POPIS TECHNICKEHO ŘEŠENÍ

IMPLEMENTACE OPATŘENÍ ÚOOÚ

VERZE 20100525 -3.0

OBSAH

1. OBECNÁ FUNKČNÍ A TECHNICKÁ SPECIFIKACE

Cílem navrženého řešení je splnění nápravných opatření vyplývajících z protokolu inspektora ÚOOÚ sp.zn. INSP2-0277/09-40, viz Protokol_inspektora_ÚOOÚ, rozhodnutí předsedy ÚOOÚ sp.zn. INSP2-0277/09-62, viz Rozhodnutí_předsedy_ÚOOÚ, dále jen („Nápravná opatření ÚOOÚ"). Provedení nápravných opatření vede k fyzickému oddělení HW/SW technologií datového centra Zadavatele tak, aby v systému centrálního úložiště elektronických receptů, viz zákon č. 378/2007 Sb., nebyla zpracovávána ani uchovávána jiná data, než údaje předepsané § 81 zákona č. 378/2007 Sb. a stanovené prováděcími předpisy. Údaje, které budou vyčleněny z centrálního úložiště elektronických receptů, budou shromažďovány a zpracovávány v samostatně konstituovaném, chráněném úložišti pro sběr a zpracování hlášení regulovaných subjektů, viz § 77 odst. 1 písm. f) a § 82 odst. 3 písm. d) zákona č. 378/2007 Sb.
Prostředkem k dosažení cíle je dodávka a implementace HW/SW technologií, provedení rekonfigurace stávajících systémů a úprava software aplikací centrálního úložiště elektronických receptů a úložiště hlášení regulovaných subjektů dle § 77 odst. 1 písm. f) zákona č. 378/2007 Sb. a § 82 odst. 3 písm. d) zákona č. 378/2007 Sb., které zajistí beze zbytku uvedený cíl.

Navržené technologie pro rozšíření hardware a software datového centra jsou vzájemně kompatibilní nejen mezi sebou, ale i se stávající technologií infrastruktury Zadavatele.

Kompatibilita je zachována jak u infrastruktury, tak i po stránce software. Stávající technologií infrastruktury se rozumí, aktivní prvky (switche, routery, firewally), stávající software technologie (serverové operační systémy, virtualizační SW, kryptační SW, sběrnice ESB, aplikační SW pro sběr dat Hlášení výdejů LP, aplikační SW pro Centrální úložiště elektronických receptů) a serverové systémy (HW servery, diskové pole, zálohování).

Dále je zajištěna kompatibilita (managementu, správy, monitoringu, interoperability a používaných protokolů) nabízených a dodávaných prvků se stávajícími používanými prvky.

1.1. ROZŠÍŘENÍ HARDWARE DATOVÉHO CENTRA

Součástí dodávky je oddělení veškerých technologií dosud využívaných společně jak pro elektronické recepty, tak pro systém hlášení. Před oddělením bude provedeno rozšíření HW kapacit v oblasti diskových polí, rozšíření výkonu virtuální infrastruktury dodávkou dalších serverů a přepínačů, dále pak systém pro zakončování SSL tunelů, systém pro loadbalancing na GTW systémy a systém zajištění vysoké dostupnosti email komunikace, tak aby byla zajištěna dále specifikovaná provozní i špičková kapacita systému hlášení dle § 77 odst. 1 písm. f) a § 82 odst. 3 písm. d) zákona č. 378/2007 Sb., vyhodnocování spotřeb léčivých přípravků dle § 13 odst. 3 písm. b) zákona č. 378/2007 Sb., shromažďování údajů o používání léčivých přípravků dle § 13 odst. 3 písm. j) zákona č. 378/2007 Sb., zveřejňování informací dle § 99 odst. 1 písm. d) a odst. 2 písm. e) a odst. 5 zákona č. 378/2007 Sb., a přijímání opatření dle § 13 odst. 2 písm. c) a písm. g) zákona č. 378/2007 Sb.

1.2. ROZŠÍŘENÍ SOFTWARE DATOVÉHO CENTRA

Součástí dodávky je oddělení veškerých softwarových prostředků, které byly dosud využívaných společně jak pro zpracování a ukládání elektronických receptů, tak pro systém hlášení. Před oddělením proběhne zřízení 2 samostatných virtuálních datových center.
Součástí dodávky je i software pro podrobné zkoumání schémat a trendů výkonu diskových polí, a to jak historicky, tak i v reálném čase. Tento software poskytne výkonný nástroj pro plánování hardwarové kapacity a také pro rozumné vyrovnání zatížení.

1.3. IMPLEMENTACE PODPŮRNÝCH SYSTÉMŮ A VÝVOJ SOFTWARE

S ohledem na znalosti provozu centrálního úložiště elektronických receptů a v souvislosti s očekávaným markantním zvýšením nároků kladených na síťovou infrastrukturu spojených s implementací nápravných opatření ÚOOÚ navrhujeme nasazení, se stávající infrastrukturou kompatibilní, ale na stávající infrastruktuře nezávislý systém zajišťující monitoring datových toků. Systému bude zajišťovat monitorování provozu, vytváření podrobných statistik o síťovém provozu v rámci komunikační infrastruktury a odhalování případného nestandardního chování systému.

Dále bude provedena analýza aplikačního SW pro systém hlášení regulovaných subjektů dle § 77 odst. 1 písm. f) zákona č. 378/2007 Sb. a § 82 odst. 3 písm. d) zákona č. 378/2007 Sb, analýza aplikačního SW pro Centrální úložiště elektronických receptů, analýza datových komunikačních rozhraní a úložiště dat, návrh úprav SW, návrh datových komunikačních rozhraní a úložiště dat, vývoj a nasazení změn aplikačního SW, včetně provedené rekonfigurace sběrnice služeb na základě požadovaných nápravných opatření ÚOOÚ a požadovaných výkonnostních parametrů. Navržené a provedené změny budou zajišťovat oddělené ukládání pseudonymizovaných identifikátorů pacienta, pokud lze na základě zákonného zmocnění zpracovávat a shromažďovat citlivé údaje pacienta. Dále bude zajištěno blokování vazby mezi odděleným pseudonymizovaným identifikátorem pacienta a záznamy o předepsaném nebo vydaném léčivém přípravku do doby udělení výslovného souhlasu pacienta s vytvořením lékového záznamu pacienta. Navržené a provedené změny budou zajišťovat správu autentizace a autorizace veškerých přístupů k oběma odděleným systémům dle nápravných opatření ÚOOÚ.

Účelem použití pseudonimizovaného identifikátoru pacienta bude možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. Do doby udělení výslovného souhlasu pacienta s vytvořením lékového záznamu pacienta nebude vazba na pseudonymizovaný identifikátor použita. Pokud by byl použit anonymizovaný identifikátor, nebylo by možné ani s výslovným souhlasem pacienta jemu jeho data zpřístupnit.

2. ROZŠÍŘENÍ HARDWARE DATOVÉHO CENTRA

2.1. SYSTÉM ZAKONČENÍ SSL SPOJENÍ SBĚRU DAT

2.1.1. POPIS NAVRHOVANÉ TECHNOLOGIE

Systém zakončení SSL spojení sběru dat navrhujeme realizovat dvojicí zařízení společnosti Cisco Systems, konkrétně Zařízeními Cisco Catalyst 6500 osazenými servisními moduly ACE. Pro tento konkrétní případ navrhujeme použití zařízení Cisco Catalyst 6504E osazeného supervizorem WS-SUP720-3B a servisním modulem Cisco ACE s následujícími licencemi: ACE-04G-LIC a ACE-SSL-15K-K9.

Takto sestavený systém splňuje následující požadavky:

- podpora vysoké dostupnosti
- redundantní zdroje napájení
- počet slotů v chassis minimálně 4
- preferovaná crossbar architektura, výkon řídícího modulu min. 400Mpps pro IPv4 routing
- podpora karty s funkcí IPSec VPN koncentrátoru
- podpora karty s funkcí IPS systému
- podpora Weighted Random Early Detection (WRED)
- podpora Weighted Fair Queuing (WFQ)

Dále pak budou tato zařízení schopna zabezpečovat komunikaci mezi centrem a vzdálenou lokalitou prostřednictvím protokolu SSL s následujícími parametry:

- Podpora SSL Version 3.0, Transport Layer Security (TLS) Version 1.0.
- Hardwarová akcelerace následujících šifrovacích algoritmů: rsa-with-rc4-128-md5, rsa-with-aes-256-cbc-sha, rsa-with-rc4-128-sha, rsa-with-aes-128-cbc-sha, rsa-export-with-des40-cbc-sha, rsa-export1024-with-rc4-56-sha, rsa-with-des-cbc-sha, sa-export1024-with-des-cbc-sha, rsa-with-3des-ede-cbc-sha, rsa-export1024-with-rc4-56-md5 a rsa-export-with-rc4-40-md5.
- Počet SSL tunelů navázaných za 1 sekundu: 15 000 SSL tunelů za 1 sekundu.
- Počet současně aktivních tunelů: 200 000 aktivních tunelů.
- Minimální propustnost při SSL šifrování: 3 Gbps.
- Podpora redundance.
- Možnost integrace se systémem PKI (hierarchie certifikačních autorit MZ) s podporou 1024-bit, 1536-bit, a 2048-bit klíčů.
- Možnost autentizace uživatele prostřednictvím certifikátu X.509 v3.
- Schopnost číst (stahovat) CRL (Certificate Revocation List) pomocí protokolů HTTP a LDAP.
- Schopnost číst CRL na základě cesty uvedené v certifikátu, nebo aby bylo možné nadefinovat min. 4 cesty k CRL manuálně.

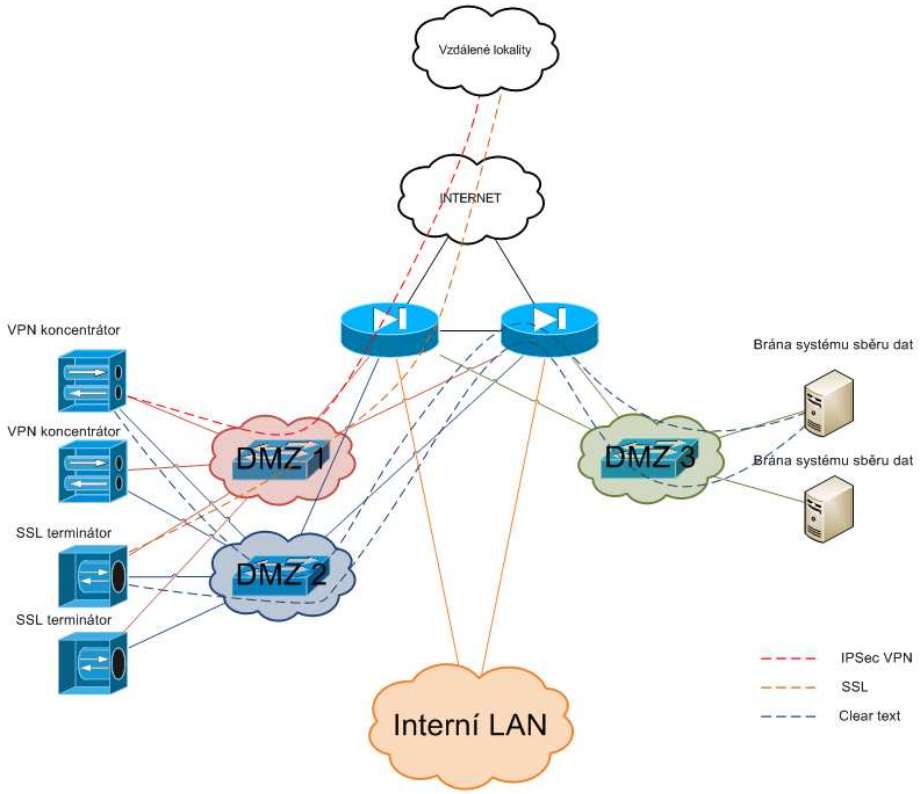
Detailní soupis a počet navrhovaných komponent:

Číslo	Obchodní název	MJ	Počet
WS-C6504E-ACE20-K9	ACE20 4G 6504E Bundle	ks	2

S733ISK9L-12233SXI	Cisco CAT6000-SUP720 IOS IP SERVICES SSH LAN ONLY	ks	2
CF-ADAPTER-SP	SP adapter with compact flash for SUP720	ks	2
ACE-SSL-15K-K9	Application Control Engine SSL License, 15000 TPS	ks	2
CAB-AC-2500W-EU	Power Cord, 250Vac 16A, Europe	ks	2
WS-SUP720-3B	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric MSFC3 PFC3B	ks	2
MEM-C6K-CPTFL512M	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	ks	2
BF-S720-64MB-RP	Bootflash for SUP720-64MB-RP	ks	2
MEM-S2-512MB	Catalyst 6500 512MB DRAM on the Supervisor (SUP2 or SUP720)	ks	2
MEM-MSFC2-512MB	Catalyst 6500 512MB DRAM on the MSFC2 or SUP720 MSFC3	ks	2
ACE20-MOD-K9	Application Control Engine 20 Hardware	ks	2
SC6K-A21-ACE	ACE A2(1) Software Release	ks	2
ACE-04G-LIC	Application Control Engine (ACE) 4Gbps License	ks	2
FAN-MOD-4HS	High-Speed Fan Module for 7604/6504-E	ks	2
PWR-2700-AC/4	2700W AC Power Supply for Cisco 7604/6504-E	ks	2
PWR-2700-AC/4	2700W AC Power Supply for Cisco 7604/6504-E	ks	2
GLC-T-OEM	1000BASE-T SFP-OEM	ks	2

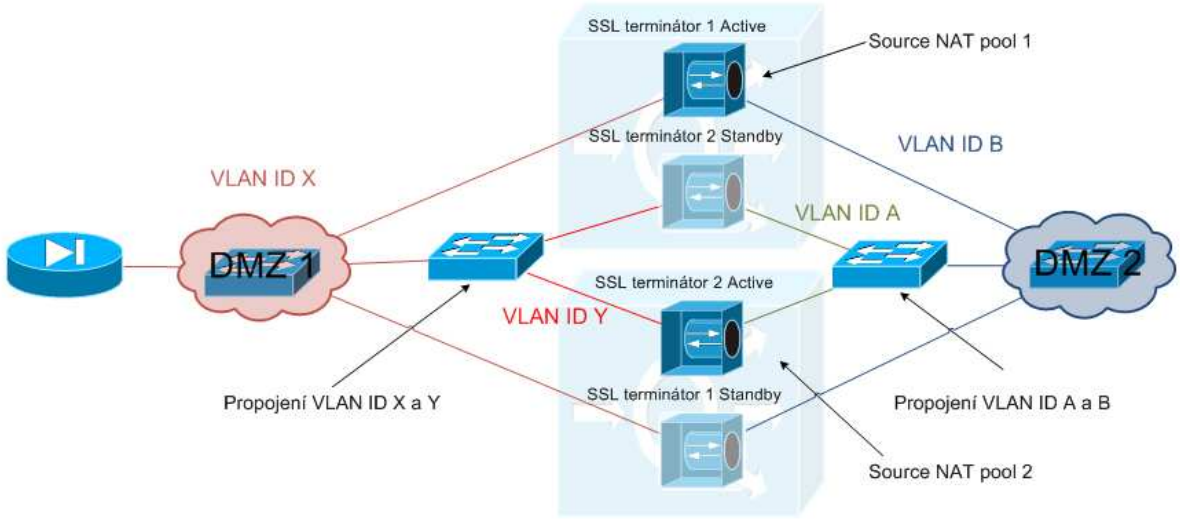
2.1.2. POPIS TECHNICKÉHO ŘEŠENÍ

Zakončování SSL tunelů navrhujeme řešit analogicky ke stávajícímu systému připojení pomocí IPSec VPN. Externí rozhraní ACE modulů sloužící pro zakončování SSL tunelů navrhujeme umístit do stejné DMZ sítě, kde se nyní nacházejí externí rozhraní stávajících VPN koncentrátorů a analogicky navrhujeme postupovat i s „interními“ rozhraními těchto modulů. Aby bylo možné zajistit správný průchod dešifrované komunikace přes firewall do DMZ, kde jsou umístěny brány systému sběru dat a zpět na ACE moduly, bude na ACE modulu prováděn překlad zdrojových adres koncových klientů na zvolené pooly IP adres, který bude na firewallu směrován na interní rozhraní modulů ACE.
Následující obrázek znázorňuje návrh topologie řešení zakončování IPSec a SSL tunelů:



Toto řešení bylo zvoleno z důvodu snadné budoucí rozšiřitelnosti a škálovatelnosti. Bez větších problémů bude možné SSL terminátorům předřadit loadbalancer a téměř libovolně zvýšit kapacitu a výkonnost celého řešení.
Aby bylo možné dosáhnout maximální možný výkon při zakončování SSL tunelů se současným ověřováním připojovaných klientů pomocí certifikátů, navrhujeme publikovat 2 veřejné IP adresy sloužící pro terminaci SSL tunelů. Aplikační logika v koncových stanicích, či jiný mechanismus (nad rámec této nabídky) rozhodne, na kterou IP adresu se koncový uživatel bude připojovat. Je nutné pouze zajistit, aby se koncový systém snažil vždy připojit na „živou“ IP v případě výpadku některého z prvků systému.
Pro dosažení maximálního využití systémových zdrojů ACE modulů navrhujeme na dodávaném zařízení vytvořit dva virtuální kontexty, kdy na každém fyzickém modulu bude aktivní jeden kontext a na druhém druhý. Na obou kontextech bude aktivní jiná VIP adresa sloužící pro zakončování SSL tunelů. Tyto VIP adresy, stejně jako IP adresy sloužící pro zajištění funkce obou kontextů budou ze stejného rozsahu. Aby bylo možné dosáhnout této logické konfigurace, provedeme virtualizaci mac adres na jednom z kontextů a bude nutné rovněž na příslušných switchích v DMZ propojení (probridgeování) 2 VLAN mezi sebou.

Znázornění výsledné logické konfigurace ACE modulů a dalších systémů:



Díky této konfiguraci bude možné lépe využít systémových zdrojů ACE modulů a bude rovněž možné bez odstávky systému případně nasadit loadbalancing příchozích SSL tunelů mezi více ACE modulů. Při tomto systému zapojení využijeme celkem 8 IP adres z DMZ pro externí rozhraní ACE modulů a 8 IP adres z DMZ pro interní rozhraní ACE modulů.
ACE modul dokáže ověřovat připojující se uživatele pomocí certifikátů X.509 v3. Tyto uživatele je možné ověřovat na základě platnosti CRL vystaveného definovanou certifikační autoritou. Na ACE modul je možné nadefinovat ověřování uživatelů z až 4 různých certifikačních autorit současně.
Navrhujeme napojení tohoto systému na PKI hierarchii certifikačních autorit Ministerstva zdravotnictví České Republiky.

2.2. ROZKLÁDÁNÍ ZÁTĚŽE DATOVÝCH TOKŮ NA GTW SYSTÉMY

Vzhledem k tomu, že poptávaný systém má být v budoucnu rozšiřitelný z loadbalancingu datového provozu na GTW systémy i na ostatní systémy komunikační infrastruktury SÚKL (bez ohledu na to, zda se nacházejí v externích, nebo interních DMZ), v navrhovaném a popisovaném řešení je již počítáno s tím, že bude sloužit k loadbalancingu datových toků na různé externí i interní systémy SÚKL. Bezpečné začlenění loadbalancingu do jednotlivých segmentů datové sítě bude řešeno pomocí virtualizace dodaného zařízení.

2.2.1. POPIS NAVRHOVANÉ TECHNOLOGIE

Systém rozkládání zátěže datových toků na GTW systémy navrhujeme řešit dvojicí modulů Cisco ACE vložených do stávajících centrálních prvků Cisco Catalyst 6500. Toto řešení navrhuje s ohledem na úsporu finančních nákladů a s ohledem na požadavek nasazení loadbalancingu na případné další

systémy SÚKL. ACE moduly navrhujeme dodat s následujícími licencemi: ACE-08G-LIC a ACE-VIRT-020.

Takto sestavený systém bude disponovat následujícími parametry:

- Propustnost zařízení v době dodání min 8 Gbps (možnost zvýšit v budoucnu na min 15 Gbps pouze vložením příslušné licence)
- Podpora virtualizace - v době dodávky bude možné vytvořit 20 virtuálních zařízení – přidáním licence je možné rozšířit na 250 virtuálních zařízení
- Podpora vysoké dostupnosti mezi různými fyzickými zařízeními a rovněž mezi jednotlivými virtuálními zařízeními
- Schopnost konfigurovat rozdělení zdrojů mezi jednotlivé virtuální zařízení. Možnost konfigurace přidělování zdrojů pro následující záležitosti: paměť pro access-listy, buffery pro syslog hlášky a TCP out-of-order (OOO) segmenty, dále pro množství současných spojení, proxy spojení, paměť pro regulární výrazy (regexp memory) a paměť pro statické nebo dynamické NAT překlady (Xlates)
- Schopnost udržet 4 000 000 současných spojení
- Podpora pro 16 000 serverů
- Schopnost modifikovat, vkládat, nebo mazat HTTP hlavičky v obou, jak v klientských požadavcích, tak i v odpovědích serverů
- Možnost nasazení jak v routed, tak i v transparentním režimu
- Podpora následujících pravidel pro loadbalancing: adaptive response, least loaded, least bandwidth, least connections, round-robin, hash address, hash cookie, hash header a hash URL
- Podpora následujících protokolů pro detekování „zdraví“ serverů: ICMP, TCP, UDP, ECHO {tcp | udp}, Finger, HTTP, HTTPS, FTP, Telnet, DNS, Simple Mail Transfer Protocol (SMTP), Internet Mail Access Protocol (IMAP), Post Office Protocol (POP), RADIUS, Keep-alive Appliance Protocol (KAL-AP), RTSP, SIP, HTTP parsování návratového kódu a Simple Network Management Protocol (SNMP)
- Schopnost udržet 16 000 instancí pro 4 000 definovaných detektorů
- Podpora pro TCP off-loading
- Podpora inspekce HTTP: http header, URL a HTTP payload
- Možnost definovat přístupová pravidla pro provoz mezi jednotlivými porty
- Schopnost sledovat stav TCP spojení, validace TCP hlavičky, velikosti TCP okénka a randomizace sekvenčního čísla TCP spojení
- Ochrana před útoky typu distributed DoS (DDoS), schopnost omezovat rychlost provozu per server
- Integrovaná hardwarově akcelerovaná inspekce a filtrování protokolů HTTP, RTSP, DNS, FTP, ICMP, SIP a LDAP
- Možnost vytvoření několika úrovní uživatelských a administrativních účtů pro kontrolování a spravování různých definovaných částí systému, v návaznosti na stávající server Cisco ACS podporující protokoly TACACS+ a RADIUS

Dále bude na takto sestaveném systému dosáhnout následujících funkcionalit:

- Zajištění loadbalancingu příchozích datových toků rovnoměrně, nebo na základě definovatelných parametrů mezi v současné době dva (v budoucnu více) systémy sloužící ke sběru dat.
- Možnost nasadit toto zařízení pro loadbalancing na systémy v různých částech síťové infrastruktury.
- Virtualizovatelnost.

- Bude možné přesně vyhradit objem zdrojů, které může využít z celkových zdrojů systému.
- Fyzické zařízení bude umožňovat vytvoření dostatečného počtu virtuálních zařízení, aby bylo schopno pokrýt, jak současné, tak i možné budoucí nároky kladené na systém.
- Virtuální zařízení je možné vkládat do cesty provozu, jak v transparentním, tak i v tzv. routed módu.
- Zařízení je schopno kontrolovat „zdraví“ různých systémů v infrastruktuře SÚKL a na základě těchto informací efektivně rozdělovat zátěž mezi jednotlivé systémy.
- Zařízení je integrovatelné se stávajícími systémy systému sběru dat a stávající komunikační infrastrukturou.

Detailní soupis a počet navrhovaných komponent:

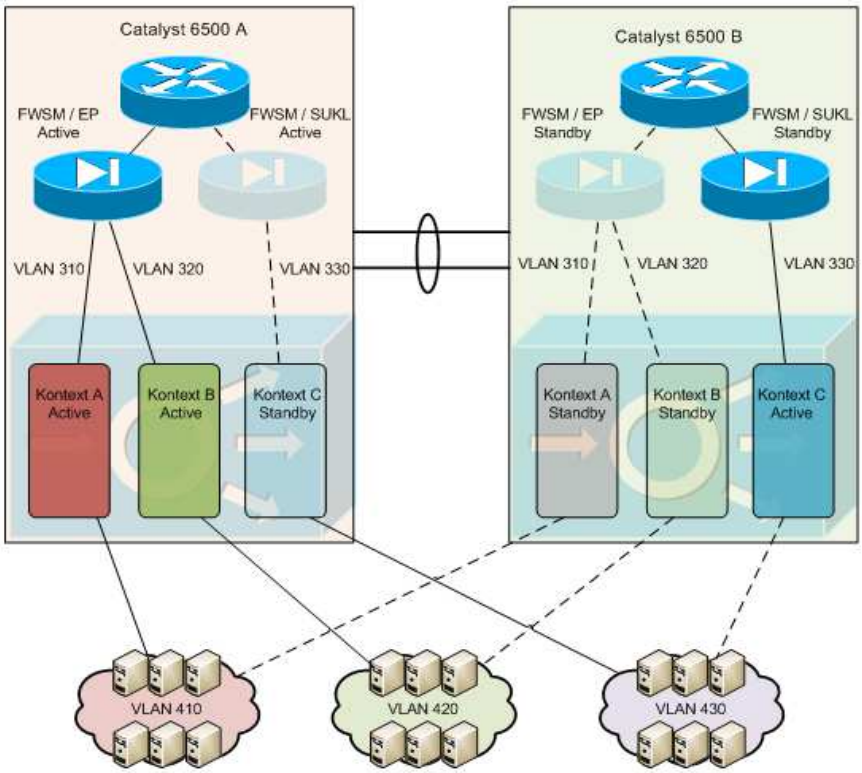
Pol.	Číslo	Obchodní název	MJ	Počet
1.	ACE20-MOD-K9=	Application Control Engine 20 Hardware	ks	2
2.	SC6K-A21-ACE	ACE A2(1) Software Release	ks	2
3.	ACE-08G-LIC	Application Control Engine (ACE) 8Gbps License	ks	2
4.	ACE-VIRT-020	Application Control Engine Virtualization 20 Contexts	ks	2

2.2.2. POPIS TECHNICKÉHO ŘEŠENÍ

Nabízené servisní moduly ACE navrhujeme provozovat v režimu vysoké dostupnosti z důvodu dosažení maximální spolehlivosti a dostupnosti externích i interních systémů SÚKL. Zařízení jsou navrhována s možností vytvořit až 20 virtuálních kontextů, přičemž je možné jednotlivé kontexty provozovat buď v tzv. routovaném, nebo bridge módu. Při nasazení do infrastruktury SÚKL navrhujeme nasazení některých kontextů v routovaném a jiných kontextů v bridgeovaném módu.

Vnitřní infrastruktura datové sítě SÚKL je tvořena dvojicí přepínačů Cisco Catalyst 6500, které jsou mimo jiné osazeny firewallovými moduly FWSM. Tyto moduly jsou provozovány v tzv. routovaném módu a v režimu vysoké dostupnosti, konkrétně v režimu Active/Active, což znamená, že při normálním běhu systému je na každém z fyzických modulů aktivní jeden virtuální kontext. Je vytvořen jeden kontext pro produkční systémy SÚKL a jeden kontext pro systémy EP. Loadbalancing provozu na vnitřní systémy navrhujeme řešit pomocí virtualizace dodávaných modulů při použití bridgeované varianty. Tento způsob navrhujeme z důvodu větší jednoduchosti a transparentnosti nasazení do infrastruktury SÚKL. Bridgeovaná varianta zapojení je v podstatě ze síťového hlediska zcela transparentní a vložení loadbalanceru do cesty provozu bude díky použití technologie VmWare velmi jednoduché (servery se v konzole VmWare pouze softwarově přesunou do jiné VLAN sítě a IP adresa serveru zůstane ze stejného subnetu, jako ta původní). Tato varianta je výhodná rovněž z důvodu, že nebude nutná žádná změna směrování v komunikační infrastruktuře.

Redundance bridge loadbalancing kontextů bude řešena tak, aby příslušné kontexty byly aktivní vždy na modulu v zařízení, kde je aktivní gateway pro loadbalancovaný systém. Gateway systémů je aktivní v závislosti na tom, jedná-li se o systém produkční, nebo EP. Navrhované blokové schéma zapojení a konfigurace pro loadbalancing vnitřních systémů je na obrázku:

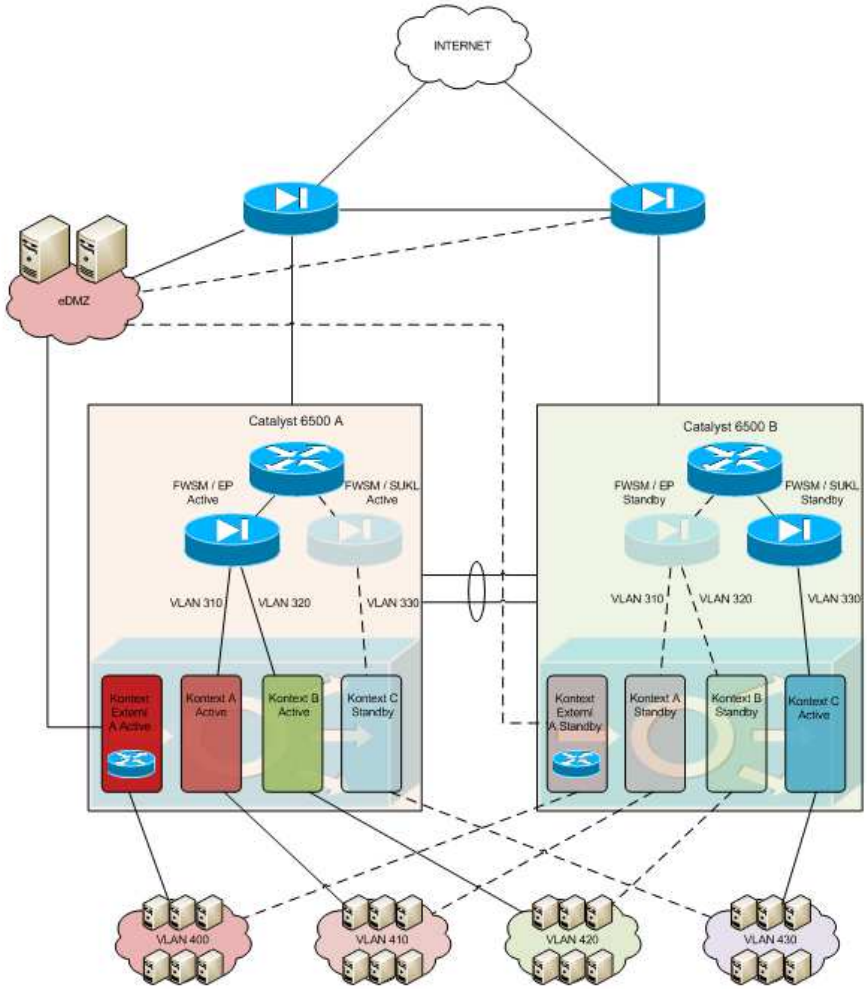


Bridgeovaná varianta nasazení má některá omezení, ke kterým je nutné přihlédnout a díky nimž není vhodná pro nasazení i pro loadbalancing externích systému SÚKL. Při použití bridgeovaného režimu pro loadbalancing externích systémů bychom brzy narazili na nedostatek volných IP adres v externích DMZ sítích. IP rozsahy vyčleněné pro externí DMZ zóny jsou značně omezeny a tak bychom v tomto případě na rozdíl od DMZ interních mohli dojít do stavu, kdy nebude možné vzniklý systém dále rozvíjet a škálovat.

Pro loadbalancing externích systémů (systémy GTW) navrhujeme používat kontextů ACE modulů v routovacím režimu. Díky tomuto nasazení zde předejdeme problému s možným vyčerpáním volných IP adres, protože reálné IP adresy serverů jsou „schované“ za NATem. Virtuální kontexty sloužící pro loadbalancing externích i interních systémů produkčního prostředí SÚKL budou aktivní na jednom fyzickém ACE modulu a analogicky kontexty sloužící pro loadbalancing externích i interních systémů spojených s EP na modulu druhém. Tuto variantu navrhujeme, aby nemohlo dojít k vzájemnému ovlivnění funkčnosti systémů EP a produkčních systémů SÚKL. Vzhledem k tomu, že propustnost, FWSM modulu je 5,5 Gbps a kapacita hlavní linky, potažmo teoretická rychlost přístupu do eDMZ je 1Gbps, dohromady tedy 6,5 Gbps, nebude ani v tomto nasazení při teoretickém plném zatížení systému ACE modul úzkým hrdlem v komunikační infrastruktuře, jelikož dodávaná licence umožňuje propustnost a ž 8Gbps na modul. Při variantě nasazení, kterou navrhujeme, tedy Active/Active bude teoreticky možné využít kapacit obou modulů.

Díky vlastnostem virtuálních kontextů a konfiguraci použité pro loadbalancing externích systémů SÚKL bude dosaženo bezpečného oddělení jednotlivých DMZ sítí, ač budou procházet jedním fyzickým zařízením.

Blokové schéma zapojení a konfigurace:



Příklad řešení loadbalancingu provozu na externí GTW WS a JMS systémy:

Externí stávající komunikační infrastruktura pro sběr dat je tvořena dvěma dvojicemi externích serverů. Tyto servery plní funkce komunikačních bran, přičemž servery ve dvojici gtw-ws01 a gtw-ws02 a dvojici gtw-jms01 a gtw-jms02 jsou redundantní. Vzhledem k tomu, že všechny 4 IP adresy těchto bran jsou již tzv. „natvrdo“ nakonfigurovány v cca. 2600 systémech třetích stran, je nutné, aby se nemuselo nastavení zařízení třetích stran měnit. Navrhujeme proto nasazení loadbalancingu těchto systémů realizovat následovně:

Použijeme jeden kontext dodávaného zařízení ACE v routovaném režimu (z důvodů popsaných výše v textu). V tomto kontextu vytvoříme 2 serverové farmy, kdy každou budou tvořit nově vytvořené VmWare klony původního systému, pouze s novou IP adresací. První serverová farma bude pro systémy WS a druhá pro systémy JMS. Dále pak vytvoříme 4 virtuální VIP adresy, které budou odpovídat současným IP adresám reálných serverů. Provoz směřující na první 2 VIP adresy (současné IP adresy systémů gtw-ws01 a gtw-ws02) budou loadbalancovány mezi servery v serverové farmě WS a druhé dvě VIP IP adresy analogicky mezi servery v serverové farmě JMS. Loadbalancing bude prováděn pomocí algoritmu vyhodnocujícího dobu vyřizování požadavků na jednotlivých koncových serverech. Na server, který bude zpracovávat požadavky nejrychleji, bude směrováno percentuálně největší množství požadavků.

Loadbalancing bude prováděn s ohledem na vytížení a „zdraví“ serverů v jednotlivých serverových farmách. „Zdraví“ těchto serverů bude monitorováno pomocí kontroly sestavení TCP spojení na port příslušné aplikace a na základě návratové komunikace ze systému vyhodnotí, zda je server schopen zpracovávat data, či nikoliv.

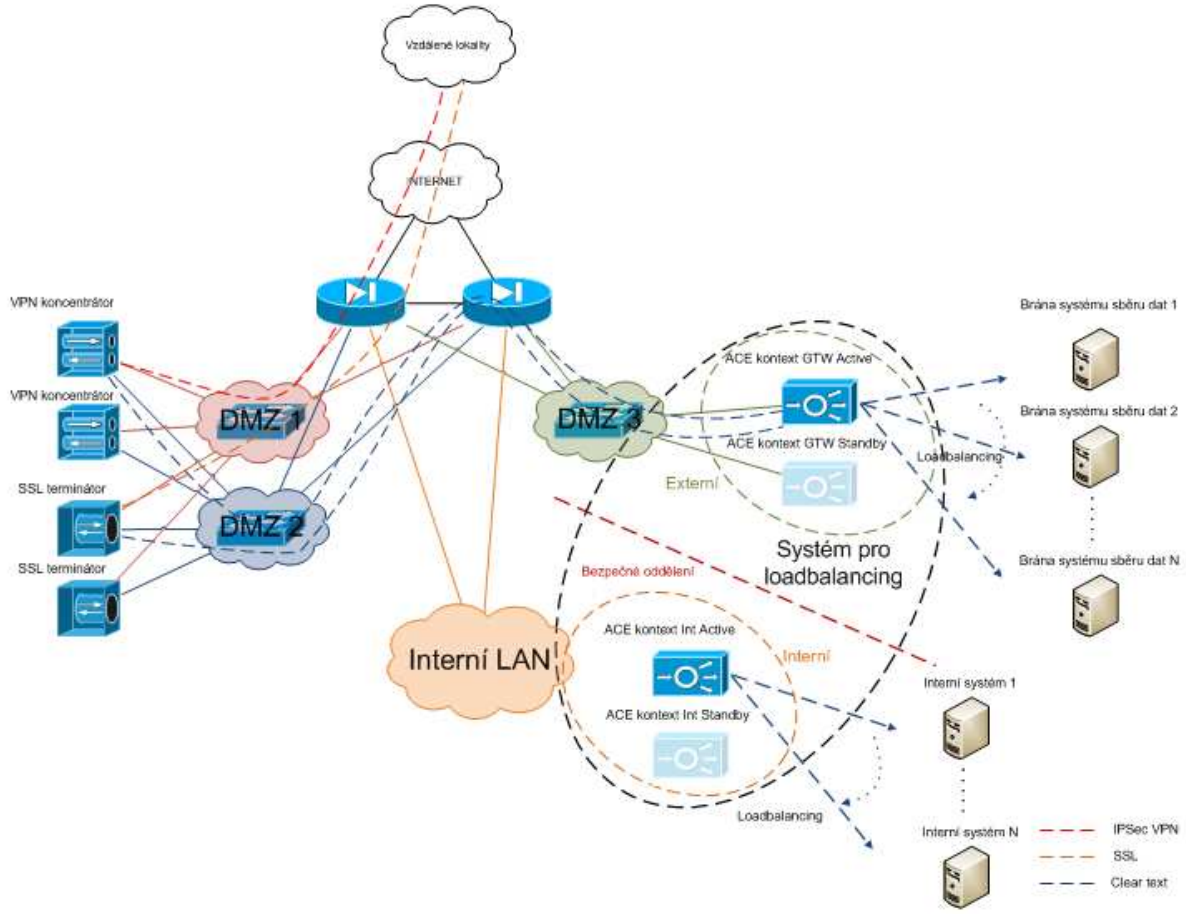
Příklad řešení loadbalancingu LDAP požadavků přicházejících na OID systémy SÚKL:

OID systémy SÚKL jsou umístěny v interních DMZ zónách za FWSM. Na těchto systémech jsou uloženy informace o identitě uživatelů. Na OID systémech pro EP jsou uloženy autentizační informace externích subjektů, které mohou přistupovat k síťovým zdrojům SÚKL. S narůstajícím počtem připojovaných subjektů rostou nároky na výkon OID serverů pro ověřování připojovaných subjektů.

Loadbalancing navrhujeme realizovat jedním virtuálním kontextem dodávaného zařízení Cisco ACE nasazeném v tzv. bridgeovaném (transparentním) režimu. Tento virtuální kontext bude vložen mezi OID servery a FWSM. Bude vytvořena jedna virtuální VIP adresa, na kterou budou směrovány veškeré autentizační toky přidružených systémů. Tyto toky budou potom transparentně loadbalancovány na reálné OID servery v závislosti na vytížení a „zdraví“ jednotlivých OID systémů. „Zdraví“ jednotlivých OID systémů se bude ověřovat dotazem z ACE na koncový systém pomocí protokolu LDAP.

Obdobně může být loadbalancing nasazen na libovolný počet systémů SÚKL. Omezující je v tomto případě pouze počet virtuálních kontextů, které lze vytvořit. Požadovaná licence umožňuje vytvořit maximálně 20 kontextů, ale zakoupením příslušné licence je tento počet možné zvýšit až na 250.

Na následujícím obrázku je schematické znázornění řešení výsledného systému loadbalancingu:



2.3. ROZŠÍŘENÍ CENTRÁLNÍCH PRVKŮ

Nabízíme rozšíření stávajících aktivních prvků Cisco Catalyst 6500 o 2 druhy modulů. První typ modulů umožní připojování aktivních prvků a serverů rychlostí 10 Gbps. Druhý typ modulů umožní připojování aktivních prvků a serverů rychlostí 10/100/1000 Mbps. Součástí je i instalace a konfigurace zařízení do stávající infrastruktury SÚKL a zajištění servisních služeb na dodané řešení.

Ve stávajících chassis WS-6509E je v každém 5 volných pozic pro vložení modulů (po instalaci loadbalanceru už pouze 4, což je nicméně stále dostatečný počet pro případný další rozvoj včetně instalace modulů poptávaných v tomto bodě.).

2.3.1. MODUL PRO PŘIPOJOVÁNÍ RYCHLOSTÍ 10GBPS

V tomto bodě nabízíme:

Dodávka a instalace 2 ks modulů do stávajících aktivních prvků CISCO Catalyst 6500.

- WS-X6716-10G-3C= - Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3C (req X2)

Každý modul bude v době dodávky osazen 6ti ks X2 modulů:

- X2-10GB-SR - 10GBASE-SR X2 Module

Budou dodány originál moduly výrobce.

Pol.	Číslo	Obchodní název	MJ	Počet
1.	WS-X6716-10G-3C=	Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3C (req X2)	ks	2
2.	X2-10GB-SR	10GBASE-SR X2 Module	ks	12

2.3.2. MODUL PRO PŘIPOJOVÁNÍ RYCHLOSTÍ 1GBPS

V tomto bodě nabízíme:

Dodávka a instalace 2 ks modulů do stávajících aktivních prvků CISCO Catalyst 6500.

- WS-X6748-GE-TX= - Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45

Pol.	Číslo	Obchodní název	MJ	Počet
1.	WS-X6748-GE-TX=	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	ks	2

2.4. ROZŠÍŘENÍ STÁVAJÍCÍCH BLADE SERVERŮ

Součástí nabídky je dodávka a instalace 2 ks blade serveru DELL PE M710 v požadované konfiguraci, včetně připojení do stávajícího blade chasi DELL PE M1000e. Součástí nabídky jsou i licence nutné k připojení nového serveru ke stávajícím diskovým polím.

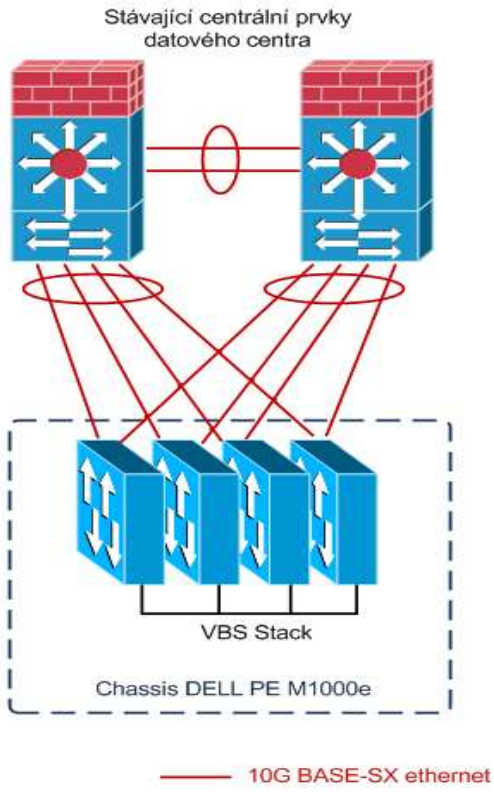
2ks Blade Server M710 v konfiguraci:

- Procesory: 2x Intel Xeon X5570 (2.93GHz, 8M Cache, 6.40 GT/s QPI, Turbo,HT), 1333MHz
- Paměť: 144GB (18x8GB Dual Rank RDIMMs) 800MHz, using 1066MHz DIMMs
- Disky: 2x 73GB SAS (15,000rpm) 2.5 inch Hard Drive Hot Plug
- Disky RAID1
- External 8X DVD-ROM USB
- Čtyři vestavěné síťové GbE Porty
- Přídavná síťová karta: Dual Port GbE I/O Card Redundant (4LAN porty)
- TCP/IP Offload Engine (4P TOE) iSCSI Key For Fabric A
- 3Yr Support for IT and 4hr Mission Critical
- Plná blade výška
- 2x 8Gbps Fibre Channel I/O Card (2x 8Gbps Fibre Channel port)

2.4.1. ETHERNET PŘEPÍNAČ DO STÁVAJÍCÍHO BLADE CHASSIS DELL

Jako ethernet přepínače do stávajícího chassis DELL navrhujeme dodání a instalaci 4 kusů přepínačů společnosti Cisco - Cisco 3130X 10Gb Stackable Switch (NFI) 16 Port určených pro chassis DELL PE M1000e. Každý v době dodání osazený 2 moduly X2-10GB-SR.

Z těchto dodávaných přepínačů navrhujeme vytvořit stoh pomocí technologie VBS. Takto vytvořený stoh se bude potom spravovat jako jeden celek a umožní redundantní připojení do stávající komunikační infrastruktury SÚKL za využití technologie etherchannel.



Tyto přepínače splňují následující vlastnosti:

Obecné vlastnosti:

- L2 / L3 přepínač s podporou IPv4 a IPv6
- IEEE 802.1D (spanning tree)
- IEEE 802.1Q (trunking)
- IEEE 802.1s (MSTP)
- IEEE 802.1w (RSTP)
- IEEE 802.3ad
- IEEE 802.1s
- IEEE 802.1x
- IEEE 802.3x full duplex na 10BASE-T, 100BASE-TX a 1000BASE-T portech
- IEEE 802.3z 1000BASE-X
- 1000BASE-SX
- 1000BASE-LX/LH
- 10GBASE-SR
- 10GBASE-LRM
- 10GBASE-CX4
- IEEE 802.1p CoS Prioritization
- IEEE 802.1Q VLAN
- podpora per-VLAN RSTP
- podpora velkých rámců (min. MTU velikosti 8900 bytů) na GE portech
- sdružování GB rozhraní do svazků min. 8Gbps, vyvažování přes porty ve svazku
- podpora NTP protokolu
- podpora DHCP Relay funkce
- Požadovaný počet portů: 20 10/100/1000BASE-T (16 interních, 4 externí)
- 2 X2 10 Gigabit porty (v době dodávky každý modul osazen 2 ks X2 10GBASE-SR modulů)
- 2 high-speed stack connectory (požadována možnost vytvořit Virtual Blade Switch)
- Požadovaný celkový přepínací výkon 128-Gbps
- Požadovaná přenosová rychlost (64-bytové pakety) 59,2 mpps
- Podpora velkých rámců (min. 9018 bytů)
- Podpora statického směrování
- Podpora směrovacího protokolu RIPv1 a RIPv2
- Požadována podpora pro minimálně 128 spanning-tree instancí
- Podpora pro min. 4000 VLAN IDs
- Možnost konfigurace VLAN pomocí protokolu VTP, který je používán v současné síťové infrastruktuře.
- Možnost spravovat zařízení pomocí protokolů SNMPv1, SNMPv2c, and SNMPv3
- Možnost sdružovat více přepínačů do jednoho logického celku a tento spravovat jako jeden
- Podpora VPN routing and forwarding (VRF) lite

Zabezpečení:

- podpora SSH v1, 2 protokolu pro vzdálenou správu přepínače
- podpora protokolu Kerberos
- podpora RADIUS protokolu pro AAA služby při přístupu k přepínačům
- podpora 802.1x protokolu s centralizovanou správou uživatelů na RADIUS serveru
- podpora přiřazení do VLAN z RADIUS serveru podle výsledků 802.1x autentizace
- možnost aplikace specifického access listu v závislosti na výsledku 802.1x autentizace
- možnost webové autentizace zabezpečené pomocí SSL pro non-IEEE 802.1x klienty
- VLAN access-listy sloužící k omezení specifického provozu uvnitř jedné sítě VLAN
- ochrana DHCP protokolu – blokování neautorizovaného DHCP provozu
- Dynamická inspekce ARP protokolu
- ochrana zdroje IP adresy zabraňující převzetí / podvržení IP adres
- možnost přesměrovat data na port přepínače (pro monitorování provozu), nebo do VLAN a tento provoz odposlouchávat až na portu jiného přepínače
- podpora paketových filtrů na jednotlivých rozhraních a na terminálových spojení na základě L2,L3,L4 informací v paketu
- možnost omezení přístupu podle MAC adres stanic, možnost omezení maximálního počtu MAC adres za portem přepínače
- ochrana spanning tree protokolu

- možnost definice „trust boundaries“ pro nastavení QoS

Klasifikace služeb (QoS):

- classification, policing, marking, queuing&scheduling
- IEEE 802.1p (class of service prioritization)
- podpora přednostní fronty (strict priority queueing)
- Shaped Round Robin (SRR) časování ve vstupních i výstupních frontách
- filtrování podle DSCP
- Rate limiting na základě IP adres, zdrojové a cílové MAC adresy, Layer 4 TCP a UDP informací

Multicast:

- podpora PIM sparse a PIM dense mode
- podpora Distance Vector Multicast Routing Protocol (DVMRP) tunnelingu
- možnost filtrování IGMP a omezení počtu současných multicast streamů per port
- podpora IGMP snooping pro IPv4 a IPv6 Multicast Listener Discovery (MLD) Verze 1 a 2

2.4.2. FC PASS-THRU MODUL DO STÁVAJÍCÍHO BLADE CHASSIS DELL

Součástí nabídky jsou požadované 2 ks Fibre Channel Pass-thru moduly plně kompatibilní s blade chassis DELL PE M1000e včetně připojení a konfigurace do stávajícího blade chasi DELL PE M1000e.

2.5. ROZŠÍŘENÍ STÁVAJÍCÍCH DISKOVÝCH POLÍ

Součástí nabídky je dodávka, instalace a konfigurace dvou rozšiřujících DAE do stávajícího diskového pole DELL CX 4-120. Nabízené diskové police jsou 100% kompatibilní s datovým úložištěm DELL/EMC CX 4 -120, provozovaným zadavatelem a to na úrovni hardware, software a poskytovatele supportu.

Součástí nabídky jsou DAE v následující konfiguraci:

- 1ks Disková police k diskovému poli DELL/EMC CX 4-120 včetně osazených pevných disků 15x 450 GB HDD FC4 15k rpm

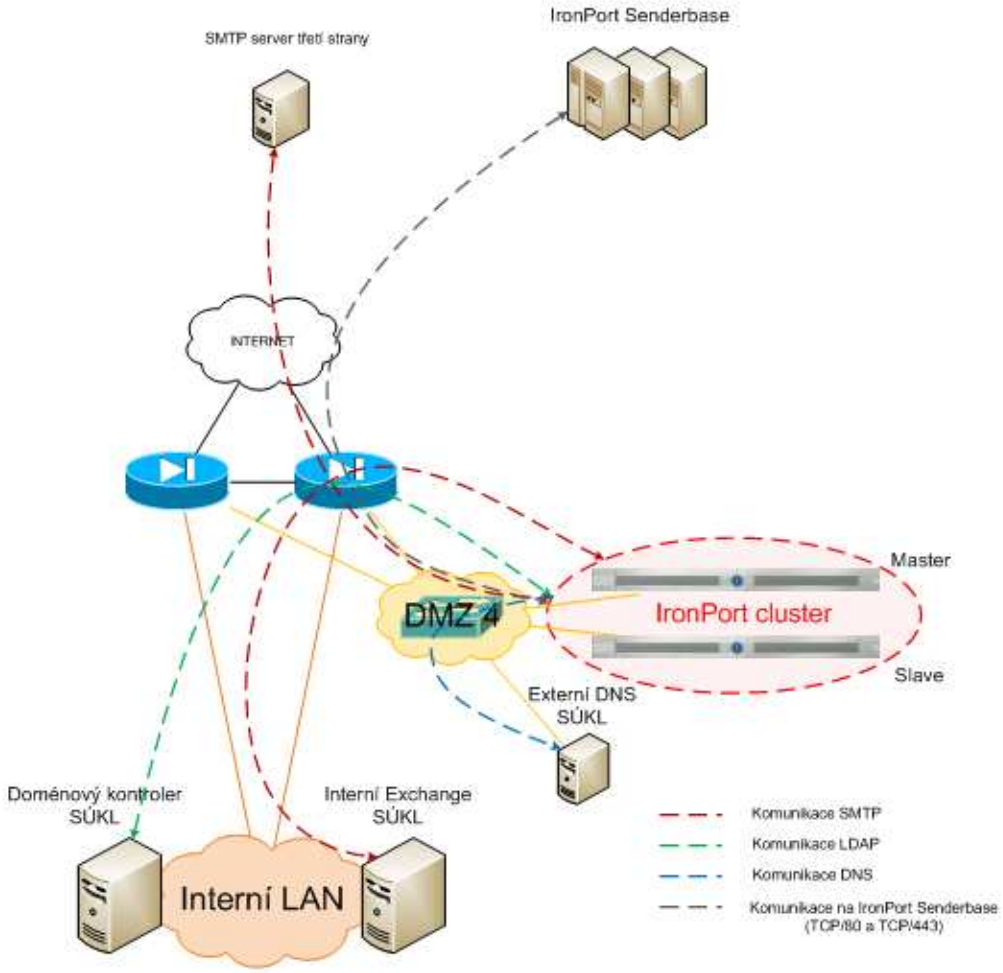
- 1ks Disková police k diskovému poli DELL/EMC CX 4-120 včetně osazených pevných disků 15x 1TB Serial ATA2 7.2k HD EMC

2.6. SYSTÉM ZAJIŠTĚNÍ KONTROLY A VYSOKÉ DOSTUPNOSTI EMAIL KOMUNIKACE

Jako systém externích emailových bran navrhujeme nasadit řešení společnosti IronPort, konkrétně dvojici emailových bran C160 provozovaných v clusteru. Cluster v tomto případě slouží pro management celého řešení z jednoho místa. Konfiguraci emailových bran můžeme rozdělit do třech úrovní Cluster level, Grop level a Machine level. Na úrovni clusteru se konfigurují funkcionality spojené se zpracováváním emailů, jako například WHITELIST a podobné. Na úrovní skupiny se konfigurují záležitosti, jako čas, časové pásmo a použitý DNS server, zde budou obě appliance v jedné skupině. Na úrovni samotného zařízení se konfigurují záležitosti spojené s IP adresací a síťovým směrováním.
Vysoké dostupnosti bude u systému externí emailové komunikace dosaženo pomocí vytvoření dvou MX záznamů pro doménu sukl.cz. Primární MX záznam bude směrován na primární appliance a sekundární MX bude směrován na sekundární appliance. Pro toto řešení budeme potřebovat vyčlenit 2 veřejné IP adresy v některé z externích DMZ sítí SÚKL.

Mezi zařízení v clusteru je možné dosáhnout loadbalancingu, buď integrací se systémem pro loadbalancing popsaným v kapitole 2.2 tohoto dokumentu, nebo pomocí konfigurace DNS serveru SÚKL tak, aby pomocí algoritmu round robin vracel na dotazy na doménu sukl.cz buď primární, nebo sekundární MX záznam.
Appliance IronPort C160 používá celou řadu sofistikovaných metod pro odhalování spamu, z nichž nejhlavnější je napojení na Senderbase, světově největší databázi informací o emailové komunikaci a o závadných a nezávadných odesílatelích pošty.
Appliance kromě jiných algoritmů na odhalování spamů používá i metodu ověřování příjemců mailů na základu existence daného uživatele v Microsoft AD. Appliance musí být tedy schopné pomocí protokolu LDAP číst v AD SÚKL.

Následující obrázek znázorňuje průběh komunikací z clusteru externích emailových bran směrem k okolnímu světu:



Přesná specifikace nabízeného řešení:

Pol.	Číslo	Obchodní název	MJ	Počet
1.	EBUN-2A-GV-SQR-3Y	Dual C 160, Anti-Spam, Anti-Virus, VOF (350, 3 years)	ks	1
2.		Email Bundle Dual Appliance 3 Years Anti-Spam 3 Years Anti-Virus 3 Years Virus Outbreak Filters 3 Years Centralized Management and 3 Years Platinum Support		

Toto řešení sestává ze 2 redundantních emailových bran, kdy každá splňuje následující parametry:

- zařízení je možné provozovat v clusteru
- zařízení je možné provozovat v clusteru v režimu loadbalancing
- možnost budoucího rozšíření o centrální jednotnou správu zařízení v clusteru jako jednoho celku (tzn., v rámci clusteru se musí automaticky replikovat konfigurace mezi jednotlivými zařízeními)
- zařízení musí být formou hardwarové „appliances“
- využívá několika technologií pro detekci spamu – detekce dle slovníku, grafické filtry, PDF filter, URL posuzování a jiné
- detekce spamu na základě reputace zdrojových IP adres
- detekce nestandardní poštovní komunikace (uchování podezřelých zpráv v karanténě do vyhodnocení výrobcem nebo zaslání nových definic)

- detekce virů a dalšího škodlivého kódu v poštovní komunikaci
- možnost nasazení více antivirových produktů od různých výrobců na zařízení
- kontrola příchozí i odchozí poštovní komunikace na jednom zařízení zároveň
- technologie filtrace spamu u nevyžádaných NDR zpráv na základě podpisu odchozích zpráv antispamovým zařízením (bounce attack protection)
- uživatelská karanténa (spam)
- možnost definování různých politik pro jednotlivé uživatele (whitelist, blacklist, maximální velikosti mailů, zakázané typy příloh apod.)
- možnost budoucího rozšíření o centrální karanténu na separátním zařízení (hardwarové appliance) pro více antispamových mailových bran
- automatická aktualizace definic (spam, viry)
- automatické stahování a aktualizace firmware přes administrační rozhraní
- zařízení má podporu DKIM, Domain Keys a SPF
- správa uživatelských účtů s různými právy
- pokročilý systém vyhledávání a reportování
- možnost zapojení do centrálního dohledu (SNMP)
- možnost budoucího rozšíření o centrální logování (SYSLOG)
- možnost ověřování existence uživatelských kont přes LDAP – funkce podporuje krátkodobé cachování, tj. bez nutnosti permanentního stahování databáze na dané mail appliance řešení
- možnost přepisování odchozích a příchozích mailových adres dle informací z LDAP
- možnost automatického ukládání statistik v pdf formátu
- možnost definovat různé antispam, antivirus a filtrovací politiky pro jednotlivé uživatele nebo pro celé skupiny uživatelů, včetně možnosti integrace s MS AD a LDAP
- možnost směrování SMTP komunikace na základě parametrů z LDAP
- možnost vytváření filtrů na emailovou komunikaci, které jsou schopny pracovat s obsahem hlaviček, těla i příloh v emailu přiřazování filtrů je možné na základě příslušnosti ke skupině v LDAP nebo MS AD
- zařízení je schopno vytvářet virtuální SMTP brány (virtuální brána = má svoji IP adresu, svůj vlastní SMTP banner, jde nastavovat provozní parametry bez vlivu na ostatní virtuální brány
- zařízení je schopno detekovat nejen spam, ale i marketingové zprávy
- zařízení je rozšiřitelné o Data Lost Prevention funkce
- Zařízení je schopno odsměrovat minimálně 43 000 emailů za 1 hodinu při použití antispam a antivirus funkcionalit
- Zařízení umožňuje vytváření pokročilých skriptů pro filtrovací politiky, včetně schopnosti jejich přiřazování uživatelům na základě skupin v LDAP/MS AD na úrovni jednotlivých filtrů.

3. ROZŠÍŘENÍ SOFTWARE DATOVÉHO CENTRA

3.1. VIRTUALIZAČNÍ SOFTWARE

Součástí nabídky je požadované rozšíření licencí SW VMware vSphere 4 pro výše uvedené Blade servery včetně zajištění implementační a servisní podpory.

Specifikace dodávaného software:

Označení výrobce	Název položky	Počet ks
VS4-ENT-PL-C	VMware vSphere 4 Enterprise Plus for 1 processor (Max 12 cores per processor)	4
VS4-ENT-PL-3G-SSS-C	Gold Support/Subscription for VMware vSphere Enterprise Plus for 1 processor for 3 year	4

3.2. SOFTWARE NA MONITORING DISKOVÝCH POLÍ

Součástí nabídky je dodávka a instalace rozšiřujícího software EMC Navisphere Analyzer pro stávající disková pole DELL CX 3-20 a DELL CX 4-120 v následujícím množství:

- 1ks CX3-20 Navisphere Analyzer Software (Kit)
- 2ks CX4-120 Navisphere Analyzer Software Kit

Dodávaný software je včetně požadované 3-leté software assurance.

4. IMPLEMENTACE PODPŮRNÝCH SYSTÉMŮ A VÝVOJ SOFTWARE

4.1. NÁVRH A IMPLEMENATCE ŘEŠENÍ VYSOKÉ DOSTUPNOSTI OID V PROSTŘEDÍ SBĚRU DAT

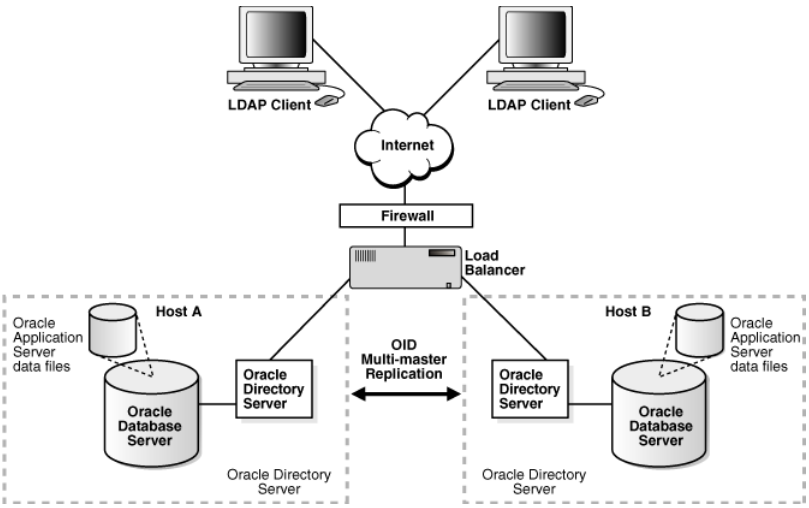
Předmětem je implementace technického řešení, které zajistí vysokou dostupnost OID pro potřeby ověřování identit externích subjektů (případně i interních) v rámci prostředí systému sběru dat SÚKL.

Navržené řešení splňuje následující požadavky:

- Navržené řešení zajišťuje vysokou dostupnost služby OID, zajištění pomocí dvou nezávislých vzájemně synchronizovaných OID serverů
- Počet registrovaných identit 100 000
- Provedení migrace identit ze stávajících systémů na nový systém OID
- Rekonfigurace interních systémů využívající služby OID
- Možnost rozšiřitelnosti řešení do geograficky vzdálených lokalit, počet N+1
- Garance funkčnosti řešení ve stávajícím VMware prostředí zadavatele

4.1.1. ZÁKLADNÍ KONCEPCE

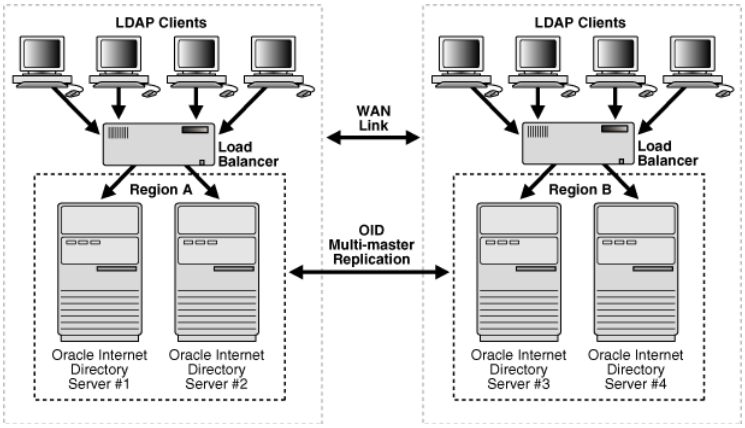
Základní řešení vychází z předpokladu, že vytváření a modifikace identit externích subjektů (lékáren, lékařů) je prováděna prostřednictvím administrátorských nástrojů nebo pomocí aplikace připojené k OID prostřednictvím standardního LDAP protokolu (LDAP klient). Nevyužívají se tak v oblasti externích identit nástroje OIM (Oracle Identity Management) a z pohledu vysoké dostupnosti se můžeme zaměřit pouze na dostupnost OID.



Základní koncepce je postavena na dvou samostatných OID serverech v jedné lokalitě, které jsou standardními nástroji Oracle multi-master replikace OID svázány do jedné replikační skupiny.
Vlastní multi-master replikace probíhá tak, že změny provedené v rámci jednoho serveru ve skupině jsou zapsány do log tabulky, jejíž obsah je replikován nástroji databáze Oracle do databází ostatních serverů ve skupině. Nad těmito servery pak běží proces, který automaticky aplikuje změny přicházející z ostatních serverů ve skupině. Časové zpoždění replikace je zanedbatelné, řádově nepřesahuje jednotky sekund, nicméně LDAP klient provádějící změny v OID si musí zachovávat persistenci spojení tak, aby veškeré změny prováděl nad jedním ze serverů a mezi servery při provádění změn nemigroval.

4.1.2. GEOGRAFICKY VZDÁLENÉ LOKALITY

Propojení geograficky vzdálených lokalit lze řešit analogicky multi-master replikací. Každá lokalita by se skládala ze dvou OID serverů. Topologie a způsob replikace mezi servery jednotlivých lokalit však bude záviset na jejich počtu. V případě 2-3 lokalit bude asi nejjednodušší zařadit všechny servery do jedné replikační skupiny a replikovat změny každý s každým.



4.1.3. ZVYŠOVÁNÍ VÝKONU

Zvýšení výkonu lze provést několika způsoby:

- Přidáním dalšího OID serveru do replikační skupiny.
- Oddělením infrastrukturní databáze OID na samostatný databázový server resp. databázový cluster RAC.

Vzhledem k tomu, že jednotlivé OID servery budou na SÚKL provozovány v prostředí virtualizace, je možné využít ke zvyšování výkonu právě prostředků virtualizace.

V případě oddělení infrastrukturních databází OID v kombinaci s provozem ve více lokalitách je nutné, aby tyto databáze spolu mohly komunikovat a replikovat tak jednotlivé změny. Tyto databáze není možné umístit do chráněné zóny.

4.1.4. PŘEDMĚT DODÁVKY

Předmět dodávky je:

a) Instalace dvou aplikačních serverů Oracle iAS EE ver. 10.1.4.0.1 na servery s operačním systémem Linux 32-bit, RedHat 4 pro zajištění provozu dvou samostatných instancí OID pro potřeby ověřování externích identit.
b) Zprovoznění Multi-Master replikace OID mezi instancemi nainstalovanými dle bodu a).
c) Kopii kmene externích identit z OID provozované do nově vytvořených instancí OID
d) Ověření funkčnosti Multi-Master replikace
e) Přenesení aktuálního kmene externích identit z OID provozované do nově vytvořených instancí OID
f) Zálohování

Součástí migrace externích identit, jejíž rozsah je stanoven bodem 4.1.4 bude i nutné provést rekonfiguraci všech systémů, které pracují se záznamy externích identit. Dále bude nutné provést rekonfiguraci interních a externích firewallů z důvodu zajištění komunikačních prostupů ze stávajících systémů na nové servery OID umístěné v CÚ prostředí SÚKL.

Upozornění:

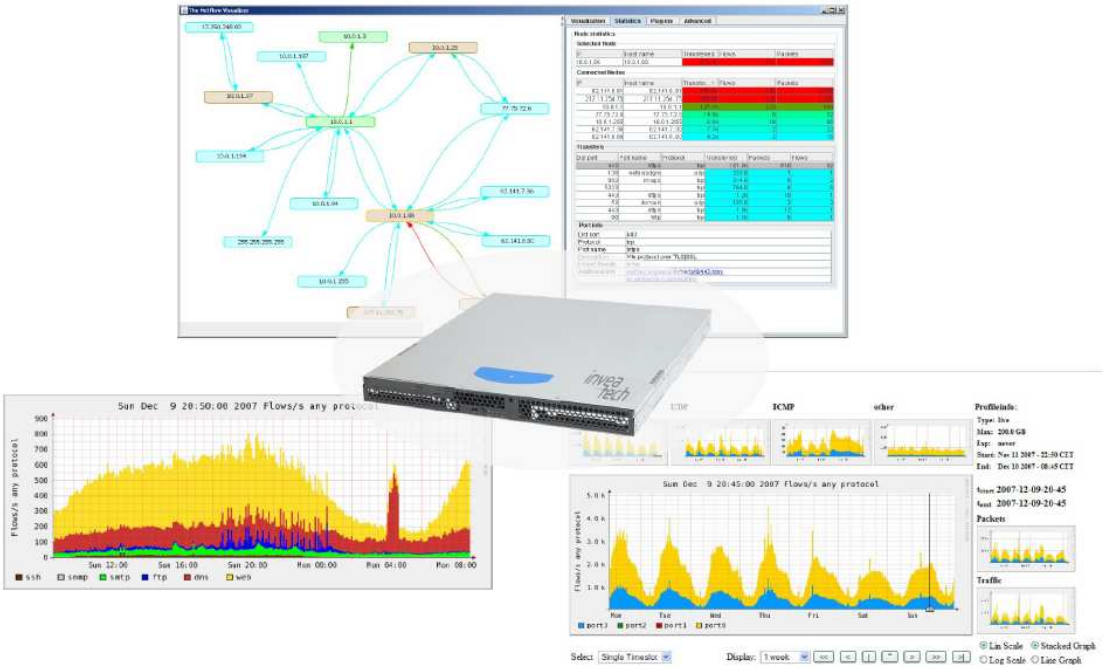
- Součástí instalace není integrace na okolní systémy jako MS AD, OAM apod.

- Objektové třídy stávajícího OID jsou rozšířeny o nestandardní atributy, což může způsobit komplikace při kopii stávajících identit na nový OID.
- Pokud bude prováděna integrace na okolní systémy jako MS AD, OAM apod., doporučujeme k tomuto přizvat dodavatele původního řešení (Oracle), aby nedošlo ke ztrátě záruk na původně dodané dílo končících v roce 2011.
- Součástí dodávky nejsou licence LINUX a ORACLE.

4.2. NÁVRH A IMPLEMENTACE SYSTÉMŮ ZAJIŠŤUJÍCÍ MONITORING DATOVÝCH TOKŮ

4.2.1. POPIS NAVRHOVANÉ TECHNOLOGIE

Systém zajišťující monitoring datových toků navrhujeme realizovat prostřednictvím zařízení společnosti InveaTech - Invea FlowMon Probe 6000 SFP osazeného 6 kusy metalických SFP modulů podporujících standard 10/100/1000 Base-T. Toto zařízení bude sloužit jak k zachytávání datových toků, tak k uchovávání záznamů o datových tocích a také k jejich vyhodnocování. Pro vyhodnocování informací o datových tocích bude na zařízení nainstalována kombinace dvou vyhodnocovacích nástrojů, Invea FlowMon Reporter a NetFlow Tracker s licencí pro 1 zařízení.



Takto sestavený systém bude poskytovat vyjmenované funkcionality a splňovat následující parametry:

- Umožní sledování všech datových toků v současné komunikační infrastruktuře.
- Umožní monitorování provozu na internetové lince (před firewally), provoz v externích i interních demilitarizovaných zónách a vnitřní síti.
- Pokryje svou působností celou redundantní komunikační infrastrukturu a bude monitorovat veškerý datový provoz i v případě výpadku některé z komponent.
- Bude „poslouchat“ provoz nejméně na 6 místech komunikační infrastruktury současně.
- Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie NetFlow (nutná podpora NetFlow v5 a NetFlow v9)
- možnost rozšíření na sledování bezpečnostních incidentů v několika lokalitách s centrální správou
- nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě
- specializované dedikované zařízení pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5, v9 - RFC3954)
- dlouhodobé ukládání statistik IP toků a jejich sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů
- plná zákaznická podpora v českém jazyce

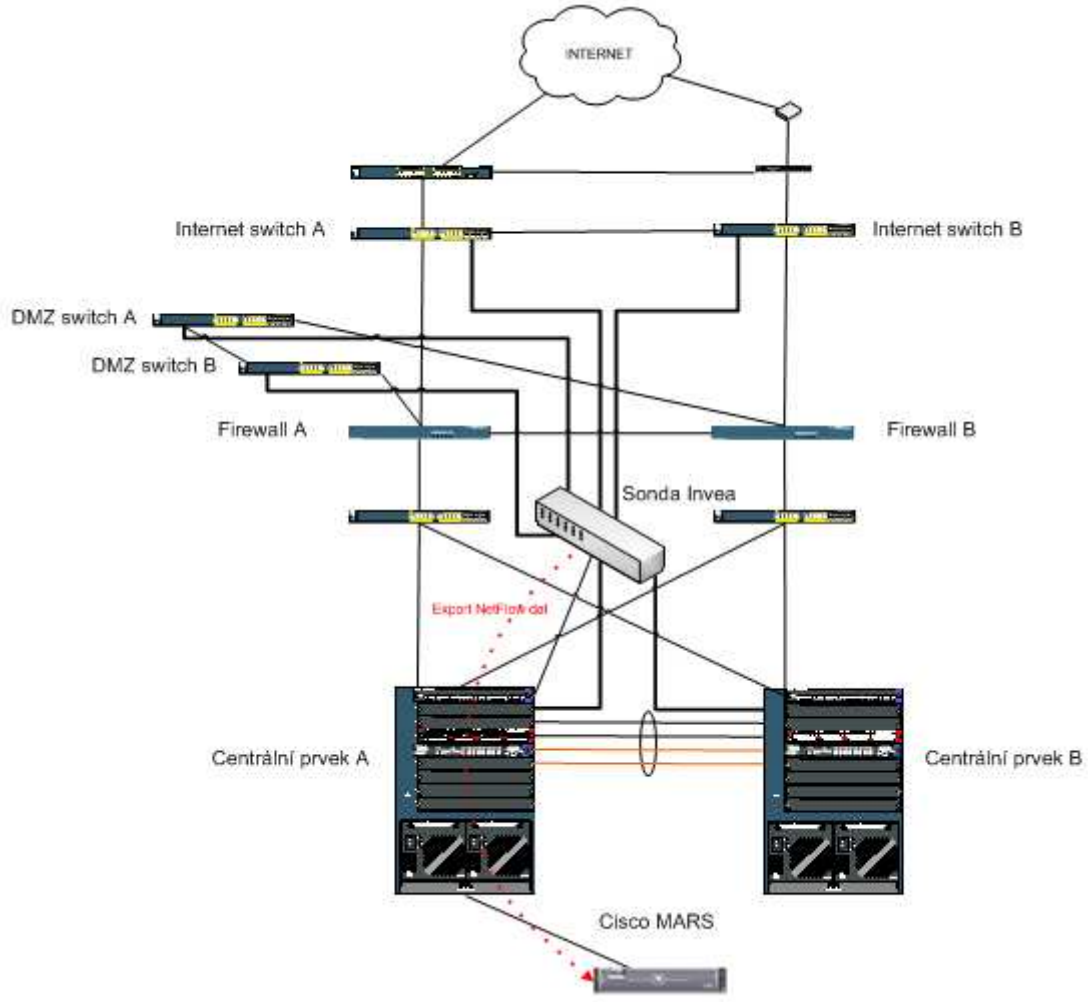
- podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 10Gb/s, otevřené rozhraní s možností integrace libovolných nástrojů i třetích stran.
- Systém zajišťující monitoring datových toků bude nezávislý na použité síťové infrastruktuře a svou funkcí nebude nijak ovlivňoval sledovanou síť.
- Ze strany monitorovacích rozhraní připojených do sledované sítě nebude zařízení detekovatelné a nebude snižovat výkonnost monitorovaných zařízení o více jak 5% výkonu.
- Vytváření síťových statistik bude prováděno jak přímo v tomto systému, tak bude přístupné i pro stávající Security management systém Cisco MARS.
- 100% přesný nezávislý autonomní zdroj NetFlow statistik s podporou IPv4, IPv6, VLAN, MPLS, NetFlow v5/v9, IPFIX (RFC 5101) na 1 Gigabit Ethernetu (s možností upgradu na 10 Gigabit Ethernet)
- snadná instalace do stávající síťové infrastruktury
- rack mount zařízení
- pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN porty)
- jeden administrativní port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS
- možnost vzdálené konfigurace s využitím protokolu Netconf (RFC 4741)
- správa uživatelů a přístupových práv na zařízení
- připojení na měřenou síť pomocí SFP transceiverů –umožňuje ad hoc změnu typu monitorované linky (metalická/optické single mód či optická multi mód) nebo kombinaci více typů linek jedním zařízením. V době dodání bude zařízení osazeno 6 ks metalických SFP modulů pro připojení pomocí konektorů RJ45 ke stávající datové síti
- možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalických rozhraních
- současné měření síťového provozu na minimálně šesti gigabitových rozhraních současně pomocí jednoho zařízení
- vestavěný kolektor pro ukládání NetFlow statistik, lokálně na zařízení mohou být uloženy statistické informace o provozu odpovídající min. 200 TB přenesených dat, nebo 1 milion toků
- časová synchronizace zařízení proti centrálnímu zdroji času na síti
- minimální výkon 500 tisíc paketů za sekundu na každém portu, možnost upgradu na verzi s wire-speed garancí
- zpracování datového provozu IPv4 a IPv6, VLAN, MPLS, uložení statistik, jejich vyhodnocení a reportování na stávající Security management systém Cisco MARS
- uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX
- dlouhodobé a stabilní zpracování na všech měřicích rozhraních
- podpora pro nastavení časů u aktivní a neaktivní expirace toků
- podpora vzorkování na úrovni paketů nebo toků
- podpora simultánního exportu NetFlow statistik minimálně na tři cíle
- podpora anonymizace dat
- podpora filtrování dat (pro různé cíle exportu různé statistiky)
- možnost dohledání každé komunikace, průběžné i koláčové grafy, podpora upozornění a reportů emailem (reporty v českém a anglickém jazyce), rozšiřitelnost o pluginy na míru
- ucelené řešení pro sledování síťové komunikace, jak v reálném čase, tak dlouhodobě
- vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH)
- generování statistik a podrobných výpisů nad volitelnými časovými intervaly
- výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu
- emailové upozornění administrátorům v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, výskyt nebezpečné anomálie, použití zakázané aplikace atd.)
- vytváření profilů pro ukládání dat vyhovující nadefinovaným filtrům (např. HTTP, FTP,
- SMTP, SSH provoz)
- podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace
- drill-down – možnost dohledat každý jednotlivý tok zaznamenaný systémem
- kombinace minimálně dvou vyhodnocovacích nástrojů v rámci systému
- otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh
- Intuitivní ovládání bez nutnosti ručního vyplňování filtrů
- Grafické výstupy ve volitelné formě - koláčové grafy, průběhové grafy, tabulky
- Možnost exportu výstupu do pdf, csv, xml

Přesná specifikace nabízeného řešení:

Pol.	Číslo	Obchodní název	MJ	Počet
1.	IFP-6000-SFP	Invea FlowMon Probe 6000 SFP	ks	1
2.	FPC-REPOTER	Invea FlowMon Reporter	ks	1
3.	NFT1001	NetFlow Tracker – 1 zařízení	ks	1
4.	1G-SFP-RJ45	SFP transceiver metalický 10/100/1000Mbps, RJ45	ks	6

4.2.2. POPIS TECHNICKÉHO ŘEŠENÍ

Zařízení popsané v předcházející kapitole navrhujeme implementovat do stávající komunikační infrastruktury za využití schopností přepínačů Cisco, na nichž je komunikační infrastruktura SÚKL postavená. Na těchto přepínačích navrhujeme nakonfigurovat zrcadlení provozu ze všech VLAN na specifický port pomocí technologie SPAN. Do tohoto portu potom bude připojen jeden z celkem 6 monitorovacích portů sondy Invea. Takto navrhujeme nakonfigurovat celkem 6 zařízení z komunikační infrastruktury SÚKL, konkrétně Centrální prvek A a Centrální prvek B, DMZ switch A a DMZ switch B a na switchích připojujících úřad do internetu, taktéž na switchi A i B. Pokud takto „ozrcadlíme“ provoz ve všech VLAN sítích protékající přes tato zařízení, dokážeme na sondě Invea zachitit nejdůležitější toky dat datového provozu v komunikační infrastruktuře SÚKL.
Toto nasazení bude pro stávající komunikační infrastrukturu zcela transparentní a nebude ji nijak ovlivňovat. Kromě ukládání statistik o síťových tocích lokálně na sondě budou data o Netflow tocích exportována na stávající Security monitoring systém Cisco MARS, kde můžou být díky použití kompatibilního standardu bez problémů zpracovávána..
Tento systém je možné dále rozvíjet přidáním dalších sond, případně externího kolektoru a dalších nástrojů pro vyhodnocování anomálií v datových tocích a různých nástrojů pro monitoring a reporting.
Obrázek plánovaného zapojení Sondy Invea do komunikační infrastruktury SÚKL:



4.3. ANALÝZA A REKONFIGURACE SYSTÉMU SONIC ESB

Cílem analýzy systému Sonic ESB a navazujících systémů bude identifikovat společné komponenty řešení ERP předepisování a výdejů LP a Hlášení výdejů LP, odhalit úzká místa stávajícího řešení a provést jejich rekonfiguraci nebo je nahradit novým řešením, které povede k plné funkčnosti řešení ve stávajícím prostředí zadavatele.
Splnit požadavky, vyplývající z protokolu inspektora ÚOOÚ sp.zn. INSP2-0277/09-40, viz Protokol__inspektora_ÚOOÚ, rozhodnutí předsedy ÚOOÚ sp.zn. INSP2-0277/09-62, viz Rozhodnutí_předsedy_ÚOOÚ, na oddělení ERP předepisování a výdejů LP a Hlášení výdejů LP do nezávislých celků tak, aby tyto systémy možné provozovat zcela odděleně.

4.3.1. ANALÝZA STÁVAJÍCÍHO STAVU KONFIGURACE

Předmětem řešení tohoto bodu bude analýza stávající instalace a konfigurace podnikové sběrnice služeb ESB a konfigurace přístupových bodů, které zajišťují vstup dat do systému a jejich zpracování v ESB službách a aplikační logikou umístěnou na aplikačních serverech.

Bude provedena analýza systémů pro:

- Hlášení výdejů LP s kontrolou výdeje OTC s omezením
- ERP pro předepisování a výdej LP

Bude provedena analýza existujících navazujících systémů, které zajišťují funkčnost systému jako celku.

4.3.1.1. ANALÝZA VSTUPNÍCH BRAN

Bude provedena analýza instalace a konfigurace systémů instalovaných na vstupních branách, které zajišťují přístup externích komunikujících subjektů a komunikují dále se systémem ESB v interním prostředí. Předmětem analýzy bude identifikace společných prvků, které je třeba oddělit.

Bude provedena analýza instalace a konfigurace systémů, které zajišťují přístup pro klienty komunikující pomocí SOAP protokolu a webových služeb. Překlad komunikace WS na JMS, napojení na ESB. Dále bude provedena analýza napojení na externí autentizační doménu včetně obsluhy více instancí autentizační domény.

Bude provedena analýza instalace a konfigurace systémů, které zajišťují přístup pro klienty komunikující pomocí JMS protokolu. Nastavení DRC spojení MQ brokeru na vstupních branách s interním ESB. Dále bude provedena analýza napojení MQ brokeru na externí autentizační doménu včetně obsluhy více instancí autentizační domény.

4.3.1.2. ANALÝZA ENTERPRISE SERVICE BUS

Bude provedena analýza instalace a konfigurace sběrnice služeb umístěné v interním prostředí, která zajišťuje příjem požadavků ze vstupních bran, provádí základní zpracování dat a komunikaci s aplikační logikou cílových systémů. Předmětem analýzy bude identifikace společných prvků, které je třeba oddělit.

Na úrovni HW bude provedena analýza využití přidělených hardwarových prostředků vyhrazených virtuálních serverů. Bude analyzováno vytížení přidělených jader CPU, alokace dostupné paměti a práce s s dostupnou pamětí, diskové operace a síťová komunikace s ostatními systémy.

Na úrovni SW bude provedena analýza konfigurace klastrového řešení instalace interního ESB a instalace MQ brokerů v eDMZ. Bude provedena analýza nastavení ACL přístupových práv pro jednotlivé komunikující systémy a nastavení ACL pro komunikaci mezi ESB a MQ brokerů na vstupních bodech.

Dále bude provedena analýza ostatních služeb provozovaných na ESB.

4.3.1.3. ANALÝZA NAPOJENÍ ESB SLUŽEB NA DB

Bude provedena analýza napojení ESB služeb na databáze pro ukládání Hlášení výdejů LP a ukládání dat žurnálu komunikace externích subjektů a úložiště. Předmětem analýzy bude identifikace společných prvků, které je třeba oddělit včetně oddělení žurnálů pro oba systémy.

4.3.1.4. ANALÝZA NAPOJENÍ ESB NA APLIKAČNÍ SERVERY

Bude provedena analýza spojení ESB s aplikačními servery s aplikační logikou pro zpracování dat ERP předepisování a výdejů LP. Bude navržena změna řešení pro minimalizaci počtu komponent systému, zrychlení přenosu dat a minimalizaci chyb při zpracování a transportu zpráv. Bude odstraněn problém s opakovaným připojením aplikačních serverů na ESB v případě výpadku ESB nebo přerušení spojení mezi těmito servery. Navržená změna bude spočívat v přesunu aplikační logiky z aplikačních serverů do ESB služeb pro minimalizaci komponent, přenosu dat a sjednocení architektury celého řešení s dalšími částmi systému.

4.3.2. NÁVRH A PROVEDENÍ ZMĚN KONFIGURACE

Na základě zjištěných nedostatků nebo závad v konfiguraci bude proveden návrh změn a proběhne samotné provedení rekonfigurace ESB, která zajistí oddělení společných komponent ERP předepisování a výdejů LP a Hlášení výdejů LP, vysokou dostupnost, průchodnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

4.3.2.1. NÁVRH A PROVEDENÍ ZMĚN VSTUPNÍCH BRAN

Cílovým stavem po provedené rekonfiguraci vstupních bran přístupových bodů budou oddělené společné komponenty ERP předepisování a výdejů LP a Hlášení výdejů LP. Společně s provedením dalších změn na úrovni ESB služeb a databázového úložiště bude zajištěno, že minimální počet JMS zpráv procházejících systémem a zpracovaných za 1 hodinu bude 800 tisíc, včetně času potřebného na obsloužení zasílaných požadavků a žurnálování komunikace a zasílaných požadavků.

Na základě provedené analýzy využití hardwarových prostředků bude provedena případná rekonfigurace virtuálních serverů na úrovni počtu přidělených jader CPU a případně přidělené RAM. Cílem bude optimalizace HW konfigurace pro běh MQ brokerů a Actional Intermediary tak, aby byla zaručena vysoká dostupnost a propustnost přístupových bodů. Konfigurace bude provedena tak, že bude zajištěna téměř lineární škálovatelnost. Podle potřeby bude upraven počet vláken pro komunikaci s externími klienty i ESB sběrnicí.

Po nasazení HW balanceru, bude provedena rekonfigurace vstupních bodů na toto řešení, tak aby byla zajištěna vysoká dostupnost, propustnost a rozkládání zátěže přistupujících klientů. Bude provedena rekonfigurace vystavených služeb s ohledem na HW balancer a změnu umístění fyzických vstupních bran.

Konfigurace bude provedena tak, že bude zajištěna případná úprava dotčených systémů tak, aby byl zajištěn bezproblémový provoz všech připojených systémů. Veškeré úpravy budou realizovány ve stávajícím prostředí zadavatele bez nutnosti HW nebo SW změn na úrovni ostatních subdodavatelů. V případě potřeby budou nevyhovující systémy nahrazeny vhodnějším a výkonnějším řešením.

Vstupní brány budou napojené na externí autentizační doménu tak, aby bylo možné veškeré vstupní požadavky autentizovat.

4.3.2.2. NÁVRH A PROVEDENÍ ZMĚN ENTERPRISE SERVICE BUS

Cílovým stavem po provedené rekonfiguraci ESB budou oddělené společné komponenty ERP předepisování a výdejů LP a Hlášení výdejů LP. Společně s provedením dalších změn provedených na vstupních branách, na úrovni ESB služeb a databázového úložiště bude zajištěno, že minimální počet JMS zpráv procházejících systémem a zpracovaných za 1 hodinu bude 800 tisíc, včetně času potřebného na obsloužení zasílaných požadavků a žurnálování komunikace a zasílaných požadavků.

Na základě provedené analýzy využití hardwarových prostředků bude provedena případná rekonfigurace virtuálních serverů na úrovni počtu přidělených jader CPU a případně přidělené RAM. Cílem bude optimalizace HW konfigurace pro běh ESB a služeb ESB tak, aby byla zaručena vysoká dostupnost a propustnost ESB sběrnice. Konfigurace bude provedena tak, že bude zajištěna téměř lineární škálovatelnost.

Konfigurace bude provedena tak, že bude realizována případná úprava dotčených systémů tak, aby byl zajištěn bezproblémový provoz všech připojených systémů. Veškeré úpravy budou realizovány ve stávajícím prostředí zadavatele bez nutnosti HW nebo SW změn na úrovni ostatních subdodavatelů. V případě potřeby budou nevyhovující systémy nahrazeny vhodnějším a výkonnějším řešením.

4.4. ANALÝZA A REKONFIGURACE SYSTÉMU SONIC ESB PRO HLÁŠENÍ VÝDEJŮ LP

4.4.1. ANALÝZA STÁVAJÍCÍHO STAVU KONFIGURACE

Předmětem řešení tohoto bodu bude analýza stávající instalace a konfigurace podnikové sběrnice služeb ESB a konfigurace přístupových bodů, které zajišťují vstup do systému pro zpracování dat Hlášení výdejů LP s kontrolou výdeje OTC s omezením. Bude provedena analýza existujících navazujících systémů, které zajišťují funkčnost celého systému Hlášení výdejů LP a kontroly výdeje OTC s omezením jako celku.

4.4.1.1. ANALÝZA VSTUPNÍCH BRAN PRO HLÁŠENÍ VÝDEJŮ LP

Bude provedena analýza konfigurace vystaveného komunikačního rozhraní a přístupových bodů pro zasílání Hlášený výdejů LP a kontroly výdeje OTC s omezením. Bude provedena analýza datového komunikačního rozhraní a příslušných definic.

Bude provedena analýza instalace a konfigurace služeb, které zajišťují přístup pro zasílání Hlášení výdejů LP pro klienty komunikující pomocí SOAP protokolu a webových služeb. Překlad komunikace Hlášení výdejů LP WS na JMS, napojení na ESB.

Bude provedena analýza instalace a konfigurace systémů, které zajišťují přístup pro klienty zasílající Hlášení výdejů LP a kontroly výdeje OTC s omezením a komunikující pomocí JMS protokolu. Nastavení DRC spojení MQ brokeru na vstupních branách s interním ESB.

Bude provedena analýza definice rozhraní XSD a WSDL pro zasílání Hlášená výdejů LP a kontrolu výdeje OTC s omezením z pohledu optimalizace a výkonu a požadavků na provoz více verzí paralelně.

4.4.1.2. ANALÝZA ESB SLUŽEB PRO HLÁŠENÍ VÝDEJŮ LP

Bude provedena analýza instalace a konfigurace sběrnice služeb umístěné v interním prostředí, která zajišťuje příjem požadavků na Hlášení výdejů LP ze vstupních bran, základní zpracování dat a komunikaci s aplikační logikou realizovanou prostřednictvím ESB služeb.

Na úrovni HW bude provedena analýza využití přidělených hardwarových prostředků pro provoz ESB kontejnerů na vyhrazených virtuálních serverech. Bude analyzováno vytížení přidělených jader CPU, alokace dostupné paměti a práce s dostupnou pamětí, diskové operace a síťová komunikace s ostatními systémy.

Na úrovni SW bude provedena analýza jednotlivých ESB kontejnerů s aplikační logikou pro zpracování dat Hlášení výdejů LP a kontroly výdeje OTC s omezením a aplikační logikou pro zpracování dat žurnálu komunikace.

Bude provedena analýza použití počtu vláken pro zpracování Hlášení výdejů LP na úrovni ESB kontejnerů.

4.4.2. NÁVRH A PROVEDENÍ ZMĚN KONFIGURACE

Na základě zjištěných nedostatků nebo závad v konfiguraci Hlášení výdejů LP bude proveden návrh změn a proběhne samotné provedení rekonfigurace, která zajistí vysokou dostupnost, průchodnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

4.4.2.1. NÁVRH A PROVEDENÍ ZMĚN NA VSTUPNCH BRANÁCH

Cílovým stavem Hlášení výdejů LP po provedené rekonfiguraci vstupních bran přístupových bodů společně s provedením dalších změn na úrovni ESB služeb a databázového úložiště bude zajištěno, že minimální počet JMS zpráv procházejících systémem a zpracovaných za 1 hodinu bude 800 tisíc, včetně času potřebného na obsloužení zasílaných požadavků a žurnálování komunikace zasílaných požadavků.

Po provedení nasazení HW balanceru, bude provedena rekonfigurace vstupních bodů na toto řešení, tak aby byla zajištěna vysoká dostupnost a rozkládání zátěže přistupujících klientů. Bude provedena rekonfigurace vystavených služeb Hlášení výdejů LP.

Konfigurace bude provedena tak, že bude zajištěna případná úprava dotčených systémů tak, aby byl zajištěn bezproblémový provoz všech připojených systémů. Veškeré úpravy budou realizovány ve stávajícím prostředí zadavatele bez nutnosti HW nebo SW změn na úrovni ostatních subdodavatelů. V případě potřeby budou nevyhovující systémy nahrazeny vhodnějším a výkonnějším řešením.

Bude provedena úprava definice vystaveného datového rozhraní XSD a WSDL. Definice rozhraní bude upravena tak, aby maximálně využívala možnosti definice XSD podle specifikace. Do definice rozhraní bude zapracován pseudonymizovaný identifikátor pacienta. Další úpravy rozhraní budou zaměřeny na minimalizaci přenášených objemů dat. Rozhraní bude upraveno s ohledem na požadavky verzování rozhraní. Pro každou verzi a revizi definice rozhraní bude vytvořen jmenný prostor, ve kterém budou definovány příslušné elementy. Pro každou verzi bude vystaveno URL možností paralelního souběhu verzí WS. Obdobně bude řešeno pro JMS.

4.4.2.2. NÁVRH A PROVEDENÍ ZMĚN NA ENTERPRISE SERVICE BUS

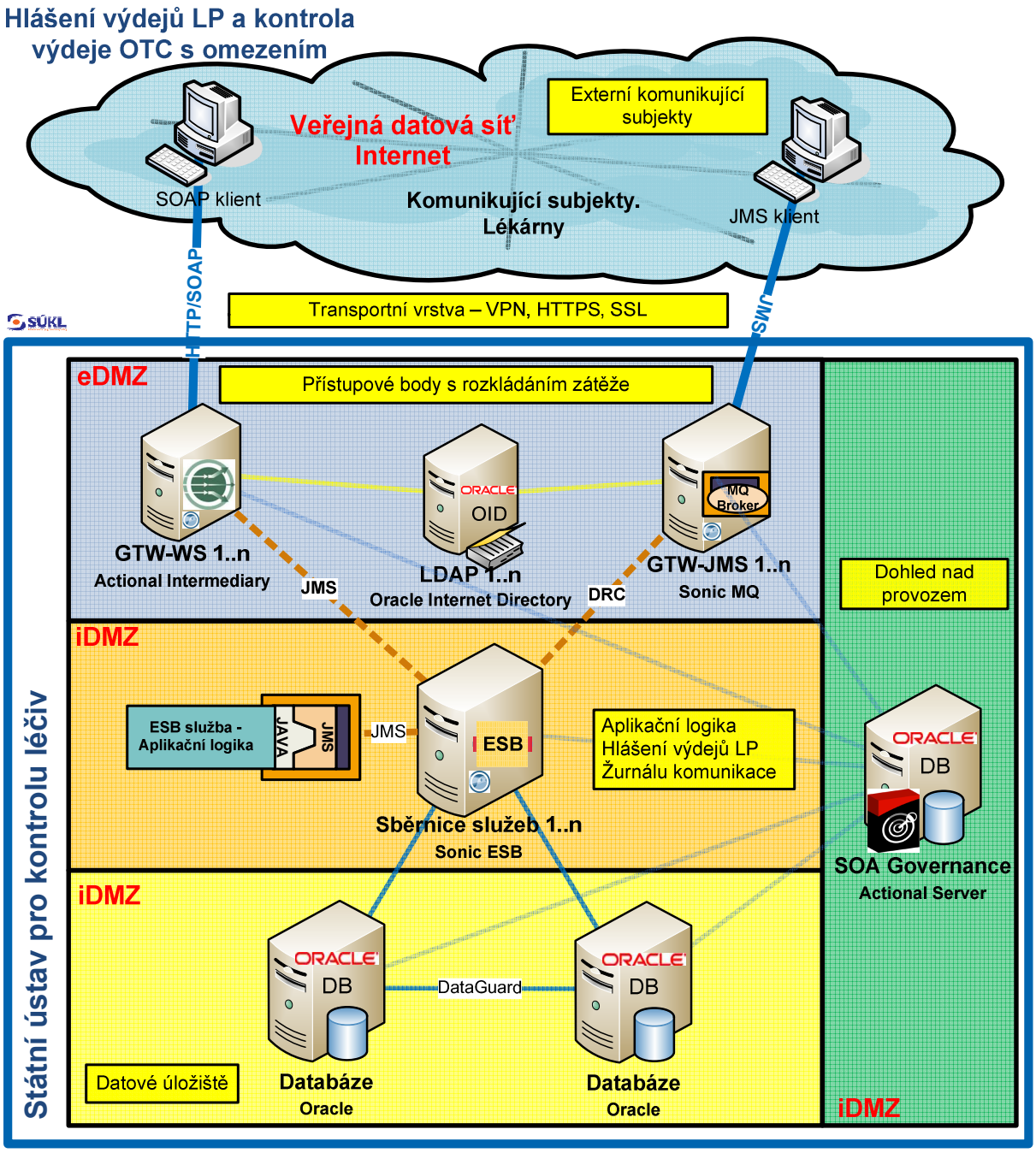
Cílovým stavem Hlášení výdejů LP po provedené rekonfiguraci ESB společně s provedením dalších změn provedených na vstupních branách, na úrovni ESB služeb a databázového úložiště bude zajištěno, že minimální počet JMS zpráv procházejících systémem a zpracovaných za 1 hodinu bude 800 tisíc, včetně času potřebného na obsloužení zasílaných požadavků a žurnálování komunikace zasílaných požadavků.

Konfigurace bude provedena tak, že bude zajištěna případná úprava dotčených systémů tak, aby byl zajištěn bezproblémový provoz všech připojených systémů. Veškeré úpravy budou realizovány ve stávajícím prostředí zadavatele bez nutnosti HW nebo SW změn na úrovni ostatních subdodavatelů. V případě potřeby budou nevyhovující systémy nahrazeny vhodnějším a výkonnějším řešením.

Na základě analýzy použití počtu vláken pro zpracování Hlášení výdejů LP na úrovni ESB kontejnerů bude nastaven jejich optimální počet z pohledu maximální průchodnosti zpráv.

4.4.2.3. ODDĚLENÉ KOMPONENTY A LOGICKÉ VRSTVY ŘEŠENÍ PRO SBĚR DAT HLÁŠENÍ VÝDEJŮ LP

Obr.: Architektura aplikace pro sběr dat Hlášení výdejů LP



4.5. ANALÝZA A REKONFIGURACE ESB SLUŽEB PRO ZPRACOVÁNÍ HLÁŠENÍ VÝDEJŮ LP A KONTROLY VÝDEJE OTC S OMEZENÍM

Předmětem řešení tohoto bodu bude analýza stávajícího stavu řešení:

- instalace a konfigurace ESB služeb aplikačního SW pro sběr dat Hlášení výdejů LP a kontroly výdejů OTC s omezením
- instalace a konfigurace ESB služeb žurnálu komunikace se subjekty vydávajícími léčivé přípravky

4.5.1. HLÁŠENÍ VÝDEJŮ LP A KONTROLA VÝDEJŮ OTC S OMEZENÍM

Na základě výsledku analýzy ESB služby pro zpracování Hlášení výdejů LP, bude proveden návrh změn, úprav a samotné provedení rekonfigurace aplikační logiky Hlášení výdejů LP, která zajistí vysokou dostupnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

Bude naprogramována nová aplikační logika ESB služeb, která nahradí původní a zajistí zpracování dat v novém rozhraní se zpětnou kompatibilitou s aktuální verzí rozhraní.

Nová aplikační logika bude navržena a realizována v souladu s principy architektury orientované na služby. Jednotlivé služby budou znovupoužitelné pro ostatní části díla.

Nová aplikační logika bude navržena tak, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Pro identifikaci pacienta, v případě že bude požadována, bude navržen nový pseudonymizovaný identifikátor, který umožní přechod z identifikace číslem pojištěnce na jiný typ identifikátoru bez ztráty informace o vazbě na pacienta nebo nutnosti použití více typů identifikátorů současně.

Bude dodána aplikační logika pro obsluhu kontroly výdeje OTC s omezením a aktivována podle potřeb zadavatele. Bude zajišťovat kontrolu vydaných OTC s omezením na pacienta, časové období a množství léčivé látky. Součástí bude i vazba na příslušné číselníky.

Vývoj nové aplikační logiky bude umožňovat zpracování dat rozhraní ve více verzích na základě jmenného prostoru uvedeného v XML zasílaných datech zpráv. Aplikační logika tímto bude umožňovat paralelní provoz více verzí současně. Pro přístup k datům uloženým ve starších verzích budou dostupné příslušné funkce, včetně funkce na zjištění verze, ve které jsou data uložena.

Veškeré chybové stavy, ke kterým bude při komunikaci externího subjektu s úložištěm docházet, budou uloženy v databázi a budou dostupné pro využití provozovatelem aplikace. Data budou uložena s identifikátorem pracoviště, které data zaslalo a identifikátorem chyby, která nastala. Bude umožněno analyzovat příčiny odmítání zasílaných dat a komunikovat s externími subjekty a řešit a odstraňovat problémy nevalidních dat.

Nová aplikační logika ESB služeb pro Hlášení výdejů LP a kontroly výdeje OTC s omezením bude postavena tak, aby byla do budoucna maximálně rozšiřitelná a bylo možné provádět potřebné změny na základě legislativních změn a požadavků zadavatele.

4.5.2. ŽURNÁL KOMUNIKACE EXTERNÍCH SUBJEKTŮ A ÚLOŽIŠTĚ

Na základě výsledku analýzy ESB služby pro zpracování dat žurnálu komunikace externích subjektů a úložiště dat, bude proveden návrh změn, úprav a samotné provedení rekonfigurace aplikační logiky žurnálu, která zajistí vysokou dostupnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

Bude naprogramována nová aplikační logika ESB služeb žurnálu, která nahradí původní a zajistí zpracování dat v novém rozhraní se zpětnou kompatibilitou s aktuální verzí rozhraní.

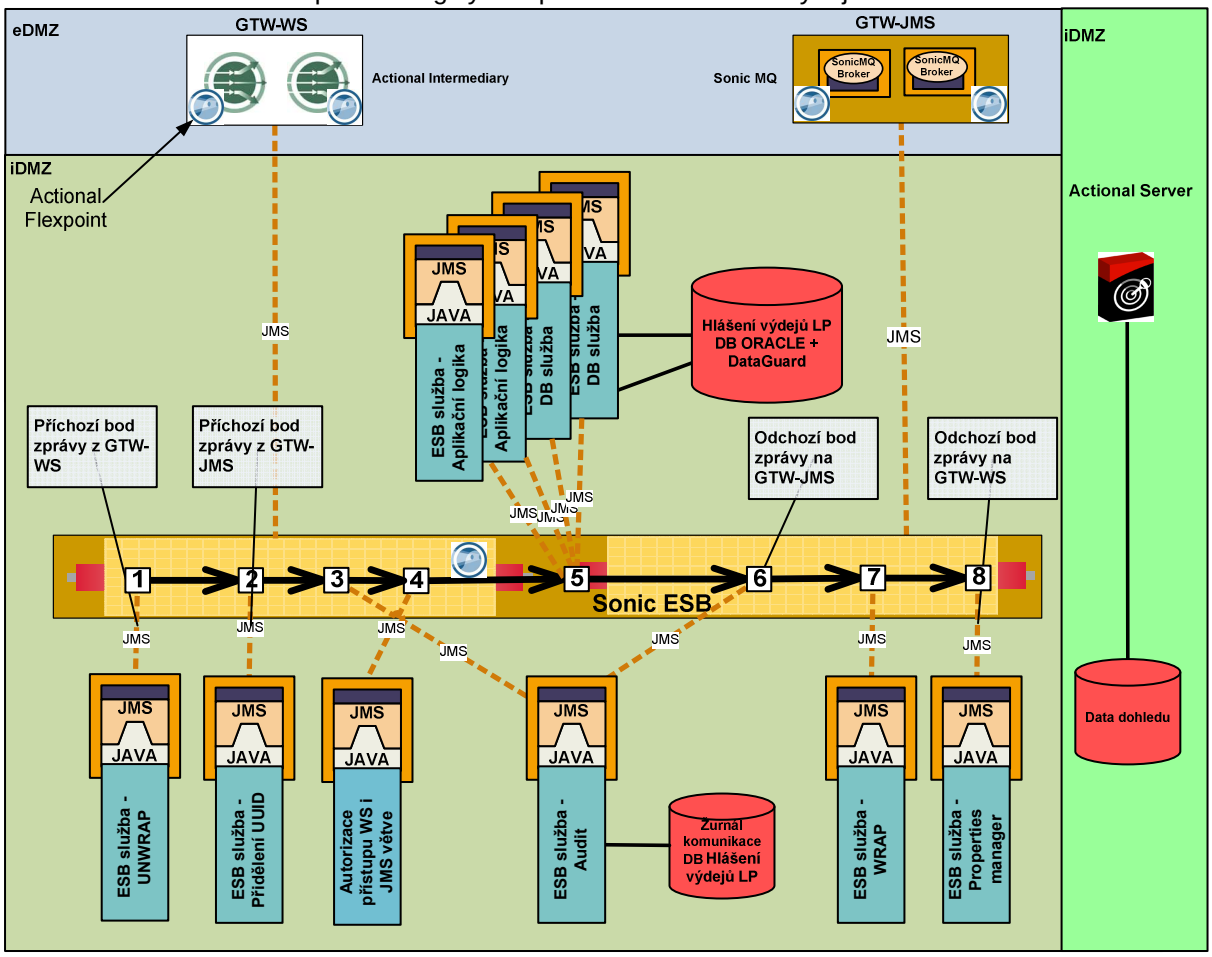
Nová aplikační logika bude navržena tak, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Aplikační logika žurnálovací ESB služby bude pouze nepřetržitě zapisovat do úložiště žurnálu, bez možnosti čtení dat. Aplikační logika bude podporovat průběžnou archivaci dat žurnálu bez vlivu na její provoz. Bude maximálně optimalizována na výkon a dostupnost.

4.5.3. ARCHITEKTURA ŘEŠENÍ HLÁŠENÍ VÝDEJŮ LP A KONTROLY VÝDEJE OTC S OMEZENÍM

Architektura aplikační logiky založená na službách pro sběr dat Hlášení výdejů LP.

Obr.: Architektura řešení aplikační logiky SW pro sběr dat Hlášení výdejů LP:



4.6. ANALÝZA A REKONFIGURACE SYSTÉMU SONIC ESB PRO ZPRACOVÁNÍ ERP PŘEDEPISOVÁNÍ A VÝDEJŮ LP

4.6.1. ANALÝZA STÁVAJÍCÍHO STAVU KONFIGURACE ERP PŘEDEPISOVÁNÍ A VÝDEJE LP

Předmětem řešení tohoto bodu bude analýza stávající instalace a konfigurace podnikové sběrnice služeb ESB, konfigurace přístupových bodů, které zajišťují vstup dat do systému pro zpracování dat předepsaných elektronických receptů a vydaných léčivých přípravků. Bude provedena analýza aplikačních serverů s aplikační logikou pro zpracování ERP předepisování a výdejů LP. Bude provedena analýza existujících navazujících systémů, které zajišťují funkčnost celého systému elektronických receptů jako celku.

4.6.1.1. ANALÝZA VSTUPNÍCH BRAN PRO ERP PŘEDEPISOVÁNÍ A VÝDEJE LP

Bude provedena analýza konfigurace vystaveného komunikačního rozhraní a přístupových bodů pro zasílání elektronických receptů a realizovaných výdejů LP. Bude provedena analýza datového komunikačního rozhraní a příslušných definic.

Bude provedena analýza instalace a konfigurace služeb, které zajišťují přístup pro zasílání ERP předepisování a výdeje LP pro klienty komunikující pomocí SOAP protokolu a webových služeb. Překlad komunikace ERP předepisování a výdejů LP WS na JMS, napojení na ESB.

Bude provedena analýza instalace a konfigurace systémů, které zajišťují přístup pro klienty zasílající ERP předepisování a výdeje LP a komunikující pomocí JMS protokolu. Nastavení DRC spojení MQ brokeru na vstupních branách s interním ESB.

Bude provedena analýza definice rozhraní XSD a WSDL pro zasílání ERP předepisování a výdejů LP z pohledu optimalizace a výkonu a požadavků na provoz více verzí paralelně.

4.6.1.2. ANALÝZA ESB SLUŽEB PRO ERP PŘEDEPISOVÁNÍ A VÝDEJE LP

Bude provedena analýza instalace a konfigurace sběrnice služeb umístěné v interním prostředí, která zajišťuje příjem požadavků na ERP předepisování a výdeje LP ze vstupních bran, základní zpracování dat a komunikaci s aplikační logikou realizovanou prostřednictvím ESB služeb.

Na úrovni HW bude provedena analýza využití přidělených hardwarových prostředků pro provoz ESB kontejnerů žurnálu a základních služeb zpracování dotazů na vyhrazených virtuálních serverech. Bude analyzováno vytížení přidělených jader CPU, alokace dostupné paměti a práce s dostupnou pamětí, diskové operace a síťová komunikace s ostatními systémy.

Na úrovni SW bude provedena analýza jednotlivých ESB kontejnerů s aplikační logikou pro zpracování dat žurnálu komunikace a základních služeb zpracování dotazů a překlad SOAP volání na JMS.

Bude provedena analýza použití počtu vláken pro zpracování dat žurnálu na úrovni ESB kontejnerů.

4.6.1.3. ANALÝZA APLIKAČNÍCH SERVERŮ A NAPOJENÍ NA ESB

Bude provedena analýza technického řešení napojení aplikačních serverů na ESB sběrnici. Bude provedena analýza aplikační logiky pro zpracování dat ERP předepisování a výdejů LP komunikace externích subjektů a centrálního úložiště.

4.6.2. NÁVRH A PROVEDENÍ ZMĚN KONFIGURACE ERP PŘEDEPISOVÁNÍ A VÝDEJE LP

Na základě zjištěných nedostatků nebo závad v konfiguraci ERP předepisování a výdejů LP bude proveden návrh změn a proběhne samotné provedení rekonfigurace, která zajistí vysokou dostupnost, průchodnost a zpracování požadovaného objemu zpráv za definovaný časový interval. Bude realizována změna na úrovni umístění aplikační logiky ERP předepisování a výdejů LP a definice komunikačního rozhraní.

4.6.2.1. NÁVRH A PROVEDENÍ ZMĚN NA VSTUPNCH BRANÁCH PRO ERP PŘEDEPISOVÁNÍ A VÝDEJE LP

Cílovým stavem ERP předepisování a výdejů LP po provedené rekonfiguraci vstupních bran přístupových bodů společně s provedením dalších změn na úrovni ESB služeb, aplikačních serverů a databázového úložiště bude zajištěno, že minimální počet JMS zpráv procházejících systémem a zpracovaných za 1 hodinu bude 800 tisíc, včetně času potřebného na obsloužení zasílaných požadavků a žurnálování komunikace zasílaných požadavků.

Po nasazení HW balanceru, bude provedena rekonfigurace vstupních bodů na toto řešení, tak aby byla zajištěna vysoká dostupnost a rozkládání zátěže přistupujících klientů. Bude provedena rekonfigurace vystavených služeb pro ERP předepisování a výdeje LP.

Konfigurace bude provedena tak, že bude zajištěna případná úprava dotčených systémů tak, aby byl zajištěn bezproblémový provoz všech připojených systémů. Veškeré úpravy budou realizovány ve

stávajícím prostředí zadavatele bez nutnosti HW nebo SW změn na úrovni ostatních subdodavatelů. V případě potřeby budou nevyhovující systémy nahrazeny vhodnějším a výkonnějším řešením.

Bude provedena úprava definice vystaveného datového rozhraní XSD a WSDL. Definice rozhraní bude upravena tak, aby maximálně využívala možnosti definice XSD podle specifikace. Do definice rozhraní bude zapracován pseudonymizovaný identifikátor pacienta. Další úpravy rozhraní budou zaměřeny na minimalizaci přenášených objemů dat. Rozhraní bude upraveno s ohledem na požadavky verzování rozhraní. Pro každou verzi a revizi definice rozhraní bude vytvořen jmenný prostor, ve kterém budou definovány příslušné elementy. Pro každou verzi bude vystaveno URL možností paralelního souběhu verzí WS. Obdobně bude řešeno pro JMS.

4.6.2.2. NÁVRH ZMĚN ŘEŠENÍ ZPRACOVÁNÍ DAT ERP PŘEDEPISOVÁNÍ A VÝDEJŮ LP

Cílovým stavem ERP předepisování a výdejů LP po provedené změně bude zajištěno, že minimální počet JMS zpráv procházejících systémem a zpracovaných za 1 hodinu bude 800 tisíc, včetně času potřebného na obsloužení zasílaných požadavků a žurnálování komunikace a zasílaných požadavků.
Bude navržena změna řešení, pro minimalizaci počtu komponent systému, zrychlení přenosu dat a minimalizaci chyb při zpracování a transportu zpráv. Bude odstraněn problém s opakovaným připojením aplikačních serverů na ESB v případě výpadku ESB nebo přerušení spojení mezi těmito servery. Navržená změna bude spočívat v přesunu aplikační logiky z aplikačních serverů do ESB služeb pro minimalizaci komponent, přenosu dat a sjednocení architektury celého řešení s dalšími částmi systému.

4.6.2.3. NÁVRH A PROVEDENÍ ZMĚN NA ENTERPRISE SERVICE BUS PRO ERP PŘEDEPISOVÁNÍ A VÝDEJE LP

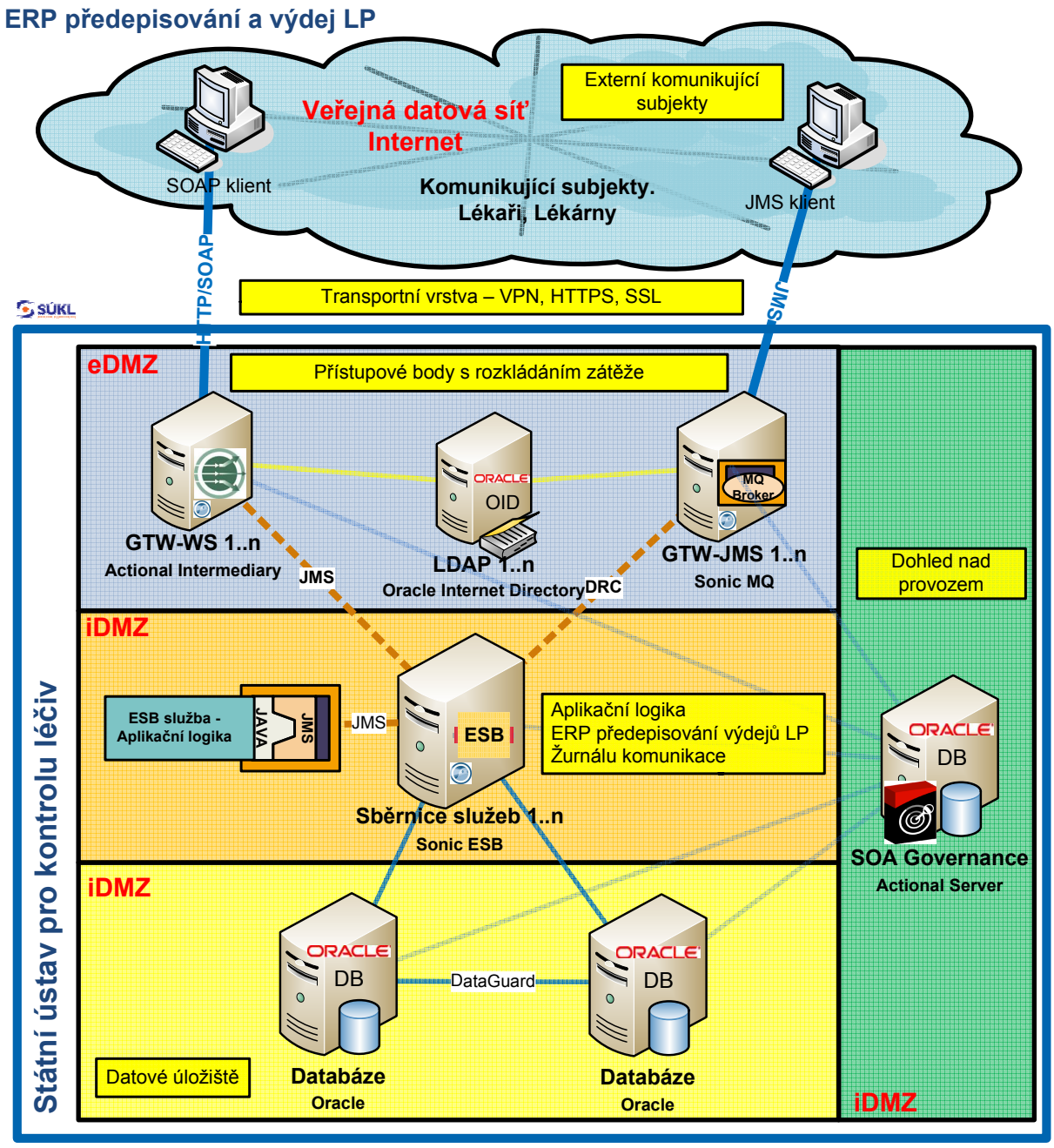
Cílovým stavem ERP předepisování a výdeje LP po provedené rekonfiguraci ESB a vývoji nové aplikační logiky společně s provedením dalších změn provedených na vstupních branách, na úrovni ESB služeb a databázového úložiště bude zajištěno, že minimální počet JMS zpráv procházejících systémem a zpracovaných za 1 hodinu bude 800 tisíc, včetně času potřebného na obsloužení zasílaných požadavků a žurnálování komunikace zasílaných požadavků.

Konfigurace bude provedena tak, že bude zajištěna případná úprava dotčených systémů tak, aby byl zajištěn bezproblémový provoz všech připojených systémů. Veškeré úpravy budou realizovány ve stávajícím prostředí zadavatele bez nutnosti HW nebo SW změn na úrovni ostatních subdodavatelů. V případě potřeby budou nevyhovující systémy nahrazeny vhodnějším a výkonnějším řešením.

Na základě analýzy použití počtu vláken pro zpracování ERP předepisování a výdejů LP na úrovni ESB kontejnerů bude nastaven jejich optimální počet z pohledu maximální průchodnosti zpráv.

4.6.2.4. ODDĚLENÉ KOMPONENTY A LOGICKÉ VRSTVY ŘEŠENÍ PRO ERP PŘEDEPISOVÁNÍ A VÝDEJŮ LP

Obr.: Architektura aplikace ERP předepisování a výdejů LP



4.7. ANALÝZA A REKONFIGURACE ESB SLUŽEB PRO ERP PŘEDEPISOVÁNÍ A VÝDEJE LP

Předmětem řešení tohoto bodu bude analýza stávajícího stavu řešení:

- instalace a konfigurace ESB služeb aplikačního SW pro ERP předepisování a výdeje LP
- instalace a konfigurace ESB služeb žurnálu komunikace se subjekty předepisujícími a vydávajícími léčivé přípravky

4.7.1. ELEKTRONICKÉ RECEPTY A VÝDEJE LP

Na základě výsledku analýzy aplikační logiky umístěné na aplikačních serverech bude proveden návrh nových ESB služeb s aplikační logikou pro zpracování ERP předepisování a výdeje LP. Bude proveden návrh změn, úprav a samotné provedení rekonfigurace aplikační logiky ERP předepisování a výdeje LP, která zajistí vysokou dostupnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

Bude naprogramována nová aplikační logika ESB služeb, která nahradí původní aplikační logiku umístěnou na aplikačních serverech a zajistí zpracování dat v novém rozhraní.

Nová aplikační logika bude navržena a realizována v souladu s principy architektury orientované na služby. Jednotlivé služby budou znovupoužitelné pro ostatní části díla.

Nová aplikační logika bude navržena tak, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Pro identifikaci pacienta, bude navržen nový pseudonymizovaný identifikátor, který umožní přechod z identifikace číslem pojištěnce na jiný typ identifikátoru bez ztráty informace o vazbě na pacienta nebo nutnosti použití více typů identifikátorů současně.

Vývoj nové aplikační logiky bude umožňovat zpracování dat rozhraní ve více verzích na základě jmenného prostoru uvedeného v XML zasílaných datech zpráv. Aplikační logika tímto bude umožňovat paralelní provoz více verzí současně. Pro přístup k datům uloženým ve starších verzích budou dostupné příslušné funkce, včetně funkce na zjištění verze, ve které jsou data uložena.

Veškeré chybové stavy, ke kterým bude při komunikaci externího subjektu s úložištěm docházet, budou uložené v databázi a budou dostupné pro využití provozovatelem aplikace. Data budou uložena s identifikátorem pracoviště, které data zaslalo a identifikátorem chyby, která nastala. Bude umožněno analyzovat příčiny odmítání zasílaných dat a komunikovat s externími subjekty a řešit problémy nevalidních dat.

Nová aplikační logika ESB služeb pro ERP předepisování a výdeje LP bude postavena tak, aby byla do budoucna maximálně rozšiřitelná a bylo možné provádět potřebné změny na základě legislativních změn a požadavků zadavatele.

4.7.2. ŽURNÁL KOMUNIKACE EXTERNÍCH SUBJEKTŮ A ÚLOŽIŠTĚ

Na základě výsledku analýzy ESB služby pro zpracování dat žurnálu komunikace externích subjektů a úložiště dat, bude proveden návrh změn, úprav a samotné provedení rekonfigurace aplikační logiky žurnálu, která zajistí vysokou dostupnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

Bude naprogramována nová aplikační logika ESB služeb, která nahradí původní a zajistí zpracování dat v novém rozhraní se zpětnou kompatibilitou s aktuální verzí rozhraní.

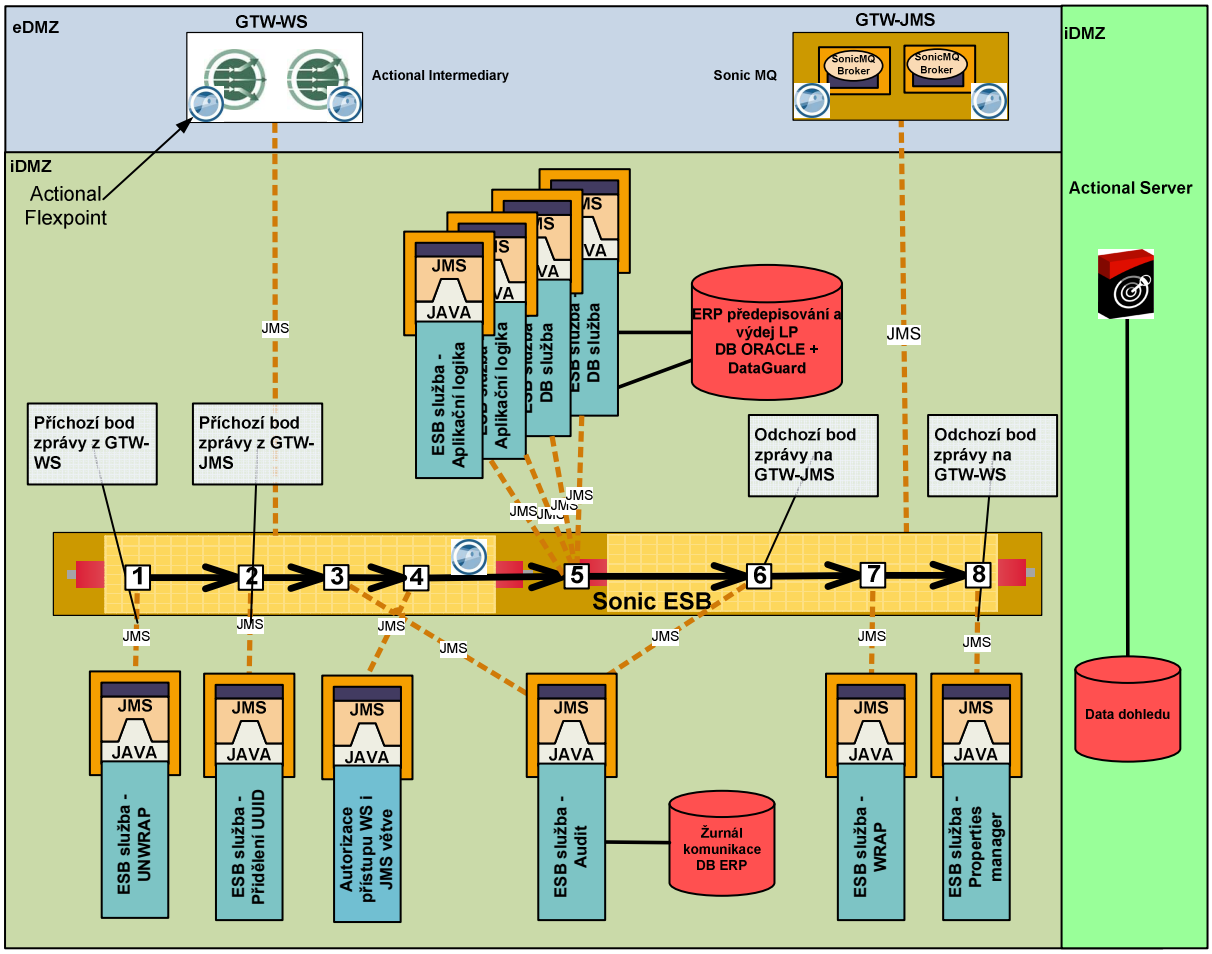
Nová aplikační logika bude navržena tak, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Aplikační logika žurnálovací ESB služby bude pouze nepřetržitě zapisovat do úložiště žurnálu bez možnosti čtení dat. Aplikační logika bude podporovat průběžnou archivaci dat žurnálu bez vlivu na její provoz. Bude maximálně optimalizována na výkon a dostupnost.

4.7.3. ARCHITEKTURA ŘEŠENÍ ERP PŘEDEPISOVÁNÍ A VÝDEJŮ LP

Architektura aplikační logiky založená na službách pro ERP předepisování a výdejů LP.

Obr.: Architektura řešení aplikační logiky SW pro ERP předepisování a výdej LP:



4.8. ANALÝZA A REKONFIGURACE DATABÁZOVÝCH SYSTÉMŮ

Cílem analýzy bude identifikovat společné komponenty datového úložiště pro řešení ERP předepisování a výdeje LP a Hlášení výdejů LP, odhalit úzká místa stávajícího řešení a provést jejich rekonfiguraci nebo je nahradit novým řešením, které povede k plné funkčnosti řešení ve stávajícím prostředí zadavatele.
Splnit požadavky vyplývající z protokolu inspektora ÚOOÚ sp.zn. INSP2-0277/09-40, viz Protokol__inspektora_ÚOOÚ, rozhodnutí předsedy ÚOOÚ sp.zn. INSP2-0277/09-62, viz Rozhodnutí_předsedy_ÚOOÚ na oddělení ERP předepisování a výdeje LP a Hlášení výdejů LP do nezávislých celků tak, aby tyto systémy možné provozovat zcela odděleně.

4.8.1. ANALÝZA DATABÁZÍ A JEJICH DATOVÝCH STRUKTUR

Předmětem řešení tohoto bodu bude analýza stávajících instalací a konfigurací databází pro:

- Hlášení výdejů LP a kontroly výdeje OTC s omezením
- ERP pro předepisování a výdej LP

Bude provedena analýza datových struktur jednotlivých systémů včetně žurnálu komunikace a vazby mezi žurnálem a datovým úložištěm jednotlivých systémů. Bude provedena analýza ostatních databázových objektů, které mají vliv na požadovaný výkon.

4.8.2. NÁVRH A PROVEDENÍ ZMĚN

Cílovým stavem navržených a provedených změn budou oddělená datová úložiště, zajištěno zpracování požadovaného počtu záznamů za 1 hodinu a to 15 mil. zpracovaných vět – čtení a zápisy. Bude provedena optimalizace datové struktury žurnálu komunikace s ohledem na pravidelnou

archivaci a vazby na data Hlášení výdejů LP a předepisování a výdeje LP. Bude provedena optimalizace umístění databázových objektů.
Databáze budou nadále provozovány s využitím technologie Oracle DataGuard.

Na základě výsledku analýzy z předchozího bodu a návrhu nového optimalizovaného datového rozhraní bude navrženo a následně provedeno oddělení společných komponent ERP předepisování a výdejů LP a Hlášení výdejů LP do samostatných datových úložišť na úrovni samostatných databází, bude provedena optimalizace datové struktury úložiště dat s ohledem na maximální výkon při čtecích a zápisových operacích. U ostatních databázových objektů bude provedena jejich revize a případná optimalizace. Navržené změny budou provedeny s ohledem na stávající úložiště a provozovaný sběr dat Hlášení výdejů LP, aby byla zachována jejich funkčnost.

4.8.3. ANALÝZA A REKONFIGURACE DATABÁZOVÝCH SYSTÉMŮ HLÁŠENÍ VÝDEJŮ LP

4.8.3.1. ANALÝZA STÁVAJÍCÍHO STAVU KONFIGURACE

Předmětem řešení tohoto bodu bude analýza stávajícího stavu řešení datových úložišť:

- instalace a konfigurace databáze pro sběr dat Hlášení výdejů LP a kontroly výdejů OTC s omezením
- instalace a konfigurace databáze žurnálu komunikace se subjekty vydávajícími léčivé přípravky

4.8.3.2. NÁVRH A PROVEDENÍ ZMĚN

Veškeré provedené změny budu realizované s ohledem na existující systémy tak, aby byla zachována jejich plná funkčnost a dostupnost. Některé části budou nahrazeny řešením, které plně nahradí původní část.

4.8.3.3. HLÁŠENÍ VÝDEJŮ LP A KONTROLA VÝDEJŮ OTC S OMEZENÍM

Na základě výsledku analýzy datové struktury databáze Hlášení výdejů LP a návrhu nového optimalizovaného datového rozhraní pro zpracování Hlášení výdejů LP, bude proveden návrh změn, úprav a samotné provedení rekonfigurace databázové struktury a ostatních databázových objektů Hlášení výdejů LP. Uvedené změny zajistí vysokou dostupnost dat a zpracování požadovaného objemu zpráv za definovaný časový interval ve spojení s aplikační logikou realizovanou formou ESB služeb. Cílem úprav je dosáhnutí minimálně stanovených hodnot jak v počtu databázových operací, tak v počtu zpracovaných zpráv za hodinu.

Bude upravena datová struktura a další databázové objekty. Tyto změny zajistí ukládání a čtení dat v novém rozhraní se zpětnou kompatibilitou s aktuální verzí rozhraní.

Upravená datová struktura bude navržena a realizována s důrazem na optimalizaci počtu čtecích a zápisových operací. Bude provedeno sjednocení typů a formátů databázových položek, optimalizace vazeb a identifikátorů jednotlivých záznamů. Maximálně bude využit generovaný identifikátor UUID bez nutnosti použití dalšího generátoru sekvencí. Jednotlivé použité principy a realizované úpravy budou znovupoužitelné pro ostatní části díla.

Datová struktura a nová aplikační logika ESB služeb bude navržena tak, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu a zpracování 15 mil. databázových záznamů za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Pro identifikaci pacienta, v případě že bude požadován, bude navržen nový pseudonymizovaný identifikátor a datová struktura pro jeho ukládání. Ta umožní přechod z identifikace číslem pojištěnce

na jiný typ identifikátoru bez ztráty informace o vazbě na pacienta nebo nutnosti použití více typů identifikátorů současně v jedné datové větě.

Bude dodána nová datová struktura pro ukládání a kontroly výdeje OTC s omezením a aktivována podle potřeb zadavatele. Nová struktura bude zajišťovat evidenci vydaných OTC s omezením na pacienta, časové období a množství léčivé látky. Součástí bude i datová struktura pro příslušné číselníky pro kontroly výdeje OTC s omezením.

Vývoj nové databázové struktury spolu s novým rozhraním bude umožňovat zpracování dat rozhraní ve více verzích na základě jmenného prostoru uvedeného v XML zasílaných datech zpráv. Aplikační logika tímto bude umožňovat paralelní provoz více verzí současně. Pro přístup k datům uloženým ve starších verzích datové struktury budou dostupné příslušné funkce, včetně funkce na zjištění verze, ve které jsou data uložena. Informace o verzi záznamu budou součástí datové struktury příslušné věty.

Veškeré chybové stavy, ke kterým bude při komunikaci externího subjektu s úložištěm docházet, budou uložené v nově navržené datové struktuře databáze. Tyto informace budou dostupné pro využití provozovatelem aplikace. Data budou uložena ve struktuře s identifikátorem pracoviště, které data zaslalo a s identifikátorem chyby, která nastala. Bude umožněno analyzovat příčiny odmítání zasílaných dat a komunikovat s externími subjekty a řešit problémy nevalidních dat.

4.8.3.4. ŽURNÁL KOMUNIKACE EXTERNÍCH SUBJEKTŮ A ÚLOŽIŠTĚ

Na základě výsledku analýzy datové struktury žurnálu komunikace externích subjektů a úložiště dat, bude proveden návrh změn a úprav datové struktury. Po provedené optimalizaci a návrhu bude realizováno samotné provedení úprav datové struktury žurnálu, která zajistí vysokou dostupnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

Datová struktura a nová aplikační logika bude navržena s důrazem na optimalizaci počtu zápisových operací do žurnálu, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu a zpracování 15 mil. databázových záznamů za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Aplikační logika žurnálovací ESB služby bude pouze nepřetržitě zapisovat do úložiště žurnálu bez možnosti čtení dat.

Aplikační logika a nově navržená datová struktura bude podporovat průběžnou archivaci dat žurnálu bez vlivu na její provoz. Bude maximálně optimalizována na výkon a dostupnost. Datová struktura žurnálu bude navržena tak, že bude složena z více sad databázových tabulek a dalších objektů, které umožní přepínání sad v reálném čase za provozu bez výpadku provozu. Aktivní sada bude sloužit pro ukládání dat žurnálu. Neaktivní sady s daty žurnálu budou off-line archivované. V případě potřeby přístupu k archivním datům žurnálu, budou data na vyžádání obnovena do databáze mimo aktivní datovou strukturu žurnálu a zpřístupněna pro práci.

4.8.4. ANALÝZA A REKONFIGURACE DATABÁZOVÝCH SYSTÉMŮ ERP PŘEDEPISOVÁNÍ A VÝDEJŮ LP

4.8.4.1. ANALÝZA STÁVAJÍCÍHO STAVU KONFIGURACE

Předmětem řešení tohoto bodu bude analýza stávajícího stavu řešení datových úložišť:

- instalace a konfigurace databáze pro ERP předepisování léčivých přípravků a výdeje léčivých přípravků na základě elektronického předpisu
- analýza stávajícího stavu řešení instalace a konfigurace databáze žurnálu komunikace se subjekty vydávajícími léčivé přípravky

4.8.4.2. NÁVRH A PROVEDENÍ ZMĚN

Veškeré provedené změny budu realizované s ohledem na existující systémy tak, aby byla zachována jejich plná funkčnost a dostupnost. Některé části budou nahrazeny řešením, které plně nahradí původní část.

4.8.4.3. ELEKTRONICKÉ RECEPTY, PŘEDEPISOVÁNÍ A VÝDEJ LÉČIVÝCH PŘÍPRAVKŮ

Na základě výsledku analýzy datové struktury databáze elektronických receptů, předepsaných a vydaných léčivých přípravků a návrhu nového optimalizovaného datového rozhraní pro zpracování ERP předepisování a výdeje LP, bude proveden návrh změn, úprav a samotné provedení rekonfigurace databázové struktury a ostatních databázových objektů databáze elektronických receptů. Uvedené změny zajistí vysokou dostupnost dat a zpracování požadovaného objemu zpráv za definovaný časový interval ve spojení s aplikační logikou realizovanou formou ESB služeb. Cílem úprav je dosáhnutí minimálně stanovených hodnot jak v počtu databázových operací, tak v počtu zpracovaných zpráv za hodinu.

Bude upravena datová struktura a další databázové objekty. Tyto změny zajistí ukládání a čtení dat v novém rozhraní se zpětnou kompatibilitou s aktuální verzí rozhraní.

Upravená datová struktura bude navržena a realizována s důrazem na optimalizaci počtu čtecích a zápisových operací. Bude provedeno sjednocení typů a formátů databázových položek, optimalizace vazeb a identifikátorů jednotlivých záznamů. Maximálně bude využit generovaný identifikátor UUID bez nutnosti použití dalšího generátoru sekvencí. Jednotlivé použité principy a realizované úpravy budou znovupoužitelné pro ostatní části díla.

Datová struktura a nová aplikační logika ESB služeb bude navržena tak, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu a zpracování 15 mil. databázových záznamů za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Pro identifikaci pacienta u elektronického receptu bude navržen nový pseudonymizovaný identifikátor a datová struktura pro jeho ukládání. Ta umožní přechod z identifikace číslem pojištěnce na jiný typ identifikátoru bez ztráty informace o vazbě na pacienta nebo nutnosti použití více typů identifikátorů současně v jedné datové větě.

Vývoj nové databázové struktury spolu s novým rozhraním bude umožňovat zpracování dat rozhraní ve více verzích na základě jmenného prostoru uvedeného v XML zasílaných datech zpráv. Aplikační logika tímto bude umožňovat paralelní provoz více verzí současně. Pro přístup k datům uloženým ve starších verzích datové struktury budou dostupné příslušné funkce, včetně funkce na zjištění verze, ve které jsou data uložena. Informace o verzi záznamu budou součástí datové struktury příslušné věty.

Veškeré chybové stavy, ke kterým bude při komunikaci externího subjektu s úložištěm docházet, budou uložené v nově navržené datové struktuře databáze. Tyto informace budou dostupné pro využití provozovatelem aplikace. Data budou uložena ve struktuře s identifikátorem pracoviště, které data zaslalo a chyby, která nastala. Bude umožněno analyzovat příčiny odmítání zasílaných dat a komunikovat s externími subjekty a řešit problémy nevalidních dat.

4.8.4.4. ŽURNÁL KOMUNIKACE EXTERNÍCH SUBJEKTŮ A ÚLOŽIŠTĚ

Na základě výsledku analýzy datové struktury žurnálu komunikace externích subjektů a úložiště dat, bude proveden návrh změn a úprav datové struktury. Po provedené optimalizaci a návrhu bude realizováno samotné provedení úprav datové struktury žurnálu, která zajistí vysokou dostupnost a zpracování požadovaného objemu zpráv za definovaný časový interval.

Datová struktura a nová aplikační logika bude navržena s důrazem na optimalizaci počtu zápisových operací do žurnálu, aby optimalizovala komunikaci s databází a umožnila zpracování požadovaného počtu 800 tisíc zpráv za hodinu a zpracování 15 mil. databázových záznamů za hodinu. Pro komunikaci s databází bude použit standardizovaný framework, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databáze.

Aplikační logika žurnálovací ESB služby bude pouze nepřetržitě zapisovat do úložiště žurnálu bez možnosti čtení dat.

Aplikační logika a nově navržená datová struktura bude podporovat průběžnou archivaci dat žurnálu bez vlivu na její provoz. Bude maximálně optimalizována na výkon a dostupnost. Datová struktura žurnálu bude navržena tak, že bude složena z více sad databázových tabulek a dalších objektů, které umožní přepínání sad v reálném čase za provozu bez výpadku provozu. Aktivní sada bude sloužit pro ukládání dat žurnálu. Neaktivní sady s daty žurnálu budou off-line archivované. V případě potřeby přístupu k archivním datům žurnálu, budou data na vyžádání obnovena do databáze mimo aktivní datovou strukturu žurnálu a zpřístupněna pro práci.

5. SERVISNÍ SMLOUVA / ZÁRUKY

5.1. ROZŠÍŘENÍ HARDWARE DATOVÉHO CENTRA

5.1.1. ZÁRUKA/ODSTRANĚNÍ ZÁVADY

Garantované požadavky Uchazeče na nově dodávanou technologii

- Uchazeč poskytne Zadavateli po dobu trvání podpory všechny relevantní SW „záplaty“, změny a verze, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad. Uchazeč se zároveň zavazuje informovat Zadavatele o nových SW verzích a funkčnostech, které mohou rozšiřovat dodané řešení způsobem, který Zadavatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Uchazeč se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- Uchazeč je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem zařízeni tak, aby v případě závady na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit bylo možné eskalovat závadu přímo k výrobci zařízení. Zároveň je Uchazeč povinen zajistit Zadavateli přistup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
- Uchazeč je povinen zajistit opravu pro dodané řešení za podmínek specifikovaných Zadavatelem v režimu 24x7x4 (počet hodin dostupnosti podpory uchazeče x počet dní v týdnu dostupnosti podpory uchazeče x doba pro odstranění zjištěné závady od nahlášení) nejméně po dobu 3 let.
- Výše specifikovanou podporu a dostupnost náhradních dílů Zadavatel požaduje nejméně po dobu 5 let.
- Záruka na HW a SW nejméně 3 roky (od výrobce)
- Při reklamačním procesu zůstává vadné zboží u zákazníka
- Bezplatný přístup k novým verzím firmware nejméně po dobu 3 let
- Řešení složitějších technických problému v češtině pomocí lokálního partnera výrobce nabízených technologií

5.2. ROZŠÍŘENÍ SOFTWARE DATOVÉHO CENTRA

5.2.1. ZÁRUKA/SERVIS SERVERY, DISKOVÉ POLE

Na nově dodávané komponenty (servery, diskové pole) splňujeme následující požadavky:

- záruka na HW 3 roky (od výrobce)
- řešení reklamace 24x7x4 (služba od výrobce), odstranění závady do 4 hodin od nahlášení po dobu záruky
- bezplatný přístup k novým verzím firmware a ovladačům
- řešení složitějších technických problému v češtině

5.2.2. ZÁRUKA SW PRO MONITORING DISKOVÝCH POLÍ

Na nově dodávaný SW pro monitoring diskových polí splňujeme následující požadavky:

- záruka na SW 3 roky (od výrobce)
- bezplatný přístup k novým verzím SW po dobu 3 roků

5.2.3. ZÁRUKA SW VMWARE

Na nově dodávaný SW VMware splňujeme následující požadavky:

- záruka na SW 3 roky (od výrobce)
- bezplatný přístup k novým verzím SW po dobu 3 roků

5.3. OSTATNÍ

Součástí servisního poplatku je i zajištění servisních služeb a plánovaného servisu v počtu 50 hodin měsíčně po dobu 36 měsíců. Servisní činnosti mohou být využívání na následující činnosti, technologie:

- Programátorské činnosti, rozšíření funkcionalit Sonic ESB

- Konfigurace, údržba a podpora systémů pro sběr dat . Zejména se jedná o technologie: Linux, Oracle, VMware, CISCO, Microsoft a Sonic ESB.

6. CELKOVÁ KONCEPCE ŘEŠENÍ

Informace pro posouzení celkové koncepce řešení.

6.1. UCELENOST KONCEPCE

Stávající komunikační infrastruktura SÚKL je budována modulárně, takže se skládá z různých funkčních bloků, které na sebe navzájem navazují. Tyto bloky potom mohou být navrhovány samostatně a propojovány navzájem. Tento postup umožňuje velkou flexibilitu a škálovatelnost při budoucím rozšiřování sítě.

Pro připojování externích subjektů je v komunikační infrastruktuře SÚKL realizován speciální blok se záměrem zabezpečovat vzdálené připojování externích subjektů ke zdrojům SÚKL. Tento blok v současné době umožňuje zakončování IPSec VPN připojení. V tomto projektu bude dle našeho návrhu rozšířen o možnost zakončování SSL spojení z externích subjektů na SÚKL , bude tedy zachována primární funkce tohoto bloku, a sice vzdálené připojování externích subjektů ke zdrojům SÚKL. Řešení zakončování SSL spojení bylo navrženo s ohledem na zajištění co největší podobnosti se systémem zakončování IPSec VPN směrem k dalším systémům SÚKL (firewally, GTW systémy, loadbalancing) a z toho vyplývající minimalizace případných dalších modifikací v navazujících blocích komunikační infrastruktury SÚKL.

Jak už bylo zmiňováno dříve, stávající komunikační infrastruktura SÚKL je budována modulárně, aby dané bloky potom mohly být navrhovány samostatně a propojovány navzájem. Díky tomu je možné doplnit komunikační infrastrukturu o blok sloužící pro loadbalancing externích, i interních systémů SÚKL. Díky schopnosti virtualizace modulů ACE je možné nasadit loadbalancer na kterémkoliv místě komunikační infrastruktury SÚKL.

Nabízené moduly pro rozšíření stávajících centrálních prvků přesně odpovídají specifikaci a jsou 100% kompatibilní se stávajícími centrálními prvky komunikační infrastruktury SÚKL, a díky tomu je zajištěn soulad s celkovou koncepcí řešení.

Nabízené přepínače pro stávající bladové chassis Dell umožňují implementaci sofistikovaných technologií pro zajištění vysoké dostupnosti a výkonnosti komunikační infrastruktury sloužící pro připojování serverů. Zajištění vysoké dostupnosti a výkonnosti komunikační infrastruktury pro připojování serverů je nezbytné z hlediska zajištění správného fungování všech stávajících i nově implementovaných systémů SÚKL.

Na zajištění bezpečné a spolehlivé emailové komunikace SÚKL s okolním světem plánujeme vytvoření nového logického bloku v rámci komunikační infrastruktury SÚKL. Tento systém bude plynule navazovat na interní groupware infrastrukturu komunikační infrastruktury SÚKL a společně tak vytvoří bezpečný a efektivní systém pro zajišťování emailové komunikace SÚKL.

Implementace sondy Invea Flowmon pro podrobný monitoring a vyhodnocování datových toků v rámci komunikační infrastruktury SÚKL je logickým doplněním bloku managementu komunikační infrastruktury SÚKL o nástroj, který je nezbytný pro zajištění bezpečnosti dat uložených na datových zdrojích SÚKL a zároveň pro zajištění správného fungování všech stávajících i nově implementovaných systémů SÚKL.

Ucelenost koncepce je zajištěna v rámci virtuální infrastruktury dodáním nového HW a SW, který je identický s již stávajícím a používaným HW a SW zadavatele. Dodávka všech součástí virtuální infrastruktury plně splňuje zadání výběrového řízení.

Navržené úpravy SW komponent zajistí celkové sjednocení použitých technologií, architektury, komunikačních rozhraní pro Hlášení výdejů LP a ERP předepisování a výdeje LP. Maximálně budou využity komponent infrastruktury zadavatele.

Vstupní brány pro přístup externích subjektů budou odděleny a nakonfigurovány samostatně pro obě aplikace. Budou využívat externí autentizační doménu OID pro autentizaci přistupujících subjektů. Vystavené komunikační rozhraní obou aplikací bude podporovat práci s více verzemi.

Aplikační logika obou aplikací bude umístěna a provozována na ESB formou ESB služeb. Nově dodané ESB služby budou použity pro obě aplikace. Jejich instance budou provozované zcela odděleně.

Databáze pro obě řešení budou mít shodně řešený návrh datové struktury. Shodné řešení bude použito i pro provoz a archivaci dat žurnálu.

6.2. BEZPEČNOST ŘEŠENÍ

Systém zakončování SSL bude umístěn v externí DMZ síti SÚKL paralelně k systému zabezpečování připojování pomocí IPSec VPN. Pro tuto DMZ síť jsou definována komunikační pravidla, která umožňují projít pouze žádoucí a přesně definované komunikaci. Dešifrovaný provoz ze vzdálených lokalit je potom ještě kontrolován IPS systémem instalovaným v centrálních firewallech ASA. Stejná politika bude aplikována i na provoz spojený s komunikací připojení pomocí SSL.
Aby bylo možné sestavit SSL tunel, bude koncový uživatel ověřován na základě osobního certifikátu vydaného některou z certifikačních autorit PKI hierarchie SÚKL (MZ), tím bude zajištěno, že pro uživatele bez platného certifikátu nebude možné SSL tunel navázat a platným certifikátem bude díky certifikační politice disponovat pouze oprávněný uživatel.

Bezpečnost řešení loadbalancingu externích a interních systémů SÚKL bude zajištěna díky konfiguraci vlastností virtualizace dodávaných modulů. Na kontext sloužící pro loadbalancing externích systémů SÚKL nebude možné se přihlásit přímo, tzv. inband, ale bude možné ho spravovat pouze out-of-band přístupem přes kontext administrativní. Přístup na tento administrativní kontext bude chráněn pomocí přesně definovaných komunikačních pravidel (odkud může administrátor přistupovat) a zároveň budou administrátorské účty ověřovány proti centrální databázi pomocí protokolu TACACS+. Na firewallech SÚKL budou dále definovaná komunikační pravidla, která umožní průchod pouze žádoucímu provozu.

Na dodávané karty do stávajících centrálních prvků bude aplikována konfigurace v souladu s bezpečnostními standardy platnými pro komunikační infrastrukturu SÚKL.

Na dodávané přepínače do stávajícího blade chassis DELL bude aplikována konfigurace v souladu s bezpečnostními standardy platnými pro zařízení fy Cisco instalovaná do komunikační infrastruktury SÚKL. Za všechna pravidla jmenujme například ověřování a logování administrátorský přístupů pomocí Serveru TACACS+.

Přes IronPort brány prochází v současné době přes 25% všech světových elektronických zpráv, používá je 8 z 10 největších ISP a více než 20% největších světových společností. Společnost Gartner označila IronPort jako vedoucí řešení pro bezpečnost elektronické pošty (Magický kvadrant email bezpečnosti pro rok 2006) a průzkum trhu společnosti IDC zařadil IronPort na první místo v email bezpečnostních zařízeních (IDC Security Appliance Tracker z července 2007). Zabezpečení elektronické pošty IronPort Email Security Appliance je v současnosti nejdokonalejší poštovní brána. Mnohé IronPort inovační technologie, jako je SenderBase, Virus Outbreak Filter nebo PostX, se staly pojmem a představují zlomové okamžiky ve vývoji email ochrany.

Invea FlowMon je kompletní řešení pro monitorování sítí na základě IP toků vyvinuté v České republice. Toto řešení založené na technologii NetFlow umožňuje úplný pohled na provoz v síti. Jedná se zejména o informace typu kdo, s kým, jak dlouho, jakým protokolem komunikoval a kolik přenesl dat. Informace o datech zachycených sondou budou dále přeposílána do stávajícího bezpečnostního systému Cisco MARS. Tyto informace dávají podrobný obrázek o dění na síti a společně s informacemi z dalších zdrojů bezpečnostních informací v komunikační infrastruktuře SÚKL pomohou odhalovat a zabraňovat případným bezpečnostním incidentům a lépe ochránit data uložená v komunikační infrastruktuře SÚKL.

Bezpečnost SAN infrastruktury, blade serverů a diskových polí je zajištěna fyzickým oddělením od provozního prostředí. Také je VMware prostředí je zcela odděleno od provozního, s vlastními ESX servery a s vlastním vCenter serverem. Zálohování je také zcela fyzicky odděleno od provozního prostředí.

Navržená koncepce SW řešení umožní plně oddělit a provozovat aplikace pro sběr dat Hlášení výdejů LP a ERP předepisování a výdejů LP.

Shodná architektura obou aplikací umožní plně oddělit jejich jednotlivé logické vrstvy:

Vstupní brány a jejich přístupové body s autentizací budou umístěné v externí DMZ.
Aplikační logika bude umístěna na ESB sběrnici v ESB službách bez možnosti přímého přístupu externích subjektů a uživatelů z prostředí zadavatele v interní DMZ.
Úložiště dat bude umístěné v další oddělené DMZ a bude přístupné pouze ESB databázovým službám pro ukládání a čtení dat.

Pro obě aplikace bude platit, že:
Vzdálený přístup a komunikace s rozhraním prostřednictvím veřejné datové sítě bude zajištěna šifrovaným spojením na úrovni VPN tunelu nebo pomocí protokolů HTTPS a SSL.
Aplikace budou provozovány se zapojením autentizace na vstupních branách a s autorizací na úrovni ESB služeb. Autentizace zasílajícího bude ověřovat, že ten kdo zasílá požadavek je opravdu ten, za koho se vydává a to podle jeho jméno a heslo. Neautentizovaný uživatel bude vždy odmítnut již na vstupu. Autorizace přístupu bude ověřovat, že autentizovaný odesilatel zasílá údaje za lékárnu a konkrétní pracoviště, za které je může zasílat. Obdobně bude probíhat autorizace pro přístup lékaře.
Veškerá komunikace mezi externím subjektem a aplikacemi bude žurnálovaná. Každý požadavek bude uložen do žurnálu v podobě, ve které byl zaslán. Na každý požadavek bude zaslána odpověď, která bude rovněž uložená do žurnálu komunikace. Žurnál komunikace bude pravidelně archivován. V případě řešení bezpečnostních incidentů bude zadavateli obnoven a zpřístupněn.

6.3. OTEVŘENOST ŘEŠENÍ

Systém pro zakončování SSL je možné konfigurovat tak, aby poskytoval SSL offload i pro jinou komunikaci, nejenom pro systém sběru dat. Díky podpoře otevřených standardů v navrhovaném řešení, je toto řešení otevřené pro napojení různých systémů SÚKL.

Řešení pro loadbalancing externích i interních systémů SÚKL podporuje téměř nepřebernou spoustu testovacích metod „zdraví“ serverů a díky tomu je možné nasadit ho na loadbalancing téměř jakéhokoliv systému. Díky tomu je toto řešení otevřené pro napojení různých systémů SÚKL.

Po rozšíření centrálních prvků o navrhované moduly bude možné připojování nových zařízení do komunikační infrastruktury jak rychlostí 1Gbps, tak rychlostí 10Gbps. Díky tomu je toto řešení otevřené a velmi flexibilní pro napojování různých systémů SÚKL.

Díky rozšíření stávajícího chassis DELL o navrhované přepínače Cisco Catalyst bude možné dále velice rychle a efektivně rozvíjet informačný systémy SÚKL díky značnému zjednodušení připojení serverů do komunikační infrastruktury SÚKL. Díky vlastnostem tohoto řešení dosáhneme velké flexibility dosažitelných konfigurací síťové infrastruktury serverů. Díky podpoře otevřených standardů je toto řešení otevřené a velmi flexibilní pro napojování různých systémů SÚKL.

Podpora industry standardů podporovaných v navrhovaném řešení pro zabezpečení emailové komunikace umožňuje kompatibilitu se všemi systémy používající protokol SMTP a zároveň nabízí potřebnou otevřenost pro rozvoj informačních systémů a technologií SÚKL.

Díky podpoře otevřených standardů v použitém řešení pro monitoring síťových toků je možné toto řešení integrovat s různými dalšími bezpečnostními nástroji, nebo jinými informačními systémy SÚKL.
Vzhledem k použití virtualizačního řešení společnosti VMware a blade šasi DELL je dané řešení plně otevřené dalšímu rozšiřování ve všech směrech. Nezávislost na platformě a otevřené standardy nabízejí větší vzájemnou slučitelnost a flexibilitu při vytváření sdílených fondů prostředků nezávislých na konkrétních platformách OS a hardwaru. Stávající blade šasi DELL je stále možné dále jednoduše rozšířit o další blade servery a jejich zapojení do stávajícího clusteru.

Návrh, rekonfigurace, oddělení a dodávka nových komponent SW části řešení aplikace pro sběr dat Hlášení výdejů LP a ERP předepisování a výdejů LP, založené na architektuře orientované na služby s maximálním využitím ESB služeb, použití XML komunikačního formátu a řešení pro zpracování více verzí komunikačního rozhraní, zajistí otevřenost řešení pro další rozšíření a napojení na další systémy.

Řešení bude možné rozšiřovat na všech jeho úrovních:
Vstupní brány bude možné nadále posilovat o další instalace Actional Intermediary a SonicMQ a zařazovat za HW balancer, který na ně rozkládá zátěž. Případně bude možné přidávat další typy komunikačních protokolů a přístupových bodů, na kterých budou služby dostupné.

Na úrovni ESB sběrnice bude možné přidávat další ESB služby podle potřeby zadavatele nebo legislativních změn a zapojovat je to procesů zpracování dat. Bude možné se napojovat na další systémy a zdroje dat zadavatele apod.

Datové úložiště bude rozšiřitelné podle potřeby včetně možnosti následného vytěžování a zpracování dat pro potřeby zadavatele a jeho další agendy.

6.4. PROCESNÍ KONTINUITA

Vzhledem k tomu, že se zde jedná o vytvoření nové, zcela nezávislé části síťového bloku sloužícího pro zabezpečování vzdáleného připojování externích subjektů ke zdrojům SÚKL, nedotkne se jeho budování nijak provozu na komunikační infrastruktuře SÚKL. Nasazení tohoto systému proběhne tedy zcela bez výpadku a za plného provozu všech součástí komunikační infrastruktury SÚKL.
V rámci implementace tohoto bloku bude nutné pouze modifikovat komunikační pravidla na stávajících centrálních firewallech SÚKL. Potřebná komunikační pravidla předem přesně specifikujeme, případně sami přímo nakonfigurujeme.

Nasazení loadbalancingu do komunikační infrastruktury SÚKL se bohužel neobejde bez krátkodobých výpadků systémů, na které se bude loadbalancing aplikovat, proto budeme samotnou instalaci tohoto systému provádět v předem dohodnutém čase. Nasazení loadbalancingu na interní systémy SÚKL je poměrně jednoduché. Zde bude výpadek v řádu sekund, kdy na úrovni prostředí VmWare dojde k přesunutí zainteresovaných serverů v rámci VmSwitche do jiné VLAN sítě. Po tomto úkonu bude funkce serverů obnovena v plném rozsahu. Následně se budou muset překonfigurovat systémy, které na dané servery komunikují, aby začaly používat jako cíl své komunikace VIP adresu ACE modulu. Na ACE modulu je pak komunikace jdoucí na tuto VIP adresu loadbalancována mezi skutečné servery. V transparentním režimu kontextu ACE může komunikace transparentně procházet i přímo na servery, takže výpadky budou minimální.

Nasazení loadbalancingu na externí systémy je o něco složitější, nicméně výpadek by také neměl přesáhnout řádů desítek sekund. Zde je nutné zajistit rychlý timeout ARP záznamů zainteresovaných systémů. Budou předem připraveny nové stroje, mezi které má být následně loadbalancován síťový provoz a rovněž konfigurace příslušného kontextu modulu ACE. Rozhraní modulu ACE bude ve stavu vypnuto. Jakmile potom dojde k vypnutí reálných serverů, bude zapnuto rozhraní modulu ACE a předem nakonfigurované VIP adresy budou odpovídat na dotazy na původní reálné servery.
Rozšíření centrálních prvků o karty pro připojování pomocí rychlostí 1Gbps a 10Gbps bude provedeno za plného provozu jak centrálních prvků, tak celé komunikační infrastruktury. Toto je možné díky tomu, jak dodávané moduly, tak centrální prvky podporují technologii hot-swap, kdy je možné vkládat a vyjímat moduly za plného provozu centrálního prvku (vyjma supervizoru).

Rozšíření blade chassis DELL bude provedeno rovněž za plného provozu, jak stávající komunikační infrastruktury, tak virtuálních serverů. Díky tomu, že v rámci datového centra SÚKL je používána virtualizace na platformě VmWare, dojde k přesunutí virtuálních serverů běžících na fyzickém serveru v bladovém chassis na jiné servery a celé bladové chassis bude možné v průběhu instalace přepínačů vypnout, aniž by uživatelé komunikační infrastruktury cokoliv zpozorovali.

Nasazení aplliancí IronPort proběhne bez zjevného výpadku, nebo nedostupnosti mailové komunikace. Několik dnů před plánovaným přepnutím na nový systém externí mailové komunikace SÚKL budou zřízeny MX záznamy v DNS s nižší prioritou, než tou, kterou má stávající externí emailový server. Jakmile bude připravené nastavení appliancí IronPort, na centrálním firewallu budou nakonfigurována komunikační pravidla tak, že bude povolena komunikace z interní exchange na appliance IronPort a zároveň bude povolena emailová komunikace z internetu směrem na tyto aplliance a zakázána SMTP komunikace na server stávající. Paralelně k těmto úkonům se překonfiguruje SMTP konektor na interní Exchange SÚKL tak, aby odchozí emaily posílal na aplliance IronPort. Uživatelé nezaznamenají žádný výpadek, pouze dojde ke zpoždění několika mailů, které se uchovají v odchozích frontách na příslušných serverech. Aby nemohlo dojít opravdu k žádnému výraznému omezení uživatelů, budeme provádět překlopení na tento systém v pozdních odpoledních hodinách.

Systém implementovaný pro monitoring datových toků v síti SÚKL je pro komunikační infrastrukturu SÚKL zcela transparentní, jeho instalace do komunikační infrastruktury tedy v žádném případě neovlivní chod komunikační infrastruktury. Drobným konfiguračním zásahem se pouze na 6 místech komunikační infrastruktury odkloní provoz na porty sondy. Samotná konfigurace Sondy nebude rovněž

mít na chod infrastruktury žádný vliv. Pro instalaci sondy budeme potřebovat dle našich instrukcí (případně nakonfigurujeme sami) na 6 specifikovaných místech odklonění provozu na sondu a dále pak přidělit IP adresu a konfiguraci portu pro management sondy.

Procesní kontinuita virtuální infrastruktury je opět zajištěna použitým virtualizačním řešením společnosti VMware. S pomocí výjimečných funkcí, jako je automatizované vyvažování zátěže a migrace virtuálních strojů v reálném čase, umožňuje technologie VMware organizacím prodloužit dobu provozuschopnosti a snížit náklady a složitost, které jsou zapotřebí k dosažení vysoké dostupnosti a možnostem zotavení po havárii. Veškeré činnosti spojené se zprovozněním daného řešení – hardwarové zapojení nových blade serverů, zapojení nových diskových polic pro stávající diskové pole, instalace a konfigurace software VMware a Navisphere Analyzer je možné provádět bez výpadku provozních systémů a je potřeba minimální součinnost s IT oddělením Zadavatele.

Návrh, rekonfigurace, oddělení a dodávka nových komponent SW části řešení aplikace pro sběr dat Hlášení výdejů LP a ERP předepisování a výdejů LP, bude využívat aktuálně instalované komponenty na vstupních branách, ESB sběrnici a databáze pro ukládání dat. Některé části, podle výsledků analýzy, budou rozděleny a instalovány odděleně. Nově budou nakonfigurovány služby pro nové verze rozhraní Hlášení výdejů LP a ERP předepisování a výdejů LP. Na tyto verze budou komunikující subjekty postupně přecházet. Aplikační servery pro zpracování ERP předepisování a výdej LP budou zrušeny a nahrazeny novou aplikační logikou umístěnou v ESB službách.
Nové instalované komunikační rozhraní bude zpětně kompatibilní s původním rozhraním a umožní externím subjektům zpřístupnit původní uložené záznamy. Nové rozhraní umožní práci s více verzemi a přístup ke starším uloženým datům. Přechod na novou verzi rozhraní bude řešen přechodným obdobím, po které budou dostupné obě verze bez nutnosti odstávky systému a přechodu na verzi novou.

Z pohledu zadavatele dojde k technologickému sjednocení řešení aplikací Hlášení výdejů LP a ERP předepisování a výdeje LP. Aplikace budou odděleny a provozovány samostatně od přístupových bodů až po datová úložiště.

Z pohledu externích subjektů dojde pouze k vydání nových verzí rozhraní a vystavení nových oddělených přístupových bodů.

6.5. KONCEPCE ZÁLOHOVÁNÍ A OBNOVY

Zařízení dodávaná pro zajištění zakončování SSL budou provozována v režimu vysoké dostupnosti Active/Active. Této funkcionality bude dosaženo díky konfiguraci virtualizace na těchto modulech. Pokud dojde k výpadku některého z dvojice hardwarových zařízení, převedou se jeho aktivní kontexty na zařízení druhé. Tím částečně klesne maximální výkon tohoto řešení, ale běžný uživatel tento výpadek vůbec nezaznamená. Díky tomu, že konfigurace těchto zařízení je vidět v čistém textu, bude tato konfigurace pravidelně automaticky zálohována na dohledový server Netprosys a v případě hardwarové poruchy může být následně velmi rychle a snadno obnovena na náhradní modul.

Zařízení dodávaná pro zajištění zakončování loadbalancingu externích i interních systémů SÚKL budou provozována v režimu vysoké dostupnosti Active/Active. Této funkcionality bude dosaženo díky konfiguraci virtualizace na těchto modulech. Pokud dojde k výpadku některého z dvojice hardwarových zařízení, převedou se jeho aktivní kontexty na zařízení druhé. Tím částečně klesne maximální výkon tohoto řešení, ale běžný uživatel tento výpadek vůbec nezaznamená. Díky tomu, že konfigurace těchto zařízení je vidět v čistém textu, bude tato konfigurace pravidelně automaticky zálohována na dohledový server Netprosys a v případě hardwarové poruchy může být následně velmi rychle a snadno obnovena na náhradní modul.

Rozšíření stávajících centrálních prvků bude provedeno tak, aby bylo dosaženo zajištění vysoké dostupnosti v komunikační infrastruktury SÚKL. Dodávané karty budou instalovány do obou centrálních prvků a to tak, že do každého centrálního prvku bude zasunuta jedna nová karta pro rychlostí 10Gbps a jedna nová karta pro připojování rychlostí 1Gbps. Připojovaná zařízení (přepínače, servery) budou potom připojovány duálně do obou centrálních prvků. Pokud tedy dojde k poruše karty, nebo celého centrálního prvky, vždy ještě existuje cesta záložní, po které bude probíhat síťová komunikace. Pokud dojde k poruše karty, je možné tuto kartu za běhu systému vyměnit a na novou se automaticky uplatní konfigurace karty původní (pokud je zasunuta do stejného slotu).

Pro případ výpadku celého zařízení budou konfigurace pravidelně automaticky zálohovány na dohledový server Netprosys. Z těchto záloh bude potom možné velice rychle nahrát potřebnou konfiguraci do vyměněného centrálního prvku.

Přepínače dodávané do stávajícího blade chassis DELL budou sestohovány do jednoho logického celku. Takto vytvořený celek bude pomocí technologie cross stack etherchannell připojen jak ke komunikační infrastruktuře, tak k jednotlivým serverů v chassis. Konfigurace tohoto logického celku bude pravidelně automaticky zálohována na dohledový server Netprosys. Díky použité architektuře je však velmi nepravděpodobné, že by tato konfigurace byla někdy potřeba, protože v případě výpadku některého z fyzických přepínačů, pořád ještě bude existovat odchozí cesta pro síťový provoz a po výměně za přepínač náhradní se tento automaticky zařadí do stohu a převezme funkci a konfiguraci přepínače původního. Konfigurace by byla potřeba pouze v případě, že by došlo k poruše všech přepínačů v chassis současně, což je poměrně nepravděpodobné.

Dodávaný systém pro zabezpečení externí emailové komunikace je navržen a realizován jako plně redundantní. Redundance je zajišťována pomocí vlastností emailové komunikace a DNS. Pro doménu sukl.cz budou zřízeny dva MX záznamy pro příjem pošty. Pokud se vzdálené emailové bráně nepodaří připojit na port TCP/25 na stroj, kam ukazuje primární MX záznam, zkusí připojení na stroj, který je uveden v sekundárním MX záznamu. Tak je v případě výpadku některého zařízení v clusteru zajištěno kontinuální fungování emailové komunikace.
Konfigurace emailových bran bude pravidelně zálohována helpdeskem Netprosys, aby bylo možné do případné vyměněné brány pomocí nástrojů v appliance IronPort naimportovat rychle konfiguraci appliance původní.

Systém implementovaný pro monitoring datových toků v síti SÚKL je pro komunikační infrastrukturu SÚKL zcela transparentní a jeho případný výpadek neohrozí chod žádného z klíčových systému komunikační infrastruktury SÚKL, proto toto řešení nebylo (v souladu se zadávací dokumentací) koncipováno jako redundantní. Pro co nejrychlejší obnovu činnosti tohoto systému bude při implementaci zhotovena speciální dokumentace, která bude popisovat postup v případě konfigurace náhradního zařízení. Tato dokumentace bude rovněž popisovat konkrétní hodnoty nastavené v instalovaném zařízení.

Z hlediska bezpečnosti a rychlosti obnovy byl navržen dvoustupňový zálohovací systém. V tomto případě jsou data nejdříve zálohována na kapacitní diskové pole, které je připojeno k zálohovacímu serveru a následně duplikována na páskovou knihovnu. Díky prvotní záloze na diskové pole jsou data nejen velmi rychle zálohována, ale především je možno je velmi rychle obnovit.

Pro zálohování navrhujeme využít možnosti virtualizačního řešení a to zálohování celých virtuálních strojů - možnost zálohovat celý server bez ohledu na instalované aplikace a obsah. Tato funkcionalita také umožní využít SAN infrastrukturu, čímž zálohovací procesy nijak neovlivňují chod a výkon daných virtuálních strojů.

Vzhledem k požadavku vysoké dostupnosti nově vytvořených DB systémů, navrhujeme jejich zálohování řešit tak, že časově a objemově náročné datové zálohy na úrovni ORACLE db budou probíhat na RO databázi a tím nebude omezen výkon primární ORACLE DB zajišťující datové operace v režimu 24x7.

6.6. ARCHITEKTURA ŘEŠENÍ

Navrhované řešení zakončování SSL podporuje otevřené standardy, které jsou platné pro všechna vyráběná síťová zařízení, tato skutečnost sama o sobě zajišťuje kompatibilitu se stávající komunikační infrastrukturou SÚKL. Navrhované zařízení je navíc od stejného výrobce (Cisco), jako stávající zařízení tvořící síťovou část komunikační infrastruktury SÚKL a díky této skutečnosti je kompatibilita zaručena na 100%.

Navrhované řešení pro loadbalancing externích a interních zdrojů SÚKL podporuje otevřené standardy, které jsou platné pro všechna vyráběná síťová zařízení, tato skutečnost sama o sobě zajišťuje kompatibilitu se stávající komunikační infrastrukturou SÚKL. Navrhované zařízení je navíc od stejného výrobce (Cisco), jako stávající zařízení tvořící síťovou část komunikační infrastruktury SÚKL a díky této skutečnosti je kompatibilita zaručena na 100%.

Dodávané moduly do centrálních prvků komunikační infrastruktury SÚKL podporuje otevřené standardy, které jsou platné pro všechna vyráběná síťová zařízení, tato skutečnost sama o sobě

zajišťuje kompatibilitu se stávající komunikační infrastrukturou SÚKL. Navrhované zařízení je navíc od stejného výrobce (Cisco), jako stávající zařízení tvořící síťovou část komunikační infrastruktury SÚKL a díky této skutečnosti je kompatibilita zaručena na 100%.

Dodávané přepínače pro rozšíření stávajícího chassis DELL podporují otevřené standardy, které jsou platné pro všechna vyráběná síťová zařízení, tato skutečnost sama o sobě zajišťuje kompatibilitu se stávající komunikační infrastrukturou SÚKL. Navrhované zařízení je navíc od stejného výrobce (Cisco), jako stávající zařízení tvořící síťovou část komunikační infrastruktury SÚKL a díky této skutečnosti je kompatibilita zaručena na 100%.

Díky podpoře otevřených standardů a standardů platných pro systémy používající SMTP v navrhovaném systému pro zabezpečení externí emailové komunikace, je zajištěna kompatibilita navrhovaného řešení se stávajícími systémy komunikační a groupware architektury SÚKL.

Navrhované řešení pro monitorování datových toků je transparentní ke stávající komunikační infrastruktuře, tím pádem nemůže v žádném případě negativně, nebo jinak ovlivnit chování komunikační infrastruktury SÚKL. Navrhované řešení podporuje otevřené standardy, které jsou platné pro všechna vyráběná síťová zařízení, tato skutečnost zajišťuje kompatibilitu se stávající komunikační infrastrukturou SÚKL.

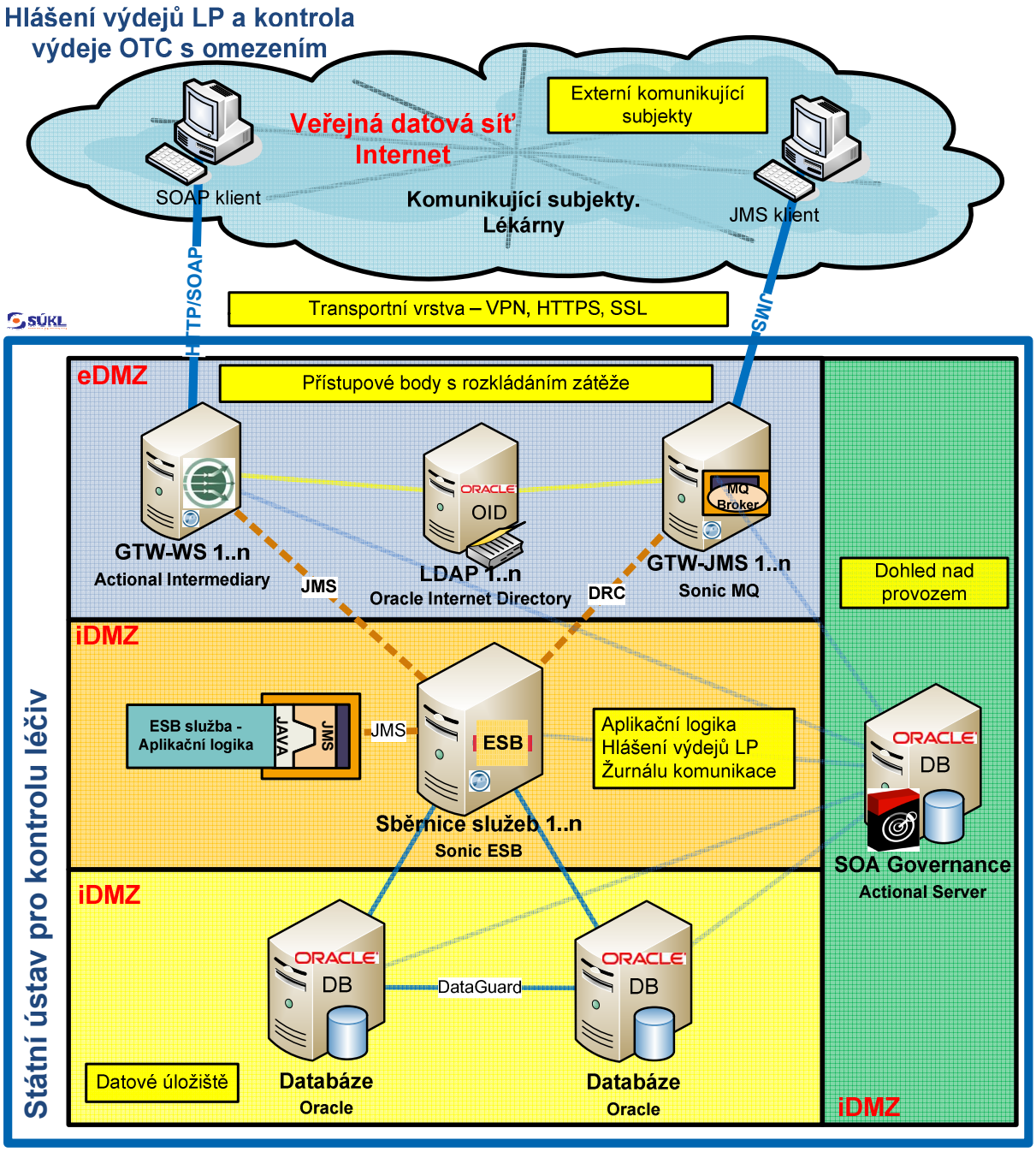
Celková architektura virtuální infrastruktury kopíruje stávající řešení infrastruktury zadavatele. Veškeré komponenty – dodávané diskové police, blade servery, virtualizační a monitorovací software – vše použité v navrhovaném řešení je 100% kompatibilní se stávající infrastrukturou zadavatele.

Základem koncepce SW části řešení aplikace pro sběr dat Hlášení výdejů LP a ERP předepisování a výdejů LP, je využití principů architektury orientované na služby. Celý systém bude složen z komponent – služeb, které plní konkrétní úkoly v procesu zpracování dat.
Celý systém bude rozdělen na logické oddělené vrstvy:
Vstupní brány umístěné v externí DMZ pro přístup externích subjektů.
ESB sběrnice pro provoz ESB kontejnerů s aplikační logikou pro zpracování dat složenou z ESB služeb řazených do procesů.

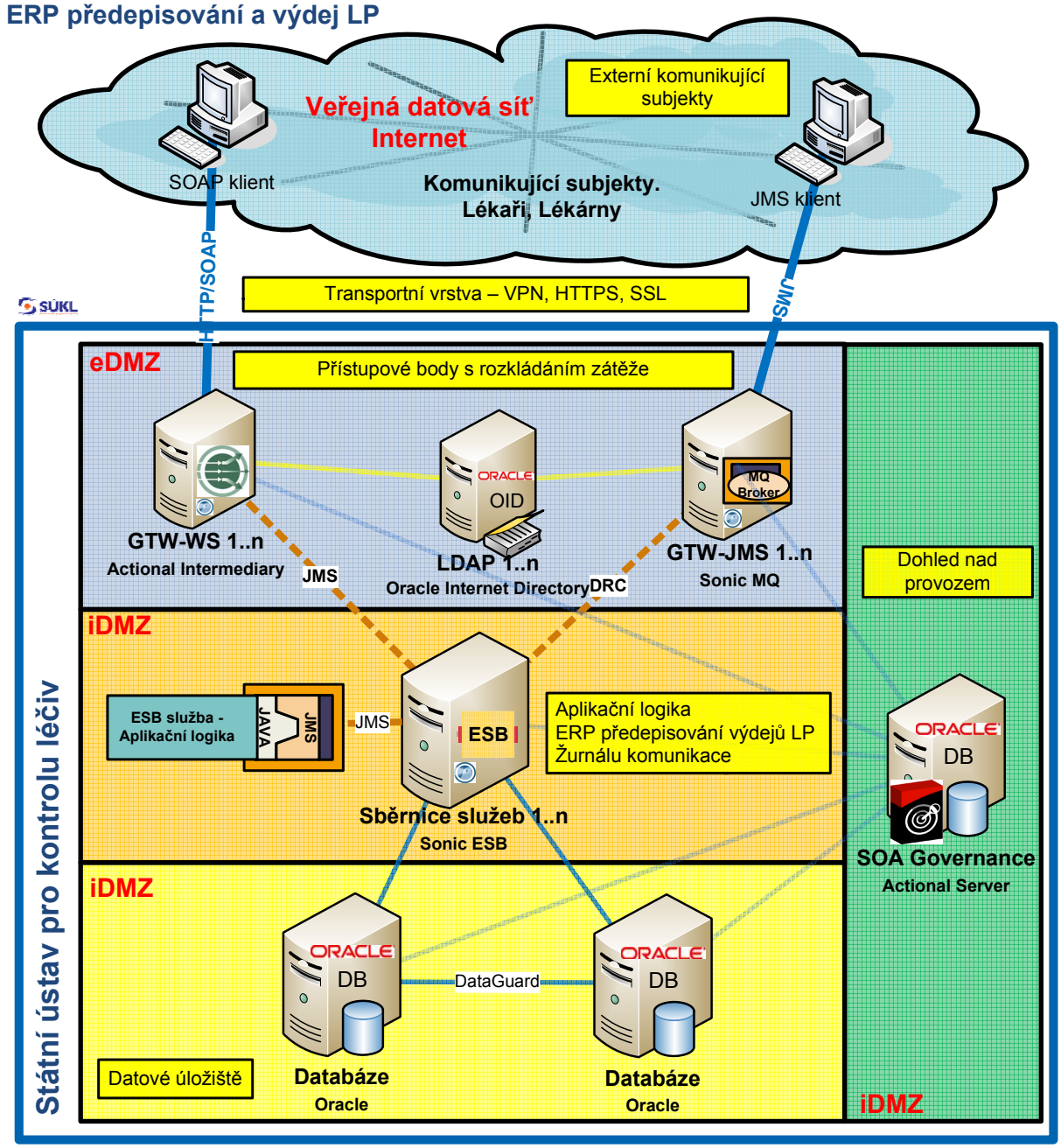
Datová úložiště pro ukládání aplikačních dat a dat žurnálu komunikace externích subjektů a úložiště. Každý celek bude umístěn v samostatné DMZ. Spojení vstupních bran a ESB sběrnice bude realizováno JMS komunikací. Spojení mezi ESB databázovými službami a databázemi bude realizováno JDBC spojením za použití standardizovaného frameworku, který zajistí bezproblémovou a optimalizovanou komunikaci Java aplikační logiky a Oracle databází.
Architektura softwarového řešení aplikační logiky obou systémů, jak pro sběr dat Hlášení výdejů LP, tak pro ERP předepisování a výdejů LP, bude založená na použití samostatných nezávislých služeb, skládaných do procesů. Tento princip zajišťuje znovupoužitelnost vyvinutých služeb, minimalizaci chyb a optimalizaci na maximální výkon celého systému.

Oddělené komponenty a logické vrstvy řešení pro sběr dat Hlášení výdejů LP a ERP předepisování a výdejů LP budou identické.

Obr.: Architektura aplikace pro sběr dat Hlášení výdejů LP

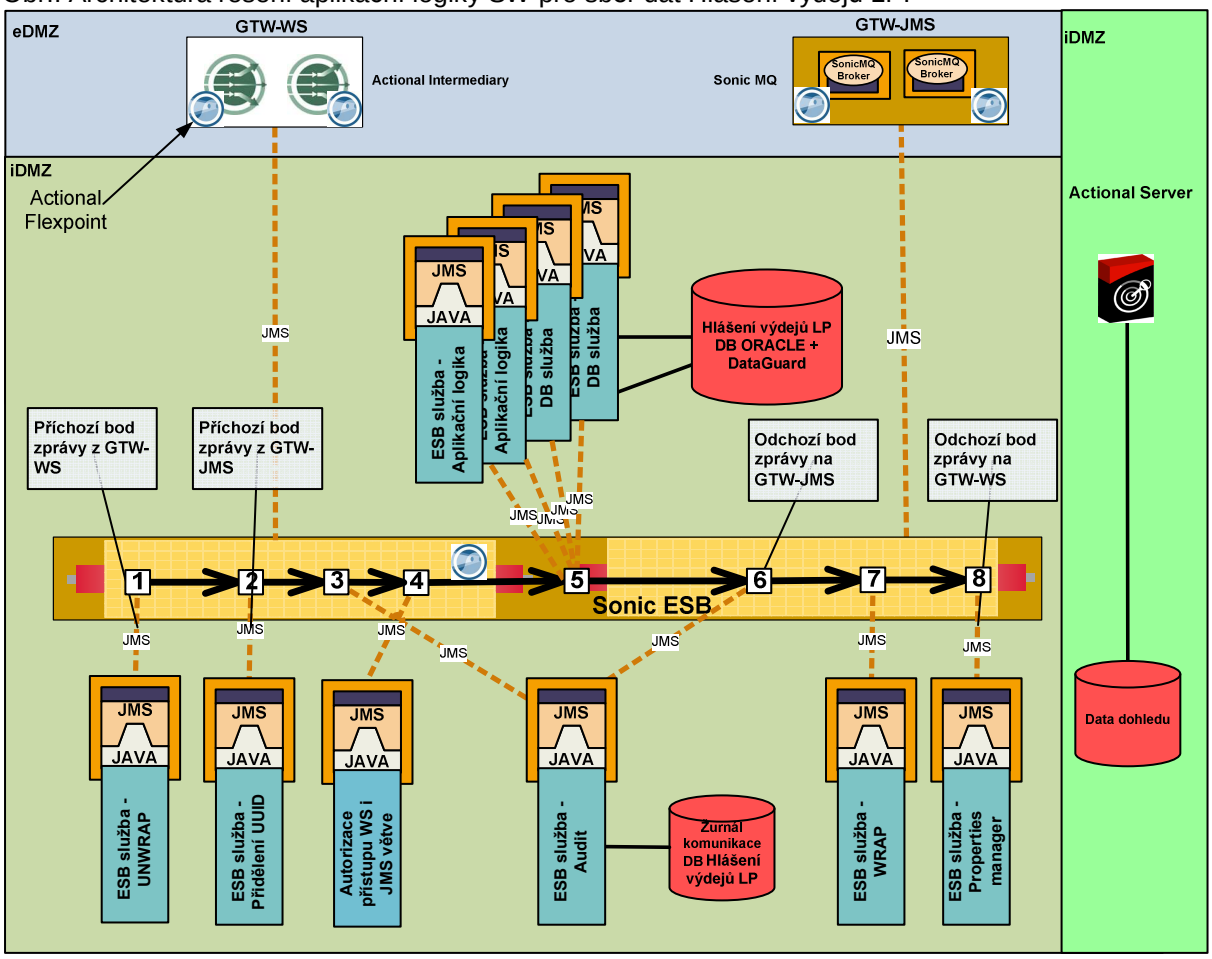


Obr.: Architektura aplikace ERP předepisování a výdejů LP

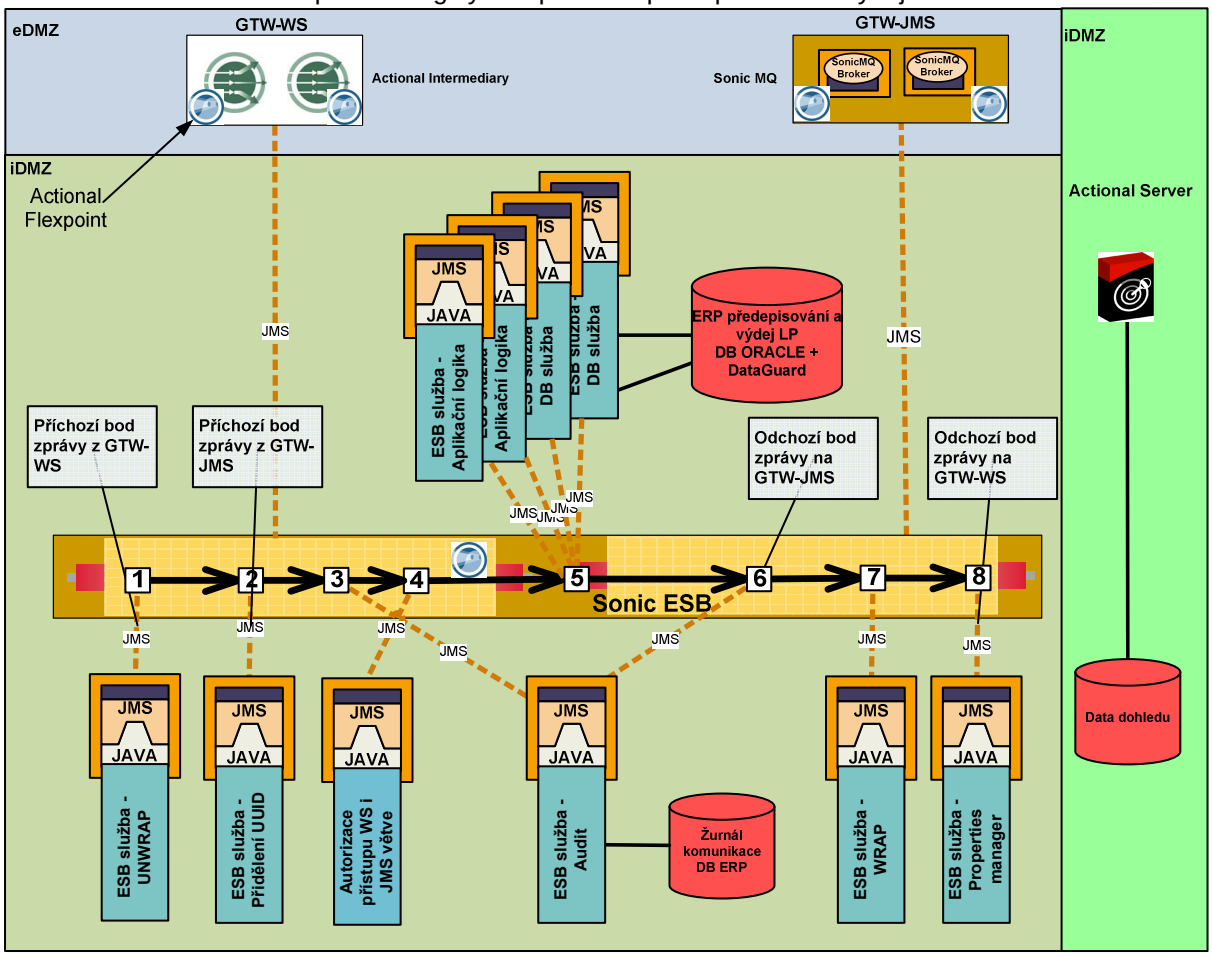


Architektura aplikační logiky založená na službách pro sběr dat Hlášení výdejů LP a ERP předepisování a výdejů LP bude identická.

Obr.: Architektura řešení aplikační logiky SW pro sběr dat Hlášení výdejů LP:



Obr.: Architektura řešení aplikační logiky SW pro ERP předepisování a výdej LP:



6.7. ROZŠIŘITELNOST, ŠKÁLOVATELNOST ŘEŠENÍ

Systém zakončování SSL může být v budoucnu bez problému rozšiřován jak ve smyslu zvyšování počtu funkcionalit systému, tak ve smyslu zvyšování výkonnosti. Výkonnost a vlastnosti virtualizace lze bez problémů zvyšovat instalací příslušných licencí. Celkovou výkonnost systému lze dále zvyšovat nasazením loadbalancingu SSL tunelů mezi více SSL terminátorů.

Dodávané řešení pro loadbalancing interních a externích systémů lze bez problémů dále rozšiřovat, jak ve smyslu zvyšování počtu funkcionalit systému, tak ve smyslu zvyšování výkonnosti. Výkonnost a vlastnosti virtualizace lze bez problémů zvyšovat instalací příslušných licencí. Díky této vlastnosti je možné zvýšit propustnost modulu na 16Gbps a počet kontextů až na 200. Dále je možné přidat další ACE moduly a pomocí virtualizace rozšířit loadbalancing téměř na libovolný počet systémů SÚKL.

Rozšíření centrálních prvků o nově dodávané moduly umožní v budoucnu větší flexibilitu při nasazování nových technologií do komunikační infrastruktury SÚKL. Připojování nových zařízení do komunikační infrastruktury bude možné jak rychlostí 1Gbps, tak rychlostí 10Gbps.

Nasazení nových přepínačů Cisco do stávajícího chassis DELL přináší větší flexibilitu a škálovatelnost výsledného řešení. Nově instalované servery budou díky možnosti využít redundantní připojení pomocí technologie cross stack etherchannell schopny lépe využít dostupnou šířku pásma komunikační infrastruktury SÚKL. Díky tomu bude možné dále velice rychle a efektivně rozvíjet informačný systémy SÚKL díky značnému zjednodušení připojení serverů do komunikační infrastruktury SÚKL. Je možné stohovat až 8 těchto přepínačů, čímž může být dosaženo toho, že síťová infrastruktura pro připojování serverů pro 2 plná bladová chassis DELL bude spravována z jednoho místa. Toto nabízí velkou flexibilitu a jednoduchost implementací změn do komunikační infrastruktury serverů.

Nasazované řešení je možné dále rozvíjet o centralizovanou karanténu Spamů, správu logů a v neposlední řadě o technologii bezpečného šifrování odesílaných emailů. Podpora industry standardů umožňuje kompatibilitu se všemi systémy používající protokol SMTP.

Navrhované řešení je možné dále škálovat, jak ve smyslu rozsahu monitorovaných síťových segmentů, tak ve smyslu objemu zpracovávaných toků dat. Tento systém je možné doplnit o další sondy, centrální kolektor a další pluginy pro vyhodnocování anomálií v síťovém provozu.

Budoucí růst virtuální infrastruktury je zajištěn použitím již zmíněného VMware řešení. Technologie VMware – virtuální infrastruktury v oboru - pomáhá organizacím konsolidovat servery a zvýšit míru využití, výrazně snižuje náklady na napájení a chlazení a umožňuje správu a automatizaci IT procesů, jejichž výsledkem je maximální dostupnost, výkon a škálovatelnost. Stávající diskovou kapacitu je stále možné jednoduše rozšířit o další diskové police, případně navýšit výkon stávajícího diskového subsystému. Také stávající blade šasi DELL je stále možné dále jednoduše rozšířit o další blade servery a jejich zapojení do stávajícího clusteru.

Z pohledu SW části řešení aplikace pro sběr dat Hlášení výdejů LP a ERP předepisování a výdejů LP bude sjednocena architektura řešení obou systémů.

Vstupní brány bude možné nadále posilovat o další instalace Actional Intermediary a SonicMQ a zařazovat za HW balancer, který na ně rozkládá zátěž. Případně bude možné přidávat další typy komunikačních protokolů a přístupových bodů, na kterých budou služby dostupné. Bude navržený princip pro verzování obou komunikačních rozhraní, který umožní do budoucna přechod na nové verze vynucené legislativou nebo požadované zadavatelem.

Aplikační logika bude umístěna ESB sběrnici do ESB služeb, bude sjednoceno řešení žurnálování komunikace. Aplikační logika bude rozčleněna do samostatných služeb pro konkrétní akce jako např. validace XML podle XSD definice apod. Vývoj a zapojení dalších ESB služeb podle potřeb zadavatele bude možné včetně zapojení do ESB procesu zpracování dat. Škálovatelnost řešení je zajištěna použitou technologií ESB a možností vytvářet další instance ESB kontejnerů s aplikační logikou podle požadovaného počtu zpracovaných zpráv.

Datové úložiště bude rozšiřitelné podle potřeby včetně možnosti následného vytěžování a zpracování dat pro potřeby zadavatele a jeho další agendy.

7. PŘÍLOHY

Tabulka plnění závazných technických a funkčních požadavků zadavatele k vyplnění pro uchazeče.

Uchazeč vyplní tabulky v poli „hodnota nabízená uchazečem“ a v poli „odkaz na produktovou dokumentaci uchazeče“.

Plnění závazných technických a funkčních požadavků na implementaci nápravných opatření ÚOOÚ s odkazy na produktovou dokumentaci u nabízených SW a HW komponent.

1. Rozšíření hardware datového centra

subkritérium	parametr	minimální hodnota požadovaná zadavatelem	hodnota nabízená uchazečem	odkaz na produktovou dokumentaci uchazeče
SYSTÉM ZAKONČENÍ SSL SPOJENÍ SBĚRU DAT				
1.	Počet SSL tunelů sestavených za 1s	14 000	15 000	Cisco_ACE_datasheet.pdf
2.	Počet současně zakončených SSL tunelů	150 000	200 000	Cisco_ACE_datasheet.pdf
3.	Propustnost při šifrování SSL	3 Gbps	3,3 Gbps	Cisco_ACE_datasheet.pdf
4.	Podpora: rsa-with-rc4-128-md5, rsa-with-aes-256-cbc-sha, rsa-with-rc4-128-sha, rsa-with-aes-128-cbc-sha, rsa-export-with-des40-cbc-sha, rsa-export1024-with-rc4-56-sha, rsa-with-des-cbc-sha, sa-export1024-with-des-cbc-sha, rsa-with-3des-ede-cbc-sha, rsa-export1024-with-rc4-56-md5 a rsa-export-with-rc4-40-md5, v hardware	ANO	ANO	Cisco_ACE_datasheet.pdf
5.	Možnost integrace s PKI	ANO	ANO	Cisco_ACE_datasheet.pdf
6.	Možnost ověřovat uživatele na základě certifikátů	ANO	ANO	Cisco_ACE_datasheet.pdf
7.	počet slotů v chassis	4		Cisco_C6504E.pdf
8.	Výkon řídícího modulu pro IPv4 routing	400 Mpps	400 Mpps	Cisco_Cat6500_Sup720.pdf
9.	Podpora karty s funkcí IPS	ANO	ANO	C6500_chassis.pdf
10.	Podpora karty s funkcí IPSec VPN koncentrátoru	ANO	ANO	C6500_chassis.pdf
11.	Podpora vysoké dostupnosti	ANO	ANO	C6500_chassis.pdf
12.	Podpora Weighted Fair Queuing (WFQ)	ANO	ANO	Cisco_IOS_12.2(33)SXH_introduction.pdf
13.	Podpora Weighted Random Early Detection (WRED)	ANO	ANO	Cisco_IOS_12.2(33)SXH_introduction.pdf
Rozkládání zátěže datových toků na GTW systémy				
1.	Propustnost v době dodání	8 Gbps	8 Gbps	Cisco_ACE_datasheet.pdf
2.	Možnost zvýšení propustnosti na min. 15 Gbps pouze vložením příslušné licence	ANO	ANO	Cisco_ACE_datasheet.pdf
3.	Podpora virtualizace	ANO	ANO	Cisco_ACE_datasheet.pdf
4.	Počet podporovaných virtuálních zařízení v době dodání	20		Cisco_ACE_datasheet.pdf
5.	Možnost rozšířit na minimálně 200 virtuálních zařízení	ANO	ANO	Cisco_ACE_datasheet.pdf
6.	Podpora vysoké dostupnosti mezi různými fyzickými zařízeními a rovněž mezi jednotlivými virtuálními zařízeními	ANO	ANO	Cisco_ACE_datasheet.pdf
7.	Možnost konfigurovat rozdělení zdrojů mezi jednotlivá virtuální zařízení	ANO	ANO	Cisco_ACE_datasheet.pdf

8.	Počet současných spojení	3 500 000	4 000 000	Cisco_ACE_datasheet.pdf
9.	Počet serverů, mezi které je možné rozdělovat zátěž	15 000	16 000	Cisco_ACE_datasheet.pdf
10.	Možnost nasazení jak v routed, tak i transparentním režimu	ANO	ANO	Cisco_ACE_datasheet.pdf
11.	Podpora následujících pravidel pro loadbalancing: adaptive response, least loaded, least bandwidth, least connections, round-robin, hash address, hash cookie, hash header a hash URL	ANO	ANO	Cisco_ACE_datasheet.pdf
12.	Podpora protokolů pro detekování „zdraví“ serverů: ICMP, TCP, UDP, ECHO {tcp | udp}, Finger, HTTP, HTTPS, FTP, Telnet, DNS, Simple Mail Transfer Protocol (SMTP), Internet Mail Access Protocol (IMAP), Post Office Protocol (POP), RADIUS, Keepalive Appliance Protocol (KAL-AP), RTSP, SIP, HTTP parsování návratového kódu a Simple Network Management Protocol (SNMP)	ANO	ANO	Cisco_ACE_datasheet.pdf
13.	Počet definovaných detektorů „zdraví“ serverů	3 500	4 000	Cisco_ACE_datasheet.pdf
14.	Podpora pro TCP offloading	ANO	ANO	Cisco_ACE_datasheet.pdf
15.	Podpora inspekce HTTP: http header, URL a HTTP payload	ANO	ANO	Cisco_ACE_datasheet.pdf
16.	Schopnost sledovat stav TCP spojení, validace TCP hlavičky, velikosti TCP okénka a randomizace sekvenčního čísla TCP spojení	ANO	ANO	Cisco_ACE_datasheet.pdf
17.	Ochrana před útoky typu distributed DoS (DDoS)	ANO	ANO	Cisco_ACE_datasheet.pdf
18.	Schopnost omezovat rychlost provozu per server	ANO	ANO	Cisco_ACE_datasheet.pdf
19.	Integrovaná hardwarově akcelerovaná inspekce a filtrování protokolů HTTP, RTSP, DNS, FTP, ICMP, SIP a LDAP	ANO	ANO	Cisco_ACE_datasheet.pdf
20.	Možnost vytvoření několika úrovní uživatelských a administrativních účtů pro kontrolování a spravování různých definovaných částí systému	ANO	ANO	Cisco_ACE_datasheet.pdf
21.	Možnost integrace se stávajícím systémem Cisco ACS	ANO	ANO	Cisco_ACE_datasheet.pdf
Rozšíření centrálních prvků (modul 10G)				
1.	Modul pro stávající zařízení Cisco Catalyst 6500	ANO	ANO	Cisco_Cat6500_10G.pdf
2.	Počet portů s možností osadit 10 Gbps moduly X2	16	16	Cisco_Cat6500_10G.pdf
3.	Max. agregace	4:1	4:1	Cisco_Cat6500_10G.pdf
4.	Množství rout pro distributed forwarding	256K	256K	Cisco_Cat6500_10G.pdf
5.	Požadovaná vzdálenost funkčnosti X2 modulu rychlostí 10 Gbps při použití vlákna MM OM3	300 m	300m	Cisco_Cat6500_10G.pdf
6.	Počet osazených adaptérů podporujících technologii 10GBASE-SR v každém dodaném modulu	6	6	N/A
Rozšíření centrálních prvků (modul 1G)				
1.	Modul pro stávající zařízení Cisco Catalyst 6500	ANO	ANO	Cisco_Cat6500_48_ 1000Base-T.pdf

2.	Počet portů 10/100/1000 Base-T	48	48	Cisco_Cat6500_48_ 1000Base-T.pdf
3.	Podpora velkých rámců, min. 9000 B	ANO	ANO	Cisco_Cat6500_48_ 1000Base-T.pdf
4.	Velikost výstupní fronty per port	1,3 MB	1,3 MB	Cisco_Cat6500_48_ 1000Base-T.pdf
5.	Určeno pro datová centra a serverové farmy	ANO	ANO	Cisco_Cat6500_48_ 1000Base-T.pdf
Rozšíření stávajících blade serverů (každý kus musí splňovat)				
1.	XEON X5570	2	2	Dell_m710_datasheet.pdf
2.	144 GB RAM	ANO	ANO	Dell_m710_datasheet.pdf
3.	8x 1Gbit LAN port	ANO	ANO	Dell_m710_datasheet.pdf
4.	8Gbps FC HBA	2	2	Dell_m710_datasheet.pdf
5.	2x 73GB SAS 15k v RAID1	ANO	ANO	Dell_m710_datasheet.pdf
Rozšíření stávajících blade serverů – Ethernet přepínač				
1.	Modul kompatibilní s blade chassis DELL PE M1000e	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
	L2 / L3 přepínač s podporou IPv4 a IPv6	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
2.	Podpora VPN routing and forwarding (VRF) lite	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
3.	Podpora per-VLAN RSTP	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
4.	Minimální počet spanning tree instancí	128	128	Cisco_Catalyst_ Blade_Switch_3130_2.pdf
5.	Možnost sdružovat více přepínačů do jednoho logického celku a tento spravovat jako jeden	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
6.	Podpora SSH v1, 2, Kerberos a SNMPv3	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
7.	Možnost webové autentizace zabezpečené pomocí SSL pro non-IEEE 802.1x klienty	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
8.	Podpora přiřazení do VLAN z RADIUS serveru podle výsledků 802.1x autentizace	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
9.	Možnost aplikace specifického access listu v závislosti na výsledku 802.1x autentizace	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
10.	VLAN access-listy sloužící k omezení specifického provozu uvnitř jedné sítě VLAN	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
11.	Ochrana DHCP protokolu – blokování neautorizovaného DHCP provozu	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
12.	Dynamická inspekce ARP protokolu	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
13.	Ochrana zdroje IP adresy zabraňující převzetí / podvržení IP adres	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
14.	Možnost přesměrovat data na port přepínače (pro monitorování provozu), nebo do VLAN a tento provoz odposlouchávat až na portu jiného přepínače	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
15.	Možnost omezení přístupu podle MAC adres stanic, možnost omezení maximálního počtu MAC adres za portem přepínače	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
16.	Podpora přednostní fronty (strict priority queueing)	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf

17.	Podpora Shaped Round Robin (SRR) časování ve vstupních i výstupních frontách	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
18.	Rate limiting na základě IP adres, zdrojové a cílové MAC adresy, Layer 4 TCP a UDP informací	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
19.	Podpora IGMP snooping pro IPv4 a IPv6 Multicast Listener Discovery (MLD) Verze 1 a 2	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
20.	Možnost filtrování IGMP a omezení počtu současných multicast streamů per port	ANO	ANO	Cisco_Catalyst_ Blade_Switch_3130.pdf
21.	Počet osazených adaptérů podporujících technologii 10GBASE-SR v každém dodaném přepínači	2	2	N/A
ROZŠÍŘENÍ STÁVAJÍCÍCH DISKOVÝCH POLÍ				
1.	Disková police k diskovému poli DELL/EMC CX 4-120 včetně osazených pevných disků 15x 450 GB HDD FC4 15k rpm (1 ks diskové police)	ANO	ANO	Dell_emc_cx4-120_datasheet.pdf
2.	Disková police k diskovému poli DELL/EMC CX 4-120 včetně osazených pevných disků 15x 1TB Serial ATA2 7.2k HD EMC (1 ks diskové police)	ANO	ANO	Dell_emc_cx4-120_datasheet.pdf
3.	Diskové police, 100% kompatibilní s datovým úložištěm DELL/EMC CX 4 -120	ANO	ANO	Dell_emc_cx4-120_datasheet.pdf
Systém zajištění kontroly a vysoké dostupnosti email komunikace				
1.	Možnost provozovat v clusteru	ANO	ANO	Ironport_c160_datasheet.pdf
2.	Dedikované HW zařízení (appliance)	ANO	ANO	Ironport_c160_datasheet.pdf
3.	Detekce spamu na základě reputace zdrojových IP adres	ANO	ANO	Ironport_c160_datasheet.pdf
4.	Detekce virů a dalšího škodlivého kódu v poštovní komunikaci	ANO	ANO	Ironport_c160_datasheet.pdf
5.	Možnost nasazení více antivirových produktů od různých výrobců na zařízení	ANO	ANO	Ironport_c160_datasheet.pdf
6.	Technologie filtrace spamu u nevyžádaných NDR zpráv na základě podpisu odchozích zpráv antispamovým zařízením (bounce attack protection)	ANO	ANO	Ironport_c160_datasheet.pdf
7.	Možnost budoucího rozšíření o centrální jednotnou správu zařízení v clusteru jako jednoho celku (tzn., v rámci clusteru se musí automaticky replikovat konfigurace mezi jednotlivými zařízeními)	ANO	ANO	Ironport_c160_datasheet.pdf
8.	Automatická aktualizace definic (spam, viry)	ANO	ANO	Ironport_c160_datasheet.pdf
9.	Možnost ověřování existence uživatelských kont přes LDAP – funkce musí umožňovat krátkodobé cachování	ANO	ANO	Ironport_ESA_7.0.0_FCS_ Advanced_Configuration_ Guide.pdf str. 3-177
10.	Možnost přepisování odchozích a příchozích mailových adres dle informací z LDAP	ANO	ANO	Ironport_ESA_7.0.0_FCS_ Advanced_Configuration_ Guide.pdf str. 3-179
11.	Možnost definovat různé antispam, antivirus a filtrovací politiky pro jednotlivé uživatele nebo pro celé skupiny uživatelů, včetně možnosti integrace s MS AD a LDAP	ANO	ANO	Ironport_ESA_7.0.0_FCS_ Configuration_Guide.pdf str. 6-185
12.	Možnost směrování SMTP komunikace na základě parametrů z LDAP	ANO	ANO	Ironport_ESA_7.0.0_FCS_ Advanced_Configuration_

				Guide.pdf str. 3-178
13.	Možnost vytváření filtrů na emailovou komunikaci, které budou schopny pracovat s obsahem hlaviček, těla i příloh v emailu přiřazování filtrů musí jít na základě příslušnosti ke skupině v LDAP nebo MS AD	ANO	ANO	Ironport_ESA_7.0.0_FCS_ Advanced_Configuration_ Guide.pdf str. 3-177 str. 5-292 IronPort_ESA_7.0.0_FCS_ Configuration_Guide.pdf str. 6-193
14.	Schopnost vytvářet virtuální SMTP brány	ANO	ANO	Ironport_ESA_7.0.0_FCS_ Configuration_Guide.pdf str. 5-105
15.	Požadovaný počet emailů odsměrovaných za 1 hodinu při použití antispam a antivirus funkcionalit	43 000	43 000	IronPort_ESA_ Performance.pdf
16.	Zařízení musí umožňovat vytváření pokročilých skriptů pro filtrovací politiky, včetně schopnosti jejich přiřazování uživatelům na základě skupin v LDAP/MS AD na úrovní jednotlivých filtrů.	ANO	ANO	Ironport_ESA_7.0.0_FCS_ Advanced_Configuration_ Guide.pdf str. 3-177 str. 5-292

2. Rozšíření software datového centra

subkritérium	parametr	minimální hodnota požadovaná zadavatelem	hodnota nabízená uchazečem	odkaz na produktovou dokumentaci uchazeče
Virtualizační software				
1.	Licence pro 4CPU	ANO	ANO	VMware ESX.pdf
2.	Licence bez omezení velikosti paměti fyzického stroje	ANO	ANO	VMware ESX.pdf
3.	3-letá podpora	ANO	ANO	VMware ESX.pdf
Software na monitoring diskových polí				
1.	Licence plně kompatibilní se stávajícími poli DELL/EMC	ANO	ANO	Navisphere Software.pdf
2.	3-letá software assurance pro dodávané licence	ANO	ANO	Navisphere Software.pdf

3. Implementace podpůrných systémů a vývoj software

subkritérium	parametr	minimální hodnota požadovaná zadavatelem	hodnota nabízená uchazečem	odkaz na produktovou dokumentaci uchazeče
Návrh a implemenatce řešení vysoké dostupnosti OID v prostředí sběru dat				
1.	Navržené řešení musí zajistit vysokou dostupnost služby OID, zajištění pomocí dvou nezávislých vzájemně synchronizovaných OID serverů.	ANO	ANO	Popis technického řešení ; kapitola 4.1.1.
2.	Počet registrovaných identit 100 000	100 000	100 000	http://www.oracle.com/us/ products/middleware/identity-

				management/index.html
3.	Možnost rozšiřitelnosti řešení do geograficky vzdálených lokalit, počet N+1	ANO	ANO	Popis technického řešení ; kapitola 4.1.2.
4.	Funkčnost řešení ve stávajícím VMware prostředí zadavatele.	ANO	ANO	viz doložená reference, funkčnost zajištěna v prostředí VMware
Návrh a implementace systémů zajišťující monitoring datových toků				
1.	Nezávislost na stávající síťové infrastruktuře	ANO	ANO	flowmon_cz.pdf
2.	Specializované dedikované zařízení pro vytváření detailních statistik IP toků	ANO	ANO	flowmon_cz.pdf
3.	Podpora IPv4, IPv6, VLAN, MPLS, NetFlow v5/v9, IPFIX (RFC 5101) na 1 Gigabit Ethernetu (s možností upgradu na 10 Gigabit Ethernet)	ANO	ANO	flowmon_cz.pdf
4.	Možnost integrace libovolných nástrojů i třetích stran	ANO	ANO	flowmon_cz.pdf
5.	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS	ANO	ANO	flowmon_cz.pdf
6.	Počet gigabitových portů pro současné měření síťového provozu	6	6	flowmon_cz.pdf
7.	Vestavěný kolektor pro ukládání NetFlow statistik	ANO	ANO	flowmon_cz.pdf
8.	Počet historických toků uložených na zařízení	1 000 000	1 000 000	flowmon_cz.pdf
9.	Požadovaný výkon pro zpracování paketů na každém monitorovacím portu za 1s	500 000	500 000	flowmon_cz.pdf
10.	Možnost integrace se stávajícím bezpečnostním zařízením Cisco MARS	ANO	ANO	flowmon_cz.pdf
11.	Podpora uživatelsky definovatelných šablon pro protokoly NetFlow v9 a IPFIX	ANO	ANO	flowmon_cz.pdf
12.	Podpora simultánního exportu NetFlow statistik minimálně na tři cíle	ANO	ANO	flowmon_cz.pdf
13.	Podpora filtrování dat (pro různé cíle exportu různé statistiky)	ANO	ANO	flowmon_cz.pdf
14.	Možnost dohledání každé komunikace	ANO	ANO	flowmon_cz.pdf
15.	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu, IP provozu nebo protokolu	ANO	ANO	flowmon_cz.pdf
16.	Výpis tzv. top N statistiky podle různých kritérií	ANO	ANO	flowmon_cz.pdf
17.	Možnost emailového upozornění administrátorům v případě vzniku uživatelem definované situace	ANO	ANO	flowmon_cz.pdf
18.	Vytváření profilů pro ukládání dat vyhovující nadefinovaným filtrům	ANO	ANO	flowmon_cz.pdf
19.	Podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace	ANO	ANO	flowmon_cz.pdf
20.	drill-down – možnost dohledat každý jednotlivý tok zaznamenaný systémem	ANO	ANO	flowmon_cz.pdf
21.	Kombinace minimálně dvou vyhodnovacích nástrojů v rámci systému	ANO	ANO	flowmon_cz.pdf
22.	Grafické výstupy ve volitelné formě - koláčové grafy, průběhové grafy, tabulky	ANO	ANO	flowmon_cz.pdf
23.	Možnost exportu výstupu do formátů	pdf, csv, xml	pdf, csv, xml	flowmon_cz.pdf
24.	Otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh	ANO	ANO	flowmon_cz.pdf

25.	Počet metalických rozhraní pro monitoring datových toků rychlostí 1 Gbps	6	6	flowmon_cz.pdf
Analýza a rekonfigurace systému Sonic ESB a ESB služeb Hlášení výdejů a OTC s omezením				
1.	Počet zpracovaných zpráv za 1 hodinu	800 000	800 000	Kap. 4.3.2.1, 4.3.2.2, 4.4.2.1, 4.4.2.2, 4.5.1, 4.5.2,
2.	Implementace anonymizovaného identifikátoru pacienta do ESB služeb	ANO	ANO	Pseudonymizovaný identifikátor 4.5.1
3.	Implementace anonymizovaného identifikátoru pacienta do komunikačních rozhraní	ANO	ANO	Pseudonymizovaný identifikátor 1.3, 4.4.2.1
4.	Paralelní provoz více verzí současně	ANO	ANO	4.4.2.1, 4.5.1
5.	Průběžná archivace žurnálu komunikace	ANO	ANO	4.5.2
6.	Plná funkčnost a dostupnost, kompatabilita s ostatními systémy	ANO	ANO	4.3.2.1, 4.3.2.2, 4.4.2.1, 4.4.2.2
Analýza a rekonfigurace systému Sonic ESB a ESB služeb Centrálního úložiště				
1.	Počet zpracovaných zpráv za 1 hodinu	800 000	800 000	Kap. 4.3.2.1, 4.3.2.2, 4.6.2.1, 4.6.2.2, 4.6.2.3, 4.7.1, 4.7.2,
2.	Implementace anonymizovaného identifikátoru pacienta do ESB služeb	ANO	ANO	Pseudonymizovaný identifikátor 4.7.1
3.	Implementace anonymizovaného identifikátoru pacienta do komunikačních rozhraní	ANO	ANO	Pseudonymizovaný identifikátor 1.3, 4.6.2.1
4.	Paralelní provoz více verzí současně	ANO	ANO	4.6.2.1, 4.7.1
5.	Průběžná archivace žurnálu komunikace	ANO	ANO	4.7.2
6.	Plná funkčnost a dostupnost, kompatabilita s ostatními systémy	ANO	ANO	4.3.2.1, 4.3.2.2, 4.6.2.1., 4.6.2.3
Analýza a rekonfigurace databázových systémů hlášení				
1.	Počet zpracovaných záznamů za 1 hodinu	15 000 000	15 000 000	4.8.3.3, 4.8.3.4
2.	Implementace anonymizovaného identifikátoru pacienta do úložiště dat	ANO	ANO	Pseudonymizovaný identifikátor 1.3, 4.8.3.3
3.	Paralelní provoz více verzí současně	ANO	ANO	4.8.3.3
4.	Průběžná archivace žurnálu komunikace	ANO	ANO	4.8.3.4
5.	Plná funkčnost a dostupnost, kompatabilita s ostatními systémy	ANO	ANO	4.8.2, 4.8.3.2
Analýza a rekonfigurace databázových systémů Centrálního úložiště				
1.	Počet zpracovaných záznamů za 1 hodinu	15 000 000	15 000 000	4.8.4.3, 4.8.4.4
2.	Implementace anonymizovaného identifikátoru pacienta do úložiště dat	ANO	ANO	Pseudonymizovaný identifikátor 1.3, 4.8.4.3
3.	Paralelní provoz více verzí současně	ANO	ANO	4.8.4.3
4.	Průběžná archivace žurnálu komunikace	ANO	ANO	4.8.4.4
5.	Plná funkčnost a dostupnost, kompatabilita s ostatními systémy	ANO	ANO	4.8.2, 4.8.4.2