z možnostjo določitve prioritizacije občutljivega prometa (zagotavljanje nizke zakasnitve) in omejevanje pasovne širine aplikacijam na vhodu in izhodu omrežnih vmesnikov z najmanj naslednjimi mehanizmi:
  o Low-Latency Queuing (LLQ),
  o Class-Based Trafic Shaping (CBTS),
  o Class-Based Trafic Policing (CBTP),
  o Policy-Based Routing (PBR),
  o Different Services (DiffServ),
• usmerjanje prometa IP z uporabo statičnih smeri (static routing) in dinamičnega usmerjanja po protokolih EIGRP, RIPv2, OSPF in BGP, IS-IS, redistribucijo usmerjevalnih protokolov, filtriranje oglaševanja smeri z uporabo filtrov IP (ACL distribute list),
• podpora protokola IPv4
• najmanj naslednje funkcionalnosti protokola IPv6:
  o naslavljanje omrežnih vmesnikov z naslovi IPv6
  o uporabo usmerjevalnih protokolov OSPFv3, BGP in statičnega usmerjanja,
  o ICMPv6,
  o filtriranje prometa IP (Access-list) glede na naslove IPv6,
  o IPv6 DCHP,
  o multicast IPv6,
  o IPv6 path maximum transmission unit (PMTU),
  o IPv6 Neighbor Discovery,
  o IPv6 stateless address autoconfiguration (SLAAC),
• podpora za IKEv1 in IKEv2,
• strojno podprto šifriranje DES, 3DES, AES 192 in AES 256 v načinih CBC in GCM,
• avtentikacija RSA (748/1024/2048 bit) in ECDSA (256/384 bit),
• zagotavljanje integritete z uporabo MD5, SHA, SHA-256, SHA-384 in SHA-512,
• zmožnost uporabe Public-key-infrastructure (PKI).
 	
Zahteve za nadzor in upravljanje:
• konfiguriranje in nadzor z uporabo ukazne vrstice prek šifrirane seje SSH oz. prek serijskega vmesnika RS-232 (konzole),
• konfiguriranje in nadzor požarne pregrade prek namenskega grafičnega vmesnika,
• upravljanje in nadzor po protokolih SNMPv1, v2c in v3 ter RMON,
• nadgradnja programske opreme prek protokola TFTP,
• možnost aktiviranja prejšnje konfiguracije,
• časovna sinhronizacija po protokolu NTP z overjanjem,	

• različne ravni administrativnega dostopa (Role Based Access Control - RBAC) - omejevanje pravic upravljanja glede na uporabniško ime, • overjanje (Authentication) in pooblaščanje (Authorization) administrativnega dostopa z uporabo strežnikov AAA po protokolu RADIUS oz. TACACS+ ali lokalne baze (na napravah) uporabniških imen in gesla, • pošiljanje sporočil zunanjemu syslog strežniku, • možnost nalaganja oziroma shranjevanja konfiguracije naprave z uporabo FTP ali TFTP strežnika, • možnost nalaganja oziroma shranjevanja konfiguracije naprave z uporabo vgrajenega vmesnika USB.	
5. Požarna pregrada	**4**
Za požarno pregrado je potrebno upoštevali spodnje tehnične zahteve. Obvezno je potrebno ponuditi štiri namenske fizične naprave (po dva na vsaki lokaciji). Požarne pregrade naj bodo pripravljene za visoko razpoložljivost. Priložiti je treba vse potrebne licence za spodnje zahteve. **Splošne zahteve požarne pregrade glede strojne in programske opreme:** • Rešitev mora omogočati visoko razpoložljivost v načinu aktivni-aktivni ali akitvni-pasivni. Izvajalni moduli morajo biti ločeni od upravljalnega modula. • Podpora delovanja v načinu gruče znotraj istega ter geografsko ločenega podatkovnega centra. • Ponujen proizvajalec požarne pregrade mora imeti v svojem portfelju podprto implementacijo virtualizirane požarne pregrade v oblačnih ponudnikih (min. Microsoft Azure in Amazon WS). • Rešitev ne sme biti omejena na število končnih uporabnikov ter strežnikov, ki prehajajo varnostne komponente. • Podpora virtualnih kontekstov na požarni pregradi tipa: požarna pregrada, stikalo, usmerjevalnik. ○ Vsaj za 3 virtualne kontekste. • Rešitev mora omogočati namestitev modula požarne pregrade na namensko strojno opremo proizvajalca (Appliance) in na strojno opremo drugih proizvajalcev (strežniki HP, Dell, Lenovo in IBM) brez uporabe prednameščene virtualne infrastrukture (VMware, HyperV) • Vsaj 5 letna prisotnost v Gartner kvadrantu vodilnih proizvajalcev požarnih pregrad in 10 let izkušenj na področju varnostnih rešitev **Minimalne zahtevane lastnosti strojne opreme (za posamezno napravo):** • velikost strojne opreme ne več kot 2 RU z možnostjo vgradnje v obstoječo komunikacijsko omaro, • priključna vrata: • minimalno 4x 10GbE (SFP+) vmesnikov, možnost razširitve do 8 • minimalno 10x 1Gb vmesnikov, možnost razširitve do 26 • podpora širitve mrežnih vmesnikov na 40GbE • Minimalno 2x 480G SSD na posamezni procesni modul v RAID1. • Minimalno 64GB RAM na posamezni procesni modul • ločena vrata za povezavo HA in upravljanje,	

- možnost delovanja vrat v različnih načinih (trust, untrust, DMZ,…),
- redundantni napajalnik (N+1) 220 V AC,
- relovanje naprave v temperaturnem razponu od 0 do 40°C.

Performančne zahteve požarne pregrade:

- prepustnost požarne pregrade vsaj 35Gbps (Firewall),
- prepustnost požarne pregrade vsaj 23Gbps (IPS),
- prepustnost požarne pregrade vsaj 20Gbps (NGFW),
- število hkratnih sej preko požarne pregrade vsaj 16.000.000,
- število novih sej na sekundo vsaj 300.000.

Minimalne zahtevane lastnosti programske opreme – požarna pregrada:

- podpora agregaciji mrežnih povezav 802.3ad,
- delovanje v L3 načinu (routing mode),
- podpora za first hop redundancy protokol (VIP naslov za kliente),
- podpora združevanju štirih ali več požarnih pregrad v gručo (cluster) na način Active-Active in Active-Passive,
- sinhronizacija sej med člani gruče,
- »Stateful« požarna pregrada,
- podpora mehanizmom za usmerjanje:
  - Statične route,
  - Multicast route,
  - OSPFv2 in v3,
  - BGP,
  - RIP,
  - PIM-SM, PIM-SSM, PIM-DM,
  - IGMP v2 in v3,
- podpora za IPv6 protokol:
  - podpora funkcionalnostim: požarna pregrade, varnostno pregledovanje prometa (npr. URL filtering, IPS, blokiranje aplikacij),
  - identifikacija uporabnikov,
  - NAT66 in NAT64.
- integracija z aktivnim imenikom,
- podpora centralnemu upravljanju in nadzoru,
- podpora centralnemu logiranju
- Možnost zaznavanja in preprečevanja DNS zahtev po imenih znanih »Command and control« strežnikov.
- Zaščita za odkrivanja in preprečevanje vdorov (IPS).
- Zaščita IPS mora temeljiti na naslednjih mehanizmih zaznavanja: podpisi (signature), anomalije protokolov, nadzor aplikacij in zaznavanje na podlagi vedenja (behavior-based detection).
- IPS zaščita mora podpirati omrežne izjeme glede na vir, cilj, storitev ali kombinacijo treh.
- IPS zaščita mora imeti možnost zajema prometa za vsako signaturo.
- Možnost vnosa IOC-jev (Indicator Of Compromise) iz zunanjih virov (datoteka, HTTP, HTTPS,..).

• IPS zaščita mora omogočati mehanizem, ki temelji na programski opremi, in ga je mogoče konfigurirati na podlagi obremenitve CPU in porabe pomnilnika. • možnost prepoznavanja in blokiranja prometa na nivoju aplikacij (vsaj: aplikacije za omogočanje oddaljene administracije, dostop do video vsebin, socialne medije, P2P, Anonymizer, škodljive aplikacije, visoko rizične aplikacije), • možnost pisanja pravil po državi (omejevanje dostopov do strežnika samo iz določenih držav), • možnost posredovanja prometa na določen port (mirror interface), • omogočena mora biti zaščita glede na lokacijo (državo) izvora prometa (GEO location protection), Ponudnik mora ponuditi centralni upravljalni sistem za vse štiri naprave, če naročnik sistem že ima potem ga ni potrebno ponuditi dodatno.	
Vzdrževanje v času veljavnosti garancije za mrežno in varnostno opremo: Za ponujeno mrežno in varnostno opremo mora veljati poseben garancijski pogoj, v katerih se ponudnik opreme obvezuje za čas pogodbe: • sprejeti prijavo okvare v režimu 24x7, • odpraviti prijavljeno okvaro na nedelujoči opremi najkasneje v roku 24x7x4 oziroma jo zamenjati z enako opremo ali njenim funkcionalnim ekvivalentom od trenutka predaje nedelujoče opreme v popravilo ponudniku (osebna dostava ali po pošti) na lokaciji ponudnikovega servisa, • vsa ponujena oprema mora vključevati podporo vzdrževanja proizvajalca za obdobje 36 mesecev, • odzivni čas naslednji delovni dan (NBD). Podpora mora biti vidna v sistemu proizvajalca.	

Lot 2: prenova in dograditev data center infrastrukture (strežniško ohišje, strežniške rezine, nadgradnja diskovnega sistema HPE 3PAR 8200)

Obstoječa naročnikova oprema v data center infrastrukturi temelji na opremi proizvajalca Hewlett-Packard Enterprise, za katero ima naročnik zagotovljene strokovnjake. V okolju je 99% opreme proizvajalca Hewlett-Packard Enterprise. Naročnik za svoje potrebe že poseduje strežniške rezine HPE BL460 in pripadajoča ohišja za strežniške rezine HPE BladeSystem c7000 ter diskovni polji HPE 3PAR 8200. S tem razpisom naročnik želi izvesti nadgradnjo podatkovnega centra s strežniškim ohišjem in strežniki, nadgraditi obstoječe diskovno polje z dodatnimi diskovnimi kapacitetami.

Vsa ponujena strežniška oprema mora biti od istega proizvajalca. Naročnik sprejme popolnoma enakovredno opremo pri tem, da bo ponudnik v tem primeru moral zagotoviti brezplačno usposabljanje in izobraževanje strokovnjakov (za 2 osebi), ki skrbijo za nemoteno delovanje sistema, za pridobitev ekvivalentnih znanj, kot so navedena v razpisni dokumentaciji. Ta usposabljanja in izobraževanja strokovnjakov (vključujoč uradno certifikacijo) morajo vsebovati pridobitev znanja za:

- povezavo enakovredne opreme z obstoječo HPE opremo,
- konfiguracija te opreme v eZdravje okolju s HPE opremo v skladu z zahtevami naročnika, vzdrževanje enakovredne opreme.

Lot 2: prenova in dograditev data center infrastrukture (strežniško ohišje, strežniške rezine, nadgradnja diskovnega sistema HPE 3PAR 8200)	**Količina**
1. Strežniško ohišje	**2**
Strežniško ohišje z naslednjimi zahtevami: • mora omogočati vgradnjo vsaj 12-ih strežniških rezin - zaradi kasnejših nadgradenj, v kolikor ponudnik te zahteve z 1 ohišjem ne more izpolniti mora ponuditi 2 ohišji, • višina strežniškega ohišja je lahko največ 10U, • vgradnja v standardno strežniško omaro globine 1000mm, • možnost vgradnje diskovne rezine ali diskovnega predala (z vgradnjo diskovnega predala se zmanjša maksimalno število vgrajenih strežnikov), • možnost vgradnje diskovnega predala, ki lahko vsebuje vsaj 16 diskov formata (2.5"), diski v predalu so dostopni vsem strežnikom, • možnost vgradnje HDD, SSD diskov v predal, • strežniško ohišje mora imeti redundantno napajanje in hlajenje, • vgrajenih mora biti vsaj 6 napajalnikov moči najmanj 2600W, • omogočati mora uporabo oddaljenega KVM, • vgrajena management modula (2), ki omogočata povezljivost na druga strežniška ohišja, • sistem moram biti upravljan z enim upravljavskim orodjem, • vgrajena posebna modula (2) za upravljanje (v redundantnem načinu) s celotno infrastrukturo, ki omogočata provisioning celotnega okolja (strojna in programska oprema) web based okolje, • priloženo upravljavsko orodje mora omogočati postavitev celotnega sistema (virtualnega in fizičnega) preko nastavljenih profilov, • ohišje mora omogočati vgradnjo vsaj 5-tih stikal za povezovanje ohišja z zunanjo infrastrukturo, • možnost vgradnje manjših strežnikov polovične višine (vsaj 8) ter večjih strežnikov (vsaj 3), • v strežniško ohišje mora biti vgrajeno podvojeno stikalo, ki ima vsaj 6 x QSFP28 uplinkov. Vsak QSFP28 port mora omogočati uplink hitrost 100Gbps. Stikalo mora imeti vgrajena vsaj dva ločena porta za povezovanje podatkovnega prometa med ohišji brez uporabe zunanjih stikal, hitrosti najmanj 100Gbps na port ○ priložena sta 2 DAC kabla 100Gb QSFP28 na QSFP28 3 metre ○ priloženi so 4x DAC kabli 10GbE SFP+ na SFP+ 5 metrov ○ priloženo je 8 adapterjev iz QSFP28 na SFP28 ○ priloženi so 4x 16Gb SFP+ transceiverji ○ priloženi so 4 optični kabli LC/LC multi mode OM4 5m ○ priložen je 1 kabel CAT6 1,2m za povezavo med ohišji ○ stikalo mora omogočati povezavo in delovanje v FC (SAN) omrežje hitrosti 32Gbps (priložene vse potrebne licence, če je to potrebno) ○ stikalo v strežniškem ohišju mora omogočati direktno in redundantno FC priključitev na obstoječi diskovni sistem HPE 3PAR 8200 brez uporabe dodatnih naprav **(v kolikor te zahteve ponudnik ne**	

more izpolniti, mora ponuditi dve (2) zunanji 24-vratni SAN stikali 32 Gb/s) • na zadnji strani ohišja naj bo možno vgraditi vsaj 6 povezovalnih modulov, v redundantnem načinu (3+3): ○ 10Gbps Ethernet pass-thru modul ○ 12Gbps SAS stikala ○ 25-50Gbps Ethernet stikala ○ 100Gbps in 32Gbps Ethernet/FC stikala ○ 16Gbps in 32Gbps FC stikala • priložena vodila za vgradnjo ohišja v komunikacijsko omaro Garancijski rok za ponujeno opremo je 36 mesecev. Ponudba naj vključuje 36 mesecev servisno podporo s strani proizvajalca za celotno konfiguracijo v režimu: odprava napake v roku 6 ur. Podpora mora biti vidna v sistemu proizvajalca.	
2. Rezinski strežnik za strežniško ohišje	**8**
Strežnik polovične višine, ki se ga vgradi v zgornje ohišje s konfiguracijo: • vgrajena dva procesorja Intel Xeon-Gold 5218R (2.1GHz/20-core/125W), • 1024 GB RAM-a (16 x 64GB Quad Rank DDR4 moduli) ○ možnost do 3TB spomina (možna menjava obstoječih modulov), ○ vsaj 8 prostih mest za kasnejše nadgradnje, ○ možnost vgradnje NVDIMM ali Intel Optane DC Persistent Memory • vgrajena ena dvo portna CNA kartica 10/20/25Gb, • skupno 3 razširitvena mesta (PCIe) - mezzazine (Ethernet ali FC ali CNA), • diskovni krmilnik 12G s podporo za RAID 1, 0 (software RAID krmilnik ni sprejemljiv), • vgrajena dva SSD diska kapacitete vsaj 240GB RI SATA 6G, • možnost vgradnje dveh diskov (SSD, HDD, NVMe) – SAS-SATA, • interni in eksterni USB 3.0 priključek, • poseben priključek za upravljanje na prednji strani strežnika, • gumb za vklop, • podpora za TPM 2.0, • podpora za UEFI (Unified Extensible Firmware Interface Forum), • oddaljen dostop KVM s polno funkcionalnostjo tudi na OS nivoju. Garancijski rok za ponujeno opremo je 36 mesecev. Ponudba naj vključuje 36 mesecev servisno podporo s strani proizvajalca za celotno konfiguracijo v režimu: odzivni čas naslednji delovni dan (NBD). Podpora mora biti vidna v sistemu proizvajalca.	
3. Rezinski strežnik za strežniško ohišje	**1**
Strežnik polovične višine, ki se ga vgradi v zgornje ohišje s konfiguracijo: • vgrajen 1x procesor Intel Xeon-Gold 5222 (3.8GHz/4-core/105W), • 128GB RAM-a (2 x 64GB Dual Rank DDR4 moduli) ○ možnost do 3TB spomina (možna menjava obstoječih modulov), ○ vsaj 8 prostih mest za kasnejše nadgradnje, ○ možnost vgradnje NVDIMM ali Intel Optane DC Persistent Memory • vgrajena ena dvo portna CNA kartica 10/20/25Gb, • skupno 3 razširitvena mesta (PCIe) - mezzazine (Ethernet ali FC ali CNA), • diskovni krmilnik 12G s podporo za RAID 1, 0 (software RAID krmilnik ni sprejemljiv), • vgrajena dva SSD diska kapacitete vsaj 240GB RI SATA 6G,	

- možnost vgradnje dveh diskov (SSD, HDD, NVMe) – SAS-SATA,
- interni in eksterni USB 3.0 priključek,
- poseben priključek za upravljanje na prednji strani strežnika,
- gumb za vklop,
- podpora za TPM 2.0,
- podpora za UEFI (Unified Extensible Firmware Interface Forum),
- oddaljen dostop KVM s polno funkcionalnostjo tudi na OS nivoju.

Garancijski rok za ponujeno opremo je 36 mesecev. Ponudba naj vključuje 36 mesecev servisno podporo s strani proizvajalca za celotno konfiguracijo v režimu: popravilo v roku 6 ur. Podpora mora biti vidna v sistemu proizvajalca.

4. Nadgradnja diskovnega podsistema HPE 3PAR 8200 - Ljubljana | **1**

Komplet

K2P89B	HPE 3PAR 8000 1.92TB SAS SFF (2.5in) SSD with All-inclusive Single-system Software	16	kos
716197-B21	HPE External 2.0m (6ft) Mini-SAS HD 4x to Mini-SAS HD 4x Cable	2	kos
E7Y71A	HPE 3PAR StoreServ 8000 SFF(2.5in) Field Integrated SAS Drive Enclosure	1	kos
H7J36A3	HPE 3Y Foundation Care CTR SVC	1	kos
H7J36A3 X8J	HPE 3PAR 8000 1.92TB+SW SFF SSD Supp	16	kos
H7J36A3 YTJ	HPE 3PAR 8000 Drive Encl Support	1	kos

5. Nadgradnja diskovnega podsistema HPE 3PAR 8200 - Maribor | **1**

Komplet

K2P89B	HPE 3PAR 8000 1.92TB SAS SFF (2.5in) SSD with All-inclusive Single-system Software	16	kos
H7J36A3	HPE 3Y Foundation Care CTR SVC	1	kos
H7J36A3 X8J	HPE 3PAR 8000 1.92TB+SW SFF SSD Supp	16	kos

6. Nadgradnja diskovnega podsistema HPE 3PAR 8200 - Ljubljana in Maribor | **4**

H6Z00A	HPE 3PAR StoreServ 8000 4-port 16Gb Fibre Channel Adapter	4	kos

Vzdrževanje v času veljavnosti garancije za mrežno in varnostno opremo:

Garancija in podpora proizvajalca celotne opreme za obdobje 3 let z možnostjo eskalacije reševanja okvare neposredno pri proizvajalcu opreme. Vključeni morajo biti originalni rezervni deli proizvajalca. Vključen mora biti dostop do novih verzij mikrokode (firmware) in ostale sistemske programske opreme za ponujeno opremo pri proizvajalcu opreme.

Lot 3: nadgradnja ter nakup programske licence (Cisco, Oracle in centralni zbiralnik logov in korelacijo dogodkov)

1. Nakup dodatnih licenc za licenčno programsko opremo Oracle | **Količina**

1 komplet

Programska oprema	**Število licenc**
ORACLE DATABASE ENTERPRISE EDITION - PROCESSOR PERPETUAL	2
ORACLE DIAGNOSTICS PACK - PROCESSOR PERPETUAL	2

ORACLE TUNING PACK - PROCESSOR PERPETUAL	2
ORACLE AUDIT VAULT AND DATABASE FIREWALL - PROCESSOR PERPETUAL	2

Zajeto mora biti letno vzdrževanje ponujenih Oracle licenc- Software Update License & Support za prvo leto:

- nove verzije (posodobitve) programske opreme,
- popravke programske opreme, varnostna opozorila,
- navodila in postopke za nadgradnjo programske opreme,
- certificiranje za večino novih proizvodov/različic drugih proizvajalcev,
- večje izdaje programov in tehnologij, kar obsega splošne vzdrževalne, izdaje določenih funkcij in posodobitve dokumentacije,
- pomoč za storitvene zahtevke 24 ur na dan vse dni v tednu,
- dostop do podpore My Oracle Support (spletni sistemi za podporo strankam, ki so na voljo 24 ur na dan vse dni v tednu), vključno z možnostjo spletne prijave storitvenih zahtevkov

2. Nakup centralni zbiralnik logov in korelacijo dogodkov - SIEM	**Količina**
1) Zahteve za administracijo in konfiguracijo sistema a) Zagotovljeno mora biti centralno upravljanje vseh komponent z enotnim spletnim vmesnikom. b) Administratorju mora biti omogočeno dodeljevanje upraviteljskih pravic glede na omrežja in skupino naprav. c) Zagotovljeno mora biti avtomatsko prepoznavanje vseh IT gradnikov. d) Zagotovljena mora biti avtomatska detekcija sprememb v konfiguraciji posameznih IT gradnikov. e) Zagotovljena mora biti prilagoditev komunikacijskih vrat (portov) med posameznimi komponentami rešitve. f) Omogočena mora biti integracija ponujene rešitve preko standardnih (API) vmesnikov. g) Omogočena mora biti kriptirana komunikacija med komponentami ponujene rešitve. h) Zagotovljena mora biti integracija s sistemi za razpoznavanje uporabnikov (LDAP, SAML). i) Ponujena rešitev mora omogočati integracijo in nove funkcionalnosti z rešitvami istega ter tudi drugih proizvajalcev, ki bodo združljive s ponujeno rešitvijo. j) Izvajalec mora v ponudbo vključiti vso programsko opremo (tudi morebitne dodatne licence), ki je potrebna za izpolnjevanje vseh zahtevanih funkcionalnosti in delovanje ponujene rešitve. k) V primeru povečanja števila naprav in dogodkov mora biti zagotovljena možnost razširitve ponujene rešitve. Zagotovljena mora biti avtomatska nadgradnja varnostnih pravil s strani proizvajalca rešitve. l) Zagotovljeni morajo biti avtomatski postopki za varnostno kopiranje podatkov. m) Zagotovljen mora biti nadzor nad komponentami rešitve in obveščanje v primeru napak. n) V podatkovno zbirko gradnikov se morajo zapisovati vse bistvene informacije o posameznem gradniku (mrežni atributi, sistemski atributi, ranljivosti). Omogočen mora biti tudi ročen vpis atributov. o) Dostop do aplikacijske trgovine z brezplačno in plačljivo dodatno vsebino (kot npr. pravila za zaznavo novih groženj, dodatki drugih proizvajalcev).	**1 komplet**

2) Arhitekturne zahteve

   a) Ponujena rešitev se mora implementirati kot virtualna naprava, nameščena v virtualizacijsko okolje naročnika (vmWare). V kolikor to ponudnik te zahteve ne more izpolniti, mora ponuditi vso potrebno namensko strojno in programsko opremo, ki bo gostila ponujeno rešitev v modelu visoke razpoložljivosti.
   b) Integriteta shranjenih podatkov mora biti zagotovljena z uporabo SHA-256 algoritma ali višje.
   c) Zagotovljeno mora biti sprejemanje vsaj 4.000 dogodkov na sekundo (angl. EPS – Event per Second) in 30.000 mrežnih tokov na minuto (angl. FPM – Flows per Minute) ali primerljivo brez dodatnih strojnih ali programskih modulov.
   d) Shranjevanje količine podatkov o dogodkih ne sme biti licenčno omejeno.
   e) Rešitev mora biti nadgradljiva z dodatnimi licencami na vsaj 10.000 dogodkov na sekundo in 150.000 mrežnih aktivnosti.
   f) Ponujena rešitev mora omogočati shranjevanje podatkov o dogodkih na diskovni sistem.

3) Zahteve za upravljanje varnostnih dogodkov in informacij

   a) Ponujena rešitev mora omogočati kratkoročno (on-line) in dolgoročno (off-line) hrambo dogodkov.
   b) Zagotovljena mora biti dolgoročna hramba na zunanjih sistemih za shranjevanje podatkov.
   c) Zagotovljena mora biti kompresija hranjenih podatkov najmanj v razmerju 6:1 (dokazila principala).
   d) Zbiranje dogodkov mora biti zagotovljeno najmanj v obliki kot Syslog, JDBC, SNMP, MS-RPC.
   e) Zbiranje dogodkov mora biti podprto za Microsoft SQL Server podatkovno zbirko.
   f) Omogočeno mora biti zbiranje dogodkov neposredno iz tabel podatkovnih zbirk in CSV datotek.
   g) Za zbiranje dogodkov ni zahtevana namestitev agentov.
   h) Zbiranje varnostnih dogodkov mora biti podprto najmanj za strežnike z operacijskim sistemom Windows in Linux.
   i) Upravljanje virov (Asset management).
   j) Vgrajena funkcionalnost analize uporabnikov UBA (User Behaviour Analytics), z možnostjo prilagajanja pravil in uporabe umetne inteligence (Machine learning), za pomoč pri zaznavi anomalij brez dodatnih licenc.
   k) Vgrajena funkcionalnost analitike DNS prometa, ki omogoča zaznavo DGA (Domain Generation Algorithms) in Squatting domen (v kolikor mora ponudnik za to vključiti dodatne licence, morajo biti le-te vključene v ponudbo);
   l) možnost integracije skenerja za ranljivosti;
   m) možnost integracije s sistemom zlonamernih zunanjih IP naslovov;

4) Normalizacija in kategorizacija dogodkov ter analitika

   a) Zagotovljeno mora biti razvrščanje in normalizacija dogodkov.
   b) Omogočeno mora biti avtomatsko prepoznavanje polj v standardiziranem (npr. JSON, LEEF, CEF) formatu.

c) Omogočena mora biti hramba izvornih in normaliziranih podatkov. d) Zagotovljena mora biti normalizacija in kategorizacija, ki bo prilagojena zahtevam uporabnika. e) Analiza in upravljanje dogodkov se mora izvajati v realnem času. f) Vgrajena mora biti prediktivna analitika in prikaz trendov. g) Omogočena mora biti agregacija in analitika dogodkov glede na različne filtre. h) Uporabniški vmesnik mora omogočati iskanje izvora dogodka. i) Pregled dogodkov in filtriranje morata biti omogočeni v realnem času. j) Ob prepoznanih anomalijah in varnostnih dogodkih mora biti omogočeno obveščanje ter alarmiranje. k) Zagotovljena mora biti revizijska sled uporabnikov administracijskega vmesnika. l) Ponujena rešitev mora imeti možnost nadgradnje z integriranim modulom za zajemanje mrežnega prometa in generiranjem obogatenega toka podatkov na mrežnem aplikacijskem nivoju. 5) Korelacija, alarmiranje in poročanje a) Zagotovljeno mora biti poročanje in izdelava poročil po meri. b) Zagotovljena mora biti avtomatska priprava poročil po urniku. c) Zagotovljene morajo biti predloge za poročila in kreiranje uporabniških predlog po meri. Poročila morajo biti skladna z ISO27001/27002 in CoBIT. d) Priprava poročil mora biti omogočena v najmanj naslednjih formatih: XML, CSV, RTF in PDF. e) Zagotovljena mora biti korelacija med posameznimi varnostnimi dogodki. f) Alarmiranje mora biti s pomočjo pravil prilagodljivo glede na zahteve uporabnika. g) Zagotovljena mora biti prioritizacija dogodkov ter določanje nivoja resnosti posameznega varnostnega dogodka. h) Zagotovljeno mora biti pošiljanje alarmov na druge sisteme preko SNMP, MAIL in Syslog protokolov. i) Sistem mora omogočati pošiljanje SMS sporočil in integracijo z zunanjimi sistemi za upravljanje incidentov. j) Omogočeno mora biti določanje lažnih alarmov (False Positive). k) V primeru ponavljajočih se dogodkov mora biti omogočeno omejevanje števila alarmov. l) Zagotovljena mora biti integracija z drugimi sistemi za odkrivanje anomalij in ranljivosti. m) Zagotovljena mora biti korelacija med dogodki iz različnih virov in sistemov. n) Posamezni gradniki IT sistemov (strežniki baz podatkov, DNS strežniki, poštni strežniki, ...) morajo biti avtomatsko prepoznani in klasificirani. 6) Upravljanje aktivnosti omrežja a) Zagotovljeno mora biti upravljanje mrežnega prometa (NetFlow, IPFIX in sFlow) iz mrežnih naprav v izvorni obliki. b) Zagotovljena mora biti prepoznava aplikacij (port in protokol). c) Zagotovljena mora biti prepoznava DoS in DDoS napadov. d) Zagotovljeno mora biti razvrščanje prometa po IP in Subnet območju. e) Zagotovljena mora biti prepoznava tveganih aplikacij. Na voljo morajo biti pravila za prepoznavo tveganih aplikacij.	

f) Zagotovljeno mora biti agregiranje in profiliranje prometa vsaj za število paketov in analitika po posameznih atributih (port, protokol, TCP flags). g) Administratorju mora biti omogočena izdelava različnih pogledov po meri glede na lastnosti virov, toka, prometa itd. h) Zagotovljeno mora biti zbiranje celotnega omrežnega prometa – PCAP in njegova analiza. i) Omogočena mora biti integracija s storitvenimi centri. j) Pogled posameznega varnostnega incidenta mora vsebovati vse relevantne podatke in povezane dogodke. k) Zagotovljeno mora biti hranjenje vseh aktivnosti povezanih s posameznim varnostnim incidentom. 7) Podpora proizvajalca za obdobje 36 mesecev od prevzema licenčne opreme a) Podpora proizvajalca mora obsegati naslednje storitve i) diagnosticiranje okvar na zahtevo, ii) dobavo in nameščanje popravkov za vso sistemsko programsko opremo, iii) dostop do popravkov, nadgradenj in novih verzij sistemske in nadzorne programske opreme pri proizvajalcu opreme, iv) dostop do baze znanja pri proizvajalcu opreme, o tehnična podpora pri proizvajalcu opreme, o pomoč pri reševanju problemov povezanih z instalirano opremo, o odpiranje problemov in spremljanje odprtih problemov 24/7 pri proizvajalcu, v) izvajalec mora imeti za potrebe reševanja problemov naročnika omogočen dostop do baz znanja pri proizvajalcu. b) Izvajanje podpore proizvajalca: i) Čas za odpravo kritične napake (bistvena degradacija sistema oziroma izpad spremljanja več kot 50 % lastnosti naprav): 24 ur, ii) Čas za odpravo nekritične napake je 3 delovne dni, iii) Izvajalec mora imeti zagotovljeno možnost prijave napak v režimu 24/7 preko spletnega portala ali elektronske pošte.	
3. Nadgradnja licence za Cisco usmerjevalnike	**Količina**
Licence za oddaljene usmerjevalnike: DNA licence (L-LIC-DNA-ADD) za usmerjevalnike ISR4331/k9 ki omogočajo uporabo sledečih funkcionalnosti: • Skupna licencirana prepustnost usmerjevalnika 200Mbit/s oz. 100Mbit/s v eno smer (DNA-P-100M-A), • administracijo usmerjevalnika z Cisco On-Prem postavitvijo, • nadgradnja usmerjevalnika mora omogočati ločeno kontrolo, upravljalnje in podpira postavitev visoke razpoložljivosti, • možna uporaba vsaj 10 virtualnih usmerjevalnih instanc (VRF) in pripadajočih privatnih omrežij (VPN),	**30**

• uporaba naprednih usmerjevalnih protokolov (nastavljanje QoS po tunelu, usmerjanje na osnovi aplikacij, podpora definiciji aplikacij po meri, podpora MPLS L2 in L3 VPN), • uporaba naprednih varnostnih orodij (Malware protection, URL Filtering, SSL proxy), • uporaba naprednih analitičnih orodij za globoki vpogled v delovanje lokacij, aplikacij, kakovost izkušnje in porabo pasovne širine (npr. vAnalytics). Podpora licence se kupuje za obdobje 36 mesecev.	
Licence za centralne usmerjevalnike: DNA licence (L-LIC-DNA-ADD) za usmerjevalnike ASR1001-X ki omogočajo uporabo sledečih funkcionalnosti: • Skupna licencirana prepustnost usmerjevalnika 5Gbit/s oz. 2,5Gbit/s v eno smer (DNA-P-2.5G-A), • administracijo usmerjevalnika z Cisco On-Prem postavitvijo, • nadgradnja usmerjevalnika mora omogočati ločeno kontrolo, upravljanje in podpira postavitev visoke razpoložljivosti, • možna uporaba vsaj 10 virtualnih usmerjevalnih instanc (VRF) in pripadajočih privatnih omrežij (VPN), • uporaba naprednih usmerjevalnih protokolov (nastavljanje QoS po tunelu, usmerjanje na osnovi aplikacij, podpora definiciji aplikacij po meri, podpora MPLS L2 in L3 VPN), • uporaba naprednih varnostnih orodij (Malware protection, URL Filtering, SSL proxy), • uporaba naprednih analitičnih orodij za globoki vpogled v delovanje lokacij, aplikacij, kakovost izkušnje in porabo pasovne širine (npr. vAnalytics). Podpora licence se kupuje za obdobje 36 mesecev.	**2**

Storitve implementacije za Lot 1, Lot 2 in Lot 3

Storitve implementacije za Lot 1,Lot 2 in Lot 3 vključujejo sledeče storitve:

- Vgradnja celotne opreme v naročnikovo okolje, namestitev povezovalnih kablov.
- Zagon in osnovna nastavitev opreme in nadgradnje na najnovejšo priporočeno različico operacijskega sistema.
- Izdelava priključitvene dokumentacije.
- Prenos znanja za novo opremo na naročnika in obstoječega vzdrževalca IT infrastrukture.

Ponudnik s spodnjim podpisom potrjuje strinjanje s specifikacijo oz. tehničnimi zahtevami naročnika.

Kraj in datum: *Žig in podpis ponudnika:*