Příloha 1.

Specifikace funkčních požadavků na Centrální místo služeb - Komunikační infrastruktura Informačních systémů veřejné správy, verze 2.0

Příloha 1.

OBSAH DOKUMENTU

Příloha 1.

Příloha 1.

Příloha 1.

SEZNAM OBRÁZKŮ

1 Úvod

1.1 Historie

Komunikační infrastruktura veřejné správy[1] byla navržena jako centralizovaná komunikační infrastruktura s Centrálním místem služeb[2], které je jediným místem výměny dat mezi jednotlivými informačními systémy veřejné správy[3] a zároveň jediným místem propojení k veřejné síti internet a specifických neveřejných sítí např. sítí Evropské unie.

Současné řešení CMS odpovídá možnostem v době jeho plánování a výstavby a také tomu, že se nepodařilo některé chystané kroky dokončit (například geografická redundance). CMS si s sebou určitým způsobem nese historii předchozích snah o vytvoření společné komunikační infrastruktury VS (GOVNET a GOVBONE).

1.2 Stručné shrnutí současného stavu

Technologie současného CMS jsou převážně instalovány v budově Ministerstva vnitra, Olšanská 4. Část technologie Interconnect[4] je umístěn v hostingovém centru Telefonica O2 Nagano. Přestože technologicky bylo počítáno s členěním do celků za cílem dosažení geografické redundance, některé z plánovaných vlastností se nepodařilo do současnosti realizovat.

Příkladem doposud nerealizovaného cíle je právě zejména zajištění geografická redundance. Díky tomuto nedostatku není CMS odolné např. proti živelným pohromám a jiným typům neplánovaných výpadků. ServiceDesk[5] pro subjekty KIVS nezajišťuje všechny požadované služby, není garantován provoz portálu CMS pro subjekty KIVS. Zároveň není dostatečně definováno řízení bezpečnostních politik jednotlivých OVM[6]. Víceméně manuální provisioning[7] služeb je zajištěn pro stávající omezený počet uživatelů.

Pro další rozvoj eGovernmentu je současné CMS omezující zejména v těchto oblastech:

- Poskytuje služby víceméně pouze pro centrální orgány
- Není definitivně dořešen hosting[8] stávajících a budoucích ISVS
- Není vybudována geografická redundance

---

[1] Dále jen KIVS

[2] Dále jen CMS

[3] Dále jen ISVS

[4] Viz. terminologický slovník

[5] Viz. terminologický slovník

[6] Orgán veřejné moci

[7] Viz. terminologický slovník

[8] Viz. terminologický slovník

- Služby Help Desku[9] a Service Desku nejsou dostatečně rozvinuté či vůbec neexistují
- Způsob zřizování služeb (service provisioning) je potřeba optimalizovat
- Míra efektivity
- Forma řízení informační bezpečnosti
- Omezená interoperabilita mezi OVM
- Nedefinované standardy a implementace SW prostředků pro integraci souvisejících IS

1.3 Cíle a mise

Z výše uvedených důvodů jednoznačně vyplývá nezbytnost modernizace CMS, aby umožnilo další rozvoj eGovernmentu v České republice. Toto nové CMS jsme nazvali CMS 2.0. Bude hlavním přípojným a propojovacím místem pro všechny základní služby eGovernmentu, ať už existující nebo nově budované (z IOP[10] nebo státního rozpočtu).

CMS má v budoucí podobě vytvořit základní stavební prvek celé KIVS. Bude realizovat služby pro výměnu dat a služeb mezi jednotlivými ISVS, resp. bude umožňovat, aby každý pracovník VS prostřednictvím služeb CMS získal efektivnější přístup k informacím, na které má dle platné legislativy nárok. KIVS také poskytuje všechny potřebné služby ke komunikaci v celé VS a zajišťuje komunikaci v rámci Evropské unie (dále jen „EU"), a to jak s orgány veřejné správy jednotlivých členských států, tak s orgány EU.

CMS dále zajistí propojení jednotlivých technologických center ORP[11] a Krajů[12], propojení regionálních a metropolitních infrastruktur, dále zajistí realizaci generických a centrálních služeb pro eGoncentra. Bude realizovat služby centrální podpory uživatelů (Služby ServiceDesk). Součástí CMS vzniknou i datové sály CMS pro hostování infrastruktury CMS a centrálních systémů eGovernment, včetně infrastruktury pro související systémy – např. Czechpoint a další. CMS má v budoucnu zajišťovat i propojení a konsolidaci služeb hlasové telefonie pro subjekty KIVS. CMS bude poskytovat infrastrukturu pro dohled, monitoring a řízení služeb poskytovaných nebo provozovaných v rámci CMS.

---

[9] Viz. terminologický slovník

[10] Integrovaný operační program

[11] Obec s rozšířenou působností

[12] Technologická centra ORP a Krajů dále jen eGoncentra

2 Současný stav

2.1 Obecný popis stávající architektury a funkcí

Infrastruktura CMS je navržena jako redundantní infrastruktura s možností dislokace do dvou geograficky rozdílných a vzájemně oddělených vzdálených nezávislých a neovlivnitelných lokalit (napájení, topologická nezávislost přípojných a propojovacích optických tras apod.)

Vzájemné propojení topologicky nezávislých lokalit CMS je řešeno prostřednictvím DWDM[13]/CWDM[14] technologie. V současnosti jsou přes DWDM technologii propojeny pouze páteřní uzly sítě InterConnect-I (Olšanská 4 – HC Nagano), ostatní bloky redundantní infrastruktury jsou dislokovány do výpočetního sálu v lokalitě Olšanská 4, Praha 3 a propojeny lokálně metalickými a multi-mode[15] optickými spoji. Přenosová kapacita prostředí CMS na úrovni fyzických rozhraní je 1 Gbit/s.

Infrastruktura je logicky rozčleněna do základních pěti funkčních celků:

- Propojovací síť poskytovatelů „InterConnect-I"
- Bezpečné propojení resortních VPN[16] „Central Firewall"
- Sdílené služby „Shared Services"
- Externí firewall[17] „External Firewall"
- Připojení k externím sítím „InterConnect-E

[13] Dense WDM (wavelength-division multiplexing), viz. terminologický slovník

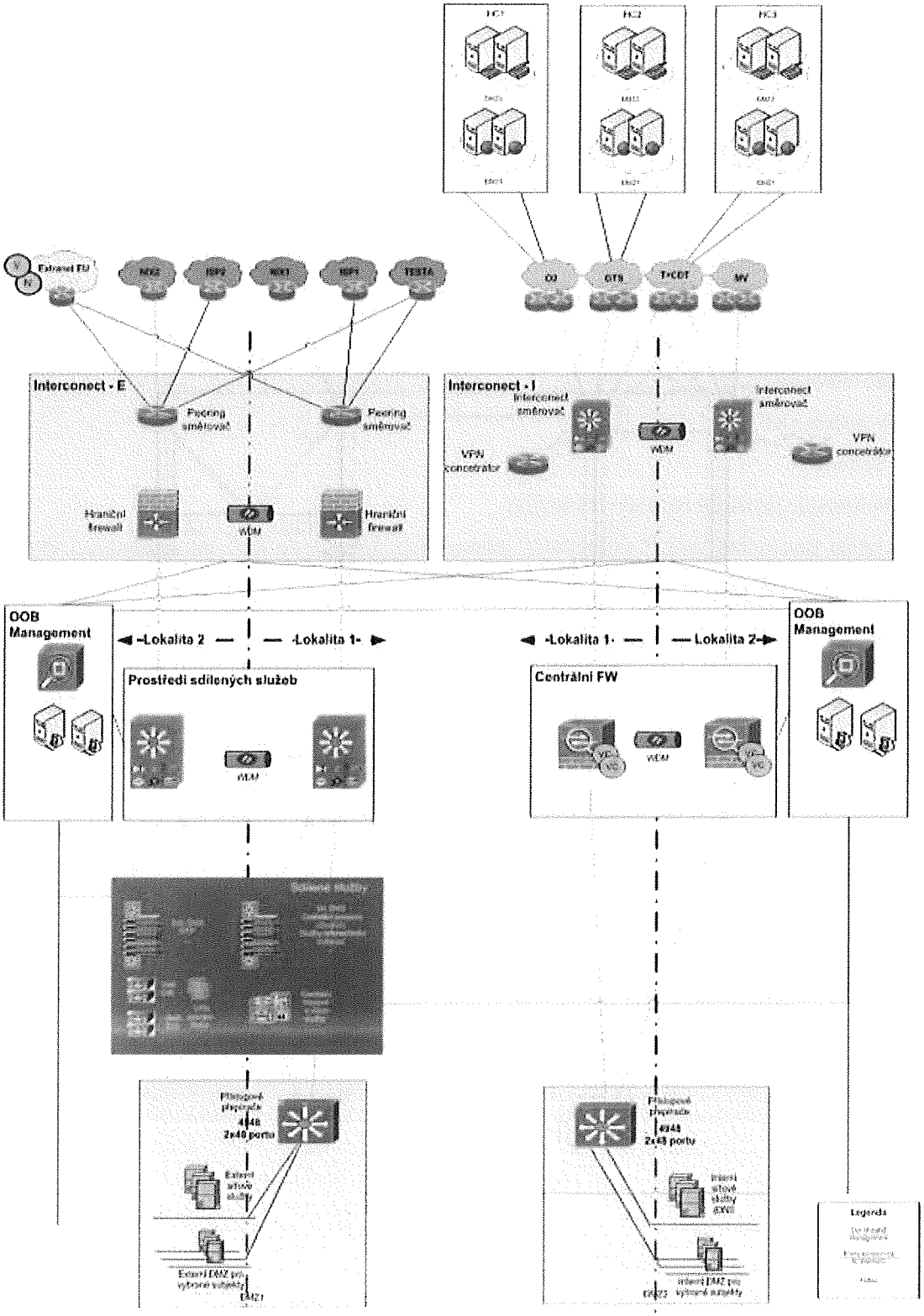
[14] Coarse WDM (wavelength-division multiplexing), viz. terminologický slovník

[15] Viz. terminologický slovník

[16] Virtual Private Network, viz. terminologický slovník

[17] Viz. terminologický slovník

Hardwarová podoba, vzájemné propojení a forma jednotlivých bloků je patrná z následujícího obrázku:



Obrázek 1 Bloky CMS - HW podoba, propojení, forma

2.1.1 Blok InterConnect-I

Primární funkcí toho bloku je propojení páteřní infrastruktury poskytovatelů (KIVS), kteří poskytují své služby pro orgány veřejné správy tak, aby se docílilo maximální možnosti volby jednotlivých dílčích služeb dle výhodnosti od různých operátorů. InterConnect-I je vybudován jako plně geograficky redundantní propojovací uzel páteřních sítí operátorů. Je určen k propojení dvou dílčích geograficky redundantních uzlů s redundantním napojením jednotlivých zúčastněných poskytovatelů.

Do propojovací sítě InterConnect-I jsou připojeni následující poskytovatelé služeb:

- Telefónica O2
- GTS Novera
- ČD Telematika
- České radiokomunikace
- Dial Telecom
- Ha-vel internet
- T-Systems
- Ministerstvo vnitra ČR (stávající ITS MVČR)

Součástí bloku jsou mimo WAN[18] směrovačů[19] připojených směrem do KIVS infrastruktury i VPN koncetrátory[20] pro terminaci šifrovaných tunelů z internetu.

Blok tedy vzájemně propojuje toky z KIVS infrastruktury (v rámci VPN realizovaných jinými poskytovateli služeb) a dále poskytuje jednoznačný přístup směrem k sousednímu bloku - Central Firewall pro realizaci bezpečnostního perimetru pro případ požadavku přístupu ke službám CMS obecně.

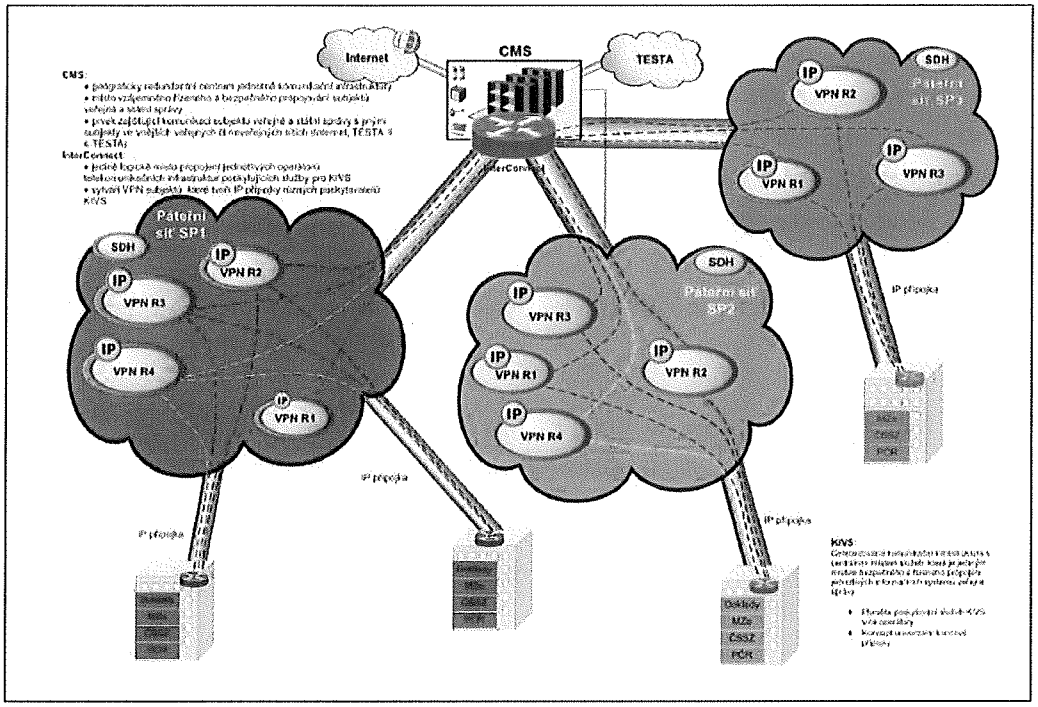
---

[18] Wide Area Network, viz. terminologický slovník

[19] Viz. terminologický slovník

[20] Viz. terminologický slovník

Z následujícího obrázku vyplývá obecná forma propojení infrastruktury KIVS na CMS:



Obrázek 2 Vazba transportní infrastruktury KIVS na CMS

2.1.2 Blok Central Firewall

Vstupní Layer-3 rozhraní každého subjektu připojujícího se do prostředí CMS je zrealizováno na pro tento subjekt vyhrazeném virtuálním firewallu[21], jakákoliv komunikace směrující ze subjektu do prostředí či naopak tedy musí projít tímto VFW.

VFW jednotlivých subjektů jsou přes své vnitřní rozhraní napojení na řídící modul zařízení CFW, který zajišťuje směrování provozu dále do prostředí.

Součástí tohoto bloku jsou i prostředky pro rozklad zátěže, které mohou být využity při směrování provozu na instance v DMZ2, apod.

Virtuální firewall jako vstupní prvek každého zákazníka do prostředí CMS obsahuje vždy minimálně 3 základní Layer-3 rozhraní:

- Vstupní rozhraní od zákazníka (ve směru od funkčního bloku IC-I). Přes toto rozhraní budou směrovány adresní rozsahy zákazníka, které využívá ve své vnitřní síti
- Vstupní rozhraní do prostředí CMS (směrem ke sdíleným službám a ostatním zákazníkům prostředí). Zde je směrována default route či konsolidovaný adresní rozsah.
- Management rozhraní (přístup management nástrojů prostředí a administrace)

[21] Dále jen VFW

Dále pak na tomto VFW mohou být vytvořena další rozhraní dle individuálních potřeb jednotlivých zákazníků – nejčastěji se bude jednat o:

- Demilitarizované zóny[22] DMZ2 (Zóny pro umístění zákaznických zařízení v hostingových centrech, která mohou obsahovat služby, které chtějí zákazníci sdílet s dalšími subjekty připojenými do prostředí či případně budou soužit jako backend pro zařízení umístěná v demilitarizovaných zónách DMZ1 (tj. pro zdroje primárně publikované do internetu). Těchto zón může být na VFW vytvořeno více v závislosti na preferencích zákazníka.
- Komunikační spojky mezi funkčními bloky (nejčastěji pro provoz, který nelze provozovat přes sdílené služby či například jeho provoz přes proxy servery nedovolují bezpečností požadavky apod.)

2.1.3 Shared Services

Základním úkolem tohoto funkčního bloku je realizace tzv. sdílených služeb, které představují další bezpečnostní stupeň v prostředí sítě CMS nebo poskytují podpůrné síťové služby.

Blok je tvořen instancemi firewallu, prostředků pro rozklad zátěže a dále L2 infrastrukturou pro připojení serverů a instancí vlastních sdílených služeb.

Příkladem bezpečnostních služeb, které jsou součástí tohoto bloku, může být Web GW, Mail GW, FTP proxy, atd.

Příkladem podpůrných služeb je DNS proxy či NTP proxy. Obě skupiny služeb se samozřejmě ve své podpůrné či bezpečnostní funkci mísí a doplňují.

Prostřednictvím firewallů tohoto bloku jsou realizovány VFW pro sítě sdílených služeb a dále též DMZ1. Prostředky pro rozklad zátěže zde slouží k balancování provozu na instance sdílených služeb a též pro rozklad zátěže na instance umístěné v DMZ1.

2.1.4 Blok External Firewall

Jedná se o standardní plně redundantní cluster externích firewallů, které představují perimetrovou ochranu prostředí směrem z Internetu.

Primárním smyslem tohoto bloku je tedy aplikace bezpečnostních pravidel pro zejména příchozí komunikaci z internetu. Dále realizuje standardní funkce překladu privátních IPv4 adres dle stanovených pravidel, základní inspekce definované sady aplikačních protokolů, atd.

2.1.5 Blok InterConnect-E

InterConnect-E je plně redundantní zdvojený peeringový přístupový uzel do sítě Internet a do externích sítí jako je např. sTESTA[23]. Blok je dále vybaven bezpečnostními moduly pro detekci průniků a anomálií.

---

[22] Viz. terminologický slovník

[23] Zabezpečená komunikační infrastruktura EU

Připojení k Internetu je realizováno redundantně vždy jedním okruhem z každého peeringového uzlu ke všem poskytovatelům.

Evropská síť sTESTA je připojena ke každému peeringovému uzlu jedním 2.048 Mbit/s okruhem.

Peeringové routery jsou připojeny na funkční blok External Firewall. Dále jsou navíc připojeny do funkčního bloku InterConnect-I pro realizaci služby „čistý Internet".

2.2 Seznam základních poskytovaných služeb v rámci stávajícího CMS

2.2.1 Základní služba CMS

Představuje IP VPN konektivitu subjektu KIVS směrem na Centrální FW CMS. Realizace „Základní služby CMS" znamená pro každou takto vytvořenou IP VPN aktivovat a alokovat na Centrálním FW CMS samostatný virtuální FW kontext daného subjektu. Realizace této služby je základní podmínkou, kterou musí subjekt splnit, pokud chce odebírat některé další služby CMS.

2.2.2 Přímé připojení k Internetu

Reprezentuje přímé poskytnutí centrálního sdíleného Internetu do IP VPN přípojky subjektu KIVS. Realizace má formu další logicky oddělené IP VPN paralelně ke standardní VPN subjektu reprezentované službou „Základní služba CMS". Adresní rozsahy služby „Přímé připojení k Internetu" mohou být přiděleny z rozsahu adres CMS, nebo z adresního rozsahu vlastněného subjektem, pokud má „provider independent adresy". Připojený Internet není žádným způsobem filtrován a kontrolován.

2.2.3 Bezpečné připojení k Internetu

Jedná se o službu připojení centrálního sdíleného Internetu přímo do zákaznické IP VPN přípojky KIVS realizované službou „Základní služba CMS". Připojení má následující vlastnosti:

- Veškerý provoz z/do Internetu je překládán
- Pro odchozí provoz bude dedikována pro každý subjekt 1 veřejná IP adresa z rozsahu přiděleného CMS
- V rámci komunikace do Internetu budou nativně povoleny následující protokoly:
  - HTTP[24]/HTTPS[25]/FTP[26] přes HTTP
  - IMAP4/IMAP4S
  - POP3/POP3S
  - FTP

[24] **Hypertext Transfer Protocol, viz. terminologický slovník**

[25] **Hypertext Transfer Protocol Secure, viz. terminologický slovník**

[26] **File Transfer Protocol, viz. terminologický slovník**

Ostatní protokoly budou implicitně blokovány a jejich povolení bude podléhat schválení provozovatele CMS a bezpečnostního správce CMS v rámci individuálního zákaznického projektu. Provoz HTTP/S je dále možno kontrolovat na přítomnost škodlivého kódu.

2.2.4 Přístup subjektů KIVS do zákaznické VPN přes Internet

Služba slouží k zajištění připojení LAN[27] sítí daného subjektu KIVS do jeho IP VPN přípojky KIVS přes Internet. Služba je určena rozsáhlým subjektům KIVS zejména pro připojení jejich regionálních pracovišť/poboček/lokalit. Takto připojená síť má stejná přístupová práva jako standardní uživatel VPN KIVS, jehož konektivita je řešena standardní formou. Přístup je realizován na bázi SSL[28] či IPSec[29] VPN tunelů přes prostředí Internet LAN – LAN formou.

2.2.5 Přístup koncových uživatelů subjektů KIVS do zákaznické VPN přes Internet

Služba slouží k zajištění přístupu koncových uživatelů daného subjektu KIVS do VPN prostředí jeho přípojky KIVS. Takto připojený uživatel má stejná přístupová práva jako standardní uživatel VPN KIVS. Přístup je realizován na bázi SSL/IPSec tunelů přes prostředí Internet formou klient – LAN. Služba je koncovému uživateli zřízena na základě žádosti subjektu KIVS, nikdy nemůže zřízení služby proběhnout na základě žádosti koncového uživatele.

2.2.6 Služby S-TESTA

Jedná se o zákaznickou službu přístupu do sítě EU. Služba je vždy zřizována na základě individuálního zákaznického projektu v souladu s požadavky EU pro provoz této sítě.

2.2.7 Propojení s jiným subjektem KIVS

Služba je určená pro vzájemnou komunikaci jednotlivých subjektů mezi sebou. Pro zřízení služby je nutný písemný souhlas obou propojovaných subjektů, až na jeho základě může být služba zřízena.

2.2.8 Služby DNS[30] Internet

Jedná se o jmenné služby směrem do Internetu.

2.2.9 Služby MTA[31]

Služba elektronické pošty zajišťuje předávání zpráv elektronické pošty jak mezi jednotlivými subjekty KIVS, tak mezi subjekty KIVS a uživateli sítě Internet. Služba zajišťuje pouze předávání zpráv, nikoliv funkcionalitu e-mailových schránek. Služba má tyto základní parametry:

- Redundantní řešení - primární a záložní MTA server

---

[27] Local Area Network, viz. terminologický slovník

[28] **Secure Sockets Layer, viz. terminologický slovník**

[29] **Internet Protocol Security, viz. terminologický slovník**

[30] Domain Name System, viz. terminologický slovník

[31] Mail Transfer Agent, viz. terminologický slovník

- Veškerý provoz elektronické pošty je kontrolován na přítomnost škodlivého kódu
- Veškerá příchozí pošta bude směrována z CMS na poštovní servery subjektu
- Každá příchozí a odchozí zpráva je kontrolována na přítomnosti virů, a zda se nejedná o spam
- Přílohy známých kompresních formátů se rozbalí a zkontrolují na viry
- Spam je klasifikován a značkován v hlavičce subjektu

2.2.10 Služby DMZ1

Služba DMZ1 je vytvoření prostředí pro publikaci služeb subjektů KIVS do Internetu. Služba spočívá ve vytvoření vlastního virtuálního FW v rámci internetového FW pro směrování DMZ sítě daného subjektu a její konektivity do Internetu. Služby DMZ1 jsou zřizovány na základě individuálního zákaznického projektu, do kterého provozovatel CMS doplní závazná bezpečnostní pravidla a tuto DMZ1 zřídí. Fyzicky jsou členské instance DMZ (servery subjektu) umístěny buď přímo u subjektu nebo v hostingovém centru. Konektivita mezi virtuálním FW a vlastními instancemi je potom realizována jako samostatná oddělená IP VPN.

2.2.11 Služby DMZ2

Služba DMZ2 je vytvoření prostředí pro publikaci služeb subjektů KIVS do CMS, nebo pro umístění back-end serverů pro publikaci aplikaci/služeb do internetu (front-end servery jsou v tomto případě v DMZ1). Službu DMZ2 je také dále možné využít pro umístění serverů subjektu bez jejich publikace do CMS (bezpečné oddělení aplikací a aplikačních serverů subjektu od jeho uživatelů). V rámci této služby je subjektu poskytnut vlastní virtuální FW pro vytvoření DMZ2 daného subjektu. Jde o totožný virtuální FW, který je subjektu přidělen v rámci služby „Základní služba CMS". Fyzicky jsou členské instance DMZ (servery subjektu) umístěny buď přímo u subjektu nebo v hostingovém centru. Konektivita mezi virtuálním FW a vlastními instancemi je potom realizována jako samostatná oddělená IP VPN.

2.3 Seznam housingových služeb

Současné CMS slouží zároveň jako housingové centrum pro následující systémy MVČR[32]:

- CzechPOINT
- GroupWise a Teaming
- Portál veřejné správy, ePUSA
- Web MVČR
- Portál CMS

Technologický sál CMS je tak částečně i konsolidačním prvkem pro rezortní systémy, pro které v současnosti chybí vlastní housingová kapacita.

[32] Ministerstvo vnitra České republiky

3 Katalog služeb CMS NGN - CMS 2.0

3.1 Kategorizace služeb

3.1.1 Služby síťové vrstvy

3.1.1.1 Přístupové služby

- Vytvoření univerzální přípojky KIVS včetně vytvoření VPN OVM mezi různými poskytovateli komunikačních služeb
- Krajský konektor CMS 2.0
- Extranet CMS 2.0
- Internetové přístupy

3.1.1.2 Propojovací služby

- Vytvoření konektoru firewall VPN OVM
- Realizace připojení lokality OVM do mateřské VPN přes Internet
- Přístup koncových uživatelů subjektů OVM do mateřské VPN přes Internet
- Realizace připojení VPN OVM do Extranetu CMS 2.0 přes Internet
- Přístup koncových uživatelů subjektů OVM menšího rozsahu do Extranetu CMS 2.0 přes Internet
- Vzájemné propojení různých VPN OVM
- Vzájemné propojení VPN OVM s VPN S-TESTA
- Bezpečné připojení VPN OVM k Internetu
- Přímé propojení VPN OVM s Internetem
- DMZ1
- DMZ2
- MTA
- Vzájemné propojení informačních systémů centrálních služeb prostřednictvím eGon Service Bus

3.1.2 Systémové a bezpečnostní služby

- Služby rozkladu zátěže
- Management služby – monitoring a reporting
- Služby účtování – billing
- Provisioning a provoz služeb

3.2 Popis služeb a jejich očekávaných parametrů v rámci CMS 2.0

3.2.1 Přístupové služby síťové vrstvy

3.2.1.1 Vytvoření univerzální přípojky KIVS včetně vytvoření VPN OVM mezi různými poskytovateli

Zajišťuje IP konektivitu mezi subjekty OVM a prostředím CMS 2.0. Dále umožňuje každému subjektu využívat služeb připojení od různých KIVS MPLS[33] operátorů – pro každé svoje přípojné místo KIVS může subjekt využít služeb jiného operátora. Každý subjekt OVM má možnost si zřídit v rámci svého MPLS připojení do KIVS jednu nebo více MPLS VPN. Hraniční směrovače CMS 2.0 směrem ke KIVS operátorům jsou připojené do všech MPLS VPN všech subjektů OVM. Datový provoz jednotlivých subjektů je striktně oddělený, přímá IP komunikace mezi různými subjekty není v rámci této služby povolena. Využití této služby je v případě připojení k CMS 2.0 povinné. Služba slouží jako prerekvizita pro ostatní služby CMS 2.0.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: jednotky tisíc
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Vzájemná izolace jednotlivých VPN
- Možnost definice tříd QoS
- Možnost aplikace transportní bezpečnosti (IpSec/SSL) – dle formy připojení a budoucích modelových standardů

3.2.1.2 Krajský konektor CMS 2.0

Služba modelově představuje formát připojení skupin subjektů OVM a státní správy do CMS 2.0 prostřednictvím sítí místních komerčních či nekomerčních operátorů. Jedná se o „prodloužení" či jakousi dislokaci hraničního připojovacího konektoru od hraničního směrovače CMS 2.0 až na hranici sítě daného poskytovatele.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: stovky
- Administraci provádí: správce CMS 2.0 a to až na hraniční směrovač do krajské sítě, který je instalován jako součást dané služby a tvoří tak i hranici odpovědnosti správce CMS 2.0
- Vzájemná izolace jednotlivých VPN

---

[33] **Multiprotocol Label Switching**, viz. terminologický slovník

- Možnost definice tříd QoS
- Možnost aplikace transportní bezpečnosti (IpSec/SSL) – dle formy připojení a budoucích modelových standardů

3.2.1.3 Extranet CMS 2.0

Jedná se o univerzální propojovací VPN. Je určena pro subjekty OVM menšího rozsahu (např. samospráva, obce „2. a 3. typu" atd.), které nespadají do žádné nadřazené resortní VPN, potřebují však zajistit přístup k „Prostředí Centrálních eGon služeb". Zajišťuje IP konektivitu mezi těmito subjekty a prostředím CMS 2.0. Můžou vznikat požadavky na vytváření více VPN typu Extranet, které budou sdružovat subjekty s podobným zaměřením, potřebami a návaznými přístupovými nároky.

Základní parametry služby:

- Spolehlivost: není definovaná
- Očekávaný počet realizací: jednotky tisíc
- Administraci provádí: správce CMS 2.0 dle definovaných standardů
- Datový provoz subjektů v Extranetu CMS 2.0 není striktně oddělen, přímá IP komunikace mezi těmito subjekty je povolena.
- Datový provoz se subjekty mimo Extranet CMS 2.0 je striktně oddělen, přímá IP komunikace s těmito subjekty není povolena.
- Třídy QoS nelze definovat
- Možnost aplikace transportní bezpečnosti (IpSec/SSL) – dle formy připojení a budoucích modelových standardů

3.2.1.4 Internetové přístupy

Zajišťuje konektivitu jednotlivých subjektů OVM do CMS 2.0 prostřednictvím veřejné sítě Internet. Jedná se o realizaci připojení subjektů OVM z lokalit či středisek, kde realizace přímé IP konektivity dle předchozích modelů služby I. či II. není z technicko-ekonomického hlediska možná či efektivní. Vždy se bude jednat o zabezpečené tunely s aplikací transportní bezpečnosti (IpSec/SSL). Vlastní forma tunelu může být typu LAN-LAN, klient – LAN či WEB based.

Základní parametry služby:

- Spolehlivost: není definovaná
- Očekávaný počet realizací: desítky tisíc
- Třídy QoS nelze definovat
- Striktní nutnost aplikace transportní bezpečnosti (IpSec/SSL)
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Za dodržování provozních a bezpečnostních standardů odpovídá: správce OVM

3.2.2 Propojovací služby síťové vrstvy

3.2.2.1 Vytvoření konektoru firewall VPN OVM

Služba slouží jako konektor k připojení jednotlivých VPN OVM do vnitřního prostředí CMS 2.0. Služba představuje dedikovaný firewall kontext, na kterém má subjekt vyvedeny své přípojky KIVS. Kontext je připojen do konsolidovaného adresního prostoru CMS 2.0 a jsou z něj přímo dostupné služby CMS 2.0. Služba realizuje stavový firewall, který poskytuje základní síťovou ochranu prostředí CMS 2.0 od síťového prostředí subjektu a zároveň zabraňuje nežádoucímu provozu mezi VPN OVM jednotlivých subjektů. Tato služba v sobě automaticky zahrnuje i služby DNS a NTP[34], jejichž používání je pro připojený subjekt žádoucí.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: jednotky tisíc
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM

3.2.2.2 Realizace připojení lokality OVM do mateřské VPN přes Internet

Služba řeší přístup koncových lokalit subjektů OVM do mateřské VPN OVM přes Internet. Služba je určena zejména pro připojení regionálních pracovišť/poboček/lokalit. Přístup bude realizován na bázi IPSec tunelů přes prostředí Internet. Ověřování přípojných bodů je řešeno certifikátem a/nebo heslem. Uživatelé vzdálené sítě mají možnost odebírat stejné služby CMS 2.0 jako uživatelé mateřské VPN.

Základní parametry služby:

- Spolehlivost: není definovaná
- Očekávaný počet realizací: jednotky tisíc
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Za dodržování provozních standardů odpovídá: správce OVM

3.2.2.3 Přístup koncových uživatelů OVM do mateřské VPN přes Internet

Služba řeší přístup koncových uživatelů subjektů OVM do mateřské VPN přes Internet. Služba slouží k zajištění přístupu koncových uživatelů do VPN prostředí jeho přípojky KIVS. Takto připojený uživatel má stejná přístupová práva jako standardní uživatel VPN OVM daného subjektu. Přístup bude realizován na bázi IPSec a/nebo SSL tunelů přes prostředí Internet. Ověřování uživatelů je řešeno certifikátem a/nebo uživatelským jménem a heslem v databázi s centrální správou. Uživatelé IPSec nebo SSL VPN mají možnost odebírat stejné služby CMS 2.0 jako uživatelé mateřské VPN.

Základní parametry služby:

- Spolehlivost: není definovaná

---

[34] **Network Time Protocol, viz. terminologický slovník**

- Očekávaný počet realizací: desítky tisíc
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Za přiřazování uživatelských oprávnění odpovídá: správce OVM

3.2.2.4 Realizace připojení VPN OVM do Extranetu CMS 2.0

Služba řeší připojení LAN sítí lokalit subjektů OVM menší velikosti (např. samospráva, obce „2. a 3. typu" atd.) do univerzální propojovací VPN – Extranet CMS 2.0. Přístup bude realizován na bázi IPSec tunelů přes prostředí Internet. Ověřování přípojných bodů je řešeno certifikátem a/nebo heslem. Uživatelé vzdálené sítě mají možnost odebírat všechny služby CMS 2.0 dostupné v rámci služby Extranet CMS 2.0.

Základní parametry služby:

- Spolehlivost: není definovaná
- Očekávaný počet realizací: jednotky tisíc
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Za dodržování provozních standardů připojení do Extranetu CMS 2.0 odpovídá: správce OVM

3.2.2.5 Přístup koncových uživatelů subjektů OVM menší velikosti do Extranetu CMS 2.0 přes Internet

Služba řeší přístup koncových uživatelů subjektů OVM menší velikosti do Extranetu CMS 2.0 přes Internet. Služba slouží k zajištění přístupu koncových uživatelů do VPN prostředí Extranet CMS 2.0. Takto připojený uživatel má stejná přístupová práva jako standardní uživatel VPN Extranet CMS 2.0. Přístup bude realizován na bázi IPSec a/nebo SSL tunelů přes prostředí Internet. Ověřování uživatelů je řešeno certifikátem a/nebo uživatelským jménem a heslem v databázi s centrální správou. Uživatelé IPSec nebo SSL VPN mají možnost odebírat všechny služby CMS 2.0 dostupné v rámci služby Extranet CMS 2.0.

Základní parametry služby:

- Spolehlivost: není definovaná
- Očekávaný počet realizací: desítky tisíc
- Administraci provádí: správce CMS 2.0 dle definovaných standardů
- Za přiřazování uživatelských oprávnění odpovídá: správce OVM

3.2.2.6 Vzájemné propojení různých VPN OVM

Služba je určená pro vzájemnou komunikaci jednotlivých subjektů OVM mezi sebou. Je komplementární ke službě DMZ2 (subjekt A pomocí „DMZ2" publikuje své služby, ostatní subjekty je pomocí „Propojení s jiným subjektem" mohou využívat).

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: desítky

- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Za přiřazování uživatelských oprávnění odpovídá: správce OVM

3.2.2.7 Vzájemné propojení VPN OVM s VPN s-TESTA

Jedná se o zákaznickou službu propojení VPN OVM se sítí EU VPN s-TESTA. Služba je vždy zřizována na základě individuálního zákaznického projektu v souladu s požadavky EU pro provoz této sítě.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: desítky
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM a správcem s-TESTA
- Za přiřazování uživatelských oprávnění odpovídá: správce OVM

3.2.2.8 Bezpečné připojení VPN OVM k Internetu

Jedná se o službu připojení centrálního sdíleného Internetu přímo do zákaznické IP VPN přípojky KIVS realizované službou „Vytvoření univerzální přípojky KIVS včetně vytvoření VPN OVM mezi různými poskytovateli". Služba slouží k bezpečnému přístupu zákaznické VPN OVM do Internetu, resp. k zpřístupnění internetových služeb. Samotnou službu realizují servery zajišťující bezpečnost filtrováním na přítomnost škodlivého kódu, detekcí na tunelování HTTP(S) protokolem a filtrováním URL[35]. Pro urychlení služby a zvýšení efektivity bude používána proxy cache[36]. Služba zároveň umožňuje subjektu OVM využívat jmenné služby DNS směrem do Internetu. Subjekt může publikovat svoji veřejnou službu pomocí odpovídajícího DNS záznamu na dedikovaném CMS 2.0 DNS. Publikace těchto DNS záznamů se provádí pouze směrem do Internetu.

Připojení má následující vlastnosti:

- Veškerý provoz z/do Internetu je překládán
- Pro odchozí provoz bude dedikována pro každý subjekt 1 veřejná IP adresa z rozsahu přiděleného CMS
- V rámci komunikace do Internetu budou nativně povoleny následující protokoly:
    - HTTP/HTTPS/FTP přes HTTP
    - IMAP4/IMAP4S
    - POP3/POP3S
    - FTP

Ostatní protokoly budou implicitně blokovány a jejich povolení bude podléhat schválení provozovatele CMS a bezpečnostního správce CMS v rámci individuálního zákaznického projektu.

Základní parametry služby:

---

[35] **Uniform resource locator, viz. terminologický slovník**

[36] Viz. terminologický slovník

- Spolehlivost: není definovaná
- Očekávaný počet realizací: stovky
- Administraci provádí: správce CMS 2.0 dle definovaných standardů
- Za přiřazování uživatelských oprávnění odpovídá: správce OVM

3.2.2.9 Přímé propojení VPN OVM s Internetem

Reprezentuje přímé poskytnutí centrálního sdíleného Internetu do IP VPN přípojky subjektu KIVS. Realizace má formu další logicky oddělené IP VPN paralelně ke standardní VPN subjektu reprezentované službou „Vytvoření univerzální přípojky KIVS včetně vytvoření VPN OVM mezi různými poskytovateli". Adresní rozsahy služby „Přímé propojení VPN OVM s Internetem" mohou být přiděleny z rozsahu adres CMS, subjekt má k dispozici část veřejného rozsahu CMS 2.0 pro svoje potřeby nebo z adresního rozsahu vlastněného subjektem, pokud má „provider independent adresy". Připojený Internet není žádným způsobem filtrován či kontrolován.

Základní parametry služby:

- Spolehlivost: není definovaná
- Očekávaný počet realizací: desítky
- Administraci provádí: správce CMS 2.0 dle definovaných standardů
- Za dodržování provozních standardů odpovídá: správce OVM

3.2.2.10 DMZ 1

Funkcí služby DMZ 1 (demilitarizovaná zóna) je publikace služeb a webová prezentace subjektů OVM směrem do Internetu. Služba spočívá ve vytvoření instance vlastního virtuálního FW v rámci internetového FW pro směrování vnější DMZ sítě daného subjektu a její konektivity do Internetu. Služby DMZ 1 jsou zřizovány na základě individuálního zákaznického projektu, do kterého provozovatel CMS doplní závazná bezpečnostní pravidla a tuto DMZ 1 zřídí. DMZ 1 může být realizována v rámci specializovaných VPN mezi CMS 2.0 a datovými centry centrálních služeb, službami typu hosting nebo housing či umístěna přímo u subjektu. Konektivita mezi virtuálním FW a vlastními instancemi je potom realizována jako samostatná oddělená IP VPN.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: stovky
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Za přiřazování uživatelských oprávnění odpovídá: správce OVM

3.2.2.11 DMZ 2

Služba DMZ 2 je vytvoření prostředí pro publikaci služeb subjektů KIVS do CMS, nebo pro umístění back-end serverů pro publikaci aplikací či služeb do internetu (front-end servery jsou v tomto případě v DMZ 1). Službu DMZ 2 je také dále možné využít pro umístění serverů subjektu bez jejich publikace do CMS (bezpečné oddělení aplikací a aplikačních serverů subjektu od jeho uživatelů). V rámci této

služby je subjektu poskytnut vlastní virtuální FW pro vytvoření DMZ 2 daného subjektu. Jde o totožný virtuální FW, který je subjektu přidělen v rámci služby „I. Vytvoření konektoru firewall VPN OVM". DMZ 2 je realizována v rámci specializovaných VPN mezi CMS 2.0 a datovými centry centrálních služeb, službami typu hosting housing.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: stovky
- Administraci provádí: správce CMS 2.0 dle technické specifikace zadané OVM
- Za přiřazování uživatelských oprávnění odpovídá: správce OVM

3.2.2.12 MTA

Služba elektronické pošty zajišťuje předávání zpráv elektronické pošty jak mezi jednotlivými subjekty KIVS, tak mezi subjekty KIVS a uživateli sítě Internet. Jedná se o službu Mail Transfer Agent (MTA) – služba bude zajišťovat pouze předávání zpráv, nikoliv mailové schránky. Služba kromě filtrování nevyžádané pošty provádí i kontrolu na přítomnost škodlivého kódu či odkazu na infikované URL.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: desítky
- Administraci provádí: správce CMS 2.0 dle definovaných standardů

3.2.2.13 Vzájemné propojení informačních systémů centrálních služeb prostřednictvím eGon Service Bus

Specializované komunikační propojení umožňující univerzální přímé propojení mezi jednotlivými IS poskytujícími centrální eGon služby navzájem. Toto propojení umožní „back-end" komunikaci mezi IS (například Základní registry publikující výpisy pro uživatele prostřednictvím ISDS). Dále služba zajistí funkcionalitu provozní podpory.

Základní parametry služby:

- Spolehlivost: 99,9%
- Očekávaný počet realizací: desítky
- Administraci provádí: správce CMS 2.0 dle definovaných standardů

eGon service bus je provozován nad komunikační infrastrukturou propojující jednotlivá datová centra hostující centrální eGon služby. Není přímo propojen mimo tento komunikační segment, přístup na něj mají pouze AISy zabezpečující centrální eGON služby s připojením svého datového centra podle pravidel připojení národních datových center (pravý horní segment propojovacího schématu CMS).

V prostředí Centrálních eGon služeb je potřeba řešit vzájemné propojení informačních systémů centrálních služeb prostřednictvím jednotné a standardní sběrnice - eGon Service Busu.

eGon Service Bus bude nasazen zejména pro :

- Komunikaci centrálních Egon služeb mezi sebou a zajištění bezpečného předávání dat mezi službami navzájem s tím, že eGON service bus žádná předávaná data neuchovává
- Eskalaci hlášení o chybových stavech a jejich řešení mezi všemi úrovněni nasazených systémů, od komunikační infrastruktury přes výpadky HW a SW platforem, aplikační výpadky až po chyby v datech a jejich eskalaci do příslušných procesů správců jednotlivých systémů.
- Publikaci datových služeb jednotlivých agendových informačních systémů rozšiřujících centrální Egon služby a orchestraci publikovaných služeb navzájem I s již existujícími centrálními službami.
- Pro připojení standardních povinných centrálních eGon služeb k ostatním AISům zabezpečujícím centrální služby – propojení na centrálu CzechPoint, na vnější rozhraní ZR, na IS DS, na PVS a další do budoucna vznikající.

Nabízené řešení musí obsahovat standardní (v rámci produktu běžně dodávané) komponenty pro registraci služeb, jejich vyhledávání, orchestraci a skládání do kompozitních aplikací a infrastrukturní komponenty zabezpečující monitoring, auditing, bezpečnost, vysoká dostupnost atp.

Nabízené řešení dále musí obsahovat konektory pro běžně používaná dohledová řešení komunikační infrastruktury, HW a SW platforem a nástroje pro tvorbu eskalačních procedur ze zpráv poskytovaných prostřednictvím těchto konektorů.

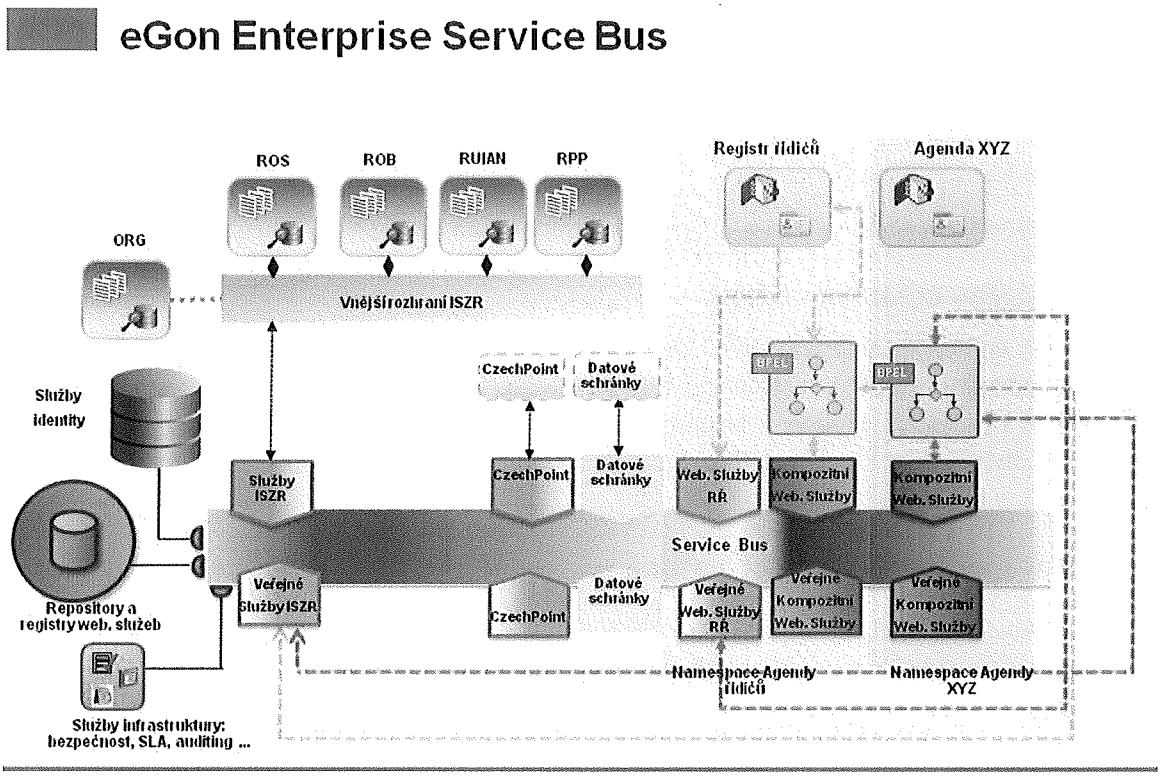
Nabízené řešení musí obsahovat konektory pro připojení služeb vnějšího rozhraní základních registrů, služeb datových schránek a služeb centrály Czechpointu jako základu pro orchestraci dalších datových služeb, návrh a standardní replikovatelný konektor pro publikaci rozšiřujících datových služeb agendových informačních systémů a nástroje pro orchestraci centrálních I rozšiřujících služeb navzájem.

Dále musí nabízené řešení obsahovat škálovatelné řešení konektoru poskytujícího orchestrované dodatečné datové služby jak v DMZ1 tak I v DMZ2 s využitím certifikace agendových informačních systémů certifikační autoritou základních registrů.

Požadovaná průchodnost – nabízené řešení musí zajistit v průměru:

- 10 tisíc zpráv (5kB – 10 kB)/s s přímou transformací a přenosem mezi libovolnými dvěma konektory na úrovni eGon Service Busu
- 1 tisíc zprav (5kB – 10 kB)/s orchestrovaných a zpracovaných v 10ti krokovém workflow procesu

Příklad architektury eGon Service Bus pro rozšiřující datové služby:



Obrázek 3 eGon ESB

3.2.3 Systémové a bezpečnostní služby

3.2.3.1 Služby rozkladu zátěže

Poskytne prostředky pro zajištění vysoké dostupnosti a škálovatelnosti služeb poskytovaných CMS 2 i systémů provozovaných v rámci služeb hostingu (Klaudie).

Služba je reprezentována zařízením load-balanceru a virtuálním host – name, provoz směrovaný na tuto adresu je dále rozkládán na konkrétní fyzické servery. Vlastní rozklad zátěže probíhá dle parametrů vrstev L3-L7 modelu TCP/IP. Může zároveň poskytovat služby proxy pro HTTPS komunikaci, kdy je vlastní šifrování přesunuto na prostředky load-balanceru a tudíž jím nejsou vytěžovány systémové prostředky serverů.

Základní parametry služby:

- Spolehlivost: dle požadavků konkrétní služby
- Očekávaný počet realizací: desítky
- Administraci provádí: správce CMS 2.0 dle definovaných standardů

3.2.3.2 Management služby – monitoring a reporting

Komplexní monitorování všech funkcí CMS 2.0, které zahrne síťovou infrastrukturu i veškeré další kritické komponenty včetně serverů a aplikací. Na základě údajů a dat z monitorovacích systémů poskytne informace o stavu systémů CMS 2 v požadované výstupní podobě a to jak z hlediska jeho

samotného běhu, tak z hlediska funkčních charakteristik jednotlivých poskytovatelů KIVS a připojených subjektů veřejné správy.

Základní parametry služby:

- Spolehlivost: dle požadavků konkrétní služby
- Očekávaný počet realizací: tisíce
- Administraci provádí: správce CMS 2.0 dle definovaných standardů

3.2.3.3 Služby účtování - billing

Představuje systém či soubor systémů pro účtování služeb. Musí disponovat funkcionalitou pro evidenci, účtování, export podkladů jednotlivých služeb a jejich nákladů. Účtovací systém musí splňovat ta nejpřísnější kritéria v bezpečnosti uložených dat, rychlosti zpracovávání účtovaných operací, spolehlivosti přístupu k datům, robustnosti s ohledem na serverovou platformu a použité databáze.

Funkcionalita řešení billingu bude zahrnovat:

- Evidenci, účtování, export dat jednotlivých služeb a jejich nákladů
- Účtování periodických, dynamických i jednorázových plateb
- Podpora různých účetních období
- Podpora různých režimů splatnosti (předplatný, platný, po splatný, kreditní) a možnost jejich kombinace
- Sledování nákladů dle parametru (klient, služba, atd.)
- Nástroje pro import SLA jednotlivých služeb
- Napojení na bankovní rozhraní, párování plateb, upomínkování
- Nástroje pro logování
- Půjde o databázové řešení integrovatelné minimálně se Service deskem

Základní parametry služby:

- Spolehlivost: 99,97%
- Očekávaný počet realizací: tisíce
- Administraci provádí: správce CMS 2.0 dle definovaných standardů

3.2.3.4 Provisioning a provoz služeb

Funkcionalita řešení provisioningu bude zahrnovat:

- Poskytnutí infrastruktury jako služby s minimálními nároky na administrativu
- Balancování výkonu
- Samoobslužný přístup uživatelů pro správu jejich prostředí
- Podporu automatizovaných konfiguračních zásahů jak na straně síťové infrastruktury, tak na straně komponent hostovaných služeb

- Správa a analýza životního cyklu virtuálních strojů (mj. zahrnuje skládání nových obrazů pomocí standardizovaných komponent v grafickém prostředí)
- Nástroje pro obnovu po výpadku
- Odolnost proti chybám na všech vrstvách (hardware, hypervisor, cloud management)
- Analýzu virtuálních obrazů v celé infrastruktuře

Základní parametry služby:

- Spolehlivost: 99,99%
- Očekávaný počet realizací: tisíce
- Administraci provádí: správce CMS 2.0 dle definovaných standardů

4 Povýšení platformy CMS na CMS NGN - CMS 2.0

Tato kapitola připravovaného projektu v sobě zahrnuje několik částí. Cílem zadavatele je zajistit upgrade stávajícího komunikačního uzlu CMS 1.0 tak, aby splňoval požadavky na nové služby, které musí komunikační uzel Centrální místo služeb v nadcházejícím období poskytovat.

Vzhledem ke stále rostoucím požadavkům na komunikační infrastrukturu a centralizaci služeb eGovernmentu a rostoucím požadavkům na bezpečnost celého CMS je třeba zásadně modernizovat Centrální místo služeb na verzi „NGN[37]", tedy CMS 2.0 a zajistit tak bezproblémové fungování nových služeb. Pro zajištění běhu těchto služeb je nutné se v rámci povýšení CMS 1.0 na CMS 2.0 zabývat těmito oblastmi:

- Zajistit dostupnost a redundanci - systém musí být navržen tak, aby byl redundantní co do lokality a jejího připojení, tak do použití jednotlivých technologií. Cílem je splnění nejnáročnějších požadavků na dostupnost jednotlivých systémů ISVS až v režimu 99,9%
- Zvýšení propustnosti komunikačního uzlu relevantně k očekávanému nárůstu připojených subjektů OVM a poskytovaným službám - upgrade na 10Gbps infrastrukturu
- Zajistit kompatibilitu veškerých použitých komponent s protokolem IPv6 a 100% připravenost k jeho budoucímu bezproblémovému nasazení bez potřeby jakýchkoliv HW či SW změn
- Vybudování krajského konektoru do CMS 2.0
- Povýšit bezpečnostní prostředky pro zajištění naplnění usnesení vlády ČR o kybernetické bezpečnosti a ochraně kritických infrastruktur
- Zajistit ochranu proti DDoS[38] útokům
- Zajistit fungování podpůrné a management infrastruktury pro CMS 2.0 (centralizace monitoringu, service desku, provisioningu, billingu, inventory)
- Implementace portálového řešení pro reporting a prezentaci stavu a dostupnosti jednotlivých realizovaných služeb
- Rozšíření síťové infrastruktury včetně centrálního managementu
- Propojení s dalšími národními datovými centry
- Nastavení standardů pro propojování a monitoring informačních systémů v rámci OVM
- Vytvoření testovacího prostředí

4.1 Konceptuální architektura prostředí CMS 2.0

CMS 2.0 slouží jako hlavní propojovací místo eGovernmentu a zajišťuje služby pro jeho čtyři základní komunikační prostředí.

Těmito prostředími jsou:

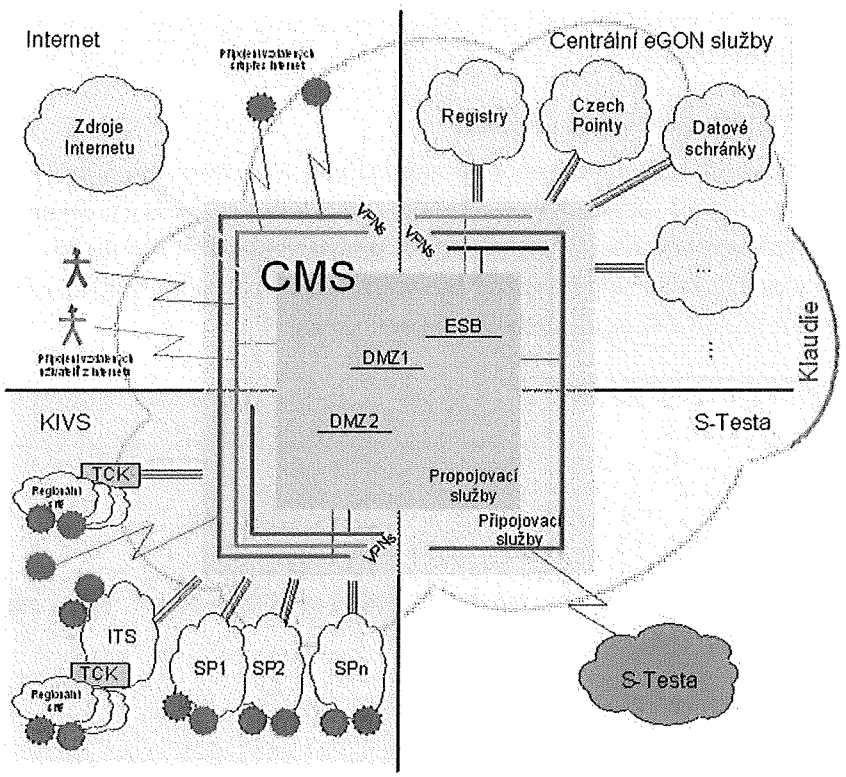
---

[37] **Next-generation network, viz. terminologický slovník**

[38] Distributed denial of service, viz. terminologický slovník

- Prostředí Internetu
- Prostředí KIVS
- Prostředí Centrálních eGon služeb
- Prostředí komunikační infrastruktury EU (např. s-TESTA)

Na následujícím obrázku jsou jednotlivá prostředí reprezentována příslušnými kvadranty se vzájemnou vazbou:



Obrázek 4 Schematické znázornění komunikačních bloků CMS 2.0

4.1.1 Prostředí Internetu

Prostředím Internetu pro účely CMS 2.0 rozumíme veškeré veřejné komunikační prostředí, do a ze kterého přistupují OVM do CMS 2.0.

Prostředí Internetu tedy zahrnuje zejména:

- Přístupy jednotlivých pracovníků OVM přes veřejné pevné sítě
- Přístupy jednotlivých pracovníků OVM přes veřejné mobilní sítě
- Připojení LAN sítí OVM přes veřejné pevné sítě

4.1.2 Prostředí KIVS

Prostředím KIVS pro účely CMS 2.0 rozumíme veškeré komunikační prostředí, do a ze kterého přistupují OVM do CMS 2.0 MIMO prostředí Internetu a sítí EU.

Prostředí KIVS tedy zahrnuje zejména:

- Sítě komerčních poskytovatelů telekomunikačních služeb připojených na základě smluv o poskytování služeb KIVS
- Integrovanou telekomunikační síť Ministerstva vnitra
- Technologická centra krajů
- Krajské regionální a metropolitní sítě (tj. typicky sítě ve vlastnictví místní samosprávy)
- Další telekomunikační sítě připojené na základě metodického pokynu o připojení metropolitních sítí

4.1.3 Prostředí Centrálních eGon služeb

Prostředím Centrálních eGon služeb rozumíme komunikační prostředí, ve kterém jsou provozovány centrální služby veřejné správy, jejichž správcem jsou centrální OVM. Jedná se typicky o celoplošné služby zaměstnancům orgánů veřejné moci případně přímo soukromoprávním uživatelům. Tyto centrální služby mohou pracovat s anonymními či registrovanými uživateli, poskytovat služby v rámci jedné agendy či sdílené služby pro několik agend či celou veřejnou správu.

Typickými příklady Centrálních eGon služeb jsou:

- Základní registry
- CzechPOINT
- Datové schránky

IS zabezpečující centrální eGon služby mohou být propojeny s jinými službami veřejné zprávy pouze prostřednictvím následujících služeb CMS 2.0:

- Vzájemným propojením různých VPN OVM
- Publikací služeb v DMZ1
- Publikací služeb v DMZ2
- eGon Service Busu

4.1.4 Prostředí komunikační infrastruktury EU

Prostředím komunikační infrastruktury EU rozumíme pro účely CMS 2.0 veškeré existující i budoucí sítě EU určené pro komunikaci a rozvoj eGovernmentu mezi jednotlivými státy EU. Jedná se o sítě „sektorové" i „univerzální". Snahou je přejít od sektorových sítí k univerzálním, tj. zejména síti sTESTA zajišťované útvarem IDABC direktorátu Enterprise and Industry EC. Sektorové sítě" jsou zřizované pro speciální agendy jinými direktoráty EC. Přestože došlo k migraci některých komunikací a je snaha používat síť sTESTA v nových agendách, staré sektorové sítě stále existují a pravděpodobně budou existovat i nadále.

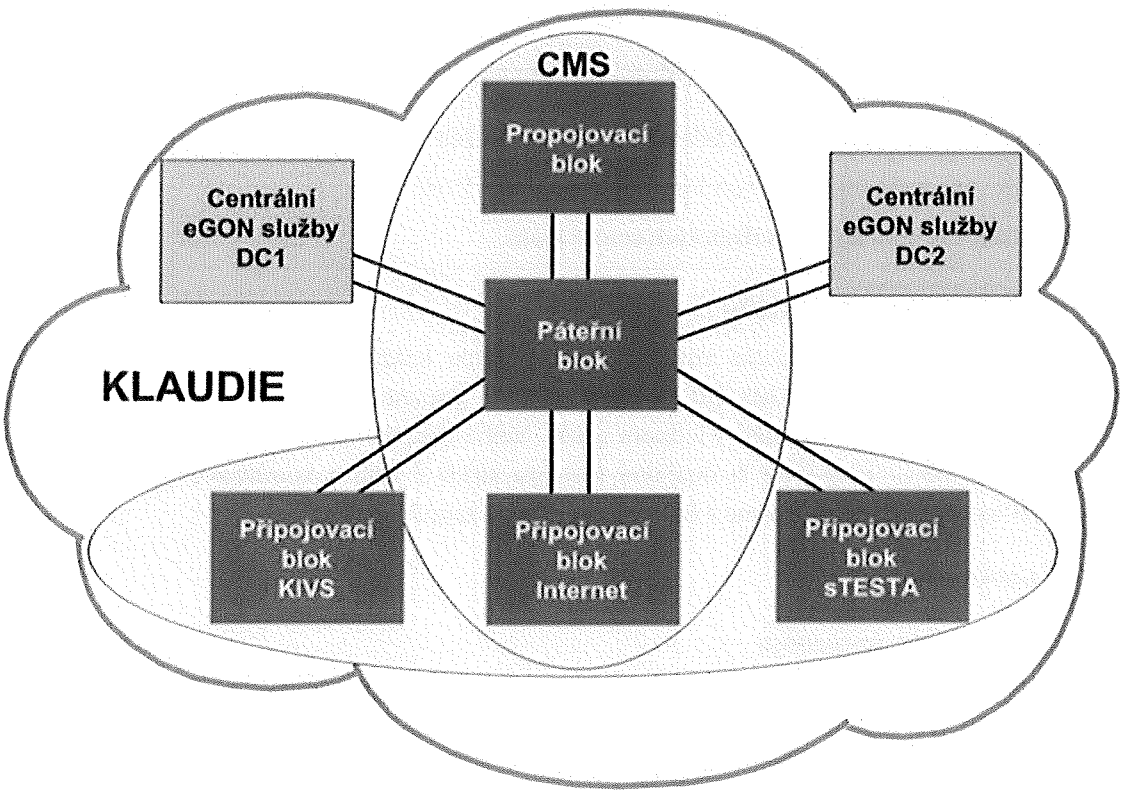
5 Model funkčních bloků

Jednotlivá komunikační prostředí jsou v reálné architektuře reprezentována funkčními HW bloky a jejich službami.

Jednotlivé funkční bloky jsou rozděleny dle své primární funkce do tří základních kategorií:

- Připojovací bloky
- Propojovací blok
- Páteřní blok

Následující obrázek schematicky znázorňuje rozložení do bloků a jejich vzájemnou inter-operabilitu. Jedná se o hrubý high level design:



Obrázek 5 Vzájemná inter-operabilita bloků CMS

5.1 Připojovací bloky

V CMS 2.0 bude mít každé ze základních komunikačních prostředí svůj připojovací blok. Připojovací bloky musí vždy pro dané prostředí zajistit obecně tyto funkce:

- Jednoznačné přiřazení vstupujících dat do příslušné VPN
- Směrování VPN dat z/do daného komunikačního prostředí (KIVS, Internet apod.), jakož i směrem do páteřního bloku CMS 2.0 (tj. směrem k propojovacím službám). Za tímto účelem musí každý přístupový blok zajišťovat dynamickou výměnu směrovacích informací jak

s příslušným komunikačním prostředím, tak s páteřním blokem (typicky dynamickými směrovacími protokoly – BGP, OSPF apod.). Toto vše samozřejmě per VPN.

- Základní zabezpečení na perimetru daného komunikačního prostředí
- Logické připojení síťových služeb specifických pro daný přístupový blok (např. externí DNS směrem do Internetu, služeb DMZ1 a DMZ2, služeb eGon Service Bus (ESB) apod. Fyzicky mohou být tyto služby realizovány na infrastruktuře souvisejícího bloku.

5.1.1 Připojovací blok KIVS

V CMS 1.0 je tento blok reprezentován blokem Interconnect-I.

Blok bude směrem ke KIVS sloužit jako soubor hraničních vysokorychlostních MPLS PE směrovačů pro přístup do infrastruktury CMS 2.0. Tyto budou následně propojeny se všemi směrovači páteřního bloku.

Připojovací blok KIVS bude realizovat následující typy připojení:

- Sítě komerčních poskytovatelů telekomunikačních služeb v rámci KIVS
- Integrovaná telekomunikační síť Ministerstva vnitra (ITS NGN)
- Konektor CMS 2.0 do technologických center krajů

5.1.1.1 Možnosti architektury

Fyzicky bude reprezentován dvojicí směrovačů, z níž bude každý umístěn na hranici jednoho z geograficky oddělených uzlů CMS 2.0 směrem ke KIVS. Variantně může být realizován dvěma dvojicemi směrovačů, každá z dvojic v jednom z uzlů. Volba mezi variantami se samostatnými šasi s redundantními řídícími logikami či duálními šasi pro každý z uzlů a kombinace by měla vždy zohledňovat možnosti dané platformy a finanční aspekty přidaných hodnot.

Hlavními aspekty jsou zde:

- Zajištění vysoké dostupnosti
- Možnosti eliminace standardních nevýhod redundantních L2 topologií v podobě nevyužitých blokovaných traktů:
    - Prostřednictvím L2 protokolů jako například standard IETF TRILL, či podobných vendorově orientovaných
    - Prostřednictvím Multi-chassis Link Aggregation (MLAG) a dalších příbuzných metod – opět dle výrobce
- Možnosti virtualizace a logické slučování jednotlivých fyzických šasi a bloků, mmj. s pomocí výše uvedených principů
- Další funkční a výkonová kritéria
- Finanční kritéria

5.1.1.2 Požadavky na funkci a topologii

Rozhraní mezi CMS a poskytovateli datové konektivity KIVS bude realizováno vždy redundantním spojem na bázi technologií Gigabit Ethernet (IEEE802.3z, příp. IEEE802.3ab) nebo 10Gigabit Ethernet

(IEEE802.3ae). Rozhraní musí podporovat tagování VLAN dle 802.1Q, jednotlivé VPN budou předávány formou jednotlivých VLAN.

Vlastní logické propojení bude realizováno formou dedikované MPLS VPN sítě v rámci CMS s příslušnou VPN v rámci sítí KIVS níže popsaným způsobem. Autonomní systémy obou sítí budou vzájemně odlišné, tudíž směrovače obou stran budou ve vzájemné funkci ASBR (Autonomous System Boundary Router).

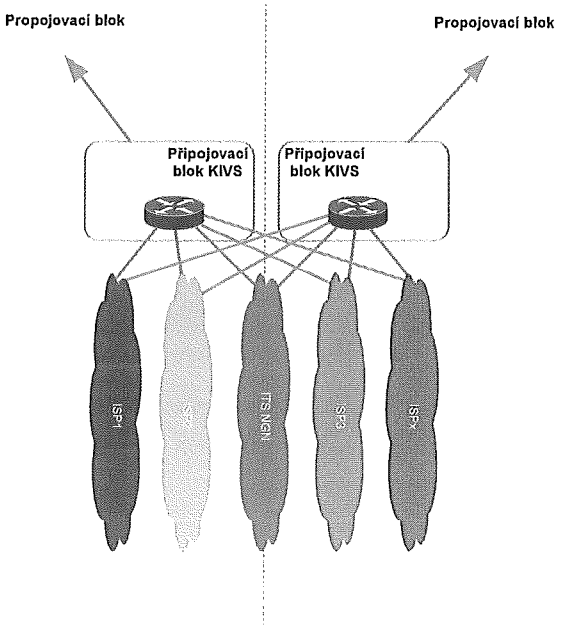
V případě, že poskytovatel konektivity KIVS využívá též technologie MPLS VPN, bude použito propojení dle RFC4364 odstavec 10a (Simple IP Interconnect).

Směrovací informace mezi propojovací sítí CMS 2.0 a jednotlivými poskytovateli datové konektivity budou předávány pomocí směrovacího protokolu eBGP-4 (dle RFC 4271).

V případě připojení formou Krajského konektoru CMS 2.0 bude na připojovacím směrovači bloku KIVS konfigurováno návazné spojovací rozhraní na vzdálené L3 zařízení v podobě MPLS PE směrovače, který bude součástí autonomního systému CMS2.0, tedy stejného jako připojovací směrovač bloku KIVS. Transportní L2 konektivita mezi připojovacím směrovačem bloku KIVS a vzdáleným PE směrovačem bude realizována prostřednictvím ITS NGN v části mezi připojovacím blokem KIVS a krajským ITS NGN TKU a následně pronajatým okruhem mezi ITS NGN TKU a vzdáleným PE směrovačem na hranici sítě lokálního poskytovatele. Vlastní forma konektivity skrze ITS NGN je řešena v rámci samostatného projektu. Pro propojení mezi PE směrovačem a směrovačem lokálního poskytovatele již dále platí výše uvedené principy.

Celá infrastruktura KIVS musí být schopna jednotného řízení kvality služby (End-to-End QoS). CMS je koncipováno jako separátní poskytovatel služeb a procesně bude definovat QoS politiky pro celý KIVS. Propojovací síť musí být schopna realizace těchto QoS politik.

Následující obrázek znázorňuje připojovací funkci bloku KIVS:



Obrázek 6 Připojovací funkce bloku KIVS

V souvislosti se změnami a potřebami v rámci povýšení na CMS 2.0 se dále požaduje:

- Navýšení kapacity připojovacího bloku tak, aby bylo možné realizovat nárůst počtu VPN, zvýšení počtu poskytovatelů KIVS a s tím spojené objemové nároky agregovaných komunikačních toků
- Veškerá komunikace směrem k ostatním připojovacím blokům a směrem k propojovacímu bloku bude probíhat přes páteřní blok
- Implementace IPv6 (Dual Stack)

5.1.1.3 Požadované základní parametry směrovačů připojovacího bloku KIVS

- Modulární platforma
- Neblokující architektura směrování, předpokládá se line-rate dle maximálních možností osazených rozhraní
- Směrovače musí mít možnost výměny klíčových HW komponent za běhu, bez degradace výkonu zařízení během výměny
- Směrovače musí mít možnost výměny částí řídících SW za běhu všech služeb bez jejich přerušení
- Směrovače musí nabízet redundanci řídících komponent
- Směrovače musí nabízet redundanci zdrojů a ventilátorů
- Distribuovaná architektura (oddělený Control Plane a Data Plane)
- HW ochrana proti DoS[39] útokům na vlastní směrovač (control plane policing)
- Plná podpora směrování IPv4 i IPv6 v hardware a to jak směrových tak více směrových vysílání
- Podpora rozhraní:
    - 1GE, minimálně 32x s možností rozšíření
    - 10GE, minimálně 8x s možností rozšíření
    - rozšiřitelnost na 40GE
    - rozšiřitelnost na 100GE
- Replikace multicastových rámců v hardware
- Podpora virtuálních směrovacích instancí - minimálně 3 tisíce
- Podpora MPLS pro IPv4/IPv6
    - MPLS L3 / L2 VPN
    - MPLS Traffic Engineering
    - VPLS[40]
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v pseudoreálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový

---

[39] Denial of service, viz. terminologický slovník

[40] **Virtual Private LAN Service, viz. terminologický slovník**

TCP/UDP port/protokol - NetFlow/IPFix nebo ekvivalent. Funkce monitorování musí být implementována bez negativních vlivů na zátěž a výkon řídících procesorů.

- Kontrola zdrojové IPv4, IPv6 adresy na fyzických i logických L3 rozhraních podle aktuální směrovací tabulky (antispoofingová kontrola ekvivalentní funkci uRPF (Unicast Reverse Path Forwarding)
- Podpora bez stavových filtrů na rozhraních v hardware bez vlivu na výkon - podle L2/L3/L4, aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní
- Podpora flexibilní práce s VLAN tagy
- Podpora Bidirectional Forwarding Detection (BFD) pro rychlou detekci poruchy mezi směrovači
- Podpora sdružování portů přes více šasi
- Podpora rozložení zátěže mezi sdruženými porty
- Podpora Jumbo Frame o velikosti minimálně 9KByte
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ dle RFC 2474, 2475, 2597, 2598, 2697, 3270):
    - Klasifikace a reklasifikace rámců/paketů na vstupu i výstupu (IEEE 802.1p, IP DSCP, IP Precedence, EXP MPLS).
    - Omezování provozu (policing) na vstupu i výstupu (kompatibilita s RFC 2697 a/nebo RFC 2698), konfigurovatelné mechanismy preventivní ochrany proti zahlcení.
    - Podpora QOS Shapingu a Policingu bez dopadu na výkon směrovače
- Tx and Rx optical power monitoring (DOM) na optických portech
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.1.1.4 Požadované základní parametry vzdálených MPLS PE směrovačů pro realizaci služby Krajský konektor CMS 2.0

- Neblokující architektura směrování, předpokládá se line-rate dle maximálních možností osazených rozhraní
- Směrovače musí nabízet redundanci zdrojů a ventilátorů
- Distribuovaná architektura (oddělený Control Plane a Data Plane)
- HW ochrana proti DoS útokům na vlastní směrovač (control plane policing)
- Plná podpora směrování IPv4 i IPv6 v hardware a to jak směrových, tak i vícesměrových vysílání
- Podpora rozhraní:
    - 1GE, min 2x
    - 10GE (v rámci rozšíření HW či licenčně), min 2x
- Replikace multicastových rámců v hardware
- Podpora virtuálních směrovacích instancí - minimálně 100

- Podpora MPLS pro IPv4/IPv6
    - MPLS L3 / L2 VPN
    - VPLS
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v pseudoreálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový TCP/UDP port/protokol - NetFlow/IPFix nebo ekvivalent. Funkce monitorování musí být implementována bez negativních vlivů na zátěž a výkon řídících procesorů.
- Kontrola zdrojové IPv4, IPv6 adresy na fyzických i logických L3 rozhraních podle aktuální směrovací tabulky (antispoofingová kontrola ekvivalentní funkci uRPF (Unicast Reverse Path Forwarding)
- Podpora bezstavových filtrů na rozhraních v hardware bez vlivu na výkon - podle L2/L3/L4, aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní
- Podpora flexibilní práce s VLAN tagy
- Podpora Bidirectional Forwarding Detection (BFD) pro rychlou detekci poruchy mezi směrovači
- Podpora rozložení zátěže mezi sdruženými porty
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ dle RFC 2474, 2475, 2597, 2598, 2697, 3270):
    - Klasifikace a reklasifikace rámců/paketů na vstupu i výstupu (IEEE 802.1p, IP DSCP, IP Precedence, EXP MPLS).
    - Omezování provozu (policing) na vstupu i výstupu (kompatibilita s RFC 2697 a/nebo RFC 2698), konfigurovatelné mechanismy preventivní ochrany proti zahlcení.
    - Podpora QOS Shapingu a Policingu bez dopadu na výkon směrovače
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.1.2 Připojovací blok Internet a sTESTA

V CMS 1.0 je tato role z převážné části reprezentována blokem Interconnect-E.

V rámci CMS 2.0 bude tento blok poskytovat primárně tyto funkce:

- Konektivita do Internetu a její zabezpečení
- Konektivita do sítí sTESTA
- VPN koncentrátory pro realizaci zabezpečených tunelovaných připojení
- Sdílené a podpůrné síťové služby (DNS, Web GW, Mail GW, apod.)

Vlastní připojovací část bloku bude tvořena dvojicí MPLS PE směrovačů, které zde tvoří agregační podvrstvu a k nimž jsou redundantně připojeny všechny potřebné funkční celky modulu. MPLS PE směrovače jsou následně propojeny se všemi směrovači páteřního bloku.

Variantou k fyzické dvojici směrovačů může být jejich virtualizace či případně - viz kapitola Možnosti architektury pro Připojovací blok KIVS.

Hlavní funkcionalitou připojovací části bude terminace všech MPLS VPN potřebných pro realizaci služeb bloku Internet/sTESTA.

5.1.2.1 Požadované základní parametry připojovacích MPLS PE směrovačů bloku Internet/sTESTA:

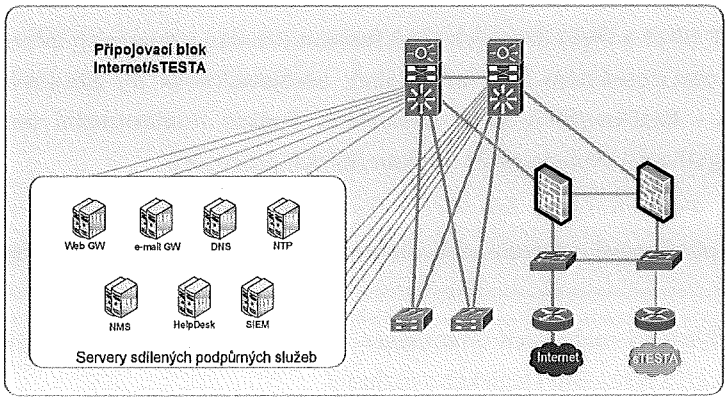
- Modulární platforma
- Neblokující architektura směrování, předpokládá se line-rate dle maximálních možností osazených rozhraní
- Směrovače musí mít možnost výměny klíčových HW komponent za běhu, bez degradace výkonu zařízení během výměny
- Směrovače musí nabízet redundanci řídících komponent
- Směrovače musí nabízet redundanci zdrojů a ventilátorů
- Distribuovaná architektura (oddělený Control Plane a Data Plane)
- HW ochrana proti DoS útokům na vlastní směrovač (control plane policing)
- Plná podpora směrování IPv4 i IPv6 v hardware a to jak směrových tak více směrových vysílání
- Podpora rozhraní:
    - 1GE
    - 10GE
    - rozšiřitelnost na 40GE
- Replikace multicastových rámců v hardware
- Podpora virtuálních směrovacích instancí - minimálně 1 tisíc
- Podpora MPLS pro IPv4/IPv6
    - MPLS L3 / L2 VPN
    - MPLS Traffic Engineering
    - VPLS
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v pseudoreálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový TCP/UDP port/protokol - NetFlow/IPFix nebo ekvivalent. Funkce monitorování musí být implementována bez negativních vlivů na zátěž a výkon řídících procesorů.
- Kontrola zdrojové IPv4, IPv6 adresy na fyzických i logických L3 rozhraních podle aktuální směrovací tabulky antispoofingová kontrola ekvivalentní funkci uRPF (Unicast Reverse Path Forwarding)
- Podpora bez stavových filtrů na rozhraních v hardware bez vlivu na výkon - podle L2/L3/L4, aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní
- Podpora flexibilní práce s VLAN tagy
- Podpora Bidirectional Forwarding Detection (BFD) pro rychlou detekci poruchy mezi směrovači
- Podpora sdružování portů přes více šasi
- Podpora rozložení zátěže mezi sdruženými porty

- Podpora Jumbo Frame o velikosti minimálně 9KByte
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ dle RFC 2474, 2475, 2597, 2598, 2697, 3270):
    - Klasifikace a reklasifikace rámců/paketů na vstupu i výstupu (IEEE 802.1p, IP DSCP, IP Precedence, EXP MPLS).
    - Omezování provozu (policing) na vstupu i výstupu (kompatibilita s RFC 2697 a/nebo RFC 2698), konfigurovatelné mechanismy preventivní ochrany proti zahlcení.
    - Podpora QOS Shapingu a Policingu bez dopadu na výkon směrovače
- Tx and Rx optical power monitoring (DOM) na optických portech
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.1.2.2 Skladba bloku Internet/sTesta

Připojovací blok Internet/sTESTA bude dále směrem do modulu připojovat tyto sub-moduly:

- Peeringové směrovače
- Směrovače sTESTA sítí
- Vnější (veřejné) firewally
    - Součástí tohoto sub-modulu budou i soubory propojovacích přepínačů externích služeb
- VPN koncentrátory
- Loadbalancery (tyto mohou být variantně přímo modulární součástí připojovacího bloku, resp. agregačních MPLS směrovačů)
- Instance sdílených služeb (Mail GW, WEB GW, DNS, NTP, atd..)
- Obrázek níže graficky znázorňuje skladbu tohoto funkčního bloku:



Obrázek 7 Skladba bloku Internet/sTesta

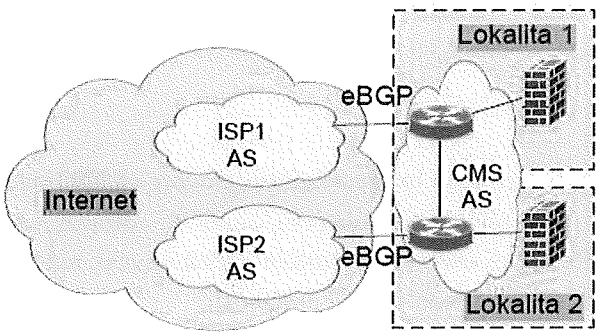
5.1.2.3 Připojení k Internetu /Internet peering/:

Za současného stavu je konektivita do internetu realizována peeringovými směrovači bloku Interconnect – E.

CMS 1.0 má přidělený vlastní veřejný BGP autonomní systém a LIR (Local Internet Registry) rozsah IPv4 adres. Peering pro IPv6 nebyl doposud realizován.

V rámci povýšení na CMS 2.0 dojde k následujícím úpravám:

- Připojení ke dvěma nezávislým poskytovatelům internetové konektivity prostřednictvím dvou směrovačů a dvěma nezávislými okruhy – tzv. BGP multi-homing dislokovanou formou do obou nodů CMS 2.0



Obrázek 8 BGP multi homing

- Každý z dvojice směrovačů bude součástí bloku Internet / sTESTA jiného CMS 2.0 nodu
- Rozhraní mezi CMS BGP a ISP[41] peeringovými směrovači bude realizováno spojem na bázi technologií Gigabit Ethernet (IEEE802.3z, příp. IEEE802.3ab), případně 10Gigabit Ethernet (IEEE802.3ae)
- Směrovače budou připojeny do bloku prostřednictvím mezilehlých L2 přepínačů rozhraním 10Gigabit Ethernet (IEEE802.3ae) směrem k vnějším (veřejným) firewallům
- Z hlediska Internetu bude mít CMS 2.0 přidělen vlastní autonomní systém včetně „Provider Independent" IP adresního prostoru – a to jak pro IPv4, tak pro IPv6 adresy (Local Internet Registry) a bude tak disponovat adresními rozsahy pro IPv4 i IPv6 nezávislými na poskytovatelích.
- Směrování a propagace těchto bloků prostřednictvím BGP-4 peeringu a jeho rozšíření pro IPv6 do internetu
- Zajištění pokud možno efektivního load-balancingu mezi oba ISP prostřednictvím standardně používaných metod (např. simultánní propagace celé a jedné poloviční masky přiděleného rozsahu každým z ISP)

5.1.2.4 Požadované základní parametry peeringových směrovačů:

- Podpora minimálně 1 milionu IPv4 prefixů ve směrovacích tabulkách
- Podpora minimálně 500 tisíc IPv6 prefixů ve směrovacích tabulkách
- Modulární platforma
- Celková propustnost ve směrování minimálně 5Gbps, 7Mpps s možností rozšíření

[41] Internet service provider, viz. terminologický slovník

- Směrovače musí mít možnost výměny klíčových HW komponent za běhu, bez degradace výkonu zařízení během výměny
- Směrovače musí mít možnost výměny částí řídících SW za běhu všech služeb bez jejich přerušení
- Směrovače musí nabízet redundanci řídících komponent
- Směrovače musí nabízet redundanci zdrojů a ventilátorů
- HW ochrana proti DoS útokům na vlastní směrovač (control plane policing)
- Podpora rozhraní:
    - 1GE
    - 10GE
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v pseudoreálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový TCP/UDP port/protokol - NetFlow/IPFix nebo ekvivalent. Funkce monitorování musí být implementována bez negativních vlivů na zátěž a výkon řídících procesorů.
- Podpora bez stavových filtrů na rozhraních v hardware bez vlivu na výkon - podle L2/L3/L4, aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní
- Podpora zónových firewallů
- Účinná ochrana proti vnějším útokům – DoS, DDoS, IP spoofing
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.1.2.5 Připojení k sTESTA síti

Připojení bude z logického hlediska realizováno prakticky shodnou formou jako u CMS 1.0.

Evropská síť sTESTA je připojena ke každému stávajícímu peeringovému uzlu bloku Interconnect – E jedním NxE1 okruhem prostřednictvím dvojice předsunutých hraničních směrovačů, jejichž výkon a vlastnosti odpovídá formě a kapacitě připojení. Tyto realizují dynamické směrování prefixů sítí sTESTA a propagují rozsah přidělený pro ČR. Do tohoto rozsahu jsou následně překládány všechny komunikační toky s prostředím sTESTA.

Veškerá komunikace v aktuálním stavu probíhá výhradně IPv4 formou.

V rámci povýšení na CMS 2.0 dojde k těmto úpravám:

- Každý z dvojice směrovačů bude součástí bloku Internet / sTESTA jiného CMS 2.0 nodu
- Směrovače budou připojeny do bloku prostřednictvím mezilehlých L2 přepínačů rozhraním Gigabit Ethernet (IEEE802.3z, příp. IEEE802.3ab) směrem k vnějším (veřejným) firewallům
- Směrem do vnějšího prostředí budou připojeny k hraničnímu směrovači sTESTA sítě rozhraním Gigabit Ethernet (IEEE802.3z, příp. IEEE802.3ab)
- Na směrovačích bude realizováno IPv6 směrování pro potřeby IPv6 komunikace se subjekty sTESTA

- Na vnějších (veřejných) firewallech bloku Internet a sTESTA bude pro oddělení tohoto provozu vytvořen dedikovaný virtuální firewall
- Virtuální firewall bude realizovat aplikaci transportních pravidel, překlady komunikace z/do přidělených adresních rozsahů pro ČR a detekci průniku

Vzhledem k plánovanému rozšíření komunikačních nároků se sítěmi sTESTA v rámci CMS 2.0 může být aktuální povýšení hraničního směrovač na výkonnější platformu. Po vyhodnocení budoucích komunikačních potřeb se sítěmi sTESTA může dojít k povýšení následně dle specifikace z následné kapitoly.

5.1.2.6 Požadované základní parametry nových směrovačů pro sTESTA:

- Podpora minimálně 300 tisíc ipv4[42] prefixů ve směrovacích tabulkách
- Podpora minimálně 100 tisíc ipv6[43] prefixů ve směrovacích tabulkách
- Celková propustnost ve směrování minimálně 400 Mbps, 0.8Mpps
- Směrovače musí nabízet redundanci zdrojů
- HW ochrana proti DoS útokům na vlastní směrovač (control plane policing)
- Podpora rozhraní:
    - 1GE
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v pseudoreálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový TCP/UDP port/protokol - NetFlow/IPFix nebo ekvivalent. Funkce monitorování musí být implementována bez negativních vlivů na zátěž a výkon řídících procesorů.
- Podpora bez stavových filtrů na rozhraních v hardware bez vlivu na výkon - podle L2/L3/L4, aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní
- Účinná ochrana proti vnějším útokům – DoS, DDoS, IP spoofing
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.1.2.7 Vnější (veřejné) firewally

V CMS 1.0 je tento sub-modul instalován jako součást bloku Interconnect-E.

Jeho funkce bude v rámci CMS 2.0 obdobná. Nicméně funkce původního CMS 1.0 bloku sdílených služeb bude v CMS 2.0 realizována jinou formou prostřednictvím ostatních modulů. Jednou z těchto funkcí bude i realizace DMZ1 sítí pro publikaci služeb jednotlivých subjektů KIVS do internetu, kterou přebere vnější firewall.

V CMS 2.0 budou veřejné firewally plnit tyto základní funkce:

---

[42] **Internet Protocol version 4, viz. terminologický slovník**

[43] **Internet Protocol version 6, viz. terminologický slovník**

- Realizace hraničního perimetru zabezpečení pro externí služby – internet a sTesta logicky separovanou formou oddělených kontextů
- Realizace rozhraní pro sítě typu DMZ1
- Aplikace pravidel transportní vrstvy
- Statické i dynamické překlady pro IPv4 služby
- Aplikační inspekce pro vybrané sady protokolů
- Zabezpečení formou IPS a DDoS ochran

Začlenění do infrastruktury:

- V rámci CMS 2.0 bloku Internet/sTesta bude aplikována vždy dvojice veřejných firewallů do každého bloku každého nodu CMS 2.0
- Dvojice bude vždy zajišťovat redundanci v rámci nodu formou clusteru Active/Active.
- Cluster bude směrem do Internetu a sTESTA sítí připojen prostřednictvím mezilehlých L2 přepínačů rozhraním Gigabit Ethernet (IEEE802.3z, příp. IEEE802.3ab) nebo 10Gigabit Ethernet (IEEE802.3ae), které budou realizovat mmj. i L2 konektivitu pro komunikaci v rámci redundantního clusteru
- Směrem do centra CMS 2.0 nodu bude cluster připojen přímo k připojovacím MPLS PE směrovačům, každý firewall clusteru vždy k oběma a to výhradně rozhraním 10Gigabit Ethernet (IEEE802.3ae)
- Jako jednu z dvojic lze po rozšíření a úpravě efektivně využít stávající cluster firewallů z bloku Interconnect-E

5.1.2.8 Požadované základní parametry vnějších firewallů:

- Podpora rozhraní:
  - 1GE – min. 2x
  - 10GE – min. 4x
- Celková propustnost ve směrování min. 10 Gbps
- Počet konkurenčních spojení min. 4 miliony
- Podpora pro 120 tisíc nových spojení/s
- Podpora 80 tisíc souběžných NAT/PAT překladů
- Celková propustnost minimálně 3Mpps
- Fyzická rozhraní firewallu virtualizovatelná pomocí 802.1q
- Podpora softwarové virtualizace dílčích firewallů – tvorba kontextů – alespoň 200
- Statefull firewall, protokolové filtry
- Podpora redundantních clusterů Active-Standby i Active-Active
- Plná synchronizace stavových informací v redundantním uspořádání
- Vestavěné nebo vestavitelné funkce IDS/IPS/DDoS
- Podpora L3 (směrovaného) i L2 (transparentního) režimu virtuálních firewallů

- Podrobná inspekce HTTP protokolu
- Možnost filtrování peer-to-peer aplikací
- Definice rolí a přístupových práv administrátorů – lokální + standardní metody AAA

5.1.2.9 VPN koncentrátory

Tato funkce je v rámci CMS 1.0 řešena v bloku Interconnect-I, kde jsou umístěny stávající VPN koncentrátory.

Služba umožňuje zakončit IPSec/SSL tunel z Internetu na VPN koncentrátoru sdílených služeb a dešifrovaná data poslat do příslušné MPLS VPN sítě subjektu KIVS. Pro přímé směrování dešifrovaných dat do jednotlivých zákaznických VPN MPLS sítí je koncentrátor připojen k uzlům InterConnect-I prostřednictvím MPLS technologie.

Podporovány jsou site-site IPSec tunely, klientské IPSec tunely i klientské SSL based tunely.

V rámci CMS 2.0 bude mít služba tunelovaného přístupu tuto podobu:

Z pohledu LAN to LAN (Site to Site) se bude na vzdálené straně vždy jednat o jednoznačně určenou IPSec konfiguraci, jejíž parametry určuje správce CMS 2.0 (parametry IKE, volba šifry, atd.). Konfigurace v centru může být zřizována správcem staticky pro každý tunel tohoto typu nebo lze využít metod dynamického tunelování. Autentizace bude realizována buď formou sdíleného klíče s definovanou úrovní kombinace, prostřednictvím certifikátu či kombinací.

Z hlediska klientského přístupu půjde o jediný připojovací uzel (definovaný jednou IP adresou, jedním doménovým jménem nebo jednou položkou ve VPN klientovi). Soustava musí umožnit implementaci ověřovacích a autorizačních služeb a podporovat požadované komunikační parametry. Pravidla komunikace jsou definována centrálně, tj. řídí je správce CMS 2.0

5.1.2.10 Kategorie tunelovaných VPN přístupů:

- Site – Site IPsec VPN
    - Je realizován mezi VPN koncentrátorem a hraničním routerem přistupujícího subjektu
    - Umožňuje realizaci řízené IP konektivity
- Klientský IPSec VPN přístup
    - Realizován prostřednictvím softwarového VPN klienta protokoly typu ESP se zapouzdřením
    - Umožňuje realizaci řízené IP konektivity
- Klientský SSL VPN přístup
    - Realizován prostřednictvím softwarového VPN klienta přes Secure Socket Layer (SSL)
    - Umožňuje realizaci řízené IP konektivity
- WEB based SSL VPN přístup
    - Realizován přes Secure Socket Layer (SSL) formou webového rozhraní
    - Není třeba instalace softwarového klienta
    - Neumožňuje přístup na úrovni IP konektivity
    - Umožňuje přístup pouze k vybraným službám z webového prohlížeče

5.1.2.11 Funkční požadavky na autentizační procesy:

- Systém umožní ověřit vzdálené uživatele minimálně dvěma nezávislými metodami současně
- Povinnými metodami jsou:
    - Uživatelské jméno a heslo
        - Statické
        - Případně určené systémem pro generování jednorázových hesel
    - PKI certifikát (X.509v3) uložený lokálně na počítači nebo na externím médiu (USB tokenech apod.)
- Systém musí umožňovat přebírat žádosti o certifikáty, přidělovat certifikáty, odebírat jejich platnost, dát k dispozici seznam neplatných certifikátů OCSP protokolem a ve formě CRL – standardní správa klíčového hospodářství
- Po ověření uživatele proti centralizované či jiné databázi budou uživateli přiřazena přístupová práva ke zdrojům a službám v CMS 2.0 i v síti subjektu, podle pravidel uložených v databázi CMS 2.0.
- Systém bude zaznamenávat informace o uživatelích připojujících se přes VPN
- Zaznamenány budou minimálně následující informace:
    - Jednoznačná identifikace uživatele
    - Počáteční a koncový čas připojení
    - Objem přenesených dat
    - Neúspěšné pokusy o připojení
- Po definovaném počtu neúspěšných pokusů bude uživatelský účet omezen či zablokován

Jelikož se plánuje značný nárůst subjektů s potřebou připojení včetně obcí s rozšířenou působností, lze očekávat značný nárůst VPN připojení všech kategorií obecně. Pouze centrální forma autentizační databáze nebude tak již dále použitelná jako jediné řešení.

Požaduje se tak možnost aplikace decentralizovaného autentizačního modelu. Toho lze dosáhnout např. formou RADIUS proxy, která bude přesměrovávat případné autentizační požadavky klientů vybraných domén na autentizační vlastní servery těchto domén.

5.1.2.12 Funkční požadavky na softwarové VPN klienty:

- VPN klient musí být dostupný pro běžné operační systémy – minimálně Windows XP, Windows Vista, Windows 7, Windows 8, Linux, MAC a dále systémy pro smart mobilní zařízení - Windows Mobile, Android a Symbian apod.
- Podporované metody ověřování musí být v souladu s výše uvedenými požadavky na autorizační služby
- Klient musí obsahovat aspoň základní stavový firewall a být schopen zkontrolovat a vynutit aktivaci personálního firewallu a zamezení připojení k dalšímu komunikačnímu prostředku nebo síti
- Metody typu split-tunneling nejsou podporovány
- Definice komunikačních parametrů a metod ochrany komunikace se musí řídit centrálně

- Klient musí být od stejného dodavatele, jako je soustava VPN koncentrátorů a musí být s touto soustavou plně kompatibilní
- Konfigurace by měla být proveditelná nejlépe pomocí jediného instalačního a konfiguračního souboru
- Distribuci, instalaci a konfiguraci VPN klientů a podporu uživatelů zajistí správce CMS 2.0

Začlenění VPN koncentrátorů do infrastruktury:

- V rámci CMS 2.0 bloku Internet/sTesta bude aplikována vždy sada dvou VPN koncentrátorů do každého bloku každého nodu CMS 2.0
- Dvojice bude vždy zajišťovat redundanci v rámci nodu formou clusteru Active/Active.
- Koncentrátory budou připojeny přímo k připojovacím MPLS PE směrovačům, každý firewall clusteru vždy k oběma a to výhradně rozhraním 10Gigabit Ethernet (IEEE802.3ae)

5.1.2.13 Požadované základní parametry VPN koncentrátorů:

- Podpora rozhraní:
  - 1GE – min. 2x
  - 10GE – min. 2x
- Celková propustnost ve směrování min. 10 Gbps
- Počet konkurenčních spojení min. 4 miliony
- Podpora až pro 120 tisíc nových spojení/s
- Celková propustnost minimálně 3Mpps
- Minimální počet simultánních SSL tunelů 2 tisíce (licenčně až rozšiřitelných na 10 tisíc)
- Minimální počet simultánních IPSec tunelů 10 tisíc
- Fyzická rozhraní firewallu virtualizovatelná pomocí 802.1q
- Plná synchronizace stavových informací v redundantním uspořádání
- Definice rolí a přístupových práv administrátorů – lokální + standardní metody AAA
- Spolupráce se systémy AAA v rámci autentizačních / autorizačních procesů klientských VPN
- Podpora redundantních clusterů Active-Standby i Active-Active

5.1.2.14 Prostředky pro rozklad zátěže – Load Balancery

Pro garanci dostupnosti, zajištění škálovatelnosti a optimalizace služeb bude použito zařízení pro vyvažování zátěže tzv. Load Balancery.

Obecný princip fungování těchto prostředků je založen na principu vytváření virtuálních adres pro konkrétní služby a následného přesměrovávání provozu na konkrétní fyzické instance dle široké škály pravidel. Množině serverů nebo jiných zařízení s vlastní IP adresou je tak přidělena jedna virtuální IP adresa (VIP) a např. serverová farma tak vystupuje vůči uživateli jako jeden logický server. Z toho plyne prakticky neomezena škálovatelnost, vysoká dostupnost a optimalizace provozu.

Každé takovéto řešení umožňuje dynamické a z pohledu uživatele transparentní přidávání a odebrání zdrojů. Rovněž výpadek jednoho nebo i více serverů zůstane před uživatelem skryt.

V CMS 1.0 jsou tyto služby poskytovány v rámci bloků Sdílených služeb a Centrálního firewallu. Slouží primárně pro rozklad zátěže v rámci infrastruktury DMZ1, DMZ2 a sdílených služeb (Web GW, Mail GW, DNS, apod.)

V rámci CMS 2.0 bude tato funkce řešena primárně právě v blokem Internet/sTESTA, kam budou Load Balancery zakomponovány. Jejich prostřednictvím bude realizován rozklad komunikace v rámci všech sdílených služeb, kde se tato funkcionalita očekává a to včetně služeb v rámci DMZ1 i DMZ2. Podobná funkcionalita se nadále nutně očekává i v bloku Centrálních eGon služeb.

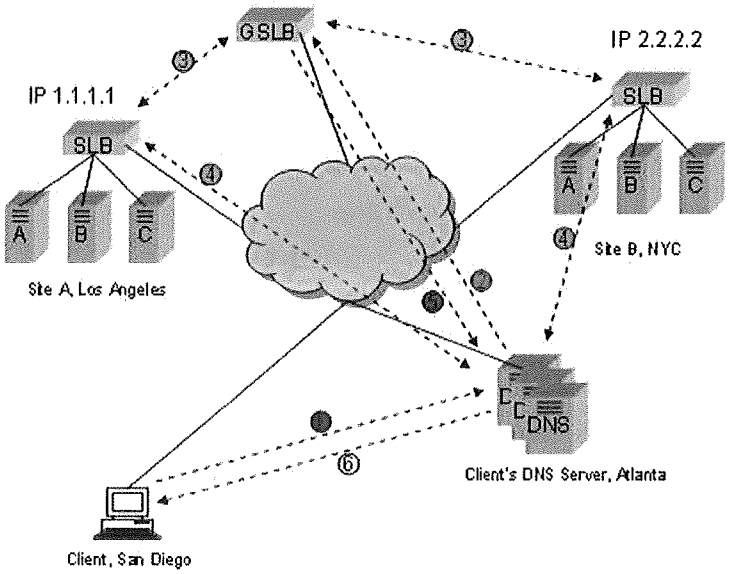
Load balancery musí v rámci tohoto bloku dále podporovat další velmi podstatnou nadstavbovou funkcionalitu a tou je rozklad zátěže mezi lokalitami nodů CMS 2.0. Tohoto bude principielně dosaženo použitím funkce GSLB (Global Server Load Balancing) v implementaci konkrétního vendorského řešení, obecné principy GSLB jsou nicméně stále shodné.

GSLB pracuje na principu rozdělení zátěže pro konkrétní lokalitu prostřednictvím rozdílných DNS odpovědí na DNS/FQDN dotazy zasílané klienty. Spolupráce GSLB instancí s DNS servery příslušných domén je tedy v tomto případě esenciální.

Klienti dostávají na své DNS dotazy odpovědi s různými adresami reprezentujícími konkrétní fyzickou či virtuální IP adresu pro službu v dané lokalitě. Tím je dosaženo rozkladu zátěže mezi vlastními lokalitami.

O konkrétní IP adrese odeslané jako DNS odpověď může rozhodovat množina volitelných faktorů. Můžou jimi být dostupnost, zatížení, zdrojové IP adresy, počty spojení, apod. Konkrétní požadavky jsou popsány v odstavci požadovaných parametrů load balancerů.

Následující obrázek principielně popisuje daný proces včetně jednotlivých fází výběru:



Obrázek 9 Load Balancing na základě GSLB principů

I zde je důležitou vlastností detekce výpadku a tudíž v tomto případě přesměrování provozu na jinou lokalitu, což je pro dané použití velmi zásadní. Jelikož mezi klientem a cílovými instancemi není realizována žádná komunikace typu health-check, musí být přesměrovávání na jinou lokalitu řešeno odlišným způsobem od klasického server load balancingu. Toho je v praxi dosaženo DNS odpověďmi obsahujícími více záznamů typu A. Tím je dosahováno konkrétní přepínání komunikace na požadovanou cílovou adresu. Metoda ovšem předpokládá podporu na straně algoritmů pracujících s DNS a FQDN jmény obecně v rámci klientů – OS, web browsery, apod.

5.1.2.15 Požadavky na funkci a topologii Load Balancerů

- V rámci CMS 2.0 bloku Internet/sTesta bude aplikována vždy sada minimálně dvou load balancerů do každého bloku každého nodu CMS 2.0
- Dvojice bude vždy zajišťovat redundanci v rámci nodu formou clusteru Active/Active, popř. Active/Standby
- Koncentrátory budou připojeny přímo k připojovacím MPLS PE směrovačům, každý load balancer clusteru vždy k oběma a to výhradně rozhraním 10Gigabit Ethernet (IEEE802.3ae)
- Variantou může být implementace load balancerů ve formě funkčních modulů přímo v rámci připojovacích MPLS PE směrovačů

5.1.2.16 Požadované základní parametry Load Balancerů:

- Podpora rozhraní:
    - 10GE – min. 2x
- Balancing aplikačního provozu na základě vrstev L3 – L7 s podporou balancingu obsáhlého setu protokolů typu až do 7. vrstvy OSI (ftp, dns, http/http, cookies, apod.)
- Propustnost minimálně 10 Gbit/s s možností rozšíření
- Podpora 802.1Q virtuálních rozhraní na fyzických portech
- Bridging/routing balancovací mód
- Client/Server NAT
- SSL hardwarová akcelerace
- Podpora redundantních clusterů Active-Standby i Active-Active
- Podpora režimu redundance se synchronizací stavových tabulek
- Propustnost až 3,5 milionu TCP spojení
- Podpora až 400 tisíc nových sestavených spojení/s
- Plná podpora IPv6
- Podporované metody pro vyvažování zátěže:
    - Kruhová metoda s vážením
    - Podle počtu navázaných spojení
    - Podle otisku zdrojové a cílové adresy
    - Podle URL a cookie
    - Na základě SNMP (např. zátěže procesorů)
    - Podle vah pro skupiny

- Monitorování stavu a zátěže zdrojů/serverů:
  - Kontinuální monitorování nejen serverů, ale i celé cesty
  - Možnost kombinace (AND/OR) více metod (např. ARP, ICMP, DNS, HTTP, TCP port, SSL Hello, SMTP, RADIUS, LDAP atd.)
  - Možnost definování intervalu pro monitorování
- Rozdělování zátěže mezi více lokalitami (tzv. GSLB – Global server load balancing):
  - Na základě DNS (load balancer si „drží" DNS A záznam pro danou službu)
  - Možnost odpovídat více DNS A záznamy
  - Na základě vlastnosti aplikací, HTTP přesměrování (např. HTTP hlavička 302 - Moved Permanently)
- Směrování zátěže na stejný server (tzv. perzistence):
  - Na základě L3/L4 parametrů (např. zdrojová IP)
  - Hash funkce na základě IP
  - Na základě L7 parametrů (statické i dynamické cookies, HTTP hlavička)
  - RADIUS
  - ID SSL spojení
- Modifikace provozu:
  - Vložení/přepsání cookie
  - Modifikace URL
  - Možnost vložit zdrojovou IP do L7 hlavičky
  - Modifikace HTTP obsahu
- Optimalizace provozu:
  - Ukončování SSL spojení (tzv. SSL offloading) což výrazně snižuje zátěž serverů a mimo jiné usnadňuje management certifikátů
  - TCP multiplexing, kdy jedno TCP spojení mezi serverem a load balancerem obsluhuje více spojení mezi klientem a load balancerem
  - Komprese http
  - Caching
- Podpora virtualizace – minimálně 200 virtuálních instancí

5.1.2.17 Infrastruktura sdílených služeb

Jedná se o skupinu síťových služeb, jejichž HW prostředí bude součástí bloku Internet/sTesta. Jde o služby podpůrného charakteru, které jsou z části potřebné k poskytování konkrétních hlavních služeb CMS 2.0 dle Katalogu služeb CMS 2.0 a z části k zajištění globální funkce síťové infrastruktury jako celku a to nejen v rámci vlastní CMS 2.0, ale i obecně v rámci KIVS.

Z hlediska CMS 1.0 jsou tyto služby realizovány v samostatném bloku Shared Services. Ani v CMS 2.0 není jejich umístění dogmaticky nutné do bloku Internet/sTesta, nicméně sem z hlediska povahy a potřeb nejvíce náleží. Variantně mohou být umístěny do bloku Datových center.

Blok bude obsahovat primárně tyto služby:

- HTTP/HTTPs proxy

- SMTP brána (MTA)
- DNS brána
- NTP brána

Součástí bloku se mohou stát další služby centrálního podpůrného charakteru, které sem mohou svou povahou náležet či jejichž umístění v tomto bloku se bude jevit efektivní.

5.1.2.18 HTTP/HTTPs proxy (WEBová Gateway/Proxy)

Služba webové proxy musí nad rámec své esenciální funkce – tedy proxy pro http/https komunikaci – poskytovat bezpodmínečně tyto nadstavbové funkce:

- Klasifikace provozu
- Následná kategorizace s případnou filtrací obsahu
- Antivirová kontrola pro http/https a ftp over http provoz
- Služba Proxy cache

CMS 2.0 musí nabízet službu URL (Uniform Resource Locators) filtrace pomocí řešení proxycache, které provádí antivirovou kontrolu webového provozu a navíc přináší podporu online databáze klasifikovaných webových stránek s možností blokování stránek s určitou klasifikací (např. pornografie, sex, zábava, p2p sítě, warez, ...) a možností individuálního blokování dalších „nežádoucích" adres. Klasifikace stránek je prováděna na základě kategorií.

CMS 2.0 musí umožnit realizovat URL politiku pro skupiny uživatelů, pro jednotlivé typy souborů a to pro libovolnou denní i noční dobu. Tento produkt také poskytuje pravidelné i „on-line" dodávané reporty včetně grafů a tabulek, které vypovídají o internetových aktivitách uživatelů. Samozřejmostí jsou i informace o denním provozu, nejčastěji požadovaných URL adresách, aktivitách jednotlivých uživatelů včetně možnosti nastavení limitu apod.

Provoz s http protokolem je dále podroben antivirové kontrole. Http proxy podporuje funkci IP spoofing což umožňuje přenos zdrojové adresy ze vstupu na výstup proxy brány. Tato funkcionalita zajišťuje pro http/https provoz jednoznačnou identifikaci uživatelské VPN sítě napříč celou infrastrukturou. Každý subjekt má přidělenu unikátní veřejnou IP adresu.

Dále systém poskytuje antivirovou ochranu souborů přenášených pomocí FTP. Provoz „ftp over http" je podroben antivirové kontrole.

Služba Proxy cache bude sloužit jako prostředník v komunikaci. Dotaz z prohlížeče Uživatele bude nejprve poslán Proxy serveru v CMS, který jej přeformuluje a pošle požadavek dále na originální - cílový server. Před odesláním požadavku zkontroluje, nemá-li tento požadovaný dokument v paměti (cache). HTTP/HTTPS/FTP Proxy v CMS bude využívat komunikace dvou typů, komunikaci klient - Proxy CMS a komunikaci Proxy CMS - Proxy VPN Uživatele.

5.1.2.19 SMTP brána (MTA či SMTP relay)

SMTP proxy zajišťuje relay mailového provozu mezi Internetem a uživatelskými VPN sítěmi. Mailový provoz je podroben antivirové kontrole. Je možné zajistit identifikaci zdrojové adresy uživatelské VPN sítě. Každý z možných subjektů bude mít pro mailový provoz přidělenu samostatnou veřejnou IP adresu.

Základní bezpečnostní politika bude blokovat veškeré zavirované zprávy. Zprávy obsahující spam pouze jednoznačně označuje (modifikací předmětu zprávy, přidáním příznaků do hlavičky zprávy).

Kontrola obsahu nemá v žádném případě charakter prověřování datového toku za účelem monitorování a zachytávání přenášených dat.

5.1.2.20 DNS brána

DNS brána poskytuje jmenné služby jednak uživatelským VPN sítím a to jak pro resolving jmen v doménách uvnitř CMS tak pro resolving doménových jmén v externích sítích jako je internet či sTESTA.

Současně DNS proxy slouží i pro vnitřní potřeby CMS 2.0, tedy poskytuje služby např. ostatním proxy branám jako je např. http/ttp/ftp/smtp proxy. V neposlední řadě je na této službě postaven základ GSLB řešení, které zajišťuje dostupnost celých nodů CMS 2.0. Jedná se tedy o zcela stěžejní síťovou službu, tudíž z hlediska infrastrukturního musí být bezpodmínečně zajištěna v modelu HA řešení s tou nejvyšší možnou dostupností.

5.1.2.21 NTP brána

Služba přesného času - NTP (Network Time Protocol) bude určena pro trvalou synchronizaci systémového času jednotlivých prvků infrastruktury. Služba NTP zajišťuje systémový čas pro synchronizaci systémových záznamů – logů a synchronizaci hraničních prvků. Synchronizovaný čas v síti bude sloužit k přesné identifikaci posloupnosti jednotlivých událostí v síti z hlediska reálného času tak, jak je zaznamenávají jednotlivé systémy. Přesný čas je nutný pro zajištění monitorování, měření a řízení sítí.

Začlenění bloku sdílených služeb do infrastruktury:

- Servery služeb budou připojeny prostřednictvím vlastních přístupových přepínačů bloku sdílených služeb
- Tyto přístupové přepínače budou posléze připojeny přímo k připojovacím MPLS PE směrovačům, každý vždy k oběma a to výhradně rozhraním 10Gigabit Ethernet (IEEE802.3ae)

5.1.3 Připojovací blok datových center

Tento blok bude reprezentovat hraniční MPLS PE směrovače propojující konkrétní datové centrum do páteřního bloku. Prozatím jsou v architektuře zvažována dvě datová centra – STC a Sazečská.

5.1.3.1 Požadavky na funkci a topologii DC bloků

Vlastní připojovací část bloku bude tvořena dvojicí MPLS PE směrovačů, které zde tvoří agregační podvrstvu a k nimž jsou redundantně připojeny všechny potřebné celky DC, ať již napřímo, či prostřednictvím přístupové podvrstvy.

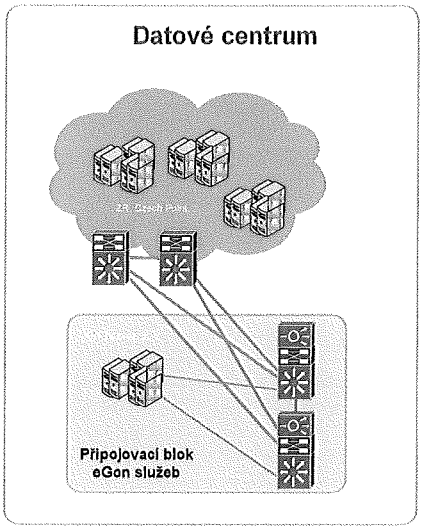
Přístupová podvrstva bude k připojovacímu bloku DC realizována stejnou formou, jaká je popsána výše pro začlenění bloku sdílených služeb do infrastruktury připojovacího bloku Internet/sTESTA.

HW nároky na MPLS PE směrovače připojovacího bloku DC jsou shodné s HW nároky připojovacích MPLS PE směrovačů bloku Internet/sTESTA.

Základním principem celého návrhu architektury CMS 2.0 by měla být modularita a redundance. Proto není podstatné, kolik bude datových center a kde budou dislokována. Pokud bude zajištěna redundantní konektivita mezi připojovacím blokem datového centra a alespoň dvěma MPLS P směrovači páteřního bloku, bude vždy zajištěna plná dostupnost a vysoká odolnost proti výpadku. V případě dislokace datového centra mimo lokality nodů CMS 2.0 se požaduje pro jeho připojovací blok konektivita na MPLS P směrovače páteřního bloku z obou nodů.

V rámci DC bloků je vždy vyžadována služba rozkladu zátěže.

Následující obrázek představuje modelové schéma DC bloku:



Obrázek 10 Modelové schéma DC bloku

5.1.3.2 Požadované parametry load balancerů pro DC bloky:

- Podpora rozhraní:
  - 10GE – min. 2x
- Balancing aplikačního provozu na základě vrstev L3 – L7 s podporou balancingu obsáhlého setu protokolů typu až do 7. vrstvy OSI (ftp, dns, http/http, cookies, apod.)
- Propustnost minimálně 10 Gbit/s s možností rozšíření
- Podpora 802.1Q virtuálních rozhraní na fyzických portech
- Bridging/routing balancovací mód
- Client/Server NAT
- SSL hardwarová akcelerace
- Podpora redundantních clusterů Active-Standby i Active-Active
- Podpora režimu redundance se synchronizací stavových tabulek
- Propustnost až 3,5 milionu TCP spojení
- Podpora až 400 tisíc nových sestavených spojení/s
- Plná podpora IPv6

- Podporované metody pro vyvažování zátěže:
    - Kruhová metoda s vážením
    - Podle počtu navázaných spojení
    - Podle otisku zdrojové a cílové adresy
    - Podle URL a cookie
    - Na základě SNMP (např. zátěže procesorů)
    - Podle vah pro skupiny
- Monitorování stavu a zátěže zdrojů/serverů:
    - Kontinuální monitorování nejen serverů, ale i celé cesty
    - Možnost kombinace (AND/OR) více metod (např. ARP, ICMP, DNS, HTTP, TCP port, SSL Hello, SMTP, RADIUS, LDAP atd.)
    - Možnost definování intervalu pro monitorování
- Směrování zátěže na stejný server (tzv. perzistence):
    - Na základě L3/L4 parametrů (např. zdrojová IP)
    - Hash funkce na základě IP
    - Na základě L7 parametrů (statické i dynamické cookies, HTTP hlavička)
    - RADIUS
    - ID SSL spojení
    - Modifikace provozu:
    - Vložení/přepsání cookie
    - Modifikace URL
    - Možnost vložit zdrojovou IP do L7 hlavičky
    - Modifikace HTTP obsahu
- Optimalizace provozu:
    - Ukončování SSL spojení (tzv. SSL offloading) což výrazně snižuje zátěž serverů a mimo jiné usnadňuje management certifikátů
    - TCP multiplexing, kdy jedno TCP spojení mezi serverem a load balancerem obsluhuje více spojení mezi klientem a load balancerem
    - Komprese http
    - Caching
- Podpora virtualizace – minimálně 50 virtuálních instancí

Požadavky na formu začlenění load balancerů do DC bloku jsou shodné jako u bloku Internet/sTESTA.

5.2 Páteřní blok:

V rámci stávajícího řešení CMS 1.0 není tento blok realizován, řešení má odlišnou architekturu.

Hlavní smysl páteřního bloku bude realizace propojení všech jednotlivých připojovacích bloků.

Ten tak musí primárně zajistit:

- Obousměrné šíření jednotlivých VPN tam, kde je to žádoucí
    - Na všechny přístupové bloky
    - Na blok propojovacích služeb

- Realizaci propojení obou lokalit nodů CMS 2.0 na páteřní úrovni

5.2.1 Požadavky na funkci a topologii páteřního bloku:

HW skladbu tohoto bloku budou tvořit vysokorychlostní MPLS směrovače typu P, vždy dva v každé lokalitě nodu CMS 2.0. Tyto mezi sebou budou propojeny vždy výhradně rozhraním 10Gigabit Ethernet (IEEE802.3ae) do kruhové topologie prostřednictvím WAN agregátních traktů v rámci DWDM sítě.

V rámci každého z nodů bude k MPLS P směrovačům připojen jeden základní MPLS směrovač v roli BGP route-reflectoru, jehož obecným smyslem je agregace a zefektivnění jinak mutlipointního BGP peeringu a následná hvězdicová distribuce směrovacích informací směrem ke konkrétním MPLS PE směrovačům.

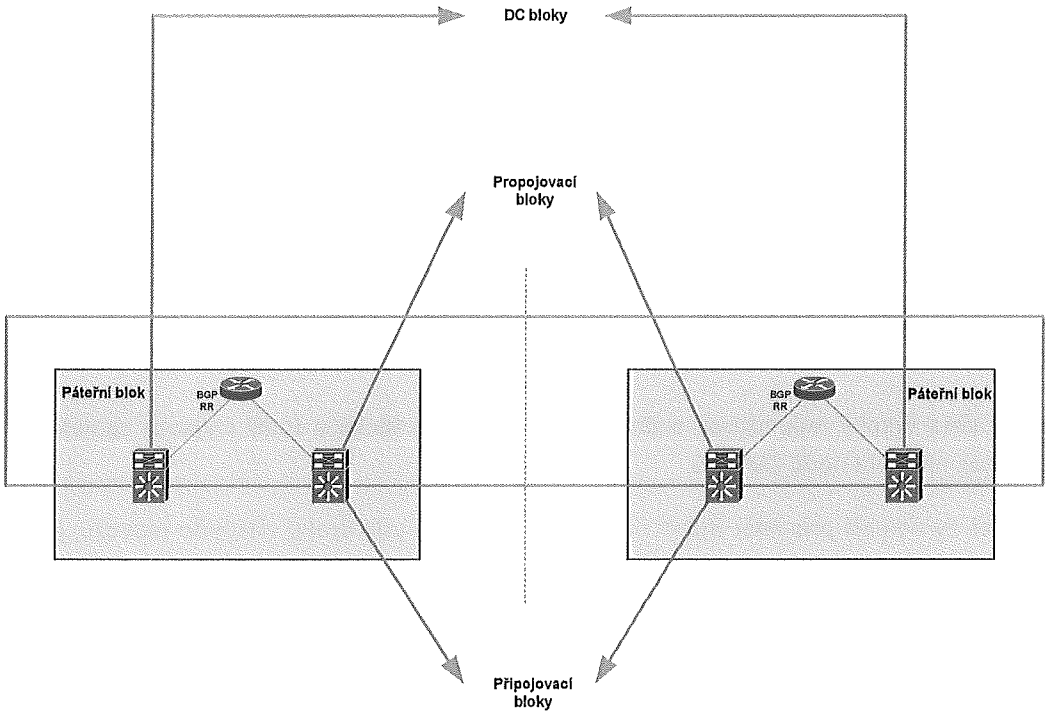
Tím bude zajištěna vysoká redundance a dostupnost páteřního bloku a tudíž i vysoce spolehlivé vzájemné propojení lokalit nodů CMS 2.0.

Páteřní část sítě by neměla provádět žádné složité operace ve smyslu druhu vlastního provozu, jako např. zajištění QoS, shaping, filtrování dle přístupových pravidel apod. Cílem je zde v maximální míře eliminovat všechny procesy, které by mohly způsobovat jakékoliv zpomalení při zpracování jednotlivých paketů. Naopak přímočaré a rychlé odeslání paketu k cílovému rozhraní je zde primárním záměrem. Zároveň by do této části nemělo být přímo připojené žádné zařízení či přímo koncový uživatel.

Páteřní vrstva je v některých ohledech v porovnání s ostatními na první pohled jednodušší, nicméně nejkritičtější částí modelu. Poskytuje velmi omezené množství služeb, jejím cílem je ale zajistit vysokou dostupnost a fungovat v plně redundantním režimu.

MPLS směrovače typu P budou fyzicky umístěny v jádru MPLS sítě a jsou odpovědné výhradně za rychlé přepínání paketů na základě značek, pouze s podporou protokolu LDP zajišťujícího jejich distribuci. Není na nich tedy k zajištění této funkcionality třeba podpory protokolu BGP a tudíž na nich BGP vůbec běžet nemusí.

Obrázek níže znázorňuje topologii páteřního bloku:



Obrázek 11 Topologie páteřního bloku

5.2.1.1 Požadované základní parametry MPLS P směrovačů propojovacího bloku:

- Modulární platforma
- Neblokující architektura směrování, striktně se vyžaduje plně line-rate dle maximálních možností osazených rozhraní
- Směrovače musí mít možnost výměny klíčových HW komponent za běhu, bez degradace výkonu zařízení během výměny
- Směrovače musí mít možnost výměny částí řídících SW za běhu všech služeb bez jejich přerušení
- Směrovače musí nabízet redundanci řídících komponent
- Směrovače musí nabízet redundanci zdrojů a ventilátorů
- Distribuovaná architektura (oddělený Control Plane a Data Plane)
- HW ochrana proti DoS útokům na vlastní směrovač (control plane policing)
- Plná podpora směrování IPv4 i IPv6 v hardware a to jak směrových tak více směrových vysílání
- Podpora rozhraní:
    - 1GE, minimálně 4x s možností rozšíření
    - 10GE, minimálně 10x s možností rozšíření
    - rozšiřitelnost na 40GE
- Replikace multicastových rámců v hardware

- Podpora MPLS pro IPv4/IPv6
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v pseudoreálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový TCP/UDP port/protokol - NetFlow/IPFix nebo ekvivalent. Funkce monitorování musí být implementována bez negativních vlivů na zátěž a výkon řídících procesorů.
- Kontrola zdrojové IPv4, IPv6 adresy na fyzických i logických L3 rozhraních podle aktuální směrovací tabulky (antispoofingová kontrola ekvivalentní funkci uRPF (Unicast Reverse Path Forwarding)
- Podpora flexibilní práce s VLAN tagy
- Podpora Bidirectional Forwarding Detection (BFD) pro rychlou detekci poruchy mezi směrovači
- Podpora sdružování portů přes více šasi
- Podpora rozložení zátěže mezi sdruženými porty
- Podpora Jumbo Frame o velikosti minimálně 9KByte
- Tx and Rx optical power monitoring (DOM) na optických portech
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.2.1.2 Požadované základní parametry BGP route-reflectorů propojovacího bloku:

- Podpora minimálně 2 milionů IPv4/IPv6 prefixů ve směrovacích tabulkách
- Směrovače musí mít možnost výměny částí řídících SW za běhu všech služeb bez jejich přerušení
- Směrovače musí nabízet redundanci zdrojů a ventilátorů
- HW ochrana proti DoS útokům na vlastní směrovač (control plane policing)
- Podpora rozhraní:
    - 1GE – min. 2x
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.3 Propojovací blok

Tato funkcionalita je v rámci CMS 1.0 realizována modulem centrálního firewallu. Propojovací služby budou v rámci CMS 2.0 realizovány samostatným propojovacím blokem.

Tento bude i zde primárně zajišťovat:

- Řízené bezpečné propojení VPN mezi sebou
- Realizaci DMZ2 sítí

- Implementaci funkcí, nutných pro realizaci propojovacích služeb, např. proxy, DNS, SMTP relay, služeb pro DMZ, služeb eGon Service Bus (ESB) apod. Předpokládá se samozřejmě využití virtualizovaného prostředí souvisejících bloků

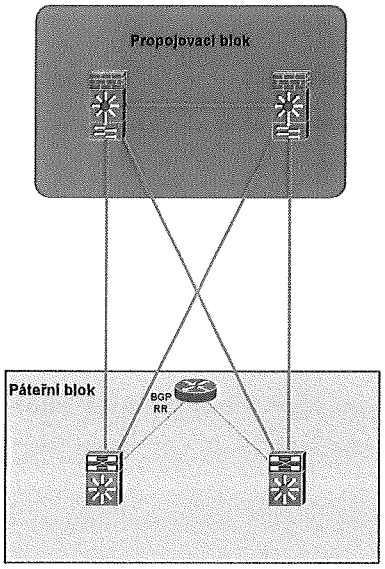
HW skladba tohoto bloku bude vedle připojovacích MPLS PE směrovačů tvořit vždy dvojice firewallů v clusteru a pracovním režimu Active/Active. Firewally zde mohou tvořit funkční kaskády pro případy vyčerpání některých systémových prostředků. Lze tedy libovolně a škálovatelně připojovat další clustery v případě nárůstu potřeb nad rámec běžícího řešení.

5.3.1 Požadavky na funkci a topologii propojovacího bloku

- Vlastní připojovací část bloku bude tvořena dvojicí MPLS PE směrovačů. MPLS PE směrovače jsou následně propojeny se všemi směrovači páteřního bloku v daném CMS 2.0 nodu a to vždy a to výhradně rozhraním 10Gigabit Ethernet (IEEE802.3ae)
- K připojovacím MPLS PE směrovačům budou připojeny oba firewally modulu, vždy každý firewall ke každému ze směrovačů a to opět rozhraním 10Gigabit Ethernet (IEEE802.3ae)
- Firewally mohou být variantně implementovány ve formě funkčních modulů přímo v rámci připojovacích MPLS PE směrovačů

Variantou k fyzické dvojici směrovačů může být jejich virtualizace či případně - viz kapitola Možnosti architektury pro Připojovací blok KIVS.

Obrázek níže ukazuje vazbu propojovacího bloku na páteřní blok:



Obrázek 12 Vazba propojovacího bloku na páteřní blok

5.3.1.1 Obecná funkce bloku

Hlavní funkcionalitou této propojovací části bude terminace všech MPLS VPN všech subjektů směrem k firewallům, které budou zajišťovat jejich bezpečnostní perimetr.

Vstupní Layer-3 rozhraní každého subjektu připojujícího se do prostředí CMS bude zrealizováno na pro tento subjekt vyhrazeném virtuálním firewallu (dále jen VFW), jakákoliv komunikace směrující ze

subjektu do prostředí či naopak tedy musí projít tímto VFW. Směrování mezi jednotlivými subjekty bude zajištěno dynamickou formou prostřednictvím BGP.

Virtuální firewall jako vstupní prvek každého zákazníka do prostředí CMS bude vždy obsahovat minimálně 3 základní L3 rozhraní:

- Vstupní rozhraní od zákazníka (potažmo ve směru od připojovacího bloku KIVS)
    - Přes toto rozhraní budou směrovány adresní rozsahy zákazníka, které využívá ve své vnitřní síti
- Vstupní rozhraní do prostředí CMS 2.0 (směrem ke sdíleným službám, datovým centrům a ostatním zákazníkům prostředí)
- Management rozhraní
- Volitelně další rozhraní – např. DMZ2

5.3.1.2 Požadované základní parametry směrovačů propojovacího bloku:

- Modulární platforma
- Neblokující architektura směrování, předpokládá se line-rate dle maximálních možností osazených rozhraní
- Směrovače musí mít možnost výměny klíčových HW komponent za běhu, bez degradace výkonu zařízení během výměny
- Směrovače musí nabízet redundanci řídících komponent
- Směrovače musí nabízet redundanci zdrojů a ventilátorů
- Distribuovaná architektura (oddělený Control Plane a Data Plane)
- HW ochrana proti DoS útokům na vlastní směrovač (control plane policing)
- Plná podpora směrování IPv4 i IPv6 v hardware a to jak směrových tak více směrových vysílání
- Podpora rozhraní:
    - 10GE, minimálně 6x s možností rozšíření
    - rozšiřitelnost na 40GE
- Replikace multicastových rámců v hardware
- Podpora virtuálních směrovacích instancí - minimálně 3 tisíce
- Podpora MPLS pro IPv4/IPv6
    - MPLS L3 / L2 VPN
    - MPLS Traffic Engineering
    - VPLS
- Podpora monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v pseudoreálném čase minimálně: zdrojová/cílová IP, zdrojový/cílový TCP/UDP port/protokol - NetFlow/IPFix nebo ekvivalent. Funkce monitorování musí být implementována bez negativních vlivů na zátěž a výkon řídících procesorů.

- Kontrola zdrojové IPv4, IPv6 adresy na fyzických i logických L3 rozhraních podle aktuální směrovací tabulky (antispoofingová kontrola ekvivalentní funkci uRPF (Unicast Reverse Path Forwarding)
- Podpora bez stavových filtrů na rozhraních v hardware bez vlivu na výkon - podle L2/L3/L4, aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní
- Podpora flexibilní práce s VLAN tagy
- Podpora Bidirectional Forwarding Detection (BFD) pro rychlou detekci poruchy mezi směrovači
- Podpora sdružování portů přes více šasi
- Podpora rozložení zátěže mezi sdruženými porty
- Podpora Jumbo Frame o velikosti minimálně 9KByte
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ dle RFC 2474, 2475, 2597, 2598, 2697, 3270):
    - Klasifikace a reklasifikace rámců/paketů na vstupu i výstupu (IEEE 802.1p, IP DSCP, IP Precedence, EXP MPLS).
    - Omezování provozu (policing) na vstupu i výstupu (kompatibilita s RFC 2697 a/nebo RFC 2698), konfigurovatelné mechanismy preventivní ochrany proti zahlcení.
    - Podpora QoS Shapingu a Policingu bez dopadu na výkon směrovače
- Směrovače by měly být z provenience jednoho výrobce za cílem dosažení plné inter-operability

5.3.1.3 Požadované základní parametry firewallů propojovacího bloku:

- Podpora rozhraní:
    - 10GE – min. 4x
- Celková propustnost ve směrování min. 10 Gbps
- Počet konkurenčních spojení min. 4 miliony
- Podpora pro 200 tisíc nových spojení/s
- Podpora 500 tisíc souběžných NAT/PAT překladů
- Celková propustnost minimálně 4Mpps
- Fyzická rozhraní firewallu virtualizovatelná pomocí 802.1q
- Podpora softwarové virtualizace dílčích firewallů – tvorba kontextů – alespoň 250
- Statefull firewall, protokolové filtry
- Podpora redundantních clusterů Active-Standby i Active-Active
- Plná synchronizace stavových informací v redundantním uspořádání
- Vestavěné nebo vestavitelné funkce IDS/IPS/DDoS
- Podpora L3 (směrovaného) i L2 (transparentního) režimu virtuálních firewallů
- Podrobná inspekce HTTP protokolu

- Možnost filtrování peer-to-peer aplikací
- Definice rolí a přístupových práv

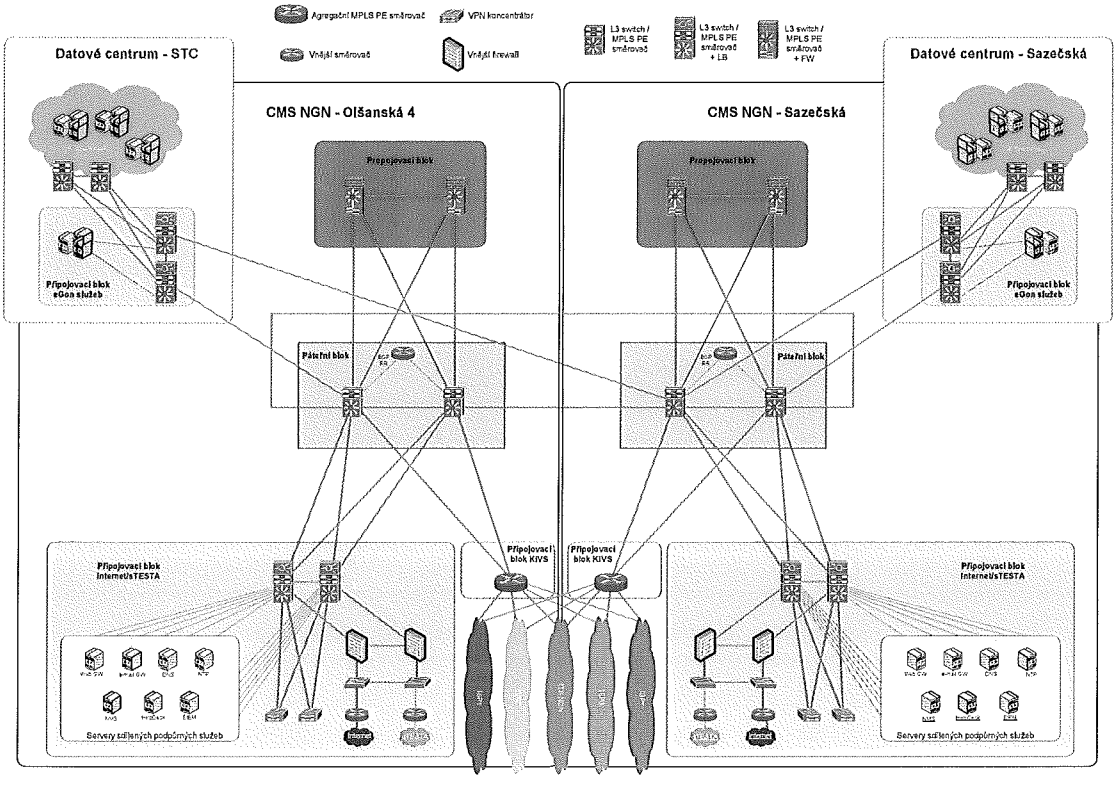
6 Celková architektura CMS 2.0

Komplexní architektura každého z nodů CMS 2.0 bude tvořena souborem výše popsaných funkčních bloků. Tyto nody musí být díky funkci jednotlivých bloků a jejich vzájemné inter-operabilitě schopny poskytovat všechny popsané služby CMS 2.0 samostatně, tedy bez sebemenší závislosti na druhém nodu. Z toho plyne i požadavek na plnou hardwarovou duplicitu obou nodů s cílem poskytnout zcela shodné systémové prostředky v rámci obou nodů.

Z hlediska topologie se předpokládá, že nody CMS 2.0 budou implementovány na lokality Olšanská 4 a Sazečská. Do lokality Sazečská nemá dnes zadavatel (MVČR) vybudovanou žádnou transportní infrastrukturu. V rámci realizace a implementace CMS 2.0 budou poskytnuty tyto spoje provozovatelem a správcem budoucího CMS 2.0 v níže uvedené podobě a kvalitě. Zároveň se předpokládá zjištění možností budoucí realizace přímého propojení infrastruktury MVČR do lokality Sazečská v rámci fáze inženýringu popisované v samostatné kapitole.

Dále se v počátku předpokládá připojení min. dvou datových center (v budoucnu dalších) a to v lokalitách Olšanská 4 (shodně s lokalitou CMS nodu) a Sazečská (Malešice).

Na obrázku níže jsou blokově rozkresleny oba nody a jejich bloky včetně propojovacích traktů pro realizaci vzájemné interoperability a modelové připojení datových center:



Obrázek 13 Interoperabilita a modelové připojení datových center

6.1 Interkomunikace mezi nody CMS 2.0 – model redundance nodů

Primární forma distribuce datových informací mezi nody CMS 2.0 bude realizována prostřednictvím páteřních směrovačů tvořících jádro páteřních bloků. Páteřní směrovače budou zajišťovat rychlou distribuci datových rámců mezi všemi připojovacími bloky a propojovacím blokem a to bez závislosti na umístění daného bloku. Destinace datových rámců bude určena prostřednictvím mechanismů load balancingu na síťových a transportních vrstvách popsaných v předchozích kapitolách. Vlastní směrování bude probíhat formou přepínání MPLS paketů, směrovače páteřního bloku budou mít status MPLS P směrovačů. Výpadek žádného z páteřních směrovačů či traktů nesmí žádným způsobem ohrozit kontinuální distribuci rámců do obou nodů, konvergence se předpokládá v horizontu desítek až stovek milisekund za použití mechanismů typu BFD (Bidirectional Forwarding Detection).

Infrastruktura traktů mezi páteřními bloky musí být plně redundantní a nezávislá, tedy min. dva zcela nezávislé trakty o kapacitě 10Gbps mezi páteřními bloky obou CMS nodů – viz. obrázek výše. Na základě aktuální topologie a možností infrastruktury budoucího provozovatele se předpokládá využití kapacity 2x10Gbps pro každý trakt formou tzv. Client Based rozkladu kapacit přes kruhovou DWDM topologii. Trakt má potom podobu dvou logických 10Gbps linek realizovaných na úrovni DWDM fyzicky vždy po odlišné části kruhu. Oba trakty jsou následně agregovány, např. prostřednictvím protokolu LAGP na L2 či podobnými metodami. Vlastní využití redundantních traktů je potom řízeno o úroveň výše, tedy v daném příkladu aktivními prvky pracujícími na druhé vrstvě nad DWDM infrastrukturou. Výhodou takového řešení je plná Active-Active forma topologie s reálně dvojnásobnou kapacitou (při standardních provozních situacích) a garancí původní kapacity 10Gbps (při neprovozních stavech transportní infrastruktury). Variantou k tomuto modelu 10Gbps DWDM traktů může být realizace redundance již na vlaství úrovni DWDM vrstvy, kdy si směrování traktu v rámci kruhu řídí samotná inteligence DWDM multiplexorů, ať již standardní metodou statických path protection v rámci kruhů či prostřednictvím virtuálních point-multipoint logických přepínačů pracujících na L2.

Realizace výše uvedených traktů se předpokládá primárně prostřednictvím virtuálních spojů na DWDM infrastruktuře či případně prostřednictvím přímých Dark Fibers.

V případě potřeby přímé L2 komunikace mezi instancemi jednotlivých bloků umístěnými v odlišných nodech bude třeba zajistit nad rámec L3 propojení na úrovni páteřního bloku i případné přímé L2 trakty mezi těmito instancemi či jejich bloky. Rozhraními pro tyto služby může být Gigabitový Ethernet, Fiber Channel, FCoE, apod. Příkladem takové komunikace může být třeba symetrizace datových polí v rámci DC bloků, synchronizace databází či synchronizace stavových informací.

Realizace výše uvedených traktů se předpokládá buď prostřednictvím virtuálních spojů na DWDM infrastruktuře či prostřednictvím L2 tunelů v rámci služeb IP/MPLS vrstvy (MPLS L2 pseudowire, VPLS, atd.).

6.2 Architektura nodu

Forma topologie a architektura každého nodu musí též klást vysoký důraz na dostupnost a redundanci v rámci nodu. Je zde striktní požadavek na vždy plně redundantní konektivitu mezi páteřním blokem a všemi sousedními bloky, viz. blokové schéma výše.

Všechny systémové komponenty realizující lokální propojení musí být vždy povinně zdvojené či min. obsahovat zdvojené řídící a podpůrné moduly.

6.3 Připojení datových center

Připojovací bloky datových center a redundance jejich architektury je požadována minimálně na úrovni ostatních bloků nodů CMS 2.0, jak je uvedeno v předcházejících kapitolách.

Zde navíc v případě, kde bude datové centrum umístěno mimo lokalitu nodu CMS, bude nutno zajistit jeho připojení na páteřní bloky obou CMS nodů pro případ zajištění dostupnosti konkrétního DC při možném komplexním výpadku jednoho z nodů CMS 2.0. V případě umístění DC do stejné lokality s nodem CMS 2.0 je na zvážení a posouzení dle možností místní propojovací i podpůrné infrastruktury, je-li připojení pouze na místní nod CMS 2.0 dostatečné. Hlediskem pro volbu propojení musí být reálnost situace, kdy by DC mohlo zůstat samostatně v provozu při případném výpadku celého místního nodu CMS 2.0.

Dalším nadstavbovým aspektem je v případě připojení datových center striktní požadavek na L2 šifrování v případě, kdy bude datové centrum připojeno pronajatou linkou poskytovanou mimo infrastrukturu vlastníka nebo správce CMS 2.0. Požadavek se považuje za nezbytný v případě, je-li ve správě poskytovatele druhá či vyšší vrstva dle modelu OSI.

6.4 Model funkční komunikace na síťové vrstvě

CMS 2.0 bude již ze své podstaty i názvu sloužit primárně jako prostředí pro realizaci bezpečných centrálních propojení mezi subjekty, přístupu k centrálním službám a datovým centrům.

Vstupními místy pro inicializaci komunikace budou (viz. kapitola Přístupové služby CMS 2.0):

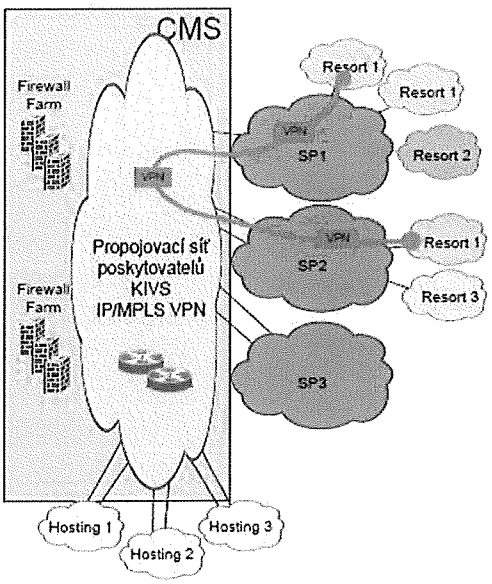
- Prostředí infrastruktury KIVS, ať již standardní formou VPN rozhraní na vstupu do připojovacího bloku KIVS či prostřednictvím služby Krajský konektor CMS 2.0
- Internetové přístupy
- Extranet CMS 2.0

6.4.1 Prostředí infrastruktury KIVS

Datové toky subjektu iniciované v tomto prostředí vstoupí do CMS 2.0 vždy prostřednictvím připojovacího bloku KIVS.

Následně nastává zásadní rozcestí v komunikaci. V případě, kdy je cílem síťová instance umístěná v rámci VPN subjektu realizované jiným operátorem KIVS, komunikace opouští Připojovací blok KIVS rozhraním VPN subjektu směřujícím k tomuto konkrétnímu operátorovi.

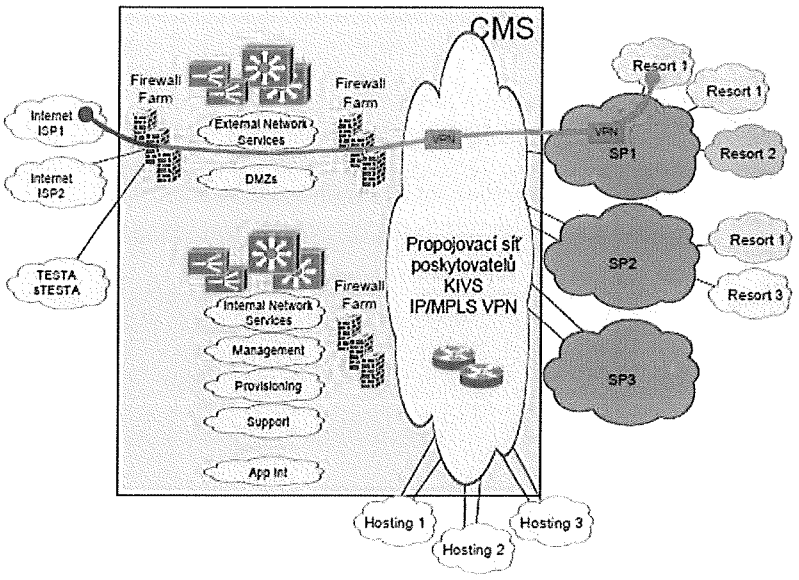
Následující obrázek reflektuje takovou formu komunikace:



Obrázek 14 Komunikace KIVS vs Service provider

Pokud však je cílem datového toku jakákoliv centrální instance či služba CMS 2.0, tok vstoupí skrze tranzitní služby páteřního modulu do Propojovacího bloku. V rámci tohoto bloku je datová komunikace terminována na virtuálním firewallu subjektu. Odsud bude následně skrze další rozhraní příslušného virtuálního firewallu s návazností na interní MPLS VPN zřízen přístup k centrálním službám, DMZ a datovým centrům dle definic bezpečnostních pravidel na virtuálním firewallu. Vlastní komunikace z virtuálního firewallu na příslušné propojovací bloky bude samozřejmě zase vždy realizována prostřednictvím páteřního modulu.

Na následujícím obrázku je znázorněn příklad této komunikace, zde konkrétně pro komunikaci navazovanou směrem do internetu:



Obrázek 15 Komunikace směrem do internetu

6.4.2 Internetové přístupy

Z povahy daného prostředí je předurčeno, že všechny přístupy tohoto typu jsou realizovány formou šifrovaných tunelů.

Datová komunikace šifrovaného kanálu vstoupí do CMS 2.0 přes rozhraní příslušného peeringového internetového směrovače a skrze veřejný firewall a příslušnou bezpečnostní definici se terminuje na VPN koncentrátoru. Veškerá tato komunikace se tak doposud odehraje výhradně v rámci připojovacího bloku Internet/sTESTA.

Odsud po příslušné formě autentizace a autorizace vstupuje již dešifrovaná komunikace do příslušné MPLS VPN subjektu a následně na Propojovací blok směrem k rozhraní příslušného virtuálního firewallu. O příslušnosti k dané MPLS VPN subjektu rozhoduje autorizační proces VPN koncentrátoru a příslušných autentizačních a autorizačních instancí (AAA). Vlastní přístup do Propojovacího bloku směrem k příslušnému virtuálnímu firewallu je samozřejmě opět realizován skrze tranzitní propojovací blok.

Další komunikace je již realizována identickou formou jako v případě přístupu přes KIVS prostředí popsaném v předcházející kapitole.

6.4.3 Extranet CMS 2.0

Dle definice uvedené v katalogu služeb je přístup do Extranetu CMS 2.0 realizován vždy přes internet.

Vlastní Extranet CMS 2.0 bude vlastně jakousi sběrnou sítí pro realizaci přístupu menších subjektů ke službám CMS 2.0. Předpokladem je, že subjekty budou plošně sdílet stejná přístupová práva k příslušným službám, což vyplyne z jejich povahy. Zde by nemělo smysl definovat samostatná

oprávnění na úrovni firewallů a obecnější řešení tohoto druhu je tak efektivní. To je vlastně i primárním smyslem služby Extranet CMS 2.0.

Můžou vznikat požadavky na vytváření více VPN typu Extranet, které budou sdružovat subjekty s podobným zaměřením, potřebami a návaznými přístupovými nároky. Tyto se mohou lišit od ostatních skupin formou svých potřeb a tudíž též definicí bezpečnostních politik. Koncept sdružování subjektů a definice obecných pravidel pro skupinu nicméně zůstává zachován.

Vlastní model komunikace do této sítě je v základu stejný jako v případě internetových přístupů obecně – viz. popis v předchozí kapitole.

Odlišnost nastává až po realizaci AAA procesu při terminaci tunelu na VPN koncentrátoru. O příslušnosti k dané MPLS VPN subjektu opět rozhoduje autorizační proces VPN koncentrátoru a příslušných autentizačních a autorizačních instancí (AAA). Rozdílem je právě forma této VPN, která bude shodná pro všechny připojující se subjekty náležející do dané skupiny Extranetu.

Další forma komunikace je již opět shodná s předchozí kapitolou popisující standardní internetové přístupy.

6.5 Obecné požadavky na šifrování

Komunikační trasy ve správě MVČR případně ve správě jím pověřeným správcem nemusí být šifrovány. Pokud budou využívány pronajaté komunikační trasy vlastněné cizími subjekty, služby ISP, případně bezdrátová pojítka, musí být datová komunikace šifrována.

Jedná se zejména o propojení jednotlivých OPS[44] v rámci kraje všude tam, kde nejsou (nebo nebudou) k dispozici optická vlákna v majetku MVČR. V takovém případě budou přenášená data kryptována hop by hop na L2 úrovni dle standardu 802.1AE (MACsec).

Také pokud dohledová síť pro OOB management[45] bude využívat služeb ISP, budou data kryptována. V tomto případě na L3 úrovni (IPSec).

---

[44] Operační středisko

[45] Out of band management, viz. terminologický slovník

7 Požadavky na management a monitoring

7.1 Globální Event management

Pro CMS je nezbytný efektivní dohled a správa komunikační infrastruktury zastřešená globálním Event Managementem. Tento management musí pokrývat všech pět funkčních oblastí definovaných ISO standardem. Jsou to:

- Management chybových stavů – detekuje, isoluje a opravuje závady vzniklé v komunikační síti.
- Konfigurační management – zahrnuje změnu konfigurací zařízení, inventarizaci zařízení a správu softwarového vybavení zařízení.
- Výkonností management – monitoruje a měří různé aspekty výkonnosti tak, aby celková výkonnost byla na akceptovatelné výši.
- Bezpečnostní management – umožňuje autorizovaným individualitám přístup k síťovým zařízením a korporátním síťovým zdrojům
- Účtovací management – informuje o využití jednotlivých komponent systému

7.1.1 Management chybových stavů

Pro žádoucí kvalitu provozu je nezbytné mít možnost být včas informován o vzniklých chybových stavech, ale také pokud možno chybovým stavům předcházet. Z toho důvodu se předpokládá využití grafické reprezentace topologie síťových prvků. Pro grafické zobrazení stavů zařízení a linek budou využity SMNP informace, RMON zprávy a události, syslog zprávy a další informace. Předpokládá se, že nasazený management systém bude schopen automaticky vyhodnotit informace získané z různých zařízení, provést korelaci a agregaci a poskytnout konsolidovanou informaci o stavu sítě a možné příčině poruchy. Musí poskytovat možnost zpětného dohledání jednotlivých událostí až za jeden rok zpětně.

7.1.2 Konfigurační management

Cílem konfiguračního managementu je umožnit efektivní konfiguraci zařízení tak, aby zřizování a konfigurace služeb pro uživatele (provisioning) bylo rychlé a efektivní. K tomu bude sloužit systém pro automatizaci konfigurací aktivních prvků systému. Konfigurované služby musí být rozděleny podle typu. Pro každý typ služby budou definovány konfigurační šablony, které zjednoduší konfiguraci a provozní údržbu systému. Dále musí konfigurační management poskytovat potřebné informace o konfiguračních souborech, HW konfiguracích, sériových číslech a SW verzích jednotlivých zařízení.

7.1.3 Výkonnostní management

Zahrnuje monitorování běžného provozu (zatížení CPU zařízení a linek, chybovost linek atd.), monitorování SLA parametrů, audit služeb, generování SLA zpráv (dostupnost, zpoždění), detailní sledování provozu na úrovni datových toků (NetFlow export ze směrovačů, vzdálení agenti poskytující informaci o odezvách apod.).

7.1.4 Bezpečnostní management

Má za úkol řídit přístup ke zdrojů v síti v souladu s lokálními pravidly tak, aby nemohla být síť úmyslně či neúmyslně poškozena. Napomáhá konfiguraci síťových zařízení v souladu s doporučenými bezpečnostními pravidly, řídí přístup uživatelů k síti při využití userID a hesel na jednotlivých zařízeních, přístupových seznamů (ACL) a AAA systémů (autentikace – povolení přístupu, autorizace – povolení činností a účtování – sledování činnosti uživatele).

7.1.5 Účtovací management (billing)

je to proces, který slouží k měření využití sítě za účelem rozúčtování nákladů na skupiny uživatelů. Používá obdobné nástroje jako výkonnostní management. Účtovací management je nezbytným základem pro SLA v případě, že je SLA stanoveno dle skupin uživatelů (různé skupiny uživatelů mají různá SLA).

7.1.6 Analýza rizik

Analýza rizik bude zahrnovat identifikování možných hrozeb a jejich dopadů na základě historických dat nebo ze simulačních modelů, určení účinnosti existujících opatření, posouzení jednotlivých rizikových scénářů, určení nezbytnosti a způsobu snižování míry rizika, výběr vhodných bezpečnostních opatření.

7.2 OOB management

Pro CMS je nezbytné mít možnost monitorovat a případně spravovat všechna zařízení i při případné poruše některého z nich. Dále je třeba zajistit, aby přístup ke správě síťových zařízení byl umožněn pouze osobám k tomu určeným. Proto je nezbytné vytvořit oddělenou dohledovou síť, která nebude využívat optickou DWDM infrastrukturu.

Tato nezávislá dohledová síť by mohla být provozována přes některého ISP (MPLS privátní síť, ethernet VPN, pronajatý okruh apod.). Při využití ISP se předpokládá nasazení IPSec kryptování. Standardním rozhraním pro OOB správu zařízení je metalické rozhraní 10/100/1000 Mbit/s.

Pro bezpečnostní monitoring prostředí CMS 2.0 bude nasazen SIEM[46] nástroj, který bude zpracovávat systémové zprávy bezpečnostního charakteru od všech aktivních komponent v prostředí CMS 2.0. SIEM nástroj musí umožňovat funkci korelace a zpracovávání jednotlivých událostí, jejich agregaci a možnost zpětného dohledání až za jeden rok zpětně.

7.3 Service Desk

Stávající systém Service desku MVČR bude upraven včetně dodávek nového HW a SW vybavení tak, aby zabezpečil bezproblémové funkce CMS 2.0 a oblasti KIVS včetně komunikace s uživateli. V rámci dobudování Service desku CMS 2.0 bude realizováno zejména následující:

- Zřízení centrálního portálu pro nahlašování poruch a požadavků.
- Vybudování call centra s automatickým odpovídacím a třídícím systémem.

---

[46] **Security Information and Event Management, viz. terminologický slovník**

- Upgrade HW platformy a přechod do databázového prostředí.
- Automatizace příjmu incidentů.
- Zřízení www přístupového rozhraní k Service Desku z různých sítí (MVČR, CMS, Internet).
- Nastavení procesů dle standardů ITIL, vytvoření jednotné databáze zařízení, případně navázání na existující NI různých systémů.
- Implementace provozního deníku.
- Navýšení klientských přístupů.

8 Vazba CMS 2.0 / ITS 2.0 – ITS NGN

Paralelním probíhajícím projektem k projektu CMS 2.0 je projekt ITS NGN. V rámci projektu ITS NGN je řešeno povýšení a rozšíření páteřní DWDM a WAN infrastruktury, která tvoří dosavadní součást sítě ITS MVČR.

Vzhledem k nezbytnému vzájemnému propojení obou funkčních celků a následné inter-operabilitě existují či musí zákonitě vzniknout další vazby mezi oběma světy.

Jak již je uvedeno výše v kapitolách popisujících návrh architektury CMS 2.0, budou hlavní nody systému umístěny na lokalitách Olšanská 4 a Sazečská. Dále jsou či budou realizována datová centra v lokalitách STC Na Vápence a opět Sazečská.

Výše uvedená topologie předpokládá existenci komunikační infrastruktury umožňující realizaci potřebných datových spojů. Část této komunikační infrastruktury poskytne právě síť ITS NGN.

Základem připojení CMS 2.0 k okolnímu světu je přístup ke KIVS infrastruktuře a veřejným sítím. Jedním ze subjektů KIVS bude právě ITS NGN, jejíž hlavní komunikační uzly v rámci Prahy budou lokality Olšanská 4 a Wintrova. V rámci připojovacího bloku KIVS Olšanská bude tedy mj. realizován přímý propoj do ITS NGN. Zároveň bude v rámci projektu IST NGN realizováno povýšení lokality STC Na Vápence tak, aby lokalita umožňovala poskytování služeb na standardní úrovni definované projektem ITS NGN. Tato část tedy bude posléze využita i pro realizaci připojení DC STC k nodům CMS 2.0

Lokalita Sazečská není ovšem prozatím z hlediska výstavby transportních infrastruktur zahrnuta do žádného ze zmiňovaných projektů. Proto je nutno prozatím zajistit konektivitu jiným způsobem. V počátku je plánováno využití transportní sítě České Pošty jakožto i budoucího správce CMS 2.0. Lokalita Sazečská tak bude do infrastruktury CMS 2.0 připojena touto formou a modelem popsaným v kapitole Interkomunikace mezi nody CMS 2.0.

9 Přípravná fáze projektu – inženýring

V rámci definice průběhu projektu byla identifikována potřeba počátečního detailního prověření stávajícího stavu za cílem stanovení přesných budoucích forem implementace jednotlivých částí. Vstupy získané pro specifikaci budoucího stavu nejsou zcela aktuální a pocházejí z různých nehomogenních zdrojů a také odlišných časových period.

Tato Specifikace funkčních požadavků tedy definuje obecnější principy a cíle, které budou dále upřesněny, rozvíjeny a konkretizovány společně s realizátorem na základě výstupů z jím provedené fáze inženýringu. Fáze inženýringu bude tak první realizační fází projektu a jakousi prerekvizitou pro následné fáze.

9.1 Definice cílů inženýringu

V rámci této fáze realizace projektu CMS 2.0 je požadováno prověření následujících oblastí a dodání podkladů jejich skutečného provedení:

- Prověření přesného HW osazení všech částí stávajících bloků CMS a jeho komplexní soupis
- Identifikace všech prvků a částí bloků využitelných pro vlastní realizaci povýšení na CMS 2.0 s přihlédnutím ke zde definovaným požadavkům na vlastnosti HW, topologii a charakter služby
- Jednoznačné a maximální využití stávajícího HW, pokud samozřejmě plně vyhovuje daným specifikům a nebude nijak omezujícím faktorem pro budoucí požadovanou architekturu a funkci
- Prověření všech skutečností, které nemusí být známy zadavateli a jenž by mohly zefektivnit navrhované řešení či jeho formu

9.2 Požadované výstupy z inženýringu

Jako výstup z této fáze projektu se požaduje:

- Kompletní seznam použitého HW s dělením na:
    - Seznam stávajícího HW, který lze použít pro realizaci s popisem jeho navrhovaného uplatnění
    - Seznam stávajícího HW, u něhož nelze najít využití s odůvodněním
- Obecný návrh technologie pro náhradu nevyužitelných částí
- Obecný návrh formy implementace navrhovaného řešení
- Případné návrhy úprav oproti stanovenému modelu na základě zjištěných skutečností původně zadavateli neznámých
- Eventuální návrhy rozšíření topologie či formy propojení bloků na základě zjištěných či historicky plánovaných skutečností a možností
- Pro lokalitu Olšanská 4 (technologický prostor CMS) provést vzhledem k nové architektuře CMS 2.0 místní šetření zaměřené na možnost jeho realizace z pohledu prostorového řešení, dostatečného elektrického příkonu (běžný provoz/záložní napájení) a chladícího výkonu. V případě nutnosti stavebních úprav zpracovat jejich výčet (rozsah) a vyčíslení jejich ceny.

9.3 Požadavky na průběh inženýringu

Inženýring podléhá potřebám projektu, tj. jeho provedení bude realizováno v takové formě, rozsahu, obsahu a čase, aby bylo vyhověno zadávací dokumentaci. Odchýlení se od zadávací dokumentace podléhá písemnému schválení zástupcem zadavatele.

Cílem inženýringu je navrhnout detailní technickou specifikaci řešení tak, aby bylo možné přistoupit k realizaci. Inženýring bude proveden zejména s ohledem na efektivní využití finančních prostředků alokovaných na projekt. To znamená zejména:

- minimalizace nákladů na inženýring jako takový za současného pokrytí požadovaných výstupů
- výstupy inženýringu počítají s využitím stávající infrastruktury v době životnosti tam, kde nejsou důvody pro její nahrazení
- maximalizace spolehlivosti, výkonnosti a bezpečnosti navrhované infrastruktury v rámci parametrů definovaných tímto dokumentem

Řešitel během fáze inženýringu umožní osobám pověřeným zadavatelem náhled do rozpracovaných materiálů týkajících se projektu. Řešitel bude zadavateli v rámci fáze inženýringu předkládat v pravidelných intervalech reporty o průběhu prací. Forma, obsah a perioda a další náležitosti budou ustanoveny smluvně mezi zadavateli a řešiteli. Před zahájením inženýrských prací bude dále mezi zadavatelem a řešitelem ustanoveno:

- rámcová forma a obsah výstupu inženýringu (obsah je definován tímto dokumentem)
- časový rámec prací, milníky
- finanční rámec, limity
- relevantní kvantitativní a kvalitativní kritéria pro akceptaci dílčích i celkového výstupu
- osoby realizující akceptaci za stranu zadavatele
- komunikační pravidla a osoby realizující výměnu informací mezi zadavatelem a řešitelem

Výstupem inženýringu je detailní technická specifikace projektu v takové podobě, jak ji definuje tento dokument.

9.4 Zachování hodnoty investic

Celý projekt CMS 2.0 bude realizován s ohledem na princip zachování investic. Tuto skutečnost musí inženýring zohlednit. Pokud existují vyhovující funkční zařízení s délkou životnosti větší než jeden rok v době ukončení projektu, budou tato použita pro CMS 2.0. Lze akceptovat odůvodněné výjimky. Použití takových zařízení nesmí narušit funkčnost, bezpečnost, stabilitu a další provozní parametry celého systému. Princip zachování hodnoty investic je nutné posuzovat v kontextu principu maximalizace přínosů projektu do budoucna.

Zkratky a terminologický slovník

AIS	Agendový informační systém.
ASBR	Autonomous System Boundary Router.
CFW	Central Fire Wall.
CMS	Centrální místo služeb
CWDM	Coarse WDM (wavelength-division multiplexing). Technologie multiplexující počet přenašečů signálu na jednom optickém vlákně za použití různých vlnových délek (barev) světla.
Demilitarizovaná zóna (DMZ)	Fyzická nebo logická část sítě, která obsahuje a vystavuje služby organizace, směřující navenek, do vnější sítě, typicky internetu.
Denial-of-service (DoS)	Útok mající za cíl znepřístupnit síťové zařízení pro jeho uživatele.
Distributed denial-of-service (DDoS)	Útok mající za cíl znepřístupnit síťové zařízení pro jeho uživatele. Je vedený z několika různých systémů zároveň.
Domain Name System (DNS)	Hierarchický distribuční jmenný systém pro počítače a jiná zařízení, připojené do internetu.
DWDM	Dense WDM (wavelength-division multiplexing). Technologie multiplexující počet přenašečů signálu na jednom optickém vlákně za použití různých vlnových délek (barev) světla. DWDM na rozdíl od CWDM používá hustší multiplex vlnových délek.
eGoncentrum	Technologické centrum ORP nebo Kraje
eGon Service Bus	Zabezpečuje propojení informačních systémů centrálních služeb.
File Transfer Protocol (FTP)	Síťový protokol sloužící k přenosu souborů, typicky v rámci internetu.
Firewall (FW)	Bezpečností softwarový nebo hardwarový prvek sítě jehož funkcí je kontrolovat příchozí a odchozí provoz prostřednictvím analýzy datových paketů.
Help Desk	Služba resp. zdroj, který poskytuje konečnému uživateli informaci nebo podporu pro využití produktu nebo služby.
Hosting	Provozování aplikace nebo informačního systému z datového centra poskytovatele.
Hypertext Transfer Protocol (HTTP)	Aplikační protokol pro přenos hypertextových dokumentů.
Hypertext Transfer Protocol Secure (HTTPS)	Protokol pro bezpečnou komunikaci v rámci sítě, především internetu. Jde o přidání bezpečnostních možností SSL ke standardní HTTP komunikaci.

IETF TRILL	Internet Engineering Task Force – Transparent Interconnection of Lots of Links.
Internet Protocol Security (IPsec)	Jedná se o soubor protokolů pro zabezpečení IP komunikace pomocí mj. autentifikace a kryptování každého IP paketu.
Internet service provider (ISP)	Společnost poskytující službu připojení k internetu.
IOP	Integrovaný operační program
Interconnect	Fyzické propojení sítě se zařízeními, které do ní nativně nepatří.
Internet Protocol version 4 (IPv4)	Čtvrtá a nejrozšířenější verze internet protokolu. Popsaný v RFC 791.
Internet Protocol version 6 (IPv6)	Poslední revize internet protokolu. Vznikla se záměrem nahradit IPv4 z důvodu omezeného počtu adres IPv4.
ISVS	Informační systémy veřejné správy. Veškeré informační systémy veřejné správy.
KIVS	Komunikační infrastruktura veřejné správy. Zahrnuje infrastrukturní komunikační prostředky, které využívá veřejná správa.
Local area network (LAN)	Lokální síť typicky nepřesahující hranice budovy nebo objektu.
MLAG	Multi-chassis Link Aggregation.
Multiprotocol Label Switching (MPLS)	Mechanismus v rámci telekomunikačních sítí, který navádí data z jednoho síťového uzlu na další bez nutnosti složitého vyhledávání ve směrovacích tabulkách.
MVČR	Ministerstvo vnitra České republiky.
Network Time Protocol (NTP)	Síťový protokol pro synchronizaci hodin mezi počítačovými systémy.
Next-generation network (NGN)	Síť nové generace postavená na myšlence, kdy jedna síť přenáší veškeré informace a služby (hlas, video, data, apod.) v paketech podobných těm, které jsou použity v rámci internetu.
Virtual Private LAN Service (VPLS)	Způsob jak zajistit multipoint to multipoint komunikaci založenou na Ethernetu.
VPN koncentrátor	Síťové zařízení zajišťující kryptování a autentifikaci.
Mail Transfer Agent (MTA)	Softwarová služba, která přenáší zprávy elektronické pošty z jednoho počítače na jiný.
Multi-mode optický spoj	Typ optického vlákna používaného v komunikacích na krátké vzdálenosti.
OPS	Operační středisko

ORP	Obec s rozšířenou působností
Out-of-band management	Systém nezávislé dohledové sítě, oddělené od dohlížené sítě.
OVM	Orgán veřejné moci
Provisioning	Proces přípravy a realizace zpřístupnění resp. poskytnutí služeb sítě zákazníkovi (uživateli).
Proxy cache	Funkce proxy serveru která ukládá navštívené webové stránky aby při příštím požadavku na jejich zobrazení mohlo dojít k načtení z proxy serveru a nikoli jejich původního zdroje.
QoS	Quality of Service.
Secure Sockets Layer (SSL)	Kryptografický protokol používaný pro zajištění komunikační bezpečnosti přes internet.
Service Desk	IT služba fungující jako jediné kontaktní místo pro uživatele systému. Zprostředkovává standardizovanou komunikaci mezi zákazníkem systému a provozovatelem systému.
Security Information and Event Management (SIEM)	Řešení umožňující analýzu (v reálném čase) bezpečnostních zpráv generovaných síťovým HW a aplikacemi.
Směrovač (router)	Zařízení přeposílající datagramy na místo určení.
sTESTA	Zabezpečená komunikační infrastruktura EU.
Uniform resource locator (URL)	Konkrétní řetězec znaků, který tvoří odkaz na internetový zdroj.
VFW	Virtuální firewall
VPN	Virtual private network. Rozšíření privátní sítě a jejích zdrojů přes veřejné sítě.
Wide area network (WAN)	Rozsáhlá síť pokrývající metropolitní, regionální, národní území.