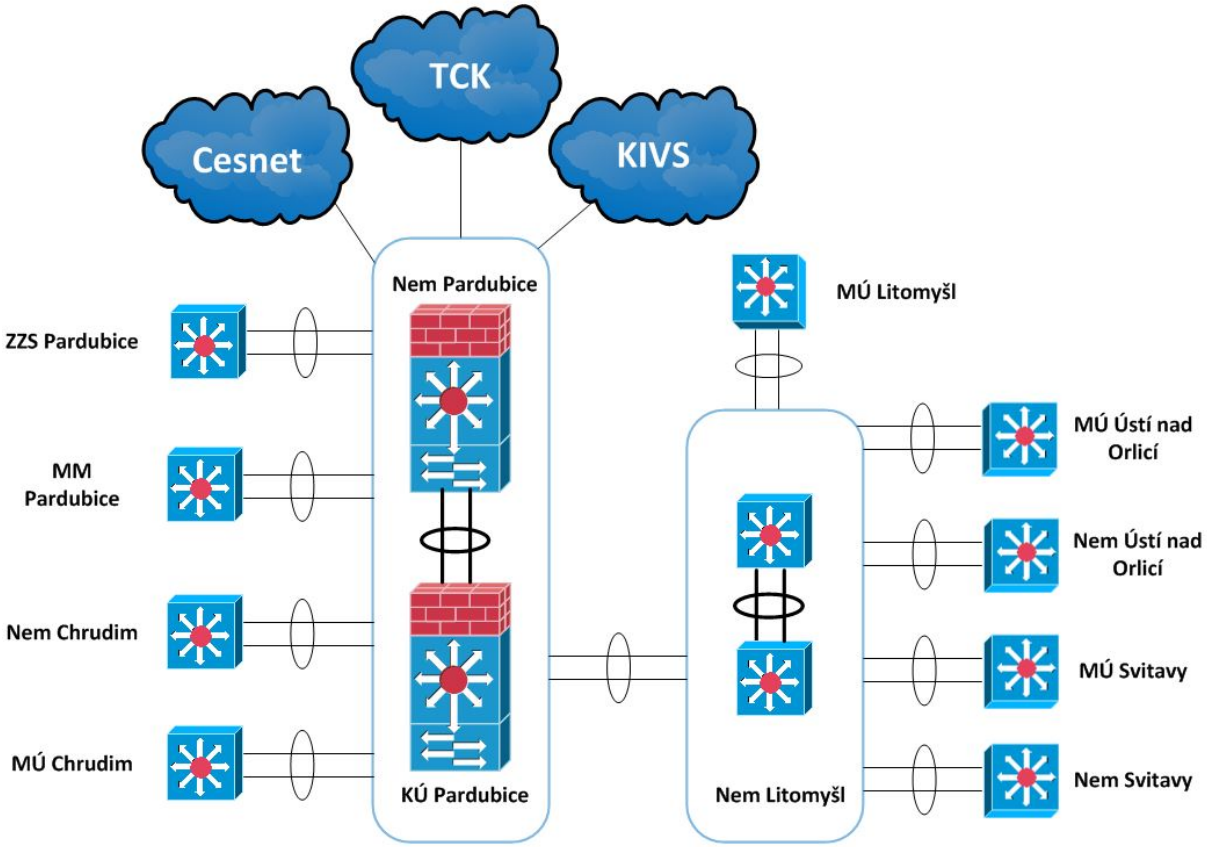
Příloha č. 2

TECHNICKÁ SPECIFIKACE

1. VÝCHOZÍ STAV – POPIS AKTUÁLNÍHO STAVU

Výchozí stav sítě včetně jeho služeb podporující eGovernment a eHealth na území Pardubického kraje vznikl v rámci IOP projektu „Regionální datová síť Pardubického kraje“.



Obrázek č. 1 – Současná topologie Regionální datové sítě

Vzniklá síť propojila celkově 11 uzlů v 12 lokalitách v celkem pěti městech kraje a v současnosti se svými napojením na Technologické centrum kraje, na krajské konektory sítě ITS-NGN a akademickou síť CESNET tvoří páteř Regionální datové sítě LabeNET.

Jádro sítě tvoří dva uzly, jeden centrální v datových centrech Nemocnice a Krajského úřadu v Pardubicích a druhý agregační v Nemocnici Litomyšl, které jsou propojeny optickou linkou o celkové instalované kapacitě 6x1Gbps. Centrální i agregační uzel jsou osazeny dvojicí zařízení, propojovací linka mezi nimi je jednoduchá, rozdělená na dva svazky pouze logicky technologií CWDM. Přístupové uzly v ostatních lokalitách jsou připojeny k oběma prvkům v centrálním či agregačním uzlu nezálohovanou optickou linkou, která je pomocí WDM rozdělena na dvě logické linky 1 Gbps – logicky jde o topologii dvojité rozvětvené hvězdy. Celá síť je tedy z hlediska topologie uzlově redundantní, logicky i na linkově redundantní, fyzicky však linkově redundantní není.

Tabulka č. 1 - Současné uzly Regionální datové sítě

Typ lokality	Adresa
Datové centrum	Pardubická krajská nemocnice, a.s. Kyjevská 44, 532 03 Pardubice
Agregační lokalita	Litomyšlská nemocnice, a.s. J. E. Purkyně 652, 570 14 Litomyšl
Koncová lokalita	Chrudimská nemocnice, a.s. Václavská 570, 537 27 Chrudim
Koncová lokalita	Orlickoústecká nemocnice, a.s. Čs. armády 1076, 562 18
Koncová lokalita	Svitavská nemocnice, a.s., Kolárova 7, 568 02 Svitavy
Koncová lokalita	Zdravotnická záchranná služba Pardubického kraje, Průmyslová 450, 530 03 Pardubice
Datové centrum	Krajský úřad Pardubického kraje, Komenského náměstí 125, 532 11 Pardubice
Koncová lokalita	Městský úřad Chrudim, Resselovo náměstí 77, 537 16 Chrudim
Koncová lokalita	Městský úřad Litomyšl, Bří Šťastných 1000, 570 20 Litomyšl
Koncová lokalita	Magistrát města Pardubice, Pernštýnské náměstí 1, 530 21 Pardubice
Koncová lokalita	Městský úřad Svitavy, T. G. Masaryka 40/25, 568 02 Svitavy
Koncová lokalita	Městský úřad, Ústí nad Orlicí Sychrova 16, 562 24 Ústí nad Orlicí

1.1.1. Odůvodnění dalšího postupu

Vytížení linek

V rámci rozvoje spojených nemocnic Pardubického kraje, eHealthu a eGovernmentu došlo k naplnění kapacity hlavně spojení mezi centrální a agregační lokalitou.

Redundance

V průběhu provozu stávající sítě vzrostl požadavek na zvýšení dostupnosti služeb vůči centrální lokalitě, fyzická redundance se tak ukázala jako nezbytná.

Změna charakteru provozu

Také zvýšení počtu tunelovaného provozu včetně jeho režie změnila charakter pohledu na budoucí úpravy sítě.

2. Požadované parametry

Vzhledem ke stále rostoucím požadavkům na komunikační infrastrukturu a bezpečnost služeb a celé RDS je třeba v rámci rozšíření Regionální datové sítě zásadně modernizovat celý projekt na RDS 2 a zajistit tak nepřetržitě fungování stávajících i nových služeb se zajištěním dostatečné průchodnosti sítě.

2.1. Obecné požadavky mimo technickou část zadávací dokumentace

1) Termín ukončení projektu a předání předmětu plnění do ostrého provozu je 30. dubna 2021. Zadavatel předpokládá práci několika týmů na realizaci zakázky.
2) Maximální cena zakázky včetně servisní podpory bude cca 128 mil. Kč s DPH. Současně platí maximální částka pro servisní podporu cca 50 mil. Kč s DPH.
3) Parametrem výběru je součet nabídkových cen za kompletní realizaci veřejné zakázky, a to zejména za kompletní dodávku RDS 2 včetně pěti let provozní podpory projektu.

2.1.1. Obsah provozní podpory projektu

4) Servisní činnost všech komponent RDS 2 po dobu platnosti servisní smlouvy.
5) Vzdálený dohled komponent RDS 2 v režimu 24 hodin x 7 dní, proaktivní monitoring
6) Pohotovost zaměstnanců zhotovitele k provedení servisního zásahu
7) Bezplatnou telefonickou konzultační a poradenskou službu v běžných záležitostech, týkajících se provozu Regionální datové sítě 2
8) Náklady na skladové zásoby náhradních dílů a materiálu v dostatečném množství pro případné opravy poruchy zařízení za předpokladu, že zařízení jsou výrobcem podporována
9) Náklady na zapůjčení náhradního zařízení
10) Cestovní náklady vzniklé v souvislosti s lokalizací a odstraňování poruchy
11) Náklady na práci servisního technika vzniklé v souvislosti s lokalizací a odstraňováním poruchy
12) Náklady na materiál a náhradní díly vzniklé v souvislosti s odstraňováním poruchy
13) Realizace pravidelného školení administrátorů zhotovitele
14) Každoroční jednodenní setkání technických správců sítě strany zhotovitele a zadavatele o budoucnosti a rozvoji Regionální datové sítě 2.
15) 50 změnových požadavků měsíčně
16) Aktualizace dokumentace jako reakce na změnový požadavek
17) Služby pravidelné technické podpory – provádění průběžné inovace produktu, jeho jednotlivých technologických částí a příslušného software, příp. firmware, zejména pravidelné opravné SW záplaty (patche), update, upgrade a nové verze.
18) Patch management dle bezpečnostního doporučení nebo doporučení výrobce
19) Pravidelné servisní prohlídky a revize předepsané výrobci.
20) Měsíční reporting provozu a plnění SLA
21) Služby servisního managera

2.1.2. Požadavky na implementaci

22) Projektové vedení realizace projektu - zadavatel požaduje projektové vedení realizace předmětu plnění. Mimimálně 1x měsíčně bude provedeno jednání v místě sídla zadavatele, kde osobně vedoucí realizačního týmu a hlavní architekt seznámí zástupce zhotovitele o stavu projektu.
23) Proškolené osoby zhotovitele musí mít možnost přebrat kontrolu nad celou sítí. Tato možnost může být jen nouzová v rámci eskalace bezpečnostního incidentu. O každé změně v síti však musí být proveden záznam.
24) Předimplementační analýza
25) Vypracování prováděcího projektu
26) Dodávka a implementace předmětu plnění
27) Hw příprava
28) Aktualizace postupů a harmonogramu s ohledem na aktuální situaci
29) HW a SW příprava, iniciace a základní konfigurace
30) Převedení konfigurace současné sítě

31) Převedení konfigurace současných služeb
32) Optimalizace sítě
33) Podpora už funkčních celků
34) Testovací provoz
35) Akceptace předmětu plnění
36) Školení
37) Dopracování dokumentací
38) Spuštění ostrého provozu
39) Spuštění technické podpory

2.2. Definování nových lokalit / uzlů

Skupina ORP je pro rozvoj Regionální datové sítě stěžejní. Jedním z primárních cílů je dovést vysokorychlostní páteřní připojení do všech ORP v Pardubickém kraji a rozvinout tak potenciálnapojení dílčích metropolitních sítí, které spolu zajistí konektivitu až k jednotlivým zakládaným a zřizovaným organizacím Pardubického kraje i ORP. Městské úřady jako takové jsou zároveň prioritním partnerem Pardubického úřadu a napojení do RDS přinese kromě naplnění indikátorů strategického cíle 4.1.10 (Regionální datová síť) i první krok pro naplnění dalších strategických cílů jako je elektronizace výkonu agend na úrovni kraje a rozvoj služeb eGovernmentu..

Vlastní ORP je v tomto případě bráno v dalším textu jako lokalita, MÚ s aktivními prvky jako PE uzel v dané lokalitě.

V oblasti zdravotnictví se novým partnerem mimo akciové společnosti Nemocnice Pardubického kraje výrazného použití sítě stávají i ostatní složky integrovaného záchranného systému. Ať už v příjmu kamerových záznamů z lokalit sítě nebo jako účastník sítě využívající Regionální datové sítě pro propojení svých základen.

Tabulka č. 2 − Definování nových lokalit / uzlů

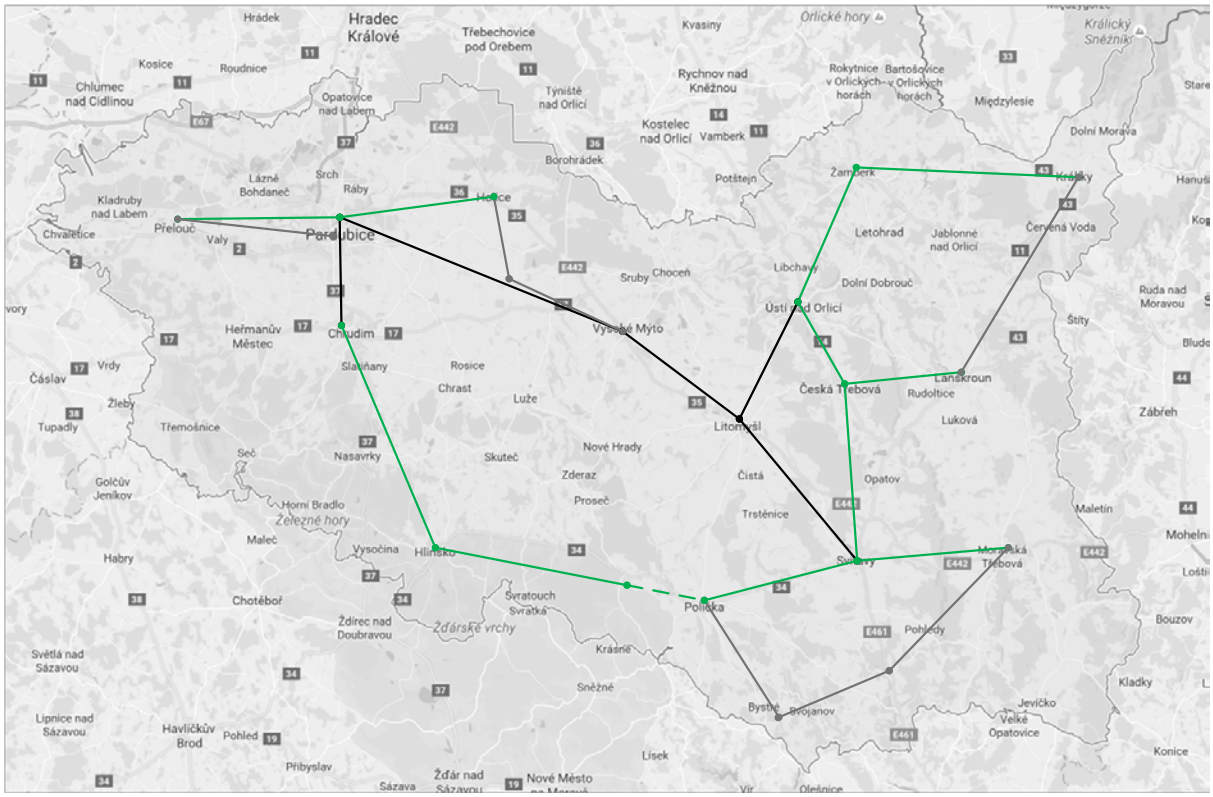
Název ORP / lokality	Název úřadu / uzlu	Adresa rozvaděčové místnosti, kde bude RDS zakončena
Česká Třebová	Městský úřad Česká Třebová	Staré náměstí 78, 560 02 Česká Třebová
Hlinsko	Městský úřad Hlinsko	Adámkova 554, Hlinsko
Holice	Městský úřad Holice	Holubova 1, Holice
Králíky	Městský úřad Králíky	Velké náměstí 5, 561 69 Králíky
Lanškroun	Městský úřad Lanškroun	nám. J. M. Marků 5, 563 01 Lanškroun
Moravská Třebová	Městský úřad Moravská Třebová	Olomoucká 178/2 571 01 Moravská Třebová
Polička	Městský úřad Polička	Palackého nám. 160, 57201 Polička
Přelouč	Městský úřad Přelouč	Československé armády 1665
Vysoké Mýto	Městský úřad Vysoké Mýto	B. Smetany 92, 566 32 Vysoké Mýto

Název ORP / lokality	Název úřadu / uzlu	Adresa rozvaděčové místnosti, kde bude RDS zakončena
Žamberk	Městský úřad Žamberk	Masarykovo nám. 166, 564 01 Žamberk

2.3. Návrhový koncept geografického modelu RRDS

Na základě realizovaného marketingového průzkumu dostupnosti tras je možný následující finální geografický model rozšíření Regionální datové sítě[1] (dále použito i ve zkratce RRDS).

Realizací projektu rozšíření vznikne novější Regionální datová síť verze 2 (dále také jako RDS 2)



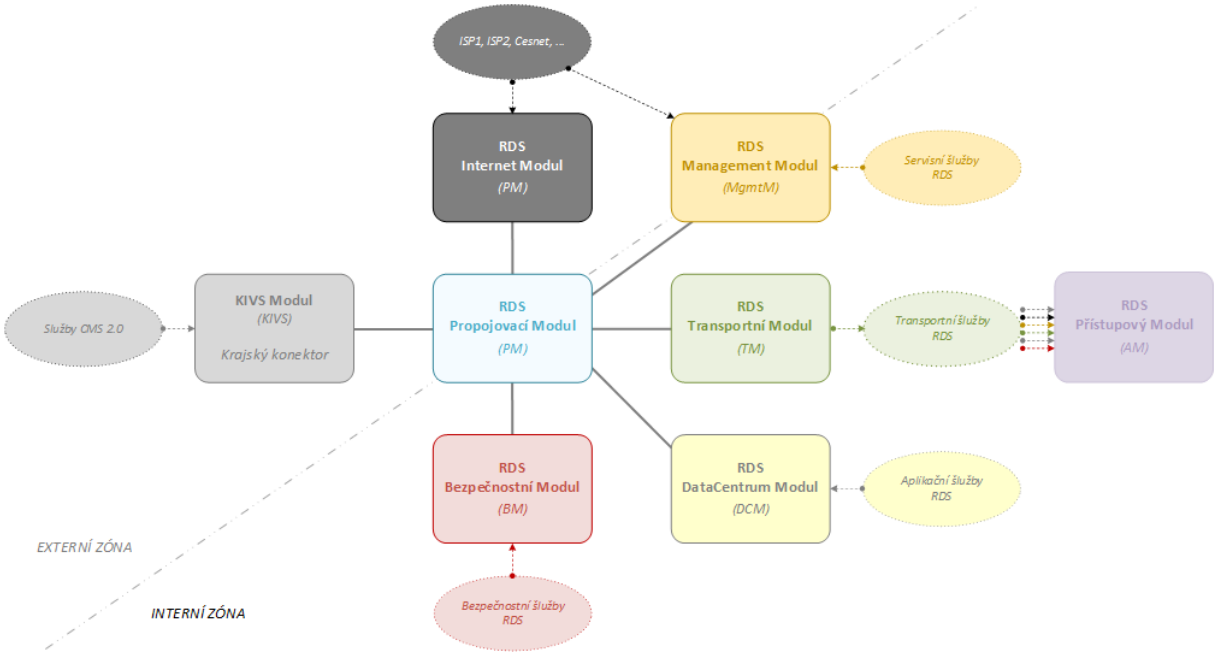
Obrázek č. 2 – Návrhový model ve fázi prvního rozšíření RDS (stav k 08/2017)

Díky pokroku v oblasti informačních technologií a i novým technologiím přenosu dat může být výsledný model RDS 2 jiný. Zadavatel netrvá na druhém a dalších kruzích, umožňuje i jejich spojování při využití jiných přenosových technologií.

2.4. High-Level architektura

Základním stavebním prvkem budou jednotlivé moduly, poskytující do celkového informačního systému definované služby, které jsou pak různorodě využívány připojenými organizacemi. Řízené propojení a směrování služeb je pak v prostředí RDS 2 zajišťováno pomocí Propojovacího Modulu (PM). Ten je také jediným vstupním a výstupním bodem služeb, které poskytují další moduly Externí zóny.

[1] *Černě je vyznačena stávající síť RDS, zeleně jsou vyznačeny trasy navrhované v projektu Modernizace infrastruktury pro sdílení informací a dat s obcemi Pardubického kraje, šedivou barvou pak trasy pro další potenciální rozvoj RDS směrem k dokruhování všech ORP.*



Obrázek 6 High-Level adrchitektura RDS 2

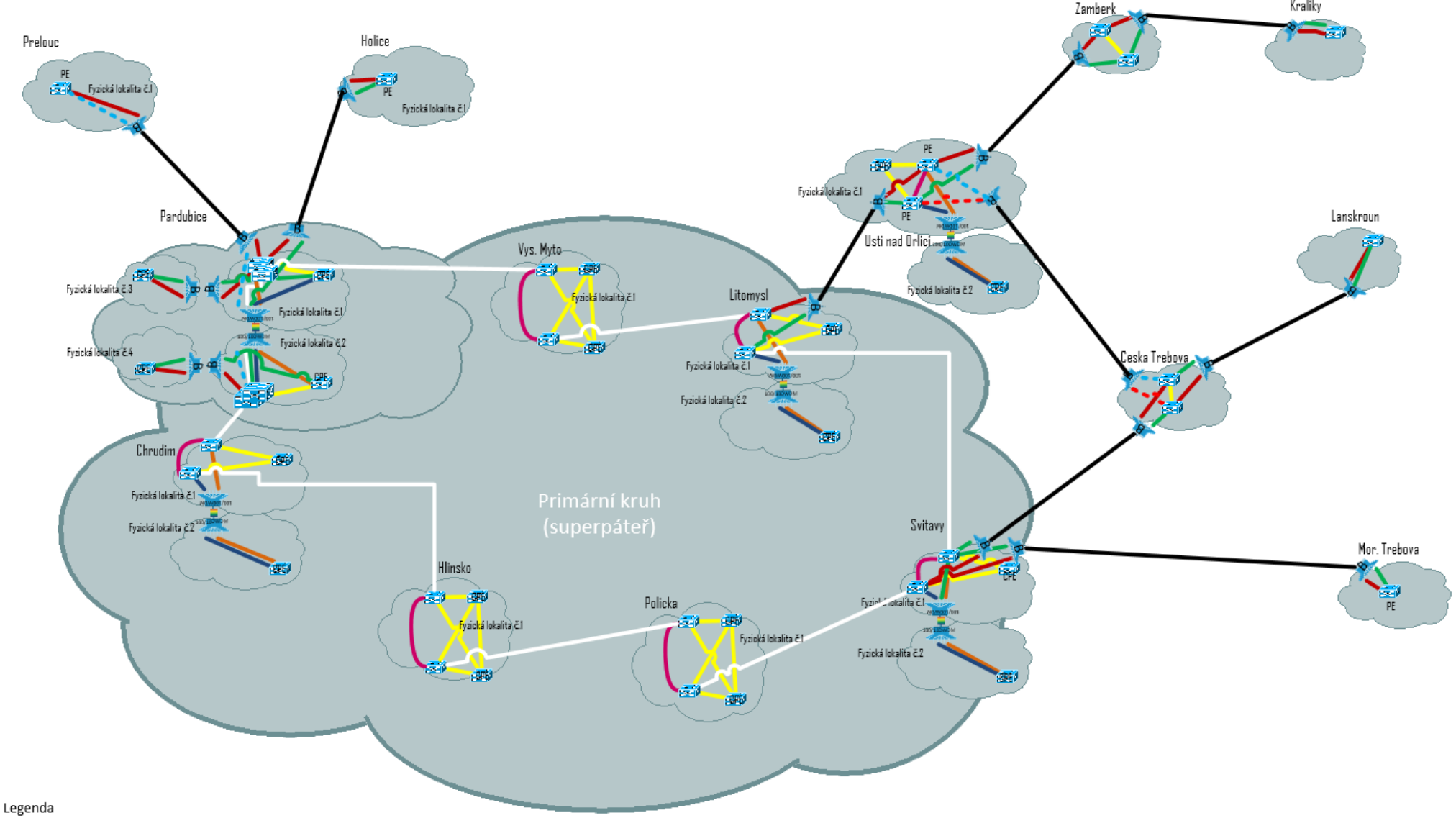
2.4.1. Architektonické moduly

Jednotlivé moduly jsou podle kontroly nad jejich konfigurací, správou a provozem rozděleny do Interní a Externím zóny. V rámci prvního kroku rozšíření se nepředpokládá vznik a provoz všech modulů najednou, ale z pohledu High-Level architektury je nutné vědět o záměru jejich realizace v dalších krocích.

RDS 2 bude ihned po rozšíření primárně infrastrukturou transportního charakteru, tzn., že její využití bude spočívat převážně v distribuci služeb svých a externí zóny k jednotlivým připojovaným organizacím pomocí Propojovacího a Transportního Modulu. Aby to bylo možné, je nutné ihned při rozšíření také řešit správu a provoz prostředí RDS 2 a to za pomocí Management modulu.

Zóna	Modul	Priorita výstavby
INTERNÍ	Management Modul (MgmtM)	ihned při rozšíření
	Propojovací Modul (PM)	ihned při rozšíření
	Transportní Modul (TM)	ihned při rozšíření
	Přístupový Modul (AM)	řeší připojované organizace
	DataCentrum Modul (DCM)	*v budoucnu*
	Bezpečnostní Modul (BM)	ihned při rozšíření
EXTERNÍ	Internet Modul (IM)	ihned při rozšíření
	KIVS Modul	ihned při rozšíření

Tabulka 3 Architektonické moduly RDS 2 a jejich priorita výstavby


Prelouc
PE
Fyzická lokalita č.1
Holice
PE
Fyzická lokalita č.1
Pardubice
Fyzická lokalita č.3
Fyzická lokalita č.1
Fyzická lokalita č.2
Fyzická lokalita č.4
CPE
Vys. Myto
Fyzická lokalita č.1
Litomysl
Fyzická lokalita č.1
Fyzická lokalita č.2
Zamberk
Kraliky
PE
Fyzická lokalita č.1
PE
Usti nad Orlici
Fyzická lokalita č.2
Lanskroun
Ceska Trebova
Chrudim
Fyzická lokalita č.1
Fyzická lokalita č.2
Primární kruh
(superpáteř)
Hlinsko
Fyzická lokalita č.1
Policka
Fyzická lokalita č.1
Svitavy
CPE
Fyzická lokalita č.1
Fyzická lokalita č.2
Mor. Trebova
PE
Legenda
10 GB SMF patchcord
2x 10 GB SMF 80 km DWDM barva 1,2
2x 10 GB SMF 80 km DWDM barva 3,4
2 x 10 GB SMF 80 km DWDM barva 5,6
100 GB SMF 40 km (bílá)
2x 10 GB SMF 80 km DWDM barva 7,8
2x 10 GB SMF 80 km DWDM barva 9,10
2x 10 GB SMF 80 km DWDM barva 11,12
Fyzická trasy (jedno, dvou vlákno)
BiDi
BiDi
DWDM BiDi jednovlákno 16 tras/32 barev
100/10DWDM
100/10DWDM
Odbočka pro 100 GB QSFP a DWDM
16 tras na dvouvlákně
2x 100 GB stack metalický propoj
Verze 2.1
12.1.2020

2.5. Obecné požadavky na architekturu a provedení projektu

2.5.1. Základní definice sítě a provozovaných dat

1) Regionální datová síť Pardubického kraje je transportní sítí, nepředpokládá se zásah do přenášených dat.
2) Většina provozu je už od zdroje šifrována, jedná se o souvislé toky informací včetně audiovizuálního obsahu.
3) Informace o funkčnosti jednotlivých uzlů je veřejná informace.
4) Uzly v nemocnicích jsou všechny prioritně zakruhované a priorizované s ostatními nemocničními uzly a to už v rámci tohoto projektu
5) Realizací tohoto projektu budou funkční MPLS uzly (PE) ve všech lokalitách.

2.5.2. Základní bezpečnostní požadavky

1) Provoz mimo transportovaná data je pod maximální kontrolou, Transportní modul je oddělen a jeho výstup vůči ostatním modulům sítě je řízen firewalem.
2) Visibilita provozu je řešena Servisními službami.
3) Přístupová oprávnění na aktivní prvky jsou řízena centrálně v rámci Servisních služeb.
4) Žádná část sítě nekomunikuje mimo projekt bez povolení administrátora. Přístup administrátorů do projektu je přes VPN.
5) Bezpečnostní doporučení akceptují legislativní požadavky ČR (Česká republika) a EU (Evropská unie), standardy bezpečnosti zadavatele, standardy výrobce a „best practice“ bezpečnostní komunity.

2.5.3. Základní požadavky spojené s realizací projektu

1) Všechny požadované podpory, licence a záruky jsou počítané ode dne předání předmětu plnění do ostrého provozu.
2) Podpory, licence a záruky pro období implementace a testovacího provozu nejsou v požadavcích popsány, ovšem zhotovitel s nimi musí na své náklady počítat.
3) Všechny části dodaných zařízení musí být určeny pro český trh, být nové, nepoužité.
4) Všechny licence se stávají majetkem zadavatele dnem předání do ostrého provozu.
5) Součástí projektu jsou i činnosti, které zhotovitel měl jako odborník vědět nebo s nimi počítat a v požadavcích nejsou popsány

2.5.4. Zákaz využití technologií určitých firem u určitých částí

1) Z důvodu neakceptovatelné míry rizika je pro všechny části sítě kromě modulu Transportního zakázáno realizovat tyto části technickými nebo programovými prostředky společností ZTE Corporation a Huawei Technologies Co. se sídlem v Čínské lidové republice, včetně jejich dceřiných firem.
2) Podkladem pro tento zákaz je varování Národního úřadu pro kybernetickou a informační bezpečnost ze dne 17.12.2018, jeho metodika ze dne 4.1.2019 a následná analýza rizik zadavatele s ohledem na kategorii přenášených dat Regionální datovou sítí.
3) Zákaz se netýká Transportního modulu, jeho služeb a jejich aktivních prvků při splnění ostatních bezpečnostních požadavků (izolování nebo oddělení Transportního modulu a jeho naprostá visibilita vůči Externí zoně).

2.5.5. Minimální konfigurace na 8 Gbps od každému uzlu v redundanci

1) Požadavky na propustnost každého uzlu s ohledem na dobu udržitelnosti projektu rostou v čase a 8 Gbps jsou nejmenší hodnotou, která musí být docílena i v případě, že existuje nějaké nefunkční přerušení části sítě ať už v aktivní nebo pasivní části
2) Architektonicky je tedy požadována minimální šířka přenosové rychlosti u každé trasy 8 Gbps násobeném počtem PE uzlů, které mohou při jakémkoliv přerušení sítě přes tuto optickou trasu protékat. Tyto počty nemusí být konečné, neboť na trasách mohou probíhat i pomocné přenosy a managementové přenosy.
3) Vždy se počítá propustnost mezi daným uzlem a DC Krajského úřadu v Pardubicích.
4) Požadovaná redundance je blíže popsána v dalších kapitolách.

2.5.6. Eliminace Single Point of Failure

1) Navržené řešení musí být v jednotlivých částech odolné proti různým výpadkům nebo přerušením, minimálně však na úrovni odolnosti vůči jednomu, jakémukoliv výpadku či přerušení.
2) Souběhy optických tras nebo jejich křížení jsou vlastním výstupem Dokumentace skutečného provedení, označené jako rizikové úseky.

2.5.7. Redundance v pasivní, aktivní i elektrické části

Pasivní část sítě

1) I při využití co nejmenšího počtu vláken by technologie na optických kabelech neměla mít omezení.
2) Fyzická redundance je dána požadavkem architektury sítě v kruzích. Vždy je tedy nutno počítat s nejvyšším rizikem přerušené optických vláken a přesměrováním provozu se zachováním požadovaných parametrů. Také další pasivní prvky se musí podílet na požadavku redundance, tedy například použití vlastního hranolu na každé optické vlákno při použití vlnového multiplexu.

Aktivní část sítě

1) Pro správné fungování redundance v síti jako celku je nutné zajistit ji i na úrovni aktivních prvků (nejen PE). U PE to např. znamená 2 aktivní prvky, každý se dvěma napájecími zdroji v každém uzlu. Pro zajištění kompatibility, jednoduché správy a konfigurace a možnosti dalšího rozšíření předpokládáme zapojení těchto PE dvou aktivních prvků do Stacku / Virtuálního chassis. Maximální redundance se týká i ostatních modulů sítě a jejich aktivních prvků.
2) Předpokladem redundance je i zdvojení všech připojení, ať už mezi sebou nebo s ostatními aktivními prvky v uzlu.

2.5.8. Infrastruktura se buduje jako neukončená

1) Regionální datová síť se buduje jako neukončená, vždy v každé fázi je naplánován další možný rozvoj.
2) Design sítě a její konfigurace nesmí mít omezení v nějakém parametru, který by mohl vzniknout přidáním dalších uzlů nebo napojením dalších subjektů a který není omezením standardu technologie (např. počet VLAN 4096).
3) Nesmí existovat ani omezení licenční. Licence pro realizaci rozšíření Regionální datové sítě jsou součástí dodávky, ale pro případ rozvoje musí buď existovat varianta rozšíření licencí jinou dodávkou (která není předmětem tohoto projektu) nebo pokrytí dalšího rozvoje už licencí v rámci tohoto projektu.
4) Zadavatel umožňuje i neomezené licence.
5) Zadavatel dále může požadovat zařízení, u nichž je předpoklad, že v rámci životnosti změní svoji roli v architektuře sítě (např. pasivní prvky DWDM se 100Gbps odbočkou)

2.5.9. Využití technologií předchozího projektu Regionální datové sítě

1) Zadavatel vzhledem k dobré zkušenosti trvá na využití MPLS v rámci Transportního modulu.
2) Zadavatel trvá dále na využití vlnového multiplexu, tedy maximálního využití optických vláken.
3) Zadavatel také trvá na využití stávajících aktivních prvků, část do Managementového modulu RDS a zbytek (6) napojení jako plnohodnotný PE přes standardní protokoly do sítě (přičemž 1/3 počtu současných aktivních prkvů je rezervována mimo síť jako zdroj náhradních dílů). Zadavatel počítá s tímto bodem jako s ověřením realizace standardních protokolů a technologií v síti.
   Všechny použité aktivní prvky musí být dovybaveny redundandními komponentami jako součást dodávky tohoto projektu, které nebudou převzaty s rezervních zařízení.
4) CWDM prvky budou staženy a použity pro lokální účely.

5) Dálkové optické trasy jsou vždy zakončeny konektorem E2000/APC. Vnitřní propojení používají SC/APC na patchpanelech nebo LC na transceiverech v modrém označení.
6) Zadavatel předá zhotoviteli plnou moc pro nakládání s optickými vlákny zadavatele pro komunikaci technickým správcem za účelem prací s těmito kabely. Zadavatel tedy neočekává, že jsou optické trasy neměnné. Zhotovitel bude moci vyjednávat s technickým správcem o změnách na těchto kabelech v existujících možných variantách změny schématu zapojení optických vláken v lokalitě Pardubice a Vysoké Mýto.

2.5.10. Využití pouze prověřené konfigurace a architektonická řešení sítí

1) Zadavatel zakazuje návrh a využití technologie vlnového multiplexování vyšší než 3 x 10Gbps, kde není zajištěno automatické rozdělení vytížení provozu jednotlivých lambd.
2) Protokol LACP a podobný, ani administrativní zásah není automatickým rozdělením vytížení provozu.
3) Zadavatel dále neumožňuje, vzhledem k povaze sítě, technické řešení, které by bylo nestandardní, nevyzkoušené nebo vyžadovalo vysoké personální nároky při provozu.
4) Zadavatel požaduje přímý přístup na Helpdesk výrobců dodaných zařízení, minimálně dodaných aktivních prvků celé sítě.

2.5.11. Interface FO moduly

1) Zadavatel umožňuje použití OEM FO transceiverů při splnění dalších podmínek
2) Jako součást dodávky je požadována dodávka Interface FO modulů (SFP/SFP+) včetně DWDM při splnění minimální přenosové rychlosti oběma směry v každém bodě sítě. Viz podmínky Transporního a jiných modulů.
3) Interface FO moduly je požadováno dodat s implementovanou sadou diagnostických funkcí DDMI - Digital Diagnostic Monitoring Interface (např. dle standardu MSA SFF-8472) pro vzdálený monitoring úrovní signálu a dalších hodnot (napětí, teplota atd.).
4) Součástí dodávky každého interface FO modulu je požadována i dodávka FO patch kabelu o délce 3m s ukončením do kabeláže E2000/LC/SC přičemž přesný typ ukončení i délka bude specifikován v rámci přípravy instalace prvků.

2.6. Management modul – Servisní služby

Jako samostatný modul je v architektuře RDS 2 použit Management Modul (…dále jen RDS-MM). Bude se jednat o samostatnou, oddělenou síť pro celkovou správu RDS 2. Tato část bude přes Propojovací modul (RDS-PM) logicky propojena do všech ostatních modulů „Interní zóny“. Úkolem RDS-MM je zajištění „Servisních služeb“

2.6.1. Servisní služby

V rámci prvního kroku rozšíření RDS se nepředpokládá vznik a provoz všech služeb najednou, ale z pohledu dimenzace HW a SW zdrojů pro jejich provoz, je nutné vědět o záměru spuštění některých služeb v dalších krocích viz. Tabulka č. 2.

Oblast	Servisní služba	Priorita spuštění
Provoz	Log Management	ihned při rozšíření
	Network Management a správa konfigurací	ihned při rozšíření
	Network Monitoring	ihned při rozšíření
	Flow Monitoring	ihned při rozšíření
	Zálohování (Backup)	ihned při rozšíření
	Out of Band Management (OOB)	ihned při rozšíření
Bezepečnost	Next Generation Firewall (NG FW)	ihned při rozšíření
	Remote VPN (R-VPN)	ihned při rozšíření
	Adresářové služby LDAP (LDAP)	ihned při rozšíření
	Služba bezpečného ověření identity (RADIUS)	ihned při rozšíření
	Anti-X ochrana serverů (AntiX-SRV)	*v budoucnu*
	Anti-X ochrana koncových zařízení (AntiX-EndP)	*v budoucnu*
	Bezpečná přístupová stanice (SAW)	*v budoucnu*
	Multifaktorová authentizace (MFA)	*v budoucnu*
	Bezpečnostní Monitoring (SIEM)	*v budoucnu*

Tabulka 4 Servisní služby RDS 2 a jejich priorita spuštění

Servisní služby mají za úkol zajistit základní potřeby chodu vlastní infrastruktury modulů v interní zóně RDS 2. Vazba využití jednotlivých Servisních služeb konkrétními moduly architektury je upřesněna v Tabulce č. 3.

Oblast	Servisní služba	Službou zajištěná část architektury				
		Management Modul	Propojovací Modul	Transportní Modul	*DataCentrum Modul*	***Bezpečnostní Modul***
Provoz	Log Management	●	●	●	○	●
	Network Management a správa konfigurací	●	●	●	○	●
	Network Monitoring	●	●	●	○	●
	Flow Monitoring	●				●
	Zálohování (Backup)	●	●	●	○	●
	Out of Band Management (OOB)	●				●
Bezepečnost	Next Generation Firewall (NG FW)	●				
	Remote VPN (R-VPN)	●				●
	Adresářové služby LDAP (LDAP)	●	●	●	○	●
	Služba bezpečného ověření identity (RADIUS)	●	●	●	○	●
	Bezpečnostní ochrana jednotlivých částí (FW)	●	●	●	○	●
	Anti-X ochrana serverů (AntiX-SRV)	○				
	Anti-X ochrana koncových zařízení (AntiX-EndP)	○				
	Bezpečná přístupová stanice (SAW)	○	○	○	○	○
	Multifaktorová authentizace (MFA)	○	○	○	○	○
	Bezpečnostní Monitoring (SIEM)	○	○	○	○	○

Tabulka 5 Vazba Servisních služeb na architekturu Interní zóny RDS 2

2.6.2. Předpokládaná forma zajištění Servisních služeb

S ohledem na snahu zajistit vysokou dostupnost (HA) prostředí RDS 2 je vyžadováno řešení redundantní co do lokality, připojení, tak do použití jednotlivých technologií. Prostředí Management modulu RDS 2 je proto rozvrženo do 2 lokalit. Předpokládá se tedy zajištění dostupnosti HW komponent umístěním minimálně do obou lokalit. Na aplikační úrovni není vždy možné zajistit aspekty HA pouhým zdvojením instalace aplikace. Také ekonomika takového designu může být v některých případech neadekvátní velikosti a účelu řešení.

Předpokládáme proto využití některé obvyklé virtualizační platformy, která řeší požadavek na HA prostředí serverů a aplikací pomocí vlastního mechanismu a to nejen na úrovni komponent zajišťujících výkon platformy (vCPU, RAM, LAN) ale také na straně společného datového úložiště v podobě Software Defined Storage (SDS). Servisní služby jsou pak provozovány pomocí Virtuálních serverů (VM) a Virtuálních Appliancí (VA) na kterých běží jejich aplikace.

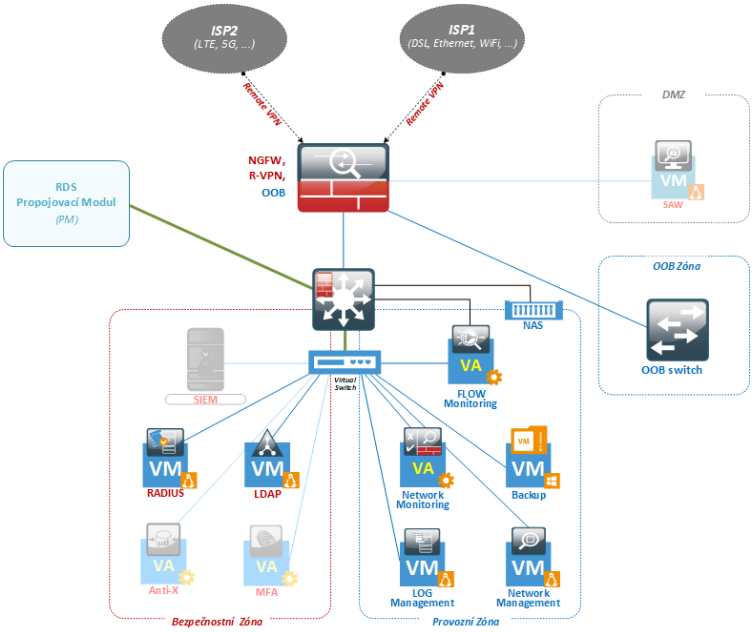
Předpokládaná forma zajištění jednotlivých Servisních služeb RDS 2 vyplívá z Tabulky č.4.

Oblast	Servisní služba	Předpokládaná forma zajištění	Stávající, využitelné licence	Předpokládané zajištění HA prostředí
Provoz	Log Management	Virtuální Appliance (VA)	GrayLog Enterprice 3.1.3.- free edition	pomocí virtualizační platformy
	Network Management a správa konfigurací	Virtuální Server (VM)	-	pomocí virtualizační platformy
	Network Monitoring	VM	Zabix 4.4	pomocí virtualizační platformy
	Flow Monitoring	VA	-	pomocí virtualizační platformy
	Zálohování (Backup)	VM	Veeam Backup & Replication Community Edition	pomocí virtualizační platformy
	Out of Band Management (OOB)	Hardware (HW)		zajištěno HW prvky (*např. virtualní chassi, HW cluster apod.*)
Bezepečnost	Next Generation Firewall (NG FW)	HW		
	Remote VPN (R-VPN)	HW		
	Adresářové služby LDAP (LDAP)	VM	Linux Debian 9 Server s OpenLDAP	min. 2x VM na různých nodech hypervisorů, HA zajištěno vlastní konfigurací aplikace (*např. aplikační cluster, synchronizace databáze apod.*)
	Služba bezpečného ověření identity (RADIUS)	VM	Linux Debian 9 s FreeRadius	
	Bezpečnostní ochrana jednotlivých částí (FW)	HW		zajištěno HW prvky
	Anti-X ochrana serverů (AntiX-SRV)	*VM*	-	*pomocí virtualizační platformy*
	Anti-X ochrana koncových zařízení (AntiX-EndP)	*VM*	-	*pomocí virtualizační platformy*
	Bezpečná přístupová stanice (SAW)	*VA*	-	*pomocí virtualizační platformy*
	Multifaktorová authentizace (MFA)	*VM*	-	*pomocí virtualizační platformy*
	Bezpečnostní Monitoring (SIEM)	*HW+VA*	-	*samostatné HW řešení*

Tabulka 6 Předpokládaná forma zajištění Servisních služeb

2.6.2.1. Aplikační architektura

Očekávaná aplikační architektura řešení se bude skládat z logických komponent dle Obrázku č. 2.



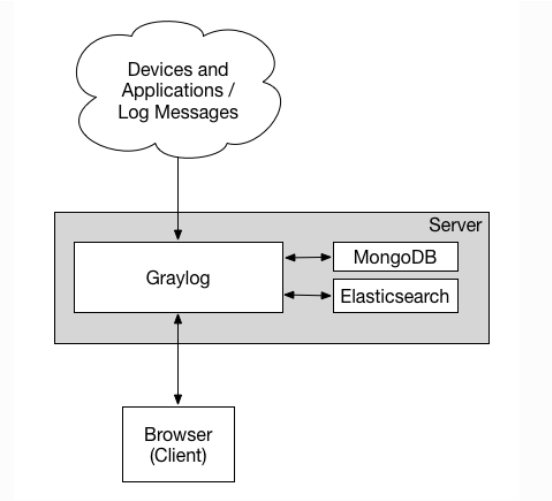
Obrázek 3 Základní logická architektura řešení Servisních služeb RDS 2

2.6.2.2. Log Management

Komponenta zajišťující sběr událostí a provozních log souborů z různých oblastí IT (servery, sítě, operační systémy, aplikace apod.). Bude nasazena aplikace **GrayLog Enterprice 3.1.3.**- free edition, kterou zadavatel využije na základě stávajících licenčních podmínek. Pořízení licencí tedy není součástí požadavků na rozšíření RDS.

V rámci rozšíření RDS je požadována implementace, která zajistí poskytování Servisní služby „Log Management" pro dotčené moduly, viz. Tabulka č. 3.

Nasazení bude ve formě VA v základním podporovaném designu dle Obrázku č. 3.



Obrázek 4 Základní design GrayLog Virtual Appliance

Protože aplikace v tomto designu neumožňuje provoz v režimu HA, bude pro její chod využita požadovaná virtualizační platforma včetně řešení SDS. Výkonové požadavky na virtualizační platformu jsou: 8x vCPU, 32GB RAM a společný diskový prostor s kapacitou 2TB.

Konkrétní rozsah implementace, včetně definice sbíraných událostí z požadovaných zdrojů, četnost a forma uložení dat, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

2.6.2.3. Network Management a správa konfigurací

Komponenta zajišťující konfiguraci a správu dodávaných aktivních prvků v rozsahu modulů Interní zóny RDS 2 , viz. Tabulka č. 3.

Základní požadované funkce a vlastnosti:

- Grafické, intuitivní rozhraní
- Terminálový přístup na aktivní prvky pomocí příkazové řádky
- Role Base Access
- Podpora protokolů minimálně LDAP, Radius, SNMP v2, SSH v2, Telnet
- Možnost provádět hromadné změny na síti
- Hromadný upgrade OS a firmware nově dodaného zařízení
- Automatické zálohy konfigurací, jejich správa a obnova nově dodávaného zařízení
- Auditní log
- Inventarizace aktivních prvků

Aplikace nemusí umožňovat provoz v režimu HA. Pro její chod bude využita požadovaná virtualizační platforma včetně řešení SDS. Předpokládané výkonové požadavky na virtualizační platformu jsou: 4x vCPU, 24GB RAM a společný diskový prostor s kapacitou 1TB.

V rámci rozšíření RDS je požadována dodávka v podobě virtuálního serveru VM se všemi potřebnými licencemi jak pro OS tak pro chod a provoz aplikace. Dále implementace, která zajistí poskytování Servisní služby „Network Management“ pro dotčené moduly, viz. Tabulka č. 3.

2.6.2.4. Network Monitoring

Komponenta zajišťující komplexní monitoring síťové infrastruktury různých oblastí IT (servery, sítě, operační systémy, aplikace apod.) v reálném čase. Bude nasazena aplikace **ZABIX v 4.4.**- free edition, kterou zadavatel využije na základě stávajících licenčních podmínek. Pořízení licencí tedy není součástí požadavků na rozšíření RDS.

V rámci rozšíření RDS je požadována implementace, která zajistí poskytování Servisní služby „Network Monitoring“ pro dotčené moduly, viz. Tabulka č.3.

Protože aplikace neumožňuje provoz v režimu HA, bude pro její chod využita požadovaná virtualizační platforma včetně řešení SDS. Výkonové požadavky na virtualizační platformu jsou: 2x vCPU, 8GB RAM a společný diskový prostor s kapacitou 0,5TB.

Konkrétní rozsah implementace, včetně definice monitorovaných zdrojů, četnosti testů, hraniční hodnoty jednotlivých monitorovaných oblastí a forma uložení dat, bude upřesněna na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

2.6.2.5. Flow Monitoring

Komponenta zajišťující komplexní monitoring datových toků (např. NetFlow, IPFIX, jFlow apod.) pouze pro prostředí Management modulu RDS 2. Technologie představuje moderní a ověřený, způsob pro monitorování sítě a nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu a škálovatelnost.

Vlastní aplikace bude řešena jako Flow kolektor. Kolektory jsou zařízení/prostředky (datová úložiště) s diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat.

Aplikace nemusí umožňovat provoz v režimu HA. Pro její chod bude využita požadovaná virtualizační platforma včetně řešení SDS. Předpokládané výkonové požadavky na virtualizační platformu jsou: 4x vCPU, 32GB RAM a společný diskový prostor s kapacitou 1TB.

V rámci rozšíření RDS je požadována dodávka v podobě virtuální appliance VA se všemi potřebnými licencemi jak pro OS tak pro chod a provoz aplikace. Dále implementace, která zajistí poskytování Servisní služby „Flow Monitoring“ pro vlastní Management modul.

Základní požadované funkce a vlastnosti řešení:

- ucelené řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflow, NetStream)
- podpora IPv4, IPv6, VLAN, MPLS
- nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce)

- bezeztrátový sběr dat na kolektoru z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlowv v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflow, NetStream)
- dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování
- otevřené a dokumentované API s možností integrace nástrojů i třetích stran
- schopnost sbírat NetFlow ze všech nově dodaných síťových prvků i z dodávané virtualizační platformy

Základní požadované funkce a vlastnosti kolektoru:

- minimálně dva 1GbE monitorovací porty, které slouží pro monitorování síťového provozu a generování NetFlow/IPFIX statistik a umožní tak monitorování a analýzu síťového provozu jakéhokoliv virtuálního prostředí bez nutnosti nasazování dalších zařízení pro generování NetFlow/IPFIX statistik
- zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik bez jakékoliv redukce
- kolektor umožní zpracování a vizualizaci flow záznamů v intervalech až 30 sekund, přičemž hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků
- podpora standardů NetFlow v5, NetFlow v9, IPFIX
- možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení
- dva administrativními (management) porty, které se používají pro konfiguraci, správu a případně i sběr flow dat
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS
- zpráva uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí
- separace dat s omezením přístupu pro jednotlivé role/uživatele
- Podpora autentizace vůči LDAP
- kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP
- časová synchronizace zařízení proti centrálnímu zdroji času na síti
- podpora IPFIX položek proměnlivé délky. Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety a jejich grafické zobrazení
- podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, Email, SQL
- podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů
- disková kapacita datového úložiště VA minimálně 1TB pro ukládání záznamů a statistik bez jakékoliv redukce v horizontu minimálně třech měsíců.
- možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti vzorkování na úrovni datových toků.
- flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky.
- uživatelsky definovatelný dashboard s podporou více záložek
- generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.

- předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV.
- automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.
- řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem).
- výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.
- systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnovat do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).
- automatická notifikace v případě vzniku uživatelem definované situace (např. Nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.
- uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány
- možnost dohledat každý jednotlivý datový tok (flow záznam).
- Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země).

2.6.2.6. Zálohování

Komponenta zajišťující komplexní řešení zálohování virtualizační platformy a provozovaných VM a VA. Bude nasazena aplikace **Veeam Backup & Replication** Community Edition , kterou zadavatel využije na základě stávajících licenčních podmínek. Pořízení licencí tedy není součástí požadavků na rozšíření RDS.

V rámci rozšíření RDS je požadována implementace, která zajistí poskytování Servisní služby „Zálohování“ pro dotčené moduly, viz. Tabulka č.3.

Protože aplikace neumožňuje provoz v režimu HA, bude pro její chod využita požadovaná virtualizační platforma včetně řešení SDS. Výkonové požadavky na virtualizační platformu jsou: 4 vCPU, 24GB RAM a společný diskový prostor s kapacitou 0,2TB. Vlastní zálohy pak budou prováděny na síťové úložiště NAS v lokalitě DC1

Konkrétní rozsah implementace, včetně definice zálohovacích pravidel, četnosti a formy zálohování, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

2.6.2.7. Out Off Band Management

Služba zajišťující možný přístup na dedikované rozhraní správy jednotlivých HW komponent Management modulu, i když je jejich vlastní operační systém nedostupný, případně v neočekávaném stavu, který neumožňuje správu prvku standardní, tzv. In-Band cestou.

V architektuře Management modulu RDS 2 se jedná především o aktivní prvky a servery. Jejich dedikované mgmt karty jsou propojeny do samostatného páru přepínačů a tím vytváří oddělenou síť. Aby bylo možné do této OOB sítě přistoupit i z jiného místa než lokalit

DC bude připojena do samostatné DMZ zóny vytvořené pomocí komponenty NGFW vzdáleného přístupu. Díky tomu bude možné také oddělit skupinu administrátorů mající oprávnění OOB používat.

Konkrétní rozsah implementace, včetně designu OOB sítě na L2 i L3 úrovni bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

2.6.2.8. Next Generation Firewall pro vzdálený přístup administrátorů

Komponenta zajišťující služby, především bezpečnostního charakteru. Úkolem je zajistit bezpečný přístup na Internet pouze pro zdroje umístěné ve vlastním Management modulu. Důvodem je potřeba automatických update, aktualizací bezpečnostních oprav a on-line přístup k tzv. Threath Inteligenci výrobců dalších komponent architektury. Protože se jedná a prvek umístěný na hranici vnitřní a vnější zóny RDS 2 bude chod těchto aplikací zajištěn vlastním, pro tyto účely specializovaným, výkonným HW. Ten může být společným i pro komponentu Remote VPN. Díky požadovaným vlastnostem a funkcím (viz. bod 2.3.1) bude zároveň s dalšími aktivními prvky Management modulu, tvořit základ pro segmentaci prostředí a bezpečné oddělení provozu jednotlivých oblastí sítě.

Konkrétní rozsah implementace, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

Funkcionalitu i zařízení tohoto firewallu a hlavního firewallu Bezpečnostní ochrany jednotlivých částí lze sloučit

2.6.2.9. Remote VPN

Další z komponent zajišťující službu bezpečnostního charakteru. Jejím hlavním úkolem je zajistit bezpečný, vzdálený přístup administrátorů, případně externích subjektů, k prostředí Management modulu RDS 2. Klíčovým, pro přístup VIP účtů k prostředí Management modulu, je jednoznačné prokázání identity. Proto je jedním z požadavků také podpora MFA (multifaktorové authentizace). Vlastní chod aplikace bude zajištěn novým HW, který může být společný i pro komponentu NGFW.

Konkrétní rozsah implementace, bude upřesněn na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

2.6.2.10. Adresářové služby (LDAP) – popis služby

Komponenta zajišťující centrální adresářové služby, především jako úložiště identit pro přístup k ostatním Servisním službám RDS 2.

Nasazení bude v podobě minimálně 2ks virtuálních serveru ve formě VM, instalovaných na na minimálně dvou nodech virtualizační platformy, kdy každý bude umístěn v jiné lokalitě a každý VM bude v aktivním stavu. Na VM bude implementován **OS Linux Debian 9 Server s démonem OpenLDAP**. Licence zadavatel využije na základě stávajících licenčních podmínek. Pořízení licencí tedy není součástí požadavků na rozšíření RDS.

V rámci rozšíření RDS je požadována implementace, která zajistí poskytování Servisní služby „Adresářové služby LDAP“ pro dotčené moduly, viz. Tabulka č. 3.

Pro chod aplikací bude využita požadovaná virtualizační platforma včetně řešení SDS. Výkonové požadavky na virtualizační platformu jsou: 2x vCPU, 8GB RAM a diskový prostor s kapacitou 0,5TB.

Konkrétní rozsah implementace, včetně definice členění do OU, zařazení uživatelů a jejich členství v OU, bude upřesněna na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

2.6.2.11. Služba bezpečného ověření identity (RADIUS) – popis služby

Komponenta zajišťující bezpečné ověření identity a následné přiřazení práv a konfigurace v závislosti na výsledku ověření i na aktivních prvcích sítě, jako jsou switche, routery, firewally apod.

Nasazení bude v podobě minimálně 2ks virtuálních serveru ve formě VM, instalovaných na na minimálně dvou nodech virtualizační platformy, kdy každý bude umístěn v jiné lokalitě a každý VM bude v aktivním stavu. Na VM bude implementován **OS Linux Debian 9 Server s démonem FreeRADIUS**. Licence zadavatel využije na základě stávajících licenčních podmínek. Pořízení licencí tedy není součástí požadavků na rozšíření RDS.

V rámci rozšíření RDS je požadována implementace, která zajistí poskytování Servisní služby „Služba bezpečného ověření identity“ pro dotčené moduly, viz. Tabulka č. 3.

Pro chod aplikací bude využita požadovaná virtualizační platforma včetně řešení SDS. Výkonové požadavky na virtualizační platformu jsou: 2x vCPU, 8GB RAM a diskový prostor s kapacitou 0,5TB.

Konkrétní rozsah implementace, včetně definice prvků, které mohou RADIUS Server využívat bude upřesněna na základě předimplementační analýzy, která je součástí požadovaných implementačních prací.

2.6.2.12. Ostatní budoucí a plánované služby

V budoucnu se očekává nasazení ještě těchto, především bezpečnostních aplikací:

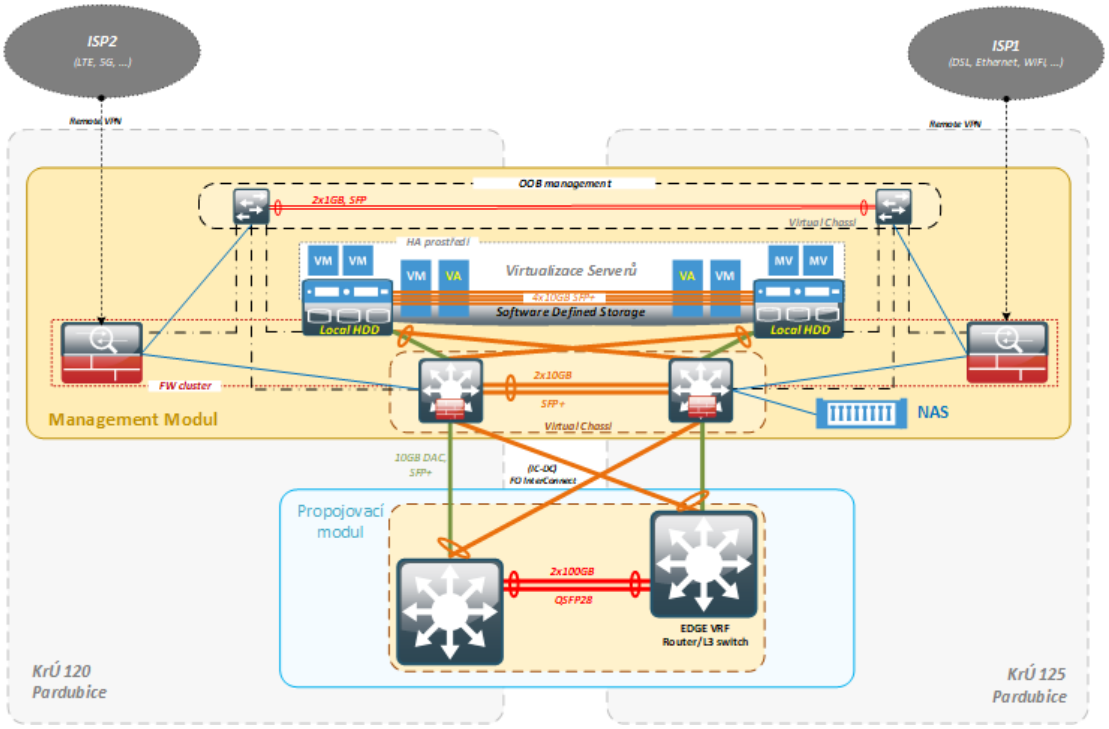
- Anti-X ochrana serverů a koncových zařízení (AntiX-EndP)
- Bezpečná přístupová stanice (SAW)
- Multifaktorová authentizace (MFA)
- Bezpečnostní Monitoring (SIEM)

Pro jejich provoz očekáváme následující využití dodávané virtualizační platformy:

- Anti-X ochrana serverů a koncových zařízení
  - 2x vCPU, 24GB RAM a diskový prostor s kapacitou 1TB
- Bezpečná přístupová stanice (SAW)
  - 2x vCPU, 16GB RAM a diskový prostor s kapacitou 0,5TB
- Multifaktorová authentizace (MFA)
  - 2x vCPU, 8GB RAM a diskový prostor s kapacitou 0,5TB
- Bezpečnostní Monitoring (SIEM)
  - Bude řešen dodávkou vlastního HW a SW

2.6.3. Architektura řešení

Management modul RDS 2 bude vytvořen přes dvě lokality - KrÚ 120 a KrÚ 125. V obou jsou stávající datová centra. Datová centra budou pro zajištění HA prostředí modulu vystavěna v režimu „Active-Active“. V případě havárie jednoho datového centra musí být druhé datové centrum schopné poskytovat všechny Servisní služby Management modulu. V lokalitě KrÚ 125 bude z pohledu RDS 2 umístěno DC1. .



Obrázek 5 Architektura řešení Management modulu RDS 2

2.6.3.1. Fyzická topologie

Popis řešení

Pro připojení do Propojovacího modulu bude využito dvou stávajících aktivních prvků HP 5800 (JC101A). Jsou kromě modulu 4x 10GB SFP+ osazeny také interním FW modulem (HP 5820 VPN Firewall Module), který umožňuje aplikaci bezpečnostních kontrol až do výkonu 6,5 Gbps. Pro činnost Management modulu je toto naprosto dostačující. Prvky budou pomocí technologie IRF konfigurovány do role tzv. Virtual Chassi, která umožňuje jejich provoz v režimu Active-Active. Tyto prvky tvoří CORE sítě vlastního Management modulu. Do nich budou pak v každém DC připojovány další HW komponenty řešení. Jedná se o servery dodávané virtualizační platformy, cluster dvou nových Next Generation Firewallů a dva stávající switche HP5800 (JC103A) zajišťující službu Out of Band Managementu, konfigurované opět do role Virtual Chassi. V DC1 bude také připojeno nové síťové úložiště NAS, dedikované pro funkce Servisní služby Zálohování.

Výkonnostní nároky – Next Generation Firewall (NGFW)

Vlastní nároky na výkon NGFW budou v tomto případě minimální. Úlohou je zajištění Servisních služeb Next Generation Firewall, Remote VPN (R-VPN) a Out of Band Management (OOB), které jsou vázány pouze k vlastními Management modulu. Důraz je spíše kladen na vysokou ochranu pomocí technologií typu Advanced Threath Protection, jako jsou např. IPS, Application Control, WebFiltering, Malware Defence a jiné. V lokalitě DC1 a DC2 bude umístěn vždy jeden HW kus NGFW. Řešení umožní konfiguraci do clusteru fungujícího v režimu minimálně Active-Pasive. Každý NGFW bude napojen do Internetu dvěma odlišnými ISP (infrastruktura Cesnet a LTE).

Základní požadované vlastnosti a funkce řešení

- HW platforma

- řízení bezpečného přístupu mezi vnější a vnitřní sítí
- segmentace zejména použitím demilitarizovaných zón
- zajištění bezpečného vzdáleného přístupu pro uživatele (SSL i IPSec VPN)
- podporou MFA pro vzdálený přístup
- podpora NGFW/UTM(Antivir, IPS, Application Control, WebFiltering, CloudSandbox servis)
- zasílání Syslog zpráv
- podpora Radius a LDAP protokolu
- zabezpečený management (GUI / CLI) - SSH, HTTPS přístup
- podpora IPv6
- podpora záložního připojení do internetu
- podpora dynamických směrovacích protokolů RIP, BGP, OSPF
- podpora HA nasazení v režimech Active/Pasive a Active/Active
- lokální úložiště: 128 GB
- porty: 2x WAN, 1x DMZ, 5x LAN vše GE RJ45
- propustnost při současně zapnutých funkcích FW, IPS, APP Control a Malware protection = threat protection: 100 Mbps
- Požadujeme dodání podpory výrobce v délce trvání min. 5 let
- Dostupnost podpory musí být zajištěna v režimu 24x7, 365 dní v roce.
- Součástí podpory musí být zajištění opravy na místě se zahájením zásahu do konce následujícího pracovního dne od diagnostiky závady.
- Podpora výrobce se musí v celé délce trvání vztahovat na veškerou softwarovou výbavu, která je součástí dodávky. Součástí dodávky musí být zajištění přístupu k aktualizacím a novým verzím veškerého software, který je součástí dodávky.

2.6.3.2. Virtualizační platforma

Popis řešení

Virtualizační platforma bude dodána jako hyperkonvergovaný systém nodů s interní diskovou kapacitou rozšiřitelný jak metodou scale-out, tak scale-up s vysokým stupněm redundance pro přežití výpadku až 50% nodů. V lokalitě DC1 a DC2 bude umístěn vždy minimálně jeden HW nod. Kromě virtualizace výkonu tedy bude řešení disponovat i virtualizací diskové kapacity tzv. Software Defined Storacge (SDS). V těchto případech je nutné zajistit dostatečnou kapacitu datových spojů mezi nody clusteru. Proto bude požadované řešení disponovat minimálně 4x10Gbps spoji , které budou dedikované pouze pro SDS řešení.

Obrázek 6 Schéma řešení virtualizační platformy

Výkonnostní nároky

Pro pořízení dostatečného výkonu HW nodů je důležité definovat nároky jednotlivých VM a VA, které budou v rámci platformy provozovány. Očekávané

výkonnostní požadavky jednotlivých logických komponent aplikační architektury Management modulu RDS 2 udává Tabulka č. 5.

Oblast	Servisní služba	vCPU	RAM (GB)	HDD (TB)	Dedikované HW LAN adaptéry
Provoz	Log Management	8	32	2	
	Network Management a správa konfigurací	4	24	1	
	Network Monitoring	2	8	0,5	
	Flow Monitoring	4	32	1	1x 1GB Base-T
	Zálohování (Backup)	4	24	0,2	
Bezpečnost	Adresářové služby LDAP (LDAP)	2	8	0,5	
	Služba bezpečného ověření identity (RADIUS)	2	8	0,5	
	Anti-X ochrana serverů (AntiX-SRV)	*2*	*24*	*1*	
	Anti-X ochrana koncových zařízení (AntiX-EndP)				
	Bezpečná přístupová stanice (SAW)	*2*	*16*	*0,5*	
	Multifaktorová authentizace (MFA)	*2*	*8*	*0,2*	
	CELKEM	32	184	7,4	

Tabulka 7 Minimální výkonnostní nároky Servisních služeb RDS 2

Další zdroje je nutné alokovat také pro vlastní zajištění chodu virtualizační platformy. Očekávané hodnoty jsou uvedeny v Tabulce č. 6.

Oblast	Komponenta	Vlastní potřeby virtualizace pro každý nod hypervisoru			
		vCPU	*RAM (GB)*	*HDD (TB)*	*Dedikované HW LAN adaptéry*
Virtualizační platforma	Virtualizace Serverů	2	4	2* 64GB Flash/USB RAID1 pro vOS	2x 10GB SFP+
	SDS	4	4	200GB	4x 10GB SFP+

Oblast	Komponenta	Potřeby virtualizace pro zajištění chodu VM a VA			
		vCPU	*RAM (GB)*	*HDD (TB)*	*Dedikované HW LAN adaptéry*
Virtualizační platforma	Virtualizace Serverů	32	184	7,4	1x 1GB Base-T
	SDS				

Tabulka 8 Minimální výkonnostní nároky na virtualizační platformu Management modulu RDS 2

Servery

Budou dodány minimálně 2 servery, nody virtualizační platformy, kdy každý bude naplňovat tyto minimální požadavky:

- Server v provedení RACK (šíře 19”), výška 2U, barevně označené hot-plug vnitřní komponenty, pro přístup ke všem komponentám serveru není nutné nářadí, zásuvné kolejnice pro instalaci do racku s výklopným, nebo výsuvným ramenem pro vedení kabelů.
- Server musí být vybaven redundantním napájením a s předozadním chlazením s dostatečným výkonem pro jeho plné osazení.

- Požadujeme dvousocketový server osazený jedním CPU s počtem 16 jader. CPU musí dosahovat hodnocení minimálně 24 300 bodů ve výsledcích publikovaných na : https://cpubenchmark.net/multi_cpu.html
- Bootování serveru musí být vyřešeno vnitřními disky pro Hypervisor. Tyto disky musí mít min. kapacitu 240GB a pod ochranou RAID1 (zrcadlené). Disky musí být provedení SSD, SHDC, SATA-DOM, nebo M.2 (mechanické, otáčivé disky se nepřipouští)
- Server musí disponovat min. 24x DIMM slot. Požadujeme osazení 6x 32GB LRDIMM, DDR4, 2666MT/s (celkem 192GB)
- server musí podporovat min. 24x2,5" diskové sloty typu hotplug. Server musí akceptovat disky s rozhraním SATA|NLSAS|SAS typu HDD (rotační)|SSD nebo jejich libovolné kombinace. Požadujeme osadit: 6x min. 1,8 GB SSD, min. SATA
- Server musí být vybaven min. dvěma 10GbE SFP+ porty typu "LAN on motherboard" (nezabírající volné PCI-E Sloty)
- Dále min. dvěma 1000Base-T porty typu "LAN on motherboard" (nezabírající volné PCI-E Sloty)
- Dvěma separátními kartami se dvěma 10GbE porty SFP+ do PCI-E slotu se odlišnou čipovou sadou než jsou 10GbE LOM porty výše
- Server musí být vybaven redundatními za provozu vyměnitelnými ventilátory a zdroji v konfiguraci N+N. Zdroje musí být v energetické třídě min. Platinum
- Server musí být vybaven nezávislým HW managementem (out of band) s dedikovaným ethernet portem typu 1000Base-T
- Management nástroje musí umět poskytovat diagnostiku serveru a ovladače pro OS bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích, tzn. i bezdiskový server poskytuje diagnostiku serveru. Nepřipouští se diagnostika spouštěná z optické mechaniky nebo jiného externího zařízení (např. USB flash disk, SD karta, atd.)
- Server musí být integrovatelný do monitorovacího systému a mít schopnost monitorování a správy out-of-band bez nutnosti instalace agenta do operačního systému
- Server musí mít schopnost automatického stahování aktualizací FW a biosů, jejich aplikace a možnost následného roll-back v případě selhání, integrované zálohování konfigurace a firmware HW zařízení serveru
- Management musí podporovat dvoufaktorovou autentizaci, filtrování přístupu na základě IP adres (IP blocking) a integraci uživatelů do AD/LDAP
- Požadujeme vestavěné GUI s podporou HTML5, nepřipouští se použití Active-X pluginů, nebo JAVA
- Podpora zabezpečení pomocí lock-down (zamrazení) nastavení serveru, verzí firmware a biosu, jako ochrana proti podvržení škodlivého kódu ve firmwarech. Případné firmware a update výrobce pro server, musí být podepsány certifikátem výrobce.
- Podpora bezpečného vymazání veškerých dat na serveru a jeho komponentách pro případ vyřazení serveru z jeho role
- Komunikace managementu pomocí: HTTPS, CLI, IPMI, WSMAN, REDFISH
- Management tohoto serveru musí být schopen integrace s ostatními servery v tomto zadání, tak aby správa probíhala z jednoho GUI
- Management musí podporovat spojení s technickou podporou výrobce a automaticky vytvářet servisní incidenty, včetně odeslání HW logů serveru (call-home) a to bez nutnosti instalace externího SW, nebo řídícího serveru
- Server v nabízené konfiguraci musí být kompatibilní s dodávanou virtualizační platformou

- Požadujeme dodání podpory výrobce v délce trvání min. 5 let
- Dostupnost podpory musí být zajištěna v režimu 24x7, 365 dní v roce.
- Součástí podpory musí být zajištění opravy na místě se zahájením zásahu do konce následujícího pracovního dne od diagnostiky závady.
- Podpora musí být dodána a garantována jako celek výrobcem zařízení včetně zajištění dodávky náhradních dílů a helpdesku.
- Součástí podpory musí být dodání certifikovaného technika do místa instalace, který provede kvalifikovanou výměnu náhradních dílů.
- Podpora výrobce se musí v celé délce trvání vztahovat na veškerou softwarovou výbavu, která je součástí dodávky. Součástí dodávky musí být zajištění přístupu k aktualizacím a novým verzím veškerého software, který je součástí dodávky.
- Záruční servis musí plně pokrývat i wear-out disků/médií hypervisoru. Pro každé opotřebené médium je požadována jeho bezplatná záruční výměna.

Virtualizace serverů

Bude dodána softwarová licence pro virtuallizační platformu, která zabezpečí pokrytí všech nabízených hypervisorů, minimálně však 2 hardwarových nodů.

Minimální požadované vlastnosti a funkcionality hypervisoru:

- Funkcionalita, která automaticky nastartuje virtuální stroje při výpadku fyzického serveru na jiném produkčním serveru ze společného diskového pole nebo opětovně restartuje dotčený virtuální stroj např. při pádu OS
- Funkcionalita, která umožní provádět diskovou zálohu a jednoduchou obnovu na úrovni image virtuálních strojů nebo jednotlivých souborů
- Rozhraní umožňující zálohovacímu SW třetí strany provádět konzistentní plné, rozdílové a přírůstkové zálohy virtuálních strojů bez zbytečného zvyšování režie a zátěže hostitelského serveru i virtuálních strojů
- Komplexní správa virtuální infrastruktury z jedné konzole a umožňující integraci s produkty třetích stran
- Software pro virtualizaci serverů včetně management konzole musí licenčně pokrývat použití pro všechny fyzické procesory dodávané v hypervisorech v rámci řešení, minimálně však pro 4 (min. 2 fyzické servery, každý min. dva procesory)
- Support na hypervisor musí být poskytován samotným výrobcem hypervisoru
- Hypervisor nainstalovaný přímo na hardware, umožňující plnou virtualizaci x86 stroje
- Virtualizace a agregace x86 strojů a k nim připojených síťových a datových úložišť do unifikovaných souborů zdrojů
- Symetrický multiprocesing zlepšující výkonnost virtuálního stroje a umožňující, aby jediný virtuální stroj využíval až 32 virtuálních procesorů současně
- Podpora operačních systémů Windows 2000 a novější, Linux, FreeBSD jako OS ve virtuálních strojích
- Podpora PV, BT, HW (paravirtualization, binary translation, harware-assist) virtualizace
- Funkcionalita, která umožňuje přidělovat virtuálním strojům více diskového prostoru než je skutečná disková kapacita
- Bezvýpadková migrace virtuálních strojů za provozu
- Replikace pouze změněných bloků dat
- Funkcionalita umožňující přesměrování zpracování antivirové a antimalware kontroly jednotlivých virtuálních strojů přes zabezpečenou virtuální instanci třetí strany

Storage - SDS

Bude dodána softwarová licence vysoce dostupného úložiště pro dodávanou virtualizační platformu. Licence zabezpečí pokrytí minimálně 2 nodů hypervisorů.

Minimální požadované vlastnosti a funkce

- Hyperkonvergovaný systém nodů s interní diskovou kapacitou rozšiřitelný jak metodou scale-out, tak scale-up s vysokým stupněm redundance pro přežití výpadku až 50% nodů
- Dvojnásobná active – active replikace dat mezi nody clusteru pro zvýšení dostupnosti dat s možností Stretched Clusteru
- Asynchronní replikace dat po pomalých linkách pro případné budoucí vytvoření DR lokality
- Lokální redundance na úrovni nodu formou hw nebo sw RAID
- Možnost Write-back/Write-through RAM cache pro datastore
- Podpora Write-through SSD cache pro zvýšení počtu IO operací za vteřinu
- Podpora automatického storage tieringu pro přesouvání dat mezi pomalými a rychlými disky
- Funkce Data Locality pro omezení síťového provozu mezi nody clusteru
- Požadovaná využitelná disková kapacita s dvojnásobnou synchronní replikací je min. 8 TB
- Pokud je systém licencován na kapacitu, požadujeme licence na celou požadovanou kapacitu
- Požadovaný výkon storage vrstvy je min. 800 IOPs
- Podpora protokolů iSCSI, NFS v4.1, SMB3,
- Podpora WEB-based managementu
- Požadovaný typ SW licence - trvalá

Ochrana dat

V rámci HW nodů virtualizační platformy se počítá se zajištěním proti výpadku flash disku technologií RAID1 a pro zajištění ochrany SDS formou RAID5.

Síťové úložiště NAS

Pro zajištění dostatečné diskové kapacity prováděných záloh VM, VA a celého prostředí dodávané virtualizační platformy bude do lokality DC1 dodáno diskové úložiště typu Network Atached Storage (NAS).

Minimální požadované vlastnosti a funkce

- NAS v provedení RACK (šíře 19”),
- výška max. 2U
- minimálně 8 šachet pro HDD
- možnost rozšíření kapacity pomocí rozšiřovací jednotky
- minimální počet šachet pevného disku s rozšiřující jednotkou: 12
- kompatibilní typ disků: 3.5" SATA HDD, 2.5" SATA HDD, 2.5" SATA SSD
- disky vyměnitelné za provozu
- 64-bit CPU architektura
- CPU: Čtyři jádra, frekvence 2.4 GHz
- vyžadovaná instalovaná systémová paměť 2 GB DDR3
- 2 paměťové sloty
- paměť rozšiřitelná na 16 GB
- komunikační porty:
    - 4x RJ-45 1GbE LAN port s podporou funkcí Link Aggregation / Failover

  - 2x Port USB 3.0
  - 1x port pro rozšiřovací jednotku
- Možnost osazení PCIe slotu přídavnou kartou LAN 10GB
- Vyžadované instalované 4ks interních HDD, optimalizovaných pro NAS a provoz v režimu 24/7, každý s vlastnostmi:
  - kapacita: 6000 GB (6TB)
  - rozhraní: SATA III, 6Gb/s
  - přenosová rychlost až: 210MB/s
  - rychlost otáček: 7200 RPM
  - vyrovnávací paměť: 256MB
  - rozměry: 3,5 HDD

2.6.4. Stávající HW zdroje a licence a jejich využití

2.6.4.1. Aktivní prvky

Stávající HW aktivních prvků, které jsou pro projekt rozšíření RDS k dispozici a předpokládá se, že budou využity:

- **pro CORE síť:**

JC103A	HP A5800-24G SFP Switch	2x
JD362A	HP A5500 150W AC Power Supply	2x
JC094A	HP 5800 16-Port Gig-T Module	2x

- **pro OOB síť:**

JC101A	HP 5800-48G Switch with 2 Slots	2x
JC087A	HP 5800 300W AC Power Supply	4x
JC095A	HP 5800 16-port SFP Module	2x
JC091A	HP 5800 4-port 10GbE SFP+ Module	2x
JD255A	HP 5820 VPN Firewall Module	2x

Součástí dodávky tohoto projektu je i rozšíření současných aktivních prvků o redundandní zdroje a další příslušenství.

2.6.4.2. SW a licence

Stávající SW a licence, které jsou pro projekt rozšíření RDS k dispozici a předpokládá se, že budou využity:

- GrayLog Enterprice 3.1.3. - free edition
- Zabix 4.4
- Veeam Backup & Replication Community Edition
- Linux Debian 9 Server s OpenLDAP
- Linux Debian 9 s FreeRadius

2.6.5. Ostatní parametry řešení

2.6.5.1. Kabeláž

Součástí řešení bude veškerá kabeláž LAN v potřebném množství pro propojení HW komponent Management Modulu a napojení na Propojovací modul. Přesné délky požadovaných kabelů budou upřesněny v rámci přípravného prováděcího projektu. Pokud nějaký kabel bude v provedení Fiber Optic, budou potřebné optické transceivery součástí dodávky na obou stranách připojení.

2.6.5.2. Implementační práce

Součástí dodávky jsou dále následující implementační a migrační práce:

- Předimplementační analýza a prováděcí projektová dokumentace včetně stanovení akceptačních kritérií, popisu a návrhu harmonogramu implementace a postupné migrace s důrazem na minimalizaci nutných odstávek provozu dle potřeb stávající RDS.
- Konfigurace všech HW a SW komponent v rámci Management modulu tak, aby byl zajištěn provoz Servisních služeb RDS 2 dle předimplementační analýzy a prováděcího projektu
- Instalace dodaného hardware do racku v rámci uvažovaných datových lokalit
- Zapojení do napájení
- Zapojení do LAN
- Příprava serverů pro prostředí virtualizační platformy
- Nastavení a konfigurace SDS
- Nastavení a konfigurace NAS
- Akceptační testy vysoké dostupnosti
- Projektové vedení
- Dokumentace dodaného řešení (Dokumentace skutečného stavu)
- Demontáž odpojených zařízení, nahrazených v realizovaném projektu

2.7. Propojovací modul

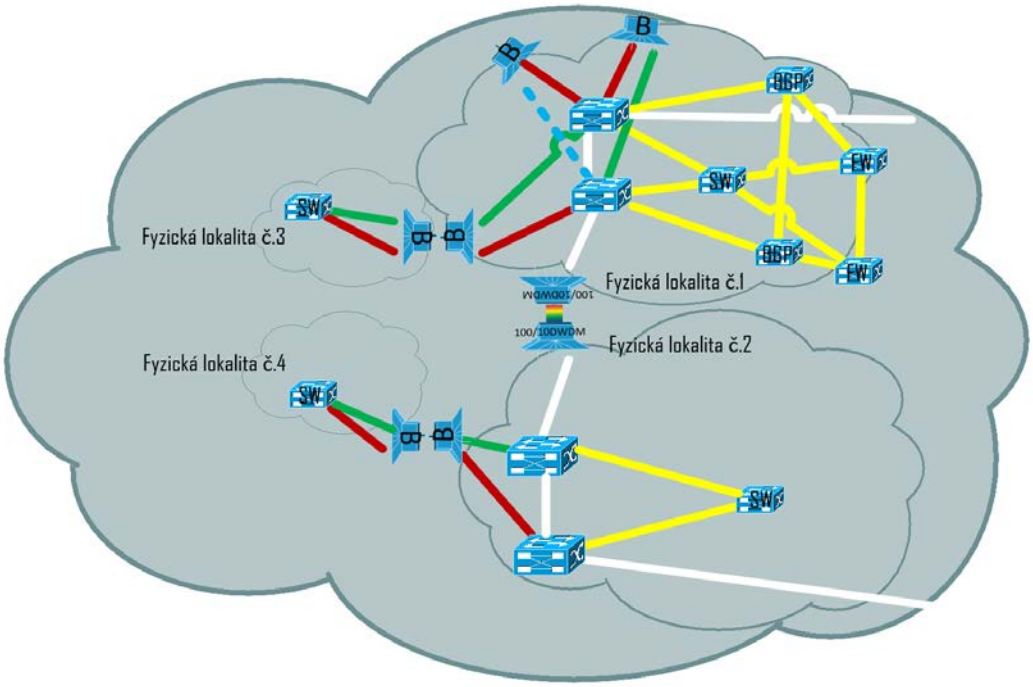
Modul je umístěna v DC Krajského uřadu (na obrázku Fyzická lokalita 1) a skládá se z edge routerů a služby firewallu (viz Bezpečnostní modul), který v současné konfiguraci umožňuje hlavně řízení komunikace různých služeb mezi sebou, komunikaci mezi moduly a komunikaci do externí zóny.

Jako součást dodávky je požadována dodávka BGP 2 kusů routerů pro zajištění provozu vlastního autonomního systému Pardubického kraje s minimálními parametry:

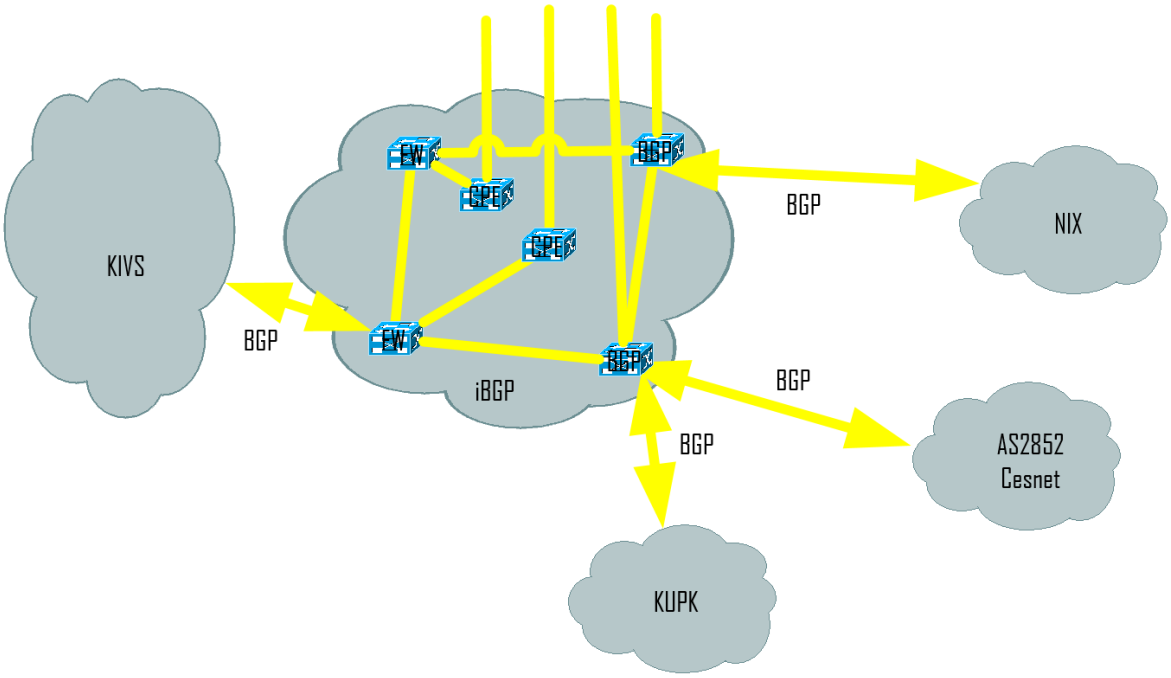
Popis funkce / vlastnosti	Požadavek
Typ přepínače	router
Formát přepínače	Standalone
Počet portů 10Gbps FO (SFP/SFP+ nebo XFP) (minimálně)	8
Při variantě univerzálních portů 10Gbps/1Gbps FO (SFP/SFP+) wire speed, počet portů minimálně	7
Řízení bufferů výstupních portů	ANO
Minimální kapacita/propustnost přepínače	160Gb/s
Minimální přepínací kapacita	150 Mpps
Směrování protokolů IPv4 a IPv6 v hardware (shodný výkon pro oba protokoly)	ANO
GRE tunelování v hardware pro IPv4 i IPv6	ANO
Rourovací protokoly static route, BGPv4, MP-BGP, OSPFv2, OSPFv3, RIPv2, RIPng, BGP4+	ANO
Policy-based routing podle ACL, Routing policies nebo obdobné	ANO
Reverse path check (uRPF)	ANO
IGMPv2, IGMPv3	ANO
IPv4 Multicast (PIM SSM, PIM SM)	ANO
IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)	ANO
First Hop Redundancy Protokol pro IPv4 i IPv6 (např. VRRP, HSRP)	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO
Min. IPv4 routes ve FIB (forwarding table) tabulce	1 000 000
Min. IPv6 routes ve FIB (Forwarding table) tabulce	256 000

multicast IPv4 a IPv6 routes ve FIB tabulce (minimálně)	8 000
Minimální počet záznamů ve směrovací tabulce pro IPv4	2 000 000
Minimální počet záznamů ve směrovací tabulce pro IPv6	1 000 000
IEEE 802.1Q	ANO
Minimální počet aktivních VLAN	4000
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO
IEEE 802.1s - Multiple Spanning Tree Protocol (min.16 instancí)	ANO
Podpora ochrany STP Roota a mechanismy kontroly BPDU	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO
Podpora jumbo rámců (min. 9200 bytes)	ANO
Implementace QoS	ANO
Minimální počet HW QoS front	8
QoS classification – ACL, DSCP, CoS based	ANO
IEEE 802.1P / DSCP priority marking a remarking	ANO
QoS Policing	ANO
QoS-Hierarchical QoS	ANO, min. 3 úrovně
Queue scheduling mechanisms, včetně SP, WRR/WFQ, SP+WRR	ANO
QoS-Dual Strict Priority Queues	ANO
IEEE 802.1ad , QinQ a VLAN mapping	ANO
Traffic shaping – IPv4 a IPv6	ANO
IPv6 QoS	ANO
L2 VPN	ANO
L3 VPN	ANO
Podpora protokolů a služeb (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO
ISATAP tunely	ANO
6to4 tunely	ANO
Konfigurovatelné prostředky pro ochranu L3 přepínače před útoky typu odepření služby (DoS) formou vhodného omezení frekvence určitých typů rámců/paketů, které jsou zpracovávány procesorem zařízení	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN) local i remote	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy, proti připojení neautorizovaného DHCP serveru.	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO
IEEE 802.3ae šifrování	ANO
Standard ACL, extended ACL, VLAN ACL, Ingress/Egress ACL – IPv4 a IPv6 IPv6 nebo obdobné	ANO
Podpora filtrování paketů založená na časovém úseku (time range) – např. při opakovaných událostech	ANO
Monitorování aplikačních toků prostřednictvím technologie NetFlow dle RFC 3954 nebo podobné. Zařízení musí umět zpracovat minimálně každý čtvrtý paket . Funkce monitorování musí být implementována bez negativních dopadů na zátěž a výkon řídících procesorů	ANO

Veškeré licence a zapnuté funkce pro advanced routing a MPLS součástí dodávky (MPLS, forwarding, MPLS load balancing, MPLS Fast Reroute, MPLS, Traffic Engineering, EoMPLS Ethernet Remote port Shutdown, Point-to-Multipoint MPLS Traffic Engineering)	ANO
ASPATH rewrite (či kompatibilní) pro IPv4 i IPv6	ANO
Řízení bufferů výstupních portů	ANO



Obrázek 7- detail Propojovacího modulu ve fyzické lokalitě Krajského úřadu



Obrázek 8 - Komunikace vůči externí zóně

2.8. Bezpečnostní modul

V současně navrženém projektu je zde umístěn pouze firewall, který slouží pro oddělení jednotlivých modulů, VPN instancí a k napojení modulu KIVS. BM bude v budoucnu obsahovat další služby pro uživatele sítě v bezpečnostní oblasti, viz tabulka.

Zadavatel vyžaduje jako součást projektu dodávku dvojice zařízení firewallu nakonfigurovanou pro zabezpečení jednotlivých VPN instancí, služeb a modulů od sebe a v komunikaci s externí zónou. Zařízení jsou požadována s následujícími parametry:

2.8.1. Firewall včetně webové proxy– minimální požadavky :

1) Rozhraní 8xSFP+
2) HW platforma, all-in-one on box
3) Provedení rackmount 19“ a redundantní integrované hotswap zdroje napájení, max 2U per node
4) Provoz v konfiguraci cluster N+1, v případě přidání dalších nodů navýšení redundance a navýšení výkonu
5) Výkonnost node/zařízení:
    a. Počet souběžných spojení 20 000 000, na port 2 500 000
    b. Počet nových spojení za vteřinu – 200 000
    c. Počet odbavených http požadavků za vteřinu s odpovědí o velikosti 8kB na rozhraní firewallu s webovým filtrem při zapnutí kategorizace (2 kategorie) a HTTPS inspekce - 9600
    d. Průchod (FW + web (64-1500 b)) 40 Gbps
6) Definice rozhraní LAN, WAN a DMZ včetně definice 128 VLAN, konfigurace 2 rozhraní pro jednu logickou linku v módu Active/Standby nebo LACP
7) Grafické rozhraní pro správu přes oddělený interface (min. HTTPS, SSH) a vzdálený šifrovaný přístup na CLI
8) Management s možností definice administrátorských rolí a účtů (napojení na Radius včetně přidělení rolí)

9) SNMP, SNMPv3 protokol – vyčítání stavu zařízení (počet aktivních session, provoz na rozhraních, počet aktivních rozhraní, …)
10) Vzdálené vyčítání informací o stavu zařízení (verze firmware, výkonové parametry, celkové zdraví zařízení, atd.), integrovatelné do centrálního konzole/dohledu
11) Aplikování nových pravidel bez ukončení běžících session (firewall i webová proxy)
12) Synchronizace času přes NTP
13) Zálohování konfigurace formou textového formátu, download/upload konfigurace
14) Historie konfiguračních změn, porovnávání verzí konfigurací
15) Zasílání NETFLOW v9 nebo IPFIX včetně informace o překladech IP adres se vzorkem max. 1:4 na min. jeden cíl
16) Plnohodnotná podpora IPv4 a IPv6 - dual-stack bez výkonového rozdílu mezi verzemi IP
17) Statické routování, protokol OSPF, BGP
18) Policy routing na základě určení zdrojové IP, cílové IP
19) Stavový paketový filter, ACL filter, Antispoofing, nastavení ratelimit (IP adresa, protokol)
20) Obranu před útoky min. DNS Query Flood, SYN Flood, UDP Flood, ICMP Flood, Ping of Death, Smurf
21) Zdrojový NAT s Port Address Translation (PAT), cílový NAT s PAT, Statický NAT, Dynamický NAT, NAT 1:1, redirect
22) Aplikační služby (proxy)- H.323, FTP, SIP, DNS s validací přes DNSSec
23) Nastavení přenosového pásma pro uživatele (garantované pásmo, maximální pásmo, řízení provozu dle definovaných politik), QoS
24) Přidělování šířky pásma v závislosti na zdrojové/cílové IP, www kategorií
25) Nasazení filtrace webového obsahu v transparentním nebo netransparentním režimu pro HTTP a HTTPS (bez nutnosti rozšifrování spojení, např. na základě SNI)
26) Výjimky z HTTPS inspekce na určené zdrojové IP, servery nebo kategorie
27) Kontrola HTTPS provozu, ověřování certifikátu na proxy
28) Definice důvěryhodných CA, podpis nedůvěryhodných CA, rozlišení typu chyb (expirace certifikátu, chybná doména, slabý šifrovací klíč …), podmíněné zpřístupnění na omezenou dobu
29) Kategorizace webových domén dle obsahu v počtu min. 50ks, kategorizační databáze nezávislá na online službě nebo cloudu, databáze kategorií v rámci dodávky
30) Samostatné kategorie domén pro www se škodlivými kódy a P2P
31) Politika přístupu uživatele na služby definovaná dle času, kategorií, cílové adresy, uživatele, skupiny uživatelů
32) Definice vlastní kategorie/politik zdrojů, cílů, identit
33) Kategorizace webových stránek podle celé URL adresy(i subdomény)
34) Ověřování přenášených souborů na základě MIME type i CONTENT type, nastavení pravidla pro zákaz přenosu
35) Detekování typů přenášených souborů v HTTP/HTTPS komunikaci
36) Definice black/white listů (uživatel, skupina, IP adresa)
37) Reklamace chybného záznamu pomocí webového formuláře, zpětná vazba, rychlost reakce na ruční hlášení do 48h v pracovní dny
38) Aktualizace webového filtru o nezařazené domény z webového provozu v pracovní dny do 48h
39) Interface pro protokol ICAP na zapojení externího antiviru (např. ClamAV)
40) Implementace explicitní proxy pomocí PAC či WPAD
41) Podpora více upstream proxy s podmíněným směrováním provozu
42) Detekce vnořených archivů
43) Monitoring/blokování aplikací např. P2P, Youtube, Facebook, IM
44) Možnost omezení šířky pásma pro streaming provoz
45) Granulární rozpoznání obsahu stránek např. Facebook (povolení přístupu na Facebook s blokováním facebook chat, atd
46) Autorizace uživatele na základě IP, subnetu, LDAP
47) Podpora LDAP/AD skupin pro přiřazení politik a skupin uživatelů

48) Monitoring provozu, statistiky provozu, periodické reporty o provozu, údaje o úspěšné kategorizaci provozu přes filter (http i https), nástroj na prohledávání logů firewallu i webové proxy, log aktivity správce zařízení
49) Nastavení doby pro uchování záznamů na lokálním úložišti logů
50) Logování na externí server přes protokol Syslog (aktivita správce, firewall log, …)
51) Zachycení provozu pro následnou analýzu (dump provozu pro následnou analýzu např. ve Wiresharku)
52) Perpetual licenční pokrytí veškeré požadované funkcionality a počty uživatelů včetně maintenace dle rámcové smlouvy, zachování funkcionality v rozsahu požadavků zadání i v případě v budoucnu nezakoupené podpory
53) Dokumentace řešení, zaškolení obsluhy v počtu 2 osob v rozsahu 4 hodiny
54) Reporty připravené, definice vlastních reportů
55) Detailní reporty pro každého uživatele, export, pravidelné odesílání na email, publikace na stránku (počeštění šablony)
56) Reporty do PDF, CSV, HTML
57) Reporty dle skupin/uživatele, IP, subnetu, atd.
58) Exporty do SIEM

2.9. Transportní modul

Jedná se o vlastní MPLS síť v území Pardubického kraje.

2.9.1. Primární kruh (superpáteř)

Zadavatel vyžaduje zakruhování lokalit s nemocnicemi. Vzhledem k počtu a charakteru napojených dalších uzlů nemocnic je požadována přenosová rychlost 100Gbps oběma směry. Minimální zakruhované uzly v primárním kruhu by měly být:

a) Nemocnice Pardubice
b) Krajský úřad Pardubice
c) Nemocnice Litomyšl
d) Nemocnice Svitavy
e) Nemocnice Chrudim

Ostatní lokality po cestě jsou předpokládané.

Primární propojení uzlů mezi sebou je 100Gbps, v rámci uzlu 2x 100Gbps a s CPE 10Gbps v redundaci a LACP.

Pro vytvoření aktivní části kruhu zadavatel požaduje:

Min. 12 ks aktivních prvků typu SB_I:

Popis funkce / vlastnosti	požadavek
Formát přepínače/zařízení	standalone
Plná podpora provozu IPv4 a IPv6 při současném provozu	ANO
Plná provozu MPLS	ANO
Počet portů 10Gbps FO (SFP/SFP+) wire speed (minimálně), porty mohou být v kombinaci rychlostí 10/25Gbps při zachování všech ostatních požadavků	16
Podpora zapojení 100 Gbps interface min 4ks	ANO
Dodání potřebných 100 Gbps FO interface dle vlastností optických propojů	ANO
Dodání 2x 100 Gbps copper stack interface do 5 m	ANO
Počet portů 1Gbps FO (SFP) wire speed	10
Při variantě univerzálních portů 10Gbps/1Gbps FO (SFP/SFP+) wire speed (minimálně)	20
Podpora OEM kompatibilních FO modulů	ANO
Podpora virtualizace – možnost sloučit dvě fyzická šasi do jednoho logického (pro L2 i L3 protokoly je virtual chassis jedním uzlem)	ANO
Přepínací výkon při libovolném typu rámce/paketu	min. 300Mpps

Podpora HOT-plug karet na všech modulárních slotech	ANO
Aplikace hot patch (podpora aplikace patchů software/firmware bez vypnutí/restartu virtual šasí)	ANO
Redundantní napájecí zdroj (interní) součástí (výsledně tedy min. 2ks), vyměnitelný za provozu	ANO
IPv6 a IPv4 protocol stacks	ANO
Management CLI rozhraní SSHv2, SNMP v1/v2/v3, FTP, TFTP pro IPv4 bez nutnosti přepínání CLI mezi virtuálními nody chassis	ANO
Podpora RADIUS klient pro AAA (autentizace, autorizace, accounting), včetně zařazování do různých skupin privilegovaných módů (např. read only, full apod.) jednotlivých uživatelů,	ANO
Logování pomocí SYSLOG a SNMP trap do navazujících monitorovacích nástrojů pro IPv4 i IPv6	ANO
Služby: ARP Proxy, DHCP Relay, DHCP Server, ICMP redirect, NTP server pro IPv4 i IPv6	ANO
Redundance všech klíčových komponent (napájecí zdroje, větráky, přepínací matice, atd), možnost výměny vadných komponent bez ovlivnění funkce systému	ANO
Schopnost upgrade SW a HW za provozu bez výpadku provozu virtual šasí	ANO
Schopnost aktivace záložních komponent při výpadku primárních (bez výpadku provozu)	ANO
Pro směrování protokolů IPv4 a IPv6 nepoužívat CPU v hardware (shodný výkon pro oba protokoly)	ANO
GRE tunelování v hardware pro IPv4 i IPv6	ANO
Rourovací protokoly static route, BGPv4, MP-BGP, OSPFv2, OSPFv3, RIPv2, RIPng, BGP4+	ANO
Policy-based routing podle ACL, Routing policies	ANO
IGMPv2, IGMPv3	ANO
IPv4 Multicast (PIM SSM, PIM SM)	ANO
IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)	ANO
Podpora multicast VPN/VRF	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) - min. 128 instancí	ANO
First Hop Redundancy Protokol pro IPv4 i IPv6 (např. VRRP, HSRP)	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO
Minimální počet routes ve FIB (forwarding table) tabulce (pro IPv4 a IPv6 údaj pro každý protokol odděleně a vždy minimálně 64 000, tedy 64 000 pro IPv4 a 64 000 pro IPv6)	64 000
Minimální počet multicast routes ve FIB (forwarding table) tabulce (pro IPv4 a IPv6 údaj pro každý protokol odděleně a vždy minimálně 64 000, tedy 64 000 pro IPv4 a 64 000 pro IPv6)	64 000
Minimální počet záznamů ve směrovací tabulce pro IPv4 a IPv6 (pro IPv4 a IPv6 údaj pro každý protokol odděleně)	500 000
Minimální počet MAC adres v tabulce	128 000
Detekce protilehlého zařízení (např. LLDP nebo CDP)	ANO
IEEE 802.3ad přes více šasi (Multichassis LAG)	ANO
Minimálně 8 linek jako součást LAG trunku	ANO
Minimální počet konfigurovatelných LAG trunků	64

IEEE 802.1Q	ANO
Minimální počet aktivních VLAN	4094
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO
IEEE 802.1s - Multiple Spanning Tree Protocol (min.16 instancí)	ANO
Podpora ochrany STP Roota a mechanismy kontroly BPDU	ANO
Protokol MVRP nebo VTP (či kompatibilní) pro definici a správu VLAN sítí	ANO
Podpora jumbo rámců (min. 9200 bytes)	ANO
Implementace QoS	ANO
Minimální počet HW QoS front per port	8
QoS classification – ACL, DSCP, CoS based	ANO
IEEE 802.1P / DSCP priority marking a remarking	ANO
QoS Policing	ANO
QoS-Hierarchical QoS	ANO, min. 3 úrovně
Queue scheduling mechanisms, včetně SP, WRR/WFQ, SP+WRR	ANO
IEEE 802.1ad , QinQ a VLAN mapping	ANO
Traffic shaping – IPv4 a IPv6	ANO
IPv6 QoS	ANO
Podpora IPSec	ANO
L2 VPN	ANO
L3 MPLS VPN	ANO
VPLS pseudo-wires, point-to-point, point-to-multipoint	ANO
Podpora protokolů a služeb per VRF (VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO
Konfigurovatelné prostředky pro ochranu L3 přepínače před útoky typu odepření služby (DoS) formou vhodného omezení frekvence určitých typů rámců/paketů, které jsou zpracovávány procesorem zařízení	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN) local i remote	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy, proti připojení neautorizovaného DHCP serveru.	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO
IEEE 802.1ae šifrování kromě portů 100Gbps	ANO
Standard ACL, extended ACL, VLAN ACL, Ingress/Egress ACL – IPv4 a IPv6 nebo obdobné	ANO
Podpora filtrování paketů založená na časovém úseku (time range) – např. při opakovaných událostech	ANO
NetFlow dle RFC 3954 nebo podobné- ,zařízení musí umět zpracovat minimálně každý čtvrtý paket. Funkce monitorování musí být implementována bez negativních dopadů na zátěž a výkon řídících procesorů	ANO
Veškeré licence a zapnuté funkce pro advanced routing a MPLS součástí dodávky (MPLS, forwarding, MPLS load balancing, MPLS Fast Reroute, MPLS, Traffic Engineering, EoMPLS Ethernet Remote port Shutdown, Point-to-Multipoint MPLS Traffic Engineering)	ANO
ASPATH rewrite (či kompatibilní) pro IPv4 i IPv6	ANO

Řízení bufferů výstupních portů	ANO

Min. 4ks aktivních prvků typu SB_II

Stejné parametry jako předchozí typu, pouze změna jediného parametru:

Podpora zapojení 100 Gbps interface min **6**ks	ANO

Zadavatel neurčuje technologii přenosu přes optická vlákna, hlavním parametrem splnění parametrů je přenosová rychlosti a funkční MPLS přenos na vyšší vrstvě.

2.9.2. Případný druhý kruh a ostatní

Pokud v rámci prvního kruhu nebudou zakruhovány všechny lokality s nemocnicemi, zadavatel požaduje konfiguraci druhého kruhu postaveného na n x 10Gbps technologii, v tomto případě 2 x 10Gbps v rámci tohoto projektu.

Vzhledem k tomu, že i ostatní lokality budou v dalších fázích zakruhovány, jsou požadavky na aktivní prvky PE stejné. Výjimkou v počtu nových PE jsou lokality Moravská Třebová, Holice a Přelouč, kde budou použity současné MPLS aktivní prvky HPE 5800A osazené redundandními zdroji.

Min. zakruhovaná lokalita v tomto projektu:

a) Nemocnice Ústí nad Orlicí

Primární propojení mezi uzly je 2 x 10Gbps, v případě použití CPE, min. 10Gbps.

Pro realizaci tohoto projektu požadujeme:

Min. 10 ks aktivních prvků splňující následující minimální parametry:

Popis funkce / vlastnosti	požadavek
Formát přepínače/zařízení	Standalone
Plná podpora provozu IPv4 a IPv6 při současném provozu	ANO
Plná provozu MPLS	ANO
Počet portů 10Gbps FO wirespeed (SFP+ nebo XFP) (minimálně),), porty mohou být v kombinaci rychlostí 10/25Gbps při zachování všech ostatních požadavků	8
Počet portů 1Gbps FO (SFP) (minimálně)	8
Při variantě univerzálních portů 10Gbps/1Gbps FO (SFP/SFP+) (minimálně)	16
Podpora OEM kompatibilních FO modulů	ANO
Podpora virtualizace – možnost sloučit dvě fyzická šasi do jednoho logického (pro L2 i L3 protokoly je virtual chassis jedním uzlem)	ANO
Minimální propustnost přepínače	160Gb/s
Redundantní napájecí zdroj (interní)) součástí (výsledně tedy min. 2ks), vyměnitelný za provozu	ANO
IPv6 a IPv4 protocol stacks	ANO
Management CLI rozhraní SSHv2, Web-Based, SNMP v1/v2/v3, FTP, TFTP pro IPv4	ANO
Podpora RADIUS klient pro AAA (autentizace, autorizace, accounting), včetně zařazování do různých skupin privilegovaných módů (např. read only, full apod.) jednotlivých uživatelů/	ANO
Logování pomocí SYSLOG a SNMP trap do navazujících monitorovacích nástrojů pro IPv4 i IPv6	ANO
Služby: ARP Proxy, DHCP Relay, DHCP Server, ICMP redirect, NTP server pro IPv4 i IPv6	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO

GRE tunelování v hardware pro IPv4 i IPv6	ANO
Rourovací protokoly static route, BGPv4, MP-BGP, OSPFv2, OSPFv3, RIPv2	ANO
Policy-based routing podle ACL, Routing policies	ANO
Reverse path check (uRPF)	ANO
IGMPv2, IGMPv3	ANO
IPv4 Multicast (PIM SSM, PIM SM)	ANO
IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)	ANO
Podpora multicast VPN	ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) - min. 128 instancí	ANO
First Hop Redundancy Protokol pro IPv4 i IPv6 (např. VRRP, HSRP)	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO
Minimální počet routes ve FIB (forwarding table) tabulce (pro IPv4 a IPv6 údaj pro každý protokol odděleně a vždy minimálně 64 000, tedy 64 000 pro IPv4 a 128 000 pro IPv6)	4 000
Minimální počet multicast routes ve FIB (forwarding table) tabulce (pro IPv4 a IPv6 údaj pro každý protokol odděleně a vždy minimálně 64 000, tedy 64 000 pro IPv4 a 64 000 pro IPv6)	64 000
Minimální počet záznamů ve směrovací tabulce pro IPv4 a IPv6 (pro IPv4 a IPv6 údaj pro každý protokol odděleně)	500 000
Minimální počet MAC adres v tabulce	128 000
Detekce protilehlého zařízení (např. LLDP nebo CDP)	ANO
IEEE 802.3ad přes více šasi (Multichassis LAG)	ANO
Minimálně 8 linek jako součást LAG trunku	ANO
Minimální počet konfigurovatelných LAG trunků	64
IEEE 802.1Q	ANO
Minimální počet aktivních VLAN	4000
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO
IEEE 802.1s - Multiple Spanning Tree Protocol (min.16 instancí)	ANO
Podpora ochrany STP Roota a mechanismy kontroly BPDU	ANO
Protokol MVRP nebo VTP (či kompatibilní) pro definici a správu VLAN sítí	ANO
Podpora jumbo rámců (min. 9200 bytes)	ANO
Implementace QoS	ANO
Minimální počet HW QoS front per port	8
QoS classification – ACL, DSCP, CoS based	ANO
IEEE 802.1P / DSCP priority marking a remarking	ANO
QoS Policing	ANO
QoS-Hierarchical QoS	ANO, min. 3 úrovně
Queue scheduling mechanisms, včetně SP, WRR/WFQ, SP+WRR	ANO
IEEE 802.1ad , QinQ a VLAN mapping	ANO
Traffic shaping – IPv4 a IPv6	ANO
IPv6 QoS	ANO
Podpora IPSec	ANO
L2 VPN	ANO
L3 MPLS VPN	ANO
VPLS pseudo-wires, point-to-point, point-to-multipoint	ANO

Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO
Konfigurovatelné prostředky pro ochranu L3 přepínače před útoky typu odepření služby (DoS) formou vhodného omezení frekvence určitých typů rámců/paketů, které jsou zpracovávány procesorem zařízení	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN) local i remote	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy, proti připojení neautorizovaného DHCP serveru.	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO
IEEE 802.1ae šifrování, minimálně na portech vůči CPE	ANO
Standard ACL, extended ACL, VLAN ACL, Ingress/Egress ACL – IPv4 a IPv6mnebo obdobné	ANO
Podpora filtrování paketů založená na časovém úseku (time range), např. při opakovaných událostech	ANO
Monitorování aplikačních toků prostřednictvím technologie NetFlow dle RFC 3954 nebo obdobné - zařízení musí umět zpracovat minimálně každý čtvrtý paket. Funkce monitorování musí být implementována bez negativních dopadů na zátěž a výkon řídících procesorů	ANO
Řízení bufferů výstupních portů	ANO
Redundance všech klíčových komponent (napájecí zdroje, větráky, přepínací matice, atd), možnost výměny vadných komponent bez ovlivnění funkce systému	ANO
Schopnost upgrade SW a HW za provozu bez výpadku provozu virtual šasí	ANO
Schopnost aktivace záložních komponent při výpadku primárních (bez výpadku provozu)	ANO

2.9.3. CPE uzly

Pro při vedení služeb co nejblíže zákazníkovi RDS 2 je navržen systém CPE na technologické bázi přenosu služeb pomocí VLAN v rámci trunk spojení a publikace služby na portech CPE. CPE je spojeno s PE minimálně dvěma propoji spojených v rámci LACP.

Jako součást dodávky je požadována dodávka celkem 30 ks switchů pro zajištění provozu s minimálními parametry:

Popis funkce / vlastnosti	Požadavek
Typ přepínače	L2 přepínač
Formát přepínače	Standalone
Podpora virtualizace – možnost sloučit dvě fyzická zařízení do jednoho logického	ANO
Počet portů 10Gbps FO (SFP+ nebo XFP), wire speed (minimálně)	8
Počet portů 1Gbps FO (SFP+ nebo XFP), wire speede) (minimálně)	6
Možnost osazení DWDM/CWDM interfaces	ANO
Podpora OEM kompatibilních FO modulů	ANO
Minimální kapacita interní sběrnice na přepínače	140Gb/s
802.1ae šifrování, minimálně na straně uplink	ANO
Aplikace hot patch (podpora aplikace patchů software/firmware bez vypnutí/restartu boxu)	ANO
Redundantní napájecí AC zdroj (interní)	ANO
IPv6 a IPv4 protocol stacks	ANO
Minimální počet MAC adres v tabulce	64000

Detekce protilehlého zařízení (např. LLDP nebo CDP)	ANO
Minimálně 6 linek jako součást LAG trunku	ANO
Minimální počet konfigurovatelných LAG trunků	20
IEEE 802.1Q	ANO
Minimální počet aktivních VLAN	4000
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO
IEEE 802.1s - Multiple Spanning Tree Protocol (min.16 instancí)	ANO
Podpora ochrany STP Roota a mechanismy kontroly BPDU	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí či kompatiblní	ANO
Podpora jumbo rámců (min. 9200 bytes)	ANO
Logování pomocí SYSLOG a SNMP trap do navazujících monitorovacích nástrojů pro IPv4 i IPv6	ANO

2.10. Změny v lokalitách

Koncové lokality se z jednotného vzoru rozdělí dle jejich umístění v infrastruktuře na několik typů:

1) Lokalita na primárním okruhu – lokalita má vždy minimálně jeden logický PE uzel (složený ze dvou fyzických zařízení) na hlavní 100Gbps páteřní síti a další CPE uzly (i více) s primárním účelem distribuce služeb a replikací vhodných portů po území lokality (tedy např. na MÚ).. V budoucnu je předpoklad rozdělení logického celku páteřního uzlu do dvou geolokačně odlišných fyzických lokalit se zachováním přenosové rychlosti.
2) Lokality na případných dalších kruzích – kopírují architekturu primárního kruhu, lišící se pouze prací s vlnovým multiplexem n x 10Gbps. CPE uzly jsou realizovány pouze v případě potřeby distribuce po území lokality.
3) Nezakruhované lokality – jsou konfigurovány jako jeden PE, pracující s technologií vlnového multiplexu n x 10Gbps. Předpokladem je budoucí zakruhování těchto uzlů.

   Nejvýznamnější změna je vytvořena v lokalitě Pardubice, kde dojde k rozdělení uzlu DC na dva samostatné uzly. V nemocnici bude vytvořen vlastní DC uzel s napojením infrastruktury nemocnice. Další nový DC uzel bude vytvořen na krajském úřadě. Ostatní uzly v lokalitě budou přeměněny na CPE. Změna vychází z analýzy současného provozu a požadavků rozvoje.

Tabulka č. 9 − Typy uzlů v jednotlivých lokalitách

Název ORP	Název úřadu	Adresa rozvaděčové místnosti, kde bude RDS zakončena	Typ uzlu
Česká Třebová	Městský úřad Česká Třebová	Staré náměstí 78, 560 02 Česká Třebová	Zakruhované PE
Hlinsko	Městský úřad Hlinsko	Adámkova 554, Hlinsko	Zakruhované PE
Holice	Městský úřad Holice	Holubova 1, Holice	PE
Králíky	Městský úřad Králíky	Velké náměstí 5, 561 69 Králíky	PE
Lanškroun	Městský úřad Lanškroun	nám. J. M. Marků 5, 563 01 Lanškroun	PE
Moravská Třebová	Městský úřad Moravská Třebová	Olomoucká 178/2, 571 01 Moravská Třebová	PE

Název ORP	Název úřadu	Adresa rozvaděčové místnosti, kde bude RDS zakončena	Typ uzlu
Polička	Městský úřad Polička	Palackého nám. 160, 57201 Polička	Zakruhované PE
Přelouč	Městský úřad Přelouč	Československé armády 1665	PE
Vysoké Mýto	Městský úřad Vysoké Mýto	B. Smetany 92, 566 32 Vysoké Mýto	Zakrunované PE
Žamberk	Městský úřad Žamberk	Masarykovo nám. 166, 564 01 Žamberk	PE
Pardubice	Zdravotnická záchranná služba Pardubického kraje	Průmyslová 450, 530 03 Pardubice	CPE
Pardubice	Magistrát města Pardubice	Pernštýnské náměstí 1, 530 21 Pardubice	CPE
Pardubice	Pardubická krajská nemocnice	Kyjevská 44, 532 03 Pardubice	DC, Zakruhované PE
Pardubice	Krajský úřad Pardubického kraje	Komenského náměstí 125, 532 11 Pardubice	DC, Zakruhované PE
Chrudim	Chrudimská nemocnice	Václavská 570, 537 27 Chrudim	Zakruhované PE
Litomyšl	Litomyšlská nemocnice	J. E. Purkyně 652, 570 14 Litomyšl	Zakruhované PE
Ústí n. O.	Orlickoústecká nemocnice	Čs. armády 1076, 562 18 Ústí nad Orlicí	Zakruhované PE
Svitavy	Svitavská nemocnice	Kolárova 7, 568 02 Svitavy	Zakruhované PE
Chrudim	Městský úřad Chrudim	Resselovo náměstí 77, 537 16 Chrudim	CPE
Litomyšl	Městský úřad Litomyšl	Bří Šťastných 1000, 570 20 Litomyšl	CPE
Svitavy	Městský úřad Svitavy	T. G. Masaryka 40/25, 568 02 Svitavy	CPE
Ústí n. O.	Městský úřad, Ústí nad Orlicí	Sychrova 16, 562 24 Ústí nad Orlicí	CPE

Stávající lokality (znázorněno černou barvou)

Projektované lokality (znázorněno zelenou barvou)

2.11. Návrh optického vedení sítí

Rozvoj Regionální datové sítě počítá s rozšířením stávající infrastruktury o další lokality, a to za předpokladu pořízení nových optických vláken. Kvalita vláken je podmíněna splněním předpokladu provozu sítě. Zadavatel tedy neříká, jaké kvality mají vlákna být, pouze sděluje, že bude chtít na těchto vláknech mít 20 let garantovanou kvalitu provozu v tomto projektu zmíněné architektury včetně jejich parametrů a služeb. Zadavatel dále nespecifikuje vyšší počet vláken. Určuje, že počet

vláken musí odpovídat požadované architektuře a jejím parametrům. Zadavatel tedy předpokládá dodávku minimálně jednoho vlákna. Každé dodané vlákno však musí splňovat požadavky v této dokumentaci uvedené a nebýt omezením pro požadovanou architekturu včetně jejího rozvoje.

Další obecné požadavky na optická vlákna (ne všechny požadavky budou funkční v souběhu na jednom vlákně, jsou však požadována i pro budoucí změny v architektuře):

1) Provoz minimálně 32 kanálů DWDM dle ITU-T G.694.1, tedy 16 logických obousměrných spojení (Tx+Rx) na jednom optickém vlákně
2) Provoz 100Gbps páteřních spojů mezi lokalitami
3) Veškerá optická vlákna, která jsou předmětem dodávky, budou vyhrazena k výlučnému užívání zadavatelem.
4) Optická vlákna musí být uložena vhodným způsobem buď v zemi (např. v HDPE trubkách, mikrotrubičkách apod.) nebo bude vedena výjimečně v kratších úsecích nadzemním vedením (celková délka nadzemního vedení bude činit maximálně 5% dodávané infrastruktury a bude označena jako rizikový úsek). Součástí dodávky nenasvícených vláken je také jejich příprava ve formě zemních spojek, odboček z tras včetně vyvázání a svaření do patchpanelů. Jedná se o tzv. pasivní část infrastruktury.
5) Garanci (záruku) za pasivní část nese dodavatel optických vláken. Na celou pasivní část infrastruktury zadavatel požaduje garanci (záruku) v délce trvání 20 let – tzn. na dodávku optických vláken a SLA na dodaná optická vlákna.
6) Optická vlákna budou zakončena konektory E2000/APC, a dále popsané jak RDS.
7) Součástí dodávky bude příslušná dokumentace celé pasivní části infrastruktury, viz požadavky Dokumentace
8) Na zadavatele bude převeden ideální spoluvlastnický podíl na optických kabelech spojený s výlučným užíváním optických vláken zadavatelem. Přesná specifikace jednotlivých optických kabelů, výše ideálních spoluvlastnických podílů nabývaných zadavatelem a počet zadavatelem výlučně užívaných optických vláken v jednotlivých optických kabelech bude uvedena v samostatné přehledné tabulce.
9) Zhotovitel zajistí základní servis závad na optických trasách (např. překopnutí kabelu) a ostatních prvcích pasivní části dodávky po dobu 20 let, viz SLA kategorie A.
10) Dále zhotovitel na základě servisní smlouvy tohoto projektu zajistí plnění SLA na dodaných optických vláknech v časových odezvách dle celkového SLA služeb tohoto projektu. Zhotovitel předpokladá servis vláken i po době udržitelnosti projektu.
11) Zhotovitel předpokládá, že u některých vláken v jeho současném vlastnictví bude muset dojít k rozpojení, přepojení, aby byly naplněny všechny požadavky funkcí. Jednání se servisním partnerem nynějších vláken bude provádět zhotovitel, náklady na změny patří opět zhotoviteli.

2.11.1. **Schématické znázornění optických vláken projektu**

Stávající stav (znázorněno černou barvou): Stávající Regionální datová síť vychází z topologie hvězda.

Projektovaný stav (znázorněno zelenou barvou)**:** Rozšíření počítá s využitím stávajících tras. Trasa Pardubice Litomyšl bude využita k připojení lokality Vysoké Mýto rozdělením na dvě části.

Změna na přepojení vlákna (přerušovaná čára): předpokládaná změn přepojení vláken v lokalitě Pardubice.

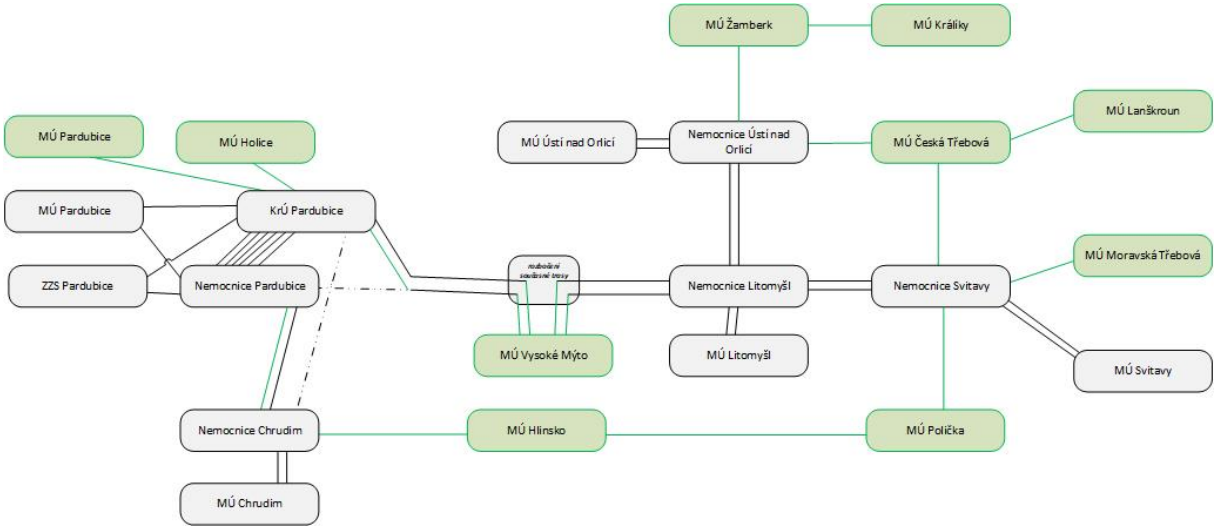


Schéma č. 1: Minimální požadovaná vlákna projektu

2.11.2. Požadavky na pasivní prvky optické infrastruktury

2.11.2.1. Primární kruh 100Gbps

Pro vlastní páteřní 100Gbps přenos není až na lokalitu Pardubice technologie vlnového multiplexování požadována, i když je umožněna.

V rámci nového architektonického návrhu však lokality, které doteď měly více PE budou změněny na kombinaci PE + CPE. Pasivní prvky však mají delší životnost než aktivní, a v případě primárního kruhu lze počítat v budoucnu s rekonfigurací pasivních aktivních prvků do 100Gbps kruhu. Nyní však 4 ks zastanou roli spojení v rámci lokality a 2 ks pro 100Gbps spojení mezi DC Nemocnicí v Pardubicích a Krajským úřadem v Pardubicích a rozmuxování dalších vláken mezi oběma DC.

6ks CWDM/DWDM MUX/DEMUX s 100Gbps odbočkou

Č.	*Vlastnost*	*Požadovaná hodnota*	*Nabídková hodnota*
	Fyzické vlastnosti a prostředí	-	
1.1	Kategorie zařízení – CWDM, DWDM MUX/DEMUX s 100Gbps odbočkou	ANO	
1.2	Formát zařízení - k montáži do stojanu 19"	ANO	
1.3	Výška zařízení	max. 1RU	
1.4	Hloubka zařízení	max. 60cm	
1.5	Provozní teplota minimální	max. 0 st.Celsia	
1.6	Provozní teplota maximální	min. 40 st.Celsia	
1.7	Počet vláken In	1	
1.8	Typ konektoru In	E2000/APC	
	Out Funkčnost 1		
2.1	Přenos	100Gbps	
2.2	Typ přenosu	4 x CWDM 1260 – 1360 nm	

Č.	Vlastnost	Požadovaná hodnota	Nabídková hodnota
2.3	Výstupní port	SC/APC QSFP port	
	Out Funkčnost 2		
3.1	Přenos	CWDM 4 kanály	
3.2	Typ přenosu	1470, 1490, 1590, 1610	
3.3	Způsob vybočení	Add/drop	
3.4	Výstupní port	SC/APC	
	Out Funkčnost 3		
4.1	Přenos	DWDM 16 kanálů	
4.2	Typ přenosu	CH21-CH36	
4.3	Výstupní port	SC/APC	

2.11.2.2. Další lokality včetně dalšího zakruhování

Předpokladem architektury je vedení 10Gbps přes jeden lambda kanál (přes dva tam i zpět), zadavatel proto požaduje dodat a realizovat mux/demux spojení přes 1 vlákno (bidi) a přesto zachovat dostatečnou rezervu kanálů do budoucna nebo pro jiné učely.

Bidi DWDM multiplexery

26 ks DWDM multiplexerů. Přenosová rychlost 10Gbps/lamda.

Č.	Vlastnost	Požadovaná hodnota	Nabídková hodnota
	Fyzické vlastnosti a prostředí	-	
1.1	Kategorie zařízení – DWDM MUX/DEMUX	ANO	
1.2	Formát zařízení - k montáži do stojanu 19"	ANO	
1.3	Výška zařízení	max. 1RU	
1.4	Hloubka zařízení	max. 48cm	
1.5	Provozní teplota minimální	max. 0 st.Celsia	
1.6	Provozní teplota maximální	min. 40 st.Celsia	
	Funkčnost		
2.1	Přenos	Bidi, po jednom vlákně	
2.2	Typ přenosu	DWDM	
2.3	Počet kanálu s obousměrnými službami	16	
2.4	Počet W/L	32	
2.5	Konektor uplink/trunk	E2000/APC	
2.6	Konektor ostatní	SC/APC	
2.7	Vložný útlum	max. 4dB	

2.11.2.3. Optické trasy 100Gbps

Č.	Vlastnost	Požadovaná hodnota	Nabídková hodnota
	Společná charakteristika		
1.1	Kategorie - optická vláknová trasa	ANO	
1.2	Obousměrný přenos	100Gbps	
1.3	Typ přenosu (ethernet, OTN, atd.)	neurčeno	
1.4	Typ optického vlákna	G.652 nebo 657	
	Trasa č.102 Chrudim nem. - Hlinsko MÚ		
2.1	Délka [m]	-	
2.2	Počet vláken	min. 1	
2.3	Útlum na vlnové délce 1310 nm [dB]	-	
2.4	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č.103 Hlinsko MÚ - Polička MÚ		
3.1	Délka [m]	-	
3.2	Počet vláken	min. 1	
3.3	Útlum na vlnové délce 1310 nm [dB]	-	
3.4	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č.104 Polička MÚ - Svitavy nem.		
4.1	Délka [m]	-	
4.2	Počet vláken	min. 1	
4.3	Útlum na vlnové délce 1310 nm [dB]	-	
4.4	Útlum na vlnové délce 1550 nm [dB]	-	

2.11.2.4. Optické trasy n x 10Gbps

Č.	Vlastnost	Požadovaná hodnota	Nabídková hodnota
	Společná charakteristika		
1.1	Kategorie - optická vláknová trasa	ANO	
1.2	Obousměrný přenos	ANO, n x 10Gbps	
1.3	Typ přenosu	DWDM	
1.2	Počet vláken	1	
1.3	Typ optického vlákna	G.652 nebo 657	
	Trasa č.202 Ústí n/O. nem. - Č. Třebová MÚ		
2.1	Délka [m]	-	
2.2	Útlum na vlnové délce 1310 nm [dB]	-	
2.3	Útlum na vlnové délce 1550 nm [dB]	-	

Č.	*Vlastnost*	*Požadovaná hodnota*	*Nabídková hodnota*
	Trasa č.203 Č.Třebová MÚ - Svitavy nem.		
3.1	Délka [m]	-	
3.2	Útlum na vlnové délce 1310 nm [dB]	-	
3.3	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č.301 Žamberk MÚ - Ústí n/O. nem.		
4.1	Délka [m]	-	
4.2	Útlum na vlnové délce 1310 nm [dB]	-	
4.3	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č.302 Žamberk MÚ – Králíky MÚ		
5.1	Délka [m]	-	
5.2	Útlum na vlnové délce 1310 nm [dB]	-	
5.3	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č. 304 Č. Třebová MÚ - Lanškroun MÚ		
6.1	Délka [m]	-	
6.2	Útlum na vlnové délce 1310 nm [dB]	-	
6.3	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č. 401 Svitavy nem. - Mor. Třebová MÚ		
7.1	Délka [m]	-	
7.2	Útlum na vlnové délce 1310 nm [dB]	-	
7.3	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č. 501 Přelouč MÚ – Pardubice KrÚ		
8.1	Délka [m]	-	
8.2	Útlum na vlnové délce 1310 nm [dB]	-	
8.3	Útlum na vlnové délce 1550 nm [dB]	-	
	Trasa č.601 Pardubice KÚ - Holice MÚ		
9.1	Délka [m]	-	
9.2	Útlum na vlnové délce 1310 nm [dB]	-	
9.3	Útlum na vlnové délce 1550 nm [dB]	-	

2.12. SLA – technické šetření stávajícího SLA, navýšení částí ve vysoké dostupnosti

Stávající SLA na dostupnost služby, je v současné době 95 %.

Transportní modul

U uzlů, které budou součástí kruhu(ů) bude požadováno navýšení SLA na dostupnost služby až na 99,5 %. Zadavatel zde očekává maximální dostupnost díky realizaci maximální redundance zhotovitelem v tomto projektu.

U uzlů, které nejsou součásti kruhu a není u nich dokončena redundance v plném rozsahu (tedy stejně jako u uzlů v kruhu(ů)), zůstává požadované SLA na služby přenášené těmito uzly na stávajících 95%.

Management modul

Pokud je daná služba požadována a provozována ve vysoké dostupnosti platí vždy vyšší SLA 99,5%.

Bezpečnostní modul

Platí vyšší SLA. Architektura bezpečnostních služeb je vždy požadována ve vysoké dostupnosti a SLA je počítáno ne na provoz prvku, ale na provoz služby.

Propojovací modul

I zde platí požadavek na vysokou dostupnost a současně na vyšší SLA na službu jako na celek.

O výši SLA jsou obě strany od počátku smluvního vztahu informovány. Měřítkem je míra redundance v kruzích. Zadavatel může povýšit nebo ponížit libovolný uzel na jiné SLA díky technickému upgrade/downgrade. Zhotovitele o tom však musí informovat včetně zdůvodnění změny požadovaného SLA.

V následujících tabulkách jsou zobrazeny požadované parametry SLA pro incidenty A, B, C, D a definice jednotlivé kategorie incidentů.

Tabulka č. 10 − Požadavky na garantované parametry SLA

Kategorie incidentu	Garantovaná doba přijetí a akceptace hlášeného incidentu	Garantovaná doba zahájení prací na řešení incidentu po řádném nahlášení a maximální doba pro pravidelné ohlašování stavu incidentu	Garantovaná doba obnovení služby
A	30 min	2 hod	do 12h
B	30 min	4 hod	Next business day
C	60 min	Next business day	5 pracovních dní
D	60 min	Next business day	Best effort
Konfigurace / změna na požádání zadavatelem	60 min	--	Next business day

Tabulka č. 11 − Kategorie incidentů

Kategorie incidentů
Incident/vada kategorie A
Prvek IT/služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody.

Kategorie incidentů
Incident/vada kategorie B
Prvek IT/služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz.
Incident/vada kategorie C
Ostatní drobné incidenty/vady, které nespadají do kategorií A a/nebo B a které nejsou způsobeny software třetích stran.
Incident/vada kategorie D
Incidenty/vady, které jsou způsobeny software třetích stran.

Tyto parametry jsou výchozími požadavkem zadavatele, zhotovitel může navrhnout parametry úměrně přísnější s ohledem na kvalitu jím realizované sítě.

2.13. Další požadavky na hw v lokalitách

Projektovaný stav (znázorněno zelenou barvou)

Tabulka č. 12 – Lokality, příslušenství projektu

Název ORP	Název úřadu	HW vybavení
Česká Třebová	Městský úřad Česká Třebová	Rack, UPS
Hlinsko	Městský úřad Hlinsko	UPS
Holice	Městský úřad Holice	Rack, UPS
Králíky	Městský úřad Králíky	Rack, UPS
Moravská Třebová	Městský úřad Moravská Třebová	Rack, UPS
Přelouč	Městský úřad Přelouč	UPS
Žamberk	Městský úřad Žamberk	UPS

2.13.1. Rack

Datový rozvaděč 3ks

Č.	*Vlastnost*	*Požadovaná hodnota*	*Nabídková hodnota*
	Fyzické vlastnosti a prostředí	-	
1.1	Kategorie zařízení - Datový stojan 19"	ANO	
1.2	Celková výška	max. 200cm	
1.3	Celková šířka	60cm	
1.4	Celková hloubka	60cm	

Č.	Vlastnost	Požadovaná hodnota	Nabídková hodnota
1.5	Stupeň krytí	IP20	
	Funkčnost		
2.1	Využitelná vnitřní výška	min. 40RU	
2.2	Provozní teplota maximální	min. 400kg	
2.3	Svislé montážní lyžiny stavitelné, rozteč 19"	min. 4	
2.4	Typ	Volně stojící	
2.5	Demontovatelné boky	ANO	
2.6	Dveře perforované v min. 80% plochy	ANO	

2.13.2. UPS

7ks záložních zdrojů napájení

Č.	Vlastnost	Požadovaná hodnota	Nabídková hodnota
	Fyzické vlastnosti a prostředí	-	
1.1	Kategorie zařízení - Záložní zdroj napájení	ANO	
1.2	Formát zařízení - k montáži do stojanu 19"	ANO	
1.3	Výška zařízení	max. 6RU	
1.4	Hloubka zařízení	max. 50cm	
1.5	Provozní teplota minimální	max. 0 st.Celsia	
1.6	Provozní teplota maximální	min. 40 st.Celsia	
1.7	Vstupní napětí	230 VAC	
	Funkčnost	-	
2.1	Výstupní výkon	min. 1500W	
2.2	Výstupní napětí	230 VAC	
2.3	Frekvence výstupního napětí	50 Hz	
2.4	Průběh výstupního napětí	Sinusoida	
2.5	Kapacita zdroje	400 Wh	
2.6	Bezúdržbová integrovaná baterie	ANO	
2.7	Dohled SNMP, IP/Ethernet 10BASE-T	ANO	

3. Školení

Zadavatel požaduje vyškolení administrativního týmu zadavatele ve všech technologiích a administrativních postupech potřebných k provozu a bezpečnosti sítě.

Školení proběhne v místě sídla zadavatele nejdříve v době testovacího provozu, materiály jsou dodány týden před vlastním školením, pokud není níže u jednotlivých školení řečeno jinak.

3.1. Povinné oblasti proškolení pro 2 osoby v oblastech

1. HW, virtualizace, zálohování, DR postupy – 2MD
2. Nastavení sítě, převzetí nových i překonfigurovaných služeb, provoz a zabezpečení, VPN, AAA – 2MD
3. Zabbix – 2 MD
4. Graylog – 1 MD

3.2. Certifikované školení

Zadavatel dále vyžaduje, aby min. 2 správci procházeli na náklady zhotovitele pravidelným školením s certifikovaným lektorem na technologie užité v síti. Školení nemusí být na stejných zařízeních ani na zařízeních stejného výrobce, vyučovací postupy však musí vést ke konfiguracím dle standardů užitých v síti. Časový rozsah každého školení je min. 5MD na osobu a může být složen z více navazujících kurzů. Jazykem školeni je čeština. Školení nemusí být realizováno v sídle zadavatele.

3.2.1. Požadovaný harmonogram:

1. Realizace projektu – 1x školení profesionálního routingu (např. CCNP Routing), 1x MPLS
2. Druhý rok provozu – 1x školení profesionálního routingu (např. CCNP Routing), 1x MPLS
3. Čtvrtý rok provozu – 1x školení profesionálního routingu (např. CCNP Routing), 1x MPLS

Zhotovitel vždy nabídne tři termíny každého školení v průběhu roku pro možnost přihlášení osob zadavatele.

4. Požadavky na dokumentaci

Struktura dokumentace musí současně splňovat také dotační podmínky. Dokumentace budou v českém jazyce, technické výrazy mohou být v jazyce anglickém. Předaná dokumentace je 1x ve standardním editovatelném formátu pro elektronickou formu (např. MS Office – Word, Excel, Visio a Open Office) a 1x v needitovatelném standardním formátu, např. PDF. Tištěná verze je také min. v jedné kopii. Zmenšit rozsah dokumentací může pouze zhotovitel.

Dokumentace zde uvedená je předána v sídle zhotovitele.

4.1. Prováděcí dokumentace

1) Před spuštěním implementace díla předloží uchazeč návrh prováděcí dokumentace ke schválení. Schválení mimo zadavatele provádí i oprávněná osoba ze sídla umístění uzlu sítě. Implementace poté bude v souladu s prováděcí dokumentací.
2) Změna v průběhu implementace je podmíněna schválením zhotovitelem a případně jím určenou další osobou (v případě změny v objektech partnera projektu).
3) Dokument obsahuje všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění do stavu odpovídajícího požadovaným parametrům zadavatele. Dokumentace a popsané aktivity musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:
    a. Detailní schéma fyzického zapojení včetně popisu, úrovní detailu je min. vlnová lamda /transceiver / port aktivního prvku.
    b. Detailní schéma logického schéma včetně popisu, úrovní detailu je vlan / vrf či jiná nejmenší virtuální jednotka.
    c. Detailní popis cílového stavu a funkcionalit jednotlivých částí.
    d. Popis přepracování adresního rozsahu, zapracování veřejných a dodavatelsky neutrálních adres zhotovitele.
    e. Způsob zajištění potřebných dodávek včetně technické podpory
    f. Způsob zajištění projektového řízení na straně uchazeče pro realizaci předmětu plnění
    g. Detailní návrh a popis postupu implementace předmětu plnění
    h. Detailní popis zajištění bezpečnosti informací
    i. Detailní harmonogram projektu včetně uvedení kritických milníků. Minimální kritické milníky pro dokumentaci uzlu Krajský úřad Pk, kde budou i obecné informace pro zadavatele:
        i. Zahájení projektu
        ii. Provedení předimplementační analýzy včetně případné první návštěvy budoucího umístění uzlu.
        iii. Předání prováděcí dokumentace
        iv. Zahájení implementace předmětu plnění
        v. Školení
        vi. Zahájení testovacího (zkušebního) provozu. Testovací provozu bude trvat minimálně 6 týdnů.
        vii. Akceptační testy
        viii. Zahájení plného provozu
        ix. Návrh akceptačních kritérií a akceptačních testů
        x. Detailní popis navrhovaných školení
        xi. Detailní popis údržby systémů
        xii. Detailní struktura dalších dokumentací
        xiii. Čestné prohlášení zhotovitele, že má vyřešeny nebo v řešení majetkoprávní vztahy k pozemkům, přes které povedou optická vlákna.

4.2. Dokumentace skutečného provedení

1) V průběhu implementace provádí zhotovitel aktualizaci prováděcí dokumentace a spuštění ostrého provozu finalizuje dokumentaci odpovídající skutečnému stavu implementace.

Součástí dokumentace je i výpis konfigurací jednotlivých aktivních prvků. V případě, že zařízení neumožňuje zobrazení konfigurace v čitelné podobě a zařízení má webové rozhraní, jsou součástí dokumentace screenshoty všeho nastavení.
2) Součástí předané dokumentace v elektronické podobě budou i zálohy všech aktivních prvků s poslední konfigurací.
3) Dokumentace skutečného provedení je zhotovitelem udržována v aktuálním stavu po dobu platnosti Smlouvy o servisní podpoře. Zálohy jsou i nadále prováděny, výpisy konfigurací jednotlivých aktivních prvků se v dokumentaci nadále neaktualizují.

4.3. Bezpečnostně-provozní dokumentace

1) Dokumentace popisující obecně stav sítě jako celku, následně se věnující bezpečnému provozu každého konkrétního uzlu z pohledu administrátorů daných uzlů.
2) Dokumentace uzlů Krajský úřad a Nemocnice Pardubice je podrobná, zahrnující informace o celé síti a rozšířená pro podrobný provoz a bezpečnou administraci celé sítě, včetně vnějšího perimetru, monitoringu a bezpečnosti.
3) Součástí dokumentace každého uzlu jsou minimálně:
4) Bezpečnostní pravidla z pohledu fyzické i síťové bezpečnosti ve vztahu k použitým aktivním prvkům a dodaným technologiím.
5) Bezpečnostní směrnice s popisem implementovaných a provozovaných bezpečnostních mechanismů a zásadami pro bezpečný provoz sítě

4.4. DR dokumentace

1) Dokumentace popisuje krok po kroku postupy při:
    a. Spuštění systému
    b. Řešení výpadku jedné komponenty. Popsány musí být možná řešení všech možných výpadků a přepnutí do redundantního režimu. Součástí je i popis správné funkce redundantní komponenty pro vizuální kontrolu.
    c. Eskalační mechanismus základního ověření funkčnosti a poté nahlášení závady dle povahy konkrétního uzlu.

4.5. Dokumentace hesel

1) Zadavatel zakazuje jakákoliv hesla v ostatních dokumentacích, umožňuje pouze jednoznačný odkaz do dokumentace hesel.
2) Hesla jsou rozdělena v kapitolách po dokumentacích nebo dle abecedně vzestupně seřazených odkazů, pokud se zhotovitel nedohodne v přípravné fázi projektu se zadavatelem jinak.

4.6. Inventární dokumentace

1) Po realizaci celého projektu je zhotoviteli předán soupis všech zařízení, každé identifikované svým produktovým označením, umístěním, množstvím v daném umístění, sériovým číslem (pokud existuje), zařazením do kategorie (služba, hardware, software, příslušenství k hw, licence k hw, jiné) a cenovým ohodnocením dané položky.

4.7. Dokumentace o licencích

1) Zadavatel obdrží soupis zařízení s připsanými jednotlivými licenčními politikami včetně případných licenčních čísel nebo kódů a jejich platnosti.

4.8. Analýza rizik

1) Zhotovitel na základě analýzy definuje možná rizika provozu Regionální datové sítě v každém uzlu zvlášť a navrhne možná opatření pro jejich snížení. Realizace opatření není součástí projektu.
2) Metodika stanovení rizik musí být standardizovaná a zopakovatelná. Zadavatel doporučuje metodiku vyhlášky č. 82/2018Sb., o kybernetické bezpečnosti.

4.9. Dokumentace měření optických vláken

1) Měření každé trasy přímou a OTDR metodou minimálně na frekvenci 1310nm a 1550nm.

4.10. Dokumentace zaměření vedení optických vláken

1) Součástí dokumentace je min.:
    a. Mapa Pardubického kraje se zakreslenou přesnou topologií optických vláken předmětu plnění.
    b. Schéma kompletní pasivní infrastruktury s označením nových částí
    c. Sada zaměření jednotlivých vedení optických vláken s přesností na 14cm s popisem délky jednotlivých tras, stručný popis uložení, informace o celkovém počtu optických vláken v kabelu a zakončení.
    d. Seznam rizikových úseků a jejich zaměření. Rizikovým úsekem jsou hlavně souběhy (do 50cm) a křížení optických tras, které mají jinak tvořit vyšší dostupnost napojených zařízení
    e. Potvrzení zhotovitele, že jsou vyřešeny majetkoprávní vztahy k pozemkům, kde jsou vedeny optická vlákna sítě zadavatele dodaná v tomto projektu.
    f. Grafické zobrazení komunikační infrastruktury v elektronické podobě v běžně používaném systému GIS – (např. ve formátu dxf, dwg, dxn, shp apod.).

4.11. Materiály k proběhlému školení

1) Materiály ke školení jsou předány do dvou týdnů po provedení školení.

Dokumentace hesel a bezpečnostní dokumentace je na přední straně výrazně označena názvem a textem v červené barvě na kontrastním podkladu:

TLP:RED – Dokument důvěrného charakteru v majetku oddělení informatiky Pardubického kraje. Je zakázáno pořizování kopií nebo zapůjčení třetí osobě bez svolení vedoucího oddělení informatiky Pardubického kraje!