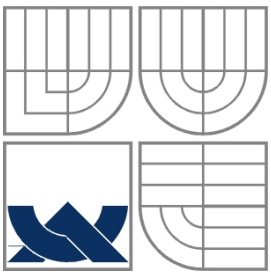
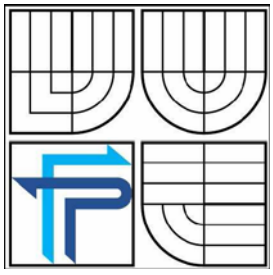


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

PROJEKT VPN PRO PŘÍSTUP KLIENTŮ DO KORPORÁTNÍ SÍTĚ OBCHODNÍHO ŘETĚZCE V REGIONU STŘEDNÍ EVROPA

PROJECT OF CLIENT-BASED VPN REMOTE ACCESS SOLUTION FOR THE WORLDWIDE RETAIL BUSINESS COMPANY IN THE REGION OF CENTRAL EUROPE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — RICHARD ONDRÁK
AUTHOR

VEDOUCÍ PRÁCE — Ing. JIŘÍ KŘÍŽ, Ph.D.
SUPERVISOR

BRNO 2008

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2007/08
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ondrák Richard

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Projekt VPN pro přístup klientů do do korporátní sítě obchodního řetězce v regionu střední Evropa

v anglickém jazyce:

Project of Client-based VPN Remote Access Solution for the worldwide Retail Business Company in the region of Central Europe

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BARTH, Wolfgang. Nagios - system and network monitoring. NO STARCH PRESS, 2006. 464 p. ISBN 1-59327-070-4.
DOSTÁLEK, Libor a kol. Velký průvodce protokoly TCP/IP: Bezpečnost - druhé aktualizované vydání. Computer Press, 2003. 592 s. ISBN 80-7226-849-X.
DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Computer Press, 2006. 536 s. ISBN 80-251-0828-7.
PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z, druhé aktualizované vydání. Computer Press, 2006. 423 s. ISBN 80-251-1278-0.
PUŽMANOVÁ, Rita. TCP/IP v kostce. KOPP, 2004. 607 s. ISBN 80-7232-236-2.

Vedoucí bakalářské práce: Ing. Jiří Kříž, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2007/08.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta podnikatelská

L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. Ing. Miloš Koch, CSc.
Děkan fakulty

V Brně, dne 15.2.2008

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Richard Ondrák

Bytem: Arnošta Valenty 670, 198 00 Praha 9

Narozen/a (datum a místo): 4.11.1979 v Brně

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta Podnikatelská

se sídlem Kolejní 2906/4, 612 00 Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

Ing. Jiří Kříž, Ph.D., ředitel Ústavu informatiky

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - □ diplomová práce
   - ■ bakalářská práce
   - □ jiná práce, jejíž druh je specifikován jako .....

   (dále jen VŠKP nebo dílo)

Název VŠKP:	Projekt VPN pro přístup klientů do korporátní sítě obchodního řetězce v regionu střední Evropa
Vedoucí/ školitel VŠKP:	Ing. Jiří Kříž, Ph.D.
Ústav:	Ústav informatiky
Datum obhajoby VŠKP:	červen 2008

VŠKP odevzdal autor nabyvateli v*:

- ■ tištěné formě – počet exemplářů 1
- ■ elektronické formě – počet exemplářů 1

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - □ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

…….... Nabyvatel

…… Autor

ABSTRAKT

Tato práce se zabývá problematikou vzdáleného přístupu klientů do korporátní sítě nadnárodního obchodního řetězce Tesco Stores v regionu střední Evropy. Na základě zhodnocení současných možností vzdáleného přístupu bude cílem práce navrhnout nové vhodné regionální řešení, které jednak nahradí všechny dosud používané systémy, a jednak splní všechny požadavky a zvyšující se nároky firemních uživatelů i dodavatelů. Řešení bude projektováno s ohledem zejména na bezpečnost, snadné použití, co nejméně náročnou správu systému a vhodné začlenění do IT infrastruktury firmy.

ABSTRACT

The aim of this Thesis is to project and describe new Client-based Remote Access Solution for the Tesco Stores retail company in the region of Central Europe. Based on facts that the all present Tesco's Remote Access Systems have not any longer met the increasing requirements and needs of corporate users and suppliers it is clear that the main scope is to find and implement such Solution that will meet and exceed all requirements. The main Project Aspects are to be the ease of use, security of the solution, unexacting administration of the system and user groups, and one unified Solution for the all Countries from the region of Central Europe that is suitably integrated in the Tesco IT infrastructure.

KLÍČOVÁ SLOVA

systém vzdáleného přístupu, VPN („virtuální privátní síť“), IPSec, IKE (Internet Key Exchange), zabezpečení, kryptování, autentizace, referenční model ISO/OSI, RADIUS server, ActiveDirectory, brána Firewall/VPN, Syslog, OWA, RAS, CITRIX/SWA, Certifikační autorita, RSA Secure ID, SLA, DMZ, LAN, WAN

KEYWORDS

Remote Access System, VPN (Virtual Private Network), IPSec, IKE (Internet Key Exchange), security, encryption, authentication, ISO/OSI model, RADIUS server, ActiveDirectory, Firewall/VPN gateway, Syslog, OWA, RAS, CITRIX/SWA, Certification Authority, RSA Secure ID, SLA, DMZ, LAN, WAN

BIBLIOGRAFICKÁ CITACE

ONDRÁK, R. *Projekt VPN pro přístup klientů do korporátní sítě obchodního řetězce v regionu střední Evropa.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2008. 78 s. Vedoucí bakalářské práce Ing. Jiří Kříž, Ph.D.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Dále prohlašuji, že citace použitých pramenů je úplná, a že jsem v práci neporušil autorská práva ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským.

V Brně dne 27.5.2008

Richard Ondrák

PODĚKOVÁNÍ

Děkuji Ing. Jiřímu Křížovi, Ph.D., za odborné vedení při vytváření této bakalářské práce, za podnětné diskuze a poskytnuté rady.

Dále děkuji svým nadřízeným a kolegům ve společnosti Tesco Stores ČR, a.s., za jejich podporu a toleranci k mým časově náročným studijním povinnostem a jejich skloubení s výkonem taktéž časově náročných pracovních povinností.

OBSAH

1. ÚVOD

Několik posledních desetiletí vývoje lidské společnosti je do značné míry ovlivňováno a směrováno masivním rozvojem informačních a komunikačních technologií a jejich pronikáním do běžného života společnosti. Využití jejich potenciálu znamená pro člověka především usnadnění a urychlení práce, proto je logické, že se tyto technologie uplatnily v největší míře v podnikání, jakožto hlavní nástroj zvyšování konkurenceschopnosti a zisku firmy. Můžeme říci, že čím větší je v dnešní době oblast podnikání firmy, tím komplexnější je využití IT technologií s cílem pro sběr, udržování a zpracování firemních dat. V případě takovýchto datových celků pak mluvíme o informačním systému firmy.

Je celkem zřejmé, že udržení takovýchto informačních systémů firmy v chodu a zachování dostupnosti dat má kritický vliv na zachování kontinuity podnikání, přežití společnosti a uplatnění na trhu. Časové nároky jsou v tomto ohledu značné. Nikoliv dny, ale hodiny či minuty rozhodují o úspěchu v dnešní společnosti. Logickým požadavkem managementu firem je tak absolutní dostupnost kritických podnikových dat 24 hodin denně. Touto úvahou se již dostáváme k problematice náplně této práce – vzdálenému přístupu různých skupin uživatelů do firemní sítě a informačního systému k firemním datům.

Dobře však víme, že není možné jen tak otevřít naše firemní informační systémy světu propojením firemní lokální sítě s internetem. Je třeba povolit přístup pouze autorizovaným uživatelům a zabezpečit systémy a data proti neoprávněnému přístupu. Vzdálený přístup jako takový je proto velmi citlivá oblast, která klade velký důraz na bezpečnost přístupu. I proto existuje mnoho různých typů přístupu a různých systémů a technologií, od publikování jednoho konkrétního systému až po přístup do celé firemní sítě (viz. kapitola 4).

Cílem prvních několika odstavců bylo kromě úvodu do problematiky dostupnosti podnikových informačních systémů, dat a vzdáleného přístupu k nim upozornit na potřebu být při výběru a plánování řešení vzdáleného přístupu do firmy velmi důkladný - kvalitně zanalyzovat požadavky, zmapovat současný stav v dané oblasti, zohlednit současné IT prostředí firmy, pečlivě navrhnout samotné řešení s ohledem na požadovanou funkčnost a především klást velký důraz na zabezpečení. A přesně to je náplní této práce.

2. VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Téma této práce bylo cíleně zvoleno jako aktuálně řešený projekt pro společnost Tesco Stores ČR a její organizačně podřízené jednotky v regionu střední Evropa (dále jen CE – Central Europe), tedy Tesco Slovensko, Tesco Polska a Tesco Maďarsko. Ve společnosti Tesco Stores ČR jsem zaměstnán, dříve jako Network specialista, nyní jako IT Security manager, a na své předchozí pozici jsem byl technickým vedoucím tohoto projektu.

Řešený projekt klade za cíl nalézt a navrhnout nový vhodný komplexní systém vzdáleného přístupu do korporátní sítě firmy v regionu CE, který by splňoval všechny stanovené požadavky, a to především plnou využitelnost dle potřeb důležitých skupin uživatelů - „business“ uživatelů, IT uživatelů a mnoha strategických IT dodavatelů.

Hlavní důvody jsou prosté. Vzdálený přístup k firemním informačním zdrojům je pro Tesco „business-critical“ službou. Nicméně nynější stav v této oblasti, tak jak bude analyzováno níže, je v regionu CE nedostatečný, a to jak z pohledu aktuálních požadavků firmy, tak z pohledu současných standardů a trendů. Velkou úlohu zde hraje taktéž otázka bezpečnosti stávajících systémů. Neméně důležitým faktorem jsou vysoké náklady na údržbu a správu stávajících systémů. Nový systém by měl nahradit minimálně jeden ze současně používaných systémů s cílem zmenšení nákladů na provoz nového systému oproti stávajícímu.

3. ANALÝZA SOUČASNÉHO STAVU

V této části práce si nejprve blíže představíme společnost Tesco Stores ČR, její postavení v rámci regionu střední Evropy, náhled na společnost z globálního hlediska, a také její stručnou historii. Posléze detailně přiblížím současný stav v oblasti vzdáleného přístupu včetně zhodnocení současných systémů. V poslední části kapitoly budou detailně rozepsány aktuální potřeby a požadavky společnosti na vzdálený přístup uživatelů k informačním systémům firmy, na základě kterých budu moci posléze navrhnout nové vhodné řešení.

3.1. Společnost

Společnost Tesco Stores je jedním ze tří největších mezinárodních maloobchodních řetězců světa působících ve 13 zemích na třech různých kontinentech, nabízející široký sortiment potravinového i nepotravinového zboží.

Tesco bylo založeno již v roce 1919 ve Velké Británii. K expanzi na zahraniční trhy však došlo až v 90. letech minulého století. V současnosti Tesco působí kromě Velké Británie a Irska především v mnoha zemích Asie, ve střední Evropě a krátce také v USA.

Do střední Evropy Tesco vstoupilo v roce 1996 koupí 13 obchodních domů od společnosti K-mart v České a Slovenské republice, a o rok dříve také vstoupilo na trhy Polska a Maďarska. Tyto čtyři země jsou posléze organizačně centralizovány pod region „Central Europe“ (střední Evropa – dále jen zkratka CE), a právě celý region CE je uvažován jako cíl projektu.

V současné době skupina Tesco provozuje celkem 3729 obchodů (z toho 747 v Evropě) a zaměstnává více jak 450.000 lidí. Jen v mateřské Velké Británii je aktuální stav 1878 prodejen a 237.000 zaměstnanců, čímž se Tesco stává největším zaměstnavatelem Velké Británie.

3.1.1. Základní údaje

Obchodní údaje o společnosti Tesco Stores ČR, a.s.

Obchodní jméno:	Tesco Stores ČR, a.s.
Právní forma:	akciová společnost
Základní kapitál:	12.906.802.000,- Kč (splaceno 100%)
Datum zápisu do O.R.:	23.3.1992 (původně K-mart, koupí K-martu došlo ke sloučení pod jméno Tesco Stores ČR v 09/1995)
Identifikační číslo:	453 08 314
Sídlo:	Praha 10, Vršovická 1527/68b, PSČ 100 00
Předmět podnikání:	39 evidovaných předmětů podnikání, z nichž nejvýznamnější je koupě zboží a prodej

Orgány společnosti – představenstvo (statutární orgán) a dozorčí rada

Předseda představenstva: Philip James Clark

Významné údaje pro ČR

- Aktuálně Tesco provozuje v ČR 98 obchodů – 55 hypermarketů – z toho 11 hypermarketů bývalého Carrefour, 37 supermarketů (do velikosti prodejní plochy 1.000m^2), 6 obchodních domů, 14 čerpacích stanic, 3 sklady pro různý typ zboží, a několik centrálních kanceláří.
- Tesco zaměstnává v ČR aktuálně 13.700 lidí
- rapidně rostoucí nabídka výrobků vlastní značky – nyní více jak 2.700

Základní údaje pro ostatní země regionu CE:

- *Slovensko* 5 obchodních domů, 44 hypermarketů, 11 supermarketů, 2 sklady; 8.200 zaměstnanců
- *Maďarsko* 76 hypermarketů, 37 supermarketů – z toho 14 bývalých NorthWest store, a 4 sklady; více jak 13.000 zaměstnanců
- *Polsko* v Polsku Tesco zaměstnává více jak 25.000 lidí
  76 hypermarketů, 42 supermarketů, 3 sklady, 21 benzínek; v roce 2007 Tesco v Polsku koupilo celou síť prodejen LP, a tím se počet obchodů vyšplhal na nynějších 257

Hospodářské výsledky za fiskální rok 2007

- obrat v Evropě vč.DPH vzrostl o 23,9% na 7,836 mld. GBP (306,78 miliard Kč) se ziskem 397 mil. GBP (15,54 mld. Kč)

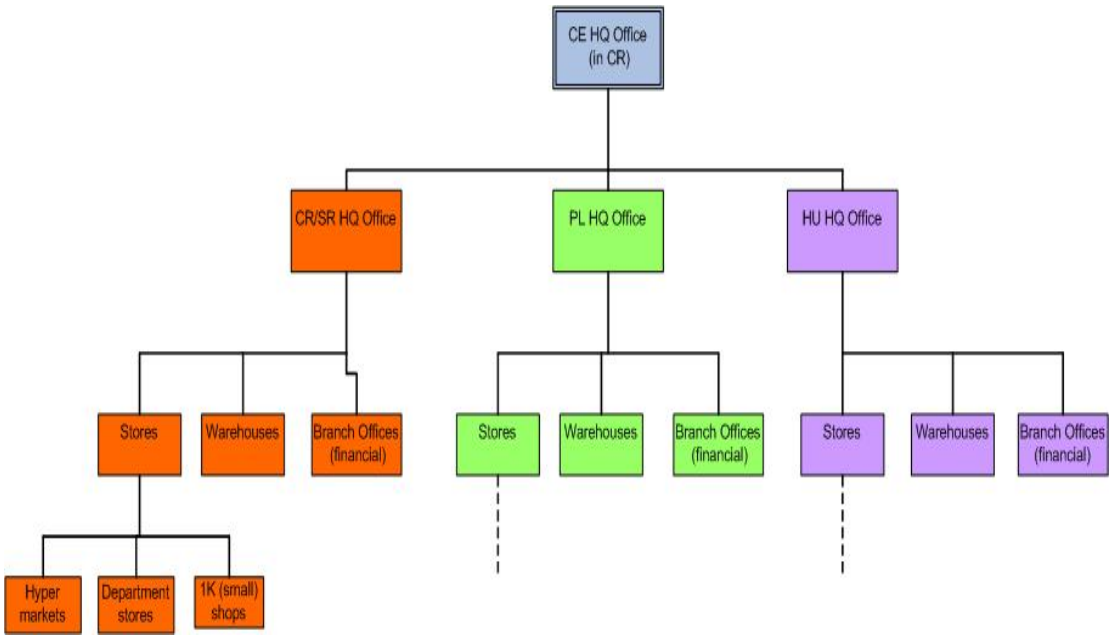
- obrat ve Velké Británii vč.DPH vzrostl o 6,7% na 37,9 mld. GBP (1,68 bil. Kč) se ziskem 2,05 mld.GBP (80,26 mld.Kč)
- obrat skupiny Tesco vzrostl o 11,1% na 51,8 mld. GBP (2,03 bil.Kč) se ziskem 2,85 mld.GBP (111,58 mld.Kč)
- obrat v ČR bez DPH vzrostl o 23% na 38,879 mld. Kč

3.1.2. Struktura společnosti v regionu CE

Pro návrh jakéhokoliv nového IT systému je důležité mít více či méně podrobný přehled o organizačním uspořádání v cílové společnosti, aby navrhovaný systém tuto strukturu plně reflektoval. Mezi podstatné důvody patří například správné nastavení uživatelských práv, cílení funkcí, datové a procesní toky, jejich vlastníci, atd.

Z toho důvodu musí být součástí analýzy i organizační struktura společnosti Tesco. Nicméně vzhledem k faktu, o jak obrovskou se jedná firmu, a o jak velkém regionu uvažujeme, je nereálné zobrazit plnou organizační strukturu. Proto zobrazím jen relevantní části struktury firmy v regionu CE, které jsou nezbytné pro návrh funkčního systému vzdáleného přístupu – obecnou strukturu jednotek v zemích a regionu a organizační strukturu IT.

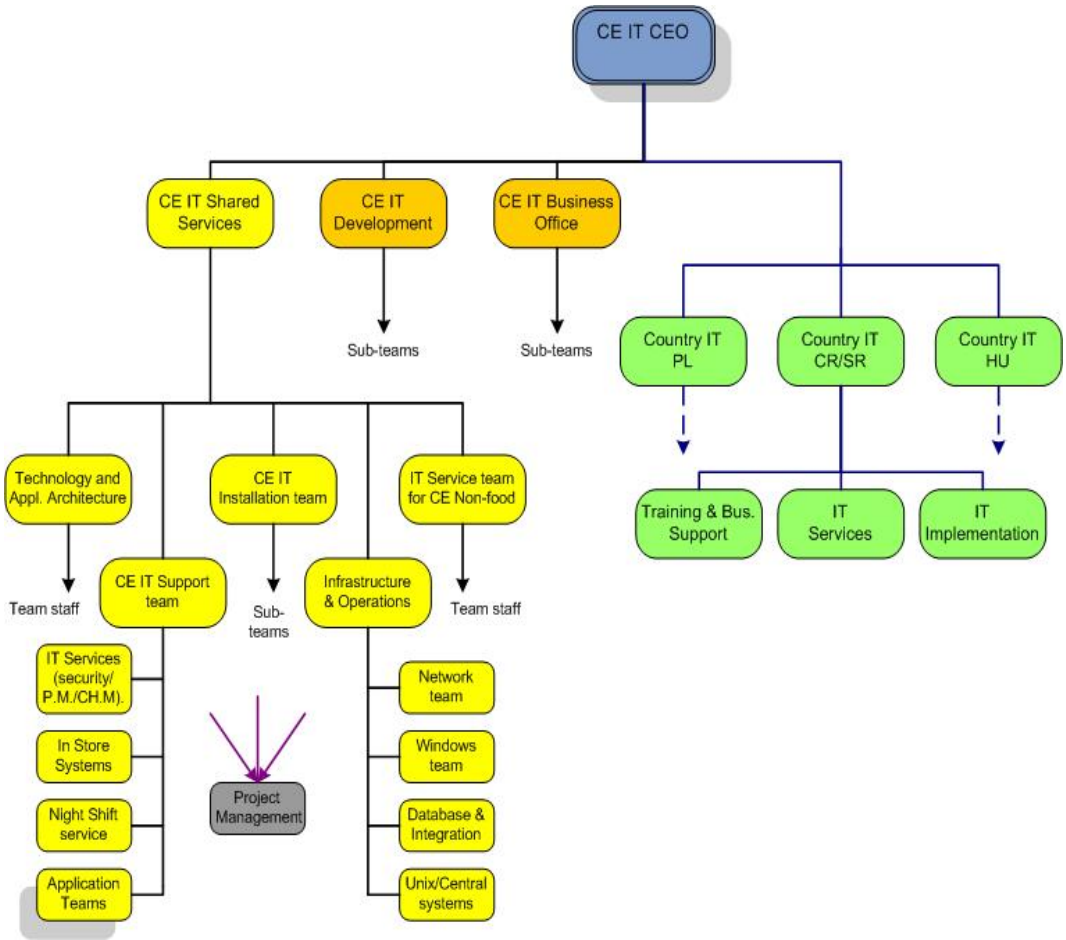
Obr.1 - Organizační struktura dle poboček pro CE:



Nejvyšší úroveň rozdělení organizační struktury dle obchodních jednotek celého regionu CE:

Nejvýše postaveným je ředitel regionu CE (CE CEO). Jemu reportují CE IT CEO regionu, a obchodní ředitelé CR/SR, PL a HU (ačkoliv jsou CR a SR 2 různé firmy, v org. struktuře vystupují jako jeden celek). Dále následují tyto divize jakožto nejvyšší úroveň rozdělení společnosti (díky centralizaci regionu jsou některé z nich pouze na úrovni zemí, jiné jsou regionální s dalším dělením na jednotlivé země): 1. Store support office, 2. Range & Space, 3. Trading law & Technical, 4. Komerční, 5. Supply Chain a Distribuce, 6. Služby zákazníkům, 7. Marketing, 8. Promoce, 9. Cenový tým, 10. Lidské zdroje, 11. Právní, 12. Corporate Purchasing, 13. Property, 14. Corporate Affairs, 15. CUP Brno, 16. IT (dělení viz. dále).

Obr.2 – Organizační struktura IT – základní dělení a relevantní týmy



Struktura IT je logickým výsledkem organizační koncepce společnosti, nastavených procesů a zodpovědnosti. Stručný náhled do fungování IT, působnosti a zodpovědnosti jednotlivých celků je popsán v následující kapitole.

Vlastníkem řešeného projektu a budoucím správcem systému v org. struktuře je CE IT Shared Services – Infrastructure & Operations – týmy Network a Wintel.

3.1.3. Struktura IT

Informační technologie a systémy jsou vzhledem k velikosti a globalizaci společnosti naprosto nezbytným prostředkem k jejímu fungování. Tomu také odpovídá velké množství jednotlivých systémů a vysoká náročnost správy a vývoje. Cílem kapitoly je nastínit pouze nejnutnější fakta o působnosti, zodpovědnosti a procesech v IT dle organizačního rozdělení, a také zobrazení náhledu síťové topologie v regionu CE, nutné pro návrh nového systému vzdáleného přístupu.

Country IT

- stojí nejníže v org. struktuře
- jsou vlastníky IT systémů dané země
- přímo spolupracují s obchodní částí společnosti, přebírají od obchodní části požadavky na změny, vývoj, atd., požadavky přetvářejí dle IT koncepce a možností a předávají je dál do nadřazeného Central Europe IT, následně pak částečně zajišťují implementaci změn
- zajišťují support uživatelů, vystupují jako „1st Level Support“ – tedy zaznamenávají a zpracovávají všechny IT incidenty (na bázi 24x7x365)

CE IT

- Central Europe IT je nadřazená jednotka, je to regionální servisní „organizace“ pro jednotlivé Country IT celky (s vlastním rozpočtem)
- CE IT je správce všech systémů v celém regionu
- CE IT zajišťuje „2nd Level Support“ – řeší všechny incidenty IT systémů oznámené „1st Level Supportem“, a to na bázi 24x7x365 (support tedy musí být

zajištěn i v noci a o víkendech – to je jeden z hlavních důvodů projektu nového systému pro vzdálený přístup)

- na jedné straně přebírá požadavky od svých „zákazníků“ – Country IT, projektuje a realizuje požadované změny dle platných koncepcí a politik, na druhé straně přebírá a lokálně upravuje globální IT koncepce a politiky z nejvýše stojící Velké Británie
- dělí se do 3 hlavních celků – zajištění služby a správy (Shared Services), vývoj nových systémů (Development), a má vlastní finanční oddělení (IT Business Office)
- obecně, role CE IT je především „High Level“ – jde tedy především o návrh a vývoj celkové koncepce, politik, procedur a projektů jednotlivých směrů IT, uvádění těchto koncepcí a nových řešení do praxe, atp. Samotná realizace koncepcí a změn do všech lokalit regionu a také hlavní jádro správy všech lokalit je úkolem **IT dodavatelů**

IT dodavatelé

- jak bylo uvedeno výše, dodavatelé jsou nedílnou součástí procesního řetězce IT, každý IT systém má „svého“ dodavatele - vzhledem k množství IT systémů, množství lokalit a diferenciaci není možné zajistit plnou správu, implementaci a instalaci interními zdroji (systém je takto nastaven)
- dodavatelé v podstatě dostanou nově vyvinutou schválenou koncepci/projekt s pilotní instalací, a sami zajistí implementaci do všech ostatních lokalit/systémů
- dodavatelé vystupují v procesu správy jako „3rd Level Support“
- správa probíhá taktéž v režimu 24x7x365 s velmi vysokým SLA (Service Level Agreement – definuje rozsah a úroveň poskytovaných služeb, včetně zajištění dostupnosti služby a doby opravy) – tedy i dodavatelé jsou důležitým vstupem pro návrh systému vzdáleného přístupu

Lokalizace IT systémů, topologie

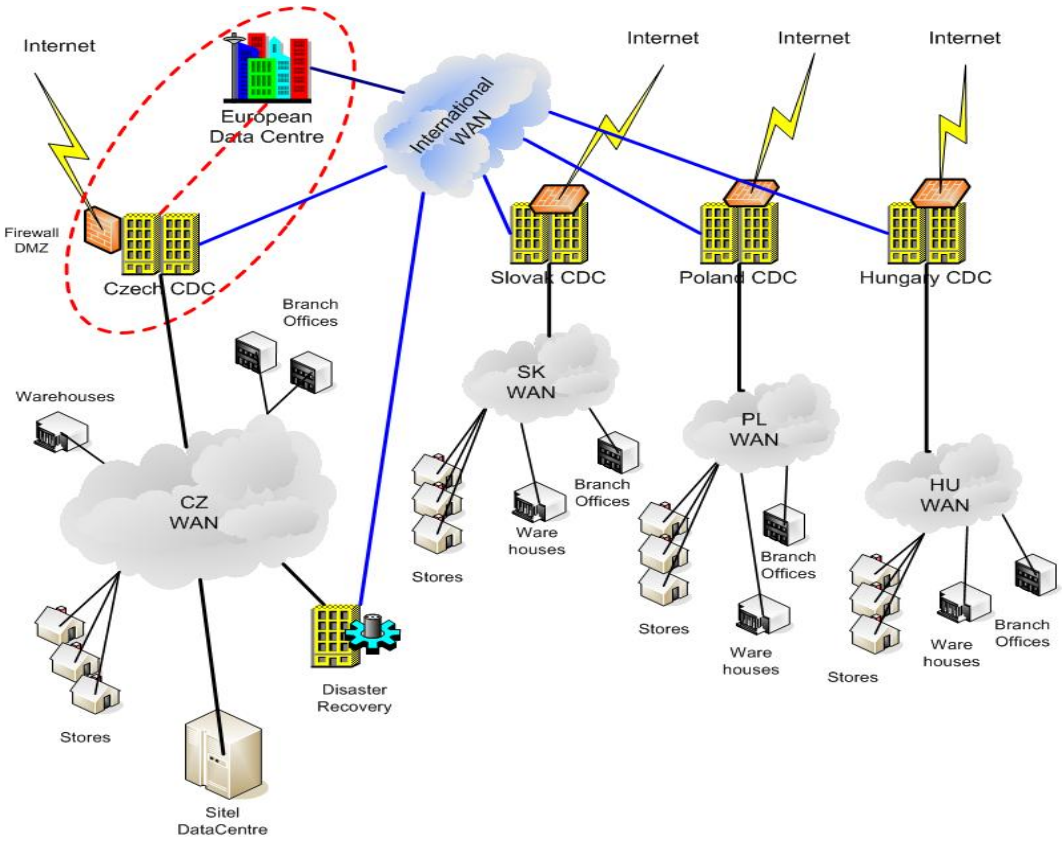
IT systémy jsou v regionu CE centralizovány. Velmi malé množství systémů má své lokální instalace přímo na jednotlivých lokalitách – obchodech (samozřejmě kromě koncových zařízení, jako pc, kasy, platební terminály, atp.).

Nadřazený prvek v IT infrastruktuře jsou „Country Data Centres“ (dále jen CDC) – datová centra v hlavní pobočce země. Zde jsou lokální instalace většiny systémů s daty pro danou zemi, na které buď přistupují uživatelé přímo, nebo prostřednictvím systémů na obchodech. Všechny pobočky jsou s CDC propojeny pomocí WAN sítě dodavatele. Každé CDC má také svoje připojení k internetu – mezi internetem a vnitřní sítí stojí Firewall s DMZ (demilitarozovaná zóna), zajišťující zabezpečení vnitřní sítě. V DMZ jsou umístěny systémy pro přístup na internet, pro publikování určitých systémů pro veřejnost, a také současné systémy pro vzdálený přístup (viz. dále).

Nejvýše ve struktuře stojí „European Data Centre“ (dále jen EDC) lokalizované v ČR. V evropském data centru jsou centralizovány naprosto všechny IT systémy společnosti, zde jsou hlavní databáze k systémům, atd. Systémy z jednotlivých CDC se replikují z EDC systémů. Všechna CDC jsou z EDC spojena mezinárodní WAN sítí dodavatele. Nutno podotknout, že EDC se fyzicky nachází ve stejné lokalitě jako české CDC (centrála Praha Letňany), sítě jsou ovšem logicky odděleny.

Celkový náhled na stručně popsanou topologii poskytuje následující obrázek.

Obr.3 – IT síťová topologie



3.2. Současný stav v oblasti vzdáleného přístupu

Cílem této kapitoly je uvést současně používané systémy pro vzdálený přístup do korporátní sítě společnosti v regionu CE, popsat jejich funkcionalitu a design, uvést náklady na jejich provoz, popsat rozdělení uživatelů, a také identifikovat případné nedostatky a rizika použití těchto systémů včetně aspektu bezpečnosti provozu.

Společnost Tesco nyní provozuje v regionu CE tři systémy pro vzdálený přístup. U dvou z nich jde o komplexní řešení pro celý region CE, obě řešení jsou typ přístupu k *n*-systémům společnosti. Třetím systémem je aplikace zajišťující přístup jen k jednomu vnitřnímu systému, provozovaná pouze v ČR.

3.2.1. Outlook Web Access (OWA)

Jde o poslední zmíněnou aplikaci, která slouží pro vzdálený přístup k jednomu systému společnosti, a to k emailovým schránkám uživatelů mimo kancelář, tedy zejména při častém cestování. Systém je postavený na technologii Microsoft mailového systému Exchange server s přístupem přes Windows ISA server, a šifrování komunikace zajišťuje SSL offloader Alteon.

Systém se provozuje pouze v ČR, slouží především pro potřeby zaměstnanců centrálních kanceláří v ČR - tedy pro vedení, manažery a zaměstnance nejvyšších regionálních celků CE, včetně CE IT; přístup má ještě také několik nejvyšších ředitelů a manažerů z jednotlivých zemí regionu – celkem systém využívá cca 700 uživatelů.

Systém má webové rozhraní, přístup je realizován přes zabezpečený webový protokol HTTPS, jako klient je tedy použit webový prohlížeč uživatele.

Ověření uživatele při připojení je realizováno pomocí jeho doménového účtu z Windows Active Directory, tedy jeho běžným přístupem do PC. Dle účelovosti systému a nastavené správě je použití bezpečné a splňuje bezpečnostní politiky.

Celkové roční náklady na správu a servis – support Alteon SSL (publikováno 12 webových serverů, tedy 1/12 nákladů), HW maintenance DMZ Windows ISA serveru, externí a interní support a správa jsou cca 360.000,- Kč.

Tento systém je naprosto vyhovující a není potřeba uvažovat o jeho nahrazení. Dále se jím tedy již ve své práci nebudu zabývat.

3.2.2. Remote Access System (RAS)

Jde o velmi zastaralý systém vzdáleného přístupu postavený na technologii Cisco v podstatě do celé korporátní sítě Tesco v regionu CE, tedy k *n*-systémům, kdy uživatelé mají možnost připojením se do povolené části sítě spustit jakoukoliv aplikaci přístupnou v dané části sítě.

Připojení uživatelů je realizováno vytáčeným telefonním spojením nebo ISDN linkou, předpokladem použití je uživatelovo vlastnictví domácí pevné telefonní nebo ISDN linky, či použití s mobilním telefonem, a taktéž vlastnictví služebního notebooku s modemem (politika použití). Systém díky tomu nabízí jen velmi malou rychlost připojení – rychlost telefonní linky je jen 56kb/s a ISDN jen 128kb/s, při použití s mobilním telefonem je rychlost dokonce ještě menší. Z důvodu velmi malé rychlosti je systém použitelný jen na málo firemních síťových aplikací (velmi pomalý pro použití emailu, sdílených disků, webových aplikací; částečně pro aplikace s „tenkými klienty“; dobře použitelný pro vzdálenou administraci přes telnet, ssh, či ftp, částečně i pro grafické typy vzdálené správy).

Stručný popis struktury systému:

Základem systému jsou speciální Cisco RAS routery, které jsou svým jedním rozhraním připojené přímo do vnitřní sítě datacentra, a na druhém rozhraní mají připojenu klasickou telefonní a ISDN linku. Routerů je v celém regionu celkem 5 – 2 v ČR (ve dvou různých částech sítě), a po jednom v zemích SK, PL, HU. Uživatel se může připojit do sítě jakýmkoliv z 5 routerů - systém je pro uživatele plně redundantní (zálohovaný). Routery bohužel nejsou zapojeny přes Firewally a zabezpečený perimetr sítě, mají však nastaveno alespoň základní omezení přístupu formou tzv. „access listů“.

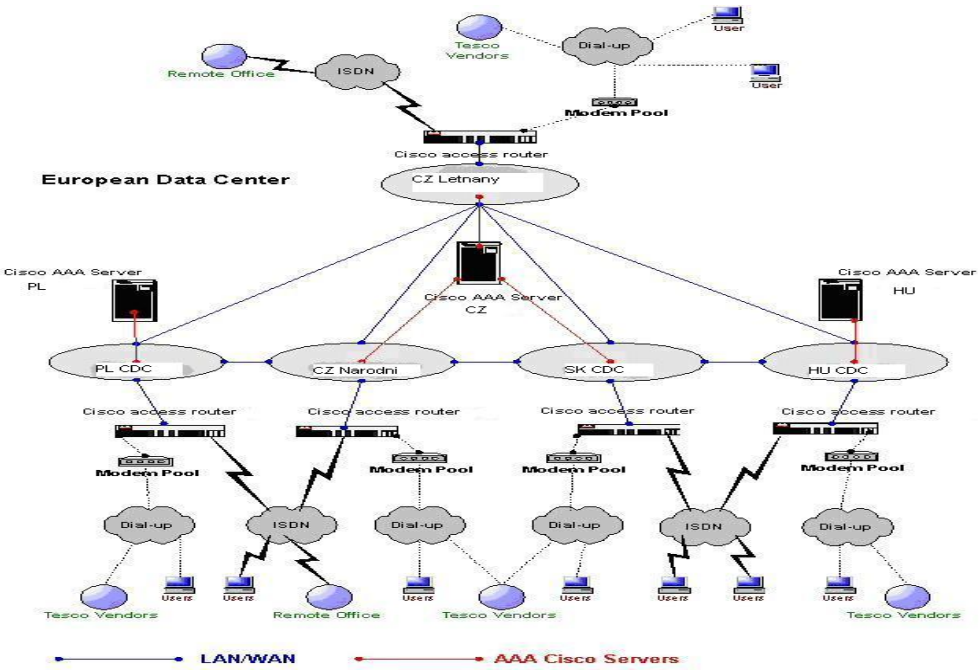
Všechny routery jsou komunikačně navázány na 3 ověřovací a zabezpečovací servery v síti – servery TACACS+, konkrétně Cisco ACS server verze 3.0. Jeden server vystupuje ve struktuře jako primární (v českém

datacentru), dva další jsou záložní (v polském a maďarském datacentru). Pomocí těchto serverů dochází k autentizaci a autorizaci uživatelů, kteří se připojí na RAS routery. Z bezpečnostních důvodů nejsou žádné uživatelské účty přímo na routerech, veškeré ověřování je z databáze ACS serverů. Databáze uživatelů na serverech je tedy lokální, spravovaná přímo na nich, nepoužívá se běžných doménových přístupů. Administrace uživatelských účtů díky tomu bohužel přináší větší nároky na zdroje.

ACS servery umožňují kromě ověření uživatele a přidělení přístupu také velmi precizní nastavení přístupových práv k síti na bázi síťových access listů – omezování přístupu na rozsahy sítě a komunikační porty protokolu TCP/IP. Práva mohou být nastavena buď na úrovni skupin, či na jednotlivé uživatele. V Tescu je využíváno pouze pro nastavení skupin, a to s velmi otevřenými přístupovými právy (historické důvody).

Provozně je systém pro Tesco velmi nákladný, jelikož se platí veškeré provolané minuty všech telefonních/ISDN linek připojených na routery. Důvod vysokého počtu provolaných minut je prostý - některé skupiny uživatelů mají z bezpečnostních důvodů nastavenu funkcionalitu „call-back“, tzn. ve chvíli, kdy se připojí k systému a ověří se svým loginem, je router odpojí, a ihned jim volá zpět na jimi nastavené číslo. Tím se přenáší náklady na připojení z uživatele na firmu.

Obr. 4 – Náhled systému RAS



Analýza uživatelů:

Tento systém je široce užívaný systém, jednak mnoha uživateli všech obchodních a IT kanceláří všech zemí regionu, a jednak mnoha IT dodavateli. Počet uživatelů je cca 2500. Uživatele můžeme rozdělit na dvě hlavní skupiny:

IT dodavatelé

Používají RAS pro servisní přístup do systémů jimi spravovaných. IT dodavatelé s málo uživateli používají 1 hromadný přístupový účet pro všechny, kde jméno odpovídá názvu firmy, účet je zařazen do jedné z běžných Tesco skupin. IT dodavatelé s více uživateli mají pro každého uživatele svůj účet, odpovídá kombinaci jména a příjmení, zařazení do skupiny pojmenované dle jména dodavatele (pouze 10 dodavatelských skupin v celém systému).

Tesco uživatelé

Používají RAS zejména pro přístup k síťovým zdrojům jejich kanceláře (sdílené disky, email, moduly informačního systému společnosti a jiné interní aplikace – tzn. v podstatě všechny interní systémy). Tesco uživatelé jsou rozděleni do následujících skupin:

1) Admin users – skupina určená pro IT administrátory z CE IT a Country IT, přístup do celého adresního rozsahu Tesco, povolené všechny porty tcp/ip, funkce call-back zapnuta individuálně dle požadavku uživatele
2) Non-callback users – nejnižší skupina – bez volání zpět, přístup omezen jen na datacentrum, do kterého se uživatel připojil
3) Internet & Non-callback users – stejně jako skupina výše, jen ještě oprávnění přístupu na internet přes Tesco systémy
4) Callback users – stejně jako skupina 2, avšak s funkcí volání zpět uživateli
5) Internet & Callback users – stejně jako skupina 3, avšak s funkcí volání zpět uživateli
6) Special users – volitelně s funkcí volání zpět, přístup do větší části sítě – nastavováno individuálně pro každého uživatele

Rozdělení uživatelů do skupin ani nastavená práva naprosto nesplňují současné požadavky a politiky, především bezpečnostní.

Náklady na provoz:

- Support a správa RAS routerů včetně HW maintenance – 150.000,-Kč/měsíc
- Průměrné náklady na všechny připojené dial-up/ISDN linky dle provolaných minut: 250.000,-Kč/měsíc
- Celkový roční náklad na provoz: 4.800.000,-kč

Shrnutí nedostatků systému RAS:

- systém je hodně zastaralý, zastaralé hw prvky skrývají potenciální bezpečnostní riziko (zvlášť router stojící mezi veřejnou sítí a Tesco sítí – při úspěšném útoku se útočník bez problémů dostane do sítě Tesca)
- samotné zapojení systému bez začlenění do perimetru sítě (přímé zapojení routeru bez ochrany Firewallem) a velmi otevřená konfigurace přístupu skupin uživatelů do sítě jsou velkým bezpečnostním rizikem
- dalším bezp. rizikem je použití pouze 1 fázové autentizace, často s velmi slabými hesly, které neodpovídají současné bezpečnostní politice společnosti
- velmi malá škálovatelnost a možnosti použití – rychlost připojení je velmi nízká, to velmi omezuje možnosti použití, od uživatele je vyžadováno telefonní či ISDN připojení
- správa náročná na zdroje – musí se spravovat samostatná databáze uživatelů, která navíc není nijak navázána na jiné databáze (tzn. například ruční kontrola aktivních uživatelů a odešlých zaměstnanců, atp.)
- vysoké náklady na provoz systému, především díky telefonním poplatkům
- nedostatečné rozdělení uživatelů do skupin, nedostatečné oddělení a identifikace externistů a IT dodavatelů
- nejsou plně využity všechny možnosti ACS serverů, nedostatečné zaznamenávání přístupu a událostí (logování)
- jedinou výhodou je neomezená možnost přístupu k celé síti všemi porty z vlastní plochy notebooku

3.2.3. CITRIX / SWA

Jedná se o nejrobustnější, nejnovější a nejvíce komplexní systém vzdáleného přístupu postavený na interním regionálním systému Citrix, s největší mírou zabezpečení, pro přístup k *n*-systémům.

Celý systém je tvořen 2 vrstvami. První vrstva - vlastní interní CITRIX systém - je terminálový systém, který zajišťuje webové publikování jakýchkoliv aplikací umístěných kdekoliv v síti tak, že vzdálená koncová aplikace (aplikační server) je „přidána“ na Windows server Citrixové farmy a „vystavena“ ve webovém rozhraní Citrixu – hlavní výhodou je tedy možnost velmi rychlého zpřístupnění aplikace libovolnému počtu interních doménových uživatelů a bez geografického omezení. Publikované aplikace jsou přístupné přes zabezpečené HTTPS webové rozhraní na vnitřním přístupovém serveru napojeném na farmu, aplikace se spouští buď ve webovém rozhraní nebo samostatném okně Windows Desktop. Uživatel však vždy musí mít nainstalován tenkého klienta ICA.

Druhá vrstva SWA/CITRIX zajišťuje bezpečný přístup uživatelů z internetu k terminal serverům. Tato vrstva je tvořena jednak dvěma servery Citrix Secure Gateway a Citrix NFuse server v CZ DMZ, a jednak autentizačními servery RSA Secure ID pro bezpečnou autentizaci uživatele tokenem SecureID – 1 server v CZ DMZ (FrontEnd), a jeden server s databází v interní síti (BackEnd). Tyto uvedené přístupové systémy SWA jsou napojeny na interní systém (první vrstvu) do vnitřní sítě. Přístupové SWA servery jsou sice jen v ČR, avšak využívají se globálně v celém regionu CE.

Externí přístup je velmi bezpečný. Jednak je použito šifrované komunikace SSL/HTTPS, a jednak je komunikace kontrolovaná a striktně omezená Firewallem. Ověření uživatele je navíc dvoufaktorové – tedy něčím, co uživatel zná (svoje doménové heslo a PIN k RSA), a něčím, co má (RSA SecureID token) – proces ověření viz. obrázek níže.

Výhodou použití systému Citrix (stejně jako jiných terminal server řešení) je snadná centrální správa aplikací, škálovatelnost, loadballancing (rozložení zátěže), malý datový tok (přenáší se jen pohyby myši a klávesnice a změny na obrazovce), velmi rychlá publikace aplikace velkému počtu klientů bez geografického

omezení. Nevýhodou je ale nutnost použití lokálního tenkého klienta ICA u každého uživatele.

Použití systému: uživatel má po připojení možnost výběru buď přímo konkrétní aplikace Tesco, nebo možnost spuštění virtuální pracovní plochy Windows se všemi standardními lokálními Tesco aplikacemi (Office, Internet Explorer, atp.) a s nástroji jako RDP, telnet, ssh apod. – tedy nástroje pro vzdálený přístup a administraci zařízení na síti. Výhodou je i možnost přístupu k lokálním datům na počítači vzdáleného uživatele, a samozřejmě přístup na sdílené disky. Nevýhodou je nemožnost použití vlastního PC profilu, a tedy nedostupnost případných nadstandardních aplikací (důležité především pro odborné IT pracovníky). V případě vzdáleného přístupu je také systém velmi náročný na rychlost připojení k internetu uživatele – systém není použitelný pod rychlost 256kb/s.

Stručný popis struktury systému:

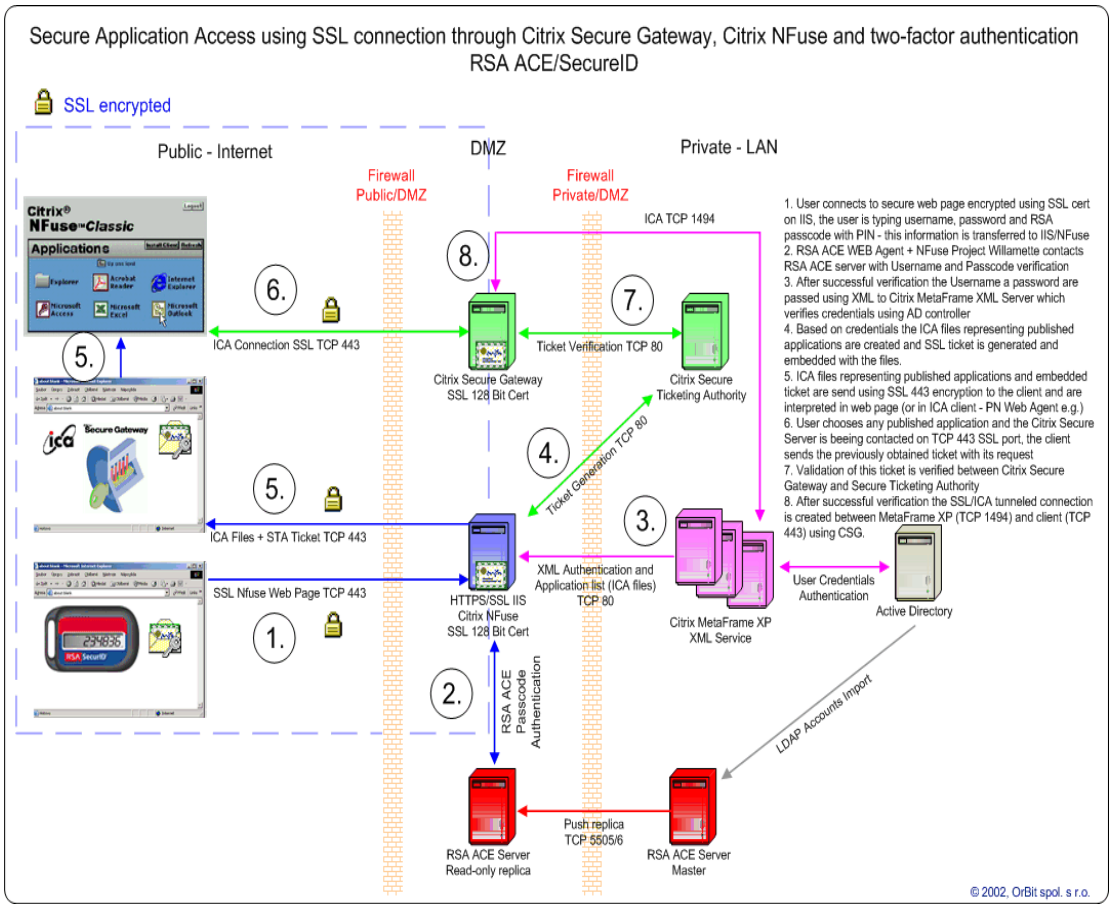
Aplikační vrstvou (v interní síti) jsou Citrixové farmy. Farmy jsou 4 – datacentrum Letňany CZ (14 serverů), datacentrum Sitel CZ (5 serverů), datacentrum PL (8 serverů) a datacentrum HU (16 serverů). Pro interní použití (tedy přístup uživatelů z vnitřní Tesco sítě) se na Citrixu provozují především finanční systémy (platební styk, objednávky, výplaty, zpracování faktur), docházkové systémy a personální systémy HR.

Publikační vrstvou interní jsou servery pro přístup uživatelů. Pro interní přístup jsou to 2 servery pro CZ a SK z Citrixové farmy v Letňanech, 1 server z PL farmy a 1 server z HU farmy. V případě výpadku přístupového serveru jeho roli převezme jiný server z farmy. Tyto přístupové servery zprostředkují ověření uživatele z Active Directory.

Publikační vrstvou externí jsou, jak již bylo napsáno, 2 servery (brány) umístěné v DMZ – Citrix Secure Gateway a Nfuse server. Na nich proběhne ověření externího uživatele přistupujícího z internetu. K tomu je využito jednak spojení do interní sítě na Active Directory, a jednak také serverů RSA – jednoho autorizačního serveru v DMZ, který komunikuje se svým databázovým serverem

ve vnitřní síti. Jakmile je uživatel ověřen, získá přístup do interní části systému ke všem publikovaným službám.

Obr. 5 – Náhled systému Citrix/SWA na perimetru sítě, komunikační toky autentizační procedury mezi klientem v internetu, DMZ a LAN



Analýza uživatelů:

Přístup je postaven na přiřazování uživatelů do skupin, skupiny jsou rozděleny do logického uspořádání dle přístupových práv k publikovaným aplikacím nebo skupinám aplikací. Každý uživatel má nastaveno členství právě v těch skupinách, jejichž aplikace potřebuje přistupovat, sdružování uživatelů do skupin je tedy funkčně organizační. Z toho vyplývá, že existuje právě tolik skupin uživatelů, kolik je publikovaných aplikací.

Uživatelé jsou administrováni v rámci aplikace Citrix, databáze Citrixu se synchronizuje dle doménové Active Direktory. Pro externí přístup je nutná také správa samostatné databáze RSA SecureID klíčů a jejich fyzické vydávání a evidence.

Základní dělení uživatelů v tomto systému je na Inetrní a Externí.

Interní

Z podstaty systému, tedy jednotné publikace mnoha aplikací pro práci uživatelů, jde v podstatě o většinu kancelářských uživatelů dané aplikace. Jedná se zejména o finanční a personální aplikace zemí regionu (viz. popis systému), tedy aplikace s mnoha uživateli. Interních uživatelů Citrixu je řádově 6000

Externí

Externí přístup z internetu je přidělován méně často, a jen v odůvodněných případech, především díky vysoké ceně SecureID klíčenky a RSA licence. Externí uživatelé jsou typově především IT administrátoři a IT support zaměstnanci, klíčoví uživatelé některých aplikací, někteří Tesco zaměstnanci zemí mimo region (UK), IT dodavatelé a externí konzultanti. Rozdělení do uživatelských skupin je stejné jako u interních uživ. (viz. výše popsané).

- počet účtů dodavatelů, konzultantů a externistů – cca 250
- počet účtů Tesco zaměstnanců – cca 1000

Náklady na provoz:

Díky robustnosti řešení, množství typů serverů a počtu jednotlivých serverů je systém nejen velmi náročný na správu, ale taky velmi drahý. A právě počet prvků pro mne znamená velmi problematické spočtení celkových nákladů, ke kterým nemám dostatek podkladů. Proto provedu pouze odhad nákladů vycházející z neúplných podkladů. Zřejmé náklady pro externí přístup se dají vyčíslit jen pro obě Citrix gateways v DMZ, RSA servery, RSA licence a počet RSA klíčů (1 klíč stojí na 2 roky provozu cca 3.000,-kč).

Celkové roční náklady na RSA: 2.700.000,-kč

Odhad poměrných ročních nákladů na provoz „externí části“ Citrix: 6.500.000,-kč

Odhad celkových ročních nákladů na provoz celého Citrix: 25.000.000,-kč

(v ceně je zahrnuto: náklady na klíče SecureID, licence RSA, licence Citrix, náklady na externí support a správu aplikací a serverů (SW a HW), hardware maintenance servis výrobcem a dodavatelem serverů, interní náklady na provoz a správu).

Shrnutí nedostatků systému Citrix/SWA:

- nevýhodou je design systému ve smyslu webového rozhraní – přístup realizovaný přes webové rozhrani SSL má smysl tehdy, pakliže jde o „client-less“ přístup, tedy přístup bez nutnosti mít instalovaného klienta v PC – pak je takový systém použitelný z jakéhokoliv pc, např. z internet café; zde je však potřeba ICA client a i přesto není možné použít k práci při vzdáleném připojení plnohodnotnou plochu vlastního notebooku
- nemožnost použití vlastní plochy a nutnost použití virtuální plochy snižuje škálovatelnost a možnosti použití, uživatel nemůže využít všechny své instalované aplikace, v podstatě nelze realizovat přístup k celé síti a všemi porty
- práce s webovým rozhraním je velmi náročná na rychlost připojení uživatele k internetu, proces spuštění při ověření přenáší velké množství dat (nepoužitelné při pomalém připojení)
- naopak webové rozhraní je ideální při použití pouze jedné publikované aplikace, hlavní síla systému je právě především v publikování aplikací
- nevýhodou je velké množství prvků systému, a tedy náročná správa a velké náklady na správu a provoz

3.3. Požadavky společnosti na vzdálený přístup uživatelů

V této kapitole identifikuji aktuální požadavky společnosti na funkci a možnosti systémů vzdáleného přístupu do firemní sítě tak, jak vyplývají ze současných firemních politik a standardů a ze současných potřeb relevantních skupin uživatelů.

Požadavky budou uvedeny a strukturovány tak, aby byly využitelné jako závazné požadavky pro návrh nového systému vzdáleného přístupu.

3.3.1. Požadavky na dostupnost připojení

- Vysoká dostupnost - požadovaný režim provozu: 24x7x365 (tedy 24hodin denně), doba výpadku jednoho přípojného bodu může být maximálně 4hodiny (SLA 99,5%)
- systém musí být redundantní (zálohovaný) – uživatel má možnost při výpadku jednoho přístupového bodu se připojit přes jiný přístupový bod (musí být nezávislé na externí i interní přípojce, tedy každé zařízení na jiné lince)
- požadavek na mobilitu uživatele – uživatel má možnost připojit se odkudkoliv mimo Tesco pomocí běžné přípojky k internetu, systém by měl být dobře použitelný jak s rychlým, tak s pomalým připojením k internetu
- dostatečná průchodnost systému pro 500 současných uživatelů
- řešení musí umožňovat nastavení QoS (quality of service) – prioritizaci datových toků, uživatelů či skupin uživatelů pro zajištění dostupnosti při přetížení pro privilegované uživatele/skupiny

3.3.2. Požadavky na uživatele

- každý přístupový bod systému pro vzdálený přístup musí být kapacitně dimenzován na 500 současně připojených uživatelů (popř. databáze na 4 tisíce uživatelů)
- systém musí mít jednoduchou a logickou funkci konfigurování a správu celých skupin uživatelů, sdružování uživatelů do skupin s přiřazením přístupových práv jak na úrovni skupin, tak na úrovni jednotlivých uživatelů s velkou škálovatelností
- systém musí mít možnost navázat autentizaci uživatele a přístup na externí databáze uživatelů přes platformu RADIUS/AAA, nejlépe na Windows ActiveDirectory

3.3.3. Požadavky na provozované aplikace a jejich dostupnost

- zpřístupnění celé sítě regionu CE (všech IP adresních rozsahů) tak, aby byly přístupné všechny produkční informační systémy společnosti včetně jejich hardwarového vybavení a všech síťových prvků (jde o nejvyšší požadovaný rozsah přístupu určený především odbornému IT personálu a dodavatelům)
- požadovaná dostupnost všech produkčních systémů vzdáleným připojením se odvíjí od stanoveného SLA pro tyto systémy, SLA pro kritické systémy je většinou v rozmezí 2 – 4hodin, u méně kritických od 6hodin do 12 – 16 hodin, vyjímečně až 24hodin, při režimu provozu 24x7x365
- při vzdáleném přístupu je potřeba současného přístupu uživatelů jak ke vzdáleným zdrojům v síti, tak k lokálním zdrojům na klientském počítači (tzn. použití vlastního uživatelského profilu na notebooku, tedy možnost použití vlastní plochy a instalovaných programů pro práci na síti)
- vyžadováno použití „clientbased“ řešení – takové, kdy má uživatel na notebooku instalován SW klienta s nastaveným profilem, kterým se připojuje k systému (a díky tomu se stane „plnohodnotným“ klientem firemní sítě tak, jako kdyby byl připojen v kanceláři)

3.3.4. Požadavky na zabezpečení

Pro zajištění maximální bezpečnosti vnitropodnikových dat musí úroveň zabezpečení systému odpovídat nejnovějším bezpečnostním standardům pro danou oblast, určeným jednak stanovenými vnitřními bezpečnostními předpisy Tesco UK, a jednak mezinárodními bezpečnostními standardy a normami (ISO 27001 a 27002, British Standard, atd.).

Systémové požadavky na zabezpečení:

- komunikace mezi klientem a systémem musí být šifrovaná pro zajištění bezpečnosti komunikace internetem – protokoly IPSec nebo SSL/TLS s podporou šifrovacích algoritmů 3DES a AES, hash MD5 nebo SHA1

- plně konfigurovatelné access listy jak pro rozhraní, tak pro skupiny vzdáleného přístupu, stavová inspekce komunikace, NAT (překlad adres mezi rozhraními), podpora QoS
- zabezpečení přístupu k administrativnímu rozhraní, podpora bezpečných protokolů SSH a HTTPS pro administraci
- požadavek na plné logování událostí včetně výstupu na externí systémy pro analýzu
- podpora pro 802.1Q (virtuální kontexty)
- vhodná možnost rozšíření použití s NAC systémy (Network admission control – kontrola parametrů systému z kterého uživatel přistupuje a přidělení, omezení či zamítnutí přístupu; nejčastěji se kontroluje instalovaný Antivirus a jeho aktualizace, Windows aktualizace, atp.), případně vestavěného antiviru

Uživatelské požadavky na zabezpečení:

- ověření uživatele - podpora skupinového profilu s klíčem nebo použití s certifikáty, následně ověření jedinečného účtu uživatele z lokální nebo vzdálené databáze, systém musí podporovat plnohodnotnou dvoufaktorovou autentizaci a tedy možnost navázání na externí systémy v síti pro autentizaci uživatele (především RADIUS server s uživatelskou databází, RSA server pro SecureID tokens, Certifikační autorita X.509, LDAP na ActiveDirectory)
- Tesco uživatel vždy musí pro vzdálené připojení použít jeho vlastní firemní notebook, který je pod správou Tesca a splňuje firemní standardy, tedy SW klient s profilem pro přístup může být instalován a nastaven pouze na notebooku splňujícím bezpečnostní požadavky firmy

3.3.5. Požadavky na správu a technologii

- důraz na minimalizaci nároků na interní i externí zdroje - po úvodní implementaci by měl být systém co nejméně náročný na běžnou údržbu a změny konfigurace, se snadným a rychlým vytvářením nových přístupů (snížení nákladů na provoz)

- jedním z hlavních kritérií pro volbu technologie systému je znalost administrace technologie jak odpovědným technickým IT personálem, tak příslušným dodavatelem služeb
- zabezpečené rozhraní pro správu s možností omezení přístupu, administrace přes šifrované SSH a HTTPS, možnost konfigurace více administračních profilů pro správu s různou úrovní oprávnění
- vzhledem k předpokládanému malému počtu přístupových prvků nemusí systém disponovat konzolí pro centrální správu
- potřeba navázání systému na externí systémy v síti pro rozšířené možnosti správy (logovací server s možností analýzy a větší historie logů, smtp, ntp, snmp, atd.)
- systém by měl být dostatečně „robustní“, s dostatečnou podporou výrobce technologie (aktualizace firmware, oprava bezpečnostních chyb...)
- výběr technologie s ohledem na její budoucnost - „price for future“

3.3.6. Požadavky na začlenění do globálního prostředí firmy

- nový systém musí být řešen jako jeden celek pro všechny 4 země regionu
- v každé ze 4 zemí regionu CE musí být 1 hlavní přístupový bod systému
- jako záložní přístupový bod může být v každé zemi druhé zařízení, nebo pro tyto účely může sloužit zařízení z jiné země regionu
- zařízení pro přístup budou vzhledem k požadavkům použití umístěny na perimetru sítě a zapojeny s maximálním důrazem na zabezpečení (dle typu zařízení buď paralelně nebo sériově s firewallem), tzn. budou umístěny v národních datacentrech CDC
- systém bude infrastrukturně navázán na existující vybrané interní systémy tak, aby využití externích služeb zvýšilo úroveň zabezpečení systému a rozšířilo možnosti správy (viz. požadavky na zabezpečení a správu)

3.4. Zhodnocení současného stavu

Po analýze a popisu současného stavu společnosti v oblasti vzdáleného přístupu do korporátní sítě firmy, popisu současných systémů a identifkiaci jejich hlavních nedostatků a rizik, a uvedení všech aktuálních požadavků společnosti na funkce a použití vzdáleného přístupu, je jednoznačným závěrem, že ani jedno řešení s typem přístupu k *n*-systémům nesplňuje stanovené požadavky.

Systém OWA je z hodnocení vyloučen, jelikož jde o jednoúčelovou aplikaci, naprosto splňující její určení.

Systém Citrix se požadavkům velmi blíží, především v zabezpečení, infrastrukturních požadavcích, dostupnosti a uživatelích, avšak rozchází se v požadavcích funkčnosti. Hlavním rozdílem je použití webového rozhraní a virtuální plochy oproti požadované vlastní ploše. Na druhou stranu však systém poskytuje bohaté možnosti publikace a přístupu k aplikacím. Z výše uvedeného důvodu, a také proto, že jde o systém primárně určený pro interní použití, nemůže být uvažováno o jeho nahrazení. Spíše může vystupovat jako vhodný doplněk případného nového systému.

Posledním řešením je velmi zastaralý RAS. O jeho nedostatcích a rizicích již bylo podrobně psáno výše. Jasným výsledkem je, že provozování tohoto systému je velkým bezpečnostním rizikem a systém by měl být co nejdříve odpojen z provozu.

Z uvedeného hodnocení je nadmíru zřejmé, že k naplnění současných požadavků firmy je třeba navrhnout a implementovat nový vhodný regionální systém pro vzdálený přístup, a mimo jiné jím nahradit RAS.

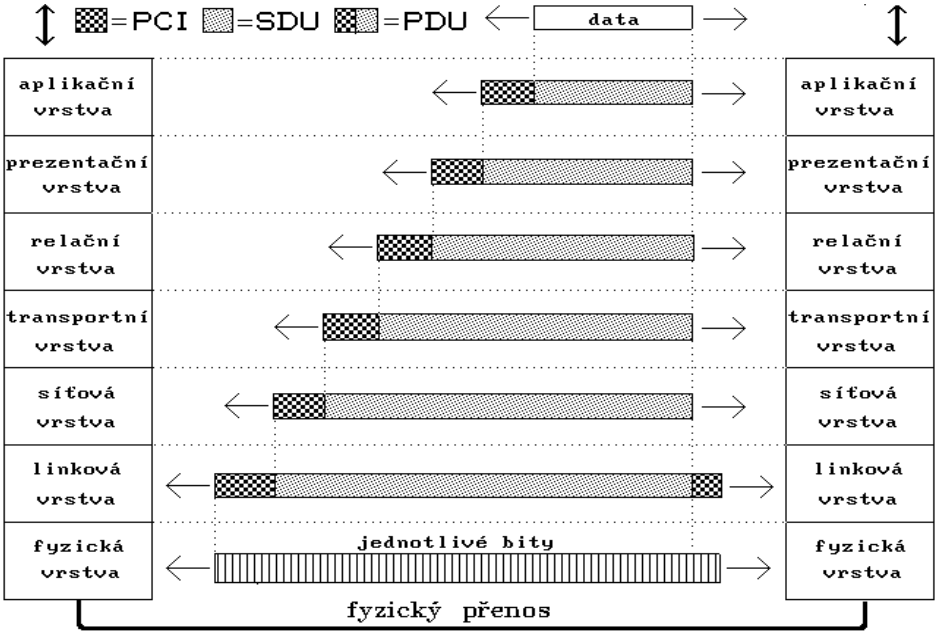
4. TEORETICKÁ VÝCHODISKA ŘEŠENÍ

V této kapitole popíšu nejdůležitější teoretické poznatky potřebné pro kvalitní a úplný návrh nového systému pro vzdálený přístup a pro nástin všech potřebných souvislostí.

4.1. Referenční model ISO/OSI

Základním stavebním kamenem a výchozím bodem datové komunikace je definice tzv. referenčního modelu ISO/OSI. Tento model vypracovala organizace ISO při snaze o standardizaci počítačových sítí nazvané OSI a v roce 1984 ho přijala jako mezinárodní normu ISO 7498. Úlohou referenčního modelu je poskytnout normovanou základnu pro účely propojování informačních systémů. Podle tohoto modelu je otevřený systém abstraktním modelem reálného otevřeného systému. Norma tedy nespecifikuje žádné detaily pro implementaci systémů, ani nepopisuje žádné komunikační protokoly, které by vyžadovaly zbytečně mnoho dalších detailů, ale uvádí jen všeobecné principy sedmivrstvé síťové architektury. Popisuje jednotlivé vrstvy, jejich funkce a služby. Vrstvy modelu zobrazuje následující obrázek.

Obr.6. – Referenční model ISO/OSI



Každá ze sedmi vrstev vykonává skupinu jasně definovaných funkcí potřebných pro komunikaci. Pro svou činnost využívá služeb své sousední nižší vrstvy. Své služby pak poskytuje sousední vyšší vrstvě. Komunikace začíná od nejvyšší vrstvy kde je přidána potřebná informace a postupuje níže. K prvotní informaci se vždy na další vrstvě přidá informace této vrstvy – viz. obrázek. Při doručování se zpětně na každé vrstvě „odlupují“ informace určené dané vrstvě.

Pro další účely této práce mne budou zajímat pouze 2. až 4. vrstva modelu, tedy linková, síťová a transportní (částečně ještě i aplikační vrsta). Tyto vrstvy velmi stručně popíšu včetně první fyzické vrstvy pro ucelený pohled.

1. Fyzická vrstva – zprostředkovává fyzickou komunikaci (spojení). Definuje elektrické a fyzikální vlastnosti zařízení a kabelů (zařízení pracující na této vrstvě: síťové adaptéry, huby, repeatery, atd.).

2. Linková vrstva – též spojová, tato vrstva poskytuje spojení mezi dvěma sousedními systémy. Seřazuje přenášené rámce, stará se o nastavení parametrů přenosu linky, oznamuje neopravitelné chyby. Formátuje fyzické rámce a opatřuje je fyzickou adresou. Příkladem je Ethernet. Poskytuje propojení pouze mezi místně připojenými zařízeními. Na této vrstvě pracují přepínače (switche).

3. Síťová vrstva – tato vrstva se stará o směrování v síti a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí, obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítích. Na této vrstvě pracují směrovače – routery. Protokoly pracující na této vrstvě – IP a ICMP, ARP, IPSec.

4. Transportní vrstva – tato vrstva poskytuje transparentní, spolehlivý přenos dat s požadovanou kvalitou. Vyrovnává různé vlastnosti a kvalitu přenosových sítí. Provádí převod transportních adres na síťové, ale nestará se o směrování. Do této vrstvy včetně pracují běžné typy firewallů (tzv. paketové filtry se stavovou inspekcí). Na této vrstvě je protokol IP rozdělen na přenosové protokoly TCP a UDP.

7. Aplikační vrstva – tato vrstva poskytuje aplikacím přístup ke komunikačnímu systému a umožňuje tak jejich spolupráci. Počátek komunikace aplikace začíná vždy zde. Aplikační Firewally pracují pracují až do této vrstvy včetně.

4.2. Vzdálený přístup

V této kapitole uvedu základní teorii o systémech vzdáleného přístupu k síti, jejich základní dělení dle typu přístupu, dle typu přenosového média, a dle typu spojených jednotek.

V následujících podkapitolách pak uvedu podrobnější detaily konceptu vzdáleného přístupu VPN (Virtual Private Network) a jejich funkci a chování na jednotlivých vrstvách ISO/OSI modelu.

Úvod do problematiky:

Vzdálený přístup k informačnímu systému je dnes standardním potřebným nástrojem využívaným v informačním prostředí. Jak je patrné ze slova „vzdálený“, tento přístup nahrazuje fyzický přístup k systému tam, kde systém není okamžitě fyzicky dostupný z důvodu vzdálenosti či časové náročnosti.

Vzdálený přístup k informačnímu systému je realizován přes datovou síť, přes nějakou síťovou infrastrukturu. Pojďme si nyní rozdělit typy vzdálených přístupů na kategorie právě dle typu přenosové sítě a dle počtu přistupovaných systémů.

2) *Dělení dle počtu cílových informačních systémů*

a) Přístup k 1 informačnímu systému

V této variantě se jedná o vzdálený přístup uživatele/skupiny uživatelů pouze k jedinému serveru či aplikaci, jde tedy čistě o jednoúčelový typ přístupu. Tento typ přístupu je de facto běžnou komunikací v rámci privátních sítí LAN, ať už pro použití aplikace či pro její vzdálenou správu administrátorem.

Tento typ přístupu je také využíván ke vzdálenému přístupu uživatele přes veřejnou síť k firemní aplikaci. Z titulu otevřené veřejné sítě jsou nároky na použití větší, především co se týče zabezpečení spojení. Do tohoto typu přístupu spadá popsaná firemní aplikace OWA.

b) Přístup k n-systémům

Varianta přístupu k více systémům najednou je naprosto odlišná od předchozí. Pro zajištění přístupu k více systémům najednou již nelze realizovat pouze účelové spojení k jedné aplikaci, ale musí být zajištěno spojení k celé síti, kde se aplikace nacházejí. Pro to je využita jiná, většinou veřejná síť.

Přístup k celé síti můžeme souhrnně označit jako koncept **VPN – Virtual Private Network**. Více o konceptu VPN dále. Tento typ přístupu můžeme ještě rozdělit na dvě větve, a to dle spojovaných celků:

I. Client to LAN

- typ přístupu, kdy ke vzdálené síti přistupuje klient (nebo více jednotlivých klientů)
- sem spadá jak RAS tak Citrix/SWA systémy

II. LAN to LAN

- typ přístupu, kdy se vzájemně spojují technologií VPN dvě (nebo více) vzdálených privátních sítí přes nějaké veřejné přenosové médium

3) Dělení dle typu přenosového média

Jde o rozdělení dle přenosového média, přes které se jednotlivé vzdálené celky spojují.

a) uzavřená linka bod – bod (komutovaná linka)

- linka je přímá mezi dvěma body – jde buď o telefonní či isdn linku, již se používá velmi málo
- RAS je příkladem typu vzdáleného systému Client-LAN přes komutovanou linku

b) otevřená síť s více uzly

- vzdálený přístup je realizován přes otevřenou síť, nejčastěji Internet, či jiné otevřené sítě typu WAN
- v otevřené veřejné síti může být komunikace mezi dvěma prvky odposlouchána a napadena, proto vyvstává nutnost ochrany takové komunikace šifrováním a autentizací (viz.dále)

- Citrix/SWA je příkladem typu vzdáleného systému Client-LAN přes otevřenou síť

Jistě by se dalo najít další možné dělení, pro účely této práce je to však dostatečné. V dalším textu budu již nadále uvažovat pouze spojení ***přes otevřenou veřejnou síť*** typu ***Client-to-LAN*** (tedy typ přístupu k *n-systémům*), tedy koncept/technologii Virtual Private Network - VPN.

Úvod do konceptu VPN:

Virtuální privátní sítí je obecně označováno spojení mezi klientem a privátním systémem/sítí nebo mezi dvěma sítěmi realizované přes veřejnou síť, kde je potřeba VPN komunikaci zabezpečit. Pro její zabezpečení se mezi dvěma spojovanými body veřejnou sítí vytváří privátní tunel, ve kterém je komunikace „schována“ před ostatním obsahem veřejné sítě.

Toto „schování“ se realizuje **šifrováním tunelu a autentizací** mezi oběma body, což popisují kapitoly 4.3. a 4.4.

Toto VPN spojení zároveň může probíhat na různých vrstvách ISO/OSI modelu dle použité metody a transportního protokolu – toto stručně popisují podkapitoly 4.2.1. až 4.2.3.

Výhody použití VPN:

- rozšíření hranic působnosti bez nutnosti budovat vlastní síťovou infrsatrukturu při zachování transparentnosti spojení
- značné finanční úspory proti budování vlastní sítě
- zaručená úroveň bezpečnosti dle zvoleného typu VPN
- možnost být stále v kontaktu s daty/systémy v lokální/firemní síti

4.2.1. VPN na linkové vrstvě

Přenosový síťový systém je použit pro spojení na fyzické a linkové vrstvě, tato síť je funkční analogií konvenční privátní datové síti. Funguje tak, že se vytvoří jakýsi permanentní tunel skrze infrastrukturu mezi dvěma body – tedy

uzavřená linka bod – bod. Při spojení více lokalit se však mezi každým bodem musí vytvořit dedikovaná linka. Nevýhodou v tomto případě je nutnost použití „výhybek“ mezi tunely (zařízení CPE), a velmi rychlý nárůst tunelů při počtu více uzlů. Výhodou je oproti tomu velká flexibilita a možnost provozovat nad tunely v podstatě jakýkoliv přenosový protokol síťové vrstvy (tedy není vázano na IP).
Použitá infrastruktura – sítě ATM a Frame Relay (není určeno pro „uživatelské použití“, ale pro doručení bezpečné WAN infrastruktury na technologii ATM nebo Frame Relay).

4.2.2. VPN na síťové vrstvě

Posun VPN o jednu vrstvu výše znamená přechod od jednotlivých pevných tunelů mezi body k představě o jednotném „obláčku“ sítě, ke kterému se jednotlivé uzly VPN sítě připojují jedinou přípojkou, přičemž mohou dynamicky komunikovat každý s každým.

Další změnou je fixní orientace na standardní protokol síťové vrstvy IP z rodiny TCP/IP (potřeba přenášet jiné protokoly je řešena zapouzdřením (encapsulací) do IP paketu).

VPN na této vrstvě se dále dělí dle vlastností a funkce použití na několik dalších typů, které stručně popisují následující podkapitoly 4.2.2.1. – 4.2.2.4.

4.2.2.1. IP over IP

Typ VPN, kde přenášené pakety IP protokolu jsou zabalené do jiných IP paketů. Ty mají vlastní hlavičku a mohou tak podléhat jiné směrovací politice.
Vlastnosti:

- tunelují se celé pakety
- umožňuje připojení mobilních účastníků
- minimálně zvětšuje režii přenášených dat
- vytvoření nového paketu - nová halvička IP paketu obsahuje informaci potřebnou pro přenos v tranzitní síti
- nastavené kontrolní mechanizmy pro přenos

NEVÝHODA – absence zabezpečení, není vhodné pro použití přes veřejnou síť!

4.2.2.2. GRE

Typ přenosu původně vyvinutý firmou Cisco. Cílem je umožnit vytvoření tunelů, které budou uzpůsobené pro přenos paketů jednoho protokolu skrze jiný protokol (nevyžaduje, aby šlo o IP protokol).

Vlastnosti:

- definuje, jakým způsobem by měly být pakety zabaleny a předány transportnímu protokolu
- je nezávislý na transportních protokolech
- vytvoření nového paketu – nedochází k přiložení původních dat hned za hlavičku jako u IPoverIP, ale data jsou nejprve zabalena do GRE protokolu a ten je teprve předán k přenosu

NEVÝHODA – opět chybí jakékoliv zabezpečení, navíc GRE poměrně hodně zvětšuje režii přenášených dat.

4.2.2.3. PPTP/L2TP

PPTP:

- využívá pro svou činnost point-to-point protokol (PPP)
- vytvoření paketu – paket je obalen do PPP, poté zabalen do upravené verze GRE, a teprve potom předán protokolu IP, který vytvoří ještě jednu hlavičku a pošle jej sítí
- protokol PPTP postaven na modelu klient – server = jedna strana nejprve spojení sestaví (realizováno TCP spojením iniciovaným klientem směrem k serveru), po navázání spojení je možné mezi klientem a serverem obousměrně posílat IP pakety
- přerušení kontrolního spojení přeruší i IP provoz

Zhodnocení:

- nedefinuje žádné zabezpečení nad přenášenými daty (vše je na PPP = slabé zabezpečení)
- podporuje jen 255 současných spojení a 1 tunel na uživatele
- obsažen v produktech Microsoft

L2TP:

- layer 2 tunneling protocol, je výsledkem spolupráce členů fóra PPTP, Cisca a organizace IETF
- kombinuje vlastnosti PPTP a L2F (layer 2 forwarding – ten vyvinut Ciscem)
- používá autentizační schéma protokolu PPP; přenáší PPP skrz sítě, které nejsou PPP; zapouzdřuje PPP datagramy pro přenos transportní sítí a v cílové adrese je datagram rozbalen
- funkce LNS (zabezpečí vlastní přístup do vnitřní sítě) a LAS (autentizace uživatele)
- plně podporuje IPSec !
- podporován spol. Microsoft od verze Windows 2000

4.2.2.4. IPSec

Protokol IP Security je bezpečnostní rozšíření protokolu IP přidáním bezpečnostních mechanizmů do IP vrstvy. Díky zabezpečení na síťové vrstvě je nezávislý na vyšších protokolech TCP/UDP. Je definován v několika desítkách norem RFC s tím, že základní jsou 2401, 2411 a 2784.

Bezpečnostní mechanizmy jsou dva:

1) Autentizace (ověřování)
   Definuje vlastní původ dat. Příjemce si může ověřit, že právě přijatý IP paket pochází opravdu od toho, kdo jej vyslal.
2) Šifrování
   Obě strany se předem dohodnou na formě a algoritmu šifrování paketu. Poté dojde k zašifrování celého paketu kromě hlavičky, případně celého paketu s přidáním nové hlavičky.

Skládá se ze dvou protokolů:

1) AH (Authentication Header)
   Zajišťuje autentizaci odesílatele a příjemce a integritu dat v hlavičce, ale vlastní data nejsou šifrována.

2) ESP (Encapsulation payload security)
   Taktéž zajišťuje autentizaci odesílatele a příjemce, a navíc přidává šifrování paketů. Vnější hlavička ale není chráněna a není zaručena její integrita, proto často používán zároveň i AH.

Vlastnosti:

- mohou se vytvářet šifrované tunely VPN, nebo se může jen šifrovat komunikace mezi dvěma počítači (vytvoření tunelu mezi dvěma stanicemi či branami a jeho zabezpečení)
- povinná součást protokolu IPv6, do IPv4 byl implementován dodatečně
- režim přenosu tunel a transport
- systém dvou databází pro šifrování – SPD (Security Policy Database) a SAD (Security Association Database) – souhrnně říkají, jak nakládat s datovými toky a jak šifrovat

Zhodnocení:

- až tento VPN protokol je díky jeho vlastnostem a zabezpečení široce podporován pro výstavbu VPN sítí, dnes je IPSec nejrozšířenějším standardem pro korporátní VPN řešení
- IPSec je integrován do všech moderních bezpečnostních systémů a Firewallů s VPN funkcionalitou

4.2.3. VPN na transportní a aplikační vrstvě

VPN na těchto vrstvách je vlastně myšlen protokol SSL (Secure Socket Layer), resp. novější a dnes více používaný protokol TLS (Transport Layer Security), který je vlastně SSL verze 3.1. Jde o protokol definující způsob šifrování a autentizace přenášených dat na úrovni vyšší vrstvy ISO/OSI modelu.

Vlastnosti:

- šifrována jsou pouze data přenášená samotnou aplikací, která SSL implementuje

- SSL využívá pro počáteční výměnu klíčů pro komunikaci asymetrické kryptografie, případně kryptografie založené na veřejném a privátním klíči (použití certifikátů)
- samotné spojení je poté zejména kvůli rychlosti a výpočetní nenáročnosti šifrováno rychlými symetrickými šiframi (např. 3DES, AES)
- pomocí hash funkcí (např. MD5, SHA1) je zajištěna integrita přenášených dat podobně jako u protokolu AH u IPSec

Zhodnocení:

- toto řešení je modernější než řešení IPSec
- podstata oproti IPSec je ovšem jiná, IPSec je protokol 3. vrstvy, jeho funkce je pouze ve vytváření virtuálních sítí nad veřejnou infrastrukturou, kdy klient se přes virtuální síť stane plnohodnotným členem sítě vzdálené
- SSL VPN oproti tomu funguje až do aplikační vrstvy, resp. na vytvoření šifrovaného spojení SSL je potřeba aplikace, která to zajistí
- SSL VPN řešení proto není vhodné na připojování klienta do vzdálené sítě (také umí, ale přes aplikační vrstvu), ale spíše na vzdálené publikování dílčích aplikací a zabezpečený přístup k nim (SSL VPN je de facto současné řešení Citrix)
- SSL VPN se v poslední době také stává velmi rozšířeným systémem integrovaným do mnoha VPN/Firewall bezpečnostních zařízení. Oproti běžné IPSec je však mnohem dražší (vyplatí se zvolit až při požadavcích na nadstandardní funkcionalitu)

Z uvedené teorie vyplývá, že jediné dva protokoly, které umí zajistit službu autentizace a šifrování, jsou IPSec VPN a SSL VPN. Pro běžný plnohodnotný přístup klienta do vzdálené sítě je vhodnější použít IPSec VPN.

4.3. Zabezpečení VPN

Zabezpečení vzdáleného přístupu VPN je řešeno na několika úrovních. První a nejdůležitější z nich je autentizace obou stran, šifrování navázání spojení a šifrování navázaného VPN tunelu. To je řešeno právě funkcí autentizace a šifrování zvolených VPN protokolů na úrovni protokolů.

Pro VPN IPSec jde o výše popsanou metodu kde:

- navázání tunelu je řešeno protokolem IKE (Internet Key Exchange), kdy dojde ke vzájemné výměně šifrovacích klíčů (použit buď sdílený klíč (preshared key) a nebo systém veřejného a privátního klíče – certifikát)
- udržování tunelu řešeno šifrováním protokolu IPSec (ESP a AH)

Pro SSL VPN jde o také výše popsanou metodu kde:

- počáteční výměna klíče je řešena asymetrickým šifrováním, příp. certifikáty
- navázané spojení pak šifrováno symetrickými šiframi (3DES, AES) a integrita zajištěna hash funkcemi (MD5, SHA1)

Celý postup můžeme zobecnit pro obě řešení na tyto metody/mechanizmy:

- Výměna klíčů klienta a brány – IKE: méně bezp. varianta je sdílený klíč, více bezpečná varianta je veřejný a privátní klíč (certifikát). Kryptografický protokol zajištující bezpečnou výměnu sdíleného klíče přes ještě nešifrovaný kanál se nazývá Diffie-Hellman a dělí se do skupin 1, 2, 5 a 7 dle délky klíče. Výměna klíče může být realizována v nebezpečném zrychleném módu 3 výměn (aggressive mode – náchylný na odposlouchání), nebo v normal modu 5 výměn. Pro výměnu veřejného a privátního klíče se používá metoda RSA.
- Šifrování navázaného tunelu: SSL metodou asymetrické kryptogtafie (bezpečnější), IPSec metodami symetrické kryptografie. Běžně používané symetrické algoritmy jsou: 3DES (168bit klíč), AES (až 256bit klíč)
- Hashovací funkce: MD5, SHA

Na zabezpečení systému VPN mají vliv také další faktory. Podstatnými z nich jsou tyto:

- celková koncepce a design systému pro vzdálený přístup – musí být realizováno dle bezpečnostních standardů (např. umístění do DMZ)
- metody autentizace identity uživatele a autorizace jeho přístupových práv (řeší následující kapitola)
- kvalitní konfigurace VPN přístupových tunelů – striktní access listy, použití QoS, pravidelné revize
- systémové zabezpečení – zabezpečení vlastní konfigurace systému - inspekce VPN komunikace, použití Firewallů, použití externích systémů kontrolujících aktuální stav a vlastnosti uživatele a kontrolujících přístup k síti (Network Admission Control)
- procesní zabezpečení – vytvoření závazných politik použití VPN, kontrola přístupů, atd.

4.4. Autentizace a autorizace

V případě vzdáleného přístupu mluvíme o autentizaci a autorizaci jako o jednom procesu, který má za cíl ověřit identitu uživatele (=autentizace) a zajistit aplikaci přístupových oprávnění do systémů (=autorizace). Obě metody by měly být vhodně zvoleny tak, aby odpovídaly zvoleným bezpečnostním požadavkům. Při volbě je třeba myslet na fakt, že čím lepší zvolená metoda, tím větší je celkové zabezpečení systému VPN.
Náhled na stupně ochrany a možné použité metody zobrazuje následující tabulka:

Stupeň ochrany	Metoda	Popis
Základní	Jméno a heslo	Autentizace pomocí statického uživatelského jména a hesla
Střední	Jméno a jednorázové heslo	Autentizace pomocí jména a jednorázově platného hesla (například S/Key)
Standardní ochrana	Dvoufaktorová autentizace bez interakce uživatele	Uživatel vlastní autentizační předmět generující jednorázová hesla bez nutnosti vložení PIN, předmět je vázán na uživatelské jméno.

Silná ochrana	Dvoufaktorová autentizace s interakcí uživatele	Uživatel vlastní autentizační předmět generující jednorázová hesla s vazbou na své přihlašovací jméno. Pro použití předmětu musí navíc zadat PIN. (například řešení SecurID, Vasco, Cryptocard)
Velmi silná ochrana	Dvoufaktorová autentizace s interakcí uživatele a kryptografickými funkcemi.	Kryptografická autentizace za použití certifikátů a předmětu chránícího privátní klíč na základě hesla (např. Smart Card).

Z tabulky je patrné, že ve všech stupních ochrany se vyskytuje heslo uživatele, ať už vázané na přístupové jméno či nějaký autentizační předmět. Je třeba mít na mysli, že je vždy bezpečnější využít k ověřování nikoliv VPN - interní, ale externí systémy/databáze uživatelů umístěné v DMZ či ve vnitřní síti dle topologie. Při existenci takových zdrojů a databází uživatelů se jednak šetří náklady a jednak čas potřebný na vytvoření databáze uživatelů a její případné duplicitní udržování s jinou databází.

Nejčastější příklady použití externích zdrojů:

- adresářové služby LDAP (Active Directory, Novell NDS, atd.)
- Kerberos, NIS, NIS+
- RADIUS / TACACS / AAA
- Certifikační Autorita
- RSA Secure ID či jiné tokeny

Velmi důležité je nastavení bezpečnostních procesů pro správu adresářových služeb či jiných databází uživatelů. Toto je nutné zejména pro sledování aktuálnosti uživatelských profilů (zda je stále zaměstnancem) a při řešení incidentů (např. zneužití uživ.přístupu). Správným nastavením procesu se zvýší celkové zabezpečení systému.

5. NÁVRH ŘEŠENÍ

V této části práce se již dostáváme k samotnému návrhu nového systému pro vzdálený přístup do interní sítě Tesco. Na základě analýzy potřeb společnosti navrhnu vhodný typ vzdáleného přístupu, vyberu konkrétní řešení a navrhnu začlenění tohoto řešení do IT struktury společnosti. Součástí návrhu bude i stručný plán implementace nového systému. Závěrem kapitoly návrh zhodnotím jak z pohledu kvantitativního, tak kvalitativního, s jasnou identifikací přínosů a případných záporů či rizik návrhu.

5.1. Návrh typu a parametrů systému vzdáleného přístupu

Na základě stanovených potřeb společnosti a jejich požadavků na funkčnost a bezpečnost systému navrhuji, aby nový systém VPN splňoval tyto podmínky:

- Systém pro vzdálené připojení bude připojen na Internet, spojení mezi klientem a bránou musí tedy být zabezpečeno tunelováním a šifrováním = systém pro přístup bude typ VPN fungující na 3. vrstvě ISO/OSI modelu (síťové vrstvě)
- Každá země regionu CE bude mít svůj přístupový bod VPN umístěný na perimetru sítě v CDC = 4 přístupové body systému (a tedy min. 4 stejná zařízení) s možností vzájemné redundance buď na úrovni systému nebo na úrovni nastavení klienta
- Protokol pro realizaci VPN – IPSec
- Podpora jak UDP VPN, tak TCP VPN
- Metoda navázání spojení: IKE, normal mode i aggressive mode
- Požadované šifrovací metody a hash: AES / 3DES, SHA1 / MD5
- Podpora minimálně 500 současných VPN tunelů v každém zařízení
- Propustnost alespoň 100Mbps.
- Podpora NAT-traversal (podpora vpn komunikace přes zařízení, které překládá ip adresy)
- Podpora QoS (funkce prioritizace a omezení šířky pásma)

- Vyžadovaný typ spojení je Client-VPN, na straně klienta musí být použit VPN client software.
- VPN klient s vpn profilem podporuje jak Group autentizaci preshared klíčem, tak klientské certifikáty – tedy funkcionalita navázání na vzdálenou certifikační autoritu
- Podpora dvoufaktorové autentizace (VPN profil s certifikátem nebo SecureID, jméno/heslo Active Directory)
- Zařízení musí mít vestavěný firewall se stavovou inspekcí komunikace
- Musí využívat existující služby infrastruktury
- Centrální vzdálená distribuce uživatelských vpn profilů pro vpn klienty
- Dále musí splnit všechny požadavky uvedené v kapitole 3.3.

5.2. Návrh a výběr technických prostředků

V této kapitole navrhnu možné technologické varianty systému splňující stanovené požadavky a parametry nového systému, včetně jejich cenové kalkulace, hlavních výhod či nevýhod. Posléze provedu ohodnocení variant dle definovaných kritérií výběru, čímž určím vítěznou variantu pro projekt.

Jde tedy o návrh těchto technických prostředků:

- 4x brána či cluster pro vzdálený přístup
- 4.000 klientů (kusů VPN Client SW, popř. jejich licencí)

Poznámka: volba vhodných existujících interních systémů pro doplnění řešení o potřebné služby je závislá na výběru technologie přístupových bran a jejich vlastnostech. Z toho důvodu bude výběr řešen až v kapitolách 5.3 a 5.4.

5.2.1. Určení kritérií a metody výběru

Výběr řešení bude dvoukolový. V prvním kole je jediné kritérium výběru, a to splnění všech požadavků z kapitoly 5.1. Do druhého kola projdou pouze ty technologie, které toto splní.

Stanovená kritéria výběru pro druhé kolo a jejich váhová hodnota:

1) pořizovací cena (cena za HW a implementaci) - váha 4
2) cena ročních nákladů na provoz a údržbu systému - váha 5
3) komfort administrace technologie (snadnost, možnosti) - váha 4
4) komfort použití systému uživatelem - váha 3
5) podpora výrobce - váha 3
6) reference technologie na trhu a „price for future“ - váha 2

Metoda výběru pro druhé kolo:

- do tabulky budou zapsána uvedená kritéria a jejich váhová hodnota a hodnocené varianty
- každá varianta dostane ke každému kritériu známkové ohodnocení dle klíče: (1=špatné, 2=průměrné, 3=dobré, 4=výborné)
- pro každé kritérium se obdržená známka násobí příslušnou váhovou hodnotou, výsledek je počet bodů
- vítězí varianta s nejvyšším součtem bodů všech kritérií

5.2.2. Stanovení množiny možných kandidátů

Jedním z nevýrazných, avšak poměrně důležitých stanovených požadavků je, že navržená technologie musí být dobře známá (resp. musí se umět spravovat) mezi zodpovědným technickým IT personálem společnosti, a i relevantním dodavatelem. Důvodem tohoto požadavku je fakt, že projekt, implementace a následná správa bude kryta z větší části interními IT zdroji firmy, což je poměrně neobvyklé. Díky tomu máme v podstatě hodně zúžený výběr jen na následující technologie, které požadovanou funkcionalitu IPSec VPN umějí dodat:

Unix/Linux
Microsoft (ISA Server)
Cisco
Juniper
3COM.

3Com nedodává potřebnou technologii, vyřazen z výběru.

Unix/Linux potřebná technologie existuje, avšak nesplňuje stanovená kritéria kapitoly 5.1. Nepostupuje do druhého kola výběru.

Windows potřebná technologie existuje. Platforma by byla silným konkurentem, avšak také nesplňuje některá stanovená kritéria (správa systému, možnosti konfigurace). Nepostupuje do druhého kola výběru.

Cisco zcela splňuje stanovená kritéria a postupuje do druhého kola výběru. Níže navrhnu vhodnou variantu postavenou na této technologii pro hodnocení ve druhém kole.

Juniper zcela splňuje stanovená kritéria a postupuje do druhého kola výběru. Níže navrhnu vhodnou variantu postavenou na této technologii pro hodnocení.

Do druhého kola výběru tedy postupuje řešení Cisco a Juniper.

5.2.3. Návrh variant a cenová kalkulace

Tato podkapitola popisuje dvě mnou navržené varianty systému pro vzdálený přístup postavené na vyhovujících technologiích Cisco a Juniper. Jde konkrétně o tyto systémy:

Varianta 1 Cisco ASA 5520 Security plus licence

Varianta 2 Juniper SSG 520M

Vzhledem k rozsáhlosti návrhu obou variant včetně podrobných cenových kalkulací jsou obě popsané varianty přílohami této práce. **Varianta 1** technologie Cisco je **PŘÍLOHOU 1** této práce. **Varianta 2** technologie Juniper je **PŘÍLOHOU 2** této práce.

V přílohách jsou podrobně rozepsány u obou variant jejich klíčové vlastnosti, výhody a nevýhody, a také zmíněná cenová kalkulace. Popis je koncipován tak, aby poskytl potřebné informace ke všem stanoveným kritériím výběru pro druhé kolo.

V této podkapitole uvedu pouze souhrn nejdůležitějších charakteristik variant s přehlednou srovnávací tabulkou nákladů.

Stručná charakteristika variant:

Varianta 1 - Cisco

Řešení technologie Cisco je přímo zaměřené na doručení VPN funkcionality se snadným použitím a s co nejmenšími náklady. To je určeno jednak tím, že existuje cílená hardwarová edice s vylepšenými VPN vlastnostmi (nadstandardní počet 750 VPN tunelů, atd.), která vznikla sloučením dřívějších VPN koncentrátorů a Firewallu, a jednak tím, že není licencováno použití běžné IPSec VPN (klienti IPSec VPN zdarma!). Její použití z uživatelského hlediska je velmi snadné při zachování velkého komfortu práce, a funkcionalita může být doručena teoreticky neomezenému počtu uživatelů. To vše je na druhou stranu vyváženo neexistencí nástrojů pro centrální správu, horšími parametry některých funkcí, nižšímu zabezpečení při základní konfiguraci (především zrychlený aggressive mode při použití VPN profilu s Preshared klíčem bez certifikátu), horší podporou výrobce, a celkově jaksi menší „robustností“ oproti konkurenční technologii.

Nejvýznamnější parametry:

- 750 současných VPN tunelů IPSec i SSL, velmi jednoduchý a komfortní IPSec Client SW s integrovanou funkcí redundance, který je navíc zdarma v neomezeném množství (licencuje se jen SSL VPN)
- VPN propustnost až 225 Mbps
- dobrá podpora všech potřebných externích systémů

Nejvýznamnější výhody:

- přímo zaměřené na doručení IPSec VPN služby
- celkově nízká cena technologie, dobrá „price for future“
- velmi dobrá znalost technologie IT personálem a dodavatelem

Nejvýznamnější nevýhody:

- chybějící nástroj pro centrální správu
- horší podpora výrobce, časté bezpečnostní chyby a upgrade firmware
- jen zrychlený aggressive mode IKE autentizace při Preshared klíči

Varianta 2 - Juniper

Řešení postavené na technologii Juniper je oproti tomu opravdu špičkou ve své kategorii. Jde čistě o moderní typy Firewallů pro náročné, kombinující mnoho různých funkcionalit jako Antivirus, IPS (systém pro prevenci průniku),

Antispam, Web filtering, a právě VPN (souhrnně označovaná technologie UTM). Samozřejmostí je server pro kompletní centralizaci systému mnoha zařízení s nadstandardními službami pro ukládání a analýzu logů a management reporting. Z hlediska VPN funkcionalit umí vše to, co Cisco, a ještě mnohem více včetně komplexní SSL VPN. Tomu odpovídá i velmi robustní VPN klient pro použití se všemi VPN funkcemi, a to jak pro IPSec tak SSL. Logickým důsledkem je pak licencování VPN klientů, což celkovou pořizovací cenu zvedá o několikanásobek oproti konkurenční variantě. Použít takový systém jednoúčelově jen na VPN je právě díky jeho možnostem a parametrům neefektivní vzhledem k vynaloženým prostředkům, takové řešení se spíše hodí jako produkční korporátní multifunkční Firewall.

Nejvýznamnější parametry:

- 500 současných VPN tunelů IPSec i SSL, robustní VPN Client SW sdružující IPSec i SSL funkcionalitu, ale licencovaný „per user“!
- VPN propustnost až 300 Mbps
- dobrá podpora všech potřebných externích systémů

Nejvýznamnější výhody:

- robustnější řešení nejen na VPN ale celou škálu služeb a Firewallingu
- výborná podpora výrobce, dobrá „price for future“
- IKE pracuje v bezpečnějším Normal módu i za použití Preshared klíčů
- server centrální správy s mnoha nadstandardními funkcemi

Nejvýznamnější nevýhody:

- vysoká pořizovací cena
- náročnější na správu také díky horší znalosti technologie

Stručné cenové srovnání:

Tab. 1. - Souhrnná srovnávací tabulka nákladů obou variant:

	Varianta 1 - Cisco	Varianta 2 - Juniper
Pořizovací cena technologie	415 280 Kč	2 327 188 Kč
Externí instalační cena	380 000 Kč	0 Kč
Roční maintenance servis	105 560 Kč	174 768 Kč
Roční cena podpory dodavatelem	2 160 000 Kč	2 700 000 Kč
Celkové provozní náklady za rok	3 213 560 Kč	3 822 768 Kč

Cenová kalkulace v Přílohách 1 a 2 je rozdělena na tyto části:

1) celková cena pořízení HW technologie (řádek 2 tabulky)
2) celková cena instalace systému (řádek 3 tabulky)
3) roční náklady na provoz (řádek 6 tabulky, součet řádků 4 a 5 a dalších nákladových položek)

Poznámka – náklady jsou vyčísleny v Kč bez DPH. Pro převod z USD a Eura byl použit kurz, který byl relevantní v době návrhu a pořízení – 1Euro = 29,00Kč; 1USD = 22,00Kč.

5.2.4. Výběr z definované množiny dle definovaných kritérií

V této podkapitole vyhodnotím obě varianty dle kritérií pro druhé kolo výběru stanovených v 5.2.1. Hodnocení je provedeno metodou popsanou v 5.2.1. Varianta, která získá nejvíce bodů, je vítězná. Hodnotící tabulka je uvedena níže.

Tab. 2. - Tabulka hodnocení variant dle kritérií:

Hodnotitel - Richard Ondrák		**Varianta 1 - Cisco**			**Varianta 2 - Juniper**		
Kritérium	**Váha**	**+ / -**	**Známka**	**Body**	**+ / -**	**Známka**	**Body**
Pořizovací cena (cena za HW a technologii)	4	sleva díky centrálnímu kontraktu	4	16	nutnost licencování uživatelů	1	4
Cena ročních nákladů na provoz a údržbu	5	relativně nízký support, ale další dodatečné náklady	3	15	dražší support díky "složitějšímu" systému	2	10
Komfort administrace technologie	4	výborná znalost, komfortní web mgmt	3	12	obdobné jako Cisco, navíc centralizace	4	16
Komfort použití systému uživatelem	3	jednoduché a rychlé použití, klient backup	3	9	klient integrovaný IPSec i SSL VPN	3	9
Podpora výrobce	3	problematičtější komunikace s výrobcem	2	6	velmi nadstandardní	4	12
Reference technologie na trhu a "price for future"	2	masové rozšíření technologie, avšak často nový firmware	3	6	především USA, nyní velmi rychle i Evropa, velmi stabilní	3	6
Celkové bodové hodnocení				**64**			**57**

Vítězem se stala se 64 body především díky ceně varianta 1, tedy Cisco ASA 5520 Security Edition.

5.3. Začlenění řešení do stávající infrastruktury a jeho funkce

V dalším textu se již dostávám k začlenění vybrané technologie do struktury společnosti a definici provozu. V této kapitole navrhnu architekturu celého systému se všemi službami a jejich funkcemi a zobrazím zapojení do současné síťové infrastruktury. Návrh designu systému a jeho funkcionalit je vypracován tak, aby přesně kopíroval všechny stanovené požadavky, a doručil firmě komfortní řešení, které co nejlépe vyplní potřeby uživatelů i firmy.

Funkce a prvky systému:

Celý systém pro vzdálený přístup je navržen tak, aby nastavil co nejvyšší úroveň bezpečnosti, a aby byl snadno spravovatelný. Z tohoto důvodu potřebujeme rozšířit funkcionalitu pro přístup i mimo zvolené přístupové brány Cisco tak, aby první fáze autentizace a vytvoření VPN tunelu byla ověřena bránou, a druhá fáze ověření proběhla externě doménovým účtem uživatele. Celý systém se proto bude skládat z těchto prvků a funkcí:

- uživatel: nainstalovaný Cisco VPN Client software, v klientovi uložen uživatelův přístupový profil s Group loginem a Group preshared klíčem pro první IKE autentizaci (tedy ověřením něčím „co mám“), po vytvoření VPN tunelu se uživatel ověřuje zásadně jeho doménovým účtem (tedy něco, „co znám“)
- přístupový bod pro navázání VPN tunelu s uživatelem a první fázi IKE autentizace: brány Cisco na perimetru internetu a Tesco LAN
- prvky pro druhou fázi autentizace - ověření doménového účtu uživatele: brána Cisco přepošle na RADIUS server Windows IAS v interní LAN, RADIUS zpracuje požadavek a dotáže se Domain Controlleru s Active Directory pro ověření zadaných údajů a jeho sady platných politik, výsledek (povolení/zamítnutí) posílá zpět na Cisco a uživateli
- automatická distribuce klientů, jejich profilů, a vzdálená správa uživatelů: doména MS Windows (Domain Controllery)

- ukládání, správa a analýza logů: export na Linux Syslog server
- mailové výstrahy ze systému: přes SMTP protokol na Exchange server

poznámka:

1) Jakmile bude mít Tesco svoji Certifikační autoritu (dodání plánováno cca za 1rok v rámci jiného projektu), rozhodně plánuji její využití pro lepší ověření uživatele a razantní zvýšení bezpečnosti (certifikát uživatele vázaný na jeho firemní notebook nahradí použití Group preshared klíče v jeho VPN profilu, který se tak stane nepřenosný).
2) Zavrhuji použití RSA Secure ID pro uvěření identity uživatele tokenem. Použití by sice přineslo o hodně vyšší zabezpečení plnohodnotnou dvoufaktorovou autentizací při současném použití s doménou, avšak za razantního zvýšení nákladů (1 token pro 1 uživ. = 3.000,-Kč na 2 roky, tzn. při 4.000 uživatelů je náklad 12mil.Kč/2roky).

Celý postup připojení uživatele můžeme stručně popsat těmito kroky: uživatel se mimo firmu připojí na internet a pustí si Cisco VPN klient. Spustí připojení svým centrálně distribuovaným profilem. V profilu je uložena uživatelova skupina, primární přístupová brána a záložní přístupová brána. Profil se spojí s nastavenou bránou a ověří se skupinovým jménem a preshared klíčem a vytvoří IKE tunel. Uživatel je dotázán na doménu, jméno a heslo. Jeho ověření zajistí RADIUS v interní LAN ve spolupráci s Active Directory databází. Při úspěšném ověření je vytvořen IPSec tunel mezi klientem v internetu a VPN bránou. Klient dostane od brány přidělenu IP adresu z interní LAN adresace vyhrazené pro VPN klienty, a klient se stává součástí vnitřní sítě Tesco. Klient má přístup do té části sítě (na ty aplikace), kam povolují jeho skupinové access listy nastavené na bráně.

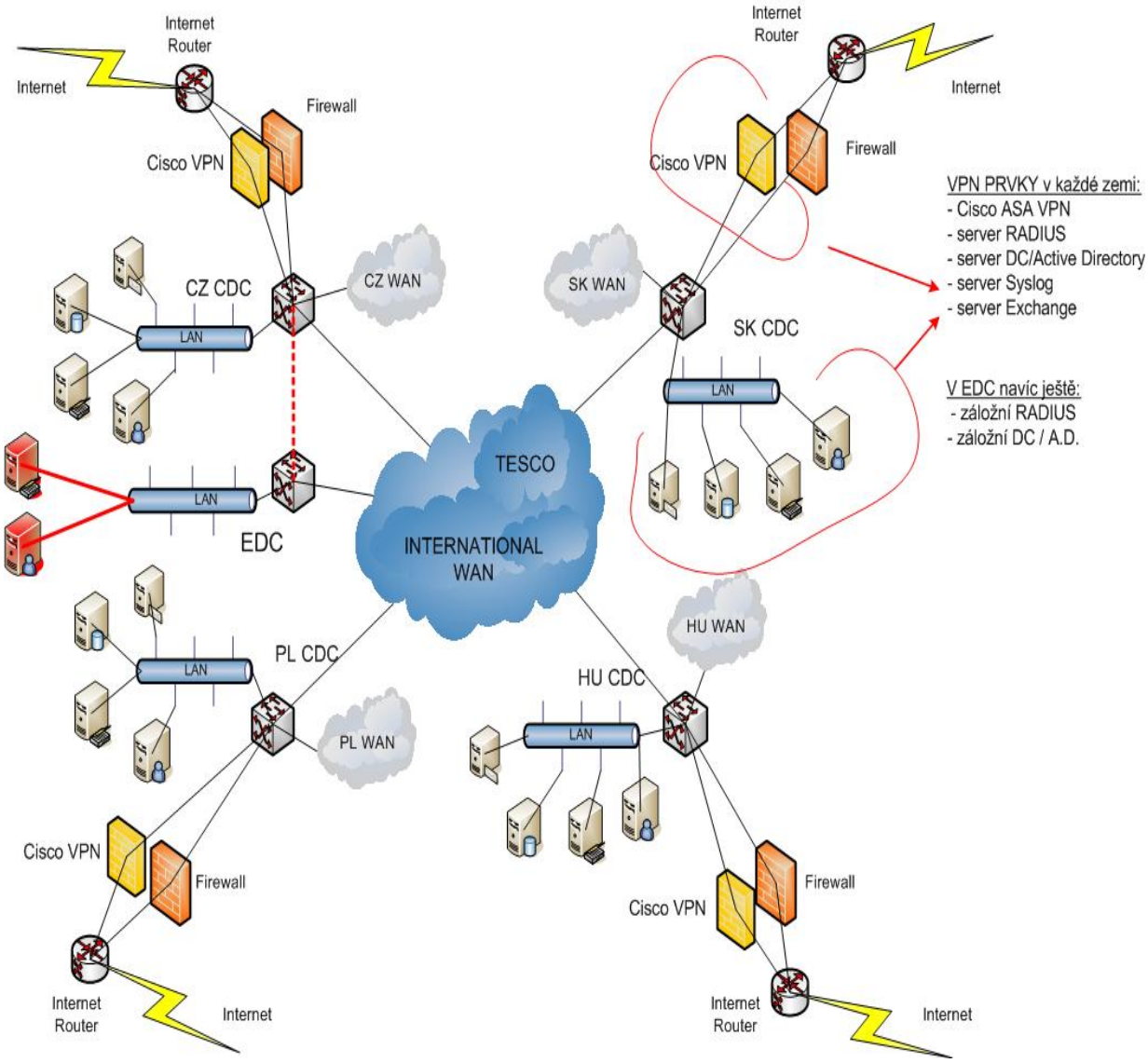
S tím, že v regionu CE existují 4 sub-domény, jsou skupiny uživatelů rozděleny dle doménového členství v jednotlivých zemích. Každá země má svůj přístupový bod a svoje vlastní navržené interní systémy. Systémy jedné země však musí zajistit přístup a ověření i uživateli z jiné země pro dodržení požadavku redundance při výpadku jedné brány.

Více o konfiguraci samotných VPN bran Cisco a dalších prvků je uvedeno v kapitolách 5.4 a 5.5.

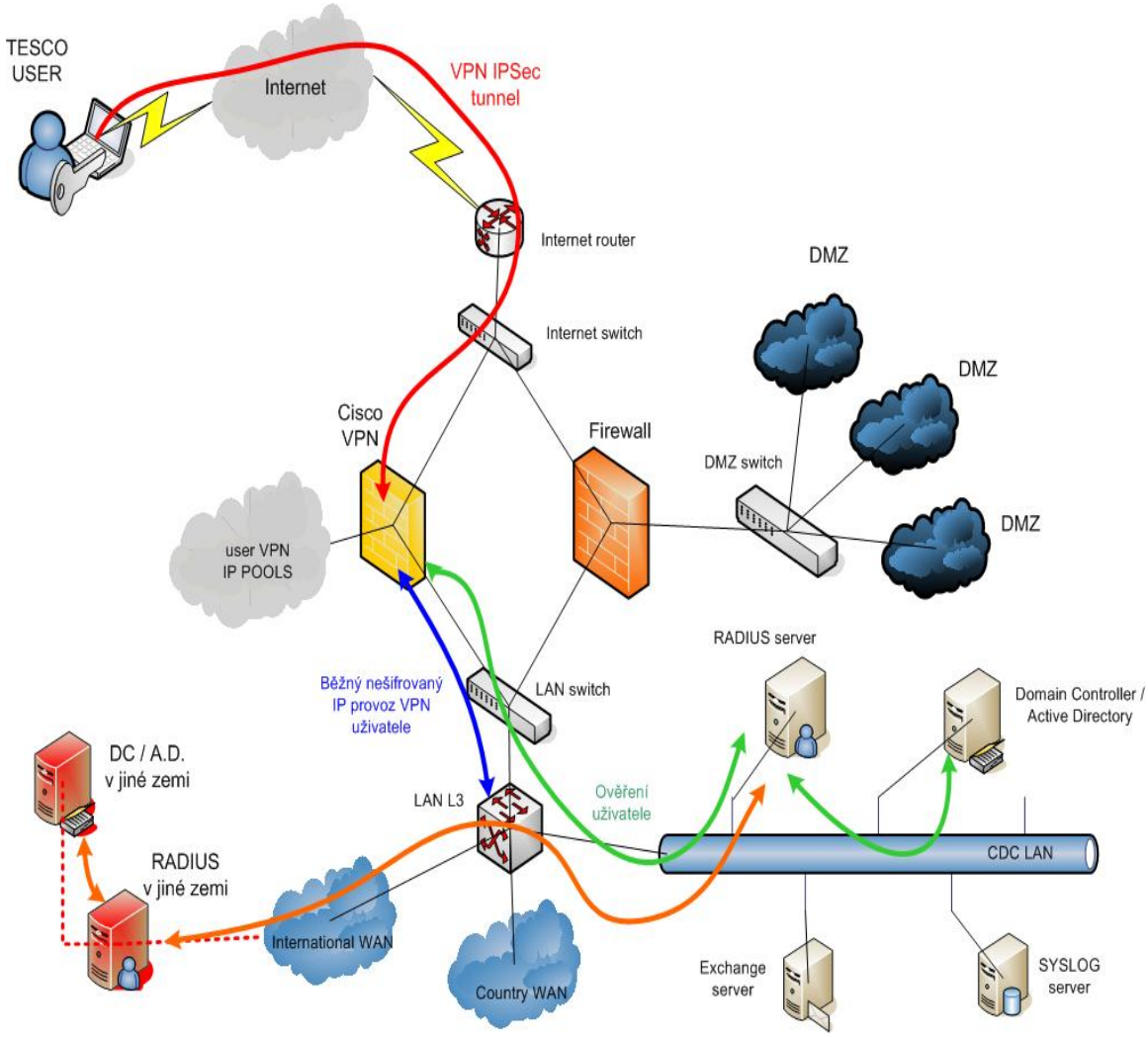
Architektura systému:

V tomto odstavci podrobně zobrazím architekturu systému a jeho začlenění do Tesco infrastruktury v celém regionu CE. Topologie zapojení přístupových bran na perimetrech datacenter a jejich navázání na vnitřní systémy jednak vychází z nastavených požadavků firmy a jednak přesně kopíruje potřebný postup připojení a jeho funkce.

Obr. 7. – Grafické znázornění topologie celého systému s interními servery infrastruktury v regionu CE:



Obr. 8. – Detail zapojení jedné země od uživatele v internetu přes VPN bránu Cisco na perimetru sítě až po servery interních služeb:



Důležitá fakta patrná ze zobrazení:

- VPN brána pro každou zemi zapojena na perimetru sítě datacenter CZ CDC, SK CDC, PL CDC, HU CDC, paralelně se stávajícím produkčním Firewallem
- na VPN bránu je routován z Internet routeru pouze VPN provoz, ostatní provoz mezi Internetem a Tescem jde nadále přes produkční Firewall
- z centrálního CDC LAN L3 switche jsou na VPN bránu routovány jen potřebné IP rozsahy
- záměrně neuvádím IP adresaci jednotlivých prvků, tuto informaci nemohu zveřejnit, obecně však uvedu toto: všechny vnitřní LAN používají neprivátní, avšak zatím v internetu neroutované ip rozsahy o velikosti A

rozdělené na menší rozsahy dle lokalit, pro zabezpečení vnitřní sítě resp. její oddělení od internetu je na VPN bráně nastaven NAT (překlad adres) tak, že celá vnitřní síť z Inside Interface se NATuje na 1 veřejnou internetovou ip adresu Outside Interface VPN brány z přiděleného public ip rozsahu (NAT na interface), přesto je však všechen provoz kromě zpětného VPN ven přes NAT zakázán

- VPN brána tedy není nastavena v Routed módu ale Firewall Transparent módu (LAN a Internet mezi sebou nejsou routovány – jsou odděleny)
- na vnějším i vnitřním interface VPN brány je povolen POUZE potřebný UDP VPN provoz (porty UDP 500, UDP 4500, ESP, na straně Outside: ANY, na straně Inside: pouze vnitřní VPN IP rozsahy), nic kromě VPN tunelů neprojde přes bránu ani z internetu do LAN, ani z LAN do internetu
- celý systém je složen z těchto prvků: 4x Cisco VPN brána, 5x RADIUS server komunikující s Domain Controllery v jednotlivých zemích (teoreticky 4x primární a 4x záložní, prakticky jsou v Tescu desítky Domain Controllerů), 4x Syslog server, 4x Exchange server (všechny externí systémy a jejich funkce popisuje následující kapitola 5.4., více o nastavení VPN bran, rozdělení uživatelů atd. v kapitole 5.5)

5.4. Potřebné služby infrastruktury

Přístupové brány pro svoji činnost potřebují tyto služby síťové infrastruktury: Syslog server, RADIUS server a Active Directory.

Jak je patrné ze schémat zapojení, přístupové brány v každé zemi mají potřebné externí systémy infrastruktury zapojeny přímo v lokální síti konkrétního datacentra. Důvodem je především jejich neustálá dostupnost (a tedy funkčnost VPN) i v případě výpadku WAN linky (většina uživatelů přistupuje právě jen na centrální IT systémy umístěné v datacentru) a také rozdílnost domén v každé zemi (cz.tesco-europe.com, sk.tesco-europe.com, atd.). Mezi externími systémy zemí musí také existovat komunikace z důvodu možnosti připojení uživatele z jedné země k přístupové bráně jiné země (funkce redundance) a tedy přesměrování příslušné komunikace z jednoho systému na jiný (především ověření uživatele).

Níže stručně popíšu nastavení 3 nejdůležitějších externích systémů – Syslog, RADIUS a Active Directory.

Poznámka: samostatná část není věnována 4. externímu systému – Exchange Serveru. Exchange slouží jen jako poštovní služba pro Cisco VPN bránu. Brána má nastaveno, že při určitém typu kritické události kromě zalogování události na Syslog také pošle výstražný email na nastavené zodpovědné administrátory.

5.4.1. RADIUS

RADIUS servery jsou nejdůležitější externí služba pro VPN. Jejich jedinou funkcí je služba ověřování uživatele (popis procesu níže). Jedná se o servery Windows server 2003 s nainstalovanou službou IAS (Internet Authentication Service) propojenou na doménovou databázi uživatelů Active Directory.

RADIUS serverů je celkem 5 – pro každou zemi (každou doménu) jeden, páty server je v EDC síti a doméně eu.tesco-europe.com, nadřazené všem ostatním doménám. Tento EDC slouží jako backup pro ostatní čtyři RADIUS servery.

Proces ověření uživatele:

- po group autentizaci a navázání IKE tunelu VPN brána pošle RADIUS serveru požadavek na ověření uživatele, kde předává informace – doména, login, heslo, ip adresa, pc, NAS parametry, a další
- RADIUS ověří autentičnost žadatele (tedy brány) a zpracuje požadavek, pokud požadavek projde přes nastavená pravidla, spojí se s Active Directory (Domain Controllerem) příslušné domény a ověří platnost poskytnutého loginu a hesla uživatele v dané doméně – zde nastupuje podproces ověření v rámci Active Directory (viz proces AD níže)
- RADIUS dostane z A.D. odpověď o ověření – povoleno / zamítnuto
- RADIUS odpoví VPN bráně – povolí / zakáže přístup dle odpovědi z AD
- RADIUS zaloguje informaci o události do interního logu, kde je obsažen čas požadavku, informace o bráně, informace o klientovi (ip adresa, jméno pc, doména, login, NAS parametry, atd.), výsledek ověření (povoleno / zamítnuto), čas přihlášení (posléze i čas odhlášení), plus další parametry

- RADIUS dané domény ověřuje pouze uživatele z této domény. Pakliže přijde na RADIUS požadavek z VPN brány od uživatele, který je z jiné domény, přeposílá tento požadavek na RADIUS server z příslušné domény do jiné země (RADIUS má pro toto nastaveny všechny ostatní RADIUSy). Kontaktovaný RADIUS provede popsaný proces ověření a výsledek předá zpět na původní RADIUS, ten výsledek opět přepošle na VPN bránu.
- výjimkou je EDC / EU Radius – ten umí zpracovat požadavky ze všech domén (VPN brána má nastaven jako primární RADIUS příslušné země, při nedostupnosti národního kontaktuje záložní EU)

(poslední dva body popisují funkci redundance, která je obsažena již ve VPN profilu uživatele, kde jsou nastaveny primární a záložní brána)

Konfigurace RADIUSu:

- RADIUS je členem domény – navázání na Active Directory databázi
- RADIUS má nastavenu 1 povolenou VPN bránu jako původce požadavků
- RADIUS má nastaveny odkazy na ostatní RADIUS servery systému
- nastavená sada dalších pravidel pro zprocesování ověření uživatele dle popisu procesu (jaké údaje musí obsahovat požadavek, jaká akce při požadavku, jaký server se kontaktuje pro ověření z AD, příslušnost ostatních RADIUS serverů z jiných domén, a další)
- RADIUS loguje veškeré ověřovací aktivity do svého logu

5.4.2. Active Directory

Služba Active Directory je doménovou LDAP databází uživatelů dostupnou přes Domain Controllery. V systému VPN plní 3 důležité funkce – primárně oveření příchozího požadavku na uživatele z RADIUS serveru, dále automatické doručení a aktualizace VPN profilů všech VPN uživatelů, a jako doména pomocí svých nástrojů a group politik vzdálenou správu uživatelů a jejich notebooků.

Domain Controllerů je v Tescu několik desítek – v podstatě na každé významnější pobočce. Každá ze 4 sub-domén CZ, SK, PL, HU má svoje dedikované controllery. Primární a sekundární controller dané domény je umístěn

vždy v datacentru země – přes tyto dva controllery RADIUS servery ověřují uživatele.

Doménové služby v Tescu poskytují Windows Servery verze 2003, doména je zkonfigurována v Native módu.

Funkcionalita ověření a konfigurace Active Directory:

- v Active Directory musí být vytvořeny Security Groups přesně podle existujících VPN skupin/profilů na VPN bráně (Tesco skupiny: VPN IT Admins, VPN IT Users, VPN HO Users, dále dodavatelské skupiny – viz. níže)
- všechny VPN Groups budou členy nadřazené Security Group „VPN Access“, na kterou se aplikují všechny příslušné doménové politiky
- přidělování VPN uživatelům se pak provede pouze přes nastavení v Active Directory, kdy je Tesco uživatel zařazen do některé z existujících VPN doménových skupin dle jeho přístupových potřeb (viz. 5.5) - přidělení přístupu bude realizováno přidáním doménového účtu uživatele do zvolené Security Group a modifikací vlastností doménového účtu (záložka Vzdálený přístup – zvolit řídit přístup dle doménových politik (přidávání/odebírání uživatelů a modifikaci doménových VPN Groups budou moci provádět jen oprávnění administrátoři – viz. 5.6.))
- na základě této změny je v případě požadavku z RADIUS serveru uživateli povolen přístup přes VPN
- na základě této změny se také aktivuje politika pro automatické doručení a aktualizaci připojovacího VPN profilu na notebook uživatele (viz.níže)
- při vzdáleném přístupu se následně bude ověřovat, zda je uživatel členem VPN skupiny, a zda typ VPN profilu odpovídá typu VPN Security Group, kde je členem (RADIUS – Active Directory)
- odlišný postup bude v případě dodavatelů při požadavku na přidání dodavatele: 1) vytvoří se jim samostatná skupina na VPN bráně, 2) vytvoření zcela nových doménových uživ. účtů typu Guest, 3) vytvoření nové VPN Security Group (odpovídá názvu dodavatele a názvu VPN skupiny na bráně), 4) přiřazení nových účtů do vytvořené skupiny. Skupina bude také členem nadřazené VPN Access, ověření přes RADIUS

tedy proběhne stejně. Rozdíl oproti Tesco uživateli bude pouze v absenci nastavení automatického doručování profilu.

Automatické doručení VPN profilu:

- po vytvoření příslušné Tesco VPN skupiny na VPN bráně bude vytvořen VPN profil pro použití v Cisco VPN Clientovi
- tento profil bude uložen na zvolené úložiště na jednom z doménových serverů (v každé doméně vlastní úložiště s vlastními profily)
- v doméně bude pro každý profil vytvořena Group Policy, která se aplikuje na příslušnou VPN Security Group - Group Policy se tedy aplikuje na každého uživatele, který je členem dané skupiny
- politika bude fungovat tak, že při každém restartu notebooku se stávající VPN profil na notebooku přepíše profilem z centrálního úložiště v doméně – jednak je tím zaručeno automatické a vzdálené první doručení profilu při přidání uživatele, a jednak je zajištěna automatická a včasná distribuce nových profilů při jakékoliv jejich změně
- součástí politiky budou také funkční kontrolní mechanizmy – např. kontrola, zda má uživatel pouze jeden jeho odpovídající profil

5.4.3. Syslog

Servery Syslog jsou určeny pro export, ukládání, reporting a analýzu všech nastavených typů událostí (logů) z Cisco VPN bran. Každá brána má v každé zemi svůj vlastní Syslog server, servery jsou tedy 4.

Jde o linuxové servery (RedHat) s běžící službou NG-Syslog a instalovanými analyzátory a reportovacími nastroji.

Ukládání logů s historií a jejich reporting patří k důležitým částem administrace systému, např. pro odhalení funkčních problémů, zpětné kontroly připojených uživatelů, sledování hackerských útoků z internetu, atp. (mimo jiné to také nařizují bezpečnostní politiky společnosti).

Konfigurace Syslog serveru:

- logy z VPN bran se budou ukládat do souborů po jednotlivých dnech

- běžící skripty zajistí každý den tyto 2 nejdůležitější funkce:
    1) na přelomu dne skript zanalyzuje denní log dle nastavených klíčových slov a vytvoří report všech nastavených událostí, ten se každý den pošle mailem administrátorům pro každodenní kontrolu.
    2) druhý skript každou minutu kontroluje denní log pro vybrané kritické události. Jestliže hledaná událost nastane, okamžitě se posílá report emailem a sms na vybrané administrátory.
- tímto postupem se budou vytvářet 4 denní reporty rozdělené dle příslušné národní VPN brány
- logy budou zůstávat na Syslog serveru uložené s historií 2 měsíce, poté se vypálí na DVD a ze serveru smažou

5.5. Konfigurace bran pro přístup a bezpečnostní politika

Tato kapitola stručně uvádí nejdůležitější nastavení VPN bran Cisco. Jednak technické nastavení brány pro přístup a jednak uživatelské nastavení VPN skupin. Uvedu také rozdělení uživatelů do skupin, zabezpečení bran a VPN tunelů a pravidla provozu. Konfigurace přístupových VPN bran Cisco z hlediska uživatelského nastavení VPN skupin doplňuje popsané procesy na externích systémech infrastruktury.

Rozdělení uživatelů do skupin/nastavené skupiny:

- na každé bráně v každé zemi budou nastaveny tyto skupiny, určené pouze Tesco uživatelům (plus stručně uvedený povolený přístup):
    1) **IT Admins**
        - skupina pro IT Administrátory (2nd level support)
        - povolený přístup do celé sítě CE přes všechny porty
    2) **IT Users**
        - skupina určená pro IT uživatele, IT support (1st level), a manažery s potřebou přístupu do celé sítě
        - přístup do celé sítě CE, avšak jen přes vyjmenované porty (běžné aplikační porty a vybrané porty pro IT správu)

3) **HO Users (Head Office)**
   - skupina pro běžné kancelářské uživatele a některé manažery
   - přístup jen do sítí datacenter (k aplikacím) a do EDC, pouze přes aplikační porty
4) **Servisní VPN tunely – Network Admin, FC Admin**
   - servisní VPN tunely pro administrátory systému
   - povolený přístup do celé sítě CE přes všechny porty
   - nastaveny jak se vzdáleným ověřením RADIUS tak s ověřením z lokální VPN databáze bran servisních uživatelů (pro případ výpadku RADIUS atp.)
5) **IT Dodavatelé**
   - na VPN bránách potřeba mnoha skupin dodavatelů se vzdáleným přístupem (cca 10 – 30 skupin v každé zemi, každá skupina průměrně 10 uživ.)
   - každý dodavatel dostane svůj vlastní VPN tunel navázaný na vlastní skupinu a uživatele v doméně
   - každý dodavatelský VPN tunel striktně povolen jen nejnutnější přístup pouze na potřebné a schválené aplikace / ip rozsahy a porty ve vnitřní síti

Technická konfigurace pro VPN skupiny:

- každá Client VPN skupina bude mít nastaveny tyto nejdůležitější části/parametry:
- VPN Object Group – nejvyšší jednotka pro samotný vzdálený přístup
- VPN Group Policy - objekt se sadou politik pro konkrétní skupinu
- VPN Access List - acccess listy sdružovány do skupin ip sítí a tcp-udp portů – Network Objects a Port Objects (vytvářejí se zvlášť, dají se použít ve více access listech), každá vpn skupina vlastní access list!
- případně Split-Tunnel Access List – pro tunelování VPN u klienta a umožnění přístupu do jeho lokální sítě
- VPN IP POOL – každá VPN skupina nastaven vlastní IP rozsah, ze kterého se klientům skupiny přidělují ip adresy –použito v Access Listech; každý IP Pool je částí adresace vnitřní sítě (příslušné zabezpečené VLAN)

- QoS politiky pro VPN skupiny – z QoS nástrojů použití omezení šířky pásma každého uživatelského tunelu z dané VPN skupiny (tzn. max. rychlost připojení uživatele) – každá VPN Group vlastní limit, limit se pak aplikuje zvlášť na každý vytvořený tunel (IT Admins – 500Kbps, IT Users 380Kbps, HO Users 300Kbps, dodavatelé většinou 300 – 400Kbps)
- případná požadovaná modifikace přístupových práv se provádí úpravou Access Listu VPN skupiny (změna pro všechny její členy)

Zabezpečení bran a pravidla provozu:

- na VPN branách mohou být vytvořeny striktně jen Client vpn tunely (LAN-to-LAN tunely zásadně jen přes produkční Firewally firmy), žádná jiná služba mezi LAN a Internetem nesmí být povolena (na to taktéž produkční Firewall)
- provozní zabezpečení vpn – client tunely jsou UDP VPN přes porty UDP 500, UDP 4500 a ESP; první fáze – IKE tunel – politika šifrování 3DES hash MD5; druhá fáze – IPSec tunel – politika šifrování AES 256bit hash SHA1; striktní Access Listy; povolený NAT-Traversal, povolené Perfect Forward Secrecy (nové klíče po timeoutu nejsou vytvářeny z těch původních), Diffie-Helmann skupina 2, bohužel jen zrychlený aggressive mode (absence certifikátů)
- zabezpečení celého systému proti průniku/neoprávněnému provozu mezi Internetem a LAN: na Outside i Inside interface zakázání veškerého provozu kromě legitimního VPN provozu na uvedených portech a z potřebných sítí, zakázání routování mezi interface, nastavení NAT ip adresace LAN na public IP Outside Interface; povolení administrace bran jen přes zabezpečené SSH a HTTPS a pouze z vybraných serverů v LAN (úplné zakázání z Internetu, částečné povolení z VPN tunelu skupiny IT Admins)
- procesní zabezpečení: vytvoření dokumentace, vytvoření politik a procedur s přesnými postupy administrace a přidělování vpn uživatelům a zvolení zodpovědných osob (viz. 5.6.); schvalovací proces; dokumentace přidělení uživateli; vytvoření závazných předpisů a politiky použití pro uživatele k podepsání a dodržování

5.6. Začlenění řešení do organizační struktury

V této kapitole stručně uvedu organizační začlenění systému do struktury společnosti vzhledem k formální a technické zodpovědnosti.

5.6.1. Organizační správa systému

Projekt celého systému organizačně spadá do organizačního celku CE IT. Jednotlivé prvky systému budou ve vlastnictví a pod správou regionálního CE IT, konkrétně CE IT Shared Services.

- technickou správu systému budou mít na starosti částečně týmy z jednotky Infrastructure & Operational a částečně dodavatel řešení (viz. další podkapitola)
- vytvoření technické dokumentace – VPN dodavatel
- procesní správa, procedury, politiky použití:
    - návrh a vypracování Network týmem (CE IT Shared Services - Infrastructure & Operational)
    - schválení, uvedení do procesu, kontrola dodržování - IT Security Manager (CE IT Shared Services - CE IT Support team – IT Services Team)
- komunikace na uživatele, doručení řešení uživatelům, dokumentace uživatelů – Country IT dané země (PC Support / Helpdesk)
- instalace VPN klientů, podpora uživatelů – Country IT dané země (PC Support / Helpdesk)
- proces přidělení VPN Tesco uživateli (zodpovědnost v řadě za sebou): Line Manager uživatele - Helpdesk – PC Support – Country IT Manager - Network Team (I&O) – Wintel team (I&O) – zpět na Country IT, pro proces přidělení využit stávající systém Service Desk
- proces přidělení VPN externímu dodavateli: schválení – vlastník kontraktu (příslušný Tesco manager), I&O Manager, Country IT Manager, technické doručení – Network team, Wintel team, VPN dodavatel

5.6.2. Technická správa systému

Technická správa prvků systému je čistě zodpovědnost vlastníků systému, tedy CE IT Shared Services. Správa je z menší části kryta vlastními zdroji (viz.dále), z větší části servisní smlouvou s VPN dodavatelem. Pouze technická správa instalací VPN klientů u uživatelů je zodpovědnost Country IT příslušné země.

- administrace klientů – Country IT – PC Support / Helpdesk
- administrace Cisco VPN bran – Network team, VPN dodavatel
- administrace Syslog – Network team, VPN dodavatel
- administrace RADIUS, Active Directory a jiných Windows prvků – Wintel team a jejich stávající dodavatel služeb

Kromě běžné administrace je třeba pravidelně vykonávat tyto činnosti na bránách Cisco (vše uvedené zodpovědnost Network team a VPN dodavatel):

- pravidlené zálohování konfigurace po každé změně v systému
- pravidelné kontroly nalezených bezpečnostních chyb a vydaných oprav firmware / nových firmware
- testování a nasazování oprav firmware / nových firmware

5.7. Plán implementace

Při zpracovávání projektu pro společnost Tesco jsem vytvořil podrobně rozepsaný plán implementace, včetně stanovení délky trvání jednotlivých úkolů a sdružených skupin úkolů, a také přiřazených zdrojů (tedy vlastníků dílčích úkolů). Plán implementace však nemá stanoven objem prací v jednotkách „ManDays“, jelikož dílčí objemy prací jednotlivých dní se vzájemně liší, a tedy je není možné souhrnně spočítat (nelze kalkulovat jednotně 1 den = 8 hodin, někdy jen 3hodiny).

Podrobný harmonogram úkolů s uvedenými detaily je **PŘÍLOHOU 3** této práce. Vložený harmonogram je tabulkou exportovanou ze zpracovaného souboru MS Project. Původní soubor MS Project – Ganttův diagram – je samostatnou **PŘÍLOHOU 4** této práce. Ganttův diagram dává náhled na přesnou časovou osu

prací včetně časového překrytí jednotlivých úkolů (časová náročnost fáze projektu není prostým součtem trvání jednotlivých úkolů – ty se často překrývají).

Zde uvedu pouze stručné informace k plánu implementace.

Potřebné zdroje k implementaci projektu:

- Network team, Network team leader, Wintel team, Net-Win Manager, I&O Manager, IT Security Manager, VPN dodavatel (Supplier)

Strukturu rozdělení prací (tzv. WBS) názorně zobrazuje obrázek č. 8 obsažený taktéž v Příloze 3.

Hlavní fáze implementace (milníky) vycházející z WBS a projektu implementace včetně časové náročnosti (podrobně rozepsáno v harmonogramu v Příloze 3 a 4):

1) Příprava návrhu systému a schválení – 80 dní (část z toho odpovídá zpracování bakalářské práce o objemu 59 dní)
2) Návrh projektu implementace a příprava zdrojů (28 dní)
3) Pilotní fáze projektu – implementace v ČR (75 dní) – končí přechodem do produkce
4) Rollout fáze – Implementace systému do PL (17 dní), Implementace do HU (16 dní), a Implementace do SK (14 dní)
5) Finální konfigurační úpravy (10 dní)
6) Technická revize – revize konfigurace, penetrační testy... (12 dní)
7) Procesní revize – kontrola dosažených cílů; vyhodnocení; revize procesů, politik a procedur; report managementu; revize dokumentace (10 dní)

Implementace projektu bude trvat celkem 262 dní. Nejdelší částí s největším počtem dílčích úkolů je pilotní fáze projektu – implementace systému do ČR, která bude trvat 75 dní. Velmi důležitými fázemi jsou technická a procesní revize projektu, kde bude hodnoceno dosažení cílů a kontrolována správnost technické a procesní realizace.

5.8. Ekonomické zhodnocení

Poslední kapitolou návrhu řešení je ekonomické zhodnocení navrženého projektu. Provedu jednak zhodnocení kvalitativní, kde se pokusím o identifikaci nejvýraznějších přínosů projektu, a jednak zhodnocení kvantitativní, kde porovnám náklady řešení s náklady zastaralého systému RAS, který bude novým projektem nahrazen.

5.8.1. Kvantitativní zhodnocení

Tato podkapitola zobrazuje peněžní vyjádření přínosů projektu. Doba jednotky produkčního cyklu systému ve společnosti je stanovena na 3 roky. Předpokládaný produkční cyklus VPN systému je stanoven na 2 jednotky cyklu, tedy 6 let. Cenové kalkulace jsou tedy vyjádřeny vzhledem k této době.

Pozn.1: všechny ceny uvedeny bez DPH

Pozn.2: předpoklad je, že cena provozních nákladů VPN se bude každý rok nepatrně snižovat. Důvodem je pravidelné klesání měsíčních nákladů na internetovou konektivitu (ročně o 5 – 10%). Tento pokles ale do kalkulace nezahrnuji.

VPN:

Celková pořizovací cena VPN systému:	795.280,-Kč
Roční provozní náklady VPN systému:	3.213.560,-Kč
Celkové náklady na období 6 let:	20.076.640,- Kč

RAS:

Roční náklady na správu:	1.800.000,- Kč
Roční náklady na tel. linky průměrně:	3.000.000,- Kč
Roční náklad celkem:	4.800.000,- Kč
Náklad na období 6 let:	28.800.000,- Kč

Rozdíl mezi RAS a VPN za 6 let:	**8.723.360,- Kč**

Ze zobrazených nákladů vychází, že VPN systém je výrazně levnější oproti RAS systému, rozdíl v nákladech za šestileté období je ***8.723.360,-Kč*** (což odpovídá zhruba nákladům na další 2,5 roku provozu VPN). Hlavní přínos nového systému však není jen ve snížení nákladů, ale především v dosažených kvalitativních přínosech.

Nyní porovnám oba systémy VPN a RAS a spočítám dobu návratnosti investice systému VPN oproti provozu systému RAS (tedy dobu, za jak dlouho se vrátí finanční prostředky vložené do investice):

Dobu návratnosti spočítám dle vzorce $t_n = I / \Delta Z$

kde t_n = doba návratnosti (roky)

I = investice (v Kč)

ΔZ = efekt (v Kč) – rozdíl nákladů na systémy

tedy

$t_n = 795.280 / (4.800.000 - 3.213.560)$

$t_n = 795.280 / 1.586.440$

t_n = 0,501 roku

Doba návratnosti investice VPN systému je proti provozu RAS systému **6 měsíců**.

5.8.2. Kvalitativní zhodnocení

Dobré kvalitativní zhodnocení a dosažení očekávaných přínosů projektu VPN je pro společnost Tesco důležitější, než samotná finanční úspora. Jak bylo určeno analýzou, systém RAS má díky zastaralosti technologie vzhledem k současným potřebám firmy mnoho závažných nedostatků a kritických bezpečnostních rizik Vzhledem k uvedeným nedostatkům a stanoveným požadavkům firmy byl kladen důraz na dosažení těchto významných přínosů, očekávání a subjektivních pocitů uživatele:

- větší mobilita uživatele vzhledem k místu připojení, komfortnější použití

- razantní zvýšení rychlosti připojení a možnost práce s pomalým i rychlým připojením k internetu (internet doma, hotel, mobil, atd.)
- zvýšení možností přístupu k interním zdrojům firmy a velká škálovatelnost nastavení přístupu
- razantní zvýšení bezpečnosti - jak na úrovni systému (konfigurační možnosti, začlenění do infrastruktury, atd.), tak na úrovni uživatele (pokročilé funkce ověřování, ověřování z více zdrojů, atd.)
- zvýšení komfortu administrace – znalost technologie, snadná a rychlá správa, výhody objektové konfigurace, automatizace
- vysoká dostupnost a redundance

- konkrétním cílem bylo dosáhnout snížení času potřebného na připojení uživatele a přístupu k interním aplikacím a IT systémům, a tedy snížení reakční doby řešení IT incidentu všemi úrovněmi IT supportu (od 1st level Helpdesk až po dodavatele). Snížení reakční doby a doby řešení incidentu znamená snížení rizika ohrožení obchodu výpadkem služby, což by přineslo pozitivní odezvu napříč společností.

Pokud bude při implementaci systému dodržena volba navržené technologie, systém bude postaven přesně dle navržené struktury, budou dorženy všechny navržené postupy, funkce, politiky, a především navržené ověřovací mechanizmy, tak budou naprosto splněna všechna uvedená očekávání.

6. ZÁVĚR

Projekt návrhu a implementace nového systému vzdáleného přístupu technologií VPN jsem minulý rok reálně zpracoval jako odpovědný zaměstnanec společnosti Tesco Stores ČR. Analýza současného stavu i požadavky společnosti přesně odpovídají skutečnosti a navržený systém byl implementován v nezměněné podobě do celého regionu Central Europe.

Samotná implementace s mým aktivním přispěním jakožto řešitele projektu, odborného IT Network specialisty, a posléze pozice IT Security manažera, proběhla dle stanoveného harmonogramu prací. Oproti plánovaným termínům byla prodloužena testovací fáze pilotní části projektu – provozu VPN v ČR. To mělo za následek časový posun rollout fáze – produkční implementaci do ostatních zemí. Implementace projektu byla dokončena na jaře roku 2008 instalací VPN v Maďarsku.

Důležitou skutečností byl požadavek firmy využít pouze existující systémy společnosti a v rámci projektu nenavrhovat nové. Jak jsem v řešení nastínil, jde především o funkci ověřování uživatele. Ověřování uživatele je realizováno méně bezpečnou variantou, kdy se používá dvoufázové autentizace preshared klíčem VPN profilu a doménovým účtem. Použití preshared klíče v důsledku znamená nechtěnou přenositelnost profilu a použití zrychleného aggresive autentizačního módu, díky němuž jde komunikace odposlouchat a preshared klíč cracknout v off-line módu. Toto riziko bylo částečně vyváženo použitím klíčů o minimální délce 30 znaků, kde je doba cracknutí na velmi výkoných clusterech cca půl roku.

Dle doporučení mého projektu byl po dokončení implementace realizován penetrační test celého systému – tedy test bezpečnosti systému proti neoprávněnému průniku. Penetrační test odhalil 2 slabiny – jednak zmíněné použití aggresive módu, a jednak potenciálně rizikové zapojení VPN bran paralelně s Firewally. Doporučení z testů bylo přepnout IKE autentizaci z aggressive na normal mode, a zapojit VPN brány za Firewall (ze směru z internetu do LAN).

Na základě výsledků penetračních testů byla přijata tato 2 opatření:

1) V horizontu 1 roku bude v rámci jiného projektu ve společnosti instalována Certifikační autorita. Byla schválena následná migrace VPN profilů uživatelů na varianty profilů, kde je kombinována Group autentizace preshared klíčem a zároveň certifikátem notebooku uživatele. To jednak odstraní použití nebezpečného aggressive módu ve prospěch normal módu IKE autentizace, a jednak zabrání možné přenositelnosti VPN profilu na jiné PC.

2) Taktéž v horizontu 1 roku je plánován projekt upgradu celého perimetru sítě Tesco v regionu CE. To znamená, že současná infrastruktura perimetru sítě bude rozšířena z jednoho clusteru 2 produkčních Firewallů (tedy mezi internetem a LAN stojí 1 vrstva Firewallu s několika DMZ) na infrastrukturu 2 clusterů (párů) Firewallů tak, že jeden cluster bude vnější pár Firewallů, a druhý cluster bude vnitřní pár Firewallů. Mezi nimi budou i 2 duplicitní DMZ – vnější DMZ a vnitřní DMZ. Toto je dnes vysoce bezpečný standard použitý zejména v bankovním sektoru. Po tomto rozšíření perimetru budou VPN brány zapojeny vždy mezi vnější a vnitřní Firewall, vrstva ochrany a inspekce komunikace se tedy zdvojnásobí.

7. SEZNAM POUŽITÉ LITERATURY

Monografie

[1] BARTH, Wolfgang. *Nagios - system and network monitoring.* NO STARCH PRESS, 2006. 464 p. ISBN 1-59327-070-4.

[2] DOSTÁLEK, Libor a kol. *Velký průvodce protokoly TCP/IP: Bezpečnost - druhé aktualizované vydání.* Computer Press, 2003. 592 s. ISBN 80-7226-849-X.

[3] DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* Computer Press, 2006. 536 s. ISBN 80-251-0828-7.

[4] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z, druhé aktualizované vydání.* Computer Press, 2006. 423 s. ISBN 80-251-1278-0.

[5] PUŽMANOVÁ, Rita. *TCP/IP v kostce.* KOPP, 2004. 607 s. ISBN 80-7232-236-2.

Normy a standardy

[6] British Standard BS 7799-2:2002. *Information Security Management System*

[7] BS ISO/IEC 17799:2000. *Information Security Management*

[8] Security Policy GT&A-07. *Network Security Policy.* Tesco Group, 2007. 45s.

[9] Security Policy GT&A-08. *Remote Access Security Policy.* Tesco Group, 2008. 39s.

[10] Security Policy GT&A-08. *Remote Access Usage Policy.* Tesco Group, 2008. 32s.

Internetové adresy

[11] Actinet. *Bezpečný vzdálený přístup* [online]. [cit. 2008-5-16]. Dostupný z www: <http://www.actinet.cz/bezpecnost_informacnich_technologii/l19/cl37/st2/j1/Bezpecny_vzdaleny_pristup.html>.

[12] Crypto-World. *Crypto news* [online]. [cit. 2008-5-8]. Dostupný z www: <http://crypto-world.info/news/index.php?sekce=c>.

[13] Crypto-World. *Security news* [online]. [cit. 2008-5-8]. Dostupný z www: <http://crypto-world.info/news/index.php?sekce=s>.

[14] HSC. *Network encryption: IPSec, SSL, SSH* [online]. [cit. 2008-5-2]. Dostupný z www: <http://www.hsc.fr/ressources/presentations/echanges3/index.html.en>.
[15] IPSec. *IPSec* [online]. [cit. 2008-4-28]. Dostupný z www: <http://www.cs.vsb.cz/grygarek/TPS-0304/projekty0304/ipsec/ipsec.html>.
[16] ISDN Server. *Průvodce nástrahami VPN* [online]. [cit. 2008-4-21]. Dostupný z www: <http://www.isdn.cz/prilohy/vpn/art.php?id=4>.
[17] Tesco. *Tesco potvrdilo svůj pokračující růst na trhu* [online]. [cit. 2008-4-3]. Dostupný z www: <http://www.itesco.cz/o_nas/tiskove_centrum/rok_2007_byl_ve_znameni_investic_do_snizovani_cen_a_vystavby_prodejen>.
[18] Tesco. *Tesco ve světě* [online]. [cit. 2008-4-3]. Dostupný z www: <http://www.itesco.cz/o_nas/o_spolecnosti/tesco_ve_svete__1>.
[19] Vše kolem VPN. *Vše co jste chtěli vědět o VPN* [online]. [cit. 2008-5-11]. Dostupný z www: <http://home.zcu.cz/~ondrous/index.php?menu=0>.
[20] Wikipedie. *IPSec* [online]. [cit. 2008-5-8]. Dostupný z www: <http://cs.wikipedia.org/wiki/IPsec>.
[21] Wikipedie. *Referenční model ISO/OSI* [online]. [cit. 2008-5-19]. Dostupný z www: <http://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI#S.C3.AD.C5.A5ov.C3.A1_vrstva>.
[22] Wikipedie. *Secure Socket Layer* [online]. [cit. 2008-5-10]. Dostupný z www: <http://cs.wikipedia.org/wiki/Secure_Sockets_Layer>.

8. SEZNAM ZKRATEK

AD	(Active Directory)	- Adresářová služba domény MS Windows
CDC	(Country Data Centres)	- Datová centra v hlavní pobočce země
CE	(Central Europe)	- Region střední Evropy
DMZ	(Demilitarized Zone)	- Demilitarizovaná zóna, perimetr sítě
EDC	(European Data Centre)	- Evropské datové centrum
HTTPS	(Hypertext Transfer Protocol over Secure Socket Layer)	- Zabezpečený protokol HTTP
IKE	(Internet key exchange)	- Protokol pro výměnu šifrovacích klíčů a navázání šifrované komunikace
IP	(Internet Protocol)	- Přenosový protokol síťové vrstvy
IPSec	(IP security)	- Skupina protokolů pro bezpečnou komunikaci
LAN	(Local Area Network)	- Lokální síť
LDAP	(Lightweight Directory Access Protocol)	- Protokol komunikace s adresářovou strukturou
NAT	(Network Address Translation)	- Překlad adres Firewallem z důvodu zabezpečení, většinou z privátní ip adresy na veřejnou ip
QoS	(Quality of Service)	- Mechanizmus zajištění dostupnosti služby prioritizací kanálů a omezením IP provozu
RAS	(Remote Access Server)	- Server vzdáleného přístupu
RDP	(Remote Desktop Protocol)	- Protokol vzdáleného přístupu
RSA	(Rivest, Shamir, Adleman)	- Algoritmus asymetrické kryptografie
SMTP	(Simple Mail Transfer Protocol)	- Prtokol elektronické pošty
SSH	(Sesure Shell)	- Protokol pro vzdálenou administraci
SSL	(Secure Sockets Layer)	- Zabezpečený protokol pro přenos dat
TCP	(Transmission Control Protocol)	- Stavový přenosový protokol transportní vrstvy
UDP	(User Datagram Protocol)	- Nestavový přenosový protokol transportní vrstvy
VPN	(Virtual Private Network)	- Virtuální síť (uzavřený tunel) veřejnou sítí mezi dvěma vnitřními sítěmi nebo klientem a sítí
WAN	(Wide Area Network)	- Rozsáhlá síť, v Tescu označena jako bezpečná síť poskytovatele spojující LAN poboček

9. SEZNAM PŘÍLOH

Příloha 1 – Podrobná specifikace technologie přístupových bran – Varianta Cisco

Příloha 2 – Podrobná specifikace technologie přístupových bran – Varianta Juniper

Příloha 3 – Harmonogram implementace projektu

Příloha 4 – Projekt implementace – samostatný soubor v MS Project
název souboru „Priloha4_Gantt_VPN_projekt.mpp“

PŘÍLOHY

Příloha 1

Podrobná specifikace technologie přístupových bran – Varianta Cisco

Varianta 1 – technologie CISCO:

Jako 1. variantu přístupových bran jsem se rozhodnul zvolit vhodně zaměřené bezpečnostní hardwarové appliance technologie Cisco, kombinující funkcionalitu Firewallu a VPN koncentrátoru, z nové produktové platformy ASA 55xx. Platforma ASA nabízí volbu mezi čtyřmi různě výkonnými řadami (5510, 5520, 5540, 5550) a čtyřmi edicemi (Firewall Edition, VPN Edition, Antivirus Edition a IPS Edition).

Zvolený konkrétní typ, který plně odpovídá všem stanoveným parametrům:
Cisco ASA 5520 Security plus license (jde o VPN Edition)

Klíčové vlastnosti technologie:

- appliance box do racku (1U)
- 5 ethernetových portů – 4x 1GB a 1x 100MB management
- 750 současných VPN IPSec spojení, 750 SSL Web VPN spojení
- nelicencované použití IPSec VPN, zdarma VPN Client software
- licencované použití SSL Web VPN, v ceně licence pro 2 uživatele
- propustnost 450 Mbps Firewall, 225 Mbps IPSec VPN
- šifrování DES/3DES/AES, hash SHA1/MD5
- aplikační inspekce trafficu, QoS, NAT, NAT-Traversal, 802.1Q
- VPN clustering a load-balancing, High availability (clustering active/passive i active/active)
- max.connections 280.000, 9.000 connections per second
- podpora externích zařízení: LDAP, RADIUS, RSA Secure ID, Certifikační autorita, Antivirus, podpora NAC systémů

Výhody:

- řada produktů přímo zaměřených pro VPN použití - větší než požadovaná kapacita IPSec VPN připojení
- nelicencované použití IPSec VPN, vlastní VPN klient zdarma
- relativně nízká cena samotných boxů, navíc Tesco má centrální kontrakt s Ciscem zajišťující 40% slevu
- redundantní funkce (backup) integrovaná přímo ve VPN klientovi, redundantní funkce i na úrovni systému
- dobrá podpora externích zařízení a systémů
- dobré reference a „price for future“ díky velkému rozšíření technologie
- velmi dobrá znalost technologie
- robustní a intuitivní ASDM webový management každého zařízení přes zabezpečené HTTPS kombinující funkce plné správy a komplexního monitoringu zařízení

Nevýhody:

- nemá centrální management, každý box či cluster má svůj
- horší podpora výrobce kvůli velkému rozšíření technologie (maintenance servis však dobrý)
- IKE autentizace umí pracovat v normal módu pouze s certifikáty, při použití vpn profilu pouze s preshared klíčem je možný jen aggressive mód (zrychlená autentizace) – to je jisté bezpečnostní riziko, autentizační komunikaci lze odposlouchat a šifru zlomit
- díky masovému rozšíření se poměrně často nalézají bezpečnostní chyby a často se vydávají nové firmware s opravou chyb – potřeba sledovat vývoj a často instalovat opravy pro zajištění potřebné úrovně zabezpečení

Cenová kalkulace celého řešení:

1) *Celková cena pořízení HW technologie:*

Po firemní slevě 40% je cena 1 boxu Cisco 3.580,-euro.

Náklady na VPN klient pro uživatele nejsou žádné.
Pořizovací cena celkem: 4 x 3.580,-eur = 14.320,-eur = **415.280,-Kč**

2) *Cena instalace technologie dodavatelem*

Smluvní cena za instalaci technologie a provedení stanovených konfiguračních zákroků a projektových prací dodavatelem: **380.000,- Kč**

3) *Roční náklady na provoz*

a) HW maintenance 24x7 4hours SLA:
   cena za 1 rok pro 1 zařízení: 910,-euro
   cena za 1 rok pro všechny zařízení: 4 x 910 = 3.640,-euro = **105.560,-Kč**

b) Smluvní cena podpory systému dodavatelem:
   měsíční cena podpory systému: 180.000,-Kč (45.000,-Kč na lokalitu)
   celková roční cena: 12 x 180.000 = **2.160.000,-Kč**

c) náklady na povýšení internetové konektivity
   Díky způsobu zapojení a použití klade tento systém zvýšené nároky na rychlost internetových přípojek v lokalitách zapojení. Uvedené ceny znamenají dodatečné náklady na internetové přípojky při požadovaném navýšení linek (navýšení o 10Mbps na lokalitu).
   CZ: +16.000,-kč/měs. = 192.000,-kč/rok
   PL: +20.000,-kč/měs. = 240.000,-kč/rok
   HU: +31.000,-kč/měs. = 372.000,-kč/rok
   SK: +12.000,-kč/měs. = 144.000,-kč/rok
   Celkové roční náklady na potřebné navýšení internetových linek činí **948.000,-Kč**

*Celkové roční náklady na provoz technologie systému činí **3.213.560,-Kč***
*Celková pořizovací a instalační cena technologie systému činí **795.280,-Kč.***

Příloha 2

Podrobná specifikace technologie přístupových bran – Varianta Juniper

Varianta 2 – technologie JUNIPER:

Jako 2. variantu přístupových bran jsem zvolil bezpečnostní hardwarové appliance technologie Juniper. Jde sice o zařízení cílené především jako Firewall, nicméně politika výrobce, přizpůsobená současným požadavkům trhu, je poskytnout spolu s firewallingem mnoho dalších funkcionalit (tzv. funkcionalita UTM). Jde především o funkce VPN, Antivirus a IPS/IDS.

Juniper nabízí dvě základní řady výrobků – nižší řada SSG a vyšší řada ISG. Stanoveným požadavkům odpovídají některé modely již v řadě SSG. Jako plně vyhovující model jsem zvolil **Juniper SSG 520M**.

Klíčové vlastnosti technologie:

- appliance box do racku (2U)
- 5 ethernetových portů – 4x 1GB a 1x 100MB management, rozšiřitelnost až na 36 portů, mnoho jiných servisních portů
- 500 současných VPN IPSec spojení, 500 SSL Web VPN spojení
- licencované! použití VPN - tedy VPN Client software, použití jak s IPSec VPN tak SSL VPN
- propustnost 650 Mbps Firewall, 300 Mbps VPN
- šifrování DES/3DES/AES, hash SHA1/MD5
- aplikační inspekce trafficu, QoS, NAT, NAT-Traversal, 802.1Q
- VPN clustering a load-balancing, High availability (clustering active/passive i active/active)
- max.connections 128.000, 10.000 connections per second
- virtualizace – virtuální zóny, virtuální routery...
- management pro centrální správu
- integrované funkce IPS a Antiviru, Antispamu a Web filtering (vše licencované)

- podpora externích zařízení: LDAP, RADIUS, RSA Secure ID, Certifikační autorita

Výhody:

- velmi dobrý Firewall s mnoha rozšířenými funkcemi (Antivirus, Antispam, IPS, Web filtering) a nativní podporou VPN s velmi dobrými parametry
- součástí řešení je NSM server pro centrální správu s mnoha přídavnými funkcemi – centrální web management, automatické zálohování konfigurace s historií, centrální monitoring a nástroj na upgrade firmware, a také úložiště logů (Syslog server s komplexním reportingem a analýzou - tj. systém by nebyl potřeba vázat na externí Syslog)
- dodavatel Tescu poskytne slevu na koupi hardwaru a licencí 30% (ceny uvedené níže jsou již ceny po slevě)
- redundantní funkce na úrovni systému clusteringem, také možnost konfigurace profilů klienta pro automatické přesměrování
- dobrá podpora externích zařízení a systémů, standardně to samé co Cisco
- dobré reference a „price for future“ díky velkému rozšíření technologie především v USA, nyní i velký boom v Evropě díky dravé politice výrobce
- velmi robustní a kompaktní systém s více přídavnými funkcemi než Cisco
- perfektní podpora výrobce a přímá komunikace
- IKE autentizace při použití preshared keys umí pracovat v aggressive i normal módu
- technologie má redundantní zdroje a vzdálený management napájení

Nevýhody:

- licencované použití VPN klientů = velký nárůst pořizovací ceny
- cena samotných boxů je sice trochu nižší než Cisco, ale potřebujeme ještě management serveru a management napájení
- provoz a podpora také dražší než u Cisca

- stručné zhodnocení je, že tato technologie je velmi vhodná jako produkční firemní Firewall, ale jen na VPN použití je zbytečně drahý a naddimenzovaný
- trochu horší znalost technologie oproti Ciscu

Cenová kalkulace celého řešení:

1) *Celková cena pořízení HW technologie:*

Po slevě 30% poskytnuté dodavatelem je ceny pořízení tyto:

- 1 box Juniper SSG 520M - 3.850,-USD
- 1 NSM management server – 7.000,-USD
- Juniper VPN remote security client - 100 users – 2.009,-USD
- 1 management napájení – 573,-Euro

Výpočet pořizovací ceny:

Boxy - 4 x 3.850,-USD = 15.400,-USD = 338.800,-Kč

Management – 1 x 7.000,-USD = 154.000,-Kč

Napájení – 4 x 573,-Euro = 2.292,-Euro = 66.468,-Kč

Licence VPN klinet – potřeba 4.000 licencí, tedy

40 x 2.009,-USD = 80.360,-USD = 1.767.920,-Kč

Celková pořizovací cena HW a licencí klientů je **2.327.188,-Kč**
Z toho cena jen za HW je 559.268,-Kč

2) *Cena instalace technologie dodavatelem*

Smluvní cena za instalaci technologie a provedení stanovených konfiguračních zákroků a projektových prací dodavatelem: **0,- Kč**
(platí při uzavření smlouvy o podpoře systému s dodavatelem na 3 roky)

3) *Roční náklady na provoz*

a) HW a SW maintenance výrobce:

1 x 1rok SSG 520M HW maintenance 24x7 4hours SLA: 1.110,-USD
1 x 1rok HW maintenance pro NSM management server: 1.920,-USD
1x 1rok Core support pro VPN Client SW (100users): 39,60USD
Výpočet:
4 x 1.110,-USD = 4.440,-USD = 97.680,-Kč
1 x 1.920,-USD = 42.240,-Kč
40 x 39,60USD = 1.584,-USD = 34.848,-Kč
Cena za 1 rok supportu pro všechny zařízení je **174.768,-Kč**

b) Smluvní cena podpory systému dodavatelem:
měsíční cena podpory systému: 225.000,-Kč
celková roční cena: 12 x 225.000 = **2.700.000,-Kč**

c) náklady na povýšení internetové konektivity
Jak bylo uvedeno ve variantě 1, systém díky způsobu zapojení a použití klade zvýšené nároky na kapacitu internetových přípojek v lokalitách zapojení. Plánované navýšení linek o 10Mbps je stejné jak pro variantu 1, tak pro variantu 2. Nebudu zde již tedy znovu rozepisovat dílčí ceny, a uvedu jen celkový roční náklad na všechny 4 přípojky:
Celkové roční náklady na potřebné navýšení internetových linek činí **948.000,-Kč**

*Celkové roční náklady na provoz technologie systému činí **3.822.768,-Kč***
*Celková pořizovací a instalační cena technologie systému činí **2.327.188,-Kč** (z toho za instalaci 0,-Kč, pouze cena HW 559.268,-Kč).*

Poznámky k cenovým kalkulacím obou variant:

Jak bylo uvedeno, tento projekt je řešen z části interními zdroji, a z části externě dodavatelem, a to především implementace systému. Následná správa

systému je zhruba z 80% kryta dodavatelem. V kalkulaci byly vyčísleny pouze externí náklady, jelikož k vyčíslení interních nemám dostatek podkladů.

Je třeba vzít v úvahu také to, že uvedené náklady jsou vyčísleny pouze k samotné technologii vzdáleného přístupu, do kalkulací již nejsou zahrnuty náklady na existující interní systémy, na které bude technologie navázána, a náklady na podporu uživatelů.

Poznámka – náklady jsou vyčísleny v Kč bez DPH. Pro převod z USD a Eura byl použit kurz, který byl relevantní v době návrhu a pořízení – 1Euro = 29,00Kč; 1USD = 22,00Kč.

Příloha 3

Harmonogram implementace projektu

Tato příloha zobrazuje přesný harmonogram implementace projektu. Plán je rozdělen až na jednotlivé úkoly, ty jsou sdruženy do skupin. Každý úkol a následně skupina úkolů má uvedenu délku jeho trvání. Díky rozpisu můžu spočítat celkové časové nároky na projekt, které jsou 262 dní.

Každý úkol má také přiřazeny vlastníky, kteří úkol v rámci projektu řeší. Zdroje odpovídají organizačnímu začlenění kapitoly 5.6.

Poznámka: tabulka je exportem zpracovaného projektu v MS Project. Některé časové periody se spolu časově překrývají, to znamená že délka trvání jedné fáze není prostým součtem všech činností dané fáze.

Přesná časová osa prací včetně překrytí (Ganttův diagram) je vyobrazena Přílohou 4 této práce – samostatným souborem MS Project.

Práce			*Trvání*	*Zdroj*
Projekt návrhu a implementace VPN systému			**262 days**	
1.	**Příprava návrhu systému a schválení**		**80 days**	
	1.1	Výběr modelu a technologie	22 days	Network
	1.2	Cenová kalkulace a srovnání se současnými systémy	22 days	Network
	1.3	Sběr dat, vytvoření interního Request for proposal = zpracování bakalářské práce (1.1 – 1.3)	37 days	Network
	1.4	Justification process, schválení projektu a rozpočtu	21 days	Net-Win Manager, IT Security manager
2.	**Příprava zdrojů a návrh projektu implementace**		**28 days**	
	2.1	Objednání HW Cisco ASA 4kusy	3 days	Network
	2.2	Objednání prací u VPN dodavatele	3 days	Network Team Leader
	2.3	Vytvoření návrhu projektu implementace	23 days	Network
	2.4	Schválení návrhu projektu implementace	5 days	Net-Win Manager, IT Security manager

	2.5	Alokace zdrojů, ověření termínů	5 days	Network Team Leader
	2.6	Dodávka HW vybavení	5 days	Supplier
3.	**Pilotní fáze projektu - implementace CZ VPN**		**75 days**	
	3.1	**Konfigurace CZ Cisco ASA**	**31 days**	Network
	3.1.1	Konfigurace základních firewall funkcí a zapojení	15 days	Network
	3.1.2	Konfigurace první testovací VPN skupiny - local	5 days	Network
	3.1.3	Dokončení kompletní pilotní VPN konfigurace	11 days	Network
	3.2	**Konfigurace ostatního HW**	**30 days**	
	3.2.1	Instalace a konfigurace syslog serveru	30 days	Supplier;Network
	3.2.2	Instalace a konfigurace RADIUS serverů	20 days	Wintel
	3.2.3	Konfigurace Windows domény - vytvoření VPN skupin, nastavení user vlastností	10 days	Wintel
	3.2.4	Konfigurace skriptů v doméně pro automatickou aktualizaci VPN profilů	10 days	Wintel
	3.2.5	Testovací provoz v rámci projektového týmu	13 days	Network
	3.2.6	Tvorba a schválení VPN Usage and Security policies	13 days	Network
	3.2.7	Tvorba technické dokumentace systému	35 days	Network
	3.3	**Pilotní provoz CZ prostředí**	**31 days**	
	3.3.1	Přidělení VPN uživatelům dle všech skupin	4 days	Network
	3.3.2	Pilotní plný provoz, feedback from users	27 days	
	3.3.3	Zpracování zpětné vazby uživatelů, odhalení chyb, zpracování požadavků na změny	10 days	Network
	3.3.4	Uživatelé vyplní Feedback Form dokumenty	5 days	
	3.3.5	Nachystání změn konfigurace na základě feedbacku z testovacího provozu	5 days	Network
	3.3.6	Implementace finálních změn v konfiguraci vzniklých analýzou zpětné vazby	8 days	Network
	3.3.7	Vytvoření a schválení procedury pro přidělování VPN a postupů řešení	20 days	Network Team Leader;Network

	3.4	**Ukončení pilotní fáze, kompletace všech vytvořených dokumentů a konfigurací, kolektizace pro implementaci do ostatních zemí!**	**1 day**	
	3.5	**Přechod CZ VPN systému do PRODUKCE!!**	**1 day**	
4.	**Implementace systému do PL**		**17 days**	
	4.1	Konfigurace a implementace PL VPN boxu	9 days	Supplier
	4.2	Instalace a konfigurace Syslog serveru	6 days	Supplier
	4.3	Instalace a konfigurace RADIUS serverů	6 days	Wintel
	4.4	Konfigurace Windows PL domain prostředí	6 days	Wintel
	4.5	Zkrácená testovací fáze PL	6 days	Network
	4.6	Přechod PL VPN systému do PRODUKCE!!	1 day	
5.	**Implementace systému do HU**		**16 days**	
	5.1	Konfigurace a implementace HU VPN boxu	9 days	Supplier
	5.2	Instalace a konfigurace Syslog serveru	6 days	Supplier
	5.3	Instalace a konfigurace RADIUS serverů	6 days	Wintel
	5.4	Konfigurace Windows HU domain prostředí	6 days	Wintel
	5.5	Zkrácená testovací fáze HU	6 days	Network
	5.6	Přechod HU VPN systému do PRODUKCE!!	1 day	
6.	**Implementace systému do SK**		**14 days**	
	6.1	Konfigurace a implementace SK VPN boxu	9 days	Supplier
	6.2	Instalace a konfigurace Syslog serveru	6 days	Supplier
	6.3	Instalace a konfigurace RADIUS serverů	6 days	Wintel
	6.4	Konfigurace Windows SK domain prostředí	6 days	Wintel
	6.5	Zkrácená testovací fáze SK	4 days	Network
	6.6	Přechod SK VPN systému do PRODUKCE!!	1 day?	
7.	**Finální konfigurační úpravy**		**10 days**	
	7.1	Revize všech konfigurací po přechodu do produkce	10 days	Network;Network Team Leader;Supplier
	7.2	Dokonfigurace backup prostředí pro redundanci, zalohované přihlášení, update profilů	10 days	Network
	7.3	Finální testy	10 days	Network;Supplier
8.	**Technická revize - zpětná analýza a kompletní revize konfigurace, penetrační testy**		**12 days**	**Network;Supplier, IT Security manager**
9.	**Procesní revize - konečná revize procesů, politik a procedur, použití, logů a reportů, kontrola dosažených cílů a celkové vyhodnocení, oficiální ukončení projektu a finální report managementu**		**10 days**	**Network;Network Team Leader;Net-Win Manager, IT Security manager**

Nákres struktury rozdělení prací WBS projektu implementace VPN systému následuje na další straně.

Struktura rozdělení prací WBS