ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ
ÚSTŘEDÍ - ÚSEK INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

Křížová 25, 225 08, Praha 5

Standard síťové infrastruktury

Verze 1.95

Historie dokumentu:

Datum vydání	Verze	Změna proti předchozí verzi	Změnil (jméno)
15.6.2006	1.0	Import dat z CSSZ-architektura-0.6	Sommer, Novák
19.6.2006	1.1	Úprava dokumentu a obrázků	Sommer, Novák
22.6.2006	1.2	Update dokumentu na základě připomínek ze schůzky na ČSSZ	Sommer, Novák
	1.3	Návrh redundance datových center	Sommer, Novák
8.8.2006	1.4	CA, BizTalk	Novák
16.8.2006	1.5	Adresní plány, pojmenování	Novák, Šmíd
25.9.2006	1.6	QoS	Novák, Šmíd
31.10.2006	1.7	Aktualizace QoS a připojení SAP	Novák
7.12.2006	1.8	Aktualizace BT a SAP	Novák, Šmíd
21.12.2006	1.81	Upgrade rychlostí WAN	Šmíd
20.03.2009	1.90	Změna QoS tříd	Novák, Šmejkal
18.01.2010	1.92	Rozklad zátěže	Novák, Šmejkal
26.4.2012	1.93	Doplnění Virtualizace v DC, jmenná konvence, adresace DC	Nardelli
30.6.2015	1.95	Požadavky na nastavení průstupů v rámci sítě ČSSZ, aktualizace adresace pro WAN lokality, zanesení změn v oblasti CORE pro rok 2015.	Nardelli, Kačírek, Šmejkal

Obsah

Seznam obrázků

1. ÚVOD

V současné době prochází integrovaný informační systém ČSSZ (dále jen IIS ČSSZ) mohutným rozvojem. V běhu či přípravě je větší množství projektů, které přímo či nepřímo ovlivňují síťovou infrastrukturu a obecnou koncepci bezpečnosti síťového prostředí ČSSZ. Vzhledem k neexistenci závazných pravidel je běžné, že různé nasazované aplikace či systémy si samy definují bezpečnost a požadavky na síťové prostředí, přičemž tyto požadavky jsou někdy rozdílné až protichůdné. Tento dokument slouží jako základ pro definování závazných požadavků pro budoucí rozvoj informačního systému ČSSZ, především při nasazování nových aplikací.

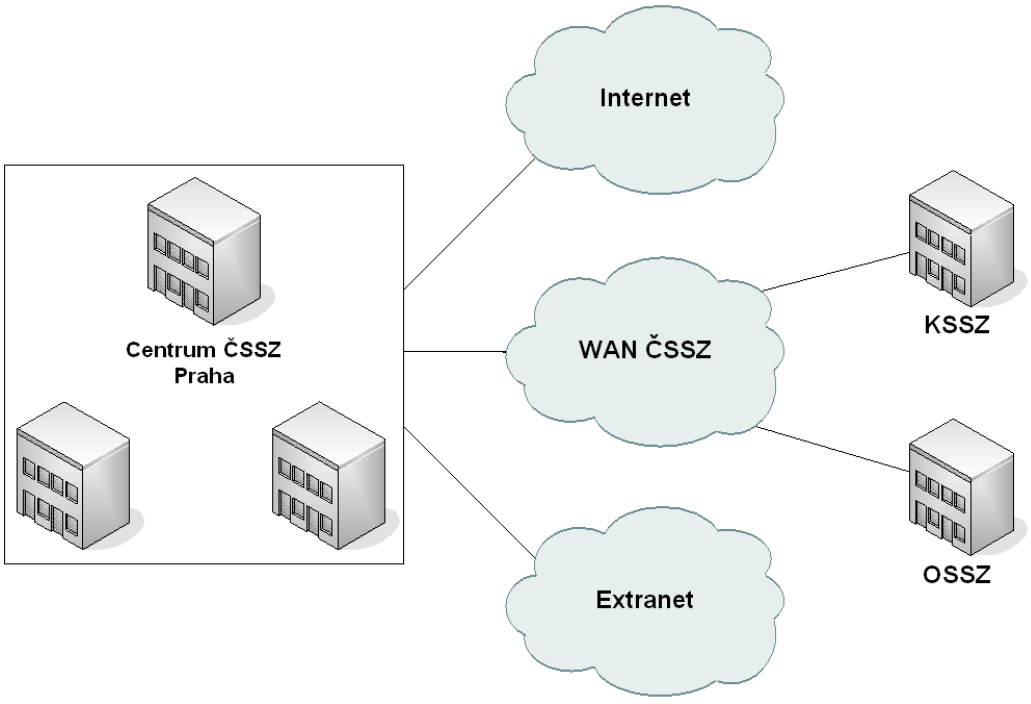
2. POPIS SÍŤOVÉHO PROSTŘEDÍ ČSSZ

Topologicky lze síť ČSSZ rozdělit na:

- Ústředí ČSSZ v Praze (lokality Křížová a Trojská),
- Pobočky ČSSZ (jednotlivá pracoviště ČSSZ, OSSZ a MSSZ),
- Externí zdroje a sítě (Internet, Extranet),

přičemž jednotlivá pracoviště ČSSZ jsou propojena WAN sítí ČSSZ.

Schématické znázornění topologie sítě je uvedeno na následujícím obrázku:



Obrázek 1 – Topologie sítě ČSSZ

Bezpečnostní politika je vymezena pravidly, standardy a dokumenty definujícími bezpečnost jednotlivých oblastí či aplikací (např. připojení k Internetu, kryptografická ochrana WAN apod.)

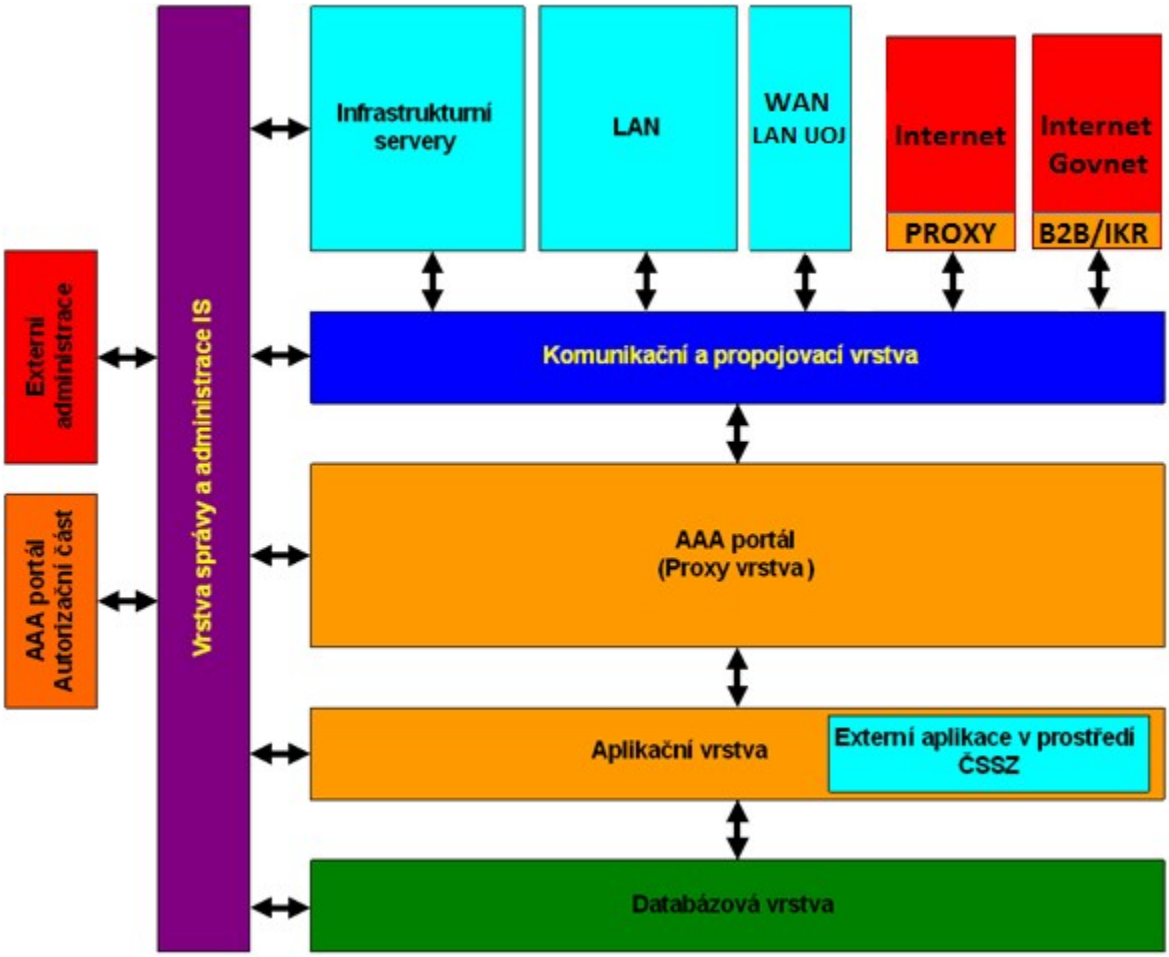
Pobočky jsou do WAN připojeny linkami s kapacitami:

malé OSSZ/LPS	10 Mbps
OSSZ	20 Mbps
Pracoviště ČSSZ	50 Mbps

Ústředí je k WAN připojeno redundantní linkou o kapacitě 300 Mbps.

2.1 Obecná koncepce architektury řešení

Vzhledem ke složitosti integrovaného informačního systému ČSSZ a z důvodu zajištění centralizace dat, aplikací a systémů je výchozím požadavkem pro konsolidaci IS definování a následné dodržování architektury síťového prostředí. V celkové architektuře jsou jednotlivé funkční celky s rozdílnou požadovanou úrovní bezpečnosti zařazeny do odpovídajících vrstev (*zón*). Právě vrstvová architektura umožňuje jasně definovat příslušnost dané aplikace či systému do odpovídající vrstvy a na rozhraních jednotlivých vrstev jednoznačně popsat datové toky a odpovídající bezpečnostní mechanismy.
Na následujícím obrázku je znázorněn cílový stav architektury síťového prostředí ČSSZ (pro snadnější rozlišení celků s rozdílnou bezpečnostní úrovní je použito barevné odlišení).



Obrázek 2 – Architektura síťového prostředí

2.2 Popis jednotlivých vrstev

2.2.1 Infrastrukturní servery

Tato vrstva zahrnuje infrastrukturní servery. Jedná se o servery Active Directory, Exchange servery, proxy servery a DNS servery. Tyto servery jsou dostupné z LAN či WAN prostředí a jsou přímo připojeny do páteřních a distribučních přepínačů. V této vrstvě na samostatném segmentu sítě je také umístěna struktura certifikačních autorit. Tento segment je monitorován IPS (Intrusion Prevention System) sondou.

2.2.2 WAN

Tato vrstva zahrnuje především uživatelské počítače ve WAN ČSSZ a dále pak ostatní zdroje či systémy (infrastrukturní aplikační servery pro lokální úroveň, tiskárny, síťové prvky,…), které jsou ze své podstaty nutné pro fungování uživatelů/uživatelských počítačů v rámci lokálních poboček propojených prostřednictvím WAN.

Na jednotlivých pobočkách jsou standardně následující typy zařízení:

- Směrovač (Cisco C2811, resp. C4331).
- Přepínače s funkcionalitou L3 pro připojení serverů (zpravidla 2x Cisco C3560).
- Přepínače s funkcí stohování pro připojení koncových uživatelů a PC (stoh prvků Cisco C2960s).
- WAN Aplikační akcelerátor (Cisco WAE 274, 474, 674).

2.2.3 LAN

Tato vrstva zahrnuje především uživatelské počítače v LAN ústředí ČSSZ, které jsou odděleny od infrastrukturních serverů a jsou napojeny na soustavu podřízených přepínačů – uživatelské přepínače. Tyto přepínače jsou dále napojeny na páteřní přepínače v komunikační a propojovací vrstvě.

2.2.4 Komunikační a propojovací vrstva

Tato vrstva zahrnuje síťové prvky zajišťující vzájemné propojení jednotlivých funkčních celků a vrstev. Zprostředkovává tedy komunikaci mezi dalšími vrstvami. Základní požadavky při páteřním propojení centrálních sítí a systémů jsou rychlost, bezpečnost a zajištění vysoké dostupnosti.

Bližší specifikace vrstvy:

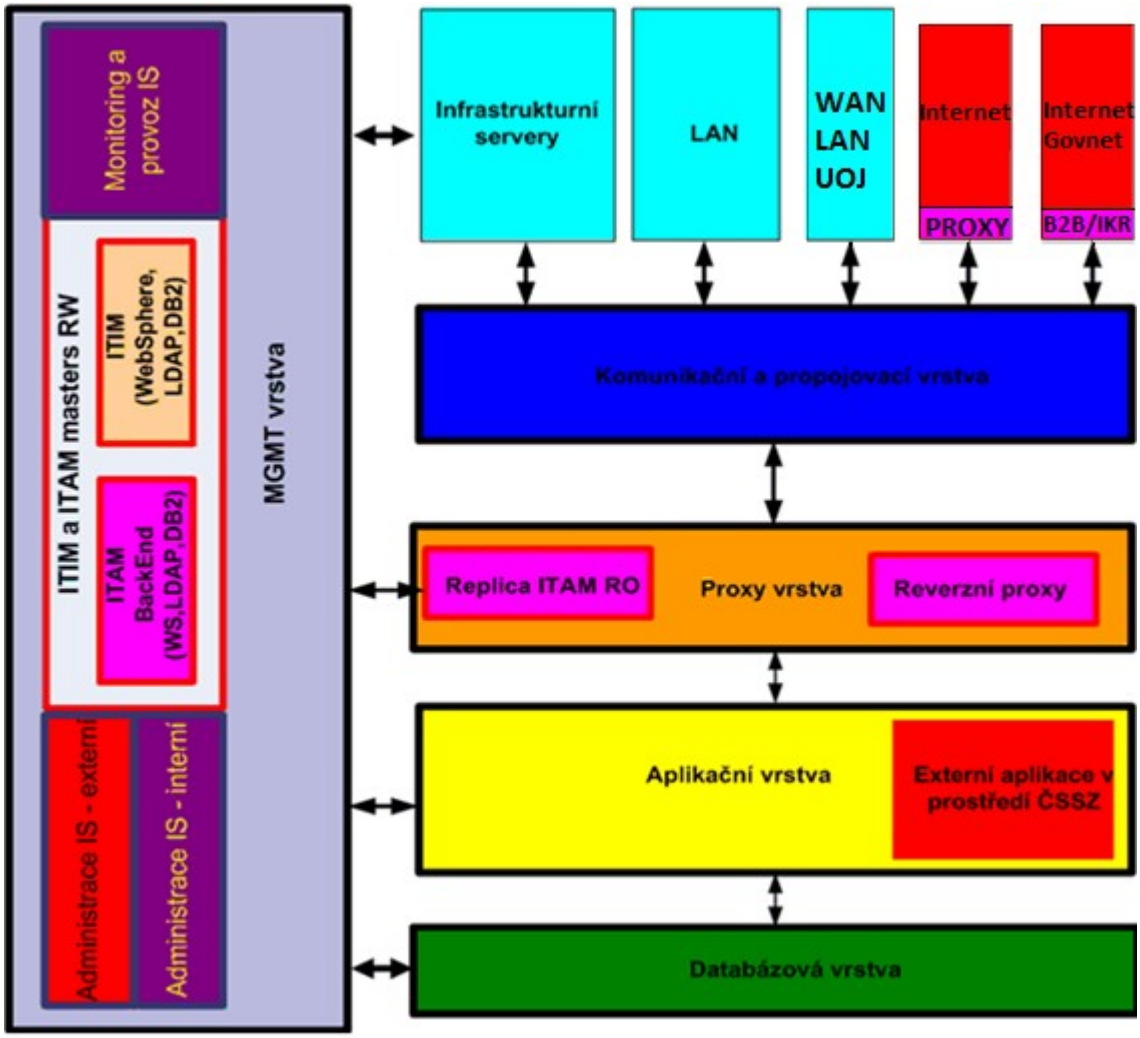
- je založena na 3 přepínačích Cisco Catalyst 6500
- pomocí FW modulů zajišťuje bezpečnostní pravidla mezi jednotlivými zónami
- pomocí integrovaných modulů zajišťuje IDS/IPS službu
- ve spolupráci s content přepínači v aplikační vrstvě zajišťuje automatizované nebo řízené přepnutí datového a aplikačního provozu z primární do záložní centrální lokality

2.2.5 Proxy vrstva

Tato vrstva je tvořena Content přepínači, jež pomocí SSL (Secure Sockets Layer) modulů zakončují SSL komunikaci od uživatelů a provádějí počáteční autentizaci pomocí klientských a serverových certifikátů. Dále jsou zde proxy servery, které mají za úkol ukončit autentizovanou komunikaci uživatele – provádí se na ní ověření tiketů protokolu Kerberos vůči serverům KDC (key distribution center – součást šifrovacího systému pro snížení rizika spojeného s výměnou šifrovacích klíčů) situovaným ve vrstvě správy a administrace. Tyto KDC servery jsou plně

synchronizovány s AD (KDC) ve vrstvě infrastrukturních serverů a vůči kerberos tiketům se chovají naprosto transparentně.

Na následujícím obrázku je tato vrstva podrobněji rozpracována ve vztahu k reverzním proxy a RO replikám ITAM (IBM® Tivoli® Access Manager), ITIM (IBM® Tivoli® Identity Manager) databází.



Obrázek 3 – Architektura síťového prostředí z hlediska proxy

2.2.6 Vrstva správy a administrace IS

Vrstva slouží k umístění administrativních a monitorovacích serverů určených ke správě systémů ve všech vrstvách. Tato vrstva je segmentována podle potřeby správy jednotlivých zón. Jako jediná má tato vrstva přístup do všech ostatních vrstev, ovšem opačný směr je omezen na vyhrazenou komunikaci (blíže specifikováno v kapitole 2.3 **Popis rozhraní mezi jednotlivými vrstvami**). V této vrstvě jsou umístěny dohledové systémy postavené na produktech Nagios a iMC. Prostřednictvím této vrstvy je také prováděna administrace jednotlivých systémů a to jak interní, tak externí. V žádném případě neprovádí zprostředkování komunikace mezi třetími vrstvami (například komunikaci Aplikační Vrstvy s databázovou vrstvou).

V této vrstvě jsou také umístěny ITAM a ITIM server master jenž se replikují do jednotlivých „read only“ serverů v jednotlivých vrstvách.(Popis viz níže)

2.2.7 Aplikační vrstva

Tato vrstva zahrnuje centrální systémy a sítě poskytující uživatelům přístup k aplikacím ČSSZ, přičemž tyto aplikace zajišťují operace nad datovou základnou (tj. databázovou vrstvou) ČSSZ. Jednotlivé aplikace jsou ve stejné bezpečnostní zóně odděleny mezi směrované L3 segmenty pro další možnost využít mechanismu load balancingu mezi jednotlivými aplikacemi.
Ve stejné vrstvě se nachází i tzv. „outsourced" aplikace (např. SAP). Aplikační vrstva je rozdělena do několika VLAN – v každé VLAN je provozována jedna aplikace.

2.2.8 Databázová vrstva

Tato vrstva zahrnuje systémy a sítě realizující centrální datovou základnu ČSSZ, která je prostřednictvím aplikací v aplikační vrstvě poskytována koncovým uživatelům (zaměstnancům).
Databázová vrstva je tvořena databázovými servery, které jsou pomocí vyhrazené SAN infrastruktury připojeny k diskovým polím a páskovým knihovnám. Veškerá síťová a SAN infrastruktura databázové vrstvy je transparentně protažena mezi oběma lokalitami. V každé z lokalit je umístěn databázový server, přičemž na této dvojici serverů je pro business critical databáze resp. aplikace vytvořen Oracle RAC Cluster.
Business critical databáze běžící na tomto clusteru jsou uloženy na primárním diskovém poli umístěném v primární lokalitě a jsou v reálném čase mirrorovány technologií PPRC na sekundární diskové pole umístěné v záložní lokalitě. V případě výpadku primárního diskového pole jsou oba databázové nody přepojeny na sekundární diskové pole. V případě výpadku jednoho databázového nodu pokračuje provoz s poloviční výkonem (pokud nejsou manuálně realokovány HW zdroje na příslušném serveru) na druhém databázovém nodu.
Databázová infrastruktura Oracle RAC clusteru je schopna transparentně poskytovat přístup aplikační vrstvě jak prostřednictvím vysoce dostupné databázové služby (včetně load balancingu a failoveru mezi databázovými nody na úrovni RAC clusteru), tak prostřednictvím přímého přístupu k jednotlivým instancím databáze (bez možnosti load balancingu a failoveru).

2.2.9 Externí sítě, Internet

Tato vrstva zabezpečuje přístup do dalších sítí a to Internet, CMS (GovNet, GovBone a TESTA).

2.3 Popis rozhraní mezi jednotlivými vrstvami

V popisu rozhraní je vynechána Komunikační a propojovací vrstva, neboť je vztahu k ostatním vrstvám (zónám) zcela transparentní.

Matice povolených/zakázaných komunikačních toků je uvedena v příloze.

2.3.1 Infrastrukturní servery - WAN

Komunikace není žádným způsobem omezena, je zprostředkována Komunikační a propojovací vrstvou.

2.3.2 Infrastrukturní servery – LAN

Komunikace není žádným způsobem omezena, je zprostředkována Komunikační a propojovací vrstvou.

2.3.3 Infrastrukturní servery – Vrstva správy a administrace IS

Komunikace směrem infrastrukturní servery -> Vrstva správy a administrace je omezena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu (např. SNMP, SYSLOG, RADIUS, terminálové služby,…), a tomu odpovídá i povolená komunikace. Komunikace je zprostředkována Komunikační a propojovací vrstvou.

2.3.4 Infrastrukturní servery – Externí sítě, Internet

Komunikace je zprostředkována Komunikační a propojovací vrstvou. Omezení pro komunikaci je specifikováno v části 4.1 - Kompletní tabulka datových toků.

2.3.5 WAN – LAN

Komunikace je zprostředkována Komunikační a propojovací vrstvou. Komunikace je povolena pouze ve směru LAN ->WAN a to pro účely vzdálené administrace systémů.

2.3.6 WAN – Vrstva správy a administrace IS

Komunikace směrem WAN -> Vrstva správy a administrace není povolena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu - např. SNMP, SYSLOG, RADIUS, terminálové služby,…) a tomu odpovídá i povolená komunikace. Komunikace je zprostředkována Komunikační a propojovací vrstvou.

2.3.7 WAN – Externí sítě, Internet

Komunikace je zprostředkována Komunikační a propojovací vrstvou. Omezení pro komunikaci je specifikováno v části 4.1 – Kompletní tabulka datových toků.

2.3.8 LAN – Vrstva správy a administrace IS

Komunikace směrem LAN -> Vrstva správy a administrace není povolena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu - např. SNMP, SYSLOG, RADIUS, terminálové služby,…) a tomu odpovídá i povolená komunikace. Komunikace je zprostředkována Komunikační a propojovací vrstvou.

2.3.9 LAN – Externí sítě, Internet

Komunikace je zprostředkována Komunikační a propojovací vrstvou. Omezení pro komunikaci je specifikováno v části 4.1 – Kompletní tabulka datových toků.

2.3.10 LAN/WAN - Proxy vrstva

Komunikace je jednosměrně navazovaná uživateli z LAN/WAN

- komunikace je založená pouze na protokolu HTTPS
- SSL komunikace je zakončena na Content přepínači
- komunikace je na rozhraní filtrována („firewalling“) a jsou zde sledovány útoky („IDS/IPS“)
- směrem do AAA proxy vrstvy se využívá content přepínačů (rozložení zátěže, přesměrování požadavků či zajištění vysoké dostupnosti)
- směrem z AAA vrstvy jsou prezentovány pouze jednotlivé služby AAA portálu (ne vlastní AAA servery), struktura AAA vrstvy je uživatelům skryta

2.3.11 Proxy vrstva – Vrstva správy a administrace IS

Komunikace směrem Komunikační a propojovací vrstva -> Vrstva správy a administrace není povolena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu - např. SNMP, SYSLOG, RADIUS, terminálové služby,…) a tomu odpovídá i povolená komunikace. Dále zde probíhá replikace ITAM, ITIM primárních serverů k jejich RO replikacím v Proxy vrstvě. Komunikace je na rozhraní filtrovaná („firewalling“) a jsou zde sledovány útoky („IDS/IPS“).

2.3.12 Proxy – Aplikační vrstva

Komunikace je jednosměrně navazovaná AAA portál servery z proxy vrstvy

- komunikace je založená na protokolu HTTP
- uvnitř HTTP protokolu je předávána informace o uživateli pro autorizaci na aplikační vrstvě
- komunikace není na rozhraní filtrovaná
- směrem do aplikační vrstvy se využívá content přepínačů (rozložení zátěže, přesměrování požadavků či zajištění vysoké dostupnosti)
- směrem z aplikační vrstvy jsou prezentovány pouze jednotlivé služby či aplikace (ne vlastní aplikační servery), struktura aplikační vrstvy je AAA portálu skryta

2.3.13 Proxy vrstva – Externí sítě, Internet

Komunikace je omezena povolenými porty a komunikací na vrstvě „Externí sítě, Internet“, která zabezpečuje firewalling.

2.3.14 Vrstva správy a administrace IS – Aplikační vrstva

Komunikace je jednosměrně navazována z vrstvy správy a administrace IS.
Jedinou výjimku tvoří: SNMP trap,…

- komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu aplikační vrstvy (např. SNMP, SYSLOG, RADIUS, terminálové služby,…)
- komunikace je na rozhraní filtrovaná („firewalling“) a jsou zde sledovány útoky („IDS/IPS“)

2.3.15 Vrstva správy a administrace IS – Databázová vrstva

Komunikace je jednosměrně navazována z vrstvy správy a administrace IS.
Jedinou výjimku tvoří: SNMP trap,…

- komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu aplikační vrstvy (např. služby - SNMP, SYSLOG, RADIUS, terminálové služby,…)
- komunikace je na rozhraní filtrovaná („firewalling“) a jsou zde sledovány útoky (IDS/IPS)

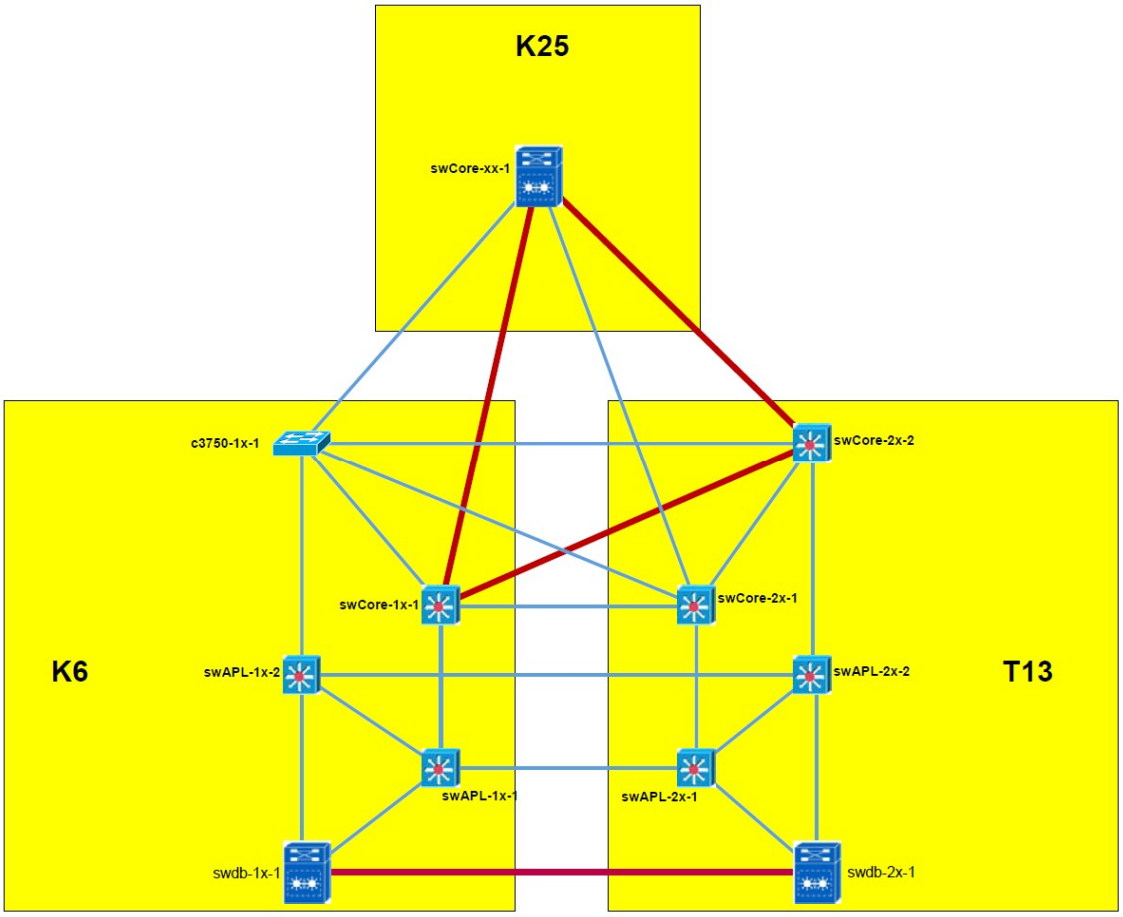
2.3.16 Aplikační vrstva – Databázová vrstva

- komunikace je jednosměrně navazovaná aplikacemi (Aplikační vrstva ->Databázová vrstva)
- komunikace je založená na požadavcích aplikací – SQL link
- na tomto rozhraní je preferována propustnost před bezpečností, proto zde není uvažováno nasazení firewallů
- aplikace se odkazuje na virtuální adresu databázového clusteru

2.4 Fyzická a logická topologie datových center

2.4.1 Fyzické zapojení datových center

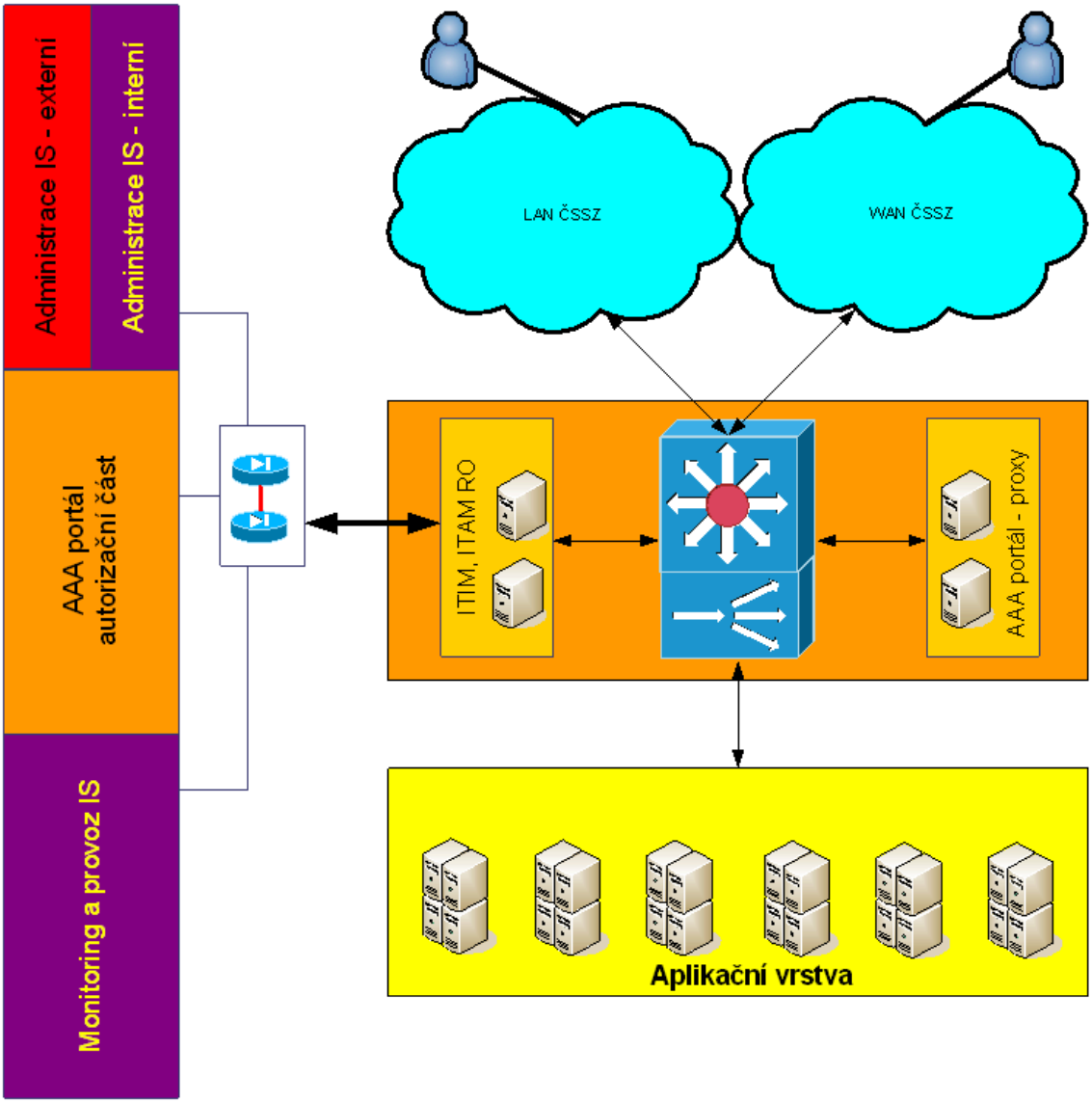
Na následujícím obrázku je znázorněno propojení páteřních prvků mezi datovými centry skrz optické propojení mezi budovami.



Obrázek 4 - Zapojení páteřní vrstvy

2.4.2 Úloha Content přepínačů v Proxy vrstvě

Jednotlivé vrstvy v navrženém modelu plně využívají mechanismu Content přepínání. Na následujícím obrázku je schematicky znázorněn datový tok od uživatelů směrem do Proxy vrstvy, Aplikační vrstvy.

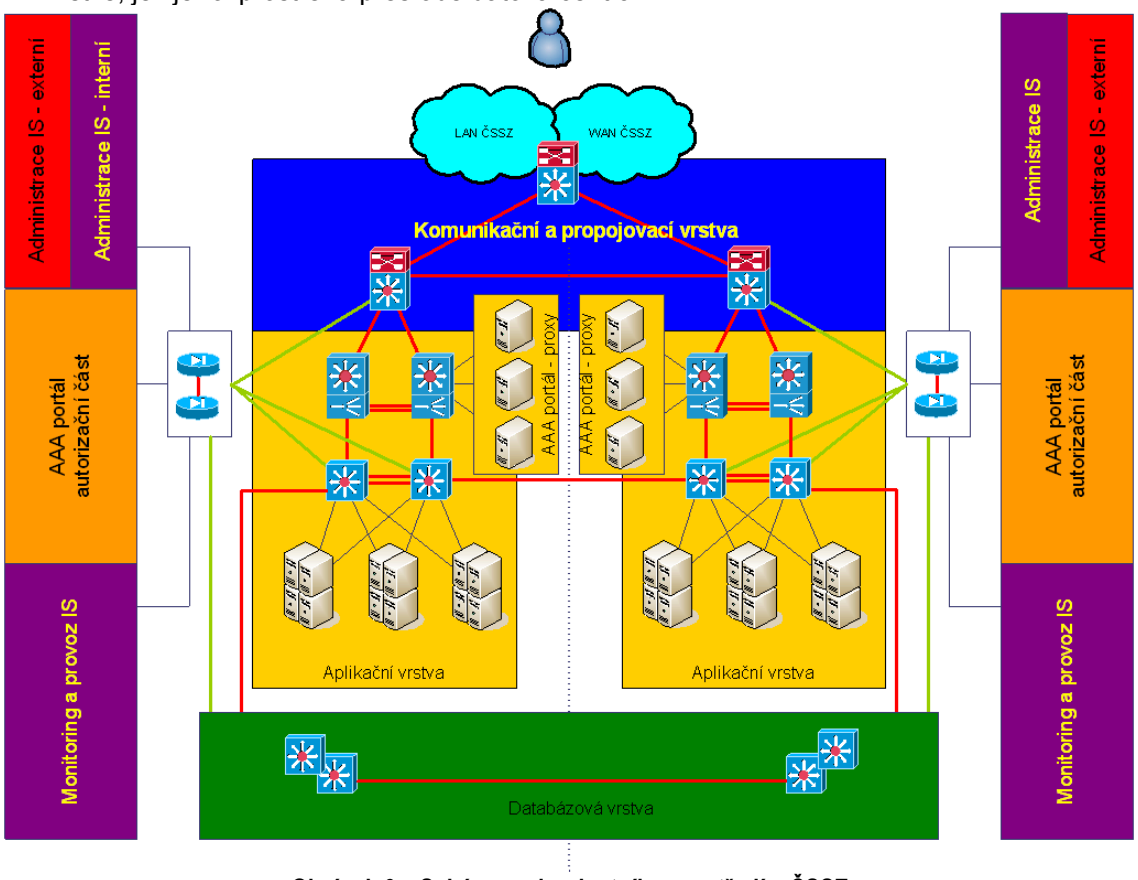


Obrázek 5 – Schéma datového toku uživatelů směrem do Proxy vrstvy, Aplikační vrstvy

Content přepínač je zde využíván pro zakončení SSL spojení od uživatele. Dále se „load balancuje“ mezi jednotlivými reverzními proxy. Od nich je požadavek na Aplikační servery, jenž je opět „load balancován“. Autorizační ověření od Aplikačních serverů směrem na ITAM, ITIM RO repliky jde skrz Content přepínače. Tento mechanismus „load balancingu“ bude též využíván pro komunikace mezi jednotlivými aplikacemi. Pouze do Databázové vrstvy není Content přepínač zahrnut. Je zde použit jiný model rozložení zátěže.

2.4.3 Redundantní zapojení datových center

Každý klient v LAN, WAN segmentu je pomocí DNS load balancingu směrován na jedno z datových center a to na příslušný AAA portál. AAA portál má přístup k aplikační vrstvě, jež je rozprostřena přes obě datová centra.



Obrázek 6 – Schéma redundantního prostředí v ČSSZ

Aplikační vrstva je propojena přes DWDM rozhraní do aplikačních přepínačů. Jednotlivé aplikace jsou spojeny přes L3 rozhraní – tj. provoz mezi nimi je směrován.
Při výpadku jednoho datového centra je klient automaticky směrován pouze na jeden Content přepínač resp. AAA portál.

2.4.4 Virtualizace v datových centrech

Součástí rozvoje infrastruktury datových center je také konsolidace IO rozhraní serverů a integrace virtualizační platformy VMware ESX do aplikační vrstvy DC.
Konsolidace IO rozhraní serverů je v infrastruktuře datových center řešena rozšířením blade šasi o nové interconnect moduly HP Virtual Connect Flex-Fabric umožňující přenos fibre channel protokolu přes rozhraní 10 gigabitethernet. Interconnect moduly VC jsou začleněné pod správu oddělení síťové infrastruktury, které zajišťuje začlenění nových modulů do síťové infrastruktury, jejich prvotní konfiguraci a případné změny nastavení dle schválených požadavků. Přístupy na konfigurační rozhraní VC jsou ověřované na centrálních autentizačních serverech pro síťovou infrastrukturu. Jednotlivým uživatelům se přidělují uživatelské role zajišťující oddělenou správu části konfigurace LAN a FC.
Z hlediska integrace virtualizační platformy VMware ESX do infrastruktury aplikační vrstvy datových center je sjednocována správa virtuálních přepínačů VMware ESX a síťové infrastruktury. Konfiguraci virtuálních přepínačů a tvorbu vNIC profilů pro virtuální servery

provádí oddělení správy sítí. Síťovým administrátorům se přiděluje při přístupu na vSwitch role umožňující pouze přidání, změnu a odstranění virtuálních přepínačů či jejich konfigurace.

2.5 IP adresace

IP adresace je stanovena prováděcím pokynem vrchního ředitele sekce IKT č. 102/2006

ČSSZ využívá na všech svých pracovištích adresy třídy A formátu 10.x.y.z s maskou 255.255.0.0, případně 255.255.255.0. Adresy pracovních stanic jsou dynamické, pro ostatní zařízení statické.

1) Adresace ústředí:

a) Druhý byte adresy:

- pro ústředí jsou rezervovány hodnoty 1 až 20 takto:
  - 1 : základní síť
  - 3 : IKR
  - 6,7 : technologické sítě provozované SBS
  - 9 : Nové DÚ
  - 10 : Síť pro outsourced SAP
  - 11 : management síť
  - 16 : testovací a vývojová síť
  - 17 : WiFi
  - 18 : směrování do sítě GovNet
  - 19 : vložená síť, ve které je šifrátor
  - 20 : demilitarizovaná zóna Firewallu

b) Třetí byte adresy:

- pro počítače kategorie PC jsou platné hodnoty odpovídající VLANám 7 - 40

Poznámka: soubor zařízení, která mají přístup do Intranetu (sítě WAN), je tedy v ústředí ČSSZ dán rozsahem třetího bytu adresy (130 až 159). Technicky je toto omezení zajištěno konfigurací šifrátoru.

Třetí byte v ústředí ČSSZ určuje rozdělení do VLAN následujícím způsobem:

Označení VLAN	Jméno VLAN	Popis	IP adresa sítě
4	4_USR_ucebna	uživatelé, učebna	10.1.4.0
7	7_CONSOLE	konsole serverů	10.1.7.0
8	8_USR_U1	uživatelé sekce 1	10.1.8.0
10	10_USR_U2	uživatelé sekce 2	10.1.10.0
12	12_USR_U3	uživatelé sekce 3	10.1.12.0
16	16_USR_U4	uživatelé sekce 4	10.1.16.0
20	20_USR_U4	uživatelé sekce 4	10.1.20.0
24	24_USR_U4	uživatelé sekce 4	10.1.24.0
26	26_USR_U4	uživatelé sekce 4	10.1.26.0

28	28_USR_U4	uživatelé sekce 4	10.1.28.0
29	29_USR_U4	uživatelé sekce 4	10.1.29.0
32	32_USR_U5	uživatelé sekce 5	10.1.32.0
33	33_USR_U5	uživatelé sekce 5	10.1.33.0
36	36_USR_ADM	administrátoři	10.1.36.0
38	38_vyvoj	programátoři	10.1.38.0
40	40_USR_U6	uživatelé sekce 6	10.1.40.0
50	50_USR_EXT	uživatelé EXT	10.1.50.0
51	51_siemens	uživatelé siemens	10.1.51.0
58	Wlan-I_Users		10.1.58.0
60	VLAN0060		10.1.60.0
80	80_SRV	Winmedit	10.1.80.0
85	85_U5PROVOZ		10.1.85.0
88	WLAN_AP	VLAN pro WiFi AP	10.1.88.0
89	NET_NAC-XX-trust		10.1.89.0
90	90_VYVOLAVACI_SYSTEM	vyvolávací systém	10.1.90.0
91	91_KAMEROVY_SYSTEM	kamerový systém	10.1.91.0
130	130_APL_SRV	servery - aplikační	10.1.130.0
134	SRV_APL134_XX	servery - aplikační	10.1.134.0
135	135_blade	servery - blade mimo farmy	10.1.135.0
138	SRV_PKIDB_HB_XX		10.1.138.0
140	SRV_INF140_XX		10.1.140.0
141	SRV_SAP_XX		10.1.141.0
142	SRV_PKI_XX		10.1.142.0
143	SRV_PKIDB_XX		10.1.143.0
144	144_WAN_SRV2		10.1.144.0
145	NET_FWCP_XX		10.1.145.0
146	146_ACS_SRV	servery - acs	10.1.146.0
147	147_mng	mng. VLAN	10.1.147.0
148	NET_AP_XX		10.1.148.0
150	150_WAN_PC	–PC-WAN	10.1.150.0
155	155_SKOLA	učebny	10.1.155.0
157	157_AUDIT	audit	10.1.157.0
160	160_Kyocera_A		10.1.160.0
161	161_Kyocera_A		10.1.161.0
162	162_Kyocera_AM		10.1.162.0
163	163_Kyocera_AM		10.1.163.0
164	164_Kyocera_C		10.1.164.0
170	170_MS_SRV	servery - Microsoft	10.1.170.0
171	171_MS_SRV	servery - Microsoft	10.1.171.0
172	172_MS_SRV	servery - Microsoft	10.1.172.0
174	174_MS_SRV	servery - Microsoft	10.1.174.0
180	180_PRN_SRV	síťové tiskárny	10.1.180.0
181	181_PRN_SRV	síťové tiskárny	10.1.181.0

182	182_PRN_SRV	síťové tiskárny	10.1.182.0
183	183_PRN_SRV	síťové tiskárny	10.1.183.0
184	184_PRN_SRV	síťové tiskárny	10.1.184.0
185	185_PRN_SRV	síťové tiskárny	10.1.185.0
186	186_PRN_SRV	síťové tiskárny	10.1.186.0
187	187_PRN_IBM	síťové tiskárny	10.1.187.0
190	190_LAN_Krizova	LAN Křížová	10.1.190.0
192	192_LAN1	propojení K25 – T13	10.1.192.0
193	193_LAN2	propojení K25 – K6	10.1.193.0
194	194_LAN3	propojení K6 – T13	10.1.194.0
217	EXT_IBM_PRINT		
221	221_SRV		10.1.221.0
248	248_MGMT_UPS	management UPS	10.1.248.0
254	254_MGMT_AP	management akt. prvků	10.1.254.0
255	255_MIRROR	mirror VLAN	
290	NET_IKR_BB		10.3.67.0
291	NET_IKR_XX		10.3.67.64
306	306_VLAN10_6	datová síť	10.6.0.0
370	mgm_WLAN	wireless mgmt	10.17.0.0
371	public_WLAN	wireless public	10.17.1.0
372	private_WLAN	wireless private	10.17.2.0

c) Čtvrtý byte:

Čtvrtý byte je pořadové číslo instalovaného zařízení.

2) Adresace OSSZ, UP PSSZ, Pracoviště ČSSZ, PSSZ a MSSZ :

a) Druhý byte adresy:

- pro OSSZ, UP PSSZ, Pracoviště ČSSZ, PSSZ a MSSZ jsou rezervovány hodnoty 21 až 122,
  mimo 36-41,43,86,118-119:

Název lokality	IP adresa sítě/prefix
Ústředí ČSSZ	10.1.0.0/16
PSSZ	10.42.0.0/16
ÚP PSSZ č. 73 se sídlem na Praze 1	10.30.96.0/20
ÚP PSSZ č. 72 se sídlem na Praze 2	10.30.128.0/20
ÚP PSSZ č. 74 se sídlem na Praze 9	10.81.0.0/16

ÚP PSSZ č. 75 se sídlem na Praze 4	10.30.64.0/20
ÚP PSSZ č. 74 se sídlem na Praze 9	10.30.48.0/20
ÚP PSSZ č. 79 se sídlem na Praze 3	10.30.80.0/20
ÚP PSSZ č. 81 se sídlem na Praze 9	10.30.176.0/20
ÚP PSSZ č. 82 se sídlem na Praze 10	10.30.208.0/20
ÚP PSSZ č. 72 se sídlem na Praze 2	10.30.192.0/20
ÚP PSSZ č. 76 se sídlem na Praze 4	10.30.112.0/20
Pracoviště ČSSZ Střední Čechy	10.31.16.0/20
OSSZ Benešov	10.31.64.0/20
OSSZ Beroun	10.31.48.0/20
OSSZ Kladno	10.31.224.0/20
OSSZ Kolín	10.31.96.0/20
OSSZ Kutná Hora	10.31.160.0/20
OSSZ Mělník	10.31.240.0/20
OSSZ Mladá Boleslav	10.31.128.0/20
OSSZ Nymburk	10.31.192.0/20
OSSZ Praha-západ	10.31.32.0/20
OSSZ Příbram	10.31.112.0/20
OSSZ Rakovník	10.31.208.0/20
Pracoviště ČSSZ České Budějovice	10.31.0.0/16
OSSZ Český Krumlov	10.32.0.0/16
OSSZ Jindřichův Hradec	10.51.0.0/16
OSSZ Písek	10.73.0.0/16
OSSZ Prachatice	10.77.0.0/16
OSSZ Strakonice	10.98.0.0/16
OSSZ Tábor	10.101.0.0/16
Pracoviště ČSSZ Plzeň	10.74.0.0/16
OSSZ Plzeň – město	10.75.0.0/16
OSSZ Plzeň – sever	10.76.0.0/16
OSSZ Domažlice	10.35.0.0/16
OSSZ Klatovy	10.54.0.0/16

OSSZ Rokycany	10.94.0.0/16
OSSZ Tachov	10.102.0.0/16
OSSZ Karlovy Vary	10.58.0.0/16
OSSZ Cheb	10.28.0.0/16
OSSZ Sokolov	10.97.0.0/16
OSSZ Liberec	10.59.0.0/16
OSSZ Česká Lípa	10.33.0.0/16
OSSZ Jablonec nad Nisou	10.48.0.0/16
OSSZ Semily	10.96.0.0/16
Pracoviště ČSSZ Ústí nad Labem	10.106.0.0/16
OSSZ Děčín	10.34.0.0/16
OSSZ Chomutov	10.29.0.0/16
OSSZ Litoměřice	10.60.0.0/16
OSSZ Louny	10.61.0.0/16
OSSZ Most	10.63.0.0/16
OSSZ Teplice	10.103.0.0/16
Pracoviště ČSSZ Hradec Králové	10.46.0.0/16
OSSZ Jičín	10.49.0.0/16
OSSZ Náchod	10.65.0.0/16
OSSZ Rychnov nad Kněžnou	10.95.0.0/16
OSSZ Trutnov	10.105.0.0/16
OSSZ Pardubice	10.71.0.0/16
OSSZ Chrudim	10.30.0.0/16
OSSZ Svitavy	10.100.0.0/16
OSSZ Ústí nad Orlicí	10.107.0.0/16
OSSZ Jihlava	10.50.0.0/16
OSSZ Havlíčkův Brod	10.47.0.0/16
OSSZ Pelhřimov	10.72.0.0/16
OSSZ Třebíč	10.104.0.0/16
OSSZ Žďár nad Sázavou	10.111.0.0/16
Pracoviště ČSSZ Brno	10.26.0.0/16
OSSZ Blansko	10.23.0.0/16
OSSZ Břeclav	10.24.0.0/16
OSSZ Hodonín	10.45.0.0/16
OSSZ Vyškov	10.110.0.0/16
OSSZ Znojmo	10.113.0.0/16

MSSZ Brno	10.25.0.0/16
OSSZ Olomouc	10.68.0.0/16
OSSZ Jeseník	10.117.0.0/16
OSSZ Prostějov	10.92.0.0/16
OSSZ Přerov	10.90.0.0/16
OSSZ Šumperk	10.99.0.0/16
OSSZ Ostrava	10.70.0.0/16
OSSZ Bruntál	10.27.0.0/16
OSSZ Frýdek Místek	10.44.0.0/16
OSSZ Karviná	10.52.0.0/16
OSSZ Nový Jičín	10.67.0.0/16
OSSZ Opava	10.69.0.0/16
OSSZ Zlín	10.112.0.0/16
OSSZ Kroměříž	10.56.0.0/16
OSSZ Uherské Hradiště	10.108.0.0/16
OSSZ Vsetín	10.109.0.0/16
ČSSZ – Křešice	10.120.0.0/16
OSSZ Třinec	10.124.0.0/16
OSSZ Vlašim	10.125.0.0/16
OSSZ Rumburk	10.126.0.0/16
OSSZ Sušice	10.127.0.0/16
OSSZ Liberec I	10.128.0.0/16
OSSZ Prostějov	10.130.0.0/16
OSSZ Uherský Brod	10.131.0.0/16
OSSZ Valašské Klobouky	10.132.0.0/16
OSSZ Krnov	10.133.0.0/16
OSSZ Písek I	10.134.0.0/16
Odloučené pracoviště Děčín	10.121.0.0/16
Odloučené pracoviště Bruntál	10.122.0.0/16

b)Třetí byte na OSSZ, UP PSSZ, pracoviště ČSSZ, PSSZ a MSSZ***:***

1 až 5	:	počítače PC
6	:	servery s OS Windows a nově instalovaný server Solaris
7	:	UPS, aktivní prvky, konsole
8	:	jakákoliv zařízení bez přístupu do sítě WAN
9	:	hardware s komunikací do internetu přes proxy

Poznámka: I zde je stanoven interval adres, z nichž lze přistupovat do Intranetu. Je dán rozsahem třetího bytu (1 až 7). Technicky je toto omezení opět zajištěno konfigurací šifrátoru.

c) ***Čtvrtý byte adresy*** na OSSZ, UP PSSZ, Pracoviště ČSSZ, PSSZ a MSSZ **:**

Čtvrtý byte je pořadové číslo instalovaného zařízení.

Pevně stanovené adresy pro všechna pracoviště:

defaultní router : 10.x.190.1

3) **Adresace Datových center**

a. **Datová centra jsou adresována následujícím způsobem**

Název lokality	IP adresa sítě/prefix	Výchozí brána
Primární centrum – vrstva aplikačních serverů - provozní	10.200.0.0/16	Dle VLANy
Záložní centrum – vrstva aplikačních serverů - provozní	10.201.0.0/16	Dle VLANy
Primární centrum – vrstva aplikačních serverů – školící	10.202.0.0/16	Dle VLANy
Záložní centrum – vrstva aplikačních serverů – školící	10.203.0.0/16	Dle VLANy
Primární centrum – vrstva aplikačních serverů – vývojové	10.204.0.0/16	Dle VLANy
Záložní centrum – vrstva aplikačních serverů – vývojové	10.205.0.0/16	Dle VLANy
Primární i záložní centrum – vrstva databázových serverů	10.9.0.0/16	Dle VLANy

b. Adresace fyzických serverů

Adresace fyzických serverů v DC je 10.20x.y.z, kde:
x – vychází z prostředí a lokality
y – oktet aplikace
z – unikátní id serveru

c. Adresace virtuálních serverů

Adresace virtuálních serverů v DC je 10.20x.y.z, kde:
x – vychází z prostředí a lokality
y – oktet aplikace
z – konstanta 179 + id serveru unikátní pro lokalitu/prostředí/aplikaci
Příklad: va1x129l01, první integrační POJ server v lokalitě K6 – 10.204.129.180

2.6 Jmenná konvence

Jmenná konvence aktivních prvků na územních jednotkách

1. WAN směrovač (šifrátor)
   Lokalita - typ prvku – pořadí v lokalitě
   Příklad: sy-c2811-1
2. LAN přepínače

Lokalita - typ prvku – rozváděč – pořadí v rozváděči
Příklad: sy-c3560-r1-1

Jmenná konvence aktivních prvků v ústředí:

1. Prvky v páteři
   Typ prvku – lokalita – pořadí v lokalitě
   Příklady: c6509-XX-1; c1002-2X-1
2. Přepínače v LAN
   Typ prvku – budova - rozvaděč – pořadí v rozvaděči
   Příklad: c3550-SB-R21-1

Jmenná konvence serverů v DC infrastruktuře:

1. Fyzické Servery
   a. Jmenná konvence: saWWXXX
   b. WW je kód lokality
   c. XXX je unikátní id serveru

2. Virtuální servery
   a. Jmenná konvence: vaWWXXXYZZ
   b. WW je kód lokality
   c. XXX je oktet aplikace
   d. Y je označení prostředí
      i. P – Produkční
      ii. T – Testovací
      iii. I – Integrační
   e. ZZ je id serveru unikátní pro lokalitu/prostředí/aplikaci
      i. Maximální hodnota id serveru je 20
   f. Příklad: va1x129I01
      i. První integrační server aplikace POJ na lokalitě K6
   g. Příklad: va2x129P01
      i. První produkční server aplikace POJ na lokalitě T13

Malá i velká písmena jsou ve jmenné službě interpretována shodně.

3. STÁVAJÍCÍ APLIKACE

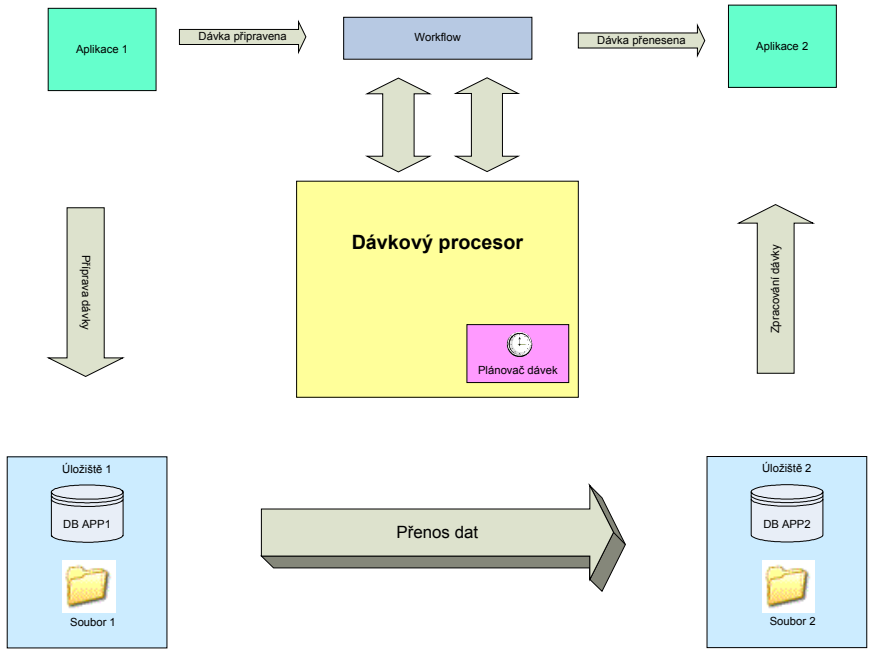
3.1 DMS

Tato aplikace nezapadá do modelu třívrstvé architektury s plným, bezpečným a škálovatelným rozdělením datové komunikace do jednotlivých vrstev. Tvoří výjimku a bude v budoucnu přepracována do standardizované podoby.
Komunikační transport dat je u této aplikace navazován klientem, který se nachází ve vrstvě LAN či WAN. Klient se odkazuje na virtuální adresu služby, která je definovaná na Content přepínači. Content přepínač zajišťuje „rozhazování“ příchozí komunikace na definované aplikační servery. Klient nemá možnost kontaktovat aplikační servery přímo, protože konkrétní adresy aplikačních serverů nejsou dosažitelné z LAN/WAN a na rozhraní Aplikační a Komunikační vrstvy je prováděna odpovídající filtrace provozu.
Klient se autentizuje pro DMS aplikaci přes „username & password“ přímo na aplikačním serveru. Aplikační server pomocí LDAP požadavku ověří klienta oproti Active Directory databázi a umožní či odmítne klientův požadavek. Tento LDAP požadavek je směrován skrz vrstvu Administrace systémů a aplikací, jenž je reprezentován firewallem PIX 535.
Na aplikaci DMS je přímo napojena Datová pumpa. Tato aplikace z pohledu transportu dat vyžaduje navázání http komunikace v obou směrech. Přenos dokumentů z PC na server ÚP je implementován jako aplikace klient/ server. Veškerá komunikace probíhá pomocí protokolu HTTP. Z hlediska komunikace je server HTTP na PC, klient v

komunikaci HTTP je součástí datové pumpy na serveru ÚP. Proces datové pumpy se spouští v pravidelných intervalech cronem na serveru ÚP.
V tomto konceptu je podle toho nastaven Content přepínač a jemu příslušná bezpečnostní pravidla tak, aby odrážela potřebnou datovou komunikaci. Na Content přepínači je nakonfigurován NAT a access listy pro přístup aplikačních serverů směrem do/z LAN/WAN pro synchronizaci těchto serverů navzájem.

3.2 BizTalk

Aplikace BizTalk je zasazena do Aplikační vrstvy ve třívrstvé architektuře ČSSZ. V této vrstvě je definována samostatná Doména pro správnou funkci mezi Aplikacemi a Biztalkem. Komunikace není nijak omezena.



Obrázek 7 – Komunikace BizTalk

Proces workflow je následující:

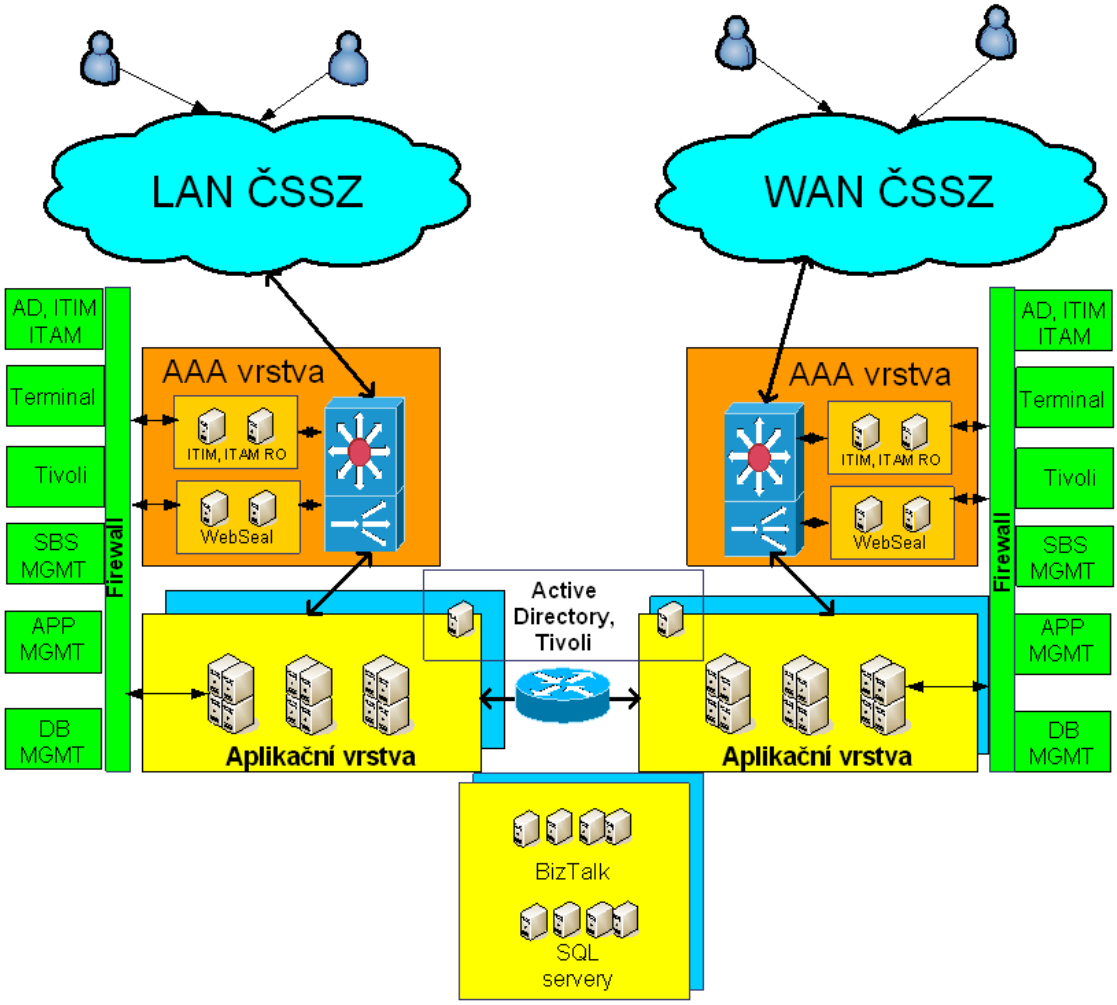
- Aplikace APP1 posílá signál WF
- WF volá APP1: „připrav data pro přenos“
- APP1 připraví data pro přenos do TMP oblasti a informuje WF
- WF volá BP: „přenes data“
- BP si vezme data z vyhrazené oblasti DB APP1 a přenese je do vyhrazené oblasti DB APP2
- BP informuje WF o ukončení přenosu dat
- WF kontaktuje APP2 s informací „máš data ke zpracování“
- APP2 zpracuje data v TMP oblasti a informuje WF, že je to hotovo
- Proces končí

3.3 Síťové schéma zapojení ITIM a ITAM

Systémy AAA portálu jsou rozprostřeny v několika síťových segmentech:
10.200.5 – WebSeal Proxy servery
10.200.6 – ITIM/ITAM RO repliky
10.11.47 – ITIM/ITAM master

V rámci mgmt zóny jsou umístěny ITIM/ITAM mastery společně s AD serverem. AAA portál je umístěn v obou lokalitách a je využíván v módu active x active dle následujícího schématu.

WAN uživatelé jsou směrovány do prostředí datového centra Trojská, kdežto LAN uživatelé jsou směrovány do prostředí datového centra Křížová 6. Tímto mechanismem je zajištěno rozložení zátěže do obou center. V případě výpadku jednoho z center, je celý provoz automaticky směrován do druhého.



Obrázek 8 – Schéma zapojení ITIM a ITAM

3.4 Definice QoS

Pro správnou funkci aplikací ve WAN prostředí ČSSZ je třeba definovat a nastavit QoS pro jednotlivé datové toky tak, aby nedocházelo k přeplnění linek nežádoucí komunikací.

Vzhledem k nasazení šifrátorů a využití MPLS-VPN (Multiprotocol Label Switching) služby od Telefónica-O2/GTS můžeme QoS rozdělit na dvě části: Klasifikace, markování a LLQ .

Klasifikace a markování je prováděno na CE směrovači ČSSZ na vstupním rozhraní. Parametry konfigurace klasifikace budou nastaveny dle potřeb jednotlivých aplikačních tříd dle přiložené tabulky. V Ústředí bude klasifikace a markování prováděno na LAN rozhraní VPN centrálního WAN směrovače.

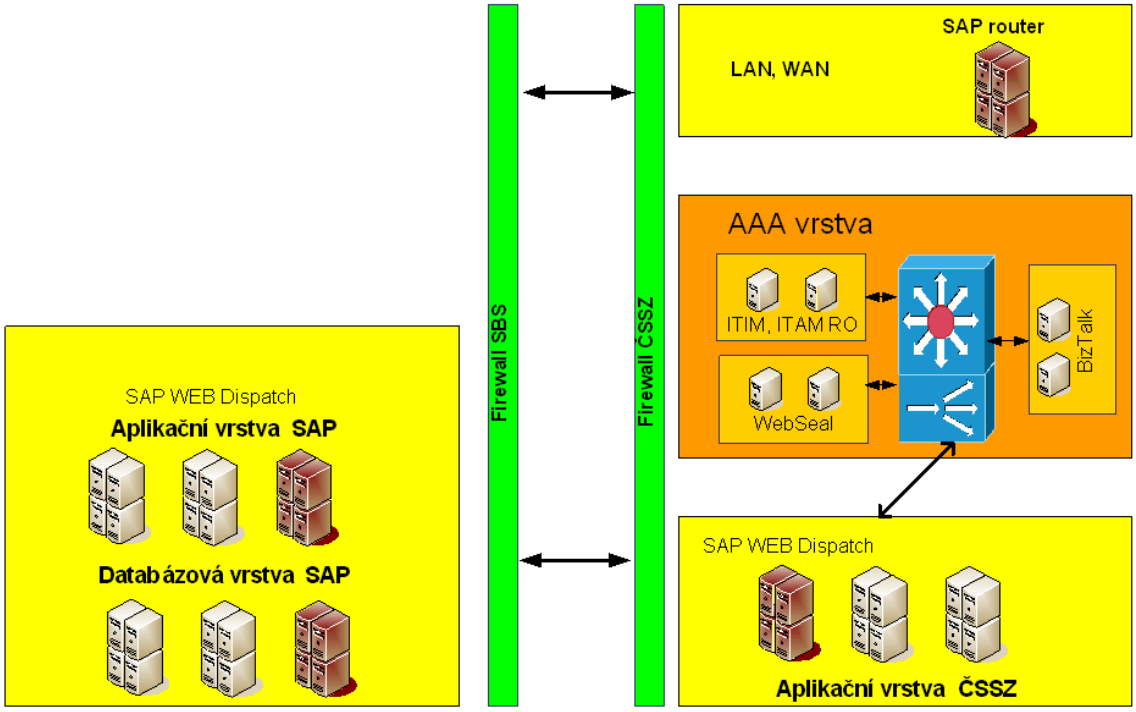
Na Tunel rozhraních VPN směrovačů (mGRE tunely) bude konfigurována pre-klasifikace, kdy hodnoty v záhlaví paketu DSCP určující třídu paketu, budou před enkrypcí paketu zkopírovány do nového záhlaví IPSec paketu a na mezilehlém

směrovači CE Telefonica-O2/GTS bude tak možno na zašifrované pakety aplikovat stávající QoS LLQ politiky.
Následující tabulka znázorňuje rozdělení do jednotlivých tříd, definici DSCP dle standardu od poskytovatele MPLS-VPN sítě a příslušnou šířku pásma v %.

Název aplikační třídy	Vyhrazené pásmo v %	Cílové adresy-aplikace
QoS-app-1/Internet	10	10.1.140.0/24:8080 10.1.128.143 - PKI-xx 10.2.128.143 - PKI-2x 10.1.128.144 - proxy-xx 10.2.128.144 - proxy-2x 10.1.140.131 - AMS 10.2.140.131 - AMS 10.1.140.133 - intranet 10.1.144.5 - Exchange 10.1.144.6 - Exchange 10.1.144.7 - Exchange 10.2.144.5 - Exchange 10.2.144.6 - Exchange 10.2.144.7 – Exchange
QoS-app-2/ AD, Admin	10	10.1.140.125 - DNS 10.2.140.125 - DNS 10.1.142.50 – CA-users 10.1.142.51 – CA-services 10.11.0.0/16 - MGMT eigrp
QoS-app-3 / DMS	10	10.1.131.3:9081-9083 10.1.131.50 10.1.131.51
QoS-app-4/APL, tlustý klient	20	10.1.135.0/24:80,443 10.1.141.0/24:3298,3299
QoS-app-5/APL, tenký klient	40	10.1.131.0/24:80-82,443 10.1.141.0/24:80,8000-8007
Default	10	Vše, co zbývá.

3.5 SAP

V infrastruktuře ČSSZ je umístěn SAP pod správou SBS, jenž komunikuje s klienty ve vrstvě LAN, WAN. Protože aplikace (SAP) potřebuje komunikovat s aplikacemi v Aplikační vrstvě, byla navržena následující komunikační infrastruktura.



Obrázek 9 – Schéma SAP

V aplikační vrstvě je instalován SAP web Dispatcher, jenž zprostředkovává veškerou komunikaci mezi novými aplikacemi a SAP prostředím. Jak je z obrázku patrno, oba světy jsou odděleny Firewally v MGMT vrstvě. Na těchto Firewallech jsou definovány prostupy pro správnou komunikaci – viz následující tabulka.

Zdrojová adresa	Cílová adresa	Cílový port	Protokol	Komponenta	Slovní popis
10.11.22.4 10.11.22.5	10.200.193.70	3298 3299	"SAP"	saprouter	komunikace aplikací VYP -> BT (NEM)
10.200.NN	10.200.15.193	8005 8105	http	SAP Web Dispatcher	přístup aplikace (BT) NEM k SAPu - VYP produktivní (DX1)
10.11.22.8	10.200.193.70	3389	RDP	Terminal services	administrativní přístup z admin zóny SBS k SAProuteru/SAP Web Dispatcheru v ČSSZ
10.11.22.10	10.200.193.70	3298 3299	"SAP"	saprouter	přístup z interního SAProuteru SBS k SAProuteru v ČSSZ
10.11.22.10	10.200.193.70	80 81	http	Apache	přístup z VYP testovacího (DX5) na BT(NEM) a KE2
10.11.22.9	10.200.193.70	80 81	http	Apache	přístup z VYP testovacího (DX5) na BT(NEM) a KE2
10.11.22.4 10.11.22.5	10.200.193.70	80 81	http	Apache	přístup z VYP konsolidačního (DX2) na BT(NEM) a KE2
10.11.22.4 10.11.22.5 10.11.22.11 10.11.22.12	10.200.15.193	80 81	http	Apache	přístup z SAP-HR produktivního (DU1) na AAA
10.11.22.7	10.200.193.70	80 81	http	Apache	přístup z SAP-HR konsolidačního (DU2) na AAA
10.11.22.7	10.200.193.70	80 81	http	Apache	přístup z SAP-HR testovacího (DU5) na AAA
10.11.22.8	10.200.193.58 10.201.193.58	3389	RDP	Terminal services	administrativní přístup z admin zóny SBS k produktivním SAProuterům/SAP Web Dispatcherům v ČSSZ po dobu podpory náběhu
10.11.22.4 10.11.22.5	10.200.193.58 10.201.193.58	3298 3299	"SAP"	saprouter	přístup z interního SAProuteru SBS k produktivním SAProuterům v ČSSZ
10.11.22.11 10.11.22.12 10.11.22.14	10.200.15.193	80 81	http	Apache	přístup z VYP produktivního (DX1) na aplikace v APP vrstvě ČSSZ prostřednictvím SAPproxy

3.6 Rozklad zátěže na servery

Pokud není aplikace bezestavová, je nutné na síťové vrstvě load balanceru ACE zajistit tzv. „session persistence“. Tento jednoznačný identifikátor se vkládá do HTTP hlavičky a pomocí něho je zajištěno na síťové úrovni přesměrování všech požadavků stále na stejný server.

V prostředí ČSSZ používáme následující identifikátory:

- iv-user - posílá WebSeal
- XX-CSSZDMSSessionHeader - posílá BizTalk (DIS, NEM WF) při komunikaci se stavovou částí DMS API (login, createDocument, logout)

Pro komunikaci na aplikační úrovni se využívá protokol HTTP 1.0. Pokud je využíván protokol HTTP 1.1. je třeba zajistit, aby v rámci jednoho TCP spojení byl použit pouze jeden konkrétní identifikátor.

4. PŘÍLOHY

4.1 Kompletní tabulka datových toků

Součástí tohoto odstavce je hrubé vymezení možných protokolů a datových toků, jež se v prostředí datových center ČSSZ mohou/nemohou vyskytovat.

Z pohledu OSI modelu na jeho třetí vrstvě koncept počítá s IP protokolem verze 4 (ICMP, ARP, směrovací protokoly – OSPF, RIP, EIGRP). Na třetí vrstvě v datovém centru se neobjeví NetBEUI, IPX, DDP atp. Ve čtvrté vrstvě OSI modelu je tok omezen na TCP resp. UDP. Na této vrstvě se neobjeví protokoly NetBEUI, RTP, SCTP, ATP, NBP, AEP, RTMP či SPX. Koncept též nepočítá s propagací Multicastů mezi vrstvami.

Cíl / Zdroj	Infrastrukturní servery	WAN	LAN	Proxy vrstva	Vrstva správy a adminitrace IS	Aplikační vrstva	Databázová vrstva	Externí sítě, Internet
Infrastrukturní servery		Neomezeno	Neomezeno	Zakázáno	Omezeno	Zakázáno	Zakázáno	Omezeno
WAN	Neomezeno		Omezeno	HTTPS	Omezeno	Zakázáno	Zakázáno	Zakázáno
LAN	Neomezeno	Omezeno		HTTPS	Omezeno	Zakázáno	Zakázáno	Zakázáno
Proxy vrstva	Zakázáno	Zakázáno	Zakázáno		komunikace AAA portálu	HTTP	Zakázáno	Zakázáno
Vrstva správy a adminitrace IS	(TS,SNMP,...)	(TS,SNMP,...)	(TS,SNMP,...)	(TS,SNMP,...)		(TS,SNMP,...)	(TS,SNMP,...)	Omezeno
Aplikační vrstva	Zakázáno	Zakázáno	Zakázáno	Omezeno	Omezeno		SQL	Zakázáno
Databázová vrstva	Zakázáno	Zakázáno	Zakázáno	Zakázáno	Omezeno	Zakázáno		Zakázáno
Externí sítě, Internet	Zakázáno	Zakázáno	Zakázáno	Zakázáno	Zakázáno	Zakázáno	Zakázáno	

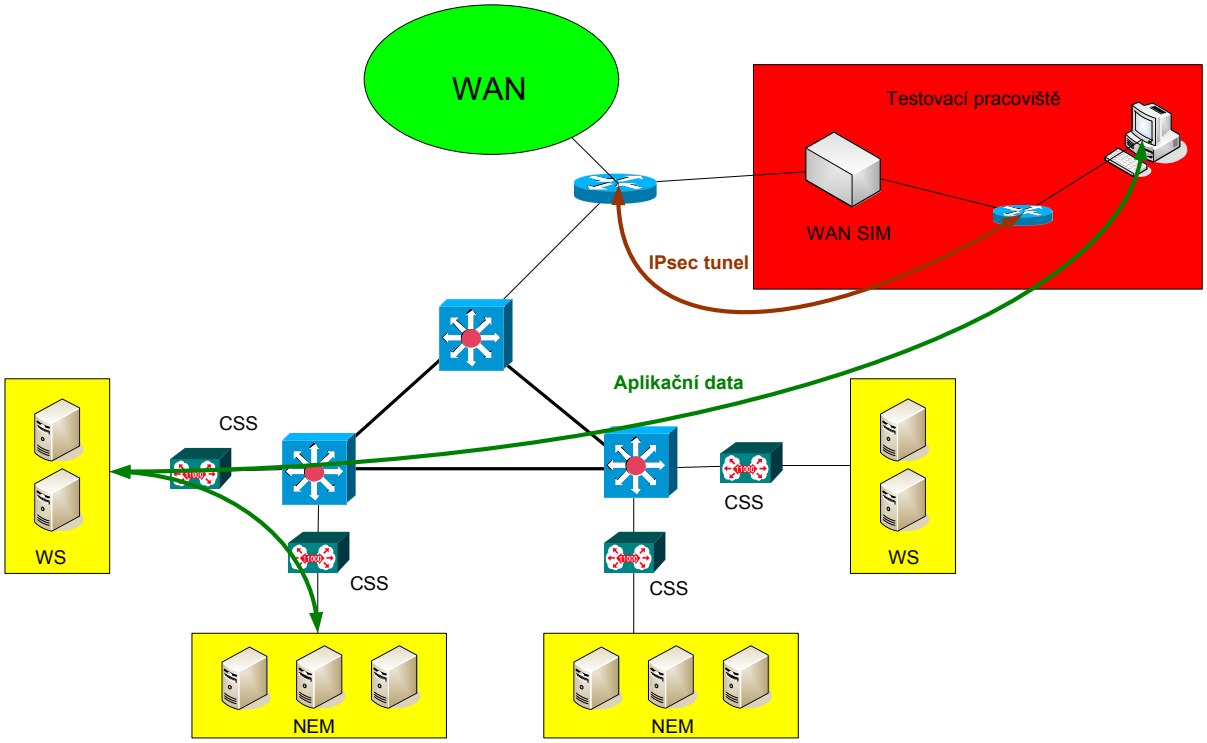
Komunikace označená v tabulce jako „omezeno“ je filtrována pravidly, která jsou nastavena na firewallech a přístupových seznamech.

4.2 Definice simulačního WAN prostředí

Celé simulační prostředí se skládá z těchto bloků:

- Dedikovaný síťový segment
- Simulace IPsec prostředí včetně MTU size
- Simulace omezení pásma – od 512kbit do 4Mbit
- Simulace latence – 0ms až 1000ms RTT
- Simulace QoS tříd
- Proměnlivý tok na lince – resp. simulace dalších souběžných aplikací
- WAN simulační box

Klient je připojen do segmentu za směrovač stejně jako na WAN pobočce. Směrovač je nastaven jako VPN šifrátor se stejným rozložením QoS tříd. WAN simulátor zajistí šířku pásma, latenci, chybovost a další datový tok. Klient přistupuje k AAA portálu a aplikacím standardně jak je zvyklý.



Obrázek 10 – Testovací prostředí WAN

Toto prostředí bylo zbudováno se záměrem „dopravit“ WAN prostředí co nejblíže vývojářům a usnadnit jim testování aplikací přes WAN síť.

5.POŽADAVKY NA PROSTUPY V RÁMCI POČÍTAČOVÉ SÍTĚ ČSSZ

5.1 Standardní prostupy

Standardním prostupem se rozumí komunikační kanál v rámci jedné nebo více vrstev, který je definován v kapitole 3.2. tohoto dokumentu.

Žádost o zajištění prostupu se podává formou tiketu ServiceDesk, jehož součástí je i řádně vyplněný, podepsaný a naskenovaný formulář „Požadavek na nastavení síťových průstupů v infrastruktuře ČSSZ“, který obsahuje všechny požadované nastavení a komunikační toky ze strany žadatele.

Žadatelem o standardní prostupy je vždy garant za ČSSZ, který je i nositelem plné zodpovědnosti za úplnost zadání.

Pokud nebude žádost obsahovat potřebné informace k nastavení na úrovni sítě, bude žadatel vyzván k doplnění, tak, aby bylo možné prostup realizovat.
V případě, že bude prostup shledán jako nestandardní, bude vrácen žadateli k přepracování.

Standardní doba na aplikaci prostupů je do 2 dnů, pokud je potřeba nastavení provést urgentně je nutné toto uvést do přiloženého formuláře ve formě poznámky.

Požadavky na prostupy nelze vyřizovat okamžitě, neboť konfigurační změny v produkční oblasti lze dělat pouze v době odstávkových oken a to v úterý a ve čtvrtek.

Požadavek na nastavení síťových průstupů v infrastruktuře ČSSZ

Standardní požadavek v souladu s platným standardem sítě ČSSZ

Žadatel

Jméno a příjmení: ..... Platnost požadavku*:

Odbor: ....

Funkce: .....

*) Pokud se jedná o dočasný požadavek, uveďte jeho platnost od – do. V případě, že uvedete pouze od, bude se pokládat průstup za trvalý.

Odůvodnění požadavku

(Žadatel popíše detailně svůj požadavek, součástí popisu bude i informace k čemu daný prostup bude sloužit a jakým systémem či aplikací bude využíván, případně k tomuto požadavku připojí též schéma či obrázek.)

Technická specifikace požadavku

Zdroj	Cíl	Protokol	Port	Popis

Zdroj - zdrojová IP adresa (servery, VIP adresy, aplikace, IP sítí atd.)
Cíl - cílová IP adresa (servery, VIP adresy, aplikace, IP sítí atd.)
Protokol – síťový protokol
Port - síťový port (např. 80,443,5666 atd.)
Popis – stručný popis požadovaného prostupu

Poznámka

(Sem napište své další poznámky, případně komentáře)

Žadatel svým podpisem stvrzuje, že se seznámil s platným standardem síťové infrastruktury a požaduje nastavení výše uvedeného požadavku. Síťové prostupy jsou zřizovány do 2 pracovních dní od přijetí požadavku.

Datum: .....

5.2 Nestandardní prostupy (výjimky ze standardu)

Nestandardním prostupem (výjimkou) se rozumí komunikační kanál v rámci jedné nebo více vrstev, který není definován v kapitole 3.2. tohoto dokumentu.

Žádost o zajištění prostupu se podává formou tiketu ServiceDesk jehož součástí je i řádně vyplněný, podepsaný a naskenovaný formulář „Požadavek na nastavení nestandardních síťových průstupů v infrastruktuře ČSSZ", který obsahuje všechny požadované nastavení a komunikační toky ze strany žadatele a příslušné podpisy všech schvalovatelů. Originál formuláře bude doručen na sekretariát odboru 52 k uložení do archivu.
Žadatelem o nestandardní prostupy je vždy garant za ČSSZ, který je i nositelem plné zodpovědnosti za úplnost zadání.

Pokud nebude žádost obsahovat potřebné informace k nastavení na úrovni sítě, bude žadatel vyzván k doplnění, tak, aby bylo možné prostup realizovat.
V případě, že bude prostup shledán jako standardní, bude vrácen žadateli k přepracování.

Standardní doba na aplikaci prostupů je do 2 dnů, pokud je potřeba nastavení provést urgentně je nutné toto uvést do přiloženého formuláře ve formě poznámky.
Požadavky na prostupy nelze vyřizovat okamžitě, neboť konfigurační změny v produkční oblasti lze dělat pouze v době odstávkových oken a to v úterý a ve čtvrtek.

Požadavek na nastavení nestandardních síťových prostupů v infrastruktuře ČSSZ

Požadavek na výjimku s platným standardem sítě ČSSZ

Žadatel

Jméno a příjmení: ..... Platnost požadavku*):
Odbor: ....

Funkce: .....

*Pokud se jedná o dočasný požadavek, uveďte jeho platnost od – do. Požadavek na výjimku má vždy dočasnou platnost, tedy je nutné uvést.

Odůvodnění požadavku

(Žadatel popíše detailně svůj požadavek, součástí popisu bude i informace k čemu daný prostup bude sloužit a jakým systémem či aplikací bude využíván, případně k tomuto požadavku připojí též schéma či obrázek.)

Technická specifikace požadavku

Zdroj	Cíl	Protokol	Port	Popis

Zdroj - zdrojová IP adresa (servery, VIP adresy, aplikace, IP sítí atd.)
Cíl - cílová IP adresa (servery, VIP adresy, aplikace, IP sítí atd.)
Protokol – síťový protokol
Port - síťový port (např. 80,443,5666 atd.)
Popis – stručný popis požadovaného prostupu

Souhlas odboru koncepcí, systémové integrace a koordinace (odb.51)

Souhlasí/nesouhlasí *)

Datum: .....

Podpis ŘO51: .....

*nehodící se, škrtněte.

6. ZÁVĚR

Tento dokument popisuje standardy komunikační infrastruktury uvnitř datových center, její členění do bezpečnostních zón a definuje směr a typ datových toků mezi nimi.

7. SEZNAM ZKRATEK

AAA	Authentication, Authorization and Accounting
ACE	Application Control Engine
ACS	Advanced Connectivity System
AD	Active Directory
ADM	Administrator
AEP	Application Environment Profile
AP	Access Point
APL	Aplikace
ARP	Address Resolution Protocol
ATP	Asynchronous Transaction Processing
B2B	Business to business
BT	Biztalk
CA	Certifikační autorita
CMS	Centrální místo služeb
ČSSZ	Česká správa sociálního zabezpečení
DB	Databáze
DC	Datové centrum
DDP	Distributed Data Protocol
DIS	Aplikace e-Podání
DMS	Document management system
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DÚ	Datové úložiště
DWDM	Dense Wavelength Division Multiplexing
DX	Označení serverů SAP
EIGRP	Enhanced Interior Gateway Routing Protocol
EXT	Externista
FC	Fibrechannel
FW	Firewall
HB	Hlavní budova
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IBM	International Business Machines Corporation
ICMP	Internet Control Message Protocol
IDS	Intrusion detection system
IIS	Integrovaný Informační Systém
IKR	Integrované Komunikační Rozhraní
IKT	Informační a Komunikační Technologie
iMC	HP Intelligent Management Center
INF	Informace
IO	Input-output
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
IS	Informační systém
ITAM	IBM, Tivoli Access Manager
ITIM	IBM, Tivoli Identity Manager
K25	Praha 5, Křížová 25
K6	Praha 5, Křížová 6
KDC	Key Distribution Center
KE	Kmenová evidence
KSSZ	Krajská správa sociálního zabezpečení

L3	Network Layer 3
LAN	Local Area Network (též LAN, lokální síť, místní síť)
LDAP	Lightweight Directory Access Protocol
LPS	Lékařská posudková služba
Mbps	Megabits per second
MGMT	Management
MPLS	Multiprotocol Label Switching
MS	Microsoft
MSSZ	Městská správa sociálního zabezpečení
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NEM	Nemocenská
NetBEUI	NetBIOS Extended User Interface
OS	Operační systém
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSSZ	Okresní správa sociálního zabezpečení
PC	Personal Computer
PIX	CISCO PIX
PKIDB	Databáze certifikační autority
POJ	Aplikace-Pojistné
PPRC	Miroring IBM
PRN	Print
PSSZ	Pražská správa sociálního zabezpečení
QoS	Quality of Service
RAC	DB cluster-Oracle
RADUIS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RO	Read-ounly
RTMP	Routing Table Maintenance Protocol
RTP	Real-Time Protocol
RTT	Round Trip Time
RW	Read-write
ŘO	Ředitel odboru
SAN	Storage area network
SAP	Systems, Applications & Products in Data Processing
SBS	Siemens Bussines Services
SCTP	Stream Control Transmission Protocol
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange
SQL	Structured Query Language
SRV	Server
SSL	Secure Sockets Layer
T13	Praha 8, Trojská 13
TCP	Transmission Control Protocol
TMP	Temporery
UOJ	Ústřední organizační Jednotka
ÚP	Územní pracoviště
UPS	Uninterruptible Power Supply/Source
USR	User
VC	Výplatní cyklus
VIP	Virtual Internet Protocol
VLAN	Virtuální LAN
vNIC	Síťová karta
VPN	Virtual Private Network
VYP	Aplikace-výplaty
WAE	WAN Accelerator Engine

WAN	Wide Area Network
WF	Workflow
WiFi	Wireless Fidelity
WS	Webová služba