Základní informatizace krajských úřadů

Realizační projekt

Kraj Vysočina

Verze 3.2

ICZ a.s.

OBSAH

1 ÚVOD

Předkládaný realizační projekt úzce navazuje na souběžně připravovaný typový projekt základní informatizace krajských úřadů a zohledňuje specifika, potřeby a priority řešení krajského úřadu. Jeho těžiště se na základě provedené analýzy a vzájemné výměny názorů se zástupci zadavatele i se zástupci krajského úřadu soustřeďuje na konkrétní řešení komunikační infrastruktury, síťové bezpečnosti, antivirové ochrany a vytvoření základního aplikačního prostředí krajského úřadu (servery, personální počítače, databázový systém apod.) do kterého je nasazeno několik nejdůležitějších aplikací. Z časových a finančních důvodů je přizpůsobení takto nasazených aplikací požadavkům zákona 365/2000 Sb. (např. vzájemná výměna informací přes referenční rozhraní apod.) přesunuta na druhou etapu informatizace krajských úřadů.

2 TECHNOLOGICKÝ MODEL

2.1 Návrh specifického řešení subsystémů

2.1.1 Subsystém komunikační infrastruktury

Při konzultacích s odpovědnými pracovníky byly stanoveny následné priority v oblasti síťové infrastruktury a připojení k síti Internet.

- Přepínače a směrovače jsou preferovány produkty společnost Cisco Systems Inc.
- Bude zachována stávající infrastruktura a bude počítáno s využitím infrastruktury nové.
- Jelikož je stávající komunikační infrastruktura pouze dočasná a bude v budoucnu vybudovaná zcela nová, bude v tomto projektu řešena komunikační infrastruktura pouze z koncepčního hlediska s uvedením vhodných zařízení pro budoucí realizaci.
- Stávající přístup k síti Internet byl shledán nevyhovujícím a bude nahrazen novým připojením.

2.1.1.1 Stávající stav

Nyní uvedeme velice stručný popis stávající komunikační infrastruktury a připojení této infrastruktury na Internet.

Lokální síť

V současné době má KÚ ve všech lokalitách k dispozici dočasnou strukturovanou kabeláž. Ta je tvořena metalickými rozvody CAT 5. Koncové stanice jsou připojeny do rozbočovačů Edimax v jednotlivých místnostech, tyto rozbočovače jsou potom připojeny přímo do centrálního přepínače Cisco. Do interní datové sítě je v současné době připojeno 120 uživatelů.

V budoucnu dojde k přestěhování KÚ do nových lokalit, kde bude vybudována zcela nová strukturovaná síť. Realizační projekt této fyzické infrastruktury bude teprve vypracován.

Interní elektronická pošta je realizována (servery i klienti) na platformě MS Exchange 2000. Interní DNS je realizován pomocí Active Directory na platformě MS Windows 2000.

Připojení na Internet

Stávající připojení na Internet je realizováno pomocí firewallu u ISP a firewallu realizovaného operačním systémem Windows s produktem WinRoute v lokalitě KÚ. Na tomto firewallu jsou také realizovány následující proxy: SMTP, http, FTP a další.

Externí jmenné služby jsou realizovány na DNS serveru, který je umístěn u ISP WebHouse a je tímto ISP také spravován.

2.1.1.1.1 Síťová architektura

Jelikož fyzická infrastruktura bude teprve vybudována, nelze konkrétně navrhnout síťovou architekturu. Proto zde zmíníme alespoň principy a doporučení, kterými by se měl budoucí návrh sítě řídit, samozřejmě se zohledněním specifik nové sítě.

Vnitřní datová síť bude koncipována jako lokální datová síť dle standardu IEEE 802.3 ve standardní verzi Ethernet poskytující maximální přenosovou rychlost 10 Mbit/s nebo ve verzi FastEthernet IEEE 802.3u poskytující maximální přenosovou rychlost 100 Mbit/s.

Spoje, kde bude z jakéhokoliv důvodu požadována vyšší šířka pásma, budou řešeny alternativně dvěmi způsoby dle požadované šířky pásma. Prvním z nich je propojení dle standardu IEEE 802.3z GigabitEthernet, druhou možností je použití technologie EtherChanel společnosti CISCO Systems Inc. agregující několik fyzických spojů do jediného logického spoje.

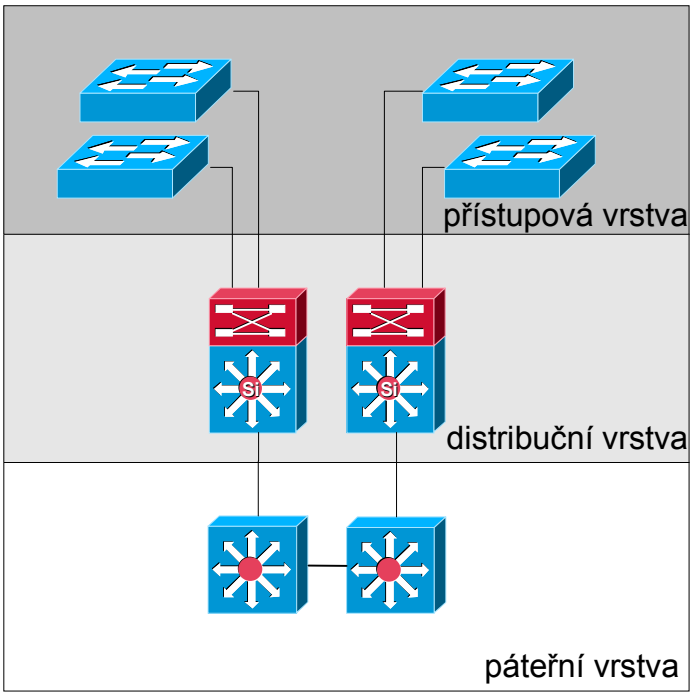
Pro docílení nezávislosti topologie sítě na fyzické topologii bude v návrhu sítě použita technologie VLAN, dle normy IEEE 802.1Q, která umožní rozdělení lokální sítě na dostatečný počet logických segmentů definovaných , bez ohledu na fyzickém umístení stanic, napříč celou vnitřní sítí. Komunikace mezi jednotlivými segmenty bude probíhat řízeným způsobem na třetí - tedy síťové - vrstvě ISO-OSI modelu.

2.1.1.1.1.1 Topologie

Při návrhu topologie bude vycházeno z hierarchického modelu. Jednotlivé prvky jsou rozděleny do několika vrstev v závislosti na funkci, kterou vykonávají. Úloha jednotlivých prvků je nejlépe patrná z následujícího obrázku.

Obr. 1

Hierarchický model



Přístupová vrstva:

Zprostředkovává přístup jednotlivých koncových zařízení do vnitřní sítě, značkuje jednotlivé rámce odpovídajícími značkami VLANů, filtruje rámce. Jednotlivé pracovní stanice mohou spolu sdílet šířku pásma. Mohou být aplikována základní bezpečnostní opatření, např. DUD (Disconect unathorized device)

Distribuční vrstva:

Zajišťuje směrování mezi VLANy, na této vrstvě jsou taktéž aplikována bezpečnostní pravidla provádějící řízení a kontrolu provozu mezi jednotlivými VLANy a pravidla pro šíření všesměrového vysílání (broadcast) a skupinového vysílání (multicast).

Páteřní vrstva:

Vyjma případu, kdy se vnitřní síť nachází v několika od sebe vzdálených budovách a nejedná se tak o LAN síť (local area network), ale o síť MAN (metropolian area network) bude páteřní vrstva kolabovat do vrstvy distribuční.

Topologií fyzické vrstvy rozumíme schéma propojení jednotlivých aktivních prvků komunikačními linkami, postihující všechny spoje, avšak abstrahující od jejich konkrétního vedení v terénu respektive v objektech.

2.1.1.1.1.2 Fyzická

Konkrétní fyzická topologie vnitřní sítě bude závislá na infrastruktuře která bude teprve vybudována. Obecně doporučujeme použít stromovou topologii. Hlavním prvkem stromu bude centrální přepínač, který zajišťuje propojení serverů a přístupových přepínačů. Jednotlivé přístupové přepínače zajišťují propojení koncových stanic, scanerů, tiskáren a dalších zařízení. Pro zajištění vyšší spolehlivosti a tím i bezpečnosti sítě předpokládáme možné zdvojení centrálních prvků a datových spojů směrem k přístupovým přepínačům. Konkrétní fyzická topologie bude popsána až v projektu, který se bude zabývat výstavbou nové komunikační infrastruktury (tento projekt je teprve v přípravě).

2.1.1.1.1.3 Logická

Vnitřní síť bude mít tyto logické části:

- interní část,
- externí část.

Externí část sítě bude v této fázi realizace tvořena pouze připojením na Internet. Detailní popis architektury připojení na Internet je uveden v kapitole 2.1.1.2.

V této kapitole se budeme zabývat pouze interní částí sítě. Logická topologie Interní sítě bude typu hvězda se středem, jenž bude realizován centrálním směrovačem. Na centrálním směrovači budou ukončeny jednotlivé logické segmenty VLANy. Použitý protokol IEEE 802.1Q umožňuje definovat až 4096 VLAN. V interní síti bude minimálně pět VLAN sítí, a to následující:

- VLAN 0 - Administrační VLAN pro aktivní prvky, v této VLAN budou všechny přepínače a centrální směrovač.
- VLAN 1 - Služební VLAN, která bude sloužit pouze pro připojení interního služebního serveru poskytujícího síťové služby pro interní síť (DNS, NTP, SMTP).
- VLAN2 - Management VLAN sloužící pro připojení serverů provádějících dohled a správu komunikační infrastruktury.
- VLAN3 až 99 - Tyto VLAN budou sloužit jako rezerva pro vytvoření dalších segmentů pro servery poskytující služby související s komunikační infrastrukturou.
- VLAN 100 až 199 - Tyto VLAN budou rezervovány pro připojení interních serverů - aplikační, souborové, adresářové atd.
- VLAN200 až 500 - Tyto VLAN budou sloužit k vytvoření segmentů pro koncové uživatele.

Výše uvedený způsob rozdělení a číslování VLAN nám poskytuje možnost již z čísla VLAN zjistit k čemu je určena a také je v návrhu dostatečná rezerva pro další rozvoj sítě.

Rozdělení uživatelů do logických segmentů je nejčastěji prováděno dle následujících metodik:

1. Rozdělení uživatelů podle jejich příslušnosti do určitého odboru či oddělení např oddělení infromatiky, účetnictvní, management apod. Toto rozdělení je v současné době nejpoužívanější a to především z důvodu bezpečnosti - lze definovat přesná pravidla komunikace mezi jednotlivými skupinami. Určitá nevýhoda může nastat v případě vyššího počtu přesunů uživatelů mezi jednotlivými odděleními, což je spojeno s vyššími nároky na administraci sítě.

2. Rozdělení uživatelů podle služeb, které budou uživatelé používat např skupina používající účetnický systém, skupina s přístupem na Internet apod. Nevýhoda tohoto způsobu rozdělení především spočívá především ve spojení různých nesouvisejících skupin uživatelů v jednom logickém segmentu (na jednom segmentu mohou být administrátoři a účetní).

Pro zařazení uživatelů do logických segmentů sítě doporučujeme použít první metodiku.

2.1.1.1.2 Fyzická vrstva

Fyzická vrstva se skládá z komunikačních linek a komunikačních rozhraní aktivních prvků, ke kterým jsou tyto linky připojeny. Aktivními prvky se pro účely tohoto projektu rozumí přepínače, případně směrovače. Komunikační linky budou realizovány pomocí kabelů UTP kategorie 6, fyzické zakončení bude provedeno konektory RJ45 nebo pomocí optických vláken v závislosti na vzdálenosti buď jako singlemode nebo multimode.

2.1.1.1.3 Linková vrstva

Linkovou vrstvou se rozumí komunikační protokoly zajišťující datovou komunikaci mezi sousedícími aktivními prvky, respektive mezi aktivními prvky připojenými k jednomu segmentu sdíleného media.Pro připojení koncových zařízení bude použito protokolu Ethernet nebo FastEthernet. V budoucnu bude možné připojit vysokokapacitní servery pomocí GigabitEthernetu.

Na všech přepínačích bude v případě redundantních tras aktivován Spanning Tree protokol, který zabraňuje tvorbě smyček v případech existence duplicitních spojů.

Celá síť bude rozdělena do několika VLAN segmentů podle protokolu IEEE 802.1Q. Koncepce jednotlivých VLAN není dosud ujasněna. Pracovně se počítá s členěním VLAN podle jednotlivých odborů, zvláštní VLAN pak bude vyhrazena serverům, jednací místnosti, zastupitelům, zvláštní VLAN bude vytvořen pro připojení k síti Internet, resp. propojení s ostatními sítěmi. Odhadované maximální množství VLAN, které je třeba vytvořit je cca 20. Navrhované prvky jsou schopny vytvářet daleko více VLANů a poskytují tak dostatečnou rezervu.

Členství v jednotlivých v VLANech bude defonováno na základě portů. Dynamické tvoření jednotlivých VLANů nebude používáno. Distribuce definice jednotlivých VLAN bude prováděna pomocí VTP domain protokolu verze 2. Tento protokol umožní definovat jednotlivé VLANy v centrální databázi pouze na jediném centrálním prvku, VTP protokol

potom zajistí distribuci této databáze do všech přepínačů v síti. VTP protokol také umožní distribuci případných změn (přidání, smazání VLAN) jednotlivým přepínačům v síti.

Komunikace mezi VLANy bude probíhat na třetí vrstvě ISO OSI modelu a bude tedy probíhat přes centrální směrovač.

2.1.1.1.4 Síťová vrstva

Lokální síť krajského úřadu řešena jako homogenní směrovaná datagramově orientovaná datová síť, využívající výhradně síťového protokolu IP verze 4 (Internet Protocol dle dokumentu IETF STD 5). Síť bude řešena tak, aby umožňovala plnou přímou IP konektivitu mezi sítěmi všech zúčastněných interních subjektů v rámci definovaných VLAN a řízenou konektivitu napříč VLANy.

2.1.1.1.5 Adresace.

Globální adresní plán

Adresní plán se bude sestávat ze dvou částí. První část bude interní adresní prostor pro potřeby interní sítě. Druhá část bude použita pro adresaci segmentů přímo přístupných z Internetu - externí DMZ, WWW DMZ, firewall atd. Adresace externích segmentů přímo připojených na Internet bude provedena registrovanými adresami oficiálně přidělenými poskytovatelem připojení do Internetu - adresace bude podrobněji rozepsána v kapitole 2.1.1.2.

Interní adresní prostor

V současné době je v síti KÚ používán adresní blok 192.168.0.0/24, což je 256 sítí třídy C o 256 adresách. Tento adresní prostor je v souladu se specifikací RFC 1918, tedy stejný adresní prostor jako byl použit v projektu OkuNet II a v souladu s doporučením projektu Třebíč. Protože dle pravidel adresace nelze použít nejnižší a nejvyšší síť třídy C z bloku 192.168.0.0/16 a ze sítě třídy C nelze opět použít nejvyšší a nejnižší adresu zbývá tedy celkem k dispozici 64516 adres. Tento adresní prostor je již v současnosti s části využit, konkrétně je využito prvních 16 sítí typu C. Pokud to bude možné, doporučujeme stávající stanice v nové sítí přeadresovat a adresní prostor rozdělit následujícím způsobem:

- První adresa třídy C, 192.168.0.0/24 bude nepoužita.
- Druhá adresa třídy C, 192.168.1.0/24 bude použita pro adresaci interních segmentů připojení na
- Třetí adresa třídy C , 192.168.2.0/24 bude využita na adresaci případných propojovacích segmentů mezi lokalitami KÚ. V současnosti takové segmenty neexistují a proto bude tato adresa nevyužita.

- Čtvrtá adresa třídy C, 192.168.3.0/24 bude využita pro adresaci loopback rozhraní směrovačů a pro adresaci přepínačů v administrativní VLAN segmentu.

- Blok adres 192.168.4.0/22 tj. čtyři adresy třídy C 192.168.4.0/24 - 192.168.7.0/24 bude sloužit jako rezerva pro adresaci aktivních prvků datových spojů a serverů adresaci segmentů

- Blok adres 192.168.8.0/21 tj osm adres třídy C 192.168.8.0/24 - 192.168.15.0/24 bude použito pro administrační či lépe řečeno management servery a serverové farmy.

- Zbývající adresy třídy C, 192.168.16.0/24 - 192.168.254.0/24 budou použity pro adresaci jednotlivých segmentů interní LAN sítě, tedy jednotlivých VLAN.

Pokud nebude možné provést přeadresaci sítě doporučujeme alespoň využít výše uvedený návrh tak že adresy sítí ve třetím oktetu zvýšíme o 16 tj místo adresy 192.169.1.0 bude 192.168.17.0.

Detailní adresace v následujících tabulkách kde je uveden rozpis adres přidělený aktivním prvkům (směrovačům a přepínačům) a přidělení bloků adres jednotlivým logickým segmentům sítě. Jelikož ze zřejmých důvodů nelze v tomto projektu uvést adresy všech stanic a serverů v sítí, uvedeme zde alespoň pravidla pro adresaci koncových zařízení v logických segmentech sítě. Pravidla vycházejí z typového projektu a jsou následující:

- V každé síti zůstane nevyužita první a poslední adresa, poněvadž první adresa je adresa sítě a druhá adresa je všesměrová tj. označuje všechny adresy v sítí.

- Směrovače budou mít v každé síti vždy nejnižší adresy a koncové („host“) části adres budou klesat směrem (ve smyslu počtu skoků) k centrálnímu internímu směrovači. Toto má význam především u spojů typu bod-bod resp. u segmentů Ethernetu, ke kterým jsou připojeny pouze dvě stanice (např. interní a externí propojovací segment), kde konce logicky blíže k centrálním interním směrovači mají nižší koncovou část adresy

- Přepínače budou adresovány dle obdobného pravidla, tj. přepínače budou mít nejnižší adresy a koncové („host“) části adres budou klesat směrem (ve smyslu počtu skoků) k centrálnímu přepínači. Bude li mít několik přepínačů stejný počet skoků k centrálnímu přepínači, budou rozděleny dle umístení (např. dle pater ve kterých jsou umístěny).

- Servery budou mít v každém segmentu nejnižší možné adresy bezprostředně vyšší než směrovače.

- Koncové stanice lze při dodržení předchozích podmínek adresovat libovolně

Tab. 1

Interní adresní prostor

Segmenty	Adresy sítí	Sumarizace
Spoj k firewallu	192.168.1.4/30	
Služební segment	192.168.1.8/29	
Propojovací segmenty	192.168.2.4/30 - 192.168.248/30	192.168.2.0/24
Loopback	192.168.3.1/32 - 192.168.3.254/32	192.168.3.0/24
Aktivní prvky	192.168.4.0/24 - 192.168.7.0/24	192.168.4.0/22
Serverové segmenty	192.168.8.0/24 - 192.168.15.0/24	192.168.8.0/21
Management Segment	192.168.8.16/28	
Proxy Segment	192.168.8.32/28	
Uživatelské segmenty	192.168.16.0/24 - 192.168.254.0/24	192.168.16.0/20 192.168.32.0/19 192.168.64.0/18 192.168.128.0/17

Tab. 2 Interní adresní prostor

Zařízení	Segment	Rozhraní	Adresa	Síťová maska
Centrální směrovač	softwarový loopback	loopback0	192.168.3.1	255.255.255.255
	spoj k firewallu	FastEthernet0/0.0	192.168.1.5	255.255.255.252
	služební segment	FastEthernet0/0.1	192.168.1.9	255.255.255.248
	management segment	FastEthernet0/0.2	192.168.8.17	255.255.255.240
	segment pro proxy server(y)	FastEthernet0/0.3	192.168.8.33	255.255.255.240
	serverová farma 2	FastEthernet0/0.4	192.168.9.1	255.255.255.0
	serverová farma 3	FastEthernet0/0.5	192.168.10.1	255.255.255.0
	serverová farma 16	FastEthernet0/0.6	192.168.15.1	255.255.255.0
	uživatelský segment 1	FastEthernet0/1.0	192.168.16.1	255.255.255.0
	uživatelský segment 2	FastEthernet0/1.1	192.168.17.1	255.255.255.0
	uživatelský segment 240	FastEthernet0/1.2	192.168.255.1	255.255.255.0
Služební server	služební segment	fxp0	192.168.1.10	255.255.255.248
Management server	management segment	fxp0	192.168.8.18	255.255.255.240
Proxy server	proxy segment	fxp0	192.169.8.34	255.255.255.240

Výše uvedený adresní plán poskytuje dostatek prostoru i pro případné rozšíření interní sítě.

2.1.1.1.6 Směrování

Směrování implementované v síti KÚ bude sloužit pro výměnu směrovacích informací protokolu IP, jež bude provozován na páteřní síti, interní síti a v externích částech sítí. Aby bylo směrování co nejefektivnější, musí především zajišťovat:

- konzistentní stav směrovacích informací v interních a externích směrovačích,
- stabilitu směrovacích údajů tak, aby byla zachována funkčnost sítě i při konečném počtu drobných poruch,
- dostupnost směrovacích informací všem sítím, které mají mezi sebou povolen přístup,
- výměnu vybraných směrovacích informací s externími systémy (Internet),
- filtraci všech nadbytečných informací tak, aby ve všech částech sítě byly dostupné pouze nezbytně nutné údaje.

Směrování v interní síti bude zajišťováno centrálním interním směrovačem gwi směrovačem. Jelikož je logická topologie interní sítě jednoduchá bude použito statických záznamů ve směrovací tabulkách.

2.1.1.2 Připojení k síti Internet

V současné době KÚ již disponuje připojením na Internet, které ale bohužel není především z hlediska bezpečnosti a možností rozšíření, vyhovující. Stávající připojení tedy bude nahrazeno připojením novým, které pouze využije již existující ISP a datový spoj na Internet. ISP pro KÚ je v současné době firma EuroWeb. Datový spoj na Internet je ralizován rádiovým spjem s rozhraním Ethernet. Námi navrhované připojení není ale závislé na konkrétním ISP a může využít služeb jakéhokoli ISP, jedinou podmínkou je v případě změny dovybavení externího směrovače příslušným rozhraním.

Připojení na Internet bude zajišťovat kontrolu komunikace mezi interní sítí. Připojení musí být navrženo tak ,aby minimalizoval možnost narušení bezpečnosti interní sítě. Při realizaci bude použito strukturální zabezpečení sítě využívající několik bezpečnostních vrstev.

Primárními cíli bezpečnostního bodu:

- zamezit neoprávněným přístupům do sítě,
- zamezit narušování chodu sítě (tzv. ‘denial of service attack’),
- zajistit bezpečný a řízený přístup uživatelů sítě k informačním zdrojům v Internetu,

- zajistit bezpečnou výměnu elektronické pošty mezi sítí KÚ a Internetem, případně s dalšími externími subjekty,
- zajistit bezpečný přístup k informacím, které KÚ hodlá veřejně poskytovat (např. veřejný WWW nebo FTP server),
- zajistit bezpečný přístup uživatelům Internetu k informačním zdrojům, které KÚ hodlá poskytovat,
- zajistit bezpečný přístup administrátorům sítě pro provádění vzdálené zprávy připojení a interní sítě.

2.1.1.2.1 Architektura připojení

Jak už bylo řečeno bude využito strukturované připojení, které se bude skládat z několika bezpečnostních přepážek, které budou realizovány externím směrovačem, firewallem a interním směrovačem.

Externí směrovač bude realizovat první bezpečnostní přepážku. K externímu směrovači bude připojen 24 portový přepínač Catalyst 3524, na kterém budou pomocí technologie VLAN vytvořeny následující segmenty:

- Propojovací segment na Internet
- ExtSeg1 - propojovací segment mezi externím směrovačem a firewallem,
- ExtSeg2 - segment pro připojení externího služebního serveru,
- ExtSeg3 - segment pro připojení externích www serverů.

Firewall bude realizovat druhou bezpečnostní přepážku. Firewall bude disponovat čtyřmi FastEthernet rozhraními, ke kterým budou připojeny následující segmenty:

- ExtSeg1,
- ExtSeg4 - segment pro možné připojení databázových serverů, jež budou spolupracovat s externími www servery,
- ExtSeg5 - jako rezerva možné budoucí připojení externích sítí,
- IntSeg1 - propojovací segment mezi firewallem a interním centrálním směrovačem gwi. (segment bude realizován pomocí přepínače a VLAN sítí).

Interní směrovač bude realizovat třetí bezpečnostní přepážku a bude realizován pomocí centrálního interního směrovače. K internímu směrovači budou připojeny následující segmenty:

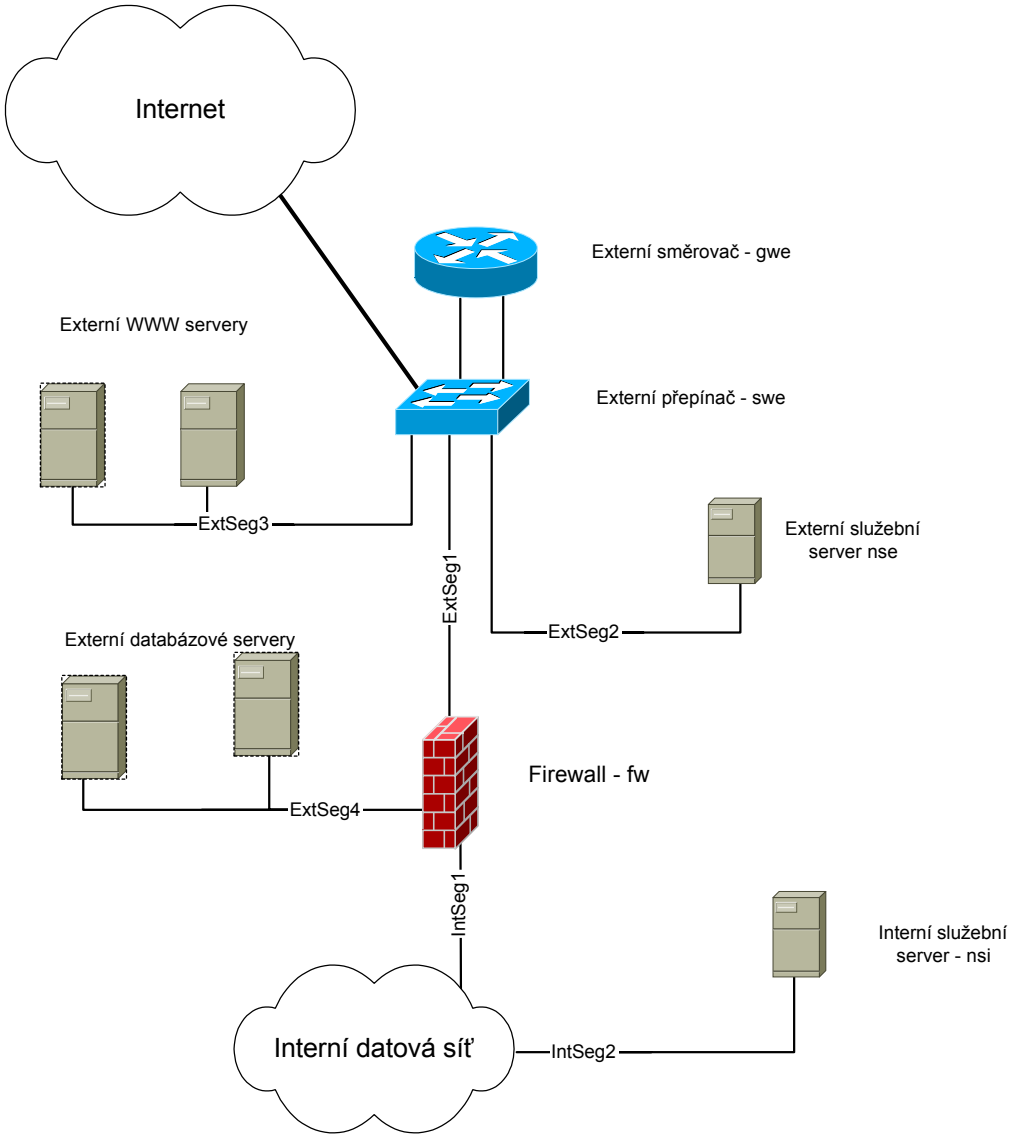
- IntSeg1,
- IntSeg2 - segment pro připojení interního služebního serveru,

- Ostatní segmenty interní datové sítě.

Architektura připojení na Internet je patrná z následujících obrázků znázorňujících fyzickou a logickou topologii.

Obr. 2

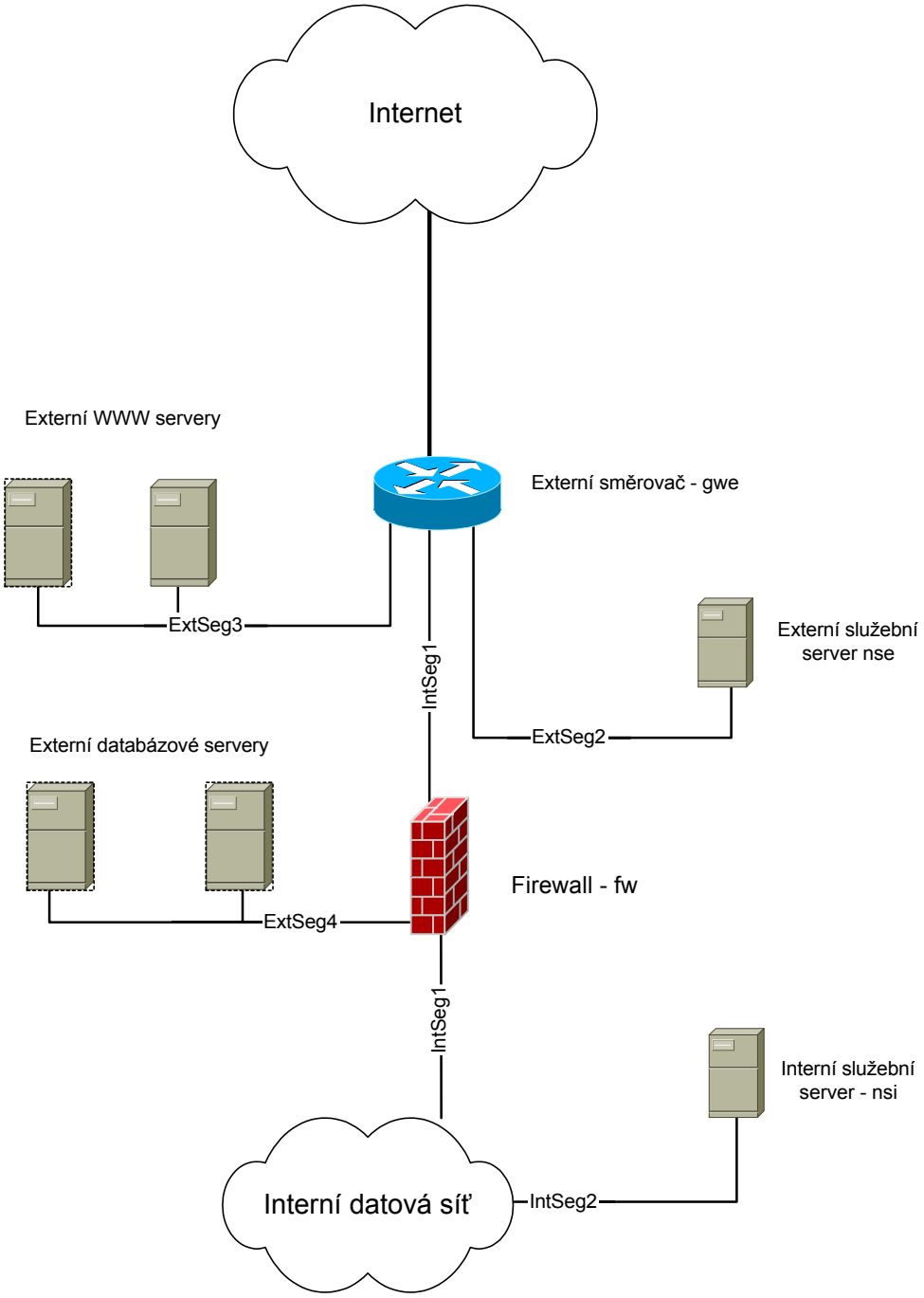
Fyzická topologie připojení na Internet



Prvky označené přerušovanou linkou nebudou realizovány v rámci první etapy.

Obr. 3

Logická topologie připojení na Internet



Prvky označené přerušovanou linkou nebudou realizovány v rámci první etapy.

2.1.1.2.1.1 *Připojení externích sítí*

Připojení externích sítí je koncepčně řešeno v typovém projektu. Pracovníci KÚ v této fázi nepožadují řešit v rámci realizačního projektu připojení externích sítí.

2.1.1.2.1.2 Adresace

Pro připojení požadováno od ISP blok o 64 adresách. Pro ilustraci budeme uvažovat o adresách v posledním oktetu 0 až 63, i když samozřejmě mohou být od ISP přiděleny bloky adres začínající adresami 64, 128 a 192, první tři oktety mohou být libovolné a označíme si je tedy REG_KU. Tento blok bude rozdělen následujícím způsobem:

- Subsíť REG_KU.0/30 tj. adresy REG_KU.0 - REG_KU.3 budou použity pro adresaci datového spoje na Internet
- Subsíť REG_KU.4/30 tj. adresy REG_KU.4 - REG_KU.7 budou použity pro adresaci segmentu ExtSeg1 který připojí firewall k externímu směrovači.
- Subsíť REG_KU.8/29 tj. adresy REG_KU.8 - REG_KU.15 budou použity pro adresaci segmentu ExtSeg2 který připojí externí služební server k externímu směrovači.
- Subsíť REG_KU.16/29 tj. adresy REG_KU.16 - REG_KU.23 budou použity pro adresaci segmentu ExtSeg3, ve kterém budou připojeny externí www servery
- Subsíť REG_KU.24/29 tj. adresy REG_KU.24 - REG_KU.31 budou použity pro adresaci segmentu ExtSeg4, ve kterém budou připojeny externí databázové servery
- Subsíť REG_KU.32/29 tj. adresy REG_KU.32 - REG_KU.39 budou použity pro statický překlad adres na firewallu.

Nevyužité adresy budou sloužit jako rezerva. Detailní adresní plán včetně adresace rozhraní jednotlivých zařízení je uveden v tab.X

Tab. 3

Zařízení	Segment	Rozhraní	Adresa	Síťová maska	DNS jméno
Externí směrovač	Přípoj na Internet	FastEthernet0/0.0	REG_KU.2	255.255.255.252	gwe gwe-fe000
	ExtSeg1	FastEthernet0/0.1	REG_KU.5	255.255.255.252	gwe-fe001
	ExtSeg2	FastEthernet0/1.0	REG_KU.9	255.255.255.248	gwe-fe010
	ExtSeg3	FastEthernet0/1.1	REG_KU.17	255.255.255.248	gwe-fe011
Externí služební server	ExtSeg2	fxp0	REG_KU.10	255.255.255.248	nse
Externí www server	ExtSeg3	fxp0	REG_KU.18	255.255.255.248	www.
Firewall	ExtSeg1	fxp0 (FastEthernet)	REG_KU.6	255.255.255.252	fw. fw-ext.
	ExtSeg4	fxp1 (FastEthernet)	REG_KU.25	255.255.255.248	fw-db.
Překlad adres - NAT	Statická adresa 1		REG_KU.33	255.255.255.255	hide1.
	Statická adresa 8		REG_KU.39	255.255.255.255	hide8.

2.1.1.2.2 Směrování

V lokalitách KÚ bude existovat pouze jediné připojení do Internetu a proto bude, z důvodů zajištění stability a bezpečnosti, použito statických směrovacích pravidel s využitím defaultních směrovacích údajů.

2.1.1.2.3 Překlad adres NAT

Vzhledem k použití privátních adres bez konektivity v síti Internet, je třeba definovat jakým způsobem budou počítače v interní části sítě KÚ komunikovat s počítači v síti Internet, tj. jakým způsobem bude docházet k sestavování spojení přes pomyslnou hranici tvořenou firewallem

Zprostředkování komunikace bude realizováno prostřednictvím firewallu. Toto zařízení zajišťuje službu překladu adres (NAT) ve smyslu RFC 1631. V našem případě bude prováděn překlad adres ve směru do Internetu. Překlad adres bude prováděn dle následujících pravidel.

- Primárně bude prováděn dynamický překlad adres N:1, tj. všechny adresy interní sítě budou přeložena na registrovanou adresu rozhraní firewallu, které bude připojeno do segmentu ExtSeg1.
- Bude-li nutné některým interním stanicím přidělit pevnou/neměnnou registrovanou adresu, bude použit překlad adres 1:1, registrovaná adresa bude vybrána ze subsítě REG_KU.32/29.

2.1.1.2.4 Firewall

Firewall bude dke požadavků pracovníků KÚ realizován na hardwarové platformě INTEL s operačním systémem FreeBSD 4.x. Tento systém je k dispozici zcela zdarma. Systém FreeBSD nabízí vysokou robustnost a odolnost proti možným bezpečnostním útokům. Součástí tohoto systému je mimo jiné podpora IP protokolu verze 6, podpora standardu IPSec s podporou šifrovacích algoritmů DES56 , 3DES, blowfish, CAST. Dále je podporována filtrace IP paketů. Systém pro filtraci paketů umožňuje u protokolů TCP/UDP/ICMP rozlišit, jedná-li se o již navázané spojení, nebo je-li spojení inicializováno

Pro obraznost je v příslušných kapitolách uvedena také varianta s využitím komerčního firewallu PIX firmy CISCO systems.

Nejdůležitější součástí firewallu je jeho bezpečnostní politika, které povoluje nebo zakazuje přístup skrz firewall. Zde uvedeme pouze základní nastavení pravidel bezpečnostní politiky, konkrétnější nastavení vyplyne až z požadavků uživatelů v KÚ. Přístup do Internetu pomocí protokolu HTTP , FTP a Ghopher bude povoleno pouze z interního proxy cache serveru, jehož popis je uveden v kapitole 2.1.1.2.5.4.

Základní pravidla budou vyházet z pravidla „co není explicitně povoleno je zakázáno“, budou také respektována pravidla řízení provozu uvedené v kap 2.1.1.3.2., pro jistotu si tato pravidla zopakujeme.

Obecná pravidla bezpečnostní politiky:

- zamezit falšování zdrojových adres,
- zamezit šíření broadcastových (resp. poškozených) paketů mimo logické segmenty lokálních sítí,
- řídit přístup k službám v interní síti, ,
- zamezit jakýmkoli pokusů o narušení bezpečnosti interní sítě,
- směrem do Internetu a externích sítí povolit pouze z předem definovaných IP adres.

Pravidla pro přístup z Internetu do interní sítě:

- z externího služebního serveru bude povolen protokol SMTP a IDENT pouze na interní služební server,
- z Internetu bude povolen protokol SSH na interní služební server (tato služba bude povolena jen v případě vzdálené administrace připojení nebo interní sítě),
- ostatní služby nebo protokoly budou zakázány.

Pravidla pro přístup z interní sítě na Internet:

- z proxy cache serveru budou povoleny protokoly HTTP, FTP a Ghoper ,
- z interního služebního serveru budou povoleny protokoly DNS, SMTP a IDENT na externí služební server,
- Povolení dalších služeb z interní sítě závisí na odpovědných pracovnících KÚ a bude řešeno až v testovacím provozu,

2.1.1.2.5 Síťové služby

Dle požadavků zadavatele budou síťové služby řešeny pouze ve vztahu k připojení k Internetu. V podstatě se jedná pouze o koncepci bezpečné realizace systému jmenných služeb , systému elektronické pošty mezi interní sítí a Internetem dále pak o koncepci synchronizace času a tzv. proxy cache služeb. Nyní si popíšeme koncepci řešení jednotlivých služeb.

Všechny zde jmenované síťové služby budou implementovány nad operačním systémem FreeBSD, který je svou stabilitou a výkonem v oblasti síťových služeb z našeho pohledu nejvhodnější.

2.1.1.2.5.1 Jmenné služby

Systém doménových jmen DNS (Domain Name System - dle STD 13 a RFC 1035) je jednou ze základních služeb v každé IP síti. DNS poskytuje službu mapování symbolických (doménových jmen) na číselné IP adresy (tzv. dopředná rezoluce) a opačně (tzv. reverzní rezoluce). Tato služba významně zjednodušuje užívání všech síťových služeb koncovým uživatelům a taktéž zjednodušuje administraci sítě a řady jiných síťových služeb

Cílem jmenného plánu je zajistit konzistentní pojmenovávání zařízení tak, aby jména byla dostatečně mnemotechnická a podporovala primární poslání DNS, tedy zjednodušení užívání síťových služeb.

Připojení na Internet bude používat domény druhé úrovně pod doménou **cz** a to **kr-vysocina.cz**. Tato doména bude oficiálně registrována v NIC. Jmenný plán dodržuje následující pravidla:

- Každá IP adresa v síti má svoje jméno v DNS (jméno bude tedy přiděleno každému rozhraní směrovače).
- Jména jsou volena tak, aby pokud možno naznačovala poslání zařízení, ke kterému se vztahují a zároveň byla krátká.
- Jména směrovačů začínají řetězcem **gw** (z anglického gateway - brána).
- Jména serverů DNS začínají řetězcem **ns** (z anglického name server).
- Mapování mezi jmény a adresami nemusí být jednoznačné, tedy jednomu jménu může odpovídat více adres (to se typicky týká směrovačů, které mají několik adres).
- Mapování mezi adresami a jmény musí být jednoznačné, tedy každé adrese odpovídá právě jedno jméno (tak, aby z adresy bylo možné, např. pro účely monitorování, jednoznačně určit doménové jméno zařízení).

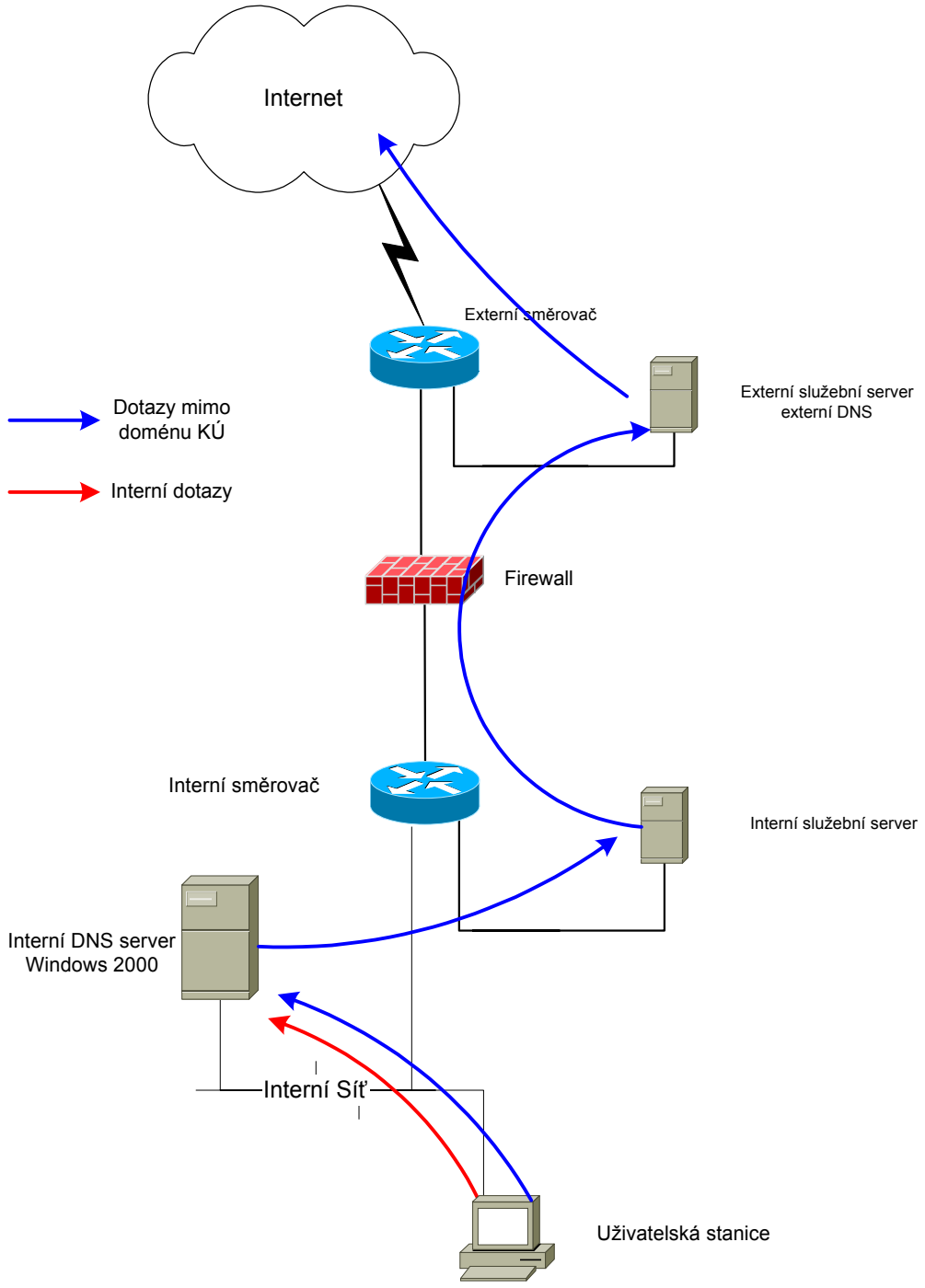
V rámci připojení na Internet bude implementovaný tzv. duální systém DNS skládající se z externí a interní části. Mezi oběma částmi bude existovat jednosměrná vazba a to tak, že interní systém se bude moci pro rezoluce jmen z domén mimo jeho vlastní dotazovat systému externího. Externí systém se však nebude moci interního systému dotazovat na nic. Interní systém bude zkonfigurovaný jako oddělený systém s vlastním tzv. kořenovým serverem. Externí DNS bude standardně, prostřednictvím delegací, napojen do DNS v Internetu. Interní DNS servery (pokud jich interní síti bude více) budou propojeny do stromové struktury prostřednictvím explicitně zkonfigurovaných adres zprostředkovatelů (anglicky „forwarder“).

Cílem této konfigurace je maximální zefektivnění fungování celého systému prostřednictvím využívání cachovacích schopností jednotlivých serverů. Předpokladem pro dosažení efektivního fungování je i správná konfigurace zařízení, která systém využívají. U nich bude nezbytné, aby se pro DNS rezoluce odkazovala vždy na svůj nejbližší server. Jednosměrné propojení mezi externí a interní částí DNS bude implementováno taktéž pomocí explicitní konfigurace adresy zprostředkovatele. Požadavky z interní části sítě na rezoluci jmen resp. adres mimo domény obsluhované jejími servery budou předávány externímu serveru, který

je (standardním mechanizmem rekurze dotazů) předá dále do Internetu. Odpovědi z Internetu budou předávány zpět po stejné cestě (viz obr).

Obr. 4

Systém rezoluce doménových jmen



Externí část DNS bude realizována na externím služebním serveru, interní část na interním služebním serveru, případně na jiném interním serveru.

Všechny DNS služby budou implementovány volně šířeným softwarem BIND (Berkeley Internet Name Daemon) nejnovější verze. Tento software je považován za de facto standard implementace obsluhy DNS

2.1.1.2.5.2 Elektronická pošta

Pro realizaci systému výměny elektronické pošty mezi interní sítí a Internetem bude použit protokol SMTP (Simple Mail Transport Protocol - dle RFC 1157) respektive jeho rozšíření varianty ESMTP (Extended Simple Mail Transport Protocol). Tento protokol je zdaleka nejrozšířenějším protokolem pro přenos zpráv elektronické pošty na světě a to především díky svému zcela výlučnému postavení v Internetu, kde je používán jako standardní a de facto jediný protokol pro tento účel.

Systém elektronické pošty se bude sestávat z následujících komponent:

- Externí poštovní server, který bude realizován externím služebním serverem umístěným v externím DMZ segment ExtSeg2 (viz)
- Interní poštovní server, který bude realizován interním služebním serverem umístěným na separátním interním segmentu IntSeg2 ()
- Centrální interní server, který bude realizován na samostatném serveru situovaném na serverovém segmentu uvnitř interní sítě.

Uživatelé v interní síti budou výhradně komunikovat s centrálním interním serverem.

Výměna zpráv elektronické pošty s Internetem bude probíhat následovně:

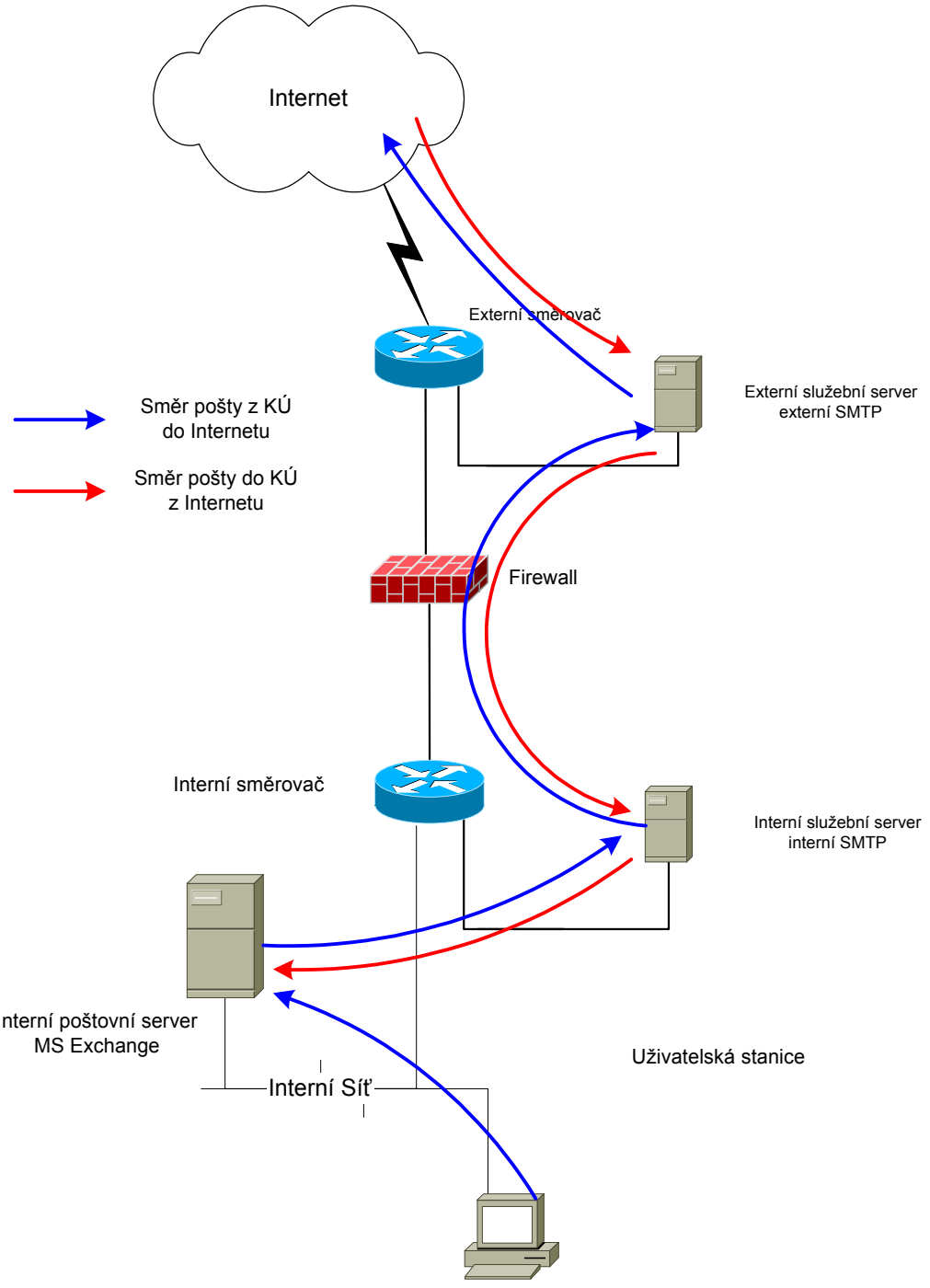
1. Lokální server nebo klient elektronické pošty v interní síti KÚ předá zprávu protokolem SMTP nebo jiným protokolem centrálnímu internímu serveru.
2. Centrální interní server předá, již pouze protokolem SMTP, zprávu internímu poštovnímu serveru.
3. Interní poštovní server na základě cílové adresy, informací v DNS a své konfigurace určí server, kterému má být zpráva předána.
4. Externí centrální server na základě informací v (externím) DNS určí server, kterému má být zpráva předána a prostřednictvím protokolu SMTP mu ji předá.

Postup při doručování zpráv z externích sítí do interní části LAN sítě bude probíhat v opačném pořadí. Všechny příchozí zprávy tedy budou nejprve přijaty externím serverem elektronické pošty (na základě informací v DNS), který zaručí jejich další předání do interní sítě. Externí server elektronické pošty bude zároveň zaručovat nemožnost jeho zneužití pro předávání zpráv elektronické pošty, které ani nepocházejí z interní sítě a ani do ní nejsou adresovány. Bude na něm zároveň možné implementovat i opatření omezující šíření

nevyžádané elektronické pošty do interní sítě. V počáteční konfiguraci však tato opatření nebudou aktivována. Způsob doručování pošty je vyobrazen na následujícím obr.

Obr. 5

Systém výměny elektronické pošty z Internetem



V každém kroku v tomto procesu dochází k ověřování oprávněnosti odesílatele předávat zprávy adresované na dotyčnou cílovou adresu, kontroluje se formát cílových adres a dochází k ukládání předávané zprávy na lokálním disku dotyčného serveru. V případě, že zprávu nelze odeslat dále, například z důvodu nefunkčnosti cílového serveru, jsou pokusy o její doručení periodicky opakovány s exponenciálně se prodlužujícími intervaly mezi jednotlivými pokusy až do vypršení konfigurovatelné maximální doby pro doručení (v základním nastavení 4 dny). V případě, že se opakovaně zprávu nedaří doručovat, je její odesílatel o této skutečnosti informován. Intervaly, po kterých je informován, je možné konfigurovat a v základním nastavení budou:

- první informace po 4 hodinách,
- druhá po 1 dni,
- třetí po 2 dnech,
- čtvrtá a poslední po 4 dnech, informující o ukončení pokusů o doručení.

V těchto intervalech je o neúspěších v doručování informován i správce systému. Potvrzování úspěšného doručení zprávy do schránky adresáta je věcí koncového serveru.

Služby SMTP serveru budou zajištěny softwarem PostFix. Poštovní server PostFix svou koncepcí zajišťuje v současné době nejbezpečnější způsob realizace poštovní komunikace. Oproti stávajícímu qmailu nebo sendmailu obsahuje programové prvky, které maximálně snižují riziko využití serveru pro útok na operační systém. Server PostFix bude nainstalován ve nejnovější verzi s všemi dostupnými opravami

2.1.1.2.5.3 Synchronizace času

Správně synchronizovaný čas na všech aktivních prvcích a serverech sítě je nezbytně nutnou podmínkou zejména pro dohled a správu sítě a systémů. Velice významnou oblast vyžadující přesnou a spolehlivou synchronizaci času tvoří celá bezpečnostní infrastruktura implementující globální bezpečnostní politiku sítě. Správnou synchronizaci času všech systémů vyžadují především následujících oblastech:

- protokoly zabezpečující oprávněnost přístupu (autentizaci a autorizaci) k síťovým zdrojům striktně vyžadují synchronizaci času,
- monitorování, analýza a řešení případných bezpečnostních incidentů potřebuje mít k dispozici záznamy s platnými časovými údaji,
- analýza řešení funkčních problému a závad v síti i v rámci jednotlivých systémů potřebuje mít na všech systémech stejný časový údaj.

Hierarchie časových serverů

Časové synchronizační servery implementované v síti KÚ budou pro synchronizaci času využívat hierarchické stromové struktury. Pro získání přesného času budou použity časové servery v Internetu. Hierarchická struktura bude následující:

- Na nejvyšší hierarchické úrovni bude časový server v Internetu.
- Na druhé úrovni bude firewall.
- Na třetí úrovni budou externí služební server a interní služební server.
- Na čtvrté úrovni budou všechny aktivní prvky (vyjma externího směrovače), servery a koncové stanice připojené v externí nebo interní části sítě KÚ.

Synchronizační servery budou navzájem spolupracovat podle modelu klient/server a to tak, že synchronizační server(y) dané hierarchické úrovně bude zároveň nakonfigurován jako klient úrovně vyšší. Uvedená struktura umožní minimalizovat jak režijní datové přenosy nezbytné pro vlastní synchronizaci, tak i případné problémy spojené s výpadkem nebo úmyslným narušením funkčnosti synchronizačního serveru

Celá hierarchická struktura je tedy navržena tak, aby umožňovala efektivní synchronizaci času v rámci celé sítě KÚ.

Implementace časové synchronizace

Synchronizace času bude implementována pomocí protokolu NTP (Network Time Protocol) verze 2 (resp. 3) specifikovaného v doporučeních IETF RFC 1119 (NTP V2) a RFC 1305 (NTP V3). Protokol umožňuje praktickou synchronizaci času v řádu milisekund (ms). Protokol NTP využívá pouze základní vlastnosti sady protokolů UDP/IP a nemá žádné speciální požadavky na komunikační médium, šířku přenosového pásma, kvalitu služeb apod.

Protokol NTP je široce rozšířen a jeho implementace je dostupná ve formě volně šiřitelných zdrojových textů v rámci Internetu pro prakticky všechny typy moderních operačních systémů. Řada výrobců implementuje tento protokol i jako integrální součást jimi dodávaného OS (např. Cisco IOS).

Pro dostupnost a zabezpečení časových serverů platí v zásadě následující pravidla:

- Server nejvyšší úrovně bude synchronizován se dvěma servery poskytujícími oficiálně synchronizační služby na Internetu. Servery budou vybrány podle jejich optimální aktuální dostupnosti.
- Všechny servery budou implementovat protokol NTP V3 (preferovaně), ale i V2 pro zajištění vzájemné kompatibility.
- Určené servery budou poskytovat synchronizační služby volně pro klienty na dané hierarchické úrovni.

Servery budou využívat pro vzájemnou synchronizaci mezi jednotlivými úrovněmi autentizované komunikace zabezpečené tajnými klíči (vždy jeden klíč pro komunikaci mezi dvěma úrovněmi) hashovanými funkcí MD5

2.1.1.2.5.4 Proxy služby

Proxy služby budou realizovány v počáteční fázi pouze u protokolů HTTP, FTP a Gopher. Proxy cache služby budou realizovány na separátním serveru určeným pouze pro tyto účely. Hlavní účely nasazení proxy služeb jsou následující:

- zvýšení výkonu (služba ukládá do cache objekty, které jsou při vícenásobném přístupu uživatelů na stejné webové stránky poskytnuty z cache, čímž dojde k ušetření přenosového pásma přípojky na Internet),
- filtrace obsahu (zákaz přístupu zaměstnanců na určité WWW stránky atd.),
- logování přístupů (statistiky přístupů k jednotlivým stránkám , atd.),
- autentizace autorizace uživatelů (ve spolupráci s využitím adresářových služeb).

Realizaci serveru zajišťující proxy služby bude provedena pomocí otevřených systémů tedy nad OS FreeBSD.. Z našeho pohledu nejvýhodnější programové vybavení je volně šiřitelný program (tj. včetně všech zdrojových kódů) SQUID, který má všechny požadované funkce.

2.1.1.3 Bezpečnost

V této kapitole uvedeme technická opatření vedoucí k co možná nelepšímu zabezpečení interní LAN sítě. Technickými opatřeními k zabezpečení sítě rozumíme bezpečnostní funkce implementované v aktivních prvcích sítě a jejich konfiguraci. Základní bezpečnostní opatření budou sloužit k zajištění:

- ochrany interních částí sítě před útoky z externích sítí,
- ochrany aktivních prvků sítě.
- ochrany uživatelských stanic patřících do různých logických segmentů sítě,
- ochrany interních serverů před možnými útoky z interní sítě.

Aktivní prvky sítě však budou umožňovat i implementaci restriktivnějších opatření, přesná pravidla budou definována bezpečnostní politikou.

2.1.1.3.1 Klasifikace uživatelů, autentizace a autorizace

Klasifikace uživatelů a systémů musí být provedena v rámci bezpečnostní politiky a proto zde nebude diskutována. Uvedeme zde pouze mechanismy jenž budou použity pro autentizaci autorizaci a účtování.

Metody autentizace, autorizace a účtování využívané aktivními prvky sítě do značné míry závisí na možnostech instalovaných operačních systémů a na metodě přístupu k nim. Předpokládáme využití následujících metod:

- Centrální autentizace a autorizace s využitím systému TACACS+ (Terminal Access Controller Access Control System), což je systém centralizované autentizace a autorizace původně vyvinutý pro ministerstvo obrany USA a později převzatý a rozšířený firmou Cisco Systems (verze plus). TACACS+ bude použit pro autentizaci přístupu ke všem směrovačům a pro přechod do privilegovaného uživatelského režimu (enable). Jako autentizační metodu bude TACACS+ využívat systém jednorázových hesel S/Key. Systém TACACS+ bude taktéž použit k centrálnímu zaznamenávání všech uživatelských akcí vykonávaných na směrovačích. Systém TACACS+ je volně dostupný včetně zdorjových kódů a je implementován na většině operačních systémů.

- Lokální autentizace jednorázovými hesly systému S/Key pro přístupy k systémové konzoli služebních serverům.

- Kryptografická autentizace metodou výzva odpověď využívající šifru DSA s délkou klíče 1024 bitů pro vzdálený přístup prostřednictvím klienta Open Secure Shell (OpenSSH).

- Autorizace uživatelských akcí na služebních serverech bude řízená přístupovými právy v OS. Zaznamenávání uživatelských akcí bude obdobně prováděno lokálně s využitím účtování (accounting).

2.1.1.3.2 Řízení provozu sítě

Základní technické prostředky pro zabezpečení provozu sítě se budou skládat především z nastavení pravidel filtrace IP paketů na všech směrovačích a nastavení bezpečnostní politiky na firewallech.

Filtrace IP paketů ve směrovačích bude základní bezpečnostní funkcí v páteřní síti. Na všech páteřních směrovačích (centrální a VPN směrovače) zkonfigurovány přístupové seznamy (access-list implementující filtraci paketů). Cílem základní filtrace paketů v rámci páteřní sítě bude především:

- zamezit falšování zdrojových adres,

- zamezit šíření broadcastových (resp. poškozených) paketů mimo logické segmenty lokálních sítí,

- řídit přístup k službám na směrovačích, ,

- řídit přístup k službám na interních serverech

- řídit vzájemnou komunikaci mezi jednotlivými logickými segmenty sítě,

- napomáhat detekci chybně konfigurovaných zařízení v síti.

Přístupové seznamy budou taktéž zabezpečovat přístup z Internetu. Cílem filtrace paketů z/do Internetu bude:

- omezit přístup pouze na protokoly zajišťující provoz virtuálních spojů.

Cílem nastavení pravidel bezpečnostní politiky firewallu v centrálním uzlu bude především:

- řídit přístup k službám poskytovaných sítí KÚ,
- řídit přístup k služebním serverům pro možnou vzdálenou správu sítě.

Všechny pakety zakázané filtry budou zaznamenávány kromě výjimek, kdy by toto způsobovalo neúměrný nárůst záznamových souborů.

2.1.1.3.2.1 Nastavení Ethernetových rozhraní na směrovačích

Všechna rozhraní směrovačů připojení jsou typu IEEE 802.3 (Ethernet). Všechny LAN porty směrovačů budou konfigurovány následovně:

- Enkapsulace IP datagramů do rámců Ethernet II podle IETF STD 0041 (resp. RFC 894).
- Bude použit protokol ARP podle IETF STD 0037 (resp. RFC 826).
- MTU sítě bude 1500 oktetů.
- Vysílání ICMP redirect bude potlačeno.
- Vysílání ICMP unreachable bude povoleno.
- Vysílání ICMP mask reply bude zakázáno.
- Přenos všech směrovacích protokolů do koncové sítě bude potlačen.
- Directed broadcast bude potlačen.
- Na rozhraní se nebude používat IP multicast.
- Přenos UDP broadcast do dalších sítí bude potlačen
- Cisco Discovery Protocol bude potlačen.
- Gateway Discovery Protocol bude potlačen.
- Veškeré pokusy o porušení bezpečnostních filtrů budou účtovány.
- Budou nastaveny vstupní i výstupní filtry pro IP datagramy (IP extended Access List – ACL).
- Kromě níže uvedených nastavení filtrů budou filtry zajišťovat ochranu proti útoku IP spoof.
- Rozhraní nebude používat překlad adres.

- Rozhraní nebude používat administrativně nastavenou směrovací politiku (policy based routing).

2.1.1.3.2.2 Nastavení filtračních pravidel na externím směrovači

Jedním z důležitých bezpečnostních prvků sítě připojení je správné nastavení filtrů pro IP datagramy na všech rozhraních všech směrovačů. Smyslem filtrů je sloužit jako primární nebo záložní ochranný mechanismus, který chrání účastníky sítě před napadením ze sítě Internet přes externí část připojení. IP filtry současně zamezují provádění útoků směrem ven do sítě Internet a slouží k řízení komunikace mezi jednotlivými zónami připojení.

Pro každý směrovač předpokládáme na každém rozhraní konfiguraci dvou filtrů: jednoho vstupního, který filtruje datagramy přicházející přes toto rozhraní do směrovače, a druhého výstupního, který filtruje IP datagramy vysílané směrovačem směrem ven z tohoto rozhraní.

V případě, že filtry nepovolují průchod určitých datagramů, bude se provádět jednak účtování takovýchto paketů (tj. na úrovni celého směrovače se udržuje tabulka zdrojových a cílových IP adres, pro které došlo k porušení filtrů spolu s celkových počtem porušení – tato tabulka slouží pro rychlou orientaci. Dále se pro každé pravidlo každého filtru udržuje počet, kolikrát pravidlo uspělo (tj. v případě pravidel zakazujících průchod datagramu se eviduje počet porušení tohoto pravidla). Dále se pro každý zakázaný datagram posílá zpět na odesílatele chybový datagram ICMP Unreachable s příčinou administrativního omezení komunikace.

Všechny filtry mají pravidla závislá na pořadí a vyhodnocují se shora dolů tj. první pravidlo, které odpovídá procházejícímu datagramu, je konečné a rozhodne o propuštění nebo zastavení tohoto datagramu. Proto musí být více specifická pravidla před pravidly obecnými. Dále musí být více používaná pravidla pokud možno co nejvíce na začátku filtrů, aby došlo na jejich vyhodnocování co nejdříve (tím se zvyšuje rychlost výpočtu filtrů a tím i zpracování datagramů).

2.1.1.3.2.2.1 Vstupní filtr rozhraní k ISP

Externí směrovač jako první odolává útokům ze sítě Internet. Jeho filtry zajišťují utajení topologie připojení před různými druhy scanů. Vstupní filtr rozhraní k ISP musí především chránit směrovač. Samotné řízení toku dat do jednotlivých zón bude realizováno na příslušných rozhraních. Za tímto účelem bude nastaven vstupní filtr takto:

- Zakazuje všechnu komunikaci na adresy externího směrovače.
- Zakazuje IP datagramy s privátními adresami dle RFC 1918.
- Vše ostatní je povoleno.

2.1.1.3.2.2.2 Výstupní filtr rozhraní k ISP

Zakazuje IP datagramy s privátními adresami dle RFC 1918 a povoluje všechnu komunikaci.

2.1.1.3.2.2.3 *Výstupní filtr DMZ rozhraní*

Filtr řídí komunikaci proudící do externí DMZ kde je umístěn externí služební server, který plní funkci externího poštovního a jmenného serveru. Filtr bude nastaven takto:

- Povoluje již TCP navázaná komunikace.
- Povoluje SMTP komunikaci odkudkoliv na služební server.
- Povoluje NTP komunikaci z firewallu na služební server.
- Povoluje SSH komunikace z firewallu na služební server.
- Povoluje HTTP a HTTPS komunikaci odkudkoliv na www server.
- Povoluje návratovou komunikaci WWWOut reflex.
- Povoluje TCP DNS komunikace z externího sekundárního DNS serveru na služební server.
- Povoluje IDENT komunikace odkudkoliv na služební server.
- Povoluje UDP DNS komunikace odkudkoliv na služební server.
- Povoluje ICMP ECHO REQUEST z externího sekundárního DNS serveru na služební server.
- Vše ostatní je zakázáno.

2.1.1.3.2.2.4 *Vstupní filtr DMZ rozhraní*

Vstupní filtr DMZ rozhraní řídí komunikaci proudící z DMZ a musí zamezit šíření útoku z DMZ. Tento filtr bude nastaven následovně:

- Povoluje již navázanou TCP komunikaci.
- Povoluje UDP DNS komunikaci ze služebního serveru kamkoliv.
- Povoluje SMTP komunikaci ze služebního serveru kamkoliv.
- Povoluje SSH komunikaci na externí služební server z vybraných adres.
- Povoluje IDENT komunikaci ze služebního serveru kamkoliv.
- Povoluje NTP komunikaci ze služebního serveru na firewall.
- Vše ostatní je zakázáno.

2.1.1.3.2.2.5 *Vstupní filtr tranzitního rozhraní*

Tento filtr řídí komunikaci proudící z externí tranzitní sítě. Jeho primární bezpečnostní funkce je chránit interní směrovač před útokem z vnitřní sítě a pořizovat tabulku spojení pro tvorbu dynamických (reflexivních) aceslistů, které budou aplikovány na zpětnou komunikaci. Filtr bude vypadat následovně:

- Povoluje již sestavená TCP spojení.
- Povoluje NTP komunikaci z firewallu na www a služební server.
- Povoluje TELNET z firewallu na externí směrovač.
- Zakazuje vše na externí směrovač.
- Povoluje sestavení TCP spojení z firewallu kamkoliv.
- Povoluje všechnu UDP komunikaci z firewallu kamkoliv.
- Povoluje všechnu ICMP komunikaci z firewallu kamkoliv.

2.1.1.3.2.2.6 *Výstupní filtr tranzitního rozhraní*

Výstupní filtr tranzitního rozhraní řídí komunikaci proudící do tranzitní sítě a tedy do interní části připojení. Z tohoto důvodu je nutná opatrnost při jeho nastavování. Filtr je navržen tak, aby propouštěl jen komunikaci jasně definovanou, nebo vyžádanou počítači z vnitřní sítě. Pravidla filtru jsou následující:

- Povoluje již sestavená TCP spojení.
- Povoluje NTP komunikaci z www a služebního serveru na firewall.
- Povoluje SMTP ze služebního serveru na firewall.
- Povoluje IDENT ze služebního serveru na firewall.
- Povoluje sestavení SSH spojení z externího služebního serveru na firewall.
- Povoluje návratové pakety TRANZOut reflex.
- Vše ostatní zakazuje a loguje.

2.1.1.3.2.3 Nastavení filtračních pravidel na interním směrovači

2.1.1.3.2.3.1 *Vstupní filtr pro interní datovou síť*

Cílem tohoto filtru je především ochrana před neúmyslným nebo úmyslným narušením integrity sítě ze strany koncových uživatelů připojených do této LAN. Vzhledem k tomu, že

v typickém provozu sítě LAN posílají koncové počítače jen krátké požadavky, zatímco přijímají relativně dlouhé odpovědi, je prováděno filtrování případného pokusu o použití protokolů NetBIOS na vstupní a nikoliv výstupní straně. Tento filtr bude mít následující pravidla (použitá v uvedeném pořadí):

- Zakazuje a protokoluje všechny pakety ICMP redirect.
- Zakazuje a protokoluje všechny pakety směřující na rozhraní směrovače.
- Zakazuje a protokoluje všechny pakety s rozsahem TCP a UDP portů 137 až 139 (jak zdrojové, tak cílové).
- Povoluje všechny pakety se zdrojovou adresou z dané koncové sítě.
- Povoluje TCP spojení z interního služebního serveru na interní mailer.
- Zakazuje a protokoluje všechny ostatní pakety.

2.1.1.3.2.3.2 Výstupní filtr pro interní datovou síť

Cílem výstupního filtru interní datové sítě je propustit pouze takové pakety, které odpovídají podporovaným službám sítě pro koncové počítače. Zvláštní pozornost je věnována ochraně některých známých chyb v prohlížečích WWW, které se snaží sestavovat odchozí spojení pomocí protokolu SMB (Server Message Block, protokol pro sdílení souborů v operačních systémech společnosti Microsoft). Dále uvedený filtr předpokládá využití pasivního klienta FTP na straně koncových počítačů. Nastavení filtru je následující:

- Povoluje všechny TCP segmenty, které patří k již sestaveným spojením.
- Povoluje všechny UDP datagramy dle reflexivní tabulky.
- Zakazuje a protokoluje pakety ICMP redirect.
- Povoluje všechny ICMP pakety.
- Zakazuje a protokoluje všechny ostatní IP pakety.

2.1.1.3.2.3.3 Vstupní filtr pro interní DMZ

Smyslem vstupního filtru je ochránit integritu sítě před instalací neautorizovaných počítačů v interní DMZ a před neautorizovaným použitím služebních počítačů. Hlavní filtraci provádí nikoliv vstupní, ale výstupní filtr služební LAN. Konfigurace filtru bude následující:

- Zakazuje a protokoluje datagramy ICMP redirect.
- Povoluje TCP segmenty pro všechna již sestavená TCP spojení pouze pro níže definované služby.
- Povoluje příchozí TCP spojení pro SSH jen ze služebního serveru.

- Povoluje sestavení TCP spojení pro službu SMTP pouze ze služebního serveru na interní poštovní server a na firewall.
- Povoluje UDP datagramy služby DNS pouze ze služebního serveru.
- Povoluje UDP datagramy služby NTP pouze ze služebního serveru.
- Povoluje UDP datagramy služby TFTP pouze ze služebního serveru na směrovač příslužné lokality.
- Zakazuje a protokoluje všechny ostatní IP pakety.

2.1.1.3.2.3.4 Výstupní filtr pro interní DMZ

Výstupní filtr pro interní DMZ tvoří jednu z hlavních součástí ochrany služebních serverů před útokem ze zbytku sítě. Výstupní filtr pro interní DMZ propouští pouze takové IP datagramy, které přesně odpovídají předem definované množině služeb, které jsou na služebních serverech dostupné. Všechny ostatní pakety jsou zakázány a protokolovány. Konfigurace filtru pro interní DMZ s jediným služebním serverem bude následující:

- Povoluje TCP segmenty pro všechna již sestavená TCP spojení.
- Povoluje příchozí TCP spojení pro následující službu SSH jen z administrátorské stanice a firewallu.
- Povoluje sestavení příchozího TCP spojení pro službu SMTP pouze z předem specifikovaných serverů (interní SMTP server a firewall).
- Povoluje UDP datagramy na port DNS, TCP datagramy na port DNS pouze ze sekundárního DNS.
- Povoluje UDP datagramy na port NTP, syslog jen ze směrovačů.
- Zakazuje všechny ostatní datagramy.

2.1.1.3.2.3.5 Vstupní a výstupní filtry pro interní tranzitní síť

Komunikace mezi zónami bude řízena filtry na rozhraních náležících do daných zón. Filtr aplikovaný na tomto rozhraní:

- Povoluje všechnu komunikaci z/do interní datové sítě,
- Povoluje veškerou komunikaci z/do interní DMZ.
- Povoluje komunikaci z firewallu na interní směrovač.
- Povoluje všechnu komunikaci z firewallu na interní služební servery.

2.1.1.3.3 Nastavení pravidel na firewallu

Při vstupu z externího směrovače jsou implementována tato základní pravidla :

- povolení předem navázaných TCP spojení,
- povolení NTP/UDP a DNS/UDP odpovědí,
- Povolení DNS UDP z vnitřního DNS serveru na externí DNS server,
- povolení SMTP z externího mail serveru na interní mail serveru a naopak,
- povolení SSH z/na vybrané počítače,
- povolení *http* a *https* provozu do DMZ,
- povolení některých ICMP zpráv (*destination-unreachable, time-exceeded, parameter-problem, echo-reply*),
- povolení *pingu* (icmp *echo-request*) z vybraných adres na firewall,
- explicitní zákaz provozu, který nechceme logovat (IP multicasty),
- zákaz a logování všeho ostatního.

Při výstupu do Internetu jsou implementována tato základní pravidla :

- povolení paketů z vnější adresy firewallu a z adresního rozsahu DMZ,
- zákaz a logování všeho ostatního.

Při výstupu do Internetu jsou implementována tato základní pravidla :

- povolení veškerého provozu (který projde předchozími pravidly z Internetu).

Při forwardování paketů mezi rozhraními jsou implementována tato základní pravidla :

- překlad adres pro vybrané počítače ve vnitřní síti, které mohou přímo přistupovat ven,
- zákaz a logování všeho ostatního.

2.1.1.3.4 Bezpečnostní monitorování provozu sítě

Monitorování či sledování sítě s ohledem na bezpečnost je velice významným prostředkem pro zajištění bezpečnosti sítě, jehož součástí jsou následující činnosti:

- monitorování pokusů o průnik přes bezpečnostní pravidla (především se jedná o pakety zakázané ve filtrech na směrovačích a pakety zakázané bezpečnostní politikou firewallu),

- sledování uživatelských přístupů k jednotlivým systémům sítě (směrovače, přepínače, služební servery a firewally) a sledování vykonávaných úkonů v rámci systému na základě záznamů ze systému TACACS+ a účtovacího systému serverů,
- sledování odchylek od typické komunikační zátěže v síti,
- sledování provozního stavu aktivních prvků (zejména start, vypnutí, výpadek rozhraní apod.),
- pravidelná kontrola integrity operačních systémů použitých aktivních prvků,
- vyhodnocování hlášení správců sítí zúčastněných KÚ o anomálním chování jimi spravovaných systémů (to předpokládá zřízení zvláštního informačního kanálu pro tyto účely).

2.1.1.4 Správa sítě

Nedílnou, a neméně důležitou, částí každé sítě je systém umožňující provádět efektivní a účinný dohled na síť a správu sítě. Dobrá organizace správy sítě má vliv i na efektivní využívání přenosových cest a aktivních prvků. Informace získané v rámci správy sítě taktéž představují základní zdroj informací v případě rozhodování o budoucím rozvoji sítě. Pracovníci KÚ dávají přednost produktu LinkAnalyse nebo volně šiřitelným produktům.

Systém správy sítě musí především zajišťovat:

- monitorování všech aktivních prvků a přenosových tras, včetně zakreslení do příslušného schématu,
- okamžité hlášení výpadku: rozhraní, přenosové trasy, systému
- automatický sběr a uchovávání účtovacích záznamů ze všech systémů sítě (směrovače, přepínače, firewally atd.)
- zálohování konfigurací aktivních prvků,
- nástroje pro provádění automatického upgrade a update softwarového vybavení

Požadavky, jenž zde byly uvedeny, lze zajistit nasazením management serveru vybaveného buď komerčním produktem jako jsou například OpenView, CiscoWorks apod. nebo volně šiřitelné nástroje jako např. Netsuite, TKIned, Mrtg a další. Rozdíly mezi komerčními a tzv free produkty jsou následující:

Požadavky, jenž zde byly uvedeny, lze zajistit nasazením management serveru vybaveného buď komerčním produktem jako jsou například OpenView, CiscoWorks apod. nebo volně šiřitelné nástroje jako např. Netsuite, TKIned, Mrtg a další. Rozdíly mezi komerčními a tzv. free produkty jsou následující:

- Výhoda komerčních produktů je v šíři implementovaných nástrojů umožňujících snadnou správu i poměrně velkých sítí, velice často podporují přímo nejvíce používané platformy (CISCO, 3COM, HP, Sun, Nortel Networks apod). Pro tyto produkty existuje podpora přímo od výrobce. Nevýhodou je především poměrně velká investiční a provozní cena. Investiční náklady zvyšuje již fakt, že většina těchto systémů podporuje pouze serverové platformy SUN, HP a IBM. Provozní cena je zvýšena placením podpory produktu a samozřejmě také placením nezbytných upgrade.

- Při konzultacích bylo diskutováno použití produktu LinkAnalyst. Tento produkt je možné použít, avšak nezajišťuje výrazně větší funkčnost, než použití volně šiřitelných produktů. Síť KÚ však, dle našeho názoru, v současné době s ohledem na její složitost nevyžaduje použití složitých sofistikovaných produktů tohoto typu. Minimální požadavky HW konfiguraci serverové části: Pentium 300 MHz, 32MB RAM, myš, color VGA monitor (1024x768), podpora protokolů Winsock-compliant TCP/IP, IPX nebo NetBEUI. Základní funkce produktu jsou:

  - Provádí monitorování stavu důležitých síťových prvků s možnosti upozornění na případný výpadek.

  - Mapování sítě a následné grafické zobrazení.

  - Zaznamenávání dat pro následnou analýzu.

  - WWW rozhraní pro zaznamenaná data.

- Výhodou nekomerčních tzv free produktů je nulová pořizovací cena a cena za případné upgrade. Dále je možné tyto produkty provozovat nad free operačních systémech typu FreeBSD, OpenBSD, NetBSD a Linux (tyto operační systémy podporují jak platformy INTEL tak napr Alpha a další). Nekomerční produkty jsou ve většině případů šířeny formou Open Source (tedy včetně zdorjových kódů) a je tedy snadné do těchto produktů dodělat potřebné specifické funkce. Poslední výhoda je také částečně nevýhodou poněvadž u těchto produktů je nutné některé potřebné funkce (v komerčních produktech obsažené) dodělat. Pro tyto produkty vetšinou neexistuje podpora tak jak ji známe u produktů komerčních. Nekomerční produkty nejsou vhodné při nasazení v rozsáhlých sítích.

Síť KÚ není nijak rozsáhlá, a proto bude v této fázi realizace výhodnější použít některý z nekomerčních produktů. Bude-li v průběhu provozu sítě zjištěno, že dohledový systém založený na těchto produktech je nedostačující, bude nutné v průběhu dalších fází informatizace krajských úřadů nasadit jeden z komerčních produktů. Provozování nekomerčního systému nám umožní lépe specifikovat požadavky na systém nový.

Pro samotnou správu sítě budou dohledovým systémem a administrátory využívány následující prostředky:

- vzdálený terminálový přístup k aktivním,

- ICMP protokol,
- vzdálené spouštění příkazů protokoly SSH a RSH,
- sběr informací z aktivních prvků prostřednictvím protokolu SNMP verze 1 (Simple Network Monitoring Protocol - dle RFC 1157),
- asynchronní hlášení předávaná protokolem SNMP (SNMP trapy),
- automatizované analýzy záznamových souborů s předáváním výsledků prostřednictvím elektronické pošty,
- centrálním zaznamenáváním běhových událostí v reálném čase prostřednictvím protokolu syslog.

2.1.1.5 Integrace hlasových služeb

V rámci sítě KuNet lze hlasové služby především využít jednak pro propojení k telefonních ústředen jednotlivých KÚ a také na propojení telefonních ústředen externích subjektů v rámci každého kraje. Integraci hlasových služeb lze v budoucnu realizovat na vpn směrovači, jehož technické parametry budou dimenzovány tak aby jej bylo možno v budoucnu snadno dovybavit příslušnými hlasovými moduly

Pro realizaci hlasových služeb nad vhodnou datovou sítí je nejvhodnější využít technologii přenosu hlasu pomocí protokolu IP tzv. VoIP (Voice over IP). Tato technologie umožňuje jednak samotný přenos hlasu protokolem IP a dále přenos nezbytné signalizace mezi zúčastněnými prvky, což jsou: směrovače, telefonní stanice, digitální/analogové telefonní ústředny, tzv. IP telefony a také určité programové vybavení na PC stanicích. Aby bylo při přenosu hlasu docíleno co možná nejmenších nároků na kapacitu sítě, budou využity kompresní protokoly.

V rámci VoIP budou použity následující protokoly:

- ITU-T standard H.323 pro přenos hlasu protokolem IP,
- SIP,
- oproti standardnímu kódovacímu protokolu G.711 (pro přenos hlasu je potřeba64kbps datového pásma) používanému v standardních telefonních sítích bude použit protokol G.729 (pro přenos hlasu je potřeba minimálně 8kbps optimálně však okolo 14 až 18kbps).

Přenos hlasu pomocí datových sítích je náročný na zpoždění a kapacitu datových spojů a v neposlední řadě na investice do nezbytných zařízení. Z těchto důvodů nedoporučujeme nasazení této technologie v první fázi informatizace KÚ. Případnou vlastní implementaci integrace hlasových služeb doporučujeme řešit až v dalších etapách procesu informatizace KÚ (složitost, časová náročnost, optimalizace nasazení zdrojů).

V rámci interní sítě lze navíc hlasové služby integrovat na úrovni koncových telefonních přístrojů. Využití tzv. IP telefonů (jedná se o telefonní přístroje využívající pro přenos hlasu

přímo lokální datovou síť,) a hlasové brány umožní převod hlasu mezi IP telefony a standardními telefonními přístroji. Jak již ale bylo řečeno, konkrétní implementaci integrace hlasových služeb v rámci datové sítě doporučujeme řešit až v dalších etapách procesu informatizace.

2.1.1.6 Možnosti rozšíření

Možnosti dalšího rozšíření lokální sítě můžeme rozdělit do následujících oblastí:

- rozšíření kapacity sítě co do počtu připojených stanic a serverů a také co do kapacity sítě.
- připojení dalších externích subjektů
- rozšíření sítě s ohledem na spolehlivost
- zavedení nových technologií

Rozšíření kapacity sítě je plně závislé na současném stavu datových spojů (metalických i optických) a na rozšiřitelnosti aktivních prvků jež budou v dané lokální síti k dispozici. V rámci všech realizačních projektů bude uvedeno několik možností nasazení aktivních prvků právě s ohledem na jejich další rozšíření. Samozřejmě že výběr vhodných aktivních prvků bude také ovlivněn finanční situací jednotlivých KÚ.

Připojení dalších externích subjektů bude realizováno pomocí vpn směrovače

Rozšíření sítě s ohledem na spolehlivost se týká především zdvojení klíčových systémů sítě jako jsou např. centrální směrovač a přepínač. Koncepce návrhu lokální sítě počítá s tímto způsobem rozšíření sítě. Je zřejmé, že zvýšení spolehlivosti není pouze záležitostí spolehlivosti jednotlivých zařízení a kvality návrhu sítě, ale je též ovlivněna kvalitou správy sítě. Správnou a kvalitní správu sítě lze docílit jednak nasazením správných produktů, ale také samotnými administrátory sítě. Proto doporučujeme v testovacím provozu bedlivě sledovat kvalitu správy sítě a v případě, že nebude vyhovující, tak buď najmout odpovídající odborníky na správu sítě nebo správu sítě přenechat externímu dodavateli, který disponuje potřebnými prostředky pro kvalitní správu sítě.

Koncepce návrhu sítě je navržena tak aby do ní bylo možné implementovat nejnovější technologie, jež zvýší kvalitu služeb poskytovaných komunikační infrastrukturou. Z nových technologií si uveďme alespoň ty které jsou z našeho pohledu nejaktuálnější:

- přenos hlasu po datové síti - technologie VoIP (Voice over IP),
- implementace řízení kvality služeb tzv. QoS (Quality of Services),
- zavedení dynamických VLAN,
- integraci komunikační infrastruktury do PKI - Public Key Infrastructure (využití PKI při autentizaci a autorizaci systémů a uživatelů). PKI především usnadní nasazení technologie IPSec a IKE.

- využití adresářových služeb při autentizaci a autorizaci uživatelů.

2.1.2 Subsystém bezpečnostní infrastruktury

V typovém projektu základní informatizace krajských úřadů byla náplň realizačních projektů bezpečnostní infrastruktury omezena (v rámci této úvodní etapy) na problematiku síťové bezpečnosti která je v tomto realizačním projektu řešena v rámci kapitoly komunikační infrastruktury.

2.1.2.1 Antivirová ochrana

Pro antivirovou ochranu systému navrhujeme, na základě požadavku informatiků KÚ, použití produktů firmy Symantec: Norton Antivirus pro desktopy a servery vč. exchange serveru, Norton Antivirus for Gateways a antivirový modul nástroje Symantec Web Security. Je pravděpodobné uzavření smlouvy o GPL licenci pro všechny krajské úřady. Tato smlouva by platila i pro organizace řízené a zřizované krajským úřadem, a to na všechny produkty Symantec. Bude-li smlouva podepsána je nutné upravit ceny uvedené v tabulce dodávaného softwaru. Je nutné zajistit licenci pro 300 uživatelů.

2.1.3 Subsystém integrační platformy

Předpokládá se maximální využití průmyslových a zejména internetových standardů:

- hardwarová platforma Intel,
- operační systémy Linux, FreeBSD, Windows 2000/XP. Vzájemná komunikace a integrace se předpokládá pomocí internetových protokolů (TCP/IP, SMTP, HTTP, LDAP ...),
- pro služební servery komunikační infrastruktury se preferuje platforma LINUX, resp. FreeBSD,
- pro ostatní servery je preferována platforma Windows 2000/XP,
- správa uživatelů s využitím Active Directory

Po dohodě se zadavatelem bude referenční rozhraní v podobě služeb VSS implementováno na KÚ až v druhé etapě informatizace na základě pilotních projektů realizovaných na MHMP.

2.1.4 Subsystém provozních činností

Návrhy na použití konkrétních aplikací, uvedené dále v projektu, vycházejí z posouzení variant navrhovaných zástupci KÚ s uvážením kladů a záporů jednotlivých variant i stanoviska většiny zástupců KÚ.

2.1.4.1 Kancelářský systém

Na základě požadavků krajských úřadů je jako kancelářský systém pro koncové uživatele navrhována platforma Microsoft Office a poštovní klient Microsoft Outlook.

Jako základní kancelářský software navrhujeme MS Office XP Czech, verze Standard, pro každý KÚ pak 10x verze Professional, 1x verze Developer. Hlavními důvody jsou opět možnost správy těchto aplikací pomocí Active Directory a také široká podpora ze strany dodavatelů ekonomických a kancelářských programových balíků.

Výhodami MS Outlook je kvalitní uživatelské rozhraní a dobrá integrace s poštovním systémem MS Exchange. S tím opět souvisí široká podpora ze strany dodavatelů ekonomických a kancelářských programových balíků.

2.1.4.2 Systém oběhu dokumentů včetně spisové služby

Podpora práce s písemnostmi bude realizována systémem GINIS-SSL (Gordic). Systém řídí a sleduje tok informací v úřadě (v elektronické i papírové formě), zabezpečuje identifikaci všech dokumentů, jednoznačnou odpovědnost pracovníků a podporuje řídící činnosti. Systém pracuje v třívrstvé architektuře s jednou centrální databází, standardně obsahuje moduly administrace, universálního spisového uzlu, podatelny, výpravny, spisovny, kartotéky, modul úkolů a usnesení. Navrhujeme využití standardního úložiště dokumentů fy Gordic. V této etapě informatizace KÚ nepočítáme s využitím úložiště dokumentů FileNET Panagon, jelikož kombinace GINIS-SSL/FileNET je, pokud je nám známo, teprve ve stádiu vývoje a nebyla dosud v žádné organizaci nasazena.

Předpokládáme 50 uživatelů tohoto systému.

Realizace podpory workflow není v rámci základní informatizace vyžadována.

2.1.4.3 Ekonomický systém

Na podporu provozních ekonomických a účetních činností je zvolen po konsultaci se zodpovědnými pracovníky KÚ informační systém GINIS-EKO dodávaný firmou Gordic, spol. s .r.o. Jihlava. Systém pracuje v architektuře klient-server a využívá centrální relační databází s dotazovacím jazykem SQL. GINIS - EKO je speciálně navržen pro potřeby orgánů veřejné správy, průběžně zohledňuje legislativní změny a je nasazen v celé řadě rozpočtových pracovišť. Sestava standardně obsahuje moduly pro práci s rozpočtem, vedení účetní agendy, pokladnu, komunikaci s bankou, evidenci majetku a administrační modul. KÚ požaduje zakoupení těchto modulů: AMD, EKO, EMA a INT.

Předpokládáme 20 uživatelů tohoto systému.

2.1.4.4 Personální systém

Systémy pro řízení personalistiky a zpracování mezd musí umožňovat práci až s 300 pracovníky evidovanými v jedné organizaci, předpokládaný počet uživatelů je 5.

Navrhujeme dle požadavku KÚ systém FLUXPAM 5 (Flux, s.r.o.), určený pro střední a velké organizace. Systém představuje komplexní řešení mzdové problematiky včetně možnosti spolupráce s některými ekonomickými balíky (mj. od firem PVT, Gordic), s evidencí docházky aj. FLUXPAM 5 je 32 bitová aplikace, schopná pracovat v síťovém i nesíťovém provozu a s různými typy databází.

V druhé etapě informatizace bude na personální systém kladen v rámci „dobré integrovatelnosti" dodatečný požadavek na implementaci služeb (poskytovaných přes referenční rozhraní nebo protokol LDAP) pro spolupráci se systémem integrované správy uživatelů, tj. se systémem aplikačně a platformově nezávislé správy uživatelů jako služby bezpečnostní infrastruktury. Dodavatel aplikace bude muset mimo jiné garantovat dodržení standardu ISVS pro informační systémy v oblasti personální a platové (v časovém limitu stanoveném zákonem 365/2000 Sb.).

2.1.4.5 Programové vybavení pro tvorbu WWW stránek

V rámci typového projektu je navrhován systém VISMO z důvodu nízké ceny a rozšíření ve státní správě. Na platformě Linux/Apache je pak možné využít některé z řady free software řešení. Pro vlastní tvorbu stránek navrhujeme Frontpage (dodáván v rámci Office), jinak např. Visual Studio.

Dle požadavku informatiků KÚ navrhujeme doplnit programem Corel Draw 9.0 (3 licence).

V rámci etapy základní informatizace krajských úřadů nejsou na tento typ programového vybavení kladeny žádné explicitní integrační požadavky.

2.1.4.6 Systém právních informací

Je doporučován systém právních informací ASPI s licencí typu LAN (file/server) s minimálně měsíční aktualizací. Tato licence umožňuje připojit libovolný počet uživatelů v rámci jednoho subjektu.

Systém ASPI je založen na původní české technologii zpracování velkých objemů textu a je faktickým standardem i ve státní správě ČR.

2.1.4.7 Geografický informační systém

Dle požadavku KÚ navrhujeme zakoupeni komponenty systému ESRI: ArcInfo, ArcIMS, 4x ArcView,a dále mapová díla v hodnotě 100.000 Kč.

2.1.5 Subsystém statutárních činností

Po dohodě se zadavatelem nebude dodávka software pro statutární činnosti řešena v první etapě informatizace KÚ.

2.2 Specifikace hardware a software

2.2.1 Hardware pro interní síť

V současné době nelze přesně navrhnou aktivní prvky interní sítě, jelikož není známa fyzické infrastruktura. Z těchto v tomto případě doporučujeme ústní konzultaci až po vybudování komunikační infrastruktury.

V rámci přerozdělení finančních prostředků na informatizaci krajů je s těmito prvky počítáno přičemž množství peněz na aktivní prvky byly určeny hrubým odhadem.

2.2.2 Hardware pro připojení na Internet

2.2.2.1 Externí směrovač - Cisco 2621

Směrovač Cisco 2621 v základní konfiguraci disponuje dvěma rozhraními typu FastEthernet, dvěma WIC sloty pro WAN rozhraní a jedním slotem pro síťový modul.. Hardwarová konfigurace směrovače je uvedena v následující tabulce

Tab. 4 Externí směrovač

Přepínač	Modul	Počet	Popis
Cisco 2621	CISCO2621	1	šasi, zdroj, pamět, procesor , 2X FastEthernet, software

2.2.2.2 Externí přepínač - Catalyst 3524

Catalyst 3512 XL, 3524XL, a 3548 XL jsou produkty ze série Catalyst 3500 firmy Cisco Systems. Tyto přepínače nabízejí výkon o rychlosti až 8 milionů paketů za sekundu a jsou ideální pro vytváření vysokovýkonných lokálních sítí. Pro větší užitek lze tyto přepínače stohovat pomocí gigabitových ethernetových rozhraní. Navíc v sobě tyto produkty obsahují podporu pro IP telefonii a hlasové služby.

Catalyst 3524 XL má 24 ethernetových 10/100 přepínaných portů a dva GBIC porty..

Všechny přepínače série Catalyst 3500XL podporují služby QoS (quality of service) založené na standardu IEEE 802.1p stejně tak jako podporují prioritizaci jednotlivých portů. Každý z těchto přepínačů podporuje technologii VLAN založenou na standardech 802.1Q a ISL. Technologie VLAN Spanning Tree (PVST+) umožňuje využívat mnohonásobná propojení jednotlivých VLAN segmentů. Každý port může být zabezpečen pomocí technologie MAC (Media access control), která zabrání komunikaci neautorizovaným stanicím. Podpora technologie TACACS+ umožňuje snadnější správu přístupu k těmto prvkům přes centrální databázi a brání neautorizovaným uživatelům v provádění zásahů do konfigurace.

Tab. 5 Externí přepínač

Přepínač	Modul	Počet	Popis
Cisco Catalyst 3524	WS-C3524-XL-EN	1	šasi, zdroj, pamět, procesor, rozhraní 24x FatEhernet, 2X Gigabit Ethernet

2.2.2.3 Externí/interní služební server

Tab. 6 oporučená konfigurace služebních serverů

Model	PC - AT
Skříň	Rack mount + 2x HotSwap Zdroje
Základní deska	ABIT SL6 (chipset intel 815, 1xAGP, 6xPCI, 1xAMR)
Procesor	Intel Pentium 3 600 Mhz
Paměť	256MB SDRAM PC133
SCSI Raid řadič	Adaptec 2100R
Pevný disk	3 x 9GB SCSI Ultar160 IBM 10000ot , HotSwap
Video adaptér	onboard
Sériové porty	onboard 2 x
Síťová karta	Intel EtherExpress Pro 10/100B

Tab. 7 Minimální konfigurace služebních serverů

Model	PC - AT
Skříň	AT Desktop
Základní deska	ABIT SL6 (chipset intel 815, 1xAGP, 6xPCI, 1xAMR)
Procesor	Intel Celeron 600 Mhz
Paměť	128MB SDRAM PC133
SCSI Raid řadič	Adaptec 29160Single (SCSI Ultra160)
Pevný disk	9GB SCSI Ultra160
Video adaptér	onboard
Sériové porty	onboard 2 x
Síťová karta	Intel EtherExpress Pro 10/100B

2.2.2.4 Firewall

2.2.2.4.1 Freeware FreeBSD

Tab. 8 Hardwarová konfigurace firewallů

Model	PC - AT
Skříň	Rack mount + 2x HotSwap Zdroje, možnost hot swap disků
Základní deska	ABIT SL6 (chipset intel 815, 1xAGP, 6xPCI, 1xAMR)
Procesor	Intel Pentium 3 600 Mhz
Paměť	256MB SDRAM PC133
SCSI Raid řadič	Adaptec 2100R
Pevný disk	3 x 9GB SCSI Ultar160 IBM 10000ot , HotSwap
Video adaptér	onboard
Sériové porty	onboard 2 x
Síťová karta	čtyř portová síťová karta - NetLux D-Link DFE570TX FastEthernet

Tab. 9 Hardwarová konfigurace firewallů

Model	PC - AT
Skříň	AT Desktop
Základní deska	ABIT SL6 (chipset intel 815, 1xAGP, 6xPCI, 1xAMR)
Procesor	Intel Celeron 600 Mhz
Paměť	128MB SDRAM PC133
SCSI Raid řadič	Adaptec 29160Single (SCSI Ultra160)
Pevný disk	9GB SCSI Ultra160
Video adaptér	onboard
Sériové porty	onboard 2 x
Síťová karta	čtyř portová síťová karta - NetLux D-Link DFE570TX FastEthernet

2.2.2.4.2 PIX Firewal

Cisco Secure PIX firewall je hardwarový firewall z produktových řad firmy Cisco systems. Zaručuje vysoký stupeň zabezpečení při zachování velkého výkonu. S nárůstem Internetu se zvyšuje nárůst bezpečnostních rizik. Existující řešení mají velmi mnoho omezení: malý výkon, problémy s bezpečností operačních systémů, cena a atd. Cisco Secure PIX Firewall netrpí žádným z předchozích nedostatků.

Klíčové vlastnosti:

- Bezpečný operační systém, který není založen na bázi Unixu a pracuje v reálném čase. Tento systém eliminuje rizika spojené s používání jiných systémů a navíc nabízí výborný výkon až 256000 současných připojení.
- Adaptive Security Algorithm (ASA). Srdcem Cisco Secure PIX firewallu je ASA, který je podstatně komplexnější a robustnější než běžný paketový filtr. Také zaručuje vyšší výkon a škálovatelnost než aplikační-proxy firewally. ASA bezpečně odděluje připojené sítě díky své vnitřní koncepci, která je zaměřená na rozlišování jednotlivých datových toků. Veškerý příchozí a odchozí provoz je kontrolován pomocí nastavené bezpečnostní politiky.

- Autentizace a autorizace uživatelů pomocí mechanizmu Cut-Through Proxy. Cisco Secure PIX Firewall nabízí unikátní technologii Cut-Through Proxy pro transparentní ověřování identity uživatelů a povolování nebo zakazování jejich tcp nebo udp konexi. Tato metoda autentizační a autorizační služby je založena na CiscoSecure Access Control Server.

- Jednoduchá instalace a programové prostředky, které zrychlují proces počátečního nastavení.

- Centralizovaná administrace. PIX Firewall Manager je Java-based GUI konfigurační nástroj umožňující administrátorům jedním kliknutím zobrazit, upravit a centrálně administrovat bezpečnostní politiky. Tento nástroj také poskytuje přístup k vnitřním statistikám. Dále generuje upozornění na neobvyklé situace a je schopen je poslat administrátorovi mailem nebo na pager.

- Standardní VPN. Podpora VPN je založena na IPsec a IKE, bez problémů spolupracuje s ostatními výrobky firmy Cisco a obsahuje klienty pro MS Win NT 4.0 a MS Win 95. VPN umožňuje mobilním uživatelům plný a bezpečný přístup do vnitřní sítě pře Internet jako přenosové medium.

- Filtrování URL. PIX firewall poskytuje možnost filtrování URL s NetPartners WebSENSE server software. PIX zkontroluje odchozí požadavky na URL oproti bezpečnostním pravidlům definovaným ve WebSENSE. Podle těchto pravidel buď zamítne nebo povolí spojení.

- Failover. Vlastnost PIX Firewall failover nabízí vysokou dostupnost (high availability) a eliminuje následky poruchy. Princip této možnosti je založen na použití dvou PIX Firewallů běžících paralelně, když jeden selže druhý automaticky přebere bezpečnostní operace.

Tab. 10 HW konfigurace PIX firewallu, počet 1

Typ směrovače	Popis
PIX Firewall 515.	šasi, zdroj, procesor 200MHz, 64MB paměti, rack mountable, 2 x základní rozhraní 10/100 + 4 další, unrestricted software, VPN klienti s DES kryptováním jsou v ceně.

2.2.2.5 Proxy server

Tab. 11 Hardwarová konfigurace firewallů

Model	PC - AT
Skříň	Rack mount + 2x HotSwap Zdroje
Základní deska	ABIT SL6 (chipset intel 815, 1xAGP, 6xPCI, 1xAMR)
Procesor	Intel Pentium 3 600 Mhz
Paměť	512MB SDRAM PC133
SCSI Raid řadič	Adaptec 2100R
Pevný disk	3 x 20GB SCSI Ultar160 IBM 10000ot , HotSwap
Video adaptér	onboard
Sériové porty	onboard 2 x
Síťová karta	Intel EtherExpress Pro 10/100B

Tab. 12 Hardwarová konfigurace firewallů

Model	PC - AT
Skříň	Rack mount + 2x HotSwap Zdroje
Základní deska	ABIT SL6 (chipset intel 815, 1xAGP, 6xPCI, 1xAMR)
Procesor	Intel Pentium 3 600 Mhz
Paměť	512MB SDRAM PC133
SCSI Raid řadič	Adaptec 2100R
Pevný disk	3 x 20GB SCSI Ultar160 IBM 10000ot , HotSwap
Video adaptér	onboard
Sériové porty	onboard 2 x
Síťová karta	Intel EtherExpress Pro 10/100B

2.2.3 FreeBSD OS

Tento systém je k dispozici zcela zdarma. Systém FreeBSD je postaven na bázi UNIXových systémů BSD, nabízí vysokou robustnost a odolnost proti možným bezpečnostním útokům. Součástí tohoto systému je mimo jiné podpora IP protokolu verze 6, podpora standardu IPSec s podporou šifrovacích algoritmů DES56, 3DES, blowfish, CAST. Dále je podporována filtrace IP paketů. Systém pro filtraci paketů umožňuje u protokolů TCP/UDP/ICMP rozlišit, jedná-li se o již navázané spojení, nebo je-li spojení inicializováno. Součástí systému je C a C++ kompilátor a všechny ostatní programy běžné v systémech UNIX např, telnet, ssh, login, atd. Systém je dodáván včetně všech zdrojových kódů.

2.2.4 MTA

Služby SMTP serveru budou zajištěny softwarem PostFix. Poštovní server PostFix svou koncepcí zajišťuje v současné době nejbezpečnější způsob realizace poštovní komunikace. Oproti stávajícímu qmailu nebo sendmailu obsahuje programové prvky, které maximálně snižují riziko využití serveru pro útok na operační systém. Server PostFix bude nainstalován ve verzi 20010228 Patchlevel 01 s všemi dostupnými opravami.

2.2.5 DNS

Všechny DNS služby budou implementovány volně šířeným softwarem BIND (Berkeley Internet Name Daemon) verze 9.x.x. Tento software je považován za de facto standard implementace obsluhy DNS

2.2.6 Proxy

Služby proxy serveru budou zajištěny volně šiřitelným produktem SQUID, který bude provozován nad OS FreeBSD. V současné době se jedná o jeden z nejpoužívanějších produktů na platformně OS typu Unix. Vyznačuje se stabilitou, robustností a vysokým stupněm bezpečnosti.

2.2.7 PIX OS

PIX je licencován bude licencován jako Unrestricted. Kryptování pro VPN je počítáno s DES. V případě požadavků na 3DES je nezbytné dokoupit licenci.

2.2.8 LinkAnalyst

LinkAnalyst je produkt nad operačním systémem Windows, který nabízí základní monitorovací funkce síťě, jejich vizualizaci a archivování dat o stavu sítě. Jedná se o produkt levnější cenové kategorie, který nabízí základní funkce a není vhodný k řízení rozsáhlejších a složitějších sítí. Funkčně je obdobný volně šiřitelným produktům, z hlediska uživatelského komfortu nabízí uživatelům práci v prostředí windows, na kterou jsou zvyklí.

2.2.9 Hardware a software pro IS KÚ

Podrobná specifikace hardware a software implementovaného v rámci tohoto realizačního projektu je vyčleněna do samostatné tabulky v příloze tohoto dokumentu.

Pro přehlednost jsou tabulky požadovaného hardware a software zpracovány samostatně. Počty softwarových licencí firmy Microsoft a antivirů vycházejí z požadovaného hardware.

2.2.9.1 Specifikace hardwarové architektury

Kromě základních služebních serverů potřebných pro komunikační infrastrukturu je nutný určitý minimální počet fyzických serverů pro aplikační software KÚ. Jako platformu zvolily všechny KÚ (kromě hl.m.Prahy) po vzájemné dohodě Microsoft Windows 2000/XP Server s použitím Active Directory jako integračního nástroje.

Doporučujeme uvážit centrální správu serverů a pracovních stanic, která mj. řeší:

- Vzdálený management PC z jedné centrální konzole,
- zobrazení informací o PC a zasílaní chybových hlášení o stavu HW na integrovanou konzoli administrátora,
- možnost otestování HW v reálném čase,
- update systémového software včetně ovladačů HW komponent, informace o právě nainstalované a aktuální verzi,
- SW dohled – ochrana před nechtěnou instalací SW na jednotlivých stanicích.

Specifikace hardware pro potřeby KÚ je uvedena dále.

Preferovanou HW platformou serverů je HP. Jsou požadovány 3 roky záruky, servis na místě typu 4/4 tj. zásah do 4 hod. a do 4 hod. odstranění závady.

2.2.9.1.1 Domain Controller

Tento server bude plnit také funkci interní provozní certifikační. Navrhuje se následující konfigurace:

- 1 / 2 Pentium III 1 GHz, 256 kB Cache,
- 1GB RAM,
- 64 bit PCI řadič, RAID5 diskové pole alespoň ze čtyř disků (jeden jako hotspare), kapacita 100 GB,
- 64 bit PCI GigaEthernet řadič.

2.2.9.1.2 Záložní Domain Controller

Server označovaný jako záložní domain controller bude plnit funkce zálohování a system managementu. Navrhujeme následující konfiguraci:

- 1x Pentium III 1 GHz, 256 kB Cache,
- 1GB RAM,
- 64 bit PCI řadič, 2x40 GB RAID1,,
- DLT nebo LTO changer
- 64 bit PCI GigaEthernet řadič.

2.2.9.1.3 File server a Terminal server

V první etapě je účelné jeho nasazení vzhledem k tomu, že KÚ požaduje také Terminal server, takže je možné obě související funkce spojit. Orientační dimenzování Terminal Serveru pro 50 uživatelů je uvedeno dále:

- 2x Pentium III 1.13 GHz, 512 kB Cache, možno použít XEON,
- min. 1 GB RAM,
- 64 bit PCI RAID řadič, RAID5 diskové pole z alespoň čtyř disků (jeden jako hotspare), kapacita min. 30 GB (podle nároků na prostor fileserveru),
- 64 bit PCI GigaEthernet řadič.

Pokud by bylo více uživatelů než 50, je doporučováno použití dalšího serveru místo posilování výkonu (u velké zátěže se nestihne vyřizovat obsluha přerušení).

2.2.9.1.4 Databázový server

Databázový server bude jeden, v případě požadavku na nákup databází MS SQL i Oracle a postupném zvyšování zatížení obou těchto databází bude nutné zřídit servery dva. Výkonové dimenzování a diskový prostor bude záležet především na zvolené variantě spisové služby (s úložištěm dokumentů v databázi nebo v úložišti FileNET). Pro diskový subsystém u databáze doporučujeme uspořádání RAID1 (zrcadlení disků) z důvodu lepší efektivnosti při diskových operacích, která je pro databázový stroj rozhodující. Jako standardní konfiguraci navrhujeme:

- 2/2 Pentium III 1 GHz, 256 kB Cache,
- 1 GB RAM,
- 64 bit PCI RAID řadič, RAID1 - zrcadlení disků-50 GB
- 64 bit PCI GigaEthernet řadič.

2.2.9.1.5 Exchange Server

Je doporučováno nasazení jednoho serverů případně nasazení dalšího menšího fyzického serveru na FaxChange a MobilChange. Doporučená konfigurace Exchange serveru:

- 2/2 Pentium III 1 GHz, 256 kB Cache,
- 1 GB RAM,
- 64 bit PCI RAID řadič, RAID5 diskové pole 100 GB alespoň ze čtyř disků, jeden jako hotspare, RAID1 diskové pole ze dvou disků (stačí 9 GB) pro transakční logy
- 64 bit PCI GigaEthernet řadič.

2.2.9.1.6 Intranetový a aplikační server

Intranetový a aplikační server je navrhován pro provoz interních aplikací KÚ, zejména intranetových v následující konfiguraci:

- 2/2 Pentium III 1 GHz, 256 kB Cache,
- 1GB RAM,
- 64 bit PCI řadič, RAID5 diskové pole alespoň ze čtyř disků (jeden jako hotspare), kapacita 100 GB ,
- 64 bit PCI GigaEthernet řadič.

2.2.9.1.7 GIS server

KÚ požaduje serverový GIS typu ESRI ArcIMS/ArcGIS. Podle informací firmy ESRI odpovídají nároky tohoto produktu této konfiguraci:

- 2/2 Pentium III 1 GHz, 256 kB Cache,
- 1GB RAM,
- 64 bit PCI řadič, RAID5 diskové pole alespoň ze čtyř disků (jeden jako hotspare), kapacita 100 GB ,
- 64 bit PCI GigaEthernet řadič.

2.2.9.1.8 Pracovní stanice

Stávající klientské stanice v síti KÚ je požadováno doplnit celkem 20 ks osobních počítačů v konfiguraci 1xCPU, 256 MB RAM, 20 GB HDD, Wake-on-LAN, 17“ Trinitron, CR-ROM. Počítače budou mít předinstalován operační systém MS Windows 200 Professional OEM

Preferovanou HW platformou pro klientské (pracovní) stanice je AutoCont. Je požadován servis počítačů na místě se lhůtou opravy do následujícího pracovního dne.

2.2.9.2 Konfigurace základního software

2.2.9.2.1 Serverový operační systém

Jako serverový operační systém je z důvodů jednoznačných preferencí zástupců krajských úřadů navrhován Windows 2000 Server (pro clustery Advanced Server) s přechodem na Windows XP. Jedná se o serverové operační systémy firmy Microsoft založené na technologii Windows NT (resp. původně Open VMS), současná verze Windows 2000 se vyznačuje zlepšenou stabilitou a podstatně lepší kompatibilitou s internetovými standardy jako je DNS a LDAP.

U serverů doporučujeme standardně konfigurovat Terminal Services (admin mode pro vzdálenou správu serveru), na Domain Controlleru pak Certificate Services pro interní certifikační autoritu. Interní DNS a DHCP budou integrované v AD tak, aby spolupracovaly s typovou komunikační infrastrukturou popsanou výše.

2.2.9.2.2 Operační systém pro pracovní stanice

Jako operační systém pro pracovní stanice je preferován operační systém Windows 2000/XP Czech z důvodů uvedených výše (zejména se jedná o jednotnou správu uživatelů), jinak Windows NT4 nebo 98/ME.

Jako doporučená politika pro využití lokálního disku na stanicích je navrhováno rozdělení na tři oblasti (C - systém a software, D - lokální data, S - swap a spool). Zálohování pracovních stanic se standardně nepředpokládá, uživatelé jsou povinni důležité soubory ukládat na file serveru, který je diskutován v předchozích podkapitolách.

2.2.9.2.3 Správa systému

Vzhledem k omezeným prostředkům na nákup serverů předpokládáme v KÚ zatím vytvoření jedné domény odpovídající doméně internetové.

Je doporučováno základní správu vnitřního IS provádět právě pomocí Active Directory pomocí Group Policy objektů. Metodicky navrhujeme rozdělit politiky na tři úrovně:

- Microsoft Original Policy,
- Project Policy,
- Customer Operational Policy.

Správci sítě úřadu pak mohou v případě potřeby přepsat nastavení MS nebo projektové politiky a následně je možné dohledat potřebné změny a přenést je v případě potřeby do projektové politiky.

Sdílené adresáře či další zdroje doporučujeme důsledně zpřístupňovat uživatelům přes Distributed File System (DFS), aby bylo možné jednak jejich přesouvání mezi fyzickými servery a disky a také eventuelní zálohování v rámci serverového clusteru s replikacemi uživatelských adresářů.

Pro další centralizaci správy pracovních stanic a případně i serverů předpokládáme nasazení Microsoft Systems Management Serveru (SMS) verze 2, který je možno získat za výhodných podmínek v rámci programového balíku BackOffice.

V dalších etapách se předpokládá upřesnění a zprovoznění PKI služeb. Prozatím doporučujeme nasazení Microsoft Certificate Services podle standardních postupů doporučených firmou Microsoft.

Doporučujeme naplánovat pro správce sítě a aplikací potřebná administrátorská školení, zejména

- Windows 2000 server, příp. Linux a FreeBSD
- Active Directory, implementace a administrace
- Microsoft Office, správa v síti
- Microsoft Exchange správa
- správa MS SQL nebo Oracle databáze
- základní školení na CISCO produkty
- školení na správu ekonomického systému, spisové služby a dalších aplikací

2.2.9.2.4 Zálohování

Navrhujeme centrální zálohování pomocí zálohovacího serveru vybaveného měničem pásek . Jako zálohovací software je navrhován standardně Veritas BackupExec, jehož omezená verze je již součástí serverového OS a je proto potřebné jen dokoupit příslušný upgrade na plnou verzi se zálohovacími agenty pro Exchange Server, případně SQL server.

2.2.9.2.5 Poštovní/kancelářský systém

Pro poštovní, resp. kancelářský systém je navrhováno nasazení produktu Exchange 2000 Server s klienty Microsoft Outlook. KÚ požaduje integraci s faxovým serverem (Datasys FaxChange, případně MobilChange). Z důvodů vyšší provozní stability je možno pro tyto další servery doporučit jejich umístění na samostatných počítačích.

2.2.9.2.6 Databázový systém

Pro provoz aplikací je požadován Oracle 8i Standard.

2.2.9.2.7 Licencování software

U firmy Microsoft proběhne licencování na základě smlouvy Microsoft Select pro kraje sjednané s ÚVIS. U základního serverového software předpokládáme licencování „per seat“, kdy KÚ nakoupí klientské licence v rámci programu Select a vlastní serverové programy buď OEM (operační systémy) nebo také v rámci programu Select.

Výběr variant a cen licencí Microsoft byl prováděn na základě dostupných informací o novém licenční programu této firmy, který je v těchto dnech teprve finalizován. Nemůže proto vyloučit, že v době nákupu software nedojde ke změnám.

V rámci nového licenčního programu přestává existovat sdružená licence Microsoft BackOffice a je nahrazována podobným produktem CORE CAL s jinou filosofií. Podle současných informací bude tento produkt dostupný pouze s udržovacími poplatky (SA), takže v tabulkách SW produktů uvádíme variantu nákupu dílčích produktů samostatně (bez SA).

3 SYSTÉMOVÁ BEZPEČNOSTNÍ POLITIKA

Systémová bezpečnostní politika Krajských úřadů byla zpracována jako část řešení typového projektu a představuje zobecnění bezpečnostních zásad, které musí být uplatněny pro každý IS KÚ.

Systémová bezpečnostní politika tvoří samostatný dokument, který je uveden jako příloha typového projektu.

Systémová bezpečnostní politika musí být před vyhlášením v KÚ upravena podle konkrétní situace KÚ zejména:

- část administrativní bezpečnosti se vztahem k bezpečnosti IS KÚ, pravomoci, zodpovědnosti, funkce,
- část personální bezpečnosti se vztahem k bezpečnosti IS KÚ,
- technická a objektová bezpečnost lokality KÚ se vztahem k bezpečnosti IS KÚ, zejména objektů/místností s vysokou koncentrací výpočetní techniky a objektů/místností, kde se pracuje s klasifikovanými informacemi,
- bezpečnost IS - část stávajících systémů jako část kapitoly 3 udávající charakteristiky IS,
- kryptografická ochrana informací v IS - je-li použita a požaduje-li se tato ochrana pro nově koncipovaný IS KÚ s ohledem na místní specifickou situaci.

Systémová bezpečnostní politika musí být vyhlášena a implementována. Implementace těch částí, které se vztahují na nově koncipovaný IS KÚ je zajištěna jako součást dodávky. Úpravy ve smyslu kap. 3.1. SBP musí být s ohledem na adaptované systémy (které nejsou součástí dodávky podle tohoto typového projektu) provedeny tak, jak v této kapitole uvedeno.

4 PŘÍLOHA 1 - SPECIFIKACE DODÁVEK

Tabulky specifikací hardware a software jsou přiloženy v samostatných souborech.

5 PŘÍLOHA 2 - SPECIFIKACE MODULŮ IS

Cenová kalkulace systému GINIS-SSL pro krajský úřad

Firma Gordic přislíbila podrobné vyjádření k integraci s DMS FileNET a Active Directory

pol.	*podpol.*	*popis*	*rozsah*	*cena Kč*	*sleva*	*cena po slevě (Kč)*	*mn.*	*celk.cena (Kč)*
	ADM základní administrace							ADM
1110	003	server	do 50000	450 000,-	50%	225 000,-		
1110	004	server	do 100000	700 000,-	50%	350 000,-		
1110	005	server	neomez	1 200 000,-	50%	600 000,-		
1110	101	klient T		20 000,-	50%	10 000,-	1	10 000,-
1110	111	klient T-AKC		14 000,-	50%	7 000,-		
1110	003	server + el. pís.	do 50000	463 500,-	**70%**	139 050,-	1	139 050,-
1110	004	server + el. pís.	do 100000	910 000,-	50%	455 000,-		
1110	005	server + el. pís.	neomez	1 560 000,-	50%	780 000,-		
	ADK správa kartotéky							ADK
1120	101	klient T-ADK		25 000,-	50%	12 500,-	1	12 500,-
	USU univerz. spisový uzel							USU
1710	101	klient T-USU		7 000,-	50%	3 500,-		

1710	111	klient T-PSU přehledy USU		7 000,-	50%	3 500,-		
1710	121	klient T-PRP před.modul		3 000,-	50%	1 500,-		
1710	201	server L		28 000,-	50%	14 000,-		
1710	202	klient L		700,-	50%	350,-		
1710	101	klient T-USU + el. pís.		9 100,-	50%	4 550,-	20	91 000,-
1710	201	server L + el. pís.		36 400,-	50%	18 200,-		
1710	202	klient L + el. pís.		910,-	50%	455,-		
	POD podatelna, TPD tisk podacích deníků							POD, TPD
1720	101	klient T-POD		7 000,-	50%	3 500,-	1	3 500,-
1720	111	klient T-TPD gen.pod.deníků		25 000,-	50%	12 500,-	1	12 500,-
	VYP výpravna							VYP
1730	101	klient T-VYP		7 000,-	50%	3 500,-	1	3 500,-
	REF referent							REF
1740	101	klient T-REF		7 000,-	50%	3 500,-		
1740	201	server L		28 000,-	50%	14 000,-		
1740	202	klient L		700,-	50%	350,-		
1740	101	klient T-REF +		9 100,-	**70%**	2 730,-	50	136 500,-

		el. pís.						
1740	201	server L + el. pís.		36 400,-	50%	18 200,-	1	18 200,-
1740	202	klient L + el. pís.		910,-	50%	455,-	30	13 650,-
	VED vedoucí							VED
1750	101	klient T-VED		7 000,-	50%	3 500,-	5	17 500,-
1750	201	server L		28 000,-	50%	14 000,-		
1750	202	klient L		700,-	50%	350,-		
	INT interface SSL							INT
1770	005	server-zdr. licence	neomez	40 000,-	50%	20 000,-	1	20 000,-
1770	101	klient T-INT		7 000,-	50%	3 500,-	1	3 500,-
	SPI spisovna							SPI
1780	001	server-zdr. licence	do 1000	3 500,-	50%	1 750,-		
1780	002	server-zdr. licence	do 5000	6 250,-	50%	3 125,-		
1780	003	server-zdr. licence	do 50000	12 500,-	50%	6 250,-	1	6 250,-
1780	004	server-zdr. licence	do 100000	25 000,-	50%	12 500,-		
1780	005	server-zdr. licence	neomez	50 000,-	50%	25 000,-		

1780	101	klient T-SPI		25 000,-	50%	12 500,-	1	12 500,-
	UKO úkoly							UKO
1790	001	server-zdr. licence	do 1000	6 500,-	50%	3 250,-		
1790	002	server-zdr. licence	do 3000	11 250,-	50%	5 625,-	1	5 625,-
1790	003	server-zdr. licence	do 50000	22 500,-	50%	11 250,-		
1790	004	server-zdr. licence	do 100000	45 000,-	50%	22 500,-		
1790	005	server-zdr. licence	neomez	90 000,-	50%	45 000,-		
1790	101	klient T-UKO		7 000,-	50%	3 500,-	20	70 000,-
1790	201	server L		50 000,-	50%	25 000,-		
1790	202	klient L		2 000,-	50%	1 000,-		
	USN usnesení							USN
1791	001	server-zdr. licence	do 200	6 000,-	50%	3 000,-	1	3 000,-
1791	002	server-zdr. licence	do 500	10 500,-	50%	5 250,-		
1791	003	server-zdr. licence	do 1000	21 000,-	50%	10 500,-		
1791	004	server-zdr. licence	do 2000	42 000,-	50%	21 000,-		
1791	005	server-zdr. licence	neomez	90 000,-	50%	45 000,-		

1791	101	klient T-USN		25 000,-	50%	12 500,-	3	37 500,-
1791	201	server L		60 000,-	50%	30 000,-		
1791	202	klient L		1 500,-	50%	750,-		
	Aplikační server							WO
5210	004	WebObjects server	neomez.	30 000,-	0%	30 000,-	1	30 000,-
	CELKEM							**646 275,-**

		Návrh cenové kalkulace systému GINIS - EKO pro jeden Krajský úřad					
Pol	*Ppol*	*Popis*	*Rozsah*	*Cena/j (Kč)*	*Množ*	*Sleva*	*Celkem (Kč)*
1110	003	GINIS - jádro IS server	do 50000 dok.	450 000,-	1	50%	225 000,-
1110	101	Administrace ADM - klient T		25 000,-	1	50%	12 500,-
1120	101	ADK Správa kartotéky externích subjektů klient T		25 000,-	1	50%	12 500,-
1130	003	Administrace EKO ADE - server	do 1000 dokladů	60 000,-	1	50%	30 000,-
1130	101	Administrace EKO ADE - klient T		15 000,-	1	50%	7 500,-
1140	101	Administrace EKO ADR - účt. vazby klient T		15 000,-	1	50%	7 500,-
1140	121	Administrace EKO ADS - administrace sestav klient T		10 000,-	1	50%	5 000,-
1140	111	Administrace EKO ADP - předkontace klient T		25 000,-	1	50%	12 500,-
1210	004	UCR Sumarizační modul rozpočtu a účetnictví server	do 5000 záp/měs.	75 000,-	1	50%	37 500,-
1210	101	UCR Sumarizační modul rozpočtu a účetnictví klient T		20 000,-	5	50%	50 000,-
1140	131	Administrace EKO ADA administrace akcí - klient T		15 000,-	1	50%	7 500,-
1140	141	Administrace EKO ADO administrace org.- klient T		20 000,-	1	50%	10 000,-
1220	003	BAR Návrh a balancování rozpočtu	do 1000 akcí	37 500,-	1	50%	18 750,-

		server	P+V				
1220	101	BAR Návrh a balancování rozpočtu klient T		20 0-	1	50%	10 000,-
1230	003	SRV Střednědobý rozpočtový výhled server	do 1000 akcí P+V	30 0-	1	50%	15 000,-
1230	001	SRV Střednědobý rozpočtový výhled klient T		20 0-	5	50%	50 000,-
1240	001	ROZ Pořizovač rozpočtových dokladů server	do 100 záp/měs.	8 000,-	1	50%	4 000,-
1240	101	ROZ Pořizovač rozpočtových dokladů klient T		18 000,-	1	50%	9 000,-
1250	003	UCT Pořizovač účetních dokladů server	do 1000 záp/měs.	37 500,-	1	50%	18 750,-
1250	101	UCT Pořizovač účetních dokladů klient T		18 000,-	5	50%	45 000,-
1260	004	INU Interface účetnictví a rozpočtu server	do 5000 záp/měs.	20 000,-	1	50%	10 000,-
1260	101	INU Interface účetnictví a rozpočtu klient T		8 000,-	1	50%	4 000,-
1310	003	BUC Komunikace s bankou server	do 1000 příkazů/měs.	10 000,-	1	50%	5 000,-
1310	101	BUC Komunikace s bankou klient T		8 000,-	1	50%	4 000,-
1320	003	KDF Kniha došlých faktur server	do 1000 fakt/měs.	15 000,-	1	50%	7 500,-
1320	101	KDF Kniha došlých faktur klient T		15 000,-	5	50%	37 500,-
1330	003	POU Poukazy server	do 1000 pouk./měs.	15 000,-	1	50%	7 500,-
1330	101	POU Poukazy klient T		15 000,-	1	50%	7 500,-
1340	003	KOF Kniha odeslaných faktur server	do 1000 fakt/měs.	12 500,-	1	50%	6 250,-

1340	101	KOF Kniha odeslaných faktur klient T		15 000,-	5	50%	37 500,-
1350	002	PRE Převodní poukazy server	do 500 pouk./měs.	7 500,-	1	50%	3 750,-
1350	101	PRE Převodní poukazy klient T		15 000,-	5	50%	37 500,-
1350	003	PPD Předpokladní doklady - server	do 1000 dokladů/měs	7 000,-	1	50%	3 500,-
1350	101	PPD Předpokladní doklady - klient T		6 000,-	1	50%	3 000,-
1370	004	POK Pokladna server	do 2000 dokladů/měs	28 000,-	1	50%	14 000,-
1370	101	POK Pokladna klient T		12 000,-	1	50%	6 000,-
1290	004	FUC finanční účtárna - server	do 5000 záp/měs.	95 0-	1	50%	47 500,-
1290	101	FUC finanční účtárna - klient T		26 0-	1	50%	13 000,-
1440	003	SML smlouvy - server	do 1000 smluv	15 0-	1	50%	7 500,-
1440	101	SML smlouvy - klient T		15 0-	1	50%	7 500,-
1350	003	PLA plán - server	do 1000 záp/rok	30 0-	1	50%	15 000,-
1350	101	PLA plán - klient T		18 0-	1	50%	9 000,-
1020	001	MPD - server	do 2 licencí	35 0-	1	50%	17 500,-
1020	101	MPD - klient T		12 0-	1	50%	6 000,-
1770	005	INT interface - server	neomezená	40 0-	1	50%	20 000,-
1770	101	INT interface - klient		7 0-	1	50%	3 500,-
1550	004	MAJ Majetek (EMA + SKL) server	do 10000 karet	88 0-	1	50%	44 000,-
1550	101	MAJ Majetek (EMA + SKL) klient T		19 0-	2	50%	19 000,-

		Moduly I.fáze celkem					**992 000,-**
		Celkem za I.fázi vč. DPH					**1 041 600,-**

Ceny projektů , prací a služeb závisí na požadavcích zákazníka a jsou kalkulovány v souladu s platným ceníkem firmy Gordic spol. s r.o.

Přesné počty jednotlivých modulů vyplynou z analýzy resp. požadavků zákazníka

FLUXPAM 5

Počet osobních čísel	25	50	100	300	500	1 000	1 500	2 000	2 500	3 000	3 500
FLUXPAM 5											
Basic	10 780										
Basic +	11 740										
Standard		13 090	25 220	31 570	41 040						
Klasik		13 860	26 570	33 690	43 800						
Klasik +		15 020	28 680	36 380	47 290	65 490	76 410	112 790	141 890	160 090	181 910
údržba	5 780	7 510	11 360	15 210	17 130	17 680	20 630	30 450	38 310	43 220	49 120
FLUXPAM 5 – síťová verze											
Klasik + do 5 stanic	16 360	19 060	36 380	47 740	62 060	85 930	100 260	148 000	186 180	210 050	238 700
Klasik + do 10 stanic			55 650	69 720	90 640	125 490	146 410	216 130	271 920	306 780	348 600
údržba do 5 stanic	7 700	9 430	15 210	20 980	21 530	23 210	27 070	39 950	50 280	56 720	64 450
údržba do 10 stanic			18 690	27 090	30 080	33 780	39 530	58 360	73 410	82 830	94 120
FLUXPAM 5 – multilicence											
Basic + pro 1 PC	12 090										
Basic + pro 2 – 5 PC	13 290										
Klasik + pro 1 PC		20 210	38 690	54 670	71 070	98 400	114 800	169 470	213 220	240 560	273 350
Klasik + pro 2 – 5 PC		22 520	43 030	61 790	80 330	111 230	129 760	191 560	240 990	271 880	308 960

údržba pro 1 PC	5 780	9 430	17 130	24 830	25 110	26 570	30 990	45 760	57 560	64 940	73 800
údržba pro 2 – 5 PC	6 300	10 330	20 300	27 830	28 530	30 030	35 040	51 710	65 070	73 410	83 420
FLUXPAM 5 - multilicence – síťová verze											
Klasik + do 5 stanic	19 640	31 480	60 360	71 310	92 700	128 360	149 770	210 080	278 130	313 780	356 560
Klasik + do 10 stanic		40 930	78 470	92 720	120 540	166 880	194 690	287 400	361 570	407 910	463 370
údržba do 5 stanic	7 700	11 850	22 910	34 180	34 300	34 670	40 440	59 690	75 090	84 720	96 270
údržba do 10 stanic		13 600	26 230	39 380	42 440	45 060	52 570	77 600	97 630	110 130	125 110

Jednouživatelské verze programu pracují s databází Access, která je dodávána s programem a je zahrnuta v jeho ceně.

Ceny uvedené u síťových verzí jsou kalkulovány pro databáze Btrieve, které nejsou součástí programu.

Pokud bude síťová verze využívat jiné databázové prostředí (např. ORACLE, SQL), násobí se cena programu a údržby koeficientem 1,5.

Rozhodující pro stanovení ceny multilicence je součet všech osobních čísel zpracovávaných firem.

Počtem osobních čísel se rozumí součet aktivních a neaktivních zaměstnanců.

Docházkový systém								
Počet osobních čísel	300	500	1 000	1 500	2 000	2 500	3 000	3 500
Základní modul	90 000	99 000	162 000	189 000	279 000	351 000	396 000	450 000
Modul Jídelna	21 800	23 760	38 880	45 360	66 960	84 240	95 040	108 000
Modul Vrátnice (1 licence)	60 000	každá další licence 42 000						
údržba Docházkového systému	18 000	19 800	32 400	37 800	55 800	70 200	79 200	90 000

údržba modulu Jídelna	4 320	4 760	7 780	9 080	13 400	16 850	19 010	21 600
údržba modulu Vrátnice	12 000	každá další licence 8 400						

NÁZEV MODULU	Basic	Basic +	Standard	Klasik	Klasik +	Cena	NÁZEV MAKRA	Basic	Basic +	Standard	Klasik	Klasik +	Cena
základní výpočet mezd *)	+	+	+	+	+	-	editace univerzálních sestav	+	+	+	+	+	-
zdravotní pojištění	+	+	+	+	+	-	editace univerzálních rekapitulací	+	+	+	+	+	-
sociální pojištění	+	+	+	+	+	-	výstup pro hromadné platební příkazy	+	+	+	+	+	-
daně	+	+	+	+	+	-	výstup pro Českou spořitelnu - disketa				+	+	800
kalendář	+	+	+	+	+	-	export do DBF		+			+	660
vyplácet zálohy		+			+	530	export do ASCII					+	660
souběžné pracovní poměry		+		+	+	800	výstup pro Eltrans						1 320
rozšířené srážky					+	1 310	výstup pro IPB a KB						1 320
rozšířené odměny					+	1 060	výstup do KDF						1 100
platová tabulka						660	rozšířená dovolená		+			+	530
FKSP						660	turnusy		+			+	1 590
funkcionář						660	ZP, hromadné oznámení					+	1 320

							organizace - disketa						
odbory						400	změna platu s příplatkem v průběhu měsíce						3 300
							mzda - úkolová, podílová a účtování na zakázku						od 9 110
							sjednocování dat						od 6 600

Moduly a makromoduly označené + jsou součástí modelů, ostatní je možno dokoupit samostatně.

CENÍK SLUŽEB IMPLEMENTACE FLUXPAM 5

Činnost	**Kč/den**
Analytické práce	9 800
Cestovní náhrady	9,90 Kč/km
Práce u klienta	9 800
Řízení projektu	13 000
Školení systému	9 800
Konzultace u zákazníka	9 800/den

REZORTNÍ SLEVY IMPLEMENTAČNÍCH PRACÍ (včetně převodu dat)

Školské úřady, vysoké školy, střední školy a učiliště,	
základní a mateřské školy (30 %)	858 Kč
Zdravotnictví a ústavy sociální péče (35 %)	796 Kč
Obce, města, okresní úřady (45 %)	650 Kč
Církve, nadace, kulturní instituce (40 %)	735 Kč
Cestovné po Praze	300 Kč

6 PŘÍLOHA 3 - SPECIFIKACE MODULŮ PRO ZÁLOHOVÁNÍ

Specifikace Veritas Backup Exec pro typové řešení zálohování

Ceny jsou koncové v Kč z katalogu Cybex, předpokládáme množstevní slevu.

1317368	BE for NT/2000 8.6 AE	31 950
1317371	BE for NT/2000 8.6 AE UPG <- MS	21 490
1317370	BE for NT/2000 8.6 AE UPG <- SS	16 190
1317372	BE for NT/2000 8.6 AE Competitive UPG	21 490
1317373	BE for NT/2000 8.6 AE UPG from Server Edition	10 990
1317394	BE for NT/2000 8.6 AE Family UPG	16 190
1317367	BE for NT/2000 8.6 SE	21 490
1317374	BE for NT/2000 8.6 SE UPG from MS	16 190
1317369	BE for NT/2000 8.6 SE UPG from SS	10 990
1317392	BE for NT/2000 8.6 SE UPG from SBS	7 090
1317393	BE for NT/2000 8.6 SE Family UPG	10 990
1317375	BE for NT/2000 8.6 SE Competitive UPG	13 490
1317381	BE for NT/2000 8.6 Intell. Disaster Recovery Option	13 490
1317382	BE for NT/2000 8.6 Intell. Disaster Recovery Option Add Remote License	5 590
1317183	BE for NT/2000 8.6 Agent for Exchange	21 490
1317383	BE for NT/2000 8.6 Agent for Notes/Domino	21 490
1317387	BE for NT/2000 8.6 Agent for Oracle	18 990
1317388	BE for NT/2000 8.6 Agent for SAP R/3 for Oracle	78 900
1317116	BE for NT/2000 8.6 Agent for MS-SQL Server	21 490
1317384	BE for NT/2000 8.6 Library Expansion Option	26 950
1317385	BE for NT/2000 8.6 Remote Agent	7 090
1317184	BE for NT/2000 8.6 Remote Agent 3-Pack	18 990

1317386	BE for NT/2000 8.6 Open File Option	18 990
1317115	BE for NT/2000 8.6 RAIDirector (RAID Option)	26 950
1317389	BE for NT/2000 8.6 Shared SO Starter Pack	42 950
1317390	BE for NT/2000 8.6 IBM ADSM Starter Pack	131 900
1317391	BE for NT/2000 8.6 IBM ADSM Client Pack	8 290
1317395	BE for NT/2000 8.6 Intelligent Image Option	26 950
1317396	BE for NT/2000 8.6 SharePoint Portal Server	21 490
1317378	BE for NT/2000 8.6 SBS Edition	21 490
1317379	BE for NT/2000 8.6 SBS Edition UPG	10 990
1317380	BE for NT/2000 8.6 SBS Edition Competitive UPG	13 490
1317366	BE BackOffice Suite 8.6 Advanced Edition	60 900
1317365	BE BackOffice Suite 8.6 Server Edition	52 900

Jako typovou konfiguraci předpokládáme:

- Backup Exec Backoffice Suite (1x NT server, 1x SQL, 1x Exchange) verze Server nebo Advanced Server
- 6x Remote Agent pro další servery
- cca 3x Disaster Recovery Option (rychlé obnovení OS)
- cca 3x Open File Option
- volitelně Agent for Oracle, RAID Option (zrychlení zálohy diskových polí) .

7 PŘÍLOHA 4 SROVNÁNÍ EKONOMICKÝCH A SPISOVÝCH IS

7.1 Spisová služba

Při volbě konkrétních produktů musí být přihlédnuto k možnostem splnění požadavků dobré integrovatelnosti v druhé etapě informatizace KÚ. Zatím je integrovatelnost deklarována jen v rámci programových balíků jednoho dodavatele, většinou jako spolupráce spisové služby s dalšími aplikacemi.

Obecně KÚ předpokládají základní typové řešení pro 50 uživatelů s využitím úložiště FileNET firmy Panagon. Hlavní výhodou tohoto řešení je dobrá integrace se zvolenou serverovou platformou Windows 2000 a jejími intranetovými službami, nevýhodou je poměrně vysoká cena, kterou je zatím možno kompenzovat nákupem menšího množství uživatelských licencí FileNET. V případě většího nasazení spisové služby, což KÚ v budoucnu předpokládají, je třeba počítat s dokupováním licencí pro další současně pracující uživatele. V blízké budoucnosti se nabízí jako variantní úložiště MS SharePoint Portal Server, který mohou KÚ získat v rámci licencí Select za výhodných podmínek.

Při nasazení FileNETu může KÚ volit nadstavby od firem Gordic, Plzeňský holding nebo PVT, případně využít konfiguraci bez použití úložiště dokumentů FileNET. Jednotlivé varianty jsou uvedeny v realizačních projektech jako možnosti výběru.

Systém GINIS-SSL firmy Gordic obecně řídí a sleduje tok informací v úřadě (v elektronické i papírové formě), zabezpečuje identifikaci dokumentů, odpovědnost pracovníků a podporuje i řídící činnosti. Systém pracuje v architektuře s jednou centrální databází, standardně obsahuje moduly administrace, universálního spisového uzlu, podatelny, výpravny, spisovny, kartotéky, modul úkolů a usnesení. Firma Gordic zatím nabízí standardně vlastní úložiště dokumentů, nově pak deklarovala spolupráci s firmou Plzeňský holding při implementaci úložiště FileNet.. Implementace úložiště dokumentů FileNET do spisové služby GINIS-SSL má být poprvé prezentována na veletrhu INVEX v říjnu 2001. Výhodou řešení firmy Gordic jsou dlouhodobé zkušenosti s implementací spisové služby ve veřejné správě.

Spisová a archivační služba PVT se nabízí standardně s integrovaným úložištěm dokumentů (DMS systémem) FileNET, jako možnost přichází v úvahu i levnější řešení na bázi technologií firmy Microsoft. Systém navrhujeme implementovat včetně dodatečných modulů pro skenování a čárový kód.

Spisová služba iGenesis firmy Plzeňský holding, a.s. je založena na spolupráci s úložištěm dokumentů FileNET. Licence na iGenesis umožňuje práci 50 uživatelů. V licenci iGenesis je neomezený počet skenovacích licencí a pracovišť včetně čárových kódů. Systém umožňuje implementaci technologií elektronického podpisu. Obecnou výhodou tohoto systému je dobrá integrace se zvolenou serverovou platformou Windows 2000.

Do výběru byla rovněž zařazena spisová služba KORÁB firmy EXPRIT. Systém pracuje na platformě Oracle Database/Application Server s použitím tenkého klienta (web browser). Klient pak využívá standardních funkcí integrovaného prostředí MS Office, pro speciální funkce existují samostatné moduly.

Realizace podpory workflow není v rámci základní informatizace vyžadována.

7.2 Ekonomický systém

KÚ navrhují ekonomické systémy GINIS, Fenix nebo ekonomický systém na platformě Great Plains s nadstavbovými moduly pro oblast veřejné správy. Vzorové kalkulace těchto ekonomických systémů včetně přehledu modulů jsou uvedeny v příloze projektu. Z důvodu integrace aplikací je vhodné kombinovat ekonomický systém a spisovou službu téhož výrobce.

Systém GINIS-EKO je dodáván firmou Gordic, spol. s .r.o. Jihlava. Systém pracuje v architektuře klient-server a využívá centrální relační databází s dotazovacím jazykem SQL. GINIS - EKO je speciálně navržen pro potřeby orgánů veřejné správy, průběžně zohledňuje legislativní změny a je nasazen v celé řadě rozpočtových organizací. Sestava standardně obsahuje moduly pro práci s rozpočtem, vedení účetní agendy, pokladnu, komunikaci s bankou, evidenci majetku a administrační modul.

V případě informačního systému Fenix společnosti PVT a.s. jde o komplexní systém zahrnující kromě modulů pro ekonomickou agendu také řízení personalistiky a zpracování mezd, evidenci majetku, evidenci docházky. Systém má rovněž moduly pro registry obyvatel, nemovitostí a ekonomických subjektů, případně GIS.

Systém MS Great Plains eEnterprise je ve státní správě nový a proto je navrhováno jeho pilotováníve vybraných krajích. Jinak se jedná o podnikový systém osvědčený i v ČR. Systém předpokládá standardně poměrně nákladnou implementaci.

7.3 Srovnání systémů

Porovnávací tabulka vlastností jednotlivých spisových služeb byla KÚ již poskytnuta dodavateli spisových služeb. Jedná se však spíše o marketingový materiál s omezenou vypovídací schopností. Následující porovnání produktů z hlediska integrovatelnosti vychází spíše z dostupných technických informací a porovnává systémy dle dodavatelů s ohledem na omezené možnosti spolupráce produktů různých dodavatelů. U ekonomických systémů je spolupráce obecně řešitelná formou exportů/importů dat, což samozřejmě není dostačující pro operace v reálném čase. U spisových služeb je základní situace obdobná, tj. je možná výměna dokumentů jakožto souborů, nikoli však informací o nich (metadat, profilů dokumentu). Pokud jsou tyto informace předávány, tak se jedná o dávkové předávání souborů ve zcela proprietárním formátu dané firmy (GORDIC), takže nelze vazby na produkty jiných dodavatelů řešit hned v rámci základní dodávky.

Na žádost KÚ je analýza členěna dle metodiky SWOT (Strengths, Weaknesses, Opportunities, Threats)

7.3.1 Gordic GINIS EKO a SSL

- **S:** Produkty jsou zavedené ve státní správě.

- **W:** Firma neposkytuje konkrétní technické informace o dalším rozvoji produktů, podle neoficiálních informací má problémy v integraci SSL s úložištěm FileNET. V produktu EKO se nedoporučuje používání modulu PaM.

- **O:** Firma deklarovala ochotu spolupracovat s Plzeňským Holdingem na integraci s úložištěm FileNET a záměr předvádět výsledky na INVEXu a pilotně nasadit v MHMP. Vyjádření k této strategii je v příloze tohoto dokumentu a bylo již také rozesláno na KÚ.

- **T:** Produkty zatím pracují ve dvouvrstvové architektuře, firmě se nemusí v dohledné době podařit zrušit vazbu na databázové úložiště či realizovat ostatní plánované úpravy. Toto riziko se zvyšuje v případě menšího zájmu o nasazované produkty či změny priorit vývoje produktů.

7.3.2 PVT Fénix EKO a SSL

- **S:** Ekonomický subsystém je zavedený v státní správě a prodávaný za výhodnou cenu, má centralizovanou správu uživatelů. Spisová služba podporuje různá úložiště (Oracle, MSSQL, FileNET) a systémy správy uživatelů (mj. Active Directory), klient je integrován do MS Windows.

- **W:** Ekonomický subsystém zatím není integrován s Active Directory.

- **O:** Firma deklaruje ochotu k zavedení správy ekonomického subsystému přes Active Directory a případně ke spolupráci s jinými produkty.

- **T:** V případě malého počtu požadavků na výše zmíněné úpravy se tyto nemusejí realizovat.

7.3.3 Plzeňský Holding Great Plains a iGenesis

- **S:** Produkty jsou plně integrované s Microsoft platformou, Active Directory a úložištěm FileNET.

- **W:** Great Plains předpokládá poměrně nákladnou implementaci. Oba produkty jsou ve státní správě nové a jejich nasazení je omezeno výhradně na prostředí Microsoft.

- **O:** Nabízí se možnost realizovat integrovaný a relativně otevřený systém v rámci prostředí Microsoft.

- **T:** Dodavatel s produkty ve státní správě dostatečně neprosadí a upraví priority dalšího vývoje svých produktů.

7.3.4 Exprit KORÁB

- **S:** Vysoce progresivní vícevrstvá architektura**.** WWW technologie je primární pro realizaci všech uživatelských funkcí. Snadná implementace produktu. Produkt je používán na magistrátě města Brna. Existuje snadno adaptibilní rozhraní pro integraci s dalšími IS.

- **W:** Vazba na jedinou platformu Oracle, správa uživatelů jen v databázi. Produkt není zatím masově nasazen ve veřejné správě

- **O:** Možnost rychlého a snadného nasazení SSL. Možnost efektivního dalšího rozvoje s využitím nových funkcí aplikačního serveru.

- **T:** Harmonogram zprovoznění nových požadavků (např. pro využití integrované správy uživatelů) bude pravděpodobně značně závislý na počtu instalací ve veřejné správě.

7.4 Příloha - aktuální vyjádření firmy GORDIC

Řešení spisovém služby GINIS SSL je otevřený komplexní,samostatně fungující systém včetně el. úložiště dokumentů a lehkého klienta univerzálního spisového uzlu fungující i v třívrstvé architektuře, který podporuje integraci s produkty předních dodavatelů systému pro správu a řízení dokumentů. (FileNet, Documentum, Microsoft). Z analýzy, kterou jsme provedli je naše integrované řešení pro KÚ (z důvodu tohoto požadavku ze strany KÚ resp. typového projektu ICZ)primárně postaveno na technologii FileNet implementované ve spolupráci s Plzeňským holdingem a.s. jak již bylo deklarováno (není to však jediná varianta řešení této integrace s FileNet) nebo Microsoft SharePoint Portal Server 2001, což je druhá námi řešená varianta implementovaná ve spolupráci se společností Infinity. Integrační práce již byly zahájeny, je vyčleněn a fuguje tým programátorů problematika je naší firmou zvládnutelná a není rozsahem odlišná od jiných integračních prací námi běžně realizovaných).Můžeme odpovědně prohlásit, že jsme připraveni uzavřít smlouvu s krajskými úřady na integrované řešení SSL s DMS, která bude funkčně a časově vyhovovat krajskému úřadu. Termín implementace integrovaného řešení bude logicky stanoven v souvislosti s termínem implementace FileNet(dosud nám tento termín není znám, ani nemáme informaci o nasazované verzi a tom, které části FileNet budou na KÚ implementovány, což jsou velmi zásadní informace z pohledu integrace obou systémů) nebo jiného DMS.

Touto integrací, která bude předvedena na lnvexu 2001 se doplňují vlastnosti sofistifikované aplikace SSL s požadavky kladené na vyspělý systém pro řízení a správu dokumentů - bezpečné úložiště dat s webovým přístupem, konzistence dat a workflow dokumentů, publikace dokumentů na webu a intranetu, fulltextové vyhledávání dokumentů, snadná výstavba intranetu, spolu s jednoduchou administrací. Přímá integrace do prostředí kancelářských aplikací MS Office a poštovního serveru MS Exchange znamenají snadnou implementaci a intuitivní práci uživatelů v prostředí ,které je jim známé.

Další výhody řešení vidíme ve spojení naší technologie s technologií SharePoint Portal Serveru (i když není v typovém projektu asi uvažován), která představuje funkční akceptaci požadavků a zároveň úsporu prostředků vzhledem k jeho pořizovací ceně a dále k výhodným

obchodním vztahům, jenž jsou uzavřeny společností Microsoft s orgány státní správy. Podle našich posledních informací FileNet připravil konektivitu na SharePoint Portal Server.

8 SEZNAM OBRÁZKŮ A TABULEK

8.1 Seznam obrázků

8.2 Seznam tabulek