

DRUŽBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI
DARS d.d.

POGLAVJE 2

PROJEKTNA NALOGA

za

Vzpostavitev OT systemske platforme (POT)

(int. ev. št. 000299/2025)

I. PROJEKTNA NALOGA

Pojmovnik

IT – Informacijska tehnologija. Namenjena je podpori poslovanja DARS in standardnih poslovnih procesov. Vključno z običajnimi namiznimi delovnimi postajami.

OT – Operativna tehnologija. Namenjena je podpori specifičnih procesov DARS, ki vključuje tudi namensko strojno in programsko opremo. Predvsem so to sistemi za podporo nadzoru in vodenju prometa na cestah v upravljanju DARS, kateremu je podrejen tudi režim delovanja opreme (kritična infrastruktura).

Platforma OT – Platforma namenjena priklopu namenske strojne opreme okolja OT in namestitvi namenske aplikativne programske opreme sistemov nadzorov in vodenja prometa DARS.

PAM – Privileged Account Management. Sistem za upravljanje dostopov in privilegiranih računov.

MAF – Manufacturer Authorization Form – Zagotovilo za polno podporo vgrajeni opremi s strani proizvajalca za celoten čas vzdrževanja.

Namen investicije (javnega naročila)

Namen investicije je zagotoviti enotno infrastrukturno platformo, ki bo zagotavljala varno okolje za delovanje storitev OT DARS.

Obseg investicije

Investicija obsega:

- Vzpostavitev platforme za upravljanje virtualnih strežnikov, ki jo je možno nadgraditi tudi za upravljanje programskih kontejnerjev.
- Nakup strežniške strojne in sistemske programske opreme za lokacije, kjer je potrebno avtonomno delovanje (LNC) in za centralno nadzorno lokacijo (GNC).
- Nakup omrežne opreme za vzpostavitev varnega hrbteničnega omrežja in omrežnih vozlišč OT platforme z vsemi potrebnimi mehanizmi zagotavljanja visoke razpoložljivosti.
- Nakup požarnih pregrad za varno avtonomno delovanje lokacij OT.
- Nakup sistema za izdelavo varnostnih kopij in učinkovito restavracijo podatkov.
- Vzpostavitev centralnih sistemskih storitev za okolje OT.
- Namestitev sond in drugih mehanizmov za spremljanje stanja in zaznavo neobičajnih dogodkov v sistemu.
- Vzpostavitev upravljaljskega in nadzornega sistema za upravljanje omrežja in varnostnih mehanizmov omrežja.

- Vzpostavitev upravljalškega in nadzornega sistema za upravljanje strežniške strojne opreme.
- Vzpostavitev centralnega nadzornega sistema za celotno platformo.
- Paralelno delovanje starega in novega okolja OT do zaključka projekta.
- Prehod med IT in OT okoljema samo preko nadzorovanih stičnih točk.
- Integracija vse dobavljene strojne in programske opreme v varno delujočo celoto.
- Vzdrževanje v projektu vzpostavljenega okolja.

Iz investicije je izvzeto:

- Lokalne Postaje (LP) z operacijskim sistemom RTOS.
- Vsa oprema in mrežne povezave do krmiljene strojne opreme (zasloni, senzorji, ...), ki se krmili preko LP.
- Nastavitve obstoječega IT okolja.
- Vzpostavljanje optičnih vlaken med lokacijami.
- Gradbena dela.
- Napeljevanje dovodnih kablov.

Potek investicije

Z izgradnjo nove platforme OT bo vzpostavljeno varnejše in bolj zanesljivo okolje za izvajanje informacijskih storitev DARS. Investicija bo potekala kot oddvojitev OT infrastrukture iz že delujočega obstoječega okolja IT. Zaradi kritičnosti procesov, ki jih nadzorni sistemi podpirajo, mora prehod povzročati čim manj motenj v rednem delovanju DARS. V skladu z zmožnostmi naročnika se bo postopoma izvajal prenos iz starega IT okolja, na novo platformo OT. Izvajal se bo tako prenos aplikacij, kot prenos mrežnih segmentov. Paralelno delovanje stare in nove platforme bo potekalo do končnega prehoda na novo platformo OT, zato mora biti nova oprema kompatibilna z obstoječim OT okoljem DARS, ki temelji na mrežni opremi proizvajalca Cisco.

Po izbiri izvajalca, se bo med uvedbo v delo, identificiralo najbolj kritične gradnike in pripravila časovnica njihove uvedbe. Posamezne module se bo vgrajevalo skladno z možnostmi naročnika za njihovo uvedbo.

Obstoječe stanje

Sistem obsega množico strežnikov, kjer tečejo različne virtualizacijske platforme ali pa strežniki delujejo samostojno z ločenimi upravljalškimi vmesniki in upravljavci. Kritični sistemi so v različnih redundantnih konfiguracijah.

Vsaka lokacija ima zaradi različnih časovnih obdobij uvedbe specifike iz časa uvedbe, kar znatno otežuje vzdrževanje.

Vzpostavljene so že nekatere centralne sistemske storitve, ki pa bodo morale biti prenovljene. Proces ločevanja OT in IT omrežja ni bil nikoli izveden v celoti.

IT omrežje je v celoti zgrajeno na tehnologijah proizvajalca Cisco. OT omrežje za industrijsko vgrajene komponente uporablja tudi industrijsko opremo proizvajalcev MOXA in AlliedTelesyn.

Omrežje je zgrajeno na sledečih tehnologijah:

- VRF
- IP/MPLS
- 802.1Q
- Tehnologija prilagojena za OT industrijska okolja
- Turbo ring

Vsebuje sledečo redno vzdrževano strojno opremo:

- Usmerjevalnike Cisco NCS/ASRIST/IR
- LAN Stikala Cisco Catalyst
- Industrijska stikala Moxa in Cisco IE
- Stikala podatkovnega centra Cisco Nexus
- Avtentikacijski sistem Cisco ISE
- Cisco požarne pregrade

Pasivna infrastruktura

Naročnik ima v lasti optično omrežje do vseh lokacij. Razvodi omogočajo redundanco povezljivosti med lokacijami. Kjer redundanca na ravni optičnega omrežja ni možna, naročnik poskrbi za redundantno povezavo, za kar se lahko uporabi mobilno omrežje z lastnim APN ali druge najete vode.

Druge tehnologije naročnika

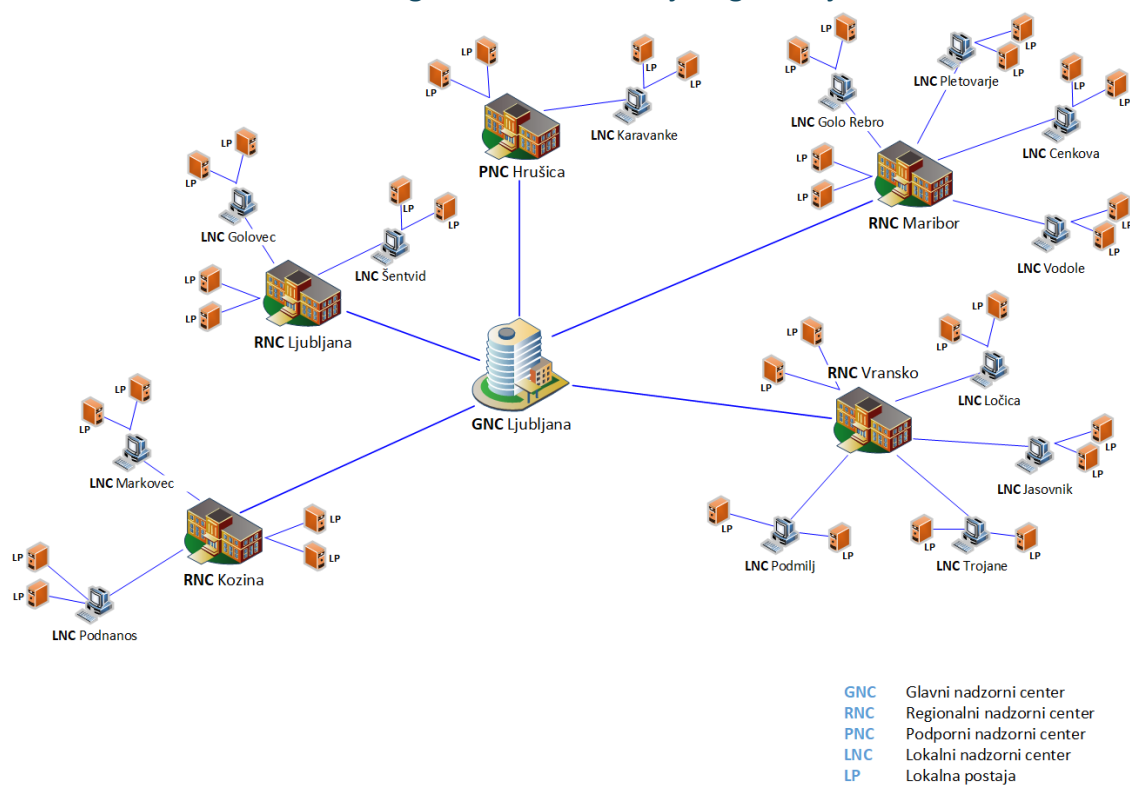
Druge tehnologije v okolju naročnika so tiste, ki jih naročnik že uporablja, vendar ne bodo integrirane z opremo dobavljeno v tem projektu. Kljub temu je v interesu naročnika, da je upravljanje opreme čim bolj poenoteno.

Osebe naročnika je že usposobljeno in upravlja virtualno okolje, ki je v celoti virtualizirano s tehnologijo VMWare.

Sistem varnostnega kopiranja je izveden na tehnologiji Veeam.

V trenutni konfiguraciji se uporabljajo mobilne storitve ponudnika Telemach (redundantna APN povezave), ki pa se lahko v času trajanja projekta spremeni.

Logična shema obstoječega stanja



Slika prikazuje logično shemo vseh gradnikov, ki jih prenavljamo. Ne vsebuje dejanskih fizičnih povezav, kot tudi ne prikazuje dejanske porazdeljenosti za potrebe visoke razpoložljivosti.

LP (Lokalna postaja) je samo element, ki se bo priključil v novo platformo kot mrežni odjemalec. LP je element spodnjega nivoja, ki se z uvedbo OT platforme ne spreminja. Spreminja pa se arhitektura omrežja, ki prenaša podatke, ki jih pošiljajo ali sprejemajo LP.

Tehnične zahteve

Tehnične zahteve za OT platformo vsebujejo opise modulov, ki jih bodo morali ponudniki ovrednotiti v predračunih. Moduli so zgrajeni iz standardnih gradnikov, ki so podrobno opisani v tehničnih specifikacijah tega naročila. Poleg standardnih gradnikov tehnične specifikacije opisujejo tudi namensko opremo, potrebno za zaključeno vzpostavitev OT platforme.

Izhodišča uporabnosti posameznih modulov so:

GNC

Glavni Nadzorni Center vsebuje vse jedrne storitve platforme. Postavitev je distribuirana na dveh neposredno povezanih aktivnih lokacijah in kot tretja lokacija za potrebe okrevanja. Jedrne storitve vključujejo centralno požarno pregrado, varnostne storitve, centralne usmerjevalnike, potrebne strežniške zmogljivosti, varnostne kopije, ...

Centralne sistemske storitve, ki jih mora ponudnik vzpostaviti na sistemu, obsegajo sledeče storitve:

Naziv	Komentar
Active directory	
DNS	Integrirano v AD
DHCP	Integrirano v AD
CA	Integrirano v AD
802.1x	
WSUS	Nameščanje popravkov za Windows okolje
PAM	Samostojna postavitve za potrebe OT
Krmiljenje vseh elementov omrežja	
Krmiljenje flote fizičnih strežnikov	
Strežniki za dostavljanje popravkov in drugih datotek	Jump strežniki za Linux distribucije ali druge ponudnike programske opreme
Datotečni strežniki	Datotečni strežniki lokalnega omrežja
Zbirnik in analizator podatkov varnostnih sond	
Sistem za upravljanje z identitetami in avtorizacijami uporabnikov omrežja	
Sistem za nadzor delovanja celotnega sistema	Odzivnost aplikacij, razpoložljivi viri, ...
Upravljanje virtualnega okolja VMWare	VMCenter
Backup	

RNC

Regionalni Nadzorni Center predstavlja zaključeno enoto, kjer so nameščeni uporabniki in njihova oprema, ki pridobivajo podatke iz LNC. Zato je od platforme OT nameščena samo komunikacijska oprema. Zagotavlja varno delovno okolje in nadzorovane povezave do kritičnih sistemov v LNC. RNC je vpet v MPLS hrbtenico, ki zagotavlja ustrezno raven redundance.

LNC

Lokalni Nadzorni Center predstavlja kritično avtonomno delujočo enoto, ki vsebuje vse potrebne vire in varnostne elemente za varno delovanje v vseh pogojih. Vključno z izpadom povezav do drugih lokacij platforme. V normalnem načinu delovanja zagotavlja procesiranje vseh podatkov, potrebnih za učinkovito vodenje in nadzor prometa, v izrednih razmerah pa tudi za avtonomno upravljanje preko delovnih postaj ob prisotnosti uporabnikov na sami lokaciji. Večina procesnih podatkov, ki jih platforma OT obdeluje, nastaja na opremi priključeni na LNC.

Skupne zahteve za opremo, ne glede na namestitev ali modul so:**Strežniška oprema**

Strežniška oprema vsebuje strežnike za virtualno okolje na posameznih lokacijah. Zaradi porazdeljenosti po lokacijah temelji arhitektura na Hyper Converged konceptu, saj bi bilo drugače potrebnih preveč diskovnih sistemov. Edini diskovni sistem je predviden samo za hrambo varnostnih kopij.

Vsi dobavljeni strežniki morajo biti podprti in dobavljeni s strani enega proizvajalca. Arhitektura virtualizacijske platforme mora temeljiti na konceptu »Hyper Converged«, ki omogoča skalabilnost procesorskih, spominskih ali kapacitet za hrambo podatkov na ravni dodajanja in odvzemanja vozlišč (node). Vsa vozlišča morajo biti za ponujeno konfiguracijo sistemske programske opreme certificirana s strani proizvajalca ponujene virtualizacijske programske opreme VMWare, ki jo naročnik že uporablja v obstoječem okolju.

Zagotovljeno mora biti centralizirano upravljanje celotne konfiguracije iz ene konzole s strani različnih upravljavcev z različnimi ravnmi pravic do ravni posameznega vira in posameznega virtualnega strežnika.

Nad vso strojno strežniško opremo mora biti vzpostavljen nadzor na daljavo (kot npr. iDrac, iLO, XCC, ...). Vključno s posodabljanjem strojne kode (firmware), priklopom prenosnih medijev na daljavo in upravljanjem zaslona na daljavo. Dostop do nadzornih modulov strežnikov mora biti centraliziran preko ene vstopne točke, kjer se tudi zbirajo alarmi, obvestila o posodobitvah in omogoča neposredno upravljanje fizičnih strežnikov (kot npr. Dell Open Manage Enterprise, HP One View, XClarity Controller...).

Vsi delovni strežniki se organizirajo v več enotno upravljanih gruč VMWare, ki lahko v primeru izpadov povezav avtonomno delujejo na posameznih lokacijah.

Mrežna oprema

Mrežna oprema vključuje, stikala, usmerjevalnike, požarne pregrade, upravljavsko programsko opremo in varnostne rešitve za nadzor vgrajene opreme in omrežja. Vsa dobavljena mrežna oprema mora biti dobavljena in podprta s strani enega proizvajalca. Zmogljivosti morajo zagotavljati primerno propustnost, kot tudi odzivnost omrežja za potrebe »Hyper Converged« arhitekture na posameznih lokacijah, kot tudi prenos podatkov vseh sistemov, ki bodo komunicirali preko platforme OT.

Potrebno je zagotavljati tako avtonomnost delovanja omrežja na ravni LNC v primeru izpadov povezljivosti, kot tudi redundanco na ravni MPLS povezljivosti.

Omrežje OT platforme mora vključevati nadzorno programsko opremo proizvajalca s sledečimi funkcionalnostmi:

- Inventar vse opreme

- Verzije programske opreme
- Alarmiranje
- Zagotovljene nove verzije programske opreme za ves čas vzdrževanja/garancije
- Shranjevanje varnostnih kopij konfiguracije
- Restavriranje konfiguracije iz varnostne kopije
- Avtomatizacija vzdrževalnih opravil in vključitve nove mrežne opreme v konfiguracijo
- Strojna oprema mora biti na zahtevanih mestih kompatibilna s programsko opremo za zaznavanje anomalij na omrežju. Zmogljivosti morajo biti v skladu z navodili proizvajalca strojne in programske opreme za nemoteno delovanje.

Omrežje OT platforme sestavljajo sledeči gradniki:

MPLS usmerjevalniki Tip 1 – Večja vozlišča

Modularna platforma, zasnovana za zagotavljanje varnega, prilagodljivega in zanesljivega omrežja v zahtevnih okoljih. Zahtevana je modularna arhitektura, ki omogoča fleksibilnost pri podpori različnih vmesnikov in storitev, kar naročniku omogoča prilagoditev naprave njihovim potrebam v prihodnosti. Platforma mora podpirati napredne funkcionalnosti za usmerjanje, varnost in avtomatizacijo, vključno z MACsec šifriranjem z linijsko hitrostjo vmesnika, MPLS, Segment Routing in SRv6, MP-BGP in VRF. Zagotavljati mora podporo avtomatiziranemu upravljanju.

MPLS usmerjevalniki Tip 2 – Preostala vozlišča

Fiksna platforma, zasnovana za zagotavljanje varnega, prilagodljivega in zanesljivega omrežja v zahtevnih okoljih. Zahtevana je fiksna arhitektura, ki omogoča fleksibilnost pri podpori različnih vmesnikov in storitev, kar naročniku omogoča prilagoditev naprave njihovim potrebam v prihodnosti. Platforma mora podpirati napredne funkcionalnosti za usmerjanje, varnost in avtomatizacijo, vključno z MACsec šifriranjem z linijsko hitrostjo vmesnika, MPLS, Segment Routing in SRv6, MP-BGP in VRF. Zagotavljati mora podporo avtomatiziranemu upravljanju.

Jedrna stikala

Fiksna platforma za lokalna omrežja, zasnovana za zagotavljanje varne, hitre in zanesljive povezljivosti v okolju z veliko uporabniki, napravami in aplikacijami. Podpirati mora ključne funkcionalnosti sodobnih lokalnih omrežij, kot so VRF, BGP, OSPF, IS-IS, napredne mehanizme segmentacije in integracijo z omrežjem WAN. Omogočati mora vzpostavitev v podvojenem načinu. Podpora MACsec šifriranju z linijsko hitrostjo vmesnika ter napredni telemetriji za proaktivno spremljanje delovanja. Zagotavljati mora podporo avtomatiziranemu upravljanju.

Dostopovna stikala

Fiksna platforma za lokalna omrežja, zasnovana za zagotavljanje varne, hitre in zanesljive povezljivosti v okolju z veliko uporabniki, napravami in aplikacijami. Podpirati mora ključne

funkcionalnosti sodobnih lokalnih omrežij, kot so VRF, BGP, OSPF, IS-IS napredne mehanizme segmentacije. Podpora varnostnim mehanizmom 802.1x, razširitvam in varnostnim dodatkom protokola STP . Omogočati mora vzpostavitev v podvojenem načinu. Podpora MACsec šifriranju z linijsko hitrostjo vmesnika ter napredni telemetriji za proaktivno spremljanje delovanja. Zagotavljati mora podporo avtomatiziranemu upravljanju.

Stikala za potrebe nadzornega sistema

Fiksna platforma za OOB (out-of-band) upravljanje omrežij, zasnovana za zagotavljanje varne, hitre in zanesljive povezljivosti do upravljaljskih vmesnikov omrežnih naprav v podatkovnem centru in poslovnem omrežju.

Upravljalni in nadzorni sistem za lokalna omrežja

Virtualizirana upravljaljska in nadzorna platforma ki omogoča centralizirano upravljanje vseh stikal omrežja. Zagotavljati mora avtomatizacijo ključnih procesov, kot so dodajanje naprav, konfiguriranje in posodabljanje programske opreme. Platforma mora omogočati stalno preverjanje skladnosti konfiguracij z vnaprej določenimi politikami ter avtomatizirano odpravljanje odstopanj. Administratorju omrežja mora omogočati napredne funkcionalnosti za odkrivanje anomalij v omrežju in spremljanje varnostnih dogodkov.

Hrbtenična stikala podatkovnega centra

Fiksna platforma, zasnovana za zagotavljanje visoko zmogljive, varne in zanesljive hrbtenične povezljivosti v podatkovnih centrih. Arhitektura mora omogočati skalabilno delovanje v »leaf and spine« topologijah ter podpira napredne funkcionalnosti za usmerjanje, varnost in avtomatizacijo. Platforma mora zagotavljati podporo za ključne usmerjevalne protokole, kot so BGP, IS-IS, OSPF in EIGRP, ter omogoča varno povezljivost z uporabo MACsec šifriranja. Poleg tega nudi podporo za EVPN VXLAN, kar omogoča učinkovito segmentacijo in razširljivost omrežja. Platforma mora omogočati integracijo s centraliziranimi sistemi za upravljanje podatkovnega centra, kar skrbnikom omogoča avtomatizirano uvajanje, nadzor in optimizacijo omrežja.

Dostopovna stikala podatkovnega centra

Fiksna platforma, zasnovana za zagotavljanje visoko zmogljive, varne in zanesljive povezljivosti na dostopni plasti podatkovnega centra. Stikala predstavljajo povezovalno točko za strežnike, shranjevalne sisteme in druge naprave, hkrati pa zagotavljajo učinkovito povezavo proti spine sloju v »leaf and spine« topologiji. Arhitektura mora omogočati skalabilno delovanje ter podpirati napredne funkcionalnosti za usmerjanje, varnost in avtomatizacijo. Platforma mora zagotavljati podporo za ključne usmerjevalne protokole, kot so BGP, IS-IS, OSPF in EIGRP, ter omogočati varno povezljivost z uporabo MACsec šifriranja. Poleg tega nudi podporo za EVPN VXLAN, kar omogoča učinkovito segmentacijo, razširljivost in povezljivost med virtualiziranimi in fizičnimi delovnimi obremenitvami. Integracija s

centraliziranimi sistemi za upravljanje podatkovnega centra skrbnikom omogoča avtomatizirano uvajanje, nadzor in optimizacijo celotne infrastrukture.

Upravljalni in nadzorni sistem podatkovnega centra

Virtualizirana upravljavska in nadzorna platforma, zasnovana za centralizirano upravljanje vseh stikal v podatkovnem centru, tako hrbteničnih kot dostopnih. Platforma omogoča avtomatizirano vzpostavitev underlay in overlay omrežij, kar bistveno poenostavi uvajanje kompleksnih leaf-spine topologij ter zagotavlja razširljivost in visoko razpoložljivost storitev. Podpira avtomatizacijo ključnih procesov, kot so dodajanje naprav, konfiguriranje in posodabljanje programske opreme, s čimer se zmanjša možnost napak in pospeši uvajanje novih rešitev.

Požarna pregrada Tip 1 – Datacenter pregrada

Zmogljiva požarna pregrada za zaščito robnih delov omrežja z drugimi omrežji. Požarna pregrada ima visoko propustnost, napredne mehanizme zaznave in preprečevanja groženj, ter se lahko upravlja preko centralnega sistema za upravljanje požarnih pregrad.

Zasnovana je za stalno posodabljanje varnostnih podpisov in inteligentnih groženj iz večih virov in omogoča integracijo z nadrejenimi sistemi za upravljanje identitet in dostopa. Upravljanje je omogočeno preko centralnega sistema, ki podpira avtomatizacijo politik, odziv na izredne dogodke in usklajevanje varnostnih pravil.

Požarna pregrada Tip 2 – Lokalna pregrada

Namenjena je zaščiti posameznih odsekov omrežja, ki morajo delovati avtonomno tudi v kritičnih situacijah brez povezave v hrbtenico OT omrežja. Visoka propustnost je zahtevana zaradi video nadzornih sistemov.

Omogoča virtualizacijo požarnih instanc (multi-instance), kar omogoča ločevanje okolij znotraj iste fizične naprave. Naprave se lahko povezujejo v gruče za potrebe redundance ali večje propustnosti. Upravljanje je omogočeno preko centralnega sistema, ki podpira avtomatizacijo politik, odziv na izredne dogodke in usklajevanje varnostnih pravil.

Upravljavski in nadzorni sistem požarnih pregrad

Centralni sistem za upravljanje požarnih pregrad je namenjena centraliziranemu nadzoru, konfiguriranju in spremljanju delovanja varnostnih rešitev v OT omrežju. Omogoča enotno upravljanje vseh nameščenih požarnih pregrad, sistemov za zaznavanje in preprečevanje vdorov, VPN povezav, ter drugih storitev, ki jih izvajajo požarne pregrade.

Avtentikacijski in avtorizacijski sistem za potrebe OT okolja

Centralizirana varnostna rešitev za upravljanje identitet, dostopa in skladnosti v OT omrežju. Omogoča avtentikacijo, avtorizacijo in revizijo za naprave in uporabnike, ter avtomatizirano uveljavljanje varnostnih politik glede na identiteto, lokacijo, vrsto naprave in stanje varnosti.

Upravljavski in nadzorni sistem za spremljanje in zaznavo neobičajnih dogodkov na OT omrežju

Sistem za spremljanje in zaznavo neobičajnih dogodkov na OT omogoča vidljivost v OT omrežju, saj zazna, katalogizira in določi komunikacije in protokole na spremljanih točkah znotraj OT omrežja. To omogoča upravljalcem, da dobijo vidljivost in preglednost nad ključnimi točkami v omrežju.

Sistem uporablja bazo proizvajalca za detektiranje gradnikov in tipov prometa, izvaja analizo prometa, ocenjuje tveganja in omogoča integracijo z drugimi varnostnimi platformami.

Drugim varnostnim platformam zagotavlja potrebne podatke za profiliranje naprav, kot tudi upravljanje varnostnih politik na požarnih pregradah.

Sonde za spremljanje in zaznavo dogodkov v OT omrežju

Sonde za spremljanje in zaznavo dogodkov v OT omrežju zagotavljajo vidnost omrežja, ki jo za svoje delovanje potrebuje sistem za spremljanje in zaznavo neobičajnih dogodkov na OT omrežju. Sonde izvajajo pregled paketov na omrežju v obliki pasivnega spremljanja prometa in zato ne dodaja zakasnitev v komunikaciji in ne posega v industrijske procese. Upravljavskemu sistemu po varni poti pošilja metapodatke o zaznanih dogodkih na omrežju.

Sonde so lahko ali namenske naprave ali programski moduli v mrežnih stikalih.

Splošni pogoji

Vsa dobavljena oprema mora imeti 5 let tovarniške garancije z zagotovljenimi vzdrževalnimi storitvami, če ni v podrobnih tehničnih specifikacijah drugače zahtevano. Za to obdobje morajo biti zagotovljeni rezervni deli in tovarniška vzdrževalna podpora (nadgradnje programske opreme, servisne storitve, ...). Vsi servisni posegi na opremi se izvajajo na mestu vgradnje.

Režim vzdrževanja in podpore je definiran v kasnejšem poglavju.

Usmerjenost ventilatorjev opreme in druge podrobnosti vgradnje, ki ne vplivajo na ceno, se definira ob potrditvi opreme za naročilo.

Ponudnik mora v ponudbi priložiti popis oziroma seznam vse ponujene opreme. Naročnik si pridržuje pravico, da ponudnika pozove k predložitvi dokumentacije, ki dokazuje izpolnjevanje podrobnih tehničnih zahtev (te so določene od strani 19 te projektne naloge naprej).

Oprema GNC

Modul GNC se sestoji iz sledečih gradnikov, ki so podrobneje opisani v detajlni tehnični specifikaciji.

Strojna oprema

Količina	Naziv	Komentar
12	Zmogljiv strežnik	S.1.1
4	MPLS usmerjevalnik Tip 1	M.1.1
4	Hrbtenično stikalo podatkovnega centra	M.1.6
6	Dostopovno stikalo podatkovnega centra	M.1.7
4	Požarna pregrada Tip 1	M.2.1
4	Jedrno stikalo	M.1.3
3	Stikalo za potrebe nadzornega sistema	M.1.5
2	Backup strežnik	S.1.3
2	Backup shranjevalni sistem	S.1.4
300	Backup programska oprema	P.1.1 Licenciranje po virtualnih strežnikih, ki se backupirajo
2	Sonda za spremljanje in zaznavo dogodkov v OT omrežjih	M.2.3
26	QSFP28 100GBASE Copper 3m	
90	SFP28 25GBASE-SR	
8	SFP+ 10GBASE Copper 3m	
8	SFP28 25GBASE Copper 3m	
12	QSFP 100G, 80km	
8	QSFP 100G, 10km	

Strežniška oprema v GNC mora v hyper converged konfiguraciji zagotavljati sledeče zmogljivosti:

- Delovanje kljub izpadu enega strežnika na eni lokaciji. Lahko pride do počasnejšega delovanja zaradi pomanjkanja izpadlih virov.
- V primeru izpada ene lokacije GNC, morajo vse informacijske storitve delovati nemoteno.
- Namestitev aktivne konfiguracije na dveh lokacijah
- Tretja pasivna lokacija za potrebe okrevanja

Upravljanje varnostnih kopij

Za potrebe zagotavljanja varnostnih kopij sistema mora biti zagotovljen neodvisni shranjevalni sistem, strežnik za programsko opremo in programska oprema za izvajanje varnostnih kopij z enako opremo in enakimi funkcionalnostmi na dveh lokacijah modula GNC.

Sistem varnostnih kopij bo centraliziran in bo izvajal kopiranje na primarno in sekundarno varnostno kopijo z vseh lokacij, ki bodo povezane v platformo OT. Ravno tako mora omogočati restavrator na poljubno lokacijo v platformi OT.

Sistem za upravljanje varnostnih kopij mora zagotavljati sledeče funkcionalnosti:

- Obstoja kopija (immutable copy) za daljše časovno obdobje .
- Samodejno preverjanje veljavnosti kopij.
- Enkripcija podatkov na shranjevalnih medijih.
- Onemogočeno spreminjanje in brisanje nedotakljivih kopij brez posredovanja več administratorjev hkrati in podpore proizvajalca.
- Zagotovljeno hitro okrevanje iz Flash medijev za celotno okolje.
- Kapaciteta sistema mora poleg hrambe 20 dnevni kopij omogočati tudi hrambo najmanj 14 mesečnih kopij in ene letne kopije.
- Vključeni mehanizmi deduplikacije in kompresije na blokovni ravni.
- Hkratno izvajanje varnostnega kopiranja z večih lokacij.
- Več različnih scenarijev izdelave varnostnih kopij.

Sistem za upravljanje varnostnih kopij bo centraliziran in bo izvajal kopiranje na primarno in sekundarno varnostno kopijo z vseh lokacij, ki bodo povezane v omrežje OT. Ravno tako mora omogočati restavracijo na poljubno lokacijo v omrežju OT.

Mrežna oprema

Mrežna oprema v GNC mora zagotavljati:

- Varno in nadzorovano vstopno točko v omrežje OT iz drugih okolij.
- Varen in nadzorovan prehod iz omrežja OT v druge omrežne segmente DARS.
- Storitve usmerjanja in varovanja mrežnega prometa.
- Upravljanje s pravico dostopa do omrežja.
- Upravljanje z redundantnimi mehanizmi na ravni celotnega sistema.
- Zaznavanje anomalij v omrežju in omrežnem prometu z nameščenimi sondami.
- Prenos podatkov o omrežnem prometu drugim storitvam za odkrivanje anomalij (SOC, SIEM, analizatorji, ...) in omogočanje varnega delovanja.

Centralne sistemske storitve

Centralne sistemske storitve predstavljajo ogrodje za delovanje celotnega segmenta OT. Ponudniki jih ponudite v modulu GNC. Nameščene so na strežnikih v modulu GNC, ki jim na ravni VMWare gruče zagotavlja visoko razpoložljivost. Vse centralne sistemske storitve morajo biti nameščene in povezane v delujočo celoto, ter so del rednega vzdrževanja. Licence za okolje Microsoft zagotovi naročnik na podlagi Enterprise Agreement pogodbe. Ponudnik pa mora zagotoviti vse licence, za spodaj navedene storitve. Storitve lahko temeljijo tudi na odprtokodnih rešitvah, vendar mora ponudnik nuditi podporo v zahtevanem režimu.

Količina	Naziv	Komentar
30 Internih uporabnikov 100 Zunanjih uporabnikov	PAM	Samostojna postavitve za potrebe OT P.1.2
Vsa ponujena stikala, požarni zidovi	Krmiljenje vseh aktivnih elementov omrežja	
Vsi ponujeni strežniki	Krmiljenje flote fizičnih strežnikov	
	Strežniki za dostavljanje popravkov in drugih datotek	Jump strežniki za Linux distribucije ali druge ponudnike programske opreme.
Licence po LNC in RNC modulih	Zbirnik in analizator podatkov varnostnih sond	
	Sistem za upravljanje z identitetami in avtorizacijami uporabnikov omrežja	M.3.6
300 virtualnih strežnikov in dobavljena oprema	Sistem za nadzor delovanja celotnega sistema	Odzivnost aplikacij, razpoložljivi viri, ... P.1.3
	Upravljanje virtualnega okolja VMWare	VMCenter P.1.4
300 virtualnih strežnikov	Backup	P.1.1

Oprema za varovanje celotne konfiguracije obsega sledeče podsisteme:

- Zbirnik in analizator podatkov varnostnih sond.
- Sistem za spremljanje in zaznavo anomalij na omrežju.
- Sistem za upravljanje z identitetami in avtorizacijami uporabnikov omrežja.
- Sistem za upravljanje privilegiranih dostopov (PAM).
- Sistem za nadzor delovanja celotnega sistema (odzivnost aplikacij, razpoložljivi viri, ...).

Oprema RNC

Zahtevana oprema za en modul

Količina	Naziv	Komentar
100	Sistem za spremljanje in zaznavo dogodkov v OT omrežju	Licence po spremljanih napravah
2	MPLS usmerjevalnik Tip 2	M.1.2
2	Jedro stikalo	M.1.3
2	Dostopovno stikalo	M.1.4
1	Administrativno stikalo	M.1.5
2	Požarna pregrada Tip 2	M.2.2
4	QSFP28 10GBASE Copper 3m	
4	SFP+ 10GBASE Copper 3m	

4	SFP28 25GBASE Copper 3m	
4	QSFP 100G, 80km	
2	QSFP 100G, 10km	

Mrežna oprema v RNC mora zagotavljati:

- Varovanje lokacije, kot zaključene celote
- Spremljanje prometa in zaznavanje anomalij
- Identifikacija in avtorizacija mrežnega prometa
- Povezljivost v omrežje OT DARS za vse uporabnike na lokaciji RNC
- Nadzor in upravljanje iz programske opreme nameščene v GNC

Oprema LNC

Zahtevana oprema za 1 modul

Količina	Naziv	Komentar
4	Lokalni strežnik	S.1.2
100	Sistem za spremljanje in zaznavo dogodkov v OT omrežju	Licence po spremljanih napravah
2	MPLS usmerjevalnik Tip 2	M.1.2
2	Jedrno stikalo	M.1.3
2	Dostopovno stikalo	M.1.4
2	Požarna pregrada Tip 2	M.2.2
1	Administrativno stikalo	M.1.5
4	QSFP28 100GBASE Copper 3m	
24	SFP28 25GBASE-SR	
4	SFP+ 10GBASE Copper 3m	
4	SFP28 25GBASE Copper 3m	
3	QSFP 100G, 80km	
2	QSFP 100G, 10km	

Strežniška oprema LNC mora v hyper converged konfiguraciji zagotavljati sledeče zmogljivosti:

- Neprekinjeno delovanje kljub izpadu enega strežnika
- Vsak strežnik mora nemoteno delovati kljub izpadu enega diska, napajalnika ali ventilatorja.
- V primeru izpada povezav do drugih segmentov omrežja mora oprema na vsaki lokaciji LNC delovati avtonomno. Upravljanje informacijske tehnologije, je lahko v času izpada povezav okrnjeno. Lokalne storitve na ravni omrežja in strežnikov za uporabnike pa morajo delovati nemoteno.

Na strežnikih LNC teče programska oprema nadzora in vodenja, ki jih upravljajo operaterji v RNC. Podatki se posredujejo tudi drugim sistemom DARS. Zato je razpoložljivost strežnikov visokega pomena.

Mrežna oprema

Mrežna oprema v LNC mora zagotavljati sledeče funkcionalnosti:

- Avtonomno delovanje lokacije v primeru izpada povezav
- Varovanje lokacije, kot zaključene celote
- Spremljanje prometa in zaznavanje anomalij
- Identifikacija in avtorizacija mrežnega prometa
- Namestitev sond za spremljanje omrežnega prometa in pošiljanje analitičnih podatkov na centralno lokacijo.
- Konfiguracija mora omogočati spremljanje vsega prometa med segmenti na lokaciji LNC.

Na mrežno opremo v LNC se priključuje OT oprema za različne sistema nadzora in vodenja prometa, ki jih uporablja DARS. Prvo procesiranje teh podatkov se praviloma izvaja na strežniški opremi v LNC in se potem posreduje naprej po sistemih DARS.

Storitev vzpostavitve sistema

Izvedbeni načrt

Izvedbeni načrt se sestoji iz dveh dokumentov, ki jih pripravi izvajalec v sodelovanju z naročnikom.

Visokonivojski načrt rešitve (HLD)

Ponudnik mora pripraviti visokonivojski načrt rešitve (HLD), ki bo zajemal arhitekturni pregled celotne rešitve, vključno s ponujenimi komponentami sistema, njihovo vlogo in medsebojnimi povezavami. Dokument mora jasno opredeliti konceptualno zasnovo, ključne funkcionalnosti ter okvirne integracijske točke. Služil bo kot osnova za pripravo podrobnega načrta (LLD) ter izvedbo rešitve.

Z visoko nivojskim načrtom se preda tudi delilnik cen opreme in storitev, ki morajo biti skladne s ponudbenimi vrednostmi.

Stroške vzpostavitve sistemov ponudnik v predračunu vkalkulira v cene posameznih ponujenih modulov.

Podrobni načrt rešitve (LLD)

Ponudnik mora pripraviti podrobni načrt rešitve (LLD), ki bo podrobno opredelil implementacijo posameznih komponent sistema, njihove nastavitve in konfiguracije. Dokument mora vsebovati natančne tehnične specifikacije, topologije, parametre in postopke izvedbe, s čimer bo zagotovljena ponovljivost in skladnost implementacije z visokonivojskim načrtom (HLD). Postopki izvedbe vključujejo analizo obstoječega stanja, pripravo vseh specifikacij za izvedbo, testne scenarije, vključno s potrditvenim testom za vsako zaključeno celoto opreme.

LLD in HLD - podrobni načrt izvedbe uskladi zahteve naročnika in ponujeno opremo. Temelji na časovnici, ki je del tega razpisa in obsega podrobnejše načrte in aktivnosti, ki so potrebne za uspešno uvedbo predmeta naročila v naročnikovem okolju.

V podrobnem načrtu so opredeljene odgovorne osebe za izvedbo, tveganja, ki potrebujejo posebno pozornost in druga pomembna dejstva za uspešno izvedbo. Končna oblika podrobnega načrta je tehnološki elaborat.

Integracija v obstoječe okolje

Mrežna oprema mora zagotavljati polno povezljivost z obstoječim IT/OT okoljem, saj se bo prehod na novo opremo izvajal postopoma. Delovanje celotnega OT okolja (stara in nova konfiguracija) mora zaradi posegov vzpostavitve novega sistema imeti čim krajša obdobja prekinitev v delovanju. Vse prekinitve v delovanju morajo biti usklajene vnaprej z vsemi deležniki naročnika.

Dokumentacija

Dokumentacija mora biti predana v ~~papirni~~ in splošno berljivi elektronski obliki. Vsebuje podrobne načrte konfiguracije, garancijske liste, popis kompatibilne dodatne opreme in rezervnih delov, navodila za uporabo in druge dokumente. Postopek predaje varnostno zaupne dokumentacije (gesla, varnostne nastavitve, ...), se opredeli v podrobnem načrtu rešitve.

Naročnik zahteva, da so vse sheme v elektronski obliki v formatu Microsoft Visio. Uporabljene morajo biti standardne knjižnice zaradi kasnejšega posodabljanja dokumentacije s strani naročnika.

Ponudnik mora na zahtevo naročniku izročiti tudi papirno verzijo dokumentacije.

Usposabljanje

Ponudnik mora ob zaključku namestitve opreme tudi usposobiti osebje naročnika za njeno upravljanje in uporabo. Usposabljanje mora potekati po uradnem kurikulumu proizvajalca pri certificiranem izvajalcu na lokaciji, usklajeni z naročnikom. Ponudnik mora zagotoviti vsaj 8 standardnih polnih izobraževalnih modulov v trajanju 3-5 dni. Enkrat letno obisk globalne konference za 2 udeležence za ponujene tehnologije po izbiri naročnika. Za izobraževanje in obisk konferenc ponudnik zagotavlja kritje kotizacij in šolnine. Potovalne stroške krije naročnik.

Poleg uradnih izobraževanj je potrebno izvesti prenos znanja na osebje naročnika. Osebje naročnika je potrebno usposobiti za izvajanje dnevniških, tedenskih in mesečnih rednih opravil na vsaki aktualni konfiguraciji opreme. Vsa navodila se predajo v pisni obliki.

Vzdrževanje

Vso nameščeno opremo in konfiguracijo mora ponudnik tudi vzdrževati in zagotavljati podporo v različnih režimih v obdobju 5 let od prevzema posamezne opreme, razen če ni v podrobnih tehničnih specifikacijah drugače zahtevano.

Režim podpore in vzdrževanja

Režim podpore in vzdrževanja temelji na redundanci vseh kritičnih gradnikov. V primeru izpada tudi redundantnega gradnika se od ponudnika pričakuje kritični režim angažiranja za vzpostavitev delovanja opreme.

Režim podpore	Odzivni čas	Čas za odpravo napake od prijave	Čas pripravljenosti	Preventivni pregled in mesečno poročanje o opremi
Kritični	2h	8h	24/7	Da
Redundantni	2h	1 delovni dan	24/7	Da
Redni	4h	Naslednji delovni dan	8/5	Ne

Režim podpore za vsako vrsto opreme je določen v podrobnih tehničnih specifikacijah. Če v podrobnih tehničnih specifikacijah režim vzdrževanja ni določen, se za opremo privzame redni način vzdrževanja.

Kritičnost napake v primeru nejasnosti določi skrbnik podpore.

Čas pripravljenosti je, ko ponudnik spremlja in odgovarja na prijave napake in izvaja potrebne aktivnosti za odpravo napake.

Odzivni čas je čas, od prijave napake do trenutka, ko ponudnik izda prvo poročilo o vrsti in postopku odprave napake.

Čas za odpravo napake je čas od prijave napake do vzpostavitve polne funkcionalnosti prizadete vzdrževane opreme.

V kritičnem in redundantnem načinu ponudnik tudi redno sodeluje s predstavnikom naročnika pri obveščanju o odpravi napake in odločanju o nadaljnjih korakih. Na zahtevo naročnika se lahko sodelovanje izvaja tudi s poročili ali sestanki v razmaku ene ure.

Ponudnik mora s planiranimi in napovedanimi nadgradnjami zagotavljati delovanje opreme na zadnji priporočeni verziji programske opreme ves čas izvajanja podpore in vzdrževanja. V dogovoru z naročnikom mora izvajati pravočasno nameščanje varnostnih popravkov.

Redno vzdrževanje in upravljanje

Redno vzdrževanje obsega vsaj sledeče aktivnosti:

- Nadgradnja sistemske programske opreme (firmware) na aktualne in podprte verzije.

- Odprava ozkih grl v konfiguraciji.
- Popravilo/zamenjava okvarjene opreme skladno z režimom podpore.
- Okvarjena oprema se zamenja z enakovredno ali boljšo novo opremo ali z originalnimi rezervnimi deli.
- Odprava napak v delovanju.
- Ažuriranje dokumentacije sistema.
- Odprava varnostnih pomanjkljivosti opreme.

Vrednost rednega vzdrževanja opreme je že del ponudbene cene opreme in se ne obračunava posebej.

Dopolnilno vzdrževanje

Dopolnilno vzdrževanje vsebuje storitve, ki jih naročnik potrebuje za izboljšanje ali nadgradnje ponujene rešitve. Izboljšanj ali nadgradenj naročnik ob pripravi javnega naročila ni mogel specificirati, saj razlogi za to še niso obstajali. Zato dopolnilno vzdrževanje obsega storitve po naročilu, ki jih naročnik naroča po urah dela. Za vsako storitev po naročilu se pripravi ponudba in oceni potrebno število ur opravljenega dela. Po opravljenem delu se izda račun, ki mora biti skladen s ponudbo.

Potek projekta

Potek naročenih del je predviden po sledeči časovnici faz. Termin »T« je trenutek uvedbe izvajalca v delo pri naročniku. Potem se za vsako fazo predvideva odstopanje v mesecih.

Faza	Začetek	Konec	Opombe
Priprava in uskladitev izvedbenega načrta (HLD, LLD)	T+0	T+2	
Vzpostavitev omrežja GNC	T+2	T+5	
Vzpostavitev strežnikov GNC	T+3	T+8	Sistemske storitve GNC so podlaga za vzpostavitev lokacij RNC in LNC.
Vzpostavitev sistema za izdelavo varnostnih kopij	T+6	T+8	Ob vzpostavitvi bo varovanih bistveno manj strežnikov, kot ob koncu projekta.
Vzpostavitev varnostnih storitev GNC	T+6	T+10	
Vzpostavitev prvega RNC	T+10	T+12	
Vzpostavitev omrežja prvega LNC	T+10	T+12	
Vzpostavitev strežnikov prvega LNC	T+11	T+12	
Vzpostavitev laboratorijskega RNC	T+8	T+10	Testno okolje, kjer se preverijo morebitne spremembe pred prenosom v produkcijsko konfiguracijo.
Vzpostavitev laboratorijskega LNC	T+8	T+10	Testno okolje, kjer se preverijo morebitne spremembe pred prenosom v produkcijsko konfiguracijo.

Revizija načrta	izvedbenega	T+11	T+12	Popravki na podlagi izkušenj prvih implementacij.
--------------------	-------------	------	------	---

Projekt vpliva neposredno na upravljanje avtocestnega omrežja, ki je v upravljanju DARS. Zaradi narave kritične infrastrukture in potrebe po delovanju 24/7 lahko pride do tveganj pri določanju časovnih rokov predvsem pri implementaciji LNC modulov.

Dobava preostalih modulov se bo izvajala sukcesivno v skladu z možnostmi implementacije. Zadnji modul bo predvidoma dobavljen v roku T+28.

Po prevzemu rešitve ponudnik zagotavlja vzdrževanje prevzete opreme.

Vse spremembe konfiguracije v času trajanja projekta, ki se obravnavajo kot sprememba izvedbenega načrta, so del izvedbe projekta.

Podrobne tehnične specifikacije posameznih gradnikov

M.1.1 MPLS usmerjevalnik Tip 1

- možnost vgradnje v standardno 19" komunikacijsko omaro,
- CPU z vsaj 6 jedri,
- vsaj 64 GB DRAM sistemskega polnilnika,
- ~~vsaj 32GB eMMC,~~
- vgrajen SSD ali eMMC pomnilnik z vsaj 480 GB prostora
- vsaj dva AC/DC modularna redundantna napajalnika z možnostjo zamenjave med delovanjem,
- redundantni ventilatorji, z možnostjo zamenjave med delovanjem,
- Možnost določitve usmeritve ventilatorjev ob naročilu opreme.
- Vmesniki
 - Možnost vgradnje razširitvenih modulov
 - Podpora modulom z naslednjimi tipi vmesnikov
 - 4x QSFP56 DD
 - 16x QSFP28
 - 16x SFP56 in 4x QSFP56
 - V napravo mora biti nameščen vsaj en razširitveni modul s 16x QSFP28 vmesniki
- Maksimalna prepustnost vsaj 6 Tbps
- Priključki za:
 - priključek RJ-45 za upravljanje (management port),
 - serijski konzolni priključek,
 - spominski priključek USB,

Funkcionalnosti in podpora za:

- podpora za MACSEC
- podpora za L2 protokole:
 - Ethernet Flow Point (EFP)
 - Bridge Domains
 - Virtual Private Wire Service (VPWS)
 - Virtual Private LAN Service (VPLS)
 - Ethernet VPN (EVPN)
 - Ethernet VPN Virtual Private Wire Service (EVPN-VPWS)
- podpora za L3 protokole:
 - IPv4 and IPv6 unicast routing
 - Virtual Routing and Forwarding (VRF)
 - Open Shortest Path First (OSPF) v2, v3
 - Intermediate System to Intermediate System (IS-IS) for IPv4 and IPv6
 - Equal-Cost Multipath (ECMP)
 - Virtual Router Redundancy Protocol (VRRP)
 - Hot Standby Router Protocol (HSRP)
 - Generic Routing Encapsulation (GRE)
 - Policy-Based Routing (PBR)
 - ACL-based Forwarding (ABF)
 - L3 Virtual Private Network (L3VPN)
- Podpora za MPLS protokole:
 - Multiprotocol Label Switching (MPLS)
 - Label Distribution Protocol (LDP)
 - MPLS Traffic Engineering (MPLS-TE) with RSVP-TE
- Podpora za segment routing:
 - Segment Routing with MPLS data plane (SR-MPLS)
 - Segment Routing with IPv6 data plane (SRv6)
 - Segment Routing Traffic Engineering (SR-TE)
 - Segment Routing Path Computation Element (SR-PCE)
 - Topology-Independent Loop-Free Alternate (TI-LFA)
 - Segment Routing On-Demand Next-Hop (SR-ODN)
 - Segment Routing Performance Management (SR-PM)
 - Segment Routing v6 Performance Management (SRv6-PM)
 - Segment Routing Data Plane Monitoring (SR-DPM)
 - Tree-SID
- podpora za upravljanja:
 - Command-Line Interface (CLI)
 - SSH, Telnet, SCP, FTP, TFTP
 - Simple Network Management Protocol (SNMP)

- Network Configuration Protocol (NETCONF)
- gRPC (Remote Procedure Calls)
- YANG models (OpenConfig, IETF)
- Model/event-Driven Telemetry (MDT)
- RPM-based software infrastructure
- Embedded Event Manager (EEM)
- Zero-Touch Provisioning (ZTP)
- Možnost zagotavljanja:
 - Secure Zero-Touch Provisioning (sZTP)
- Podpora za multicast
 - IPv4 and IPv6 multicast routing
 - Protocol Independent Multicast – Sparse Mode (PIM-SM)
 - PIM – Source Specific Multicast (PIM-SSM)
 - Internet Group Management Protocol (IGMP) v3
 - Multicast Listener Discovery (MLD) v2
 - Multicast Label Distribution Protocol (mLDP)
 - MPLS Point-to-Multipoint Traffic Engineering (MPLS P2MP-TE)
 - Next Generation multicast VPN (NG mVPN)
- Podpora za QoS
 - Virtual Output Queueing (VOQ) with deep packet buffering
 - Class-based 3-level hierarchical QoS
 - Policing, shaping, remarking
 - Multilevel priority queuing
 - Random Early Detection (RED), Weighted RED (WRED)
 - Dual Queue Limit (DQL)
- Zagotavljanje varnosti:
 - ⊖ MACsec ~~and IPsec~~
 - Control Plane Protection (CoPP)
 - Management Plane Protection (MPP)
 - Local Packet Transport Services (LPTS)
 - Authentication, Authorization, and Accounting (AAA)
 - Access Control Lists (ACL) for IPv4, IPv6, and L2
 - BGP FlowSpec
 - Unicast Reverse Path Forwarding (uRPF)
 - Možnost zagotavljanja:
 - 802.1X
 - IPsec
- Podpora za protokole in funkcionalnosti časovne sinhronizacije:
 - Enhanced Synchronous Ethernet (eSyncE)
 - Enhanced Ethernet Synchronization Message Channel (eESMC)
 - ⊖ ~~IEEE 1588-2008 Precision Time Protocol (PTP): T-GM, T-BC, Virtual Port, A-PTS~~

- G.8275.1, G.8275.2, G.8265.1, G.8273.2 Class C
- Network Time Protocol (NTP)
- Možnost zagotavljanja:
 - IEEE 1588-2008 Precision Time Protocol (PTP): T-GM, T-BC, Virtual Port, A-PTS
- Podpora za protokole operacije, administracija in upravljanja
 - Link Layer Discovery Protocol (LLDP)
 - Cisco Discovery Protocol (CDP)
 - Internet Control Message Protocol (ICMP)
 - Dynamic Host Configuration Protocol (DHCP), DHCP Relay
 - Bidirectional Forwarding Detection (BFD) v4, v6
 - MPLS OAM
 - Connectivity Fault Management (CFM)
 - Y.1731 Delay Measurement (DM)
 - Y.1731 Synthetic Loss Measurement (SLM)
 - Two-Way Active Measurement Protocol (TWAMP, TWAMP Lite)
 - IP SLA (Service-Level Agreement)
 - NetFlow, sFlow, IPFIX 315
 - Switch Port Analyzer (SPAN, ERSPAN, SPAN to file)
 - Dying Gasp

Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potrebna ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe.

Zahtevana združljivost:

- združljivost z upravljavskim sistemom specificiranim v poglavju M.3.4

Režim podpore: Redundantni

M.1.2 MPLS usmerjevalnik Tip 2

- višina 1U z možnostjo vgradnje v standardno 19" komunikacijsko omaro,
- CPU z vsaj 4 jedri,
- vsaj 16GB DRAM sistemskega pomnilnika,
- 32GB eMMC,
- vsaj dva AC/DC modularna redundantna napajalnika z možnostjo zamenjave med delovanjem,
- redundantni fiksni ventilatorji,

- ~~Možnost določitve usmeritve ventilatorjev ob naročilu opreme.~~

- Vmesniki:
 - vsaj 4 fiksni QSPF28 vmesniških rež s podporo za hitrosti 40/100GE
 - vsaj 24 fiksni SFP28 vmesniških rež s podporo za hitrosti 1/10/25GE,
 - vsaj 4 fiksne RJ-45 vmesniške reže s hitrostjo 10/100/1000M
- maksimalna propustnost 1004Gbps,
- Priključki za:
 - priključek RJ-45 za upravljanje (management port),
 - spominski priključek USB,
 - USB konzolni priključek
 - serijski konzolni priključek,

Funkcionalnosti in podpora za:

- podpora za MACSEC,
- podpora za L2 protokole:
 - Ethernet Flow Point (EFP)
 - Bridge Domains
 - Virtual Private Wire Service (VPWS)
 - Virtual Private LAN Service (VPLS)
 - Ethernet VPN (EVPN)
 - Ethernet VPN Virtual Private Wire Service (EVPN-VPWS)
- podpora za L3 protokole:
 - IPv4 and IPv6 unicast routing
 - Virtual Routing and Forwarding (VRF)
 - Open Shortest Path First (OSPF) v2, v3
 - Intermediate System to Intermediate System (IS-IS) for IPv4 and IPv6
 - Equal-Cost Multipath (ECMP)
 - Virtual Router Redundancy Protocol (VRRP)
 - Hot Standby Router Protocol (HSRP)
 - Generic Routing Encapsulation (GRE)
 - Policy-Based Routing (PBR)
 - ACL-based Forwarding (ABF)
 - L3 Virtual Private Network (L3VPN)
- Podpora za MPLS protokole:
 - Multiprotocol Label Switching (MPLS)
 - Label Distribution Protocol (LDP)
 - MPLS Traffic Engineering (MPLS-TE) with RSVP-TE
- Podpora za segment routing:
 - Segment Routing with MPLS data plane (SR-MPLS)
 - Segment Routing with IPv6 data plane (SRv6)
 - Segment Routing Traffic Engineering (SR-TE)

- Segment Routing Path Computation Element (SR-PCE)
 - Topology-Independent Loop-Free Alternate (TI-LFA)
 - Segment Routing On-Demand Next-Hop (SR-ODN)
 - Segment Routing Performance Management (SR-PM)
 - Segment Routing v6 Performance Management (SRv6-PM)
 - Segment Routing Data Plane Monitoring (SR-DPM)
 - Tree-SID
- podpora za upravljanja:
 - Command-Line Interface (CLI)
 - SSH, Telnet, SCP, FTP, TFTP
 - Simple Network Management Protocol (SNMP)
 - Network Configuration Protocol (NETCONF)
 - gRPC (Remote Procedure Calls)
 - YANG models (OpenConfig, IETF)
 - Model/event-Driven Telemetry (MDT)
 - RPM-based software infrastructure
 - Embedded Event Manager (EEM)
 - Zero-Touch Provisioning (ZTP)
 - Secure Zero-Touch Provisioning (sZTP)
- Podpora za multicast
 - IPv4 and IPv6 multicast routing
 - Protocol Independent Multicast – Sparse Mode (PIM-SM)
 - PIM – Source Specific Multicast (PIM-SSM)
 - Internet Group Management Protocol (IGMP) v3
 - Multicast Listener Discovery (MLD) v2
 - Multicast Label Distribution Protocol (mLDP)
 - MPLS Point-to-Multipoint Traffic Engineering (MPLS P2MP-TE)
 - Next Generation multicast VPN (NG mVPN)
- Podpora za QoS
 - Virtual Output Queueing (VOQ) with deep packet buffering
 - Class-based 3-level hierarchical QoS
 - Policing, shaping, remarking
 - Multilevel priority queuing
 - Random Early Detection (RED), Weighted RED (WRED)
 - Dual Queue Limit (DQL)
- Zagotavljanje varnosti:
 - MACsec and IPsec
 - Control Plane Protection (CoPP)
 - Management Plane Protection (MPP)
 - Local Packet Transport Services (LPTS)
 - Authentication, Authorization, and Accounting (AAA)

- Access Control Lists (ACL) for IPv4, IPv6, and L2
 - BGP FlowSpec
 - Unicast Reverse Path Forwarding (uRPF)
 - 802.1X
- Podpora za protokole in funkcionalnosti časovne sinhronizacije:
 - Enhanced Synchronous Ethernet (eSyncE)
 - Enhanced Ethernet Synchronization Message Channel (eESMC)
 - IEEE 1588-2008 Precision Time Protocol (PTP): T-GM, T-BC, Virtual Port, A-PTS
 - G.8275.1, G.8275.2, G.8265.1, G.8273.2 Class C
 - Network Time Protocol (NTP)
- Podpora za protokole operacije, administracija in upravljanja
 - Link Layer Discovery Protocol (LLDP)
 - Cisco Discovery Protocol (CDP)
 - Internet Control Message Protocol (ICMP)
 - Dynamic Host Configuration Protocol (DHCP), DHCP Relay
 - Bidirectional Forwarding Detection (BFD) v4, v6
 - MPLS OAM
 - Connectivity Fault Management (CFM)
 - Y.1731 Delay Measurement (DM)
 - Y.1731 Synthetic Loss Measurement (SLM)
 - Two-Way Active Measurement Protocol (TWAMP, TWAMP Lite)
 - IP SLA (Service-Level Agreement)
 - NetFlow, sFlow, IPFIX 315
 - Switch Port Analyzer (SPAN, ERSPAN, SPAN to file)
 - Dying Gasp

Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe.

Zahtevana združljivost:

- združljivost z upravljavskim sistemom specificiranim v poglavju M.3.4

Režim podpore: Redundantni

M.1.3 Jedrno stikalo

Tip stikala:

- Vgradnja v standardno 19" komunikacijsko omaro.
- Priložen pribor za vgradnjo v 19" omaro.

Napajanje:

- vsaj dva neodvisna napajalnika (redundantna zasnova)
- možnost zamenjave napajalnika pri delujoči napravi (Hot swap)
- priklop na 100-240 V AC, 50-60 Hz,
- Redundantni ventilatorji za hlajenje z možnostjo menjave med delovanjem (Hot Swap).

Lastnosti vmesnikov:

- vsaj 48 24 vrat 1/10/25 Gbps z SFP/SFP+/SFP28 vmesniki
- vsaj 4 vrata 40/100G Gbps z QSFP+/QSFP28 vmesniki

Razpoložljivost in razširljivost:

- podpora povezavi dveh stikal v enotno logično entiteto s skupno točko upravljanja:
 - o podpora za SSO (»Stateful Switchover«)
- podpora za NSF (Non-Stop Forwarding)
- skupni upravljavski in kontrolni podsistem, združena podatkovna podsistema
- podpora za vzpostavitev dvojne povezave (Multi-chassis Etherchannel - MEC) brez potrebe po uporabi algoritmov vpetega drevesa (STP)
- sposobnost izločanja zank in zagotavljanje redundance na OSI L2: podpora za STP, Multiple STP in RSTP (Multiple/Rapid/Spanning Tree Protocol)
- podpora protokolu STP za vsak VLAN posebej
- omogočati mora nadgradnje sistema brez izgube funkcionalnosti (»In-Service Software Upgrade, ISSU«)
- podpora združevanju GigaEthernet povezav v grupo (»link aggregation«), vsaj do 8 povezav v grupi
- zaščita vrat pred broadcast, multicast in unicast preobremenitvijo (»storm control«).

Zmogljivosti:

- prepustnost stikala po pasovni širini najmanj 2 3 Tbps
- podpora paketom (MTU) dolžine vsaj 9216 zlogov (tim. jumbo paketi)
- podpora za istočasno hranjenje vsaj 80.000 MAC naslovov

Funkcionalnosti:

- podpora VLAN:
 - o podpora najmanj 4000 VLAN-ov
 - o usmerjanje med vsaj 4000 VLAN-i
 - o podpora privatnim VLAN-om (podpora več VLAN-om znotraj istega omrežnega segmenta)
 - o avtomatsko razpošiljanje nastavljenih VLAN-ov do sosednjih vozlišč
- podpora 802.1p (Priority Tagging)
- podpora 802.1Q (VLAN)
- podpora usmerjevalnim protokolom:
 - o RIPv2, RIPv6, OSPFv2, OSPFv3, BGPv4, BGPv6, EIGRP, EIGRPv6, IS-ISv4
- podpora za IP multicast za naslednje protokole:

- Bidirectional PIM
 - PIM Sparse Mode
 - PIM SSM
- podpora protokolu IGMP v1, v2 in v3
 - IGMP snooping
 - IGMP immediate leave
 - IGMP state limit – omejevanje števila IGMP grup na vmesnik
- podpora programsko definiranemu dostopu (SD-Access)
 - VXLAN, SDA Edge, SDA Border, SDA Control-Plane, VNI
- podpora virtualnemu usmerjanju znotraj stikala (VRF)
- podpora vsaj enemu od FHRP (First Hop Redundancy Protocols) protokolov kot so VRRP ali HSRP

Varnost:

- varnost na nivoju vrat z overjanjem uporabnikov po standardu IEEE 802.1x protokolu ter z dinamičnim dodeljevanjem VLAN-ov
- aktiviranje varnostnih filtrov preko protokola 802.1x
- podpora overjanju uporabnika preko spletnega vmesnika ali naslova MAC
- podpora varnostnim filtrom, ki se časovno avtomatsko spreminjajo
- varnostni filtri morajo podpirati možnosti odločanja, glede na fizični ali logični vmesnik ter naslove nivoja 2 do 4 (MAC, IP, TCP/UDP)
- podpora SSH, Kerberos in SNMPv3 protokolov za administracijo
- podpora za overjanje preko protokola TACACS+ in RADIUS
- podpora prepuščanju prometa samo določenih naslovov MAC na posameznem vmesniku
- podpora preverjanju izvora paketov ARP in preprečevanja pošiljanja paketov z napačno vsebino relacije IP-MAC (ARP inspection)
- omogočeno filtriranje paketov BPDU ter preprečevanje priklopa stikal z manjšimi prioritetami BPDU kot jih ima korensko stikalo
- možnost odmetavanja prometa DHCP iz nezaupnih priključkov (DHCP snooping)
- preprečevanje priklopa naprav z napačnim naslovom IP na fizični vmesnik
- podpora IPv6 FHS (First Hop Security)
 - IPv6 snooping
 - IPv6 ND
 - IPv6 RA guard
 - IPv6 DHCP guard
 - IPv6 Source guard
 - IPv6 Prefix guard
- avtomatsko onemogočanje fizičnih priključkov ob zaznavanju prekomernih napak
- možnost zakasnenega avtomatskega aktiviranja priključkov, ki so bili onemogočeni zaradi prekomernih napak
- Podpora standardu 802.1ae (MACsec) na vseh vmesnikih z linijsko hitrostjo in šifriranjem AES-256-bitov
- podpora varnega zagona programske opreme; vse datoteke morajo biti ustrezno kriptografsko podpisane in stikalo mora znati preveriti istovetnost.

Podpora za QoS:

- 8 izhodih vrst (queues) na vsakem vmesniku
- možnost definiranja vsaj ene prioritete vrste
- kontrola algoritma za strežbo izhodnih vrst (scheduling)
- podpora fleksibilnemu omejevanju pasovne širine prometa za vrsto ali cel vmesnik (WRED itd.)
- razvrščanje paketov (classifying)
- traffic policing (omejevanje prometa na določeno število kbit/s) za posamezen fizični vmesnik
- omejevanje poplavljanja s prometom Unicast, Broadcast in Multicast za vsakega posebej ločeno na vmesnik.
- označevanje oz. barvanje paketov (marking - nastavljanje QoS bitov),
- podpora za zbiranje informacij o podatkovnih tokovih in pošiljanje poročil na centralni sistem za upravljanje
- limitiranje prometa do CPU enote stikala

Nadzor in upravljanje:

- podpora za upravljanje in konfiguracijo preko CLI, SSH in WEB vmesnika
- možnost upravljanja preko vmesnika:
 - o USB mini Type B console port
 - o RJ-45 console port
- možnost upravljanja preko ločenega fizičnega vmesnika Ethernet
- možnost za aktiviranje prejšnje konfiguracije
- podpora TFTP za nadgradnjo programske opreme, ter prenosu konfiguracij z in na napravo
- uporaba protokola NTP za časovno sinhronizacijo (sprejem in odajanje)
- možnost odkrivanja sosednjih naprav (Neighbor learning)
- podpora protokolom SNMPv1, v2c in v3
- podpora najmanj 4 skupin RMON
- podpora prenosa sporočil stikala do strežnika sporočil Syslog
- možnost preslikave prometa enega ali več vmesnikov oziroma navideznega omrežja na izhod za priklop analizatorja prometa (SPAN)
- možnost preslikave prometa enega ali več vmesnikov oziroma navideznega omrežja na poseben VLAN, ki ga lahko zaključimo na vmesniku drugega stikala (Remote-SPAN)
- strojna podpora za pošiljanje SPAN prometa preko IP omrežja na oddaljeno lokacijo
- podpora mehanizmu za preverjanje in onemogočanje enosmernosti povezave na optičnih vmesnikih (UDLD)
- podpora za avtomatsko konfiguriranje stikala (PXE, ZTP, Plug&Play)
- podpora protokolom NETCONF in RESTCONF
- podpora protokolu gNMI
- podpora avtomatskemu proženju skript glede na različne akcije v stikalu (npr: sprememba konfiguracije, napaka na vmesniku, časovne definirane akcije, kritični alarmi,...)
- podpora pošiljanja e-mail sporočil neposredno iz stikala
- možnost izvajanja Python skript na stikalu,
- možnost izvajanja namenskih aplikacij v izoliranih kontejnerjih na samem stikalu

- možnost zajema paketov na samem stikalu ter shranjevanje v obliki primerni za pregled v analizatorju prometa Wireshark ali podobno
 - o možno nastaviti ACL za filtriranje prometa
 - o možnost enostavnega pregleda zajetih paketov
- upravljanje stikala preko ponujenega upravljalnega in nadzornega sistema

Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe.

Zahtevana združljivost:

- združljivost s ponujenim upravljalnim in nadzornim sistemom za lokalna omrežja

Režim podpore: Redundantni

M.1.4 Dostopovno stikalo

Tip stikala:

- Vgradnja v standardno 19" komunikacijsko omaro
- možnost združevanja več stikal v eno skladovno enoto z enotno konfiguracijo in 1 naslovom IP za upravljanje
- možnost sestava sklada do 8 stikal, pri čemer so stikala lahko različnih konfiguracij znotraj iste družine stikal.

Napajanje:

- Dva neodvisna napajalnika (Hot swap)
- priklop na 100-240 V AC
- zagotavljanje napajanja drugim stikalom sklada, če njihovi napajalniki odpovedo
- možnost dodeljevanja višek moči napajalnika enega stikala drugim stikalom v skladu
- možnost menjave hladilnikov stikala med delovanjem stikala.

Lastnosti vmesnikov:

- vsaj 48 10/100/1000 Ethernet portov RJ-45
- vsaj 8 rež za optične 10 Gbps vmesnike SFP+
- možnost kasnejše zamenjave optičnih vmesnikov za zmogljivejše 40Gbps vmesnike
- podpora za optične module SFP+ (10Gb/s) s podporo za enorodovna in večrodovna vlakna (SR, LR, ER, CWDM in DWDM)
- namenski vmesniki za povezavo v sklad hitrosti 480Gb/s
- namenski vmesniki za deljenje napajanja med stikali.

Razpoložljivost in razširljivost:

- vsa stikala v skladu imajo kopijo konfiguracije

- zmožnost izločanja zank in zagotavljanje redundance na OSI L2: podpora za STP, Multiple STP in RSTP (Multiple/Rapid/Spanning Tree Protocol)
- podpora protokolu STP za vsak VLAN posebej
- podpora združevanju GigaEthernet povezav v grupo (Link aggregation), do 8 povezav v grupi
- podpora združevanju v grupo preko več stikalu v skladu
- zaščita vrat pred broadcast, multicast in unicast preobremenitvijo (storm control)
- preklop nadzora nad skladom ob odpovedi master stikala mora biti za uporabnike nemoteč (<100ms).

Zmogljivosti:

- prepustnost stikala po pasovni širini najmanj 200 Gb/s
- prepustnost sklada vsaj 480Gb/s
- prepustnost stikala po številu paketov najmanj 100 Mpkt/s
- podpora jumbo paketom dolžine vsaj 9150 zlogov
- podpora vsaj 30000 naslovov MAC.

Funkcionalnosti:

- podpora VLAN:
 - o podpora najmanj 1900 VLAN-ov
 - o možnost usmerjanja med vsaj 1000 VLAN-i
 - o podpora privatnim VLAN-om (podpora več VLAN-om znotraj istega omrežnega segmenta)
 - o avtomatsko razpošiljanje nastavljenih VLAN-ov do sosednjih vozlišč
- podpora 802.1p (Priority Tagging)
- podpora 802.1Q (VLAN)
- podpora protokolu PIM
- podpora protokolu IGMP v1, v2 in v3
- IGMP snooping v1 in v2
- IGMP fitiranje v1 in v2
- podpora usmerjevalnim protokolom BGP, OSPF in protokolu HSRP
- podpora za VXLAN in VRF.

Varnost:

- varnost na nivoju vrat z overjanjem uporabnikov po standardu IEEE 802.1x protokolu ter dinamičnim dodeljevanjem VLAN-ov
- aktiviranje varnostnih filtrov preko protokola 802.1x
- podpora overjanju uporabnika preko spletnega vmesnika ali naslova MAC
- podpora varnostnim filtrom, ki se časovno avtomatsko spreminjajo
- varnostni filtri morajo podpirati možnosti odločanja, glede na fizični ali logični vmesnik ter naslove nivoja 2 do 4 (MAC, IP, TCP/UDP)
- podpora SSH, Kerberos in SNMPv3 protokolov za administracijo
- podpora za overjanje preko protokola TACACS+ in RADIUS

- podpora prepuščanju prometa samo določenih naslovov MAC na posameznem vmesniku
- podpora preverjanju izvora paketov ARP in preprečevanja pošiljanja paketov z napačno vsebino relacije IP-MAC (ARP inspection)
- omogočeno filtriranje paketov BPDU ter preprečevanje priklopa stikal z manjšimi prioritetaми BPDU kot jih ima korensko stikalo
- možnost odmetavanja prometa DHCP iz nezaupnih priključkov (DHCP snooping)
- preprečevanje priklopa naprav z napačnim naslovom IP na fizični vmesnik
- podpora IPv6 FHS (First Hop Security)
 - o IPv6 snooping
 - o IPv6 ND
 - o IPv6 RA guard
 - o IPv6 DHCP guard
 - o IPv6 Source guard
 - o IPv6 Prefix guard
- avtomatsko onemogočanje fizičnih priključkov ob zaznavanju prekomernih napak
- možnost zakasnjene avtomatskega aktiviranja priključkov, ki so bili onemogočeni zaradi prekomernih napak
- Podpora standardu 802.1ea (MACsec) na vseh vmesnikih z linijsko hitrostjo in šifriranjem AES-128-bitov
- s strojno podporo MACsec za AES-256 bitov z nadgradnjo licence
- podpora upravljanju šifrirnih ključev odjemalcem in stikalom preko sistema za upravljanje identitetami in avtorizacijami uporabnikov
- strojna podpora za analizo šifriranega prometa z dodatno licenco
- podpora varnega zagona programske opreme v stikalu; vse datoteke morajo biti ustrezno kriptografsko podpisane in stikalo mora znati preveriti istovetnost.

Podpora za QoS:

- 8 izhodnih vrst (queues) na vsakem vmesniku
- možnost definiranja vsaj ene prioritete vrste
- kontrola algoritma za strežbo izhodnih vrst (scheduling) po principu SRR (shaped round robin) ali WRR (weighted round robin)
- vgrajen mehanizem za preprečevanje zasičenja vhodne/izhodne vrste (uteženo odmetavanje - WTD)
- razvrščanje paketov (classifying)
- traffic policing (omejevanje prometa na določeno število kbit/s) za posamezen fizični vmesnik
- omejevanje poplavljanja s prometom Unicast, Broadcast in Multicast za vsakega posebej ločeno na vmesnik
- označevanje oz. barvanje paketov (marking - nastavljanje QoS bitov),
- vsi QoS mehanizmi (scheduling, classifying, policing in marking) so wire-rate. Njihova uporaba ne sme vplivati na prepustnost in delovanje ostalih funkcij stikala/sklada

- podpora za zbiranje informacij o podatkovnih tokovih in pošiljanje poročil na centralni sistem za upravljanje
- stikalo mora imeti kapaciteto za zbiranje statistike za vsaj 60000 sočasnih podatkovnih tokov
- strojna podpora za prepoznavanje vsaj 1300 aplikacij na omrežnem nivoju in možnost klasificiranja, izvajanje statistike in pošiljanje poročil na centralni sistem za upravljanje

Nadzor in upravljanje:

- podpora za upravljanje in konfiguracijo preko CLI, SSH in WEB vmesnika
- možnost upravljanja preko vmesnika USB
- možnost upravljanja preko ločenega fizičnega vmesnika Ethernet
- podpora shranjevanju in nalaganju konfiguracije stikala v format ASCII
- možnost aktiviranja prejšnje konfiguracije
- podpora TFTP in FTP za nadgradnjo programske opreme, ter prenosu konfiguracij
- podpora protokolu NTP za časovno sinhronizacijo
- možnost odkrivanja sosednjih naprav (Neighbor learning)
- podpora protokolom SNMPv1, v2c in v3 ter podpora najmanj 4 skupin RMON
- podpora prenosa sporočil stikala do strežnika sporočil Syslog
- možnost preslikave prometa enega ali več vmesnikov oziroma navideznega omrežja na izhod za priklop analizatorja prometa (SPAN)
- možnost preslikave prometa enega ali več vmesnikov oziroma navideznega omrežja na poseben VLAN, ki ga lahko zaključimo na vmesniku drugega stikala (Remote-SPAN)
- strojna podpora za pošiljanje SPAN prometa preko IP omrežja na oddaljeno lokacijo
- podpora mehanizmu za preverjanje in onemogočanje enosmernosti povezave na optičnih vmesnikih (UDLD)
- omogočanje prenosa informacij o nastavljenih VLAN-ih med sosednjimi vozlišči
- podpora za avtomatsko konfiguriranje stikala preko protokola iPXE (Plug&Play)
- podpora protokolom NETCONF in RESTCONF
- podpora protokolu gNMI
- podpora avtomatskemu proženju skript glede na različne akcije v stikalu (npr: sprememba konfiguracije, napaka na vmesniku, časovne definirane akcije, kritični alarmi,...)
- podpora pošiljanja e-mail sporočil neposredno iz stikala
- možnost izvajanja Python skript na stikalu
- možnost izvajanja namenskih aplikacij v izoliranih kontejnerjih na samem stikalu
- možnost izvajanja aplikacije Wireshark na samem stikalu
- podpora upravljanju stikala preko ponujenega upravljalnega in nadzornega sistema

Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe

- Sonda za vidljivost Sistema za spremljanje in zaznavo dogodkov v OT (P.1.5). V obliki programske opreme na stikalu ali namenske naprave priključene na stikalo.

Zahtevana združljivost:

- združljivost s ponujenim upravljalnim in nadzornim sistemom (M.3.3)

Zahtevani povezovalni kabli in dodatna oprema:

- priloženi morajo biti vsi potrebni povezovalni moduli in kabli za povezovanje stikal v sklad (za podatkovni prenos in za deljenje napajalne moči),

Režim podpore: Redundantni

M.1.5 Stikalo za potrebe nadzornega sistema

Tip stikala:

- skladovno stikalo za vgradnjo v standardno 19-palčno komunikacijsko omaro
- možnost združevanja več stikal v eno skladovno enoto z enotno konfiguracijo in 1 naslovom IP za upravljanje
- možnost sestava sklada do 8 stikal, pri čemer so stikala lahko različnih konfiguracij znotraj iste družine stikal

Razpoložljivost in razširljivost:

- vsa stikala v skladu imajo kopijo konfiguracije
- zmožnost izločanja zank in zagotavljanje redundance na OSI L2: podpora za STP, Multiple STP in RSTP (Multiple/Rapid/Spanning Tree Protocol),
- podpora protokolu STP za vsak VLAN posebej
- podpora združevanju GigaEthernet povezav v skupino (Link aggregation), do 8 povezav v skupini
- podpora združevanju v skupino preko več stikal v skladu
- zaščita vrat pred broadcast, multicast in unicast preobremenitvijo (storm control)
- preklop nadzora nad skladom ob odpovedi master stikala mora biti za uporabnike nemoteč

Napajanje:

- Dva napajalnika
- priklop na 100-240 V AC
- možnost menjave napajalnikov med delovanjem stikala

Lastnosti vmesnikov:

- vgrajene vsaj 4 reže SFP za optične vmesnike 10 Gbps
- vsaj 24 10/100/1000 Ethernet portov RJ-45
- podpora Auto-MDIX na vseh vmesnikih UTP
- možnost samodejne konfiguracije vmesnika glede na priključeno napravo

Funkcionalnosti:

- podpora VLAN:

- podpora najmanj 1024 VLAN-ov
- možnost avtomatskega razpošiljanja nastavljenih VLANov do sosednjih vozlišč
- podpora 802.1p (Priority Tagging)
- podpora 802.1Q (VLAN)
- podpora protokolu RIP in OSPF
- podpora protokolu PIM (PIM SM in SSM)

Zmogljivost:

- prepustnost sklada vsaj 70Gb/s
- podpora paketom (MTU) dolžine vsaj 9190 zlogov (tim. jumbo paketi)

Varnost:

- varnost na nivoju vrat z overjanjem uporabnikov po standardu IEEE 802.1x protokolu ter dinamičnim dodeljevanjem VLAN-ov
- aktiviranje varnostnih filtrov preko protokola 802.1x
- podpora overjanju uporabnika preko spletnega vmesnika ali naslova MAC
- podpora varnostnim filtrom, ki se časovno samodejno spreminjajo
- varnostni filtri morajo podpirati možnosti odločanja, glede na fizični ali logični vmesnik ter naslove nivoja 2 do 4 (MAC, IP, TCP/UDP)
- podpora SSH in SNMPv3 protokolov za upravljanje
- podpora za overjanje preko protokola TACACS+ in RADIUS
- podpora prepuščanju prometa samo določenih naslovov MAC na posameznem vmesniku
- podpora preverjanju izvora paketov ARP in preprečevanja pošiljanja paketov z napačno vsebino relacije IP-MAC (ARP inspection)
- omogočeno filtriranje paketov BPDU ter preprečevanje priklopa stikal z manjšimi prioritetami BPDU, kot jih ima korensko stikalo
- možnost odmetavanja prometa DHCP iz nezaupnih priključkov (DHCP snooping)
- preprečevanje priklopa naprav z napačnim naslovom IP na fizični vmesnik
- samodejno onemogočanje fizičnih priključkov ob zaznavanju prekomernih napak
- možnost zakasnenega samodejnega aktiviranja priključkov, ki so bili onemogočeni zaradi prekomernih napak

Podpora za QoS:

- 8 izhodnih vrst (queues) na vsakem vmesniku
- možnost definiranja vsaj ene prioritete vrste
- kontrola algoritma za strežbo izhodnih vrst (scheduling) po principu SRR (shaped round robin) ali WRR (weighted round robin)
- vgrajen mehanizem za preprečevanje zasičenja vhodne/izhodne vrste (uteženo odmetavanje - WTD)
- razvrščanje paketov (classifying)
- traffic policing (omejevanje prometa na določeno število kbit/s) za posamezen fizični vmesnik
- omejevanje poplavljanja s prometom Unicast, Broadcast in Multicast za vsakega posebej ločeno na vmesnik
- označevanje oz. barvanje paketov (marking - nastavljanje QoS bitov)

- vsi QoS mehanizmi (scheduling, classifying, policing in marking) so wire-rate. Njihova uporaba ne sme vplivati na prepustnost in delovanje ostalih funkcij stikala/sklada
- podpora za zbiranje informacij o podatkovnih tokovih in pošiljanje poročil na centralni sistem za upravljanje
- stikalo mora imeti kapaciteto za zbiranje statistike za vsaj 16000 podatkovnih tokov

Nadzor in upravljanje:

- podpora za upravljanje in konfiguracijo preko CLI, SSH in WEB vmesnika
- možnost upravljanja preko naslova IPv6
- možnost upravljanja preko vmesnika USB
- možnost upravljanja preko ločenega fizičnega vmesnika Ethernet
- podpora shranjevanju in nalaganju konfiguracije stikala v format ASCII
- možnost aktiviranja prejšnje konfiguracije
- podpora TFTP in FTP za nadgradnjo programske opreme ter prenosu konfiguracij
- podpora protokolu NTP za časovno sinhronizacijo
- možnost odkrivanja sosednjih naprav (Neighbor learning)
- podpora protokolom SNMPv1, v2c in v3 ter podpora RMON
- podpora prenosa sporočil stikala do strežnika sporočil Syslog
- možnost preslikave prometa enega ali več vmesnikov oziroma navideznega omrežja na izhod za priklop analizatorja prometa (SPAN)
- možnost preslikave prometa enega ali več vmesnikov oziroma navideznega omrežja na poseben VLAN, ki ga lahko zaključimo na vmesniku drugega stikala (Remote-SPAN)
- podpora mehanizmu za preverjanje in onemogočanje enosmernosti povezave na optičnih vmesnikih (UDLD)
- omogočanje prenosa informacij o nastavljenih VLAN-ih med sosednjimi vozlišči
- podpora za avtomatsko konfiguriranje stikala preko protokola PXE (Plug&Play)
- podpora protokolom NETCONF in RESTCONF
- podpora avtomatskemu proženju skript glede na različne akcije v stikalu (npr: sprememba konfiguracije, napaka na vmesniku, časovne definirane akcije, kritični alarmi...)
- podpora pošiljanja e-mail sporočil neposredno iz stikala
- možnost nadgradnja več omrežnih naprav preko nadzornega sistema
- možnost programabilne digitalne arhitekture za zagotavljanje boljše preglednosti komunikacije na omrežnem nivoju za lažjo diagnostiko, identificiranje in odpravljanje napak za namen zagotavljanja boljše storitve/uporabniške izkušnje)
- možnost uporabe konfiguracijskih predlog
- podpora funkcionalnosti "Plug-and-play"
- možnost upravljanju stikala preko sistema ponujenega sistema za upravljanje in nadzor lokalnega omrežja
- možnost upravljanja stikala preko sistema za upravljanje z identitetami in avtorizacijami uporabnikov

Zahtevana programska oprema in licence:

- programska oprema mora zagotavljati vse zgoraj naštetе zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba dodatna licenca, mora biti ta ponujena že v ponudbi.

Zahtevana združljivost:

- združljivost ponujenim upravljalnim in nadzornim sistemom lokalnega omrežja

Režim podpore: Redni

M.1.6 Hrbtenično stikalo podatkovnega centra

- podpora za IPv4 in IPv6,
- podpora za VXLAN EVPN fabrics,
- podpora za protokole:
 - Border Gateway Protocol (BGP),
 - Open Shortest Path First (OSPF),
 - Enhanced Interior Gateway Routing Protocol (EIGRP),
 - Routing Information Protocol Version 2 (RIPv2),
 - Protocol Independent Multicast Sparse Mode (PIMSM),
 - Source-Specific Multicast (SSM),
 - Multicast Source Discovery Protocol (MSDP),
- podpora za standarde upravljanja:
 - Ansible,
 - Chef,
 - Puppet,
 - SALT,
 - RESTCONF/NETCONF,
 - JSON based RPC over HTTP/HTTPs,
- podpora za kriptiranje s prepustnostjo vsaj 1 Gbps na vseh vtičnicah za:
 - IEEE 802.1ae MAC Security (MACsec),
 - Cloudsec (VTEP to VTEP encryption),
- upravljanje medpomnilnika (intelligent buffer management) s podporo za:
 - prepoznavanje majhnih in velikih pretokov podatkov (mice and elephant flows) na omrežju in preprečevanje preobremenjenosti povezav (link congestion),
 - Approximate Fair Dropping (AFD),
 - Elephant Trap (ETRAP),
 - Dynamic Packet Prioritization (DPP),
- podpora za RDMA over Converged Ethernet in DCB protokole:
 - Priority-based Flow Control (PFC),
 - Enhanced Transmission Selection (ETS),
 - Data Center Bridging Exchange Protocol (DCBX),
 - Explicit Congestion Notification (ECN),
- podpora za visoko razpoložljivost z uporabo:
 - Virtual Port-Channel (vPC) tehnologije,

- Equal-Cost MultiPath (ECMP) usmerjanja,
- operacijski sistem s podporo za:
 - medsebojno neodvisne procese za protokole usmerjanja,
 - možnost ponovnega zagona posameznega procesa brez izgube stanja (restart without loss of state),
 - brezprekinitveno nameščanje popravkov med delovanjem (hot patching),
- podpora za centralno upravljanje s ponujenim sistemom za upravljanje omrežja podatkovnega centra,
- možnost nadzora mrežnega prometa s podporo za:
 - Test Access Points (TAPs),
 - Switched Port Analyzer (SPAN) aggregation.
- višina 1U z možnostjo vgradnje v standardno 19" komunikacijsko omaro,
- vsaj dva redundantna napajalnika z možnostjo zamenjave med delovanjem,
- redundantni ventilatorji z možnostjo zamenjave med delovanjem,
- Možnost definiranja usmerjenosti ventilatorjev ob naročilu opreme.
- vsaj 36 fiksnih QSPF28 vmesniških rež,
- podpora za 40/100 Gbps na vseh vmesnikih,
- podpora za 1/10/25 Gbps z uporabo razdelilnih (breakout) kablov,
- CPU z vsaj 4 jedri,
- vsaj 24GB sistemskega pomnilnika,
- SSD pogon vsaj 128 GB,
- predpomnilnik (system buffer) vsaj 40 MB,
- priključek RJ-45 za upravljanje (management port),
- priključek SFP+ za upravljanje (management port),
- priključek USB,
- priključek RS-232,
- prepustnost (switching capacity) do vsaj 7,2 Tbps (bitov na sekundo)
- prepustnost (forwarding rate) do vsaj 2,4 Bpps (paketov na sekundo),
- največje število IPv4 Longest Prefix Match (LPM) routes: 880000,
- največje število IPv4 host entries: 880000,
- največje število MAC address entries: 256000,
- največje število multicast routes: 128000,
- število Internet Group Management Protocol (IGMP) snooping groups: vsaj 8000,
- največje število ACL entries (per slice the forwarding engine) ingress: 5000,
- največje število ACL entries (per slice the forwarding engine) egress: 2000,
- največje število VLANov: 4096,
- število Virtual Routing in Forwarding (VRF) instanc: vsaj 1000,
- največje število ECMP poti: 64,
- največje število port channels: 512,
- največje število povezav na port channel: 32,

- število aktivnih SPAN sej: vsaj 4,
- največje število VLANov v RPVST instancah: 3967,
- največje število Hot-Standby Router Protocol (HSRP) grup: 490,
- število Network Address Translation (NAT) entries: vsaj 1023,
- največje število Multiple Spanning Tree (MST) instanc: 64.

Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe.

Zahtevana združljivost:

- združljivost s ponujenim upravljalnim in nadzornim sistemom omrežja podatkovnega centra
- Združljivost s ponujenim Dostopovnim stikalom podatkovnega centra v Leaf-Spine konfiguraciji (M.1.7)

Režim podpore: Redundantni

M.1.7 Dostopovno stikalo podatkovnega centra

- podpora za IPv4 in IPv6,
- podpora za VXLAN EVPN fabrics,
- podpora za protokole:
 - Border Gateway Protocol (BGP),
 - Open Shortest Path First (OSPF),
 - Enhanced Interior Gateway Routing Protocol (EIGRP),
 - Routing Information Protocol Version 2 (RIPv2),
 - Protocol Independent Multicast Sparse Mode (PIMSM),
 - Source-Specific Multicast (SSM),
 - Multicast Source Discovery Protocol (MSDP),
- podpora za standarde upravljanja:
 - Ansible,
 - Chef,
 - Puppet,
 - SALT,
 - RESTCONF/NETCONF,
 - JSON based RPC over HTTP/HTTPS,
- podpora za kriptiranje s prepustnostjo vsaj 1 Gbps na vseh vtičnicah za:
 - IEEE 802.1ae MAC Security (MACsec),
 - Cloudsec (VTEP to VTEP encryption),

- upravljanje medpomnilnika (intelligent buffer management) s podporo za:
 - prepoznavanje majhnih in velikih pretokov podatkov (mice and elephant flows) na omrežju in preprečevanje preobremenjenosti povezav (link congestion),
 - Approximate Fair Dropping (AFD),
 - Elephant Trap (ETRAP),
 - Dynamic Packet Prioritization (DPP),
- podpora za RDMA over Converged Ethernet in DCB protokole:
 - Priority-based Flow Control (PFC),
 - Enhanced Transmission Selection (ETS),
 - Data Center Bridging Exchange Protocol (DCBX),
 - Explicit Congestion Notification (ECN),
- podpora za visoko razpoložljivost z uporabo:
 - Virtual Port-Channel (vPC) tehnologije,
 - Equal-Cost MultiPath (ECMP) usmerjanja,
- operacijski sistem s podporo za:
 - medsebojno neodvisne procese za protokole usmerjanja,
 - možnost ponovnega zagona posameznega procesa brez izgube stanja (restart without loss of state),
 - brezprekinitveno nameščanje popravkov med delovanjem (hot patching),
- podpora za centralno upravljanje s ponujenim sistemom za upravljanje omrežja podatkovnega centra
- možnost nadzora mrežnega prometa s podporo za:
 - Test Access Points (TAPs),
 - Switched Port Analyzer (SPAN) aggregation.
- višina 1U z možnostjo vgradnje v standardno 19" komunikacijsko omaro,
- vsaj dva redundantna napajalnika z možnostjo zamenjave med delovanjem,
- redundantni ventilatorji z možnostjo zamenjave med delovanjem,
- pretok zraka od zadaj naprej, izhod zraka na strani, kjer so vmesniki (port side exhaust),
- vsaj 6 fiksnih QSPF28 40/100 Gbps vmesniških rež (uplink ports),
- vsaj 48 fiksnih 1/10/25 Gbps vmesniških rež (downlink ports),
- CPU z vsaj 6 jedri,
- vsaj 32GB sistemskega pomnilnika,
- SSD pogon vsaj 128 GB,
- predpomnilnik (system buffer) vsaj 40 MB,
- priključek RJ-45 za upravljanje (management port),
- priključek USB ali RS-232,
- prepustnost (switching capacity) do vsaj 3,6 Tbps (bitov na sekundo),
- prepustnost (forwarding rate) do vsaj 1,2 Bpps (paketov na sekundo),
- največje število IPv4 Longest Prefix Match (LPM) routes: 1792000

- največje število IPv4 host entries: 1792000,
- največje število IPv6 Longest Prefix Match (LPM) routes: 896000,
- največje število IPv6 host entries: 1792000,
- največje število MAC address entries: 512000,
- največje število multicast routes: 128000,
- število Internet Group Management Protocol (IGMP) snooping groups: vsaj 8000,
- največje število ACL entries (per slice the forwarding engine) ingress: 5000,
- največje število ACL entries (per slice the forwarding engine) egress: 2000,
- največje število VLANov: 4096,
- število Virtual Routing in Forwarding (VRF) instanc: vsaj 1000,
- največje število ECMP poti: 64,
- največje število port channels: 512,
- največje število povezav na port channel: 32,
- število aktivnih SPAN sej: vsaj 4,
- največje število VLANov v RPVST instancah: 3967,
- največje število Hot-Standby Router Protocol (HSRP) grup: 490,
- število Network Address Translation (NAT) entries: vsaj 1023,
- največje število Multiple Spanning Tree (MST) instanc: 64.

Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potreba ustrezna licenca ali naročnina, mora biti vključena za ves čas trajanja pogodbe.

Zahtevana združljivost:

- združljivost z upravljavskim in nadzornim sistemom
- Združljivost s ponujenim Hrbteničnim stikalom podatkovnega centra v Leaf-Spine konfiguraciji

Režim podpore: Redundantni

M.2.1 Požarna pregrada Tip 1

Splošne lastnosti

- požarna pregrada za vgradnjo v 19" telekomunikacijsko omaro,
- podpora za IPv4 in IPv6 promet,
- požarna pregrada mora imeti podvojen napajalni sistem, ki se ga lahko zamenja v stanju delovanja naprave

- požarna pregrada mora imeti bliskovni pogon (SSD disk) velikosti vsaj 900 GB in prosto režo za vgradnjo dodatnega diska
- spomin 128 GB RAM
- temperaturno območja delovanja: vsaj od 0 °C do +40 °C,
- najmanjše število vmesnikov:
 - o 8× 1/10 Gigabit (SFP+)
 - o namenski konzolni vmesnik za nadzor in upravljanje (RJ-45)
 - o USB vmesnik
 - o Možnost razširitve 4x40/100/200 Gigabit
- Vmesniki morajo podpirati povezovanje do 4 fizičnih vmesnikov v en logični vmesnik – "link aggregation" po protokolu IEEE 802.1ax (LACP)
- podpora funkcionalnostim in protokolom:
 - o VPN Lan2Lan povezovanje in oddaljen dostop s klientom
 - o Lan2Lan podpora verzijam Ikev1 in Ikev2
 - o Omogočati mora mehanizme kakovosti storitev (QoS) in omogočati prioritizacijo občutljivega prometa in omejevanje pasovne širine aplikacijam na vhodu in izhodu omrežnih vmesnikov
 - o 802.1q in izbiro oznake VLAN-a med številkami 1 in 4094
 - o DHCP server, DHCP relay
 - o Usmerjevalni protokoli: BGP, OSPF, EIGRP
 - o Podpora za multicast usmerjanje in nastavitve PIM RP
 - o Možnost delovanja v gruči vsaj do 16 naprav
 - o Podpora za 100 virtualnim usmerjevalnim instancam (VRF)
 - o PxGrid2.0 za integracijo z ISE
 - o Podpora pravilom, ki vključujejo SGT oznake
- delovanje v načinu »active/active« ali »active/standby«

Tehnična specifikacija in zahtevane funkcionalnosti opreme

- Prepustnost požarne pregrade:
 - o z vključenimi AVC funkcionalnostmi: vsaj 60 Gbps

o z AVC in s »Threat Prevention« funkcionalnostmi: vsaj 60 Gbps

- Št. sočasnih povezav preko požarne pregrade z vključenim AVC: vsaj 15 milijonov
- Št. novih povezav na sekundo z vključenim AVC: vsaj 350.000
- VPN IPSec prepustnost: 45 Gbps
- Multi instance način - več primerkov kontejnerjev na enem samem ohišju, ki delujejo kot popolnoma neodvisne naprave.
- Upravljanje požarnih pregrad (pisanje in nameščanje politik se morata izvajati iz enotne točke) mora biti izvedeno z ločenim virtualiziranim centralnim sistemom za upravljanje za okolje VMware
- Pregled, zapis in filtriranje logov se mora izvajati na centralnem upravljalnem sistemu
- Rešitev mora zagotavljati avtomatsko posodobitev baz posameznih varnostnih mehanizmov s strani proizvajalca (Threat Prevention) za celoten čas trajanja pogodbe
- Omogočati mora simulacijo prehoda prometa prek požarne pregrade in analizo varnostnih nastavitvev, ki se aplicirajo v primeru simuliranega prometa

M.2.2 Požarna pregrada Tip 2

Splošne lastnosti

- požarna pregrada za vgradnjo v 19" telekomunikacijsko omaro,
- podpora za IPv4 in IPv6 promet,
- požarna pregrada mora imeti podvojen napajalni sistem, ki se ga lahko zamenja v stanju delovanja naprave
- požarna pregrada mora imeti bliskovni pogon (SSD disk) velikosti vsaj 900 GB in prosto režo za vgradnjo dodatnega diska,
- spomin 64 GB RAM
- temperaturno območja delovanja: vsaj od 0 °C do +40 °C,
- najmanjše število vmesnikov:
 - o 8× 100M/1G BASE-T Ethernet vmesniki (RJ-45)
 - o 8× 1/10 Gigabit (SFP+)
 - o namenski konzolni vmesnik za nadzor in upravljanje (RJ-45)
 - o USB vmesnik

- Vmesniki morajo podpirati povezovanje do 4 fizičnih vmesnikov v en logični vmesnik – "link aggregation" po protokolu IEEE 802.1ax (LACP)
- podpora funkcionalnostim in protokolom:
 - o VPN Lan2Lan povezovanje in oddaljen dostop s klientom
 - o Lan2Lan podpora verzijam Ikev1 in Ikev2
 - o Omogočati mora mehanizme kakovosti storitev (QoS) in omogočati prioritizacijo občutljivega prometa in omejevanje pasovne širine aplikacijam na vhodu in izhodu omrežnih vmesnikov
 - o 802.1q in izbiro oznake VLAN-a med številkami 1 in 4094
 - o DHCP server, DHCP relay
 - o Usmerjevalni protokoli: BGP, OSPF, EIGRP
 - o Podpora za multicast usmerjanje in nastavitve PIM RP
 - o Možnost delovanja v gruči vsaj do 8 naprav
 - o Podpora za 15 virtualnim usmerjevalnim instancam (VRF)
 - o PxGrid2.0 za integracijo z ISE
 - o Podpora pravilom, ki vključujejo SGT oznake
- delovanje v načinu »active/active« ali »active/standby«

Tehnična specifikacija in zahtevane funkcionalnosti opreme

- Prepustnost požarne pregrade:
 - O z vključenimi AVC funkcionalnostmi: vsaj 16 Gbps
 - o z AVC in s »Threat Prevention« funkcionalnostmi: vsaj 16 Gbps
- Št. sočasnih povezav preko požarne pregrade z vključenim AVC: vsaj 2 milijone
- Št. novih povezav na sekundo z vključenim AVC: vsaj 128.000
- VPN IPSec prepustnost: 10 Gbps
- Multi instance način - več primerkov kontejnerjev na enem samem ohišju, ki delujejo kot popolnoma neodvisne naprave.
- Upravljanje požarnih pregrad (pisanje in nameščanje politik se morata izvajati iz enotne točke) mora biti izvedeno z ločenim virtualiziranim centralnim sistemom za upravljanje za okolje VMware

- Pregled, zapis in filtriranje logov se mora izvajati na centralnem upravljalnem sistemu
- Rešitev mora zagotavljati avtomatsko posodobitev baz posameznih varnostnih mehanizmov s strani proizvajalca (Threat Prevention) za celoten čas trajanja pogodbe
- Omogočati mora simulacijo prehoda prometa prek požarne pregrade in analizo varnostnih nastavitev, ki se aplicirajo v primeru simuliranega prometa

Režim podpore: Redundantni

M.2.3 Sonda za spremljanje in zaznavo dogodkov v OT omrežju

Sonda za spremljanje in zaznavo dogodkov v OT omrežju mora biti kompatibilna s ponujenim sistemom za spremljanje in zaznavo dogodkov v OT (P.1.5). Je v obliki naprave, ki se lahko namesti na DIN letev v zahtevnih okoljskih pogojih. Naprava je lahko namenska sonda ali ima še druge funkcionalnosti. Namen naprave ni spremljanje OT omrežja na ravni dostopovnih stikal, ampak orodje za spremljanje tudi drugih delov omrežja, ki niso predmet tega projekta.

Tehnične specifikacije:

- Vsaj 2x 1000 Base-T RJ-45
- Sondiranje na vsaj gigabitnem mrežnem vmesniku
- Vsaj 2x 1000 Base-X SFP uplink
- Zaščita vsaj IP 30, brez ventilatorja
- Sondažna programska oprema mora omogočati IDS na podlagi redno posodobljenih IPS podpisov za zaznavanje novih in neznanih groženj.

Vključena licenca za vsaj 100 spremljanih naprav.

Režim podpore: Redni

M.3.1 Upravljalni in nadzorni sistem požarnih pregrad

Sistem je integriran z ostalimi nadzornimi sistemi za upravljanje mrežne opreme. Zaradi namenske funkcionalnosti upravljanja požarnih pregrad mora imeti sledeče značilnosti:

- Centralno upravljanje vseh požarnih pregrad, politik in nastavitev iz enotne konzole.
- Spremljanje in analiza dogodkov z naprednimi filtri, poročili in obveščanje o incidentih.
- Upravljanje varnostnih politik z možnostjo definiranja pravil glede na aplikacijo, uporabnika ali omrežno cono.
- Avtomatizirano posodabljanje varnostnih podpisov.
- Integracija z drugimi varnostnimi sistemi preko API vmesnikov.

Režim podpore: Redni

M.3.2 Upravljavski in nadzorni sistem omrežja podatkovnega centra

Opis sistema je v splošnih tehničnih specifikacijah.

M.3.3 Upravljalni in nadzorni sistem za lokalna omrežja

Funkcionalnosti in podpora za:

- nadzorna plošča z enostavnim pregledom statusa omrežja, odjemalcev ter aplikacij
- samodejno odkrivanje naprav in njihovega inventarja v topologiji omrežja
- zahtevana integracija s ponujenim sistemom za upravljanje identitet in avtoriziranje
- odkrivanje in prikaz topologije omrežja
- definiranje inventarja omrežnih naprav in dodeljevanje v uporabniške skupine
- prilagoditev prikaza topologije omrežja glede na uporabnikove želje
- funkcionalnost PnP (Plug&Play) za instantno postavitve stikal, usmerjevalnikov ali kontrolerjev dostopnih točk. Omrežne naprave imajo vgrajeni PnP agent, ki samodejno vzpostavi povezavo do PnP strežnika (na aplikaciji), le-ta pa napravi pošlje ustrezno verzijo operacijskega sistema ter konfiguracijske nastavitve.
- podrobnejši vpogled v delovanje aplikacij, dostopnih točk, kontrolerjev dostopnih točk ter odjemalcev
- prikaz stanja posamezne naprave (0-100%) za stikala, usmerjevalnike in dostopne točke
- pregled vrednosti stanja naprave za nazaj
- možnost izvajanja CLI ukazov na skupini naprav
- možnosti izdelava tipičnih konfiguracij ali predlog za postavitve omrežnih naprav
- enostavno kreiranje politik ACL ter njihovo namestitve na omrežju
- enostavno kreiranje politik QoS ter njihovo namestitve na omrežju
- pregled poteka prometa od izvora do ponora na topologiji omrežja
- pri pregledu pretoka upošteva sezname ACL in njihov vpliv na delovanje željenega toka podatkov
- vidljivost aplikacij v omrežju
- izdelovanje poročil po meri na podlagi vnaprej definiranih osnutkov
- možnost upravljanja s programsko opremo naprav in enostavno nadgrajevanje omrežnih naprav
- avtomatizacijo na podlagi omrežne politike
- možnost »časovnega skoka nazaj« za vpogled stanja na omrežju v obdobju, ko so se pojavile anomalije
- porazdeljena detekcija varnostnih anomalij
- proaktivno odkrivanje napak na omrežnih napravah ter vgrajene procedure za vodeno pomoč pri odpravi napak v omrežju
- možnost neposrednega komuniciranja med nadzornim sistemom in naprednejšo točko dostopa za zbiranje neposrednih paketov posameznega odjemalca in njegove statistike
- preverjanje zmogljivost aplikacij na omrežju (izguba paketov, zakasnitve ter paketno

»tresenje«),

- zbiranje telemetričnih podatkov (Netflow, SNMP, Syslog)
- možnost integracije z zunanjimi sistemi kot npr. IPAM in ITSM (IT service management)
- API vmesnik za integracije drugih sistemov
- možnost vzpostavitve nadzornega sistema v visoko razpoložljivem načinu (HA)

Upravljanje naprav:

- nadzorni sistem mora podpirati nadzor ponujenih stikal

Zahtevana programska oprema, naročnine in licence:

- programska oprema mora zagotavljati vse zgoraj zahtevane funkcionalnosti,
- v primeru, da je za delovanje zgoraj naštetih funkcionalnosti potrebna ustrezna licence ali naročnina, mora biti le-ta vključena za ves čas trajanja pogodbe

Režim podpore: Redundantni

M.3.4 Upravljalni sistem za MPLS omrežje

1. Sistem

- Aplikacija za upravljanje MPLS omrežja mora podpirati namestitev v obliki navideznega stroja (angl. Virtual machine) ali samostojnega strežnika
- Podpora lokalni namestitvi v lokalno okolje VMware
- Podpora namestitvi z najmanj 2 ločenima omrežnima vmesnikoma
 - Prvi vmesnik služi upravljavskemu dostopu (angl. OOB) do nadzornega sistema
 - Drugi vmesnik služi povezavi do omrežnih naprav
- Zmožnost širitve sistema povezano z rastjo omrežja (rast števila naprav, povezav, povezav internega usmerjevalnega protokola, politik, storitev)
- Podpora vzpostavitvi v načinu popolne podvojenosti

2. Splošno

- Zmožnost zbiranje podatkov o logičnih in fizičnih objektih pridobljenih s strani naprav
- Zagotavljati enoten uporabniški vmesnik za vključevanje in spremljanje naprav, zagotavljanja storitev, virtualizacijo in optimizacijo SR politik, prikaz inventarja naprav in storitev ter vizualizacijo topologije.
- Zmožnost izrisa in vizualizacije topologije storitve s pomočjo 3D zemljevida

- Omogočati analizo zgodovinskih zapisov vseh inventarnih virov, topologije in sprememb storitev.
- Tabelarni prikaz naprav, vmesnikov, kartic, povezav, SR politik in storitev
- Omogočati samodejno odkrivanje omrežnih virov, storitev in statusa razpoložljivosti na podlagi NETCONF/YANG za fizično topologijo in odkrivanje storitev
- Prikaz in vizualizacija inventarja omrežnih naprav in storitev na zemljevidu in logični shemi
- Odkrivanje povezav z omogočenim internim usmerjevalnim protokolom (angl. IGP) skupaj z metriko povezave (angl. cost), IS-IS area, OSPF device ID, SRGB,BW
- Odkrivanje topologije internega usmerjevalnega protokola z mehanizmom BGP-LS
- Odkrivanje fizičnih in L2 povezav med dvema sosednima napravama
- Podpora optimizaciji omrežja v realnem času s pomočjo protokolov, kot sta BGP-LS in PCEP (angl. Path Computation Element Protocol).
- Podpora zaprto-zančni (angl. Closed Loop) optimizaciji omrežja na podlagi specifičnih YANG modelov za podrobne vpogleds v stanje omrežja in storitev ter ustrezno ukrepanje po potrebi.
- Podpora standardnemu vmesniku (IETF ACTN) za integracijo z ostalimi sistemi (angl. Northbound) in izvajanje IP CRUD operacij
- Podpora hierarhičnemu abstraktnemu pogledu na celotno omrežje, ki ga upravlja, s ciljem zmanjšanja kompleksnosti ter uporabe minimalnega nabora parametrov za učinkovito porabo virov in skalabilnost.

3. SR-PCE

- Zagotavljanje SR-PCE zmogljivosti in »statefull« PCE funkcionalnost, ki omogočata nadzor in premikanje TE tunelov za optimizacijo omrežja.
- Z uporabo SR-PCE komponente mora nadzorni sistem omogočati odkrivanje SR politik in povezav tipa L3, konfiguriranih v omrežju. Odkrite SR politike morajo biti vizualizirane in nadzorovane preko nadzornega sistema.
- Nadzorni sistem mora uporabljati kombinacijo telemetrije in Segment Routing PCE (SR-PCE) za analizo in izračun optimalnih TE tunelov.
- Nadzorni sistem mora samodejno odkriti in vključiti (angl. onboard) omrežne naprave, ki sodelujejo v PCE topologiji v spremljanje.
- Nadzorni sistem skupaj s SR-PCE zmogljivostmi mora podpirati SR-TE politike, ki temeljijo na vrednosti zakasnitve v internem usmerjevalnem protokolu.

4. SR-MPLS, SR-TE, RSVP-TE

- Podpora odkrivanja RSVP-TE tunelov vključno z njihovo potjo in preslikavo na podlagi poti v internem usmerjevalnem protokolu.

- Podpora prikazu uporabljenih poti LSP, prikaz dogodkov spremembe poti LSP na zemljevidu.
- Podpora odkrivanju in prikazu poti na podlagi atributa »Tree-SID«
- Podpora odkrivanju poti, ki temeljijo na SR CS
- Podpora odkrivanju poti in vizualizacija, ki temeljijo na SR Flex-Algo
- Zagotavljanje sočasne vizualizacije v realnem času za omrežne poti in infrastrukturo ter politike, ki temeljijo na protokolih SR-TE in RSVP-TE
- Podpora ustvarjanju in aktiviranju RSVP-TE in SR TE politik z eksplicitno določenimi vrednostnimi SLA
- Podpora vizualizacije topologije v realnem času vseh naprav, povezav, njihove uporabe, SR TE politik ali RSVP-TP tunelov vzpostavljenih v omrežju
- Podpora prikazu posamezne SR TE politike in prikaz na zemljevidu
- Podpora prikazu celotne topologije in zmožnost prikaza podrobnejšega prikaza posamezne TE politike.
- Podpora prikazu in predogledu SR TE in RSVP-TE politike pred namestitvijo in aktivacijo v omrežju.
- Podpora metodologiji CRUD za SR TE in RSVP-TE politike
- Podpora samodejnega odkrivanja celovitosti omrežnih virov, storitev in razpoložljivosti, ki temelji le na PCEP za odkrivanje poti LSP in njihovih stanj. PCEP mora zagotavljati informacije o poteh (LSP) z različnimi protokolnimi razširitvami za podporo RSVP, RSVP-TE, SR in SR-TE.
- PCE mora sprožiti izračun poti za alternativno »najboljšo« pot LSP.

5. Upravljanje storitev

- Podpora vzpostavitvi L2VPN storitev na osnovi IETF L2NM modelov z ustreznimi vrednostmi SLA.
- Podpora vzpostavitvi L3VPN storitev na osnovi IETF L3NM modelov z ustreznimi vrednostmi SLA.
- Podpora vizualizaciji SR politik in VPN storitev kot prekrivanje na zemljevidu omrežne topologije
- Podpora vzpostavitvi in vizualizaciji EVPN ELAN in E-Tree storitev.
- Podpora vzpostavitvi L3VPN in L2VPN storitev s specficirano SR politiko in ustreznimi vrednostnimi SLA.

6. Realno-časovno zbiranje podatkov

- Podpora telemetriji preko gRPC (angl. Network Management Interface -gNMI)
- Podpora zbiranju informacij o zmogljivosti v realnem času ter optimizacijo omrežja za zagotavljanje vrednosti SLA.
- Podpora zmožnosti zbiranja podatkov na osnovi standardnih zahtev.

- Podpora zbiranju informacij o napakah in zmogljivosti v realnem času ter optimizirati omrežje za zagotavljanje vrednosti SLA.
- Podpora uporabi podatkovnega rudarjenja (angl. data mining) za analizo.
- Podpora zbiranju ustreznih podatkov iz omrežnih naprav z uporabo več protokolov, vključno s CLI, SNMP in Model Driven Telemetry.

7. ZTP

- Podpora klasičnim zmožnostim Zero Touch Provisioning(ZTP).
- Podpora varnemu načinu ZTP v skladu s RFC8572.
- Podpora ločeni nadzorni plošči za informacije in aktivnosti povezane z ZTP

Režim podpore: Redundantni

M.3.6 Sistem za upravljanje z indentitetami in avtorizacijami uporabnikov omrežja

- Avtentikacijo naprav in uporabnikov z uporabo standardnega protokola IEEE 802.1X in vsaj naslednjih metod EAP: EAP-MD5, EAP-TLS, PEAP, EAP-FAST.
- Komunikacijo z drugimi omrežnimi napravami z uporabo varnostnih protokolov RADIUS.
- Avtentikacijo uporabnikov in naprav z uporabo naslednjih baz podatkov: lokalna baza podatkov uporabnikov, lokalna baza podatkov naprav, zunanji strežnik RADIUS, zunanji strežnik LDAP, zunanji imenik Windows Active Directory, digitalna potrdila.
- Popolno integracijo z bazo podatkov Active Directory za izvajanje funkcije enotne prijave. Uporabniško ime in geslo, ki se uporabljata pri avtentikaciji sistema Windows, je treba uporabljati tudi za druge nadzore dostopa, ne da bi ju bilo treba ponovno vnesti.
- Avtentikacijo uporabnikov prek portala HTTPS z avtomatsko preusmeritvijo.
- Preverjanje digitalnih potrdil v skladu z naslednjimi merili: Podpora za registracijo vsaj dveh zunanjih overiteljev potrdil, podpora za prenos seznama preklicanih potrdil (CRL) prek protokola HTTP, podpora za protokol OCSP za preverjanje stanja potrdila.
- Avtorizacija mora zagotavljati: dodelitev VLAN, polno podporo za standard IEEE 802.1AE, vključno z dodelitvijo »Security TAG (STG)«, kot je opisano v IEEE 802.1AE, podporo za spremembo avtorizacije (CoA) protokola RADIUS.
- Upravljanje začasnih uporabniških računov – gostje/svetovalci
- Ustvarjanje začasnih uporabniških računov mora podpirati različne profile z različnimi privilegiji in vsaj naslednje: profil gosta z dostopom samo do interneta prek HTTP, profil svetovalca z dostopom samo do interneta in intraneta prek HTTP.
- Podpora za časovne profile, ki so dodeljeni začasnemu računu ali skupini začasnih računov. Skrbnik uporabniškega računa lahko določi začetek in konec veljavnosti za vsak začasni račun posebej.

- Upravljanje, konfiguracija in spremljanje celotnega sistema prek grafičnega spletnega vmesnika.
- Okno za stalno spremljanje preverjanja pristnosti v realnem času s trenutnim prikazom naslednjih podatkov o preverjanju pristnosti: ura in datum, stanje preverjanja pristnosti, uporabniško ime/naprava in MAC naslov, IP naslov, NAD, vmesnik, razlog za napako, način preverjanja pristnosti, protokol preverjanja pristnosti.
- Implementacija v virtualnem okolju stranke z najmanj 1 virtualno napravo (Vmware).
- Licence in podpora proizvajalca za 180 končnih naprav.

Režim podpore: Redundantni

S.1.1 Zmogljiv strežnik

Osnovne lastnosti:

- Vgradnja v 19" strežniško omaro (rack)
- Izvlečno vodilo
- Mehanska roka za upravljanje kablov
- Višina do največ 2U
- Možnost vgradnje procesorjev serije AMD EPYC 9005 ali novejše

Procesor:

- 2x AMD EPYC 9135 ali zmogljivejša, vsak z:
 - osnovni takt vsaj 3.65GHz
 - vsaj 16 jeder

Pomnilnik:

Podprto:

- vsaj 12 DDR5 DIMM mest za vsak processor
- maksimalen takt 6400MHz
- do 6TB skupne kapacitete
- ECC, SDDC, ECC Error Check

Vgrajeno:

- vsaj 512GB
- vsaj 12 zapolnjenih DDR5 DIMM mest
- takt vsaj 6400MHz

Shranjevanje podatkov:

Podprto:

- možnost vgradnje 12x 2.5" hot swap diskov
- podpora SAS, SATA, NVMe priključkom
- možnost vgradnje M.2 NVMe zagonskih diskov
- zaščita RAID1 za zagonske diske

Vgrajeno:

- vsaj 4x 3.84TB SSD (NVMe, read intensive, 2.5", hot swap)
- 2 x 960GB SSD (NVMe, read intensive, M.2) zagonska diska v RAID 1 konfiguraciji

Razširitvena mesta:

- **Možnost raširitve do vsaj 10x PCIe Gen4/5**
- OCP razširitev

Povezljivost Ethernet:

- vsaj 8x 10/25GbE SFP28 na dveh (2) ločenih karticah
- SFP28 MM priloženi

Možnost nadgradnje s FC priključki do hitrosti vsaj 64Gbit/s

Napajanje in hlajenje:

- redundančno napajanje in hlajenje
- ventilatorji in napajalniki hot swap
- 2x vsaj 1000W (Titanium, hot swap)
- 2x vsaj 4.3m napajalni kabli

Servisni priključki:

- Spredaj: vsaj **VGA+ 2x USB 3.1, od tega vsaj en USB 3.1** ~~+VGA~~
- Zadaj: 3x USB, **od tega vsaj en USB 3.1** + 1x VGA
- Servisni priključek: 1x RJ45 (10/100/1000 Mbps)

Konfiguracija ustreza:

- Standard ASHRAE Razred A2 z delovanjem od 10°C do 35°C

Upravljanje sistema:

- Zaznavanje napak v sistemu za procesorje, pomnilnik, VRM, diske, napajalne enote in ventilatorje (PFA)
- Možnost deljenja virtualne konzole z vsaj 6 uporabniki.
- Možnost blokiranja določenega IP-ja.
- Spremljanje obremenjenosti procesorja, pomnilnika in porabe energije v realnem času, možnost omejevanja moči (vključno s zgodovinskimi podatki).

Podprti operacijski sistemi:

- Microsoft Windows Server 2025
- Red Hat Enterprise Linux (RHEL) 9 in 10
- SUSE Linux Enterprise Server (SLES) 15
- VMware vSphere (ESXi) 8
- Konfiguracija certificirana kot vSAN ESA ReadyNode
- Konfiguracija narejena vsaj po specifikaciji vSAN-ESA-AF-0 iz dokumenta Broadcom vSAN ESA ReadyNode Hardware Guidance (<https://compatibilityguide.broadcom.com/pages/vsan-esa-readynode-hardware-guidance>)"

Priložene licence za programsko opremo:

- VMware Cloud Foundations (32 jeder oz. skladno s ponujeno velikostjo procesorja, 5 let)

Vzdrževanje:

- 5 let vzdrževanja v režimu
 - servisni paket proizvajalca opreme
 - razpoložljivost za prijavo napak 9x5
 - zagotovljena odprava naslednji delovni dan
- zagotovljeni rezervni deli vsaj 7 let
- vzdrževanje zagotavlja proizvajalec

S.1.2 Lokalni strežnik**Osnovne lastnosti:**

- Vgradnja v 19" strežniško omaro (rack)
- Izvlečno vodilo
- Mehanska roka za upravljanje kablov
- Višina do največ 2U
- Možnost vgradnje procesorjev serije AMD EPYC 9005 ali novejše

Procesor:

- 1x AMD EPYC 9135 ali zmogljivejši:
 - O osnovni takt vsaj 3.65GHz
 - O vsaj 16 jeder

Pomnilnik:**Podprto:**

- vsaj 12 DDR5 DIMM mest za vsak processor
- maksimalen takt 6400MHz
- do 6TB skupne kapacitete
- ECC, SDDC, ECC Error Check

Vgrajeno:

- vsaj 384GB
- takt vsaj 6400MHz

Shranjevanje podatkov:

Podprto:

- možnost vgradnje 12x 2.5" hot swap diskov
- podpora SAS, SATA, NVMe priključkom
- možnost vgradnje M.2 NVMe zagonskih diskov
- zaščita RAID1 za zagonske diske

Vgrajeno:

- vsaj 3x 3.84TB SSD (NVMe, read intensive, 2.5", hot swap)
- 2 x 960GB SSD (NVMe, read intensive, M.2) zagonska diska v RAID 1 konfiguraciji

Razširitvena mesta:

- **Možnost razširitve do vsaj 10x PCIe Gen4/5**
- OCP razširitev

Povezljivost Ethernet:

- vsaj 8x 10/25GbE SFP28 na dveh (2) ločenih karticah
- SFP28 MM priloženi

Možnost nadgradnje s FC priključki do hitrosti vsaj 64Gbit/s

Napajanje in hlajenje:

- redundančno napajanje in hlajenje
- ventilatorji in napajalniki hot swap
- 2x vsaj 1000W (Titanium, hot swap)
- 2x vsaj 4.3m napajalni kabli

Servisni priključki:

- Spredaj: vsaj **VGA + 2x USB, od tega vsaj en USB 3.1 + VGA**
- Zadaj: 3x USB, **od tega vsaj en USB 3.1 + 1x VGA**
- Servisni priključek: 1x RJ45 (10/100/1000 Mbps)

Konfiguracija ustreza:

- Standard ASHRAE Razred A2 z delovanjem od 10°C do 35°C

Upravljanje sistema:

- Zaznavanje napak v sistemu za procesorje, pomnilnik, VRM, diske, napajalne enote in ventilatorje (PFA)
- Možnost deljenja virtualne konzole z vsaj 6 uporabniki.
- Možnost blokiranja določenega IP-ja.
- Spremljanje obremenjenosti procesorja, pomnilnika in porabe energije v realnem času, možnost omejevanja moči (vključno s zgodovinskimi podatki).

Podprti operacijski sistemi:

- Microsoft Windows Server 2025
- Red Hat Enterprise Linux (RHEL) 9 in 10
- SUSE Linux Enterprise Server (SLES) 15
- VMware vSphere (ESXi) 8
- Konfiguracija certificirana kot vSAN ESA ReadyNode
- Konfiguracija narejena vsaj po specifikaciji vSAN-ESA-AF-0 iz dokumenta Broadcom vSAN ESA ReadyNode Hardware Guidance (<https://compatibilityguide.broadcom.com/pages/vsan-esa-readynode-hardware-guidance>)"

Priložene licence za programsko opremo:

- VMware Cloud Foundations (16 jeder oz. skladno s ponujeno velikostjo procesorja, 5 let)

Vzdrževanje:

- - 5 let vzdrževanja v režimu
 - servisni paket proizvajalca opreme
 - razpoložljivost za prijavo napak 9x5
 - zagotovljena odprava naslednji delovni dan
- - zagotovljeni rezervni deli vsaj 7 let
- - vzdrževanje zagotavlja proizvajalec

S.1.3 Backup strežnik**Osnovne lastnosti:**

- Vgradnja v 19" strežniško omaro (rack)
- Izvlečno vodilo

- Mehanska roka za upravljanje kablov
- Višina do 2U
- Možnost vgradnje procesorjev serije AMD EPYC 9005 ali novejše

Procesor:

- 2x AMD EPYC 9135 ali zmogljivejša, vsak z:
 - osnovni takt vsaj 3.65GHz
 - vsaj 16 jeder

Pomnilnik:**Podprto:**

- vsaj 12 DDR5 DIMM mest za vsak processor
- maksimalen takt 6400MHz
- do 6TB skupne kapacitete
- ECC, SDDC, ECC Error Check

Vgrajeno:

- vsaj 512GB
- vsaj 6 zapolnjenih DDR5 DIMM mest
- takt vsaj 6400MHz

Shranjevanje podatkov:**Podprto:**

- možnost vgradnje 32x 2.5" hot swap diskov
- podpora SAS, SATA, NVMe priključkom
- možnost vgradnje M.2 NVMe zagonskih diskov
- zaščita RAID1 za zagonske diske

Vgrajeno:

- vsaj 4x 3.84TB SSD (NVMe, read intensive, 2.5", hot swap)
- 2 x 960GB SSD (NVMe, read intensive, M.2) zagonska diska v RAID 1 konfiguraciji

Razširitvena mesta:

- **Možnost raširitve do vsaj 10x PCIe Gen4/5**
- OCP razširitev

Povezljivost Ethernet:

- vsaj 8x 10/25GbE SFP28 na dveh (2) ločenih karticah
- SFP28 MM priloženi

Možnost nadgradnje s FC priključki do hitrosti vsaj 64Gb

Napajanje in hlajenje:

- redundančno napajanje in hlajenje
- ventilatorji in napajalniki hot swap
- 2x vsaj 1000W (Titanium, hot swap)
- 2x vsaj 4.3m napajalni kabli

Servisni priključki:

- Spredaj: vsaj **VGA+** 2x USB, **od tega vsaj en USB 3.1 + VGA**
- Zadaj: 3x USB, **od tega vsaj en USB 3.1 + 1x VGA**
- Servisni priključek: 1x RJ45 (10/100/1000 Mbps)

Konfiguracija ustreza:

- Standard ASHRAE Razred A2 z delovanjem od 10°C do 35°C

Upravljanje sistema:

- Zaznavanje napak v sistemu za procesorje, pomnilnik, VRM, diske, napajalne enote in ventilatorje (PFA)
- Možnost deljenja virtualne konzole z vsaj 6 uporabniki.
- Možnost blokiranja določenega IP-ja.
- Spremljanje obremenjenosti procesorja, pomnilnika in porabe energije v realnem času, možnost omejevanja moči (vključno s zgodovinskimi podatki).

Podprti operacijski sistemi:

- Microsoft Windows Server 2025
- Red Hat Enterprise Linux (RHEL) 9 in 10
- SUSE Linux Enterprise Server (SLES) 15
- VMware vSphere (ESXi) 8
- Konfiguracija certificirana kot vSAN ESA ReadyNode
- Konfiguracija narejena vsaj po specifikaciji vSAN-ESA-AF-0 iz dokumenta Broadcom vSAN ESA ReadyNode Hardware Guidance (<https://compatibilityguide.broadcom.com/pages/vsan-esa-readynode-hardware-guidance>)"

Priložene licence za programsko opremo:

- Licenca za programsko opremo za Backup je opisana v poglavju P.1.1

Vzdrževanje:

- 5 let vzdrževanja v režimu
 - servisni paket proizvajalca opreme
 - razpoložljivost za prijavo napak 9x5
 - zagotovljena odprava naslednji delovni dan
- zagotovljeni rezervni deli vsaj 7 let
- vzdrževanje zagotavlja proizvajalec

S.1.4 Backup shranjevalni sistem

Shranjevalni sistem Flash za varnostne kopije, hitro okrevanje in DR

1. Kapaciteta - sistem mora zagotavljati naslednje kapacitete za varnostne kopije:

- 220 TB raw kapacitete na vsaj 12 NVMe modulih, možnost širitve do 500 TB raw kapacitete brez menjave kontrolerjev (tj. zgolj z dodajanjem shranjevalnih kapacitet).
- Zagotovljena kapaciteta za vsaj 700 TB podatkov/varnostnih kopij, ki je v celoti zaščitena z dvojno pariteto, pri tem mora zagotavljati vse zahtevane zmogljivosti.
- Vsi posegi za nadgradnje kapacitet morajo biti izvedljivi brez prekinitev dostopa strežnikov do podatkov.

2. Zmogljivost - kapacitete za varnostne kopije in hitro okrevanje v primeru večjega napada:

- Zmogljivost prenosa podatkov za shranjevanje varnostnih kopij (zapisovanje) vsaj 4 GB/s oziroma vsaj 14 TB/uro.
- Zmogljivost prenosa podatkov za okrevanje (branje) vsaj 10 GB/s oziroma 36 TB/uro.
- Za namene »Instant Recovery« za takojšne okrevanje večjega obsega je zahtevana prepustnost vhodno izhodnih operacij do strežnikov vsaj 150.000 IOPS pri velikosti IO blokov 32 KB in razmerju 60:40 za read/write.
- Povprečna zakasnitev manj kot 4 ms pri dostopu do podatkov pri zahtevanih IOPS in značilnostih v prejšnji zahtevi. Zahtevana je garancija proizvajalca.
- Vse zmogljivosti morajo veljati ob naslednjih vklopljenih funkcionalnostih istočasno: deduplikacija, kompresija, šifriranje, thin, dvojna pariteta. Enako mora veljati ne glede na zasedenost kapacitet sistema vse do 100% zasedenosti. Za doseganje rezultatov lahko sistem nadgradite z dodatnimi kapacitetami.
- Zahtevane zmogljivosti morajo biti zagotovljene tudi ob izpadu enega krmilnika.

3. Priključki:

- vsaj 4 x 64Gb/s FC priključki z vključenimi 64 Gb/s FC optičnimi vmesniki tipa MM.
- 4x 25 Gb/s Ethernet port za replikacijo, z vključenimi optičnimi vmesniki vsaj 25 Gb/s tipa MM.
- Namenski priklopi 4x 1Gb/s RJ-45 za nadzor in upravljanje.
- NVMe-oF preko FC in RoCE preko Ethernet.
- Povezljivost preko NVMe in NVMe-oF (FC, RoCE, TCP)
- Dostop do kapacitet preko FC, iSCSI, RoCE, SMB in NFS.

Nadgradljivost:

- Sistem mora podpirati pri nadgradnjah priklope dodatnih polic izključno z NVMe mediji izključno preko NVMe povezav, hitrosti vsaj 100 Gb/s.
- Podpora vgradnji priklopov za strežnike: do 64 Gb FC, 10, 25 in 100 Gb Ethernet.
- Vsi posegi za nadgradnje povezav morajo biti izvedljivi brez prekinitev dostopa strežnikov do podatkov.

4. Pomnilniški mediji:

- Možno je vgraditi shranjevalne medije tipa Flash in sicer NVMe ali novejši.
- V primeru okvare shranjevalnega modula mora sistem samodejno ponovno vzpostaviti dvojno zaščito podatkov. Dopusten je tudi dodatni shranjevalni modul z vlogo »hot-spare«, ki ni del osnovne zahtevane surove kapacitete.
- Brezplačna zamenjava Flash shranjevalnih medijev, ki odpovejo ne glede na dosežen/presežen nivo izrabe (write endurance limit) v garancijskem ali kadarkoli kasneje v vzdrževalnem obdobju.

5. Programska oprema in licence:

- Vključena mora biti programska oprema in licence za celotno kapaciteto za vse zahtevane funkcionalnosti.
- Vključeno mora biti izvajanje posnetkov stanj (Snapshot) in fizičnih kopij (Clone), pri tem mora biti vključena možnost definiranja varovanih skupin za posamezne LUNe ali skupine LUNov za zagotavljanje konsistenčnosti podatkov. Vključena možnost uporabe kopij podatkov večkratno, podprto upravljanje preko ssh in RestAPI za avtomatizacijo.
- Zrcaljenje mora vključevati FC in TCP/IP povezave z naslednjimi možnostmi:
 - Aktivna raztegnjena gruča dveh sistemov za zagotavljanje bralno pisalnih funkcij za vsak LUN na dveh lokacijah istočasno.
 - Sinhrono in asinhrono zrcaljenje (repliciranje) podatkov posameznih LUNov ali celovite varovane skupine LUNov na oddaljeni sistem.

- Replikacija na enega ali več sorodnih sistemov z možnostjo definiranja frekvence replikacij, življenjske dobe posnetkov replikacij in samodejnega brisanja zapadlih replik.
- Vsi tipi zahtevanih zrcaljenj morajo biti zagotovljeni znotraj osnovnega sistema, brez dodatna strojne in programske opreme.

6. Visoka razpoložljivost:

- Popolnoma redundančna arhitektura s podvojenimi komponentami brez enojne točke odpovedi (kontroler, napajalni modul, hladilni modul, predpomnilnik, baterijsko ščitenje predpomnilnika).
- Zaščita vsebine predpomnilnika za zapise ob izpadu napajanja (baterijska ali druga ustrezna tehnologija/rešitev). Ugašanje sistema ob izpadu napajanja ne sme ogroziti podatkov v sistemu.
- Avtomatski zagon sistema po povrnitvi napajanja v manj kot 15 minutah do polne funkcionalnosti.
- Vse nadgradnje programske in strojne opreme se mora izvajati brez prekinitve dostopa do kapacitet za strežnike.
- Minimalna zaščita kateregakoli LUN-a s podporo hkratne odpovedi dveh diskov v posamezni polici (N+2 oz dual parity oz. ekvivalent RAID-6)
- Tudi ob izpadu delovanja dveh diskov mora sistem ponovno vzpostaviti dvojno zaščito tudi v primeru 100% zasedenosti kapacitet.

7. Sistem mora omogočati »stretched cluster« platformo za doseganje višje razpoložljivosti, porazdelitve obremenitev in istočasno aktivno uporabo na dveh lokacijah:

7.1 Raztegnjene kapacitete med dvema lokacijama (zakasnitev na povezavah manj kot 10 ms):

- Vključena mora biti funkcionalnost za postavitev aktivne gručice dveh ponujenih sistemov v delovanju active-active na razdalji do 150 km oziroma do največje zakasnitve 10 ms. S tem mora biti zagotovljena funkcionalnost dostopa do istega podatka istočasno na obeh sistemih tako za branje kot tudi za pisanje.
- Omogočati mora istočasno branje in pisanje na obeh lokacijah na skupno logično eno za kapacitete (isti LUN/volume).
- Delovati mora na način, da je zapis vsakega podatka potrjen na obeh lokacijah pred potrditvijo do strežnika.
- Podpirati mora FC in IP povezave za sinhronizacijo.
- Vsi tipi zahtevanih zrcaljenj morajo biti zagotovljeni znotraj osnovnega sistema, dodatna strojna in programska oprema ni dopuščena.

7.2 Omogočati mora tudi samodejno asinhrono zrcaljenje primarnih podatkov sistema (ali raztegnjene gruče) na rezervni sistem na oddaljeni lokaciji, ki mora izpolnjevati naslednje:

- Upravljanje vseh sistemov mora biti zagotovljeno v enotnem upravljalnem vmesniku, brez dodatne strojne in programske opreme.
- Okrevanje oddaljene kopije na primarni sistem znotraj shranjevalnega sistema z enim ukazom, velja tudi za raztegnjene kapacitete.
- Nastavitve varovanja dodatne asinhronre kopije znotraj skupne politike na primarnih sistemih.
- Vsi tipi zahtevanih zrcaljenj morajo biti zagotovljeni znotraj osnovnega sistema, dodatna strojna in programska oprema ni dopuščena.
- Samodejno izvajanje varne offline neizbrisljive kopije na kateremkoli sistemu, ki mora biti nespremenljiva in neizbrisljiva v sistemu vsaj do 30 dni. Funkcionalnost mora biti privzeto vklopljena na sistemu. Za morebitno spreminjanje politike/brisanje/spreminjanje ure na sistemu je potrebno odpreti incident pri proizvajalcu opreme in se avtenticirati istočasno z več skrbniki in z večfaktorsko avtentikacijo.

8. Integracija v backup okolje Veeam - Ponujeni sistemi morajo podpirati Veeam napredne funkcionalnosti integracije druge generacije (USAPI v2):

- Prenos izdelovanja »hitrih snapshotov« iz vSphere na primarni in sekundarni storage v replikaciji in v aktivni gruči.
- Explorer za Veeam okrevanje direktno iz snapshotov na shranjevalnem sistemu.
- Različna politika hranjenja snapshotov za primarne in sekundarne shranjevalne sisteme.
- Testiranje okrevanja iz snapshotov na primarnem ali sekundarnem sistemu.
- Orkestracija in prenos snapshotov na sekundarni shranjevalni sistem, tudi za izdelovanje varnostnih kopij iz sekundarnega shranjevalnega sistema, vse iz Veeam vmesnika.

9. Funkcionalnosti:

- Sistem mora vključevati funkcionalnost »Unified«, kar pomeni hkratno možnost dostopa do kapacitet preko Block in File (NAS) načina, pri čemer mora podpirati SMB in NFS protokole.

- Vsi podatki se morajo deduplicirati in kompresirati še predno se zapišejo na shranjevalne medije, hkrati mora biti vedno vklopljena navidezna kapaciteta (Thin) za vse LUNe. Deduplikacijo in kompresijo ni možno izklopiti.
- Vedno vklopljeno sprotno šifriranje podatkov, ki se zapisujejo na shranjevalne medije. Pri tem ne sme biti ogrožena visoka razpoložljivost za vse elemente rešitve, šifriranje mora potekati z vsaj 256 bitnem ključem, ki mora biti razpršen še na ostale komponente sistema. Podatki ne smejo biti berljivi iz medijev brez osnovnega sistema. Podpirati mora zunanje upravljanje šifrirnih ključev (KMIP) in Smartcards za hipno nedosegljivost celotne vsebine podatkov.
- Samodejno razvrščanje zapisanih podatkov na vse medije v sistemu.
- Povečanje velikosti LUN ob delovanju brez vpliva na zmožljivost.
- Povečanje kapacitete sistema z dodajanjem shranjevalnih kapacitet ob delovanju brez izgube zmožljivosti.
- Omogočena nadgradnja sistema z zmožljivejšimi oziroma s kontrolerji novejšje generacije med delovanjem in brez kopiranja podatkov in brez prekinitve dostopa do podatkov. Med posegom zmožljivosti ne smejo biti nižje od zgoraj zahtevanih.
- Nadzorna programska oprema:
 - Upravljanje, nadzor in obveščanje, ki se mora izvajati na samem sistemu in je dostopen preko ukazne vrstice in spletnega vmesnika v grafični obliki.
 - Upravljanje dveh sistemov mora biti zagotovljeno v enotnem upravljalnem vmesniku, brez dodatne strojne in programske opreme. Upravljanje obeh sistemov se lahko izvaja istočasno iz enega sistema.
 - Vključena mora biti programska oprema/funkcionalnost znotraj krmilnikov ponujenega sistema, ki omogoča pregled nad zmožljivostmi in obremenjenostjo sistema v realnem času in za v preteklost do 1 leta, vključeni morajo biti vsaj parametri: IOPS, MB/s, Response time (Latency) in sicer ločena za pisanje in za branje.
 - Nadzor delovanja in obremenitev ponujenih sistemov z vsemi ključnimi vitalnimi kriteriji preko varnega spletnega dostopa https
 - Omogočeno upravljanje diskovnih kapacitet namenjenih uporabi iz VMware okolja preko naročnikovega obstoječega vmesnika za upravljanje virtualnega okolja VMware (vCenter) za celotno kapaciteto. Pri tem mora omogočati vpogled v vse elemente od virtualnega diska, virtualnega in fizičnega strežnika do elementov znotraj shranjevalnega sistema in sicer mora omogočati analizo zazakasnitve, prenos podatkov in IO operacij na vseh zgornjih gradnikih na poti med shranjevalnim sistemom in virtualnimi strežniki.
 - Podpora funkcionalnosti VMware vVol.

10. Tehnične karakteristike:

- Vgradnja v standardno 19 palčno računalniško omaro, vodila morajo biti priložena.

- Podvojeno napajanje s priklopom na vsaj 2 neodvisna vira napajanja. Napajalnike se lahko zamenja med delovanjem (hot swap)

11. Ostalo:

- Oprema proizvedena v Evropski uniji.
- Proizvajalec mora biti zadnjih 5 let uvrščen v vodilni kvadrant v poročilu analitske hiše Gartner za področja shranjevalnih sistemov.
- Vsa potrebna oprema, gonilniki, dokumentacija, priključni in mrežni kabli idr. za vgradnjo in priklop morajo biti priloženi.

12. Režim vzdrževanja:

- Veljajo splošne zahteve za redundantni režim vzdrževanja.
- V primeru izteka življenske dobe ali izrabe katerekoli komponente znotraj sistema se le to nadomesti v okviru vzdrževanja brez dodatnih stroškov za naročnika.
- Poseg zamenjave mora biti izveden brez prekinitve delovanja za strežnike in aplikacije in med posegom ne sme priti do zmanjšanja zmogljivosti sistema.

P.1.1 Backup programska oprema

Veeam Enterprise plus za 300 virtualnih strežnikov za obdobje 3 let.

Sukcesivna dobava po 100 virtualnih strežnikov glede na uspešen prevzem posameznih modulov.

Postavitev distribuirana na dveh strežnikih na ločenih lokacijah.

Samodejne nedotakljive offline varnostne kopije znotraj primarnega strežnika.

Samodejna replikacija offline kopij med primarnim in sekundarnim strežnikom.

Izveden ustrezen hardening sistema:

- Večfaktorska avtentikacija
- večosebna avtentikacija za izvedbo kritičnih posegov
- Možnost zaznave malware napada in okuženosti kopij med izvajanjem varnostnega kopiranja
- Samodejno testiranje okrevanja za ključne podatke, strežnike in njihove procese s samodejnim obveščanjem o uspešnosti.
- Priprava DRP načrta za hiter prekop sistema na sekundarno lokacijo z možnostjo hitrega okrevanja v najkrajšem možnem času.
- Rešitev mora zagotavljati vzpostavitev celotnega modula v nekaj minutah.

P.1.2 Sistem za upravljanje dostopov in privilegiranih računov

Sistem mora omogočati funkcije upravljanja (samodejna menjava gesel in določanje politik dostopa) privilegiranih računov v:

- Operacijski sistemi: Windows, Unix, Linux, iSeries (AS/400), zSeries (OS/390)
- Podatkovne baze: Microsoft SQL, Microsoft SQL Cluster Service, Oracle, Informix, MySQL, Sybase Adaptive Server Enterprise, DB2, Informatica, MariaBD, MongoDB, PostgreSQL

Sistem mora zagotavljati podporo (zaščito računov in samodejno rotacijo skrivnosti) za vse naprave, ki podpirajo ODBC različice 2.7 ali višje.

Upravljanje privilegiranih sej

- Sistem mora podpirati izolacijo sej in spremljanje brez razkritja gesla/SSH ključa privilegiranega računa uporabniški postaji.
- Snemanje sej z indeksiranjem podatkov mora biti na voljo kot možnost politike.
- Upravljanje varnostno občutljivih dogodkov, vključno z omejevanjem nabora ukazov, ki jih lahko uporabnik izvaja.
- Sistem mora omogočati kategorizacijo posnetih uporabniških sej z vnaprej določenimi ravnmi tveganja.
- Sistem mora imeti vgrajena analitična orodja, ki omogočajo samodejno zaznavanje sumljivih dejavnosti privilegiranih uporabnikov.

Arhitektura

- Sistem mora omogočati namestitev osrednje zbirke poverilnic na ločen, utrjen operacijski sistem.
- Posamezni funkcionalni moduli morajo biti od istega proizvajalca in se morajo med seboj integrirati.
- Sistem mora omogočati hranjenje ključev osrednje zbirke poverilnic na varnem mediju (kot npr. HSM).

Dodatne zahteve

- Sistem mora podpirati najmanj 10.000 upravljanih privilegiranih računov brez poslabšanja zmogljivosti.
- Sistem mora omogočati razširitev do 100.000 upravljanih privilegiranih računov v porazdeljeni arhitekturi.
- Sistem mora biti certificiran s standardom Common Criteria EAL2 ali višjim oziroma biti v postopku certificiranja.

Zahteve za zaščito oddaljenega dostopa

- Rešitev mora omogočati varen, privilegiran oddaljen dostop za zunanje ponudnike brez potrebe po uporabi VPN rešitev in izpostavljanja omrežja naročnika internetu.
- Rešitev mora omogočati biometrično overjanje (na podlagi prepoznave obraza ali prstnih odtisov na pametnem telefonu) ali druge oblike dvofaktorske avtentikacije.

P.1.3 Sistem za nadzor okolja

Sistem mora omogočati:

- Nadzor strežnikov na nivoju operacijskih sistemov (Linux, Windows), na nivoju virtualizacijske platforme in strojne opreme
- Omogočeno mora biti spremljanje posameznih virov (CPU, Disk, mrežni priključki , ...)
- Opozarjanje s prilagodljivimi pravili za obveščanje (SMS; e-mail, skripte, ...)
- Možnost prilagajanja grafične nadzorne plošče o stanju celotnega sistema.
- Vgrajeno zbiranje metrik zmogljivosti
- Podpora za razpršen nadzor po modulih sistema in z različnimi nivoji pravic uporabnikov
- Razširljivost z vtičniki
- Sistem lahko agregira podatke ponujenih namenskih upravljaljskih sistemov

P.1.4 Sistem za upravljanje virtualnega okolja

VMCenter v redundantni postavitvi v obsegu 400 virtualnih strežnikov.

P.1.5 Sistem za spremljanje in zaznavo dogodkov v OT omrežju

Sistem se sestoji iz centralnega strežnika, kjer se zbirajo in analizirajo podatki pridobljeni s sondami. Sonde zajemajo podatke o dogodkih OT omrežja na ravni dostopovnih stikal (M.1.4), na vseh stikalih tega tipa. Zajem podatkov je neinvaziven in ne vpliva neposredno na mrežni promet. Sonde za zajem podatkov o dogodkih OT omrežja na ravni dostopovnih stikal so lahko namenske naprave ali programski moduli v stikalih. Sistem mora podpirati sledeče funkcionalnosti:

- Centralizirano varnostno nadzorovanje in vidnost nad celotnim OT omrežjem
- Globinsko spremljanje in analiza (DPI) industrijskih protokolov
- Napredno poročanje, ocena tveganj in spremljanje ranljivosti končnih točk
- Avtomatsko odkrivanje naprav, protokolov in ustvarjanje kataloga OT imrežja
- Uporaba IPS podpisov za zaščito pred novimi grožnjami. Podpisi se redno posodablajo.
- Sistem nudi pregled, obdelavo in koreliranje podatkov zbranih s sondami.
- Vizualizacija vseh ključnih informacij o stanju OT omrežja.
- Povezava s sistemom za upravljanje z identitetami in avtorizacijami (M.3.6) za dinamično upravljanje politik dostopa
- Možnost posredovanja podatkov v SIEM naročnika

- Delovanje sond mora biti neodvisno od trenutne povezljivosti s strežnikom (vsi zajeti podatki se morajo posredovati po ponovni vzpostavitvi povezave)

Predvideno je licenciranje po številu naprav, ki jih sistem spremlja. Količina shranjenih podatkov je omejena samo z zmogljivostjo diskovnega polja naročnika in ne zahteva dodatnih licenc.

N.1.1 Nepredvidena dela in oprema

Kot nepredvidena dela in oprema se predvideva oprema, ki je odvisna od pogojev namestitve in je naročnik ni mogel predvideti v tem popisu. So pa ta oprema in dela nujni za zaključek projekta.

DRUŽBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI

DARS, d. d.