Využití VPN pro komunikaci na poplachové přijímací centrum a jeho rizika

Use VPN for Communication to Alarm Receiving Center and its Risks

Bc. Frydrych Pavel

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Pavel Frydrych**
Osobní číslo:	**A11282**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Využití VPN pro komunikaci na poplachové přijímací centrum a jeho rizika**

Zásady pro vypracování:

1. **Vysvětlete základní koncepci systémů dohledových poplachových přijímacích center (DPPC).**
2. **Stručně zpracujte normy týkající se DPPC.**
3. **Zpracujte komunikační kanály z hlediska nákladů v Česku.**
4. **Zpracujte komunikační cesty a protokoly, využívající VPN.**
5. **Vyhodnoťte rizika spojená s využíváním VPN.**
6. **Naznačte další vývoj v oblasti komunikace na DPPC.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ČSN EN 50518-1. Dohledová a poplachová přijímací centra – Část 1: Umístění a konstrukční požadavky. Praha: Český normalizační institut, 2011.**
2. **ČSN EN 50518-2. Dohledová a poplachová přijímací centra – Část 2: Technické požadavky. Praha: Český normalizační institut, 2011.**
3. **ČSN EN 50518-3. Dohledová a poplachová přijímací centra – Část 3: Pracovní postupy a požadavky na provoz. Praha: Český normalizační institut, 2012.**
4. **PALOVSKÝ, Radomír. Informační a komunikační sítě. Vyd. 1. Praha: Oeconomica, 2010. ISBN 978-802-4517-292.**
5. **KINDL, Jiří. Projektování bezpečnostních systémů. 1. vyd. Zlín: Univerzita Tomáše Bati, 2004, 134 s. ISBN 80-731-8165-7.**

Vedoucí diplomové práce: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Práce se zabývá problematikou dohledových, poplachových a příjímacích center, zejména pak jejich vzájemnou komunikací s ústřednami a možnostmi využití VPN protokolu pro jejich zabezpečenou komunikaci v síti Internet.

Klíčová slova:

DPPC, VPN, Internet, Bezpečnost komunikace, Bezpečnostní rizika

ABSTRACT

Abstrakt ve světovém jazyce:

The work deals with the alarm receiving centers, especially their communications with central security units and the possibilities of using VPN protocol for secure communications on the Internet.

Keywords: ARC, VPN, Internet, Security communication, Security risks

Rád bych poděkoval zejména vedoucímu práce Ing. Rudolfovy Drgovy za jeho výstižné připomínky, cenné podněty ke zlepšení a ochotu řešit vše, co bylo potřeba. Chtěl bych také poděkovat Martinu Vondrašovy z ČTÚ, který mi velice ochotně poskytl veškeré informace a vysvětlil mi problematiku stanovování poplatků za využívání radiových spekter. V neposlední řadě bych chtěl poděkovat všem, kteří mě podporovali při studiích a při vypracování této práce. Všem velmi děkuji.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Ve své diplomové práci se budu zabývat problematikou dohledových, poplachových a přijímacích center, zejména pak jejich komunikací s ústřednami se zaměřením na využití VPN. V teoretické části nejdříve shrnu legislativní požadavky s přihlédnutím k aktuálním normám týkajících se této problematiky. V praktické části se budu věnovat zpracování komunikačních kanálů z hlediska nákladů na jejich provoz a výstavbu v rámci České Republiky. Dále zpracuji komunikační cesty a využívané protokoly, včetně šifrování VPN. V závěru práce se budu věnovat rizikům spojeným s využíváním VPN a pokusím se naznačit další možný vývoj v oblasti komunikace na DPPC.

I. TEORETICKÁ ČÁST

1 CHARAKTERISTIKA DOHLEDOVÝCH POPLACHOVÝCH PŘÍJÍMACÍCH CENTER (DPPC)

Dohledové a poplachové přijímací centrum (DPPC) je dispečerské zařízení, vybavené výpočetní technikou, která vyhodnocuje poplachové a informační stavy z ústředen instalovaných ve střeženém objektu. Zprávy jsou na toto zařízení přenášeny různými způsoby (telefonní linkou, mobilní sítí, radiovou sítí, internetem atd.) DPPC slouží k vyhodnocování údajů přenášených z ústředen střežených objektů. Výstupy ze systému jsou zpracovány softwarem DPPC, který umožňuje podrobný přehled o stavu objektu a nabízí i další doplňkové služby pro snadnější práci dispečera a efektivní reakci na vznik daných událostí. Po vyhodnocení poplachového signálu se vyrozumí - dle smluvních podmínek: zákazník, oprávněná osoba, policie či havarijní služba, nebo se vydá pokyn zásahové jednotce k provedení předepsaných činností. Pokud dojde k narušení objektu, je tento prověřen výjezdovou skupinou. Elektronická forma ostrahy objektů je klienty preferována vzhledem ke snadné dostupnosti a relativně nízkým pořizovacím nákladům poplachových a zábranných a tísňových systémů (PZTS). [6]

1.1 Obecné požadavky na provoz DPPC

Základní funkcí DPPC je vyhodnocovat zprávy z bezpečnostních i jiných zařízení zákazníka, které tyto informace odešlou na tento pult. Operátoři DPPC pak provádí, dle typu události kroky, vedoucí k vyřešení přijaté zprávy dle smlouvy a směrnic dané služby. Dálková ochrana přes pult centralizované ochrany je v dnešní době jedním z nejspolehlivějších způsobů, jak ochránit majetek.

Kvalita poskytovaných služeb je závislá na rychlosti zásahu, profesionalitě zaměstnanců a technice přenosu dat. Správně provedený zásah je veden tak, aby byly na nejnižší možnou míru sníženy škody na napadeném objektu ze strany pachatele i ze strany zasahujících pracovníků. Velmi důležitý je důraz na ochranu života a zdraví všech účastníků zásahu. Rychlost zásahu je nejvíce ovlivněna dojezdovým časem, tedy dobou, kterou potřebuje vozidlo zásahové skupiny k přesunu z místa svého stálého stanoviště do místa napadeného objektu. Tuto dobu ovlivňuje řada faktorů, kdy většinu z nich nelze ovlivnit (hustota provozu, kvalita a charakter provozu, počasí atd.). Mimo tyto vlivy je důležitá také vzdálenost nejbližšího stanoviště zásahové skupiny. Právě zde se projevuje výhoda vlastních vozidel – stanoviště jsou rozmisťována tak, aby byla zákazníkům vždy co nejblíže.

Kvalita služeb také závisí na dobře definovaných a provedených postupech. Je důležité co nejvíce minimalizovat čas od vyhlášení poplachu do kontroly objektu, mít zpracovány velmi podrobné postupy, které musí každý pracovník dokonale znát a dodržovat. Má-li být zásah rychlý a hladký, nelze se spoléhat na improvizaci pracovníků. Jsou vytvářeny obecné a specifické scénáře (modelové situace), které jsou neustále zdokonalovány. Zaměstnanci jsou pravidelně přezkušováni nejen ze znalostí těchto postupů.

Bezúhonní a profesionální pracovníci jsou tedy další komponentou, jež je pro úspěšnou ochranu majetku naprosto nezbytná. Každý uchazeč o práci v zásahových skupinách musí splnit řadu kritérií (věk 21 let, trestní bezúhonnost, vlastnictví zbrojního průkazu a řidičského oprávnění, minimálně dvouletá praxe atp.). Mimo to je přísně zkoumána fyzická a psychická způsobilost k vykonávání činnosti. Pracovníci jsou pravidelně ze svých znalostí a dovedností zkoušeni a dále proškolováni k rozšíření potřebných profesních parametrů.

Volba správného způsobu přenosu dat z objektu na pult centralizované ochrany je podstatným rozhodnutím. Přenos dat musí splňovat základní požadavky: musí být kontrolovaný (přenosová cesta musí být odolná proti napadení pachatelem) a zprávu o poplachu je třeba co nejrychleji přenést na pult centralizované ochrany. Zařízení pro přenos dat musí být schopno předávat zprávy o všech stavech v objektu. [7]

K základnímu vybavení operačního střediska patří:

- homologovaný pult centralizované ochrany včetně záložního zdroje,
- speciální samostatné linky pro přenos signálů z PZTS objektů do DPPC,
- archivační počítač DPPC s provozní databází všech střežených objektů,
- zařízení pro komunikaci (základnová vysílačka, pevný a mobilní telefon),
- aktuální archiv protokolů všech výjezdů zásahové jednotky,
- aktuální archiv strážních listů fyzické ostrahy,
- dokumentace (manuály, objektové směrnice, metodické pokyny, atd.).

Personální podmínky:

Z hlediska personálního obsazení pracovišť DPPC je trvalý požadavek na obsazení odborně vyškoleným personálem.

Obsluha DPPC by měla splňovat tyto podmínky:

- umět řešit mimořádné situace,
- umět pracovat ve stresu a v časové tísni,
- znát DPPC po technické a provozní stránce,
- umět komunikovat,

Požadavky na členy zásahových jednotek:

- disciplinovanost.
- fyzická zdatnost,
- perfektní znalost metodiky zásahu,
- znalost místopisu střežených objektů,
- zběhlost a zkušenost při používání zbraně a ostatních donucovacích prostředků.

[6]

1.2 Integrace v provozování DPPC

Poskytovatelé služeb DPPC musí řešit otázku, zda DPPC centralizovat (integrovat) na minimum pracovišť, řešit přenos dat centrálně a zásahové jednotky pracovišť DPPC mít rozmístěné po celé ČR. Jde o diskutabilní otázku, vyhovující převážně ekonomicky i personálně silným firmám. Poplachovou informaci lze přenášet na velké vzdálenosti a to bleskově. Centralizací lze ušetřit náklady na personál dispečinku i technické náklady na zbudování DPPC. Zásahová jednotka pak musí být co nejblíže objektu, ve kterém je zaznamenáván poplach. Problém spočívá v ekonomické efektivitě neboli vytíženosti. Velké firmy průmyslu komerční bezpečnosti jsou často v mylném domnění, že když vybudovaly nákladný technicky moderní DPPC, musí mít větší inkaso poplatků, než zásahová firma v místě poplachu, což může být i firma čítající jen dvě desítky pracovníků. Každopádně pro centralizaci svědčí zlepšující se přenosové cesty, čemuž vyhovují jak sítě pevných telefonních linek, tak sítě mobilních operátorů a internetu. [7]

1.3 Služby na DPPC

Služby na DPPC u soukromých agentur jsou postaveny na komerčním základě. Provozovatelé nabízejí různé nabídky služeb, které se liší postupem dispečera po příjmu poplachové informace a samozřejmě také cenou. Konkurence je velká, a proto je třeba nabízet zákazníkům služby tzv. na míru. Zde jsou uvedeny některé z příkladů služeb nabízených bezpečnostními agenturami. Pochopitelně se služby mohou prolínat nebo doplňovat.

- **Monitoring**

Základní nabídka služeb obsahuje vždy monitoring stavu bezpečnostního systému. Tato služba zaručuje sběr, vyhodnocení a archivaci příchozích zpráv. Pokud je přijata poplachová nebo jiná zájmová zpráva, operátor DPPC předá tuto informaci na předem domluvené telefonní čísla zákazníka v daném pořadí. Je potom na zákazníkovi, zda situaci na objektu prověří sám anebo vydá příkaz k výjezdu zásahové skupiny DPPC. Při telefonních hovorech lze po domluvě ze strany zákazníka využívat i předem domluvených hesel pro identifikaci osoby, která rozhoduje o způsobu prověření poplachu.

- · **Zásah**

Zásah znamená, že výjezdová skupina na základě poplachové zprávy jede na místo ověřit situaci, případně provést preventivní či represivní opatření v rámci zákona. Zásah je téměř vždy službou spojenou s monitoringem, protože lze těžko reagovat ne něco, o čem nevíme. Zásahová skupina je vedena k cíli operátorem DPPC a ten jim také předává aktuální informace o stavu v objektu.

Provozovatelé DPPC mají dva přístupy k této službě. První z nich je, že v měsíčním paušálu jsou zahrnuty i případné všechny výjezdy k objektu. Ve druhém případě zákazník platí za každý výjezd.

Druhý případ je vhodnějším prostředkem jak zákazníka naučit být pozorným při obsluze bezpečnostního systému protože 90 % výjezdů je na základě poplachu způsobeného pracovníky zákazníka.

Postupy reakce dispečera můžou být různé dle smlouvy. Reakcí může být volání kontaktních osob, čekání na zrušení poplachu platným kódem či heslem, vyslání výjezdové skupiny po uplynutí intervalu pro zrušení, nebo okamžitý výjezd.

- **· Patrol**

Patrol systém je preventivní nástroj ochrany objektů, je to v podstatě namátková fyzická ostraha. Provádí ho výjezdová skupina DPPC. Jde vlastně o využití zásahové jednotky v době, kdy neprovádí zákrok na základě poplachové informace. Je to nástroj jak lépe využít času pracovníků zásahové jednotky v době jejich pohotovosti a zároveň zlepšit ekonomické výsledky.

Služba funguje tak, že výjezdová skupina v době své služby provádí dle harmonogramu preventivní kontroly stavu objektů a jejich okolí. Celá tato služba má preventivní charakter a působí na okolí podvědomím, že objekt není úplně bez kontroly. V případě přijaté poplachové zprávy je Patrol systém přerušen a prioritu má výjezd k napadenému objektu. V činnosti Patrol systému potom hlídka pokračuje, pokud není vytížená kontrolou poplachů na hlídaných objektech.

- · **Doplňkové služby**

Doplňkovými službami provozovatel DPPC v podstatě vylepšuje komfort placených služeb. Jedná se například o vyrozumění odpovědné osoby, pokud není objekt v určitou dobu zastřežen. Je možné také zasílat SMS zprávy o stavu objektu. Například informace o tom, kdo a v kolik odemkl a zamkl objekt. Umožňuje-li to technické zařízení na objektu klienta, je možné provádět z dispečinku DPPC vzdálenou správu elektronických zařízení (topení, klimatizace, osvětlení atd.), taktéž je možné informovat klienta o výpadku elektrické energie nebo poruchy telefonní linky.

Velmi rozšířenou službou jsou pravidelné měsíční nebo týdenní výpisy z historie objektu, zasílané poštou nebo v elektronické podobě. Ve výpisu jsou obsaženy všechny informace, které z daného objektu na DPPC přišly. Je možné sledovat docházku do objektu, otevírací dobu mimo pracovní přístup zaměstnanců atd.

Jednou z nejrozšířenějších služeb je kontrola odkódování a zakódování objektu. Jde o službu, která klientovi umožní pomocí DPPC kontrolu svého objektu, zda došlo k aktivaci či deaktivaci PZTS v danou chvíli. V praxi to znamená, že v případě nezakódování objektu do stanoveného času je klient telefonicky informován, popř. SMS. U objektů, kde je vyšší riziko, či na přání klienta je možné okamžitě vysílat zásahovou skupinu. Mezi další služby patří písemná zpráva o provedeném zásahu, kontrola automatických testů, funkční zkoušky PZTS, prověření objektu v případě výpadku spojení při použití radiové sítě, rady a nabídky z praxe. Na DPPC lze také provozovat dálkový dohled pomocí kamerového systému

CCTV, pokud jím střežený objekt disponuje. Dohled lze provádět v případě přijatého poplachu přímo v dané místnosti, anebo v pravidelných intervalech.

- · **Servis**

Pokud je provozovatel DPPC zároveň i dodavatelem bezpečnostních systémů, může zákazníkovi nabídnout v rámci zvýšeného měsíčního paušálu služby za DPPC také non-stop servis bezpečnostního zařízení. V praxi to znamená, že v případě servisních hlášek na DPPC operátor DPPC vyrozumí technika, který sám zákazníkovi nahlásí poruchu a domluví termín opravy. Zákazníkovi tak odpadá starost o kontrolu funkčnosti systému. Technik by měl být v pohotovosti 24 hodin tak, aby bylo možno provést okamžité opravy i v mimopracovní dobu.

- · **Ostraha**

Ostraha se využívá v případě reálného napadení objektu. Výjezdová skupina provede zásah a v případě skutečného napadení objektu informuje zákazníka a Policii ČR. Provozovatel DPPC byl měl mít v záloze i pracovníky fyzické ostrahy, kterou je potřeba na místě zajistit do příjezdu zákazníka, popřípadě do začátku pracovní doby zaměstnanců v objektu. Fyzická ostraha je nutná, pokud po pachateli zůstaly škody na majetku např. rozbité dveře či okna. Nebo v případě zajištění stop popř. pokud není systém PZTS plně funkční. I tato služba by měla být sjednána v rámci smlouvy.

Většina provozovatelů DPPC v průmyslu komerční bezpečnosti nabízí služby od zajišťování fyzické ostrahy, montáže PZTS, CCTV až po převozy hotovostí a cenin. Zákazník se pouze rozhoduje, kterou ze široké škály služeb využije pro ochranu svého majetku. [6]

1.4 DRUHY DPPC

1.4.1 Autonomní nezávislé zařízení tzv. Reky

Jsou samostatná zařízení, která obsahují záložní zdroj a jsou schopna samostatného provozu, po určitou dobu) např. 12 hodin i bez napájení 230V. Rek většinou obsahuje sloty pro různé moduly – telefonní linková karta, ISDN karta, radiokarta, karta pro tiskárnu. Jednotlivé karty mají svoji vnitřní paměť až na 2000 událostí, pro případ výpadku, nebo servisního zásahu ne REKU. Tím že nevyužívají žádný operační systém, jsou velmi spolehlivé a málo náchylné k „padání“ systému. Na čelní straně takového reku většinou najdeme ovládací a programovací klávesnici a display. Zprávy jsou zobrazovány na displeji a při příchodu rovněž tisknuty on-line na tiskárně protože displeje reků jsou max. dvouřádkové a zprávy by se ztrácely. Nevýhodou reků je, že zobrazují zprávy v číselném formátu, chybí jim textový překlad, proto jsou méně adresné a rozklíčování číselného kódu zabere čas. Obsluha při příchodu zprávy musí podle pomocné dokumentace zjistit podle číselné řady, o jaký objekt se jedná, jaký typ zprávy je signalizován a případně z které zóny je hlášen poplach. Provoz jen takového typu DPPC omezuje používání libovolných překladových tabulek pro bezpečnostní ústředny. Měl by být dodržen postup, že například kódy začínající 3. jsou vyhrazeny pro poplach (u všech objektů) tak aby bylo pro obsluhu hned jasné, jaký typ zprávy zpracovává. Složitější to je ovšem u velkokapacitních ústředen, které mají například 256 zón. Potom nastává problém jak jednoduše vytvořit programovací tabulku pro přenosové zprávy. [8]

Nicméně tato zařízení se v dnešní době již nepoužívají, jelikož jejich použití není příliš komfortní a při rozsáhlých systémech DPPC je již téměř nelze využít. Zmiňuji je jen proto, že patří neodmyslitelně do historie těchto systémů. V současné době většina DPPC center pracuje na PC architektuře, kterou rozeberu níže.

1.4.2 PC architektura

Jsou systémy běžící na architektuře současných jak desktopových, tak serverových hardwarových komponent. V případě tak důležitého systému jako je DPPC se předpokládá využití kvalitních serverových komponent včetně redundantních a záložních zdrojů, pro případ výpadku elektřiny. Na tomto HW je nainstalován operační systém a příslušný software DPPC od libovolného dodavatele (Kronos NET, NAM, SIMS atd.)

Do této stanice se vkládají rozšiřující karty pro potřebnou komunikaci s PZTS (telefonní, rádiová, GSM/UMTS, ADSL. Případně mohou být tato zařízení připojena externě pomocí rozhraní v PC (USB, RS-232, 485)

Instalovaný software komunikuje s ústřednami pomocí vybraných komunikačních kanálů.

Tento systém nám poskytuje nejen možnost zpracovávat velké množství zpráv najednou, díky rychlosti dnešních PC systémů, ale umožňuje nám hlavně přehledné zobrazení potřebných kanálů na obrazovkách. Díky tomuto komfortu dispečerského pracoviště jsme schopní velice rychle a efektivně reagovat.

Navíc při dnešních cenách serverových komponent není třeba uvažovat o používání HW určeného pro stolní PC, což by se nemuselo vyplatit nejen z důvodu stability a nemožnosti redundance.

2 NORMY TÝKAJÍCÍ SE DPPC

2.1 Legislativa

Protože každý návrh, realizace a provoz bezpečnostní technologie musí respektovat platné normy, byly donedávna všeobecné požadavky pro poplachové zabezpečovací a tísňové systémy upraveny normou ČSN EN 50131-1. Vlastní přenos signálů a základní zásady provozu DPPC pak byly řešeny normami řady ČSN EN 50136, zejména technickými normami ČSN EN 50136-2-2 a ČSN EN 50136-1-4. Na poplachové zabezpečovací systémy se dále vztahují některé další technické normy z hlediska požadavků na elektromagnetickou kompatibilitu (ČSN EN 50081 a ČSN EN 50082), elektrickou bezpečnost (ČSN EN 61140ČSN 33 2000-4-41), telekomunikační a rádiové zařízení (ČSN ETS 300 065 ED.1). V současné době, respektive s platností od 1. ledna 2011, jsou dohledová a poplachová přijímací centra řešena normami ČSN EN 50518-1, ČSN EN 50518-2 a ČSN EN 50518-3.

2.2 Normativní zásady provozu

Norma ČSN EN 50518-1 se vztahuje na veškerá dohledová a poplachová přijímací centra. Stanovuje minimální požadavky na návrh, konstrukci a funkční zařízení pro budovy, v nichž se uskutečňuje monitorování, příjem a zpracování (poplachových) signálů generovaných poplachovými systémy jako integrální část celkového procesu zajištění bezpečí a zabezpečení. Dohledové centrum tak musí například splňovat předepsanou sílu zdí, okna s balistickou a požární odolností, detekční zařízení plynu, dostatečné množství bezpečných datových úložišť, komunikačních tras a hardwaru, jakož i automatizovanou zálohu napájecích okruhů pro případ velkoplošného výpadku elektrického proudu. Požadavky normy se vztahují jak na případy dálkové konfigurace, v nichž více systémů přenáší informace do jednoho nebo více poplachových přijímacích center, tak na případy jediného centra určeného pro monitorování a zpracování poplachů generovaných jedním nebo více poplachovými systémy, nalézajícími se v tomtéž perimetru příslušného místa. Dále jsou v ní uvedeny stavební požadavky na dohledová centra z hlediska odolnosti proti napadení, proti požáru a na ohodnocení rizik.

Norma ČSN EN 50518-2 se vztahuje na veškerá dohledová a poplachová přijímací centra (DPPC), která monitorují, přijímají anebo zpracovávají signály, jež vyžadují okamžitou

reakci. Norma stanovuje technické požadavky, zahrnuje funkční kritéria a ověřování výkonnosti.

Norma ČSN EN 50518-3 stanovuje požadavky na personál, pracovní postupy a provoz dohledových poplachových center. Dále specifikuje požadavky na výcvik, bezpečnostní prověření a lustraci personálu, v neposlední řadě pak požadavky na testování center, správu databází a likvidaci údajů, řízení nouzových stavů, evakuačních postupů a audit poplachových dohledových center. [9]

3 KOMUNIKAČNÍ KANÁLY NA DPPC

3.1 Jednotná telefonní síť (JTS)

Po tomto médiu je dnes přenášeno nejvíce zpráv na DPPC. Velké rozšíření těchto druhů přenosů sebou přinesla hlavně dostupnost a cena. V objektech, kde se instalována PZTS je ve většině případů přítomnost telefonní linky. Tato se první připojí do ústředny PZTS a následně se z ústředny PZTS vytvoří připojení pro koncové zařízení. Takovéto připojení je vždy nutno dodržet, aby byla splněna podmínka priority vysílání informací ústřednou na DPPC. Tam kde je například pobočková telefonní ústředna musí být signál veden do PZTS a následně teprve do telefonní ústředny. Tímto řešením je umožněno běžné používání telefonní linky pro hovory. V případě, že dojde na ústředně PZTS k události, tato zajistí přerušení stávajícího hovoru – uvolní si linku, pokud není volná – po dobu nezbytně nutnou předá informaci DPPC a znovu linku uvolní pro další použití. Další důvod rozšíření přenosu po telefonní lince je to, že každá ústředna PZTS má v sobě zabudovaný telefonní komunikátor nutný pro přenos na DPPC a proto odpadají dodatečné náklady na pořízení zařízení (radiovysílač, GSM brána) nutného pro přenos po jiných přenosových kanálech, které se pohybují přibližně od 10 do 20 tisíc.

Nevýhodou přenosu po JTS je zejména nemožnost kontroly spojení – přenosové cesty a to díky nákladům za telefonické spojení. Běžně se využívá testu spojení 1x za 24 hodin. Je třeba si uvědomit, že předání zpráv dochází na základě sestaveného telefonického spojení DPPC. Proto lze říct, že co událost nebo balík událostí je vlastně telefonní hovor. Díky tarifikaci operátorů stojí přenesení informace např. „o zamčení“ zákazníka 2,80 Kč, protože tarifikace je dána za započatých 120 sec, i když samotné přenesení takové zprávy trvá cca 10-30 sec.

Na straně DPPC jsou telefonní linky zapojené do zařízení DPPC (telefonní karty). Využívají se minimálně dvě linky. Nastavení je takové, že když jedna telefonní linka je obsazena příjmem informací z objektu A a na toto číslo se pokouší předat informaci objekt B je telefon přesměrován na volné telefonní číslo DPPC. Provozovatelé DPPC by měli zajistit utajení telefonního čísla zapojeného DPPC (nezveřejnění v telefonním seznamu), aby zamezili zlomyslnému volání a tím blokování linek DPPC. V poslední době provozovatelé mohou využívat tzv. virtuální barevné linky ve formátu 842 xxx xxx, které umožňují softwarovým nastavením vytvářet směrování. To znamená, že při dovolání na první tel. číslo v případě jeho obsazení dojde ve zlomku sekundy k překlopení na druhé

telefonní číslo atd. Tím se zamezí prodlení předání zprávy na DPPC a zvýší se možná průchodnost komunikačních kanálů. Barevné linky jsou vlastně virtuální čísla, pod kterými existují fyzicky telefonní čísla a přípojky JTS na straně objektu. Používáním těchto linek je také operátorem zvýhodněno tarifikací 1,80Kč/30 sec. A následně je účtováno po vteřině. Jsou provozovatelé DPPC, kteří využívají barevných linek s vyšší tarifikací např. 11,- Kč/1 sec s tím, že operátor mu následně vrací např. 40% hovorného do zákazníků. Je to obdobné jako u placených audiotextových služeb. [8]

3.2 ADSL – datový přenos

V dnešní době se čím dál častěji používá přenosů pomocí datového pásma linky, tento typ přenosu má nespornou výhodu v tom, že jsme schopní detekovat přerušení datového spojení na DPPC. Další výhodou je, že nedochází během komunikace k přerušení hovorové linky a tato komunikace probíhá současně a nezávisle na hlasových službách. ADSL přenos je dostupný na drtivé většině telefonních přípojek a je také velice dostupnou alternativou k připojení k DPPC z důvodu poměrně nízkých provozních nákladů. Tyto linky jsou zpravidla velice stabilní a v případě jejího selhání můžeme využít komunikaci s ústřednou pomocí mobilní sítě nebo jiné metody dostupné na ústředně. V drtivé většině poskytovatelů jsou poskytovány časově a datově neomezené tarify, které nám negenerují žádné další náklady nad sjednaný paušální poplatek. V dnešní době již je většinou nějaká forma připojení do sítě internet využívána a tudíž je toto připojení využíváno i pro jiné účely než je připojení na DPPC. V případě, že na lince běží současně více druhů komunikace, je nutné uplatňovat pravidla QOS (Quality of service), tak, aby byla prioritní komunikace na DPPC. Tento proces může být realizován upřednostněním konkrétní IP adresy ve firewallu hraničního směrovače, sloužícího k připojení do sítě nebo také klasickou prioritizací paketů.

3.3 Mobilní sítě (GSM/GPRS, UMTS/3G)

Pro přenos informací o objektu se také velmi často používá moderních sítí mobilních operátorů, které mají nespornou výhodu ve velkém pokrytí vysílači po celé České Republice a není problém připojit objekt téměř kdekoli. V případě, že není dostupná síť jednoho operátora, je zpravidla možné využít síť jiného, který je v dosahu. Pokud nastane situace, kdy není dostatečná úroveň signálu, je možné využít pro posílení signálu zesilovač, případně výkonnější anténu, pro dosažení požadované úrovně. V případě využití datové komunikace je samozřejmě výhoda obousměrné komunikace mezi pracovištěm

dispečinku a systémem instalovaným v objektu. Díky obousměrné komunikaci můžeme prakticky v jakémkoli intervalu kontrolovat funkčnost spojení. Bohužel v drtivé většině nabízených tarifů je velmi omezený počet dat, a z tohoto důvodu se nám nevyplatí kontrolovat spojení v intervalu kratším než 10 minut. U běžně velkého domu bychom si měli vystačit s datovým limitem 1GB. Tento tarif nabízí v současné době např. T-Mobile včetně samostatné sim karty za slušných 349Kč

3.4 Rádiové sítě

Nejdražší, ale také asi nejspolehlivější je vybudování vlastní radiové sítě, o kterou se stará a provozuje provozovatel DPPC. Jelikož se jedná o přístupovou radiovou síť, vyžaduje povolení a přidělení frekvenčního pásma od Českého telekomunikačního úřadu (ČTÚ). Tyto sítě fungují na frekvenci 400-470MHz

Jako příklad jsem zvolil radiovou síť Global a Global 2 od společnosti NAM systém a.s.

Charakteristika buňkových rádiových sítí Global a Global 2

Základní podmínkou pro fungování takovýchto sítí je, aby obsahovala dostatečný počet sběrných stanic. Sběrná stanice je inteligentní retranslační stanice, která hlídá spojení s jí přidělenými objekty a posílá dále všechny významové zprávy. Zároveň může pracovat jako objektové zařízení (vysílač). Sběrné stanice komunikují na 1 nebo 2 kmitočtech.

V sítích Global komunikují jak vysílače, tak i sběrné stanice na jedné frekvenci.

V sítích Global 2 komunikují na jedné frekvenci vysílače se sběrnými stanicemi a na druhé frekvenci probíhá komunikace mezi sběrnými stanicemi.

Sběrné stanice musí být umístěny na co nejvyšších místech s přímou viditelností na PCO. Je ekonomicky prokazatelné, že se cena jedné sběrné stanice zaplatí při instalaci 10 až 20 objektových vysílačů. Hlavními úsporami jsou nižší telekomunikační poplatky, snadná montáž a méně servisních zásahů z důvodu lepší kvality spojení.

V praxi může jedna sběrná stanice obsluhovat až 200 vysílačů. V zástavbě doporučujeme na čtverec 2x2 km namontovat jednu sběrnou stanici. Sběrné stanice mají vždy venkovní antény, umístěné nad okolním terénem (obdobně jako převaděče GSM telefonů). Potom se Vám nestane, že po namontování vysílače budete hledat spojení. Tento model je v praxi vyzkoušen a plně se osvědčil.

Základním typem vysílače v rádiových sítích Global a Global 2 je širokopásmový vysílač TSM 452W s výkonem 1 W. Výkon vysílače je skokově nastavitelný v rozsahu 0,1 až 1 W.

Pro objekty, které vyžadují vyšší vysílací výkon, jsou určeny širokopásmové vysílače TSM 454 W s výkonem 5 W. Taktéž výkon těchto vysílačů je skokově nastavitelný v rozsahu 0,5 až 5 W.

Výkony vysílačů se vždy nastavují na nejmenší dostatečný výkon pro spojení s nejbližšími dvěma sběrnými stanicemi. Toto zabezpečí provoz asi 2000 vysílačů na dvou frekvencích v lokalitě o průměru 60 km s možností kontroly všech objektů do 5 minut a s minimálními výpadky komunikace. Všechny objekty budou mít vnitřní antény.

3.4.1 Poplatky za rádiovou síť:

Poplatky za využívání radiových kmitočtů nám stanovuje Zákon o elektronických komunikacích č. 127/2005 Sb., který výrazně snížil poplatky za využívání radiových spekter. Tento zákon byl novelizován v roce 2012 zákonem 273/2012 Sb. Přičemž stanovování poplatků za využití radiového spektra zůstává beze změn. Výrazné snížení poplatků se dotklo především frekvenčně úsporných rádiových sítí, jakými jsou právě buňkové sítě Global a Global 2.

Pro orientaci zde uvádím výši poplatků podle nového zákona:

Rádiová síť v konfiguraci pevných stanic

Tab. 1 – Roční poplatky za radiovou síť v konfiguraci pevná stanice

Kmitočtové pásmo	**406,1-410 MHz**	**420-430 MHz**
Šířka kmitočtového kanálu	25 kHz	20 kHz
Počet pevných vysílacích stanic	**Roční poplatek**	**Roční poplatek**
1	4125	3300
5	5625	4500
50	22500	18000
100	41250	33000
150	60000	48000

Výše poplatků platí pro maximální vyzářený výkon vysílačů do 10 W

Výše těchto poplatků závisí na šířce kmitočtového pásma a vysílacím výkonu. Částka, která je vypočtena jako roční poplatek se skládá z části za přidělené radiové spektrum a poplatku za jednotlivou stanici. Výše poplatku za jednotlivé stanice závisí na vyzřeném

výkonu, přičemž maximální výkon je stanoven na 10W. Přidělování jednotlivých kmitočtů se řídí plánem pro využití radiového spektra. Radiové sítě pro komunikaci na DPPC spadají do pásma 380-470 MHz a řídí se částí plánu pro využití radiového spektra č. PV-P/15/02.2009-4.

Pro privátní radiové sítě komunikující s DPPC jsou dle informací z Českého telekomunikačního úřadu (ČTÚ) přiřazovány v současné době frekvence z pásma 406,1 – 410 MHz v požadované šířce pásma. Některé dříve vydané frekvence jsou z pásma 420-430 MHz, kde tyto zařízení již jen dožívají a nově jsou vydávány pouze v pásmu 406,1-410 MHz.

Z ČTÚ mi byl poskytnut neoficiální dokument v Excelu, ve kterém lze jednoduše stanovit výši ročních poplatků jednoduchým vyplněním tabulky. Ovládání samotného programu je velice jednoduché a uvádím stručný návod pro stanovení poplatků. Tento dokument je možné volně šířit jako neoficielní pomocný nástroj.

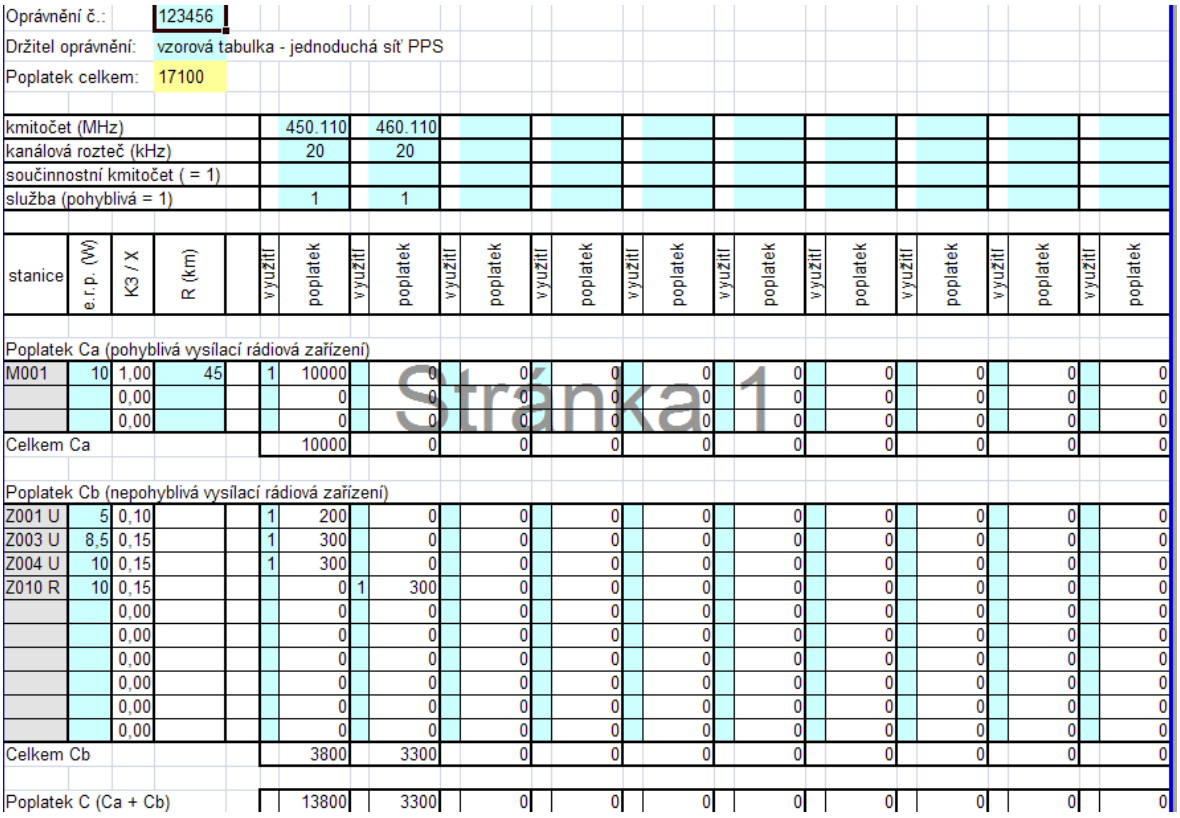
Psát lze pouze do modrých políček. Jsou zde dvě části:

- pro mobilní pohyblivou službu s definovaným rádiusem působnosti v oblasti, který má vliv zejména na maximální hodnotu poplatku, vysílacím výkonem a využitím
- pro nepohyblivé vysílací rádiové zařízení s definovaným vysílacím výkonem a využitím

Při využití těchto tabulek je nutné využít tabulku o správném počtu řádků, pro požadovaný počet kmitočtů. Jelikož nemůže být využito více tabulek a následně jejich součet. Všechny stanice se musí vejít do jedné tabulky, jinak by nebyl stanoven poplatek korektně.

Pokud se nějaký parametr potvrzuje, vloží se do modrého políčka číslo 1 (=ano). Tj. pro PPS je 1, pro např. spojení bod-bod nechat prázdné.

Obr. 1: Ukázka z programu pro výpočet poplatků za radiovou síť



Oprávnění č.:	123456																				
Držitel oprávnění:	vzorová tabulka - jednoduchá síť PPS																				
Poplatek celkem:	17100																				
kmitočet (MHz)					450.110		460.110														
kanálová rozteč (kHz)					20		20														
součinnostní kmitočet (= 1)																					
služba (pohyblivá = 1)					1		1														
stanice	e.r.p. (W)	K3 / X	R (km)		využití	poplatek	využití	poplatek	využití	poplatek	využití	poplatek	využití	poplatek	využití	poplatek	využití	poplatek	využití	poplatek	využití	poplatek
Poplatek Ca (pohyblivá vysílací rádiová zařízení)																					
M001	10	1,00	45		1	10000		0		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
Celkem Ca						10000		0		0		0		0		0		0		0		0
Poplatek Cb (nepohyblivá vysílací rádiová zařízení)																					
Z001 U	5	0,10			1	200		0		0		0		0		0		0		0		0
Z003 U	8,5	0,15			1	300		0		0		0		0		0		0		0		0
Z004 U	10	0,15			1	300		0		0		0		0		0		0		0		0
Z010 R	10	0,15				0	1	300		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
		0,00				0		0		0		0		0		0		0		0		0
Celkem Cb						3800		3300		0		0		0		0		0		0		0
Poplatek C (Ca + Cb)						13800		3300		0		0		0		0		0		0		0

Vybudování této sítě ovšem přináší obrovskou finanční náročnost jak na straně provozovatele, tak na straně zákazníka, který si musí zakoupit, případně pronajmout vysílací zařízení pro připojení na DPPC.

3.5 Celosvětová síť Internet

V dnešní době existuje celá řada možností připojení do této celosvětové sítě, v úvodu této kapitoly jsem zmínil ADSL linku. V dnešní době se využívají stále častěji optické sítě, které jsou budovány nejen na rozlehlých sídlištích, ale vzhledem ke stále nižší pořizovací ceně i na vesnicích.

Samozřejmě nesmím opomenout zmínit všudypřítomné WIFI sítě, se kterými se setkáváme prakticky na každém rohu. Bohužel v některých lokalitách je to jediná možnost rozumného připojení k této síti. Zpravidla jsou WIFI sítě budovány ve volných pásmech a tudíž nám hrozí vysoké riziko možného zarušení jiným zařízením a tím znemožnění komunikace.

Vzhledem k široké využitelnosti této sítě, nebývá zpravidla investice do paušálu za neomezené připojení k internetu pouze pro potřeby DPPC, ale také pro klasické prohlížení webových stránek a dalších služeb. Opět jako u ADSL je samozřejmě nutné

nakonfigurovat směrovač, tak, aby byly upřednostňovány pakety na DPPC před ostatním provozem na síti.

3.5.1 Shrnutí jednotlivých typů připojení na DPPC

Tab. 2 – Shrnutí nákladů, charakteristiky a výhod jednotlivých typů přenosů

Radiový vysílač	Telefonní linka	Internet ADSL,VDSL/ GPRS, UMTS
Charakteristika: **Bezdrátové připojení nejvyšší kvality. Vysílače jsou homologovány rovněž pro přenos poplachů požárních systémů (EPS).**	**Charakteristika:** Nejběžnější způsob napojení. Telefonní komunikátor obsahuje většina ústředen EZS v základním vybavení.	**Charakteristika:** Moderní a efektivní drátové připojení s vysokou spolehlivostí a bezdrátovou záložní cestou GPRS. Komunikace s PCO pomocí datových sítí, SMS, GSM. Splňuje požadavky kategorie 4 tj. nejvyšší rizika (dle AČR)
Porovnání: + pravidelná kontrola spojení v intervalu 5-10 minut + rychlý přenos informací + obtížná sabotáž přenosu + homologováno pro EPS - vysoká pořizovací cena, nízké provozní náklady - Vysoké náklady na vybudování sítě	**Porovnání:** nulové pořizovací náklady, + možnost využití stávající vybudované infrastruktury - vysoké provozní náklady - příchozí telefonní linka nebývá vždy dobře chráněna proti poškození	**Porovnání:** + pravidelná kontrola spojení v intervalu: internet 2 min., GPRS 10min. + nízké provozní náklady + pořizovací náklady jsou přijatelné a díky levnému provozu se rychle vrátí + pomocí záložní komunikační cesty lze dosáhnout vysoké spolehlivosti připojení k PCO
Zřízení: 5-20000 Kč Někdy možnost pronájmu k ceně měsíčního paušálu¨	**Zřízení:** 0 Kč	**Zřízení:** 5-10000 Kč
Provozní náklady měsíčně: žádné někdy platba za přenesená data poskytovateli sítě	**Provozní náklady měsíčně:** Minutové hovorné dle paušálu 300-1000Kč	**Provozní náklady měsíčně:** Měsíční paušál 300-1000 Kč

II. PRAKTICKÁ ČÁST

4 KOMUNIKAČNÍ CESTY A PROTOKOLY VYUŽÍVAJÍCÍ VPN

4.1 Co je to VPN?

V anglickém originále je to „Virtual private networks“ (VPN), v češtině přeloženo jako „virtuální privátní sítě. V praxi se jedná v podstatě o použití tulenovacích protokolů a bezpečného šifrování komunikace mezi dvěma, případně více sítěmi.

VPN nám zajišťuje vytvoření jakési virtuální soukromé sítě na již existující veřejně přístupné síťové infrastruktuře, tak, aby bylo možné bezpečně komunikovat mezi subjekty.

VPN sítě jsou vytvářeny na základě použití specializovaného softwaru, hardwaru případně jejich kombinace.

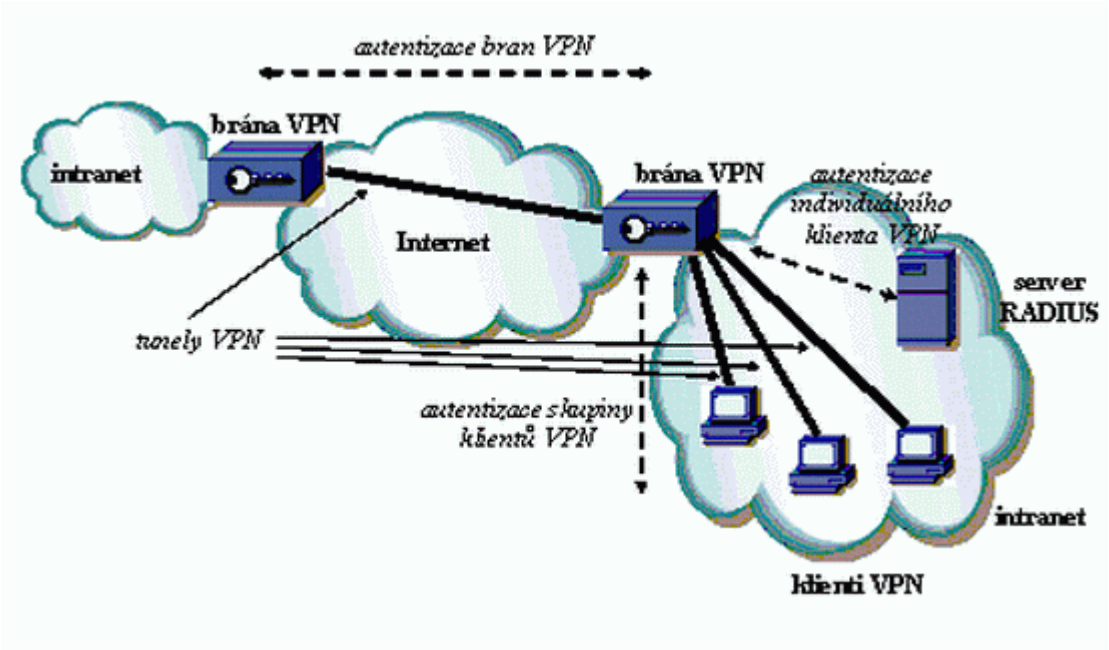
Hlavním důvodem pro vytváření VPN tunelů je požadavek na zabezpečení soukromé komunikace prostřednictvím veřejné sítě, zpravidla internetu. Problémem je nutnost při vytvoření tunelu tzv. vytáčení a vytvoření samotného tunelu, toto není problémem, pokud se jedná o vytvoření pár desítek tunelů. V případě, že se počty tunelů budou dostávat k jednotkám tisíců, je již poměrně značný problém v použitém hardwaru, samozřejmě pokud budeme mít centrální pobočku, na kterou se nám bude připojovat několik tisíc uživatelů najednou, nemůžeme očekávat, že nám to vydrží nějaký obyčejný směrovač připojený prostřednictvím ADSL linky. Tyto masivní aplikace si žádají proprietární řešení v podobě výkonných směrovačů, které mají optimalizaci a dostatečný výkon pro tunelování tisíců VPN.

4.2 Autentizace VPN

Pro navázání bezpečné komunikace se využívají mechanizmy autentizace (ověřování totožnosti komunikujících stran ve VPN) a řízení přístupu (autorizace pro přístup k privátním síťovým prostředkům).

Autentizace ověřuje totožnost dvou koncových bodů VPN a uživatelů posílajících zprávy přes VPN. Koncovým bodem může být klient VPN, brána VPN nebo směrovač či firewall. Autentizace probíhá na několika úrovních (viz obrázek 1): vzájemná autentizace bran VPN a autentizace klientů VPN vůči branám VPN, která může probíhat ve dvou úrovních - autentizace skupiny klientů VPN sdílejících stejné tajné heslo (typicky při propojení pobočkových intranetů) a následně autentizace jednotlivého člena skupiny individuálním heslem za využití serveru RADIUS (Remote Authentication Dial-In User Service). [16]

Obr. 2: Autentizace VPN [16]



U VPN propojující více lokálních sítí, by mělo být heslo unikátní pro každý tunel. Všeobecně by se měly dodržovat zásady bezpečnosti pro tvorbu a obměnu hesla. Heslo by mělo obsahovat malé velké písmena, nemělo by obsahovat lehce uhodnutelné fráze, případně slovníkové hesla. Bezpečné heslo by mělo mít alespoň 14 znaků a mělo by se alespoň 1x měsíčně měnit. Samozřejmě v případě desítek, stovek či tisíc tunelů, je to administrativně náročné. Tento problém řeší digitální certifikáty, které jsou unikátní pro každé spojení. Správce sítě, má v případě uniknutí certifikátu možnost jej zneplatnit.

4.3 Šifrování VPN

Šifrování zajišťuje bezpečnost přenášených dat skrze tunely VPN. Chrání je před případnou modifikací během přenosu, či jejich podvržení. Využívané metody šifrování v rámci VPN tunelů:

- Hash funkce – Secure Hash Algorithm (SHA), Message Digest (MD5) – tyto funkce jsou zpravidla používány pro uložení hesla v bezpečné (nečitelné) formě
- Algoritmus symetrické kryptografie – International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES, 3DES), používají se pro šifrování probíhající komunikace z důvodu jejich nízké náročnosti na výpočetní výkon a snadného využití v reálném čase

- Algoritmus asymetrické kryptografie – River, Shamir and Adlerman (RSA) – využívá se hlavně pro přenos tajného klíče pro symetrickou šifru z důvodu vysokého stupně zabezpečení komunikace

4.4 Komunikační cesty

4.4.1 Celosvětová síť Internet

V dnešní době je v podstatě nejvyužívanější centrální přenosovou trasou tato síť, ke které je možné se připojit pomocí spousty různých technologií.

4.4.2 Komunikační cesty pro připojení k internetu:

4.4.2.1 Optické vlákno

Je skleněné nebo v dnešní době nejvíce využívané plastové vlákno, které je schopné přenášet světelný paprsek ve směru osy. Na bázi optických vláken je dnes postavena celá páteřní síť internetu a rychlosti na těchto technologiích sahají až k 100 Gbit/s. Standard pro tuto rychlost byl vyvinut teprve nedávno a to v roce 2010. Takováto rychlost se využívá opravdu jen na nejvytěžovanějších spojích v rámci největších serveroven v Evropě. V České republice tuto technologii využívá například sdružení NIX.CZ.

Samozřejmě nižší rychlosti jsou dnes běžně dostupné i normálním smrtelníkům a jsou hojně využívány lokálními poskytovateli internetu k připojení domů a svých uzlů. Ve Zlíně máme například firmu Internext s.r.o. Která má vlastní rozsáhlou síť v rámci několika měst a také jako jedna z mála má kapacitu 2x10Gbit/s do pražského datacentra, které je napojeno na ostatní datacentra v zahraničí.

4.4.2.2 Připojení přes pevnou linku ISDN/ADSL/VDSL

Toto připojení se vyvíjí již několik desetiletí, nejdříve jsme měli možnost využívat vytáčené připojení k internetu, které bylo analogové, tento způsob měl maximální rychlost 56kbit/s. Po několika letech tato technologie byla nahrazena technologií ISDN.

ISDN byla již plně digitální, ale měla stále časovou tarifikaci a u nás se příliš neuchytila, z důvodu finanční náročnosti, ale ve své podstatě se již jednalo o širokopásmové stálé připojení. Zde jsme se dostali na maximální rychlost 128kbit/s v případě dostupnosti dvou kanálů. K připojení pomocí ISDN byla potřeba ISDN ústředna. Tato technologie

umožňovala zároveň využívat tel. Linku, a internetové připojení. V poměrně rychlém časovém horizontu přišlo plnohodnotné ADSL.

ADSL toto připojení je nejčastěji využívaný typ DSL (Digital Subscriber Line – technologie umožňující využití stávající vedení telefonu pro vysokorychlostní připojení k internetu) toto připojení má několik standardů, lišících se v dostupné maximální rychlosti pro upload a download. Nejvyšší rychlost v rámci standardu ADSL2+ download 28Mbit/s a upload 3,5Mbit/s. Bohužel s rostoucí vzdáleností k ústředně tato rychlost nepříjemně klesá. Maximální vzdálenost je cca 8km. Nástupcem této technologie je VDSL.

VDSL oproti předchozímu ADSL má několikanásobný nárůst v maximální rychlosti v obou směrech. VDSL využívá širší šířku pásma a to až 30 MHz. Zde je daleko větší propad rychlosti na vzrůstající vzdálenosti od ústředny. Maximální rychlost je 100Mbit/s, ale tato rychlost je pouze teoretická a lze ji dosáhnout v ideálním případě do vzdálenosti 300m. V současné době je nejvyšší nabízená rychlost na trhu až 40Mbit/s za 606Kč (Telefonica O2), ovšem této rychlosti je v podstatě díky nastavení agregace nemožné.

4.4.2.3 WIFI

Vzhledem k rychlosti modernizace a vysoké ceny připojení ADSL, se naskytla možnost právě této technologii využívající volné mikrovlnné pásma nejdříve v kmitočtech 2,4GHz a nyní nejpoužívanější 5GHz.

Tyto sítě za posledních 10 let prodělali mnohé změny, které se projevovali hlavně ve vývoji nových standardů. Tento typ připojení se u nás ujal nejvíce asi z důvodu relativně nízké ceny za připojení, která byla téměř poloviční než připojení přes telefonní linku. Díky tomuto se klientům z dlouhodobého hlediska vyplatila investice do dražších zařízení v počátcích této technologie, byly poskytovány rychlosti okolo 1Mbit/s přičemž maximální rychlost byla 11Mbit v případě 802.11b. V dnešní době není výjimkou nabízená rychlost okolo 30Mbit/s a to převážně díky rozšiřování 802.11n. Níže pro srovnání uvádím tabulku používaného standard 802.11 a maximálních teoretických rychlostí.

Tab. 3: Přehled standardů IEEE 802.11 [11]

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]
původní IEEE 802.11	1997	2,4	2
IEEE 802.11a	1999	5	54
IEEE 802.11b	1999	2,4	11
IEEE 802.11g	2003	2,4	54
IEEE 802.11n	2009	2,4 nebo 5	600
IEEE 802.11y	2008	3,7	54
IEEE 802.11ac	2013	5	1000
IEEE 802.11ad	2014	2,4 , 5 a 60	7000

4.4.2.4 Mobilní datové sítě GPRS/UMTS (2G, 3G, 4G)

Další z možností komunikačních cest jsou technologie používané mobilními operátory k zajištění hlasových a datových sítí. Toto odvětví prodělalo za poslední léta taktéž obrovské množství změn, vývoj nových technologií a standardů. Tyto sítě jsou provozovány na různých kmitočtech, které přiděluje ČTÚ v různých dražbách. V rámci ČR máme poměrně uzavřený trh, o čemž svědčí i letošní tahanice okolo dražby nových pásem a puštění dalšího operátora na trh. U nás jsou využívány kmitočty GSM 900/1800MHz a UMTS 2100 MHz. Dle standardů rozlišujeme sítě na několik generací a to 2G, 3G, 4G.

Přičemž ve většině měst jsou rozšířeny sítě 3G. V současné době se dostávají do provozu také sítě 4G LTE (Mladá Boleslav – T-Mobile), u kterých je zatím testována maximální rychlost a stabilita. Jedná se v podstatě o pilotní projekty. Nicméně zařízení podporující tento typ vysokorychlostní sítě neustále přibývá a velcí hráči na našem trhu mají v plánu touto technologií pokrýt velká města a snad se dočkáme i rozšíření do menších měst. Jednotlivé generace sítí se vyznačují především zvyšující se rychlostí datové komunikace. Přehled jednotlivých generací uvádím v následující tabulce.

Tab. 4: Přehled jednotlivých generací a technologií [12]

Označení generace	**2G**	**2.5G**	**2.75G**	**3G**	**3.5G**	**3.75G**	**3.9G**	**4G**
Název technologie	CSD, HSCSD	GPRS	EDGE, CDMA 1xRTT	UMTS, CDMA 1xEV-DO	HSPDA	HSUPA	LTE	LTE-Advanced WiMax-2
Název mobilní sítě	GSM	GSM	GSM, CDMA2000	UMTS, CDMA2000	UMTS	UMTS	E-UTRAN	E-UTRAN, WiMax

Tab. 5: Přehled jednotlivých sítí, jejich maximálních rychlostí a max. vzdálenosti od vysílače [12]

Název technologie	**Rok uvedení**	**Přenosová frekvence**	**Maximální teoretická rychlost dat. Přenosu**	**Způsob přenosu dat**	**Max. vzdál. vysílače a přijímače**
GPRS (síť GSM)	1997	900/1800 MHz	80 kbps	Symetrický / Asymetrický	35 km
EDGE (síť GSM)	2004	900/1800 MHz	218/134 kbps	Symetrický / Asymetrický	30 km
1xRTT (síť CDMA2000)	2004	450-2100 MHz	307/153 kbps	Asymetrický	54 km
1xEV-DO (síť CDMA2000)	2004	450-2100 MHz	3.1/1.8 Mbps	Asymetrický	54 km
UMTS (W-CDMA) (síť UMTS)	2000	1885-2200 MHz	2048 kbps	Symetrický / Asymetrický	2 km
HSDPA (HSDPA+) (síť UMTS)	2004	873/1900 MHz	14.4 (42 Mbps)	Technologie pouze pro Downlink	6 km
HSUPA (HSUPA+) (síť UMTS)	2005	873/1900 MHz	5.76 Mbps (7.2 Mbps)	Technologie pouze pro Uplink	5 km
LTE (síť E-UTRAN)	2008	V Evropě obvykle 800, 1800, 2600 MHz	100/50 Mbps	Symetrický / Asymetrický	30 km

4.4.2.5 WIMAX

Další z možností bezdrátové komunikace nám poskytuje technologie WIMAX, jedná se o poměrně drahou technologii, která se u nás prosadila jen v menším měřítku. Nicméně se jedná o velice kvalitní technologii schopnou přenést poměrně vysoký objem dat. Výhodou tohoto systému je, že pracuje na frekvenčních pásmech, které podléhají licenci, a tudíž nám nehrozí téměř žádné rušení. Toho je dosáhnuto striktní politikou ČTÚ, při přidělování frekvencí. Technologii WIMAX nám definuje standard 802.16, který vznikl již v roce 2002 a definoval nutnost přímé viditelnosti ve frekvenčním pásmu 10-66 GHz. Maximální

rychlost byla při vysokých frekvencích až 134 Mbit/s. V roce 2003 přišla nová specifikace 802.16a, která přináší snížení frekvence u této technologie na 2-11 GHz, teoretický dosah při těchto frekvencích je 40-70 km. Snížením frekvence došlo také ke snížení přenosové kapacity na 70Mbit/s. Podstatným rozdílem mezi těmito dvěma specifikacemi je, že 802.11a nevyžaduje přímou viditelnost mezi stanicemi.

Obr. 3: Mobilní stanice WIMAX [11]

V současné době je technologie WIMAX zařazena do standardu mobilních sítí 4. Generace

Tab. 6: Používané frekvence pro WIMAX [11]

Frekvence [GHz]	Licencování
3,5	Licencované, mezinárodní pásmo
10,5	Licencované, mezinárodní pásmo
2,5 – 2,7	Licencované, USA, S. Amerika
2,4	Nelicencované, mezinárodní
5,725 – 5,825	Nelicencované, mezinárodní

4.4.2.6 Radioreléové mikrovlnné spoje (ALCOMA, SVM, ORCAVE, RACOM, SAF atd.)

Tyto spoje jsou využívány v mnoha odvětvích, využívají je jak mobilní operátoři, tak poskytovatelé internetu, státní sektor i armáda. Tyto spoje pracují jak v licenčním tak bezlicenčním pásmu 10-80 GHz a přenosové kapacity se pohybují od 10Mbit/s až po 2,5 Gbit/s. Tyto spoje jsou konstruovány pro spoje typu bod-bod. Obecně platí, že čím vyšší frekvence tím vyšší přenosová rychlost, ale zase čím vyšší frekvence tím nižší použitelná vzdálenost pro danou přenosovou kapacitu. Tyto spoje jsou konstruovány jako:

- IDU - skládá se z vnitřní jednotky, která je propojena koaxiálním kabelem s anténou.
- ODU – za anténou je umístěna vysílací jednotka a jsou pevně spojeny v jeden celek, napájení je řešeno obvykle po Ethernet kabelu CAT 7

Ceny těchto jednotek začínají na několika desítkách tisíc a končí v řádech milionů.

Obr. 4: Radioreléové mikrovlnné spoje ALCOMA [13]

4.4.2.7 Optická pojítka FSO (LaserBit, TereScope, Ronja, MRV, SONAbeam atd.)

Tento typ komunikačního zařízení využívá v podstatě dva základní principy komunikace:

- Laserové pojítka
- Infračervené spoje

Tyto spoje dokážou v současnosti přenést obrovské množství dat, ale bohužel vzhledem k nutnosti přímé viditelnosti, pouze na krátkou vzdálenost. Tyto spoje jsou konstruovány na vzdálenosti do 2km. Nicméně se nedoporučuje dělat takto dlouhé spoje bez adekvátní zálohy, jelikož při hustém dešti nebo mlze, jsou tyto spoje nepoužitelné. Konstrukčně jsou taktéž řešeny jako pojítka bod-bod. Mají téměř nulovou latenci, a proto jsou také na krátké vzdálenosti využívány. V dnešní době snižování ceny výstavby optických sítí, se od nich pomalu upouští, jelikož bezpečnější a lepší je vybudovat na takto krátkou vzdálenost optickou trasu. Tyto spoje jsou schopny poskytnout kapacitu až 10Gbit/s ovšem pouze na vzdálenost 850m. Tyto profi spoje se šplhají do řádů milionů a z tohoto důvodu je lepší vybudovat optickou trasu. Nicméně do oblastí, kde není možné jiné řešení, jsou i tyto spoje alternativou.

Obr. 5: FSO pojítko od společnosti MRV

4.4.3 Intranet

Tato síť běží v podstatě na stejných komponentách jako internet, ale není připojena k veřejné síti Internet a slouží převážně jako vnitropodniková komunikační síť. V této architektuře je také možné využít výhody VPN tunelů, ale v případě tohoto modelu, je poměrně zbytečné jej využívat. Jediné využití by bylo v případě nemožnosti přímé komunikace mezi dvěma subjekty anebo snaha o skrytí komunikace a přenášených dat v rámci intranetu.

4.5 Protokoly využívající VPN na síťové vrstvě

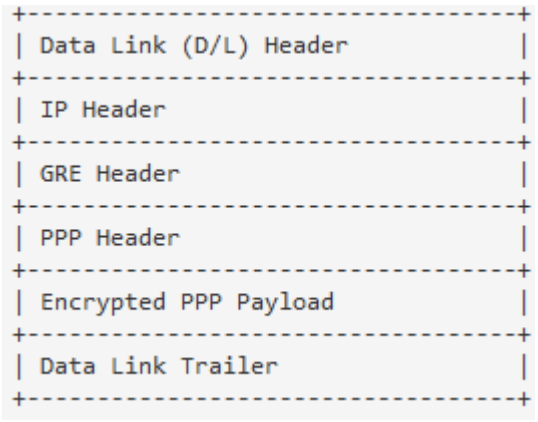
4.5.1 IPoverIP

Tento protokol definuje tunelování přímo IP protokolu, které se využívá prakticky při všech sestaveních VPN tunelu. Jeho nespornou výhodou je možnost tunelovat neveřejnou síť, aby probíhala korektně komunikace. Toto je základem každého VPN tunelu.

4.5.2 GRE

Tento protokol byl původně vyvinut společností CISCO, cílem bylo vytváření tunelů skrze jiné protokoly. Tento protokol nevyžaduje, aby přenosový protokol byl IP. Tento protokol se využívá ve spojení s protokolem PPTP. Protokol GRE je využíván k zapouzdření paketu

Obr. 6: Formát paketu protokolu GRE [14]



4.5.3 PPTP (Point-to-Point Tuneling)

Tento typ tunelu byl uveden na trh společností Microsoft, a je podporován na všech verzích Windows, samozřejmě je kompatibilní i s ostatními operačními systémy. Využívá buď autentizační metodu MSCHAP-v2 který může být ovšem narušen pokud uživatelé zvolí slabá hesla do 10 znaků.

V tomto případě, pokud se útočníkovy podaří odchytit heslo v šifrované podobě, je možné jej v reálné době prolomit na běžném hardwaru. V případě silných hesel se nemusíme u tohoto protokolu obávat jeho prolomení.

Další možností autentizace je pomocí EAP-TLS, které využívá certifikátu k ověření identity.

4.5.3.1 Zranitelnost PPTP

Firma Counterpane Internet Security, založená Brucem Schneierem (mj. spoluautorem šifrovacích technologií Blowfish a Twofish), zveřejnila informace o zranitelnosti protokolu PPTP. Dle Schneiera a Mudge, kteří se podrobně zabývali implementací PPTP od společnosti Microsoft, je autentizační protokol slabý a je napadnutelný slovníkovým útokem. Většinu hesel lze bezproblémově odhalit během několika hodin a problém se týká obou typů šifrování (40-bitového i 128-bitového). Mimo to lze v návrhu nalézt i řadu dalších chyb, díky kterým lze proti možnému šifrování vést další útoky. Není problém zneužít mechanismus dohody spojení v PPTP a otevřít si tak jeho spojení. Proti uživatelům PPTP od Microsoftu se tak snadno dá vést několik vážných útoků s odepřením služeb. [15]

4.5.4 L2TP (Layer 2 Tunneling protocol)

Tento typ tunelu je v podstatě vychází ze standardu L2F (Layer 2 Forwarding) od společnosti CISCO a protokolu PPTP od Microsoftu, tento protokol má lepší vlastnosti než jeho předchůdce. Navíc je při jeho použití možné použít standardizovaný protokol pro šifrování IPSec, potom mluvíme o L2TP/IPSec. Výhodou tohoto protokolu je silné šifrování a dvojí autentizace. Ovšem velkou nevýhodou jsou jeho problémy s NAT (Network Adress Translation) Jediná možnost, jak zprovoznit L2TP/IPSec na NATované síti je podpora směrovače NAT-T (IPSec NAT Travelstar), kterou ovšem nemají levné SoHo (Smal Office Home Office) směrovače.

L2TP využívá dva základní typy uzlů:

- **LAS (L2TP Access Concentrator**) – klient protokolu L2TP, přístupový koncentrátor sítě. Vytváří tunel mezi serverem a uzly koncentrátoru LAS pro přenos PPP rámců jednotlivých uzlů do vzdálené sítě.
- **LNS (L2TP Network Server)** – je server protokolu L2TP, který v rámci tunelů zřizuje relace pro jednotlivá koncová zařízení připojená k přístupovému koncentrátoru.

4.5.5 IPSec (IP Security)

Šifrovací protokol využívající různé kryptografické technologie, které zajišťují důvěrnost (např. šifrování DES, 3DES, AES), integritu (hashováním MD5, SHA) a autentizaci. Je to v současné době jedno z nejbezpečnějších řešení v oblasti VPN

4.5.5.1 Princip činnosti

Vytváří logické kanály – *Security Associations* (SA), které jsou vždy jednosměrné, pro duplex se používají dvě SA.

Bezpečnostní rozšíření vypadá následovně:

Ověřování – při přijetí paketu může dojít k ověření, zda vyslaný paket odpovídá odesilateli či zda vůbec existuje.

Šifrování – obě strany se předem dohodnou na formě šifrování paketu. Poté dojde k zašifrování celého paketu krom IP hlavičky, případně celého paketu a bude přidána nová IP hlavička.

Základní protokoly (jsou často používány zároveň, protože se vzájemně doplňují):

Authentication Header (AH) – zajišťuje autentizace odesílatele a příjemce, integritu dat v hlavičce, ale vlastní data nejsou šifrována.

Encapsulating Security Payload (ESP) – přidává šifrování paketů, přičemž vnější hlavička není nijak chráněna a není zaručena její integrita. [11]

4.6 Protokoly využívající VPN na transportní a aplikační vrstvě

4.6.1 SSL (Secure socket layer)

Tento typ protokolu využívá, asymetrického a symetrického šifrování, k ověření totožnosti před samotným přenosem je používán princip asymetrické kryptografie (použití veřejného a privátního klíče). Po autentizaci je spojení šifrováno pomocí symetrických šifer (DES, 3DES, AES, Blowfish atd.) z důvodu malé výpočetní náročnosti. Integritu přenášených dat poté zajišťují hashovací funkce (MD5, SHA).

SSL umožňuje bezpečnou komunikaci vzdáleného uživatele přes veřejnou síť internet. Využívá se jako alternativa k VPN IPSec, SSL VPN pracující na aplikační vrstvě je ovšem slabší z hlediska zabezpečení, jelikož nešifruje veškerou komunikaci, ale pouze některé aplikace typu client-server.

Řešení pomocí SSL má nespornou výhodu v nákladech na provoz, šifrování zajišťuje samotná aplikace, ve které je SSL implementováno. SSL se spíše hodí pro šifrování komunikace běžící na webovém rozhraní, případně e-mailu nebo sdílení souborů.

SSL VPN se většinou využívá pro připojení většího množství klientů k firemnímu serveru. Díky možnosti centrální správy klientských přístupů pomocí LDAP (Active Directory) či RADIUS serveru apod. Je jednoduché ověřit přístup pomocí uživatelského jména a hesla. Tyto aplikace nám přináší pohodlnou správu všech uživatelů.

Obr. 7: IPSec a SSL VPN

5 RIZIKA SPOJENÁ S VYUŽÍVÁNÍM VPN

Při připojování do podnikové sítě prostřednictvím VPN technologie je nutné brát v úvahu také rizika, která vznikají využíváním tunelování. VPN se využívá hlavně z důvodu úspory nákladů a možnosti připojení se do podnikové sítě pokud možno odkudkoli. Při této komunikaci je nutné řešit zejména otázky důvěrnosti a integrity dat a informací.

5.1 Všeobecná rizika VPN přístupu

5.1.1 Riziko uživatelského přístupu

VPN nám poskytují velice snadný přístup z Internetu do podnikové sítě, interních databází apod. Bezpečnost VPN tunelu je pouze tak silná jako použité metody k ověření uživatele přistupujícího pomocí vzdáleného VPN připojení. Jednoduché metody zabezpečení prostřednictvím statických slabých hesel umožňují použít metody slovníkových útoků, odposlouchávání komunikace případně využití sociálního inženýrství. Dvou faktorová autentizace je minimálním požadavkem pro bezpečnou autentizaci uživatelů. Tato autentizace spočívá ve dvou faktorech pro ověření přístupu, při kterém uživatel „něco“ ví (jméno a heslo) a „něco“ má (USB token, RFID karta, generátor jednorázových hesel apod.). Díky použití nějakého hardwarového prvku je pro případného útočníka téměř nemožné získat přístup k uživatelskému účtu aniž by si toho uživatel všiml. V případě hardwarových tokenů, by jej musel uživateli odcizit, čehož by si s největší pravděpodobností uživatel všiml. V některých specifických případech je možno využít také tří faktorovou autentizaci, která spočívá ve využití třetího prvku a to biometriky (např. otisky prstů, duhovka apod.)

5.1.2 Riziko nezabezpečeného počítače

Vzdálený přístup je velkou hrozbou zabezpečení sítě. Každý počítač, ze kterého se přistupuje do firemní sítě, by měl splňovat požadavky na zabezpečení stanovený firmou. Jelikož nedostatečně chráněný počítač by mohl při připojení do vnitropodnikové sítě začít šířit různé viry, červy trojské koně do vnitřní sítě. Přes tyto kanály by se mohla zhostit citlivých dat neoprávněná osoba. Minimálně by měla být provedena kontrola poslední aktualizace antiviru, před přístupem do podnikové sítě z neznámého zařízení.

5.1.3 Riziko rozděleného tunelování (Split tuneling)

Tento případ nastává, pokud vzdálený počítač komunikuje s privátní a veřejnou sítí zároveň aniž by veškerou komunikaci probíhající VPN tunelem ukončila. Toto je příležitost pro útočníky využívající zranitelnosti sdílené sítě a vzdáleného přístupu k PC. Skrz tento počítač poté mohou využít přístup do vnitřní sítě opakovaně.

Proti tomuto riziku je v podstatě jednoduchá ochrana a to nastavení VPN tunelu tak aby veškerá komunikace probíhala prostřednictvím VPN tunelu. Toto má všem také limity v podobě zpravidla nízkého uploadu připojení a tudíž komunikace s internetem, která bude probíhat skrz bránu ve vnitropodnikové síti, bude značně zpomalena. Nicméně obrovskou výhodou je, že komunikace bude probíhat přes hraniční směrovač podnikové sítě, kde jsme schopni danou komunikaci prohnat bezpečnostními filtry. Veškerá komunikace podléhá bezpečnostní politice podniku.

5.2 Rizika SSL VPN tunelů

Tyto rizika jsou ve své podstatě „větší“ nežli u jiných tunelů z důvodu přistupování zpravidla pomocí webového prohlížeče.

5.2.1 Nedostatečné zabezpečení počítače

SSL VPN umožňuje přístup do podnikové sítě prostřednictvím téměř jakéhokoli počítače. Veřejně dostupný PC nemusí mít zcela v pořádku softwarové vybavení, např. antivirový software, vypnutý nebo chybějící firewall. Pokud dojde k využití takového stroje pro přístup ke kritickým aplikacím, můžou být jeho prostřednictvím šířeny viry, červy či jiná „havěť“. Můžou být také využity pro tzv. backdoor, což je bezpečnostní díra pro přístup útočníka. V takovém případě selže i silná autentizace pro ochranu sítě, jelikož útočník se „přilepí“ na živou relaci prostřednictvím Trojana a zaměří se na vnitřní síť.

5.2.2 Keylogery

Zařízení nebo program určený pro zachycení stisknutých kláves. SSL VPN klientské počítače mohou být náchylnější k programům zaznamenávajícím stisky kláves, případně na umístění hardwarového keylogeru. Hlavně v případě přístupu z veřejně dostupných počítačů. Takováto zařízení nesplňují bezpečnostní požadavky pro připojení do podnikové sítě. Keylogery velice snadno dokáží zachytit kompletní přístupové údaje do sítě.

5.2.3 Man in the middle útok

Při tomto typu útoku, útočník zachytí ověření uživatele a další informace. Útočník pak používá tyto informace k přístupu k vnitřní síti. Během tohoto procesu útočník slouží jako proxy server, který podvrhne falešné VPN SSL, přes tuto bránu projde veškerá komunikace, přihlašovací údaje zadá uživatel na skutečný cílový web. V závislosti na propracovanosti falešného proxy serveru, jsou buď odeslána data ze skutečného serveru uživateli a komunikace probíhá, anebo je mu vrácena „Stránka není dostupná“

Tento útok zpravidla funguje, pokud uživatel není schopen ověřit důvěryhodnost serveru, na který přistupuje. Uživatel zpravidla nečte a neověřuje certifikát serveru a důvěřivě klepne na tlačítko „Ano“ a příjme nabízený certifikát natrvalo. V případě nastavené nízké úrovně zabezpečení prohlížeče, ani ten uživatele nevaruje před podvrženým certifikátem.

5.2.4 Hardwarové omezení

V případě dvou faktorové autentizace může uživatel narazit na problém, že v případě veřejně dostupného stroje jsou zakázány čtečky karet, či USB porty. V tomto případě nejde ani tak o riziko ve smyslu bezpečnosti přístupu, jako spíše o znemožnění přístupu k síti, v případě vysokého zabezpečení komunikace.

6 VÝVOJ V OBLASTI KOMUNIKACE NA DPPC

V dnešní době je již poměrně snadné připojit ústřednu na DPPC, otázkou je zabezpečení této komunikace. VPN tunelování řeší jak otázku zabezpečení, tak překonání NAT, které stávajícím systémům neumožňuje připojit se na DPPC z ústředny, které není přidělena veřejná IP adresa. Existují sice webové služby jako je www.paradoxmyhome.com, které sice umožňují připojení naší ústředny do internetu a její následnou správu, ale nikoli komunikaci s DPPC.

V letošním roce jsem se zúčastnil semináře pořádaného ÚNMZ Praha, kde se projednával nový americký standard pro komunikaci SIA DC-09, který řeší komunikaci s DPPC na úrovni struktury přenášené zprávy. Tento standard bude určitě v nejbližších letech implementován do značné části dodávaných řešení, jak na straně DPPC tak na straně ústředen. Jelikož je v současné době zpracováván do formy technické normalizační informace.

V budoucnosti by se měla dle mého názoru komunikace na DPPC pomocí veřejné sítě ubírat směrem VPN tunelů. Z mnou zpracovaných řešení mi vychází nejlépe využití SSL VPN z důvodu jeho jednoduchosti. Sice tento tunel není tak vysoce zabezpečený jako L2TP/IPSec, ale vzhledem k úskalím, která jsou potřebná pro správný chod a připojení pomocí L2TP/IPSec.

V případě použití dostatečně silných hesel o délce alespoň 14 znaků a dodržení základních zásad bezpečnosti by mohlo být dostatečné využití tunelů na bázi PPTP, které je nejsnáze propagovatelné skrz NAT a uzly, které nám stojí v cestě.

V dnešní době se již začíná pomalu přecházet na IPv6 adresy z důvodu vyčerpávání maximální kapacity IPv4 adres. U IPv6 je již IPSec implementován přímo v protokolu a tudíž by mělo dojít ke zjednodušení vytvoření komunikace. Nespornou výhodou IPv6 je také, že neobsahuje žádný NAT nebo cokoliv podobného. Jednoduše jsou prostě všechny adresy veřejné. V tomto případě již není potřeba vytvářet jakékoli virtuální tunely a prostě mezi dvěma směrovači zapneme šifrování pomocí IPSec. Tento nový adresní systém sebou přináší, další úskalí, která budou muset být v budoucnu řešena. Ale to je dle mého názoru otázka poměrně vzdálené budoucnosti.

ZÁVĚR

Po zpracování této diplomové práce jsem dospěl k několika závěrům.

Přenos poplachových zpráv na DPPC je v dnešní době velice aktuální a zatím je stále využíváno především jednotné telekomunikační sítě a GSM komunikátorů. V případě komunikace prostřednictvím internetu je nutné pro spojení využít veřejnou IP adresu, kterou nedisponují všechna internetová připojení. Z důvodu úspory veřejných adres je velice často využíváno NAT, k překladu adres na jedinou veřejnou. U některých poskytovatelů je nutné si za veřejnou IP připlatit. Někteří poskytovatelé nám ji poskytnou za jednorázový poplatek např. 50Kč někdy více, případně pouze na vyžádání. Ti, kteří chtějí vydělat více, si stanovují měsíční poplatek ke standardnímu paušálu za internetové připojení.

Nicméně musím podotknout, že někteří velcí hráči na poli internetového připojení mají již veřejnou IP adresu v rámci své služby pro každého zákazníka. V případě veřejné adresy je již pouze problematickým prvkem koncový směrovač u zákazníka, který musí být správně nakonfigurován tak, aby upřednostňoval komunikaci s ústřednami a přeposílal požadavky z WAN rozhraní na adresu komunikačního rozhraní ústředny. V dnešní době je již využíváno časově neomezené připojení, takže není nutno se omezovat v ověřování dostupnosti spojení.

V případě ADSL či GPRS/UMTS připojení je často poskytována veřejná IP adresa každému zákazníkovy. Vzhledem k rozšiřující se počítačové kriminalitě je nutné přenos zpráv na DPPC lépe zabezpečit. K tomuto zabezpečení a odstranění nežádoucích vlivů typu NAT a veřejné IP adresy nám slouží tunelování.

V dnešní době je dostupná široká škála protokolů tunelování využívaných pro VPN, některé bohužel mají problém právě s překonáváním NAT, které jsou jim po cestě vystaveny, dle mého názoru by bylo vhodné využít tunel PPTP vzhledem k jeho jednoduchosti a jednoduchému průchodu aktivními prvky, které mu stojí v cestě, jediná nevýhoda tohoto tunelu je nižší zabezpečení než u L2TP/IPSec. Ovšem při použití silných hesel, se riziko prolomení tohoto tunelu minimalizuje. Nevýhodou je nutnost použití směrovače, který nám bude vytáčet tento tunel.

V případě veřejné IP adresy od poskytovatele, je možnost využít také L2TP/IPSec, který je bezpečnější a dosud nebyl zaznamenán jeho průlom. Ovšem jeho použití sráží problémy s provozem na NAT, takže je vhodné jej použít pouze v místě s veřejnou IP adresou.

Pokud by se výrobci rozhodli integrovat VPN klienty do komunikačních modulů pro jejich ústředny, bylo by vhodné využít komunikační protokol VPN SSL, který je relativně snadný na implementaci a šifrování komunikace zprostředkovává server, na který se připojujeme, vzhledem k možnosti tunelovat pouze jeden port a nikoli celou komunikaci jako u předchozích tunelů se jedná o velice elegantní způsob spojení s DPPC.

Využití VPN tunelů pro komunikaci s DPPC vyžaduje taktéž výkonné směrovače na straně provozovatele DPPC, pro velkou většinu klasických směrovačů je velice obtížné mít otevřeno velké množství tunelů současně. Pro vzdálený přístup jsou na trhu speciální bezpečnostní brány (Security remote access), které umožňují tisíce až desetitisíce současných tunelů. Příkladem mohou být brány od společnosti CISCO série ASA 55xx, které jsou také stohovatelné a vrcholné modely této řady umožňují v rámci jednoho řešení až 50 000 současných tunelů.

VPN tunely jsou zajisté budoucností komunikace na DPPC, v dnešní době se již začíná rozšiřovat protokol IPv6, který má již v sobě zabudovánu funkci šifrování pomocí IPSec. Tento internetový protokol nezná žádné překlady adres, tím pádem jsou veškeré adresy veřejné a stačí pouze zapnout šifrování mezi dvěma body.

ZÁVĚR V ANGLIČTINĚ

After processing this thesis I have come to several conclusions. Transmission of alarm messages in ARC is nowadays very important, is still used primarily single telecommunication network and GSM communicators. In the case of communication via the Internet is required for the connection, use a public IP address, which does't have any Internet connection. The sake of saving addresses is very often used Network address translation to a single public. Some providers need to pay extra for a public IP. Some providers give it to us for a fee such as 50 CZK sometimes more, or only on request. Those who want to earn more, a fixed monthly fee for the standard fee for internet connection.

However, I must point out that some of the big players in the field of Internet connections have been public IP address as part of their service to each customer. In the case of a public address is already only problematic element end router at the customer service, who must be properly configured to give priority of communication with the control requirements and the messages were sent from the WAN interface to the address of the communication interface panel. Nowadays it is used by unlimited access so you do not need to be limited in checking the availability of the connection.

In the case of ADSL or GPRS / UMTS connection is often provided to the public IP address of each customer. Due to the growing cyber crime is necessary to transfer messages to the DPPC more secure. This security and remove unwanted influences the type of NAT a public IP address we can use tunneling.

Nowadays, it is available a lot of protocols used for VPN tunneling, some unfortunately have a problem just with overcoming NAT, which are exposed to them along the way, in my opinion it would be appropriate to use PPTP tunnel due to its simplicity and easy pass on active elements, which he stand in the way, the only downside of this tunnel is less secure than L2TP/IPSec. However, with the use of strong passwords, the risk of breaking this tunnel is minimized. The disadvantage is the need for a router that we will dial the tunnel.

In the case of public IP addresses from the provider, you can also use L2TP/IPSec, which is safer and has been achieved his breakthrough. Its recommended use it only with the public IP addresses. If the producers decided to integrate VPN clients into modules for their panels, it would be appropriate to use the communication protocol SSL VPN, which

is relatively easy to implement and provides encryption server to which you are connecting, due to the possibility of tunneling only one port and not a communication to the previous tunnel is a very elegant way to connect with DPPC.

Use of a VPN tunnel for communication with DPPC also requires performance routers on the operator's side of DPPC, for most conventional routers is very difficult to have a large number of open tunnels simultaneously. For remote access on the market are special routers for Security remote access, allowing thousands to tens of thousands of simultaneously tunnels. An example can be taken from Cisco ASA 55xx series, which are also stackable and top models in this series provide a single solution to 50,000 simultaneously tunnels.

VPN tunnels are certainly the future of communication DPPC, nowadays are starting to expand IPv6, which already has a built-in encryption function using IPSec. The Internet protocol hasn’t any address translation, therefore all addresses are public and you only need to turn on encryption between two points.

SEZNAM POUŽITÉ LITERATURY

[1] ČSN EN 50518-1. Dohledová a poplachová přijímací centra - Část 1: Umístění a konstrukční požadavky. Praha: Český normalizační institut, 2011.

[2] ČSN EN 50518-2. Dohledová a poplachová přijímací centra - Část 2: Technické požadavky. Praha: Český normalizační institut, 2011.

[3] ČSN EN 50518-3. Dohledová a poplachová přijímací centra - Část 3: Pracovní postupy a požadavky na provoz. Praha: Český normalizační institut, 2012.

[4] PALOVSKÝ, Radomír. Informační a komunikační sítě. Vyd. 1. Praha: Oeconomica, 2010. ISBN 978-802-4517-292.

[5] KINDL, Jiří. Projektování bezpečnostních systémů. 1. vyd. Zlín: Univerzita Tomáše Bati, 2004, 134 s. ISBN 80-731-8165-7.

[6] ZAPLETAL, Pavel. Perspektiva PPC. Univerzita Tomáše Bati ve Zlíně, 2009. UTB Zlín. Diplomová práce

[7] LAUCKY, V. *Technologie komerční bezpečnosti I.*. Zlin: Univerzita Tomaše Bati ve Zlině, 2004. 64 s. ISBN 80-7318-194-0.

[8] VYORÁLEK, R. Pulty centralizované ochrany. Zlín, 2005. 59 s. Univerzita Tomáše Bati ve Zlíně. Bakalářská práce.

[9] Bezpečnost s profesionály. Praha: KPKB ČR, 2013, roč. 2013, č. 1. ISSN 1805-854X.

[10] NAM system a.s. [online]. [cit. 2013-05-21]. Dostupné z: http://www.nam.cz/

[11] Wikipedie - otevřená encyklopedie [online]. [cit. 2013-05-23]. Dostupné z: https://cs.wikipedia.org/

[12] Technologie mobilního internetu – od CSD po LTE Advanced. [online]. 2012 [cit. 2013-05-23]. Dostupné z: http://www.internetprovsechny.cz/mobilni-internet-a-lte/

[13] ALCOMA a.s. [online]. [cit. 2013-05-21]. Dostupné z: http://www.alcoma.com

[14] Pomoc a podpora Microsoft[online]. [cit. 2013-05-23]. Dostupné z: http://support.microsoft.com/

[15] THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

[16] Bezpečnost ve VPN: IPSec versus SSL. [online]. 2006 [cit. 2013-05-27]. Dostupné z: www.dsl.cz/clanek/515-bezpecnost-ve-vpn-ipsec-versus-ssl

[17] Využití protokolu SSL pro vytváření VPN (2). [online]. 2004 [cit. 2013-05-27]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Vyuziti-protokolu-SSL-pro-vytvareni-VPN-2-452004

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARC	Alarm Receiving center - Dohledové poplachové přijímací centrum
DPPC	Dohledové poplachové přijímací centrum
IP	Internet protokol
VPN	Virtuální privátní síť
PZTS	Poplachový Zabezpečovací a Tísňový systém
ČR	Česká Republika
SMS	Krátká textová zpráva
CCTV	Kamerový systém
ISDN	Integrated Services Digital Network (Digitální síť umožňující přenos hlasu a dat současně
ADSL	Asymmetric Digital Subscriber Line (Asymetrická digitální síť umožňující přenos hlasu a dat)
PC	Osobní počítač
HW	Hardware
SW	Software
GSM	Global system for Mobile - Mobilní síť
GPRS	General Packet Radio Service - Datový přenos po mobilní síti
UMTS	Universal Mobile Telecommunications System - Datový přenos po mobilní síti – další generace
USB	Universal serial bus
JTS	Jednotná telefonní síť
QOS	Quality of service
NAT	Network adress translation
ČTÚ	Český telekomunikační úřad
PPS	Požární poplachový systém

WIFI	Wireless fidelity
PCO	Pult centralizované ochrany
AČR	Armáda České republiky
EPS	Elektronická požární signalizace
RADIUS	Remote Authentication Dial-In User Service
SHA	Secure hash algorithm
MD5	Message digest
IDEA	International Data Encryption Algorithm
DES	Data Encryption Standard
RSA	River, Shamir and Adlerman
WIMAX	Worldwide Interoperability for Microwave Access
FSO	Optická pojítka
PPTP	Point-to-Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
IPSec	IP security
GRE	Generic Routing Encapsulation
MSCHAP-v2	Windows Domain Controller Autentizace
EAP	Extensible Authentication Protocol
TLS	Transport Layer Security
SoHo	Small Office Home Office
SA	Security Associations
AH	Autentification Header
ESP	Encapsulating Security Payload
SSL	Secure Sockets Layer
LDAP	Lightweight Directory Access Protocol

RFID	Radio frequency identification
ÚNMZ	Ústav pro technicou normalizaci, meteorologii a státní zkušebnictví
IPv4	Internet protocol verze 4
IPv6	Internet protocol verze 6

SEZNAM OBRÁZKŮ

SEZNAM TABULEK