VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

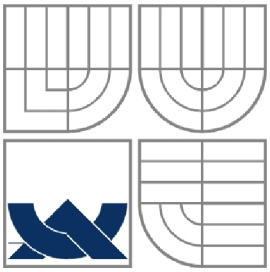
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

WEBOVÝ PORTÁL PRO GENEROVÁNÍ ZPRÁV O SÍŤOVÉM PROVOZU

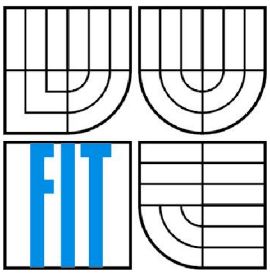
BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE Ondřej Klement
AUTHOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

WEBOVÝ PORTÁL PRO GENEROVÁNÍ ZPRÁV O SÍŤOVÉM PROVOZU

WEB PORTAL FOR NETWORK TRAFFIC REPORTING

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — Ondřej Klement
AUTHOR

VEDOUCÍ PRÁCE — Ing. Jiří Tobola
SUPERVISOR

BRNO 2007

Zadání bakalářské práce/6835/2007/xkleme02

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav počítačových systémů Akademický rok 2007/2008

Zadání bakalářské práce

Řešitel: **Klement Ondřej**
Obor: Informační technologie
Téma: **Webový portál pro generovaní zpráv o síťovém provozu**
Kategorie: Web

Pokyny:

1. Seznamte se s technologiemi pro tvorbu webových informačních systémů (HTML, CSS, PHP, Javascript, MySQL apod.).
2. Stručně se seznamte s technologií NetFlow pro monitorování sítí.
3. Proveďte analýzu požadavků pro systém umožňující tvorbu reportů, grafů a tabulek na základě NetFlow dat. Systém musí poskytovat podporu široké škály statistik (top uživatelé, nejnavštěvovanější servery, doby činnosti na síti, souhrnné statistiky sítě atp.).
4. Vytvořte detailní návrh tohoto systému a vhodně jej modelujte.
5. Navržený systém realizujte a otestujte, funkčnost systému demonstrujte na vhodně zvoleném vzorku dat.
6. Zhodnoťte dosažené výsledky a diskutujte možnosti dalšího rozšíření systému.

Literatura:

- Dle pokynů vedoucího.

Při obhajobě semestrální části projektu je požadováno:

- Splnění prvních tří bodů zadání.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Tobola Jiří, Ing.**, UPSY FIT VUT
Datum zadání: 1. listopadu 2007
Datum odevzdání: 23. ledna 2008

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav počítačových systémů a sítí
612 66 Brno, Božetěchova 2

L.S.

Kotásek

doc. Ing. Zdeněk Kotásek, CSc.
vedoucí ústavu

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami

1. **Pan**

Jméno a příjmení: **Ondřej Klement**
Id studenta: 84314
Bytem: Padělíky 480/42, 642 00 Brno
Narozen: 28. 05. 1985, Brno
(dále jen "autor")

a

2. **Vysoké učení technické v Brně**

Fakulta informačních technologií
se sídlem Božetěchova 2/1, 612 66 Brno, IČO 00216305
jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....
(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
bakalářská práce

Název VŠKP: Webový portál pro generovaní zpráv o síťovém provozu
Vedoucí/školitel VŠKP: Tobola Jiří, Ing.
Ústav: Ústav počítačových systémů
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:
tištěné formě počet exemplářů: 1
elektronické formě počet exemplářů: 2 (1 ve skladu dokumentů, 1 na CD)

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 pořizování 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

Náplní této bakalářské práce je návrh, analýza a implementace webového portálu pro generování zpráv o síťovém provozu. Dále se tato práce zabývá analýzou možností vytváření grafů, tabulek a statistik z dat, získaných prostřednictvím technologie NetFlow. Právě technologie NetFlow je klíčovým prvkem a celá tato práce je na ní postavena. Cílem této práce je možnost snadného, přehledného a jednoduchého monitorování síťového provozu a následné analýzy získaných dat v podobě vygenerovaných souhrnných zpráv. Pro implementaci byly zvoleny jazyky PHP a HTML. Zprávy o síťovém provozu budou generovány v dnes velmi oblíbeném formátu PDF.

Klíčová slova

Webový portál, zprávy o síťovém provozu, síťový provoz, síť, report, NetFlow, NfDump, PHP, HTML, CSS, XML, JavaScript, PDF.

Abstract

The main subject of this bachelor thesis is an proposal, analysis and implementation of the web portal for network traffic reporting. This work also deals with analysis of creating graphs, tables and statistics from data gained by NetFlow technology. The NetFlow technology itself is the key element in this thesis and this work is based on it. The main goal of this thesis is to make a simple tool for monitoring and analyzing the network traffic by generating complex reports. For the implementation itself, PHP and HTML have been chosen. Reports will be generated as well-know PDF documents.

Keywords

Web portal, network traffic reports, network traffic, network, report, NetFlow, NfDump, PHP, HTML, CSS, XML, JavaScript, PDF.

Citace

Klement Ondřej: Webový portál pro generování zpráv o síťovém provozu. Brno, 2008, bakalářská práce, FIT VUT v Brně.

Webový portál pro generování zpráv o síťovém provozu

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Jiřího Toboly. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Ondřej Klement
23.1.2008

Poděkování

Velmi rád bych na tomto místě poděkoval Ing. Jiřímu Tobolovi za poskytnutou pomoc a konzultace při tvorbě této práce.

Obsah

1 Úvod

Dnešní doba je velmi ovlivněna rychlým nástupem a velkým rozšířením přístupu k internetu, jak ve firmách, tak i v malých domácnostech. S tímto rozšířením plynou mnohé výhody, ale také mnohá úskalí. Jedním z nich může být například zneužití přístupu k internetu k jiným činnostem, než které jsou vaší pracovní náplní, šíření nelegálních dat a souborů a také různá nebezpečí, převážně v podobě počítačových virů. Mezi možné řešení tohoto problému mohou patřit různé blokace, omezení přístupu nebo například sledování činnosti uživatelů. Nutností je neustálé sledování aktuálních trendů a zlepšování kvality poskytovaných služeb, stejně tak zvýšení jejich efektivnosti a jejich celková optimalizace. Pro tyto, ale i mnohé další činnosti, spojené se správou sítě, je nutná důkladná analýza síťového provozu. K efektivní analýze je zapotřebí dostatek podkladů a statistik. Právě tvorbou statistik a generováním zpráv o síťovém provozu se zabývá tato práce. Další možné využití, spolu s detailními popisy jednotlivých stádií vývoje této práce, nastíníme v následujících kapitolách.

Vše potřebné o specifikaci zadání a požadavků, následné analýze a možné podobě výsledného systému, se dozvíte ve druhé kapitole. V třetí kapitole se seznámíme s technologií NetFlow, na které je celá tato práce postavena a s nástroji pro práci s touto technologií. Následující kapitola se zabývá návrhem možného řešení a vytvořením modelu navrženého systému. Obsahuje také diagram případů užití.

Pátá kapitola je věnována samotné implementaci systému, jsou zde uvedeny všechny použité technologie a knihovny. Můžete se zde dočíst o rozdílech mezi uživatelským a administrátorským rozhraním. Dále tato kapitola obsahuje letmý popis jednotlivých skriptů a vzor jednoho z XML konfiguračních souborů. Je zde i stručně nastíněno ovládání aplikace. Šestá kapitola obsahuje poznatky z testování systému, naleznete zde i požadavky pro běh systému a popis instalace na server.

Sedmá a předposlední kapitola této zprávy se zabývá možnostmi budoucího rozšíření systému. Závěrečná kapitola shrnuje celou tuto práci, obsahuje také návrhy na možné vylepšení a rozšíření systému.

2 Specifikace a analýza požadavků

Prvním krokem při tvorbě jakékoliv práce a projektu je důkladná specifikace požadavků se zadavatelem projektu. Následuje analýza těchto požadavků a nastínění možného řešení. V této části vývoje nového programu je nutné, aby došlo k pochopení zadavatelových požadavků, k vysvětlení případných nedostatků a dále i případně vyžádat další nezbytné informace od zadavatele.

2.1 Specifikace požadavků

Úkolem této práce je vytvoření webové aplikace, která by uživateli, zejména správci sítě, poskytla nástroj pro sledování síťového provozu, dále vytváření a sledování různých síťových statistik a také usnadnění případné archivace jednotlivých zpráv.

Jak již bylo řečeno, aplikace bude webového charakteru v jazyce HTML nebo XHTML. Pro implementaci by měl být použit skriptovací jazyk PHP. Při implementaci vzhledu budou použity kaskádové styly CSS. V případě potřeby může být použit například i javascript.

Hlavní komunikační částí by mělo být webové uživatelské rozhraní. Jako každé správně řešené uživatelské rozhraní by mělo být jednoduché na pochopení, přehledné a lehce ovladatelné, tedy User-friendly. Rozhraní by mělo být optimalizováno pro rozlišení 1024x786 a větší, tedy pro 19‘‘ monitory a větší, což je v dnešní době již poměrně standardní vybavení. Díky tomu bude využita větší pracovní plocha a bude zvýšena přehlednost celého rozhraní. Portál by měl být psán v anglickém jazyce, popřípadě ve více jazycích.

Tato práce je přímo založena na technologii NetFlow a pro svou činnost využívá nástroje NfDump. Aplikace bude přes příkazovou řádku komunikovat s nástrojem NfDump a následně bude zpracovávat jeho výstup. Pro testovací účely budou nutná NetFlow záznamy.

Výsledkem bude generování dokumentu ve formátu PDF, který bude obsahovat přehlednou tabulku a graf. Graf by měl být moderní, proto by se mělo jednat o tzv. ‚koláčový‘ graf. Reporty ve formě e-mailu, s přiloženým PDF dokumentem, budou odesílány na e-mailové adresy uživatelů tak často, jak si uživatel nastaví.

Dále by měl portál rozlišovat dva typy uživatelů, tedy administrátora a obyčejného uživatele. Pouze administrátor může vytvářet uživatelské účty a umožňovat tak dalším uživatelům přístup k portálu. Dále pouze administrátor bude mít přístup k datům všech uživatelů na síti. Ostatní uživatelé budou moci vidět pouze statistiky filtrované na rozsah IP adres, které vlastní a které jim při registraci a vytvoření účtu administrátor přidělí.

2.2 Analýza požadavků

Po specifikaci požadavků by měla přijít jejich důkladná analýza a návrh možného řešení. Implementace aplikace, jako webový portál, je výhodná hned z několika hledisek. Bude dostupná téměř odkudkoliv, jediným omezením je připojení k internetu, které je v dnešní době již velice rozšířené a počet přípojek stále stoupá. Jediné, co je ze strany klienta zapotřebí, je internetový prohlížeč. Není tedy nutné instalovat další software, navíc internetových prohlížečů existuje celá řada a jsou poskytovány jako freeware. Aplikace se tedy stane platformě nezávislou. Stejně tak na straně serveru nebude mít tato aplikace mnoho požadavků. Další výhodou je možnost aktualizace aplikace a implementace různých rozšíření, aniž by bylo nutné klientovi cokoliv posílat či předávat. Klient ani nemusí nic přeinstalovat a měnit. Všechny aktualizace a změny v aplikaci probíhají přímo na serveru.

Objem dat, který je zapotřebí uchovávat, není příliš veliký, proto bylo rozhodnuto, že aplikace nebude používat databázový server, ale pouze konfigurační soubor ve formátu XML. Aplikace tedy bude fungovat i na serveru, kde není nainstalovaný databázový server.

Portál musí obsahovat možnost výběru z několika statistik, které budou zobrazovány v přehledné formě tak, aby se v nich uživatel mohl lehce orientovat. Výsledný report by měl být ve formátu, který je rozšířený, známý a k jeho otevření a čtení není zapotřebí dokoupení dalšího software na straně klienta. Proto byl zvolen velmi oblíbený formát PDF, který je navíc i platformě nezávislý.

2.2.1 Uživatelské rozhraní

Uživatelská část je hlavním prostředkem pro komunikaci mezi uživatelem a samotnou aplikací. Jak již bylo řečeno, musí být přehledné a dobře ovladatelné. Požadavkem bylo vytvořit rozhraní pro obyčejné uživatele a pro administrátora. Lišit by se navzájem měly hlavně rozdílnými možnostmi a právy. Uživatel samozřejmě bude disponovat menšími možnostmi než administrátor.

Uživatel musí mít možnost ukládat nastavení posílání reportů. Při uložení bude zadávat jakou statistiku chce poslat a jak často se má posílat. Bude si moc vybrat mezi různými typy statistik. Uživatel bude moci jednotlivé nastavení přehledně spravovat. Všechna nastavení bude možno vypsat, nějakým přehledným způsobem, nejlépe v tabulce. Uživatel si bude moci nechat zobrazit aktuální statistiku podle výběru. Pokud bude chtít, nechá si ze zvolené statistiky vygenerovat report ve formátu PDF a bude si moci tento report i nechat poslat na e-mail.

2.2.2 Administrátorské rozhraní

Jak již bylo v předchozí kapitole řečeno, administrátorská část se od uživatelské liší převážně možnostmi a funkcemi. Požadavky na design a vzhled jsou stejné jako u uživatelského rozhraní. Není nutné mít dvě vzhledově a stylově různá prostředí, důležité je, aby se lišila funkčně.

Stejně jako obyčejný uživatel si administrátor bude moci ukládat, měnit a mazat svoje nastavení posílaných reportů. Dále mu bude umožněno zobrazení statistik přímo na webu. Oproti obyčejnému uživateli, ale bude administrátor vidět data všech uživatelů, tedy statistiky nebudou filtrovány na určitý rozsah IP adres.

2.2.2.1 Správa uživatelů

Hlavním rozdílem bude možnost správy uživatelů. Administrátor tedy bude moci vytvářet nové uživatelské účty. Při vytvoření nového účtu přidělí uživateli přihlašovací jméno, heslo a rozsah IP adres, kterými daný uživatel disponuje.

2.2.3 Automatické odesílání

Mimo samotné uživatelské rozhraní musí tato aplikace zajistit automatické generování reportů a jejich následné odeslání na e-mailové adresy. Jak často a jaké statistiky se budou odesílat, si nastaví jednotliví uživatelé přímo v uživatelském rozhraní aplikace. Tento skript tedy musí pracovat nezávisle na portálu samotném.

2.2.4 Bezpečnost

Jak již bylo řečeno v úvodu, s rozvojem internetu přibývá i mnoho úskalí s tímto spojených. Proto se, především v posledních letech, klade veliký důraz na bezpečnost webových aplikací a uživatelských dat. Riziko útoku či zneužití dat sice není u této aplikace tak vysoké, jelikož jejím primárním využitím je vnitřní síť, přesto je nutné alespoň s dobrým zabezpečením počítat. Aplikace by měla být chráněna heslem a jeho posílání šifrováno. Pokud možno měl by být přístup k aplikaci přes zabezpečený protokol https.

2.2.5 Reporty

Portál by měl uživateli nabídnout různé typy statistik a stejně tak různé formy zobrazení. Uživatel si bude moci statistiky prohlédnout ve formě grafu, tabulky nebo ve formě přehledného dokumentu typu PDF. Zobrazení bude probíhat buď přímo na webu, nebo budou reporty odeslány na e-mailovou adresu uživatele. Odeslání bude moci být okamžité, popřípadě naplánované jako událost.

2.2.5.1 Souhrnné reporty

Kromě jednotlivých statistik by měl portál poskytovat i možnost posílání tzv. souhrnných statistik z delšího časového úseku. Cílem těchto statistik je poskytnout uživateli možnost komplexního souhrnu dění na síti, během určitého časového úseku. Uživatel bude mít možnost, vybrat si z několika přednastavených statistik tak, aby souhrnný report co nejvíce vyhovoval jeho požadavkům.

2.2.5.2 Typy statistik

Jak již bylo řečeno, portál by měl uživateli nabídnout různé typy statistik, především s ohledem na možnosti a znalosti uživatele, ale také s ohledem na využití jednotlivých statistik. Portál bude obsahovat jednak statistiky přednastavené, ale i volitelné. Přednastavené statistiky jsou určeny hlavně běžným uživatelům. Jedná se o nejpodstatnější možné statistiky, které by každý uživatel mohl potřebovat. Pro uživatele, kteří chtějí víc, nebo potřebnou statistku nenachází mezi přednastavenými, jsou tu volitelné statistiky. Použitím této možnosti si uživatel bude moci vytvořit jakoukoliv statistiku si přeje.

2.2.6 Možnost nasazení

Klasickým případem využití portálu může být objekt, kde je k síti/internetu připojeno několik firem. Existuje zde správce sítě, který má na starost správu celé sítě. Tento správce sítě je v našem případě i administrátor našeho portálu. Právě on má tedy plnou kontrolu nad chodem portálu a rozhoduje o přístupu firem, respektive uživatelů, na portál. Pro jednotlivé firmy vytváří uživatelské účty a přiděluje jim odpovídající rozsah IP adres. Díky tomuto portálu pak může být práce správce jednodušší. Z reportů správce sítě může sledovat a analyzovat síťový provoz, nejenom celé sítě, ale i jednotlivých uživatelů. Na základě reportů může detekovat možné útoky na síť či potencionálně zavirované počítače. Dále díky těmto reportům bude moci zefektivnit činnost sítě a zlepšit poskytované služby, případně tyto služby přizpůsobit potřebám jednotlivých firem. Na druhé straně pověřený pracovník firmy bude mít možnost kontrolovat činnost jednotlivých zaměstnanců či kvalitu poskytovaných síťových služeb.

3 Technologie NetFlow

Technologie NetFlow by se dala definovat jako proces měření síťových toků. Síťový tok je definovaný, jako posloupnost paketů, majících společnou vlastnost a procházejících sledovaným bodem za určitý čas. Základním prvkem této technologie je NetFlow síťový protokol pro přenos záznamů o síťových tocích. Tento protokol byl vyvinut společností CISCO a je přizpůsoben, aby běžel na zařízeních, kde je povolen CISCO IOS. IOS (Internetwork Operating System) je operační systém, který se používá na většině CISCO směrovačích (router) a přepínačích (switch).

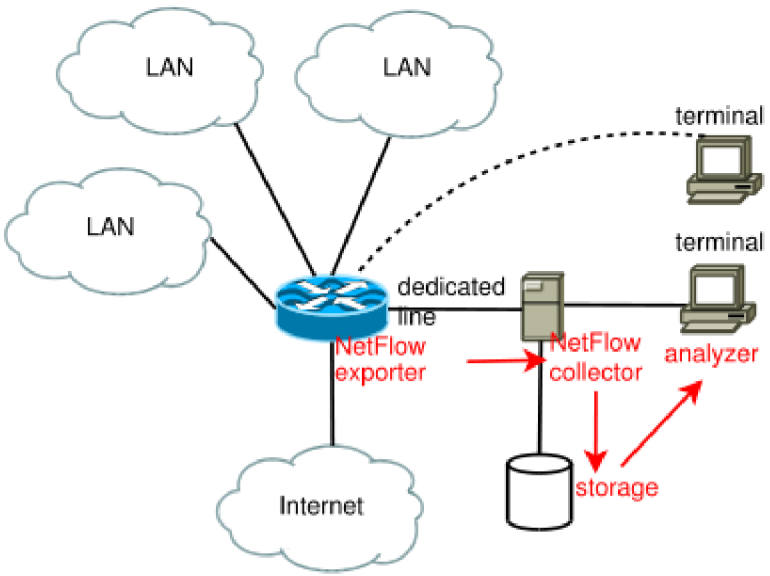
Pokud je na zařízení NetFlow povolen, pak zařízení generuje NetFlow záznamy. Tyto záznamy jsou exportovány jako UDP (User Datagram Protocol) nebo SCTP (Stream Control Transmission Protocol) pakety. NetFlow záznamy jsou následně shromažďovány a ukládány pomocí NetFlow kolektoru.

3.1 Jak funguje NetFlow

Jak již bylo řečeno, NetFlow je protokol pro přenos záznamů o síťových tocích a také pro měření síťových toků. Fungování tohoto protokolu lze dobře popsat na *obrázku 1.1,* kde můžete vidět schéma technologie NetFlow. Síť obsahuje prvek *NetFlow exporter* a *NetFlow collector*.

NetFlow exporter přijímá pakety a exportuje z nich záznamy o síťovém provozu, konkrétně při zahájení komunikace na síti, začne sbírat data o této komunikaci a skončí až při ukončení této komunikace. Konec komunikace může být po vypršení časového intervalu, ukončení TCP spojení nebo při hrozbě přetečení čítačů.

Tyto záznamy jsou odesílány do *NetFlow collector*, který je ukládá. Kolektor přijme paket a extrahuje z něj záznam. Záznamy mohou být ukládány například na server, na pevný disk nebo do databáze. *Analyzer* na tomto obrázku znázorňuje terminál (počítač), ze kterého je možno se záznamy pracovat. Na tomto terminálu může také docházet k zobrazování dat, tvorbě statistik a analýze těchto statistik.



Obr. 1.1.: Schéma NetFlow

3.2 NetFlow záznamy

NetFlow síťové toky dat jsou definovány jako pětice: zdrojová IP adresa, cílová IP adresa, zdrojový port, cílový port a IP protokol. NetFlow záznamy obsahují mnoho užitečných informací o daném toku dat. Existuje několik verzí záznamů. Nejpoužívanější je v5. Nejnovější pak v9.

Mezi informace, které NetFlow záznam obsahuje patří například:

- Počet bytů a paketů v daném toku dat.
- Časové vymezení začátku a konce přenosu dat.
- Hlavičky síťové vrstvy: zdrojová a cílová IP adresa, zdrojový a cílový port, apod.

3.3 Nástroje

Pro práci se záznamy NetFlow dat existuje řada nástrojů. V této práci byl použit nástroj NfDump, více o tomto nástroji je napsáno v *kapitole 2.5*. Mezi další nástroje patří následující:

- nfcapd – tento nástroj čte NetFlow data přímo ze sítě a ukládá je do souborů.
- nfdump – *viz. kapitola 2.5.*
- nfprofile – čte data ze souborů, uložených nástrojem nfcapd, tato data filtruje podle uložených profilů a poté vyfiltrovaná data ukládá do souborů pro pozdější použití.
- nfreplay – čte a posílá data uložená v souborech po síti do dalších počítačů.
- nfclean – skript pro promazání starých dat, může se spouštět periodicky.

Více informací o technologii NetFlow lze nalézt například na adrese http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html.

3.4 Použití

Technologie NetFlow skýtá velké možnosti, co se použití týče. Můžeme vybrat například následující: sledování aplikací a uživatelů, zvýšení bezpečnosti na síti, omezení útoků na síť, odhalení nesprávných konfigurací, dokonalý přehled o situaci na síti, plánování kapacity sítě, ale také například účtování a fakturace, či kontrola FUP.

Co se uživatelů týče, můžeme pomocí NetFlow například sledovat: kdo nejvíce vytěžuje kapacitu linky, kdo nejvíce navštěvuje stránky se zakázanou tématikou, kdo nejvíce stahuje zakázaná data nebo kdo v pracovní době tráví čas na webových stránkách, chatu či komunikací přes programy typu Jabber, ICQ nebo Yahoo messanger.

Dále je tu možnost předvídat růst zatížení sítě a plánovat vylepšování a optimalizaci sítě. Optimalizací sítě je možné snížit provozní náklady a zvýšit spolehlivost a výkonnost. Další důležitou vlastností NetFlow je možná identifikace a upozornění na nechtěné aktivity v síti, jako jsou útoky DoS, viry, červi a skenování portů.

3.5 NfDump

Nástroj pro čtení a zpracování NetFlow dat. Je distribuován pod BSD licencí. Umožňuje tvorbu mnoha druhů statistik z NetFlow dat. Podporuje Netflow záznamy ve verzích v5, v7 a v9.

Jako příklad syntaxe použití můžeme uvést dotaz na statistiku TOP 10 uživatelů, kteří stáhli nejvíce dat přes port 80 (WWW server).

```
nfdump -R/path/.../ -n 10 -s ip/bytes `port 80`
```

Parametr `-R` znamená, že budou brána v potaz všechna data ve složce `/path/.../`, `-n` je počet údajů, `-s` je klíč statistiky / klíč pro seřazení dat a text v uvozovkách určuje filtr, v našem případě bereme v úvahu pouze data, kde port je roven 80.

Tento nástroj obsahuje celou řadu možností, jak bude výsledná statistika vypadat. Data lze filtrovat a řadit podle mnoha různých klíčů. Podrobné informace je možno nalézt na oficiální adrese http://nfdump.sourceforge.net/.

4 Návrh

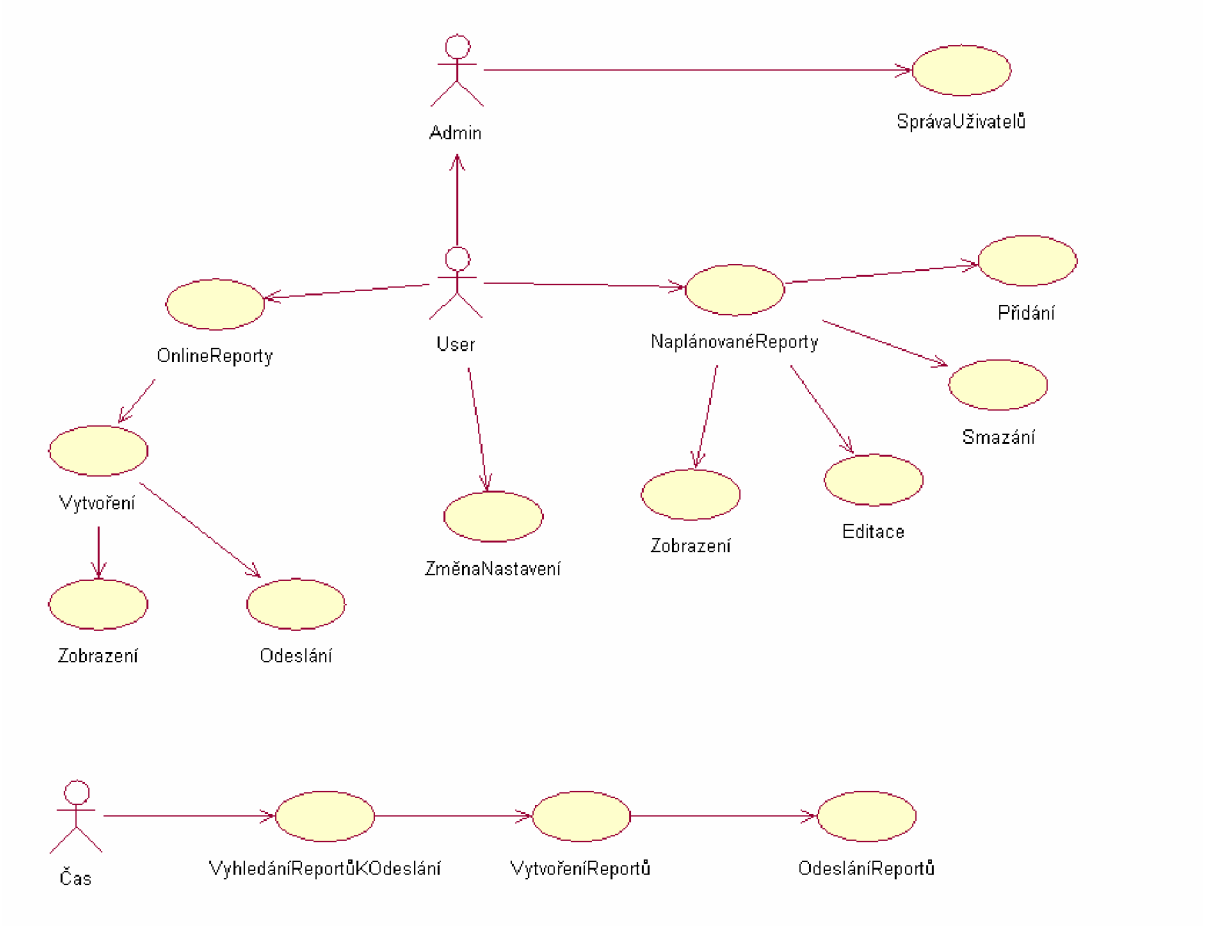
Po analýze požadavků přichází na řadu návrh řešení a implementace. Při návrhu systémů bychom nejprve měli vytvořit model daného systému. Pro tento způsob návrhu se nejčastěji používají modelovací jazyky. Jedním z nich je například jazyk UML.

4.1 UML

Unified Modelling language je modelovací jazyk, který se nejčastěji používá ve softwarovém inženýrství. Umožňuje tvorbu abstraktních modelů a diagramů, které se nejvíce využívají při návrhu a specifikaci systémů. UML podporuje objektově orientovaný přístup k analýze. V našem případě byl použit diagram případů užití (Use Case Diagram), a to při tvorbě návrhu řešení této aplikace.

4.1.1 Diagram případů užití (Use Case Diagram)

Use Case diagram je určen k definici chování systému z pohledu uživatele. Jedná se v podstatě o scénáře pro použití tohoto systému a graficky v něm zachycujeme interakce uživatele se systémem samotným. Use case diagram vytvořený při tvorbě této práce můžete vidět níže na *obrázku 2.1.*



Obr. 2.1.: Diagram případů použit

5 Implementace

5.1 Použité technologie

5.1.1 HTML

Hypertext Markup Language je značkovací jazyk pro tvorbu webových stránek a publikaci dokumentů na internetu. Jedná se o textový jazyk, který používá značky (tagy) k formátování. Původem vznikl z univerzálního značkovacího jazyka SGML (Standard Generalized Markup Language). Jeho vývoj je ovlivněn vývojem internetových prohlížečů.

Jazyk HTML byl poprvé navržen v roce 1990 spolu s protokolem HTTP pro jeho přenos. Autorem byl Tim Berners-Lee. První verze ještě nepodporovala grafický režim, poté však nastal rychlý vývoj a v roce 1997 byla vydána verze 4.0, která se až na několik drobností a oprav podobá verzi aktuální. Standarty jazyka HTML vydává od verze 3.2 konsorcium W3C. V čele tohoto konsorcia je autor původní formy HTML Tim Berners-Lee.

V současné době se nejvíce používá verze jazyka HTML 4.01 z roku 1999, která se ale postupně nahrazuje novým jazykem XHTML. Právě jazyk XHTML se měl stát nástupcem jazyka HTML, ale v roce 2007 byla sestavena skupina, která má za úkol vytvoření jazyka HTML ve verzi 5. XHTML je stále vyvíjeno a očekává se jeho verze 2.0.

První verze jazyka XHTML se objevila v roce 2000. Tento jazyk vyhovuje požadavkům pro tvorbu XML, ale zároveň je zpětně kompatibilní s jazykem HTML. Aktuální verze je 1.1. Mezi rozdíly oproti jazyku HTML například patří psaní značek (tag) malými písmeny, ukončení všech značek (tag), i když se jedná o nepárové značky a dále dokument musí začínat XML deklarací. Jazyk XHTML byl použit i v této práci, příklad použité hlavičky uvádím níže.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="cs" lang="cs">
```

5.1.2 PHP

Hypertext Preprocessor je universální skriptovací jazyk pro tvorbu dynamických webových stránek s volně dostupným zdrojovým kódem. PHP kód je přímo začleněný v HTML kódu stránky, je interpretovaný a provádí se na straně serveru. PHP je možné použít nejen při tvorbě webových stránek, ale také při tvorbě desktopových aplikací.

Tento jazyk původně vznikl odvozením z jazyka PERL a velice se podobá jazyku C, ale také třeba jazyku Java. V dnešní době se jedná o velice populární jazyk pro tvorbu webových stránek. Nejčastěji se používá v kombinaci s databází, obvykle s databází typu SQL. Výhodou je velká rozšiřitelnost v podobě doplňujících knihoven. I v této práci byly využity některé doplňující knihovny, jako například FPDF, JpGraph či PHP Mailer. Výborná je i podpora, co se protokolů týče. PHP umí pracovat s mnoha protokoly, např. s HTTP, HTTPS, SMTP, POP, IMAP a dále.

Jazyk PHP se poprvé objevil v roce 1994 a jeho autorem byl Rasmus Lerdorf. Původně bylo PHP určeno pouze pro osobní potřeby autora. První oficiální název byl Personal Home Page Tools. PHP poté prošlo mnoha změnami. V roce 1997 bylo společně s formulováním základů verze PHP3, také změněno jméno tohoto jazyka na PHP Hypertext Preprocessor. V současné době se nejčastěji používají verze 4 a 5. Poslední je verze 5.2.5 z roku 2007.

5.1.3 XML

Extensible markup language je značkovací jazyk vyvinutý konsorciem W3C. Stejně jako HTML patří do podskupiny jazyka SGML. Dále umožňuje vytváření různých značkovacích jazyků a je spojen s nástupem XHTML. Aktuální je verze 1.1.

XML nemá žádné předdefinované značky a umožňuje tak uživatelům tvořit jejich vlastní značky. Je převážně určen pro publikování dokumentů a výměnu dat mezi aplikacemi. Jeho syntaxe je přísnější než u jazyka HTML. XML nepopisuje vzhled výsledného dokumentu, ale zabývá se

především popisem struktury dokumentu z hlediska obsahu. Výsledný vzhled dokumentu se definuje pomocí přidaného stylu.

XML dokument je vždy textový a Unicode. Často se používá kódování UTF-8. Každý dokument by měl být správně strukturovaný (well-formed), tedy měl by obsahovat jeden kořenový element, neprázdné elementy by měly mít jak zahajovací, tak ukončovací značku a všechny hodnoty atributů by měly být v uvozovkách. Ze stejných vlastností vychází i výše zmiňovaný jazyk XHTML.

5.1.4 CSS

Cascading style sheets neboli kaskádové styly jsou jazykem, určeným pro popis vzhledu HTML stránek. Hlavím úkolem jazyka je oddělení struktury, obsahu a funkce HTML stránky od jejího vzhledu. Kaskádové styly je možno také použít v kombinaci s jazykem XML.

Velkou výhodou tohoto jazyka je možnost přehledné modifikace vzhledu stránky, široká škála možností při tvorbě vzhledu a hlavně zpřehlednění samotného kódu HTML stránky. Jazyk CSS však má i negativní stránky, hlavně co se kompatibility týče. Podpora standardů u některých prohlížečů je neúplná a často vede k problémům při zobrazování některých HTML stránek.

CSS byl navržen a standardizován konsorciem W3C. Byl vydán ve dvou specifikacích CSS1 a CSS2. V současné době se vyvíjí verze CSS3.

5.1.5 Javascript

Javascript je objektově orientovaný jazyk, syntaxí je podobný jazykům C++ a Java. Jeho autorem je Brendan Eich a poprvé byl standardizován v roce 1997. Stejně jako v případě PHP se jedná o skriptovací jazyk.

Kód v Javascriptu se, naopak od PHP, provádí na straně klienta, kam je odeslán se stránkou. Z toho plyne jasná výhoda, že pomocí Javascriptu můžeme provádět akce ještě před odesláním na server. Tímto způsobem můžeme například zrychlit a zefektivnit práci se stránkami. Možnou nevýhodou je občasná blokace spouštění Javascriptu ze strany klienta, převážně z bezpečnostních důvodů.

5.1.6 SSL

Jedná se o protokol pro možnosti zabezpečené komunikace, který je postaven na kryptografii veřejným klíčem. Stará se o autentizaci, šifrování a výměnu certifikovaných veřejných klíčů. SSL pracuje mezi aplikační a transportní vrstvou. Komunikace mezi klientem a serverem probíhá následujícím způsobem. Klient inicializuje spojení a žádá nastavení SSL, server odpovídá odesláním nastavení, certifikátu a veřejného klíče. Server prokáže svoji identitu pomocí odeslání zprávy šifrované tajným klíčem. Klient generuje relační náhodný klíč, ten zašifruje veřejným klíčem serveru a odešle na server. Server potvrdí příjem. Nyní se zahájí komunikace šifrovaná relačním klíčem.

Při šifrování se využívají algoritmy MD5, SHA1, DES, AES a další. Nejčastěji se tento protokol využívá ve spojení s HTTP. Vzniká tak nadstavba zvaná HTTPS. HTTPS poskytuje vyšší bezpečnost dat a komunikace. Implicitně pracuje na portu 443.

5.2 Použité knihovny

5.2.1 Práce s XML

Místo databáze byl v této práci použit konfigurační soubor ve formátu XML. Do souboru se data zapisují, data se editují, dochází k jejich mazání i vyhledávání. Procházení XML souborů je implementováno pomocí knihovny Expat, která je již obsažena v instalaci PHP. Tato knihovna je volně přístupná, jedná se o open source. Jejím autorem je James Clark a stáhnout se dá na adrese http://www.jclark.com/xml/expat.html.

Pro tvorbu a zápis XML souborů byla použita knihovna XML_Serializer. Tato knihovna je přístupná pod PHP licencí a je stažitelná z adresy http://pear.php.net/package/XML_Serializer/. Jedná se o poměrně dobře propracovanou knihovnu, která je jednoduchá, co se použití týče a obsahuje dostatek funkcí pro tvorbu a možnosti nastavení výsledných XML souborů.

5.2.2 Tvorba PDF

Pro zprávy o síťovém provozu byl použit formát PDF (Portable document format). PDF je formát pro ukládání dokumentů, vyvinutý firmou Adobe. Výsledný dokument nemusí obsahovat jen text, ale i různé tabulky či obrázky. Výhodou PDF formátu je jeho nezávislost na použitém zařízení. Dokument se také zobrazí stejně, jak pod operačním systémem UNIX, tak pod Microsoft Windows. Právě jeho nezávislost a dostupnost bezplatných prohlížečů ho v dnešní době řadí mezi velice často používané a oblíbené formy dokumentů.

O vytvoření PDF dokumentu se v aplikaci stará knihovna FPDF. Velké F na začátku názvu knihovny značí slovo free, v překladu volný. Jedná se tedy o volně přístupnou knihovnu. Domovská stránka této knihovny je http://www.fpdf.org.

5.2.3 Tvorba grafů

Pro jednoduché a výstižné zobrazení statistik se velmi často používají grafy. Není tomu jinak ani v této aplikaci. S ohledem na současný trend se statistiky generují jako tzv. grafy ‚koláčové'. Pro generování grafů byla použita knihovna JpGraph. Opět se jedná o knihovnu volně stažitelnou, naleznete ji na adrese http://www.aditus.nu/jpgraph/. Jedná se o velice dobře propracovanou knihovnu, která podporuje tvorbu mnoha různých typů grafů.

5.2.4 Práce s e-maily

Jedním z hlavních komunikačních prostředků aplikace je komunikace přes e-mailové zprávy. Pomocí e-mailů se posílají jednotlivé reporty uživatelům. K přenosu e-mailových zpráv se používá protokol SMTP. Jedná se o protokol pracují nad TCP, který komunikuje na portu 25.

PHP samo o sobě obsahuje funkci mail(), která slouží k odesílání e-mailových zpráv. Bohužel tato funkce je velmi jednoduchá a limitovaná v použití, navíc je její použití často nepřehledné. Proto byla v aplikaci použita volně šířitelná knihovna PHP Mailer. Knihovna je stažitelná na adrese http://phpmailer.codeworxtech.com/.

5.2.5 Automatické spouštění skriptů

Více než uživatelské rozhraní je pro tuto aplikaci důležitější automatické spouštění PHP skriptu, který se stará o automatické odesílání reportů. Skript je spouštěn periodicky každý den v danou hodinu. Nastavení automatického spuštění bylo umožněno díky programu crontab.

Jedná se o program, který pracuje s Cron Deamonem. Ten umožňuje naplánovaní a spuštění určité události ve zvolený čas. Takto můžeme například automaticky spouštět skripty na serveru v daném časovém intervalu. Pro práci s crontabem musíme být připojení přes ssh, například pomocí volně stažitelného programu putty. Crontab editujeme příkazem `crontab -e`, aktuální nastavení lze vypsat příkazem `crontab -l`. Syntaxe jednotlivých událostí je uvedena níže.

```
* * * * * /usr/local/bin/php /path/to/file.php
```

Kde file.php je spouštěný skript a jednotlivé hvězdičky reprezentují, kdy se má skript spouštět. Význam jednotlivých hvězdiček je následující: (hodina), (minuta), (den v měsíci), (měsíc v roce), (den v týdnu).

5.2.6 Šifrování dat

Pro zvýšení bezpečnosti dat je v dnešní době nutností citlivá data šifrovat. Pro šifrování dat byl použit volně šiřitelný kód v jazyce javascript MD5. Jedná se o hashovací funkci s 128bitovým klíčem. Po zadání citlivých dat (hesel) se data ještě před odesláním zašifrují a spolu s nimi se pošle i náhodně generovaný kontrolní řetězec. Po přijetí na straně serveru se data porovnají s daty v souboru. Šifrování pomocí MD5 bylo použito i pro zašifrování dat v souborech.

5.3 Popis vybraných skriptů

V této části jsou stručně popsány skripty, ze kterých je webový portál složen. Nejedná se o všechny skripty, ale pouze o některé vybrané. Zároveň popis těchto skriptů je pouze obecného charakteru.

index.php Hlavní skript celé aplikace. Je zde vytvořena hlavička HTML stránky i přilinkování kaskádových stylů a javascript souborů. Převážně, ale tento skript obstarává práci se Sessions.

Dále zajišťuje přihlašování a odhlašování uživatelů. Kontroluje zadaná hesla a kontrolní řetězce při přihlášení. K této činnosti využívá algoritmu HMAC_MD5. V neposlední řadě zajišťuje kontrolu nečinnosti uživatele a jeho případné odhlášení. Doba, po které je uživatel odhlášen ze systému, je uložena jako konstanta ve skriptu config.php. Po odhlášení uživatele dochází ke smazání všech dočasných pomocných souborů.

login.php Přihlašovací skript, obsahuje formulář pro přihlášení. Po potvrzení odeslání se data zašifrují pomocí funkce MD5 a pak teprve odešlou na server. Spolu s daty se posílá i skrytý kontrolní řetězec, který vznikne zřetězením a zašifrováním náhodně vygenerovaného čísla a hesla.

xmlget.php Hlavní skript pro práce s XML soubory. Využívá funkcí knihovny XML Serializer a Expat. Expat je přímo obsažený v instalaci PHP. Skript zajišťuje zápis, mazání a editaci dat v XML, stejně tak jejich výpis či vyhledání.

savedate.php Zde je obsažen formulář pro přidávání nových reportů a kalendář pro nastavení data odeslání reportů. Pro svou činnost skript využívá javascriptové soubory *calendar.js* a *forms.js*. První z nich obsahuje funkce pro práci s kalendářem, druhý z nich pak funkce pro kontrolu vstupních dat ještě před odesláním na server. Pokud jsou data odeslána v pořádku, jsou předána skriptu *xmlget.php* pro uložení.

showdata.php Tento skript je podobný jako výše zmíněný skript *savedata.php*. Není ale určen pro přidání nových reportů, ale pro zobrazení či vytvoření reportu online. Opět tedy obsahuje formulář pro zadání reportu, ten ale při úspěšném odeslání požadavku nepředává skriptu *xmlget.php* pro zápis, ale předá řízení skriptu *nfdump.php*.

nfdump.php Skript obsahuje funkci pro práci s nástrojem nfdump. Komunikace s tímto nástrojem probíhá přes příkazovou řádku. Jednotlivé příkazy se nejprve sestaví z cesty k datům a z jednotlivých parametrů. Testovací data jsou uložena v adresářích podle roku, měsíce a dne, kdy byla pořízena. NfDump pracuje s daty, která spadají do uživatelem zvoleného období. Tedy například, pokud si uživatel vybere posílání statistik jednou měsíčně, pak jsou brána v potaz data za dobu jednoho měsíce před aktuálním dnem odeslání. Ostatní parametry jsou doplněny podle výběru typu statistiky.

outputparser.php Hlavní náplní tohoto skriptu je parsování výstupu z nástroje nfdump. Tento výstupní text je ‚rozsekán' na potřebné položky či věty, které jsou následně poslány skriptům *makepie.php* a *makepdf.php*. Tento skript dále zajišťuje překlad IP adres na doménová jména pomocí příkazu *host*.

makepie.php Tento skript pracuje s knihovnou JpGraph. Na základě parsovaných dat ze skriptu *outpuparser.php* generuje graf, který se uloží do souboru typu PNG na server. Pokud se jedná o zobrazení statistiky online, pak je tento graf začleněn do HTML kódu.

makepdf.php Zde se opět využívá volně šiřitelné knihovny, tentokráte se jedná o knihovnu FPDF, pro tvorbu dokumentů formátu PDF. Jako vstup jsou opět použita parsovaná data ze skriptu

outputparser.php, ze kterých jsou tvořeny tabulky a podle který jsou tvořeny nadpisy a text. Dále se do dokumentu přidává graf vytvořený skriptem *makepie.php*.

sendmail.php I zde je využita volně dostupná knihovna, tentokráte se jedná o knihovnu pro odesílání e-mailů PHP Mailer. Jako příloha je odeslána zpráva ve formátu PDF. Pro získání e-mailu uživatele se použije funkce ze skriptu *xmlget.php*.

func.php Skript s pomocnými funkcemi, které využívají ostatní skripty, mj. obsahuje funkce pro kontrolu zadaných dat, dále funkci pro otevření požadované stránky a také php verzi funkce MD5.

config.php Skript s konstantami, které jsou využity v ostatních skriptech. Při instalaci aplikace je nutná změna některých z nich. Jedná se o konstanty, definující cestu k souborům a knihovnám, konstanty jednotek a také konstanty určující velikosti písma a různých dalších prvků portálu.

settings.php Poskytuje možnost změny uživatelského nastavení, tedy hesla a e-mailu. Dále umožňuje uživateli nastavit generování komplexních reportů za určité období. Všechna data odeslána přes formulář jsou nejprve kontrolována pomocí javascriptových funkcí a hesla jsou šifrována ještě před samotným odesláním. Spolu s hesly je poslán ještě kontrolní řetězec.

managment.php Skript určený výhradně pro administrátory systému. Vytváří formulář pro přidání nových uživatelů, kontroluje zadaná data i pomocí javascriptových funkcí, obsažených v souboru *forms.js*. Odeslaná a správná data předává skriptu *xmlget.php* k zápisu do XML souboru. Umožňuje data o uživatelích editovat, či uživatele mazat.

xmldeluser.php Funkce obsažená v tomto skriptu se volá pokaždé, když administrátor smaže některého z uživatelů. Funkce prohledá XML soubor s konfigurací reportů, jestli zde neexistuje položka, která patří právě smazanému uživateli, pokud ano, pak ji smaže.

javascript skripty forms.js a calendar.js Jedná se o pomocné skripty, které obsahují funkce pro práci s kalendářem, potažmo pro kontrolu dat, odeslaných přes formuláře.

5.4 Uživatelské prostředí

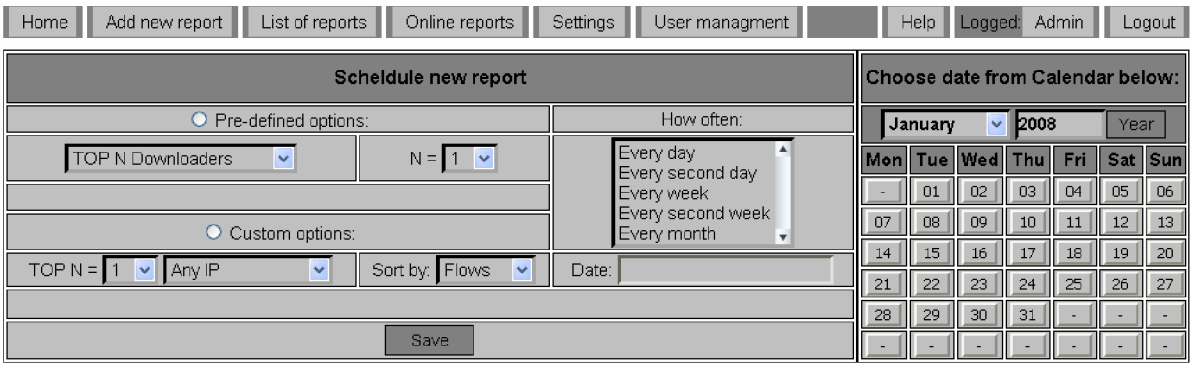
Při tvorbě uživatelského prostředí byl kladen důraz na funkčnost a přehlednost. Zároveň bylo nutné, aby funkčně splňovalo zadané parametry. Uživatelské prostředí neoplývá různými grafickými prvky, je naopak z tohoto pohledu poměrně strohé. Tímto je zaručena vysoká přehlednost a jednoduchost celého rozhraní.

Uživatel může plánovat posílání reportů, toto nastavení přidávat, editovat či mazat. Dále je mu k dispozici možnost nechat si zobrazit statistiku online a v případě potřeby z této statistiky vygenerovat report a odeslat ho na e-mail. Samozřejmostí je možnost změny uživatelových nastavení, konkrétně se jedná o změnu aktuálního hesla pro přístup na portál a změna e-mailu.

Uživatel si také může nechat posílat souhrnné reporty za určité období. Může si vybrat mezi měsíčním posíláním a týdenním. Týdenní posílání probíhá každé pondělí, měsíční poté vždy každý

první den v měsíci. Tyto souhrnné reporty se mohou skládat z několika statistik. Uživatel má na výběr z celkem šesti předefinovaných statistik.

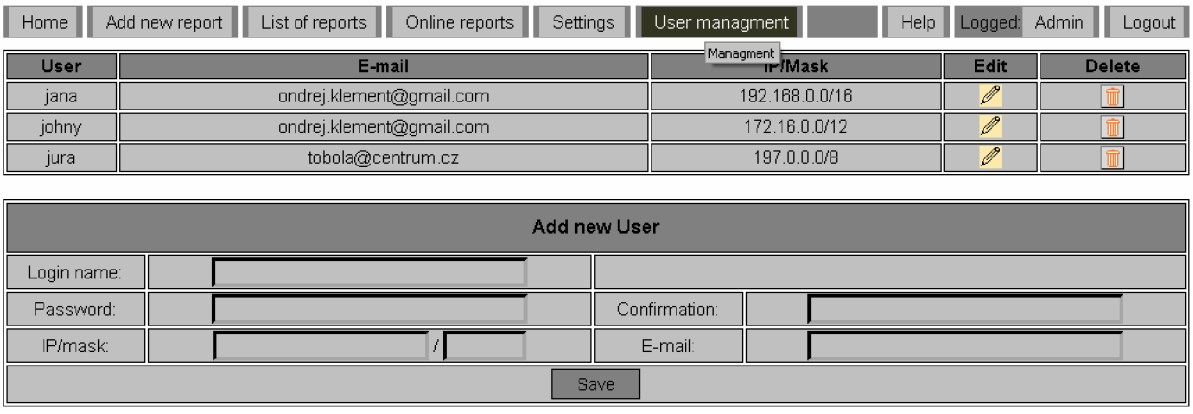
Na *obrázku 5.1.* můžete vidět formulář pro naplánování nového reportu a kalendář. Uživatel si tedy může vybrat mezi předdefinovanými a volitelnými statistikami. Při volbě předdefinované statistiky stačí již jen specifikovat počet položek statistiky, u volitelných je nutné specifikovat všechny parametry, tedy počet položek, hlavní položku statistiky a klíč pro seřazení dat. Dále uživatel vybere jak často požaduje statistiky posílat a nakonec v kalendáři zvolí datum odeslání. Nyní již stačí pouze potvrdit volby stiskem tlačítka Save.



Obr. 5.1.: Naplánování nového reportu

5.5 Administrátorské prostředí

Administrátorské prostředí se vzhledově ani stylově neliší od prostředí uživatelského. Stejné je i ovládání, jediný rozdíl je funkčnosti. Administrátorovi je umožněna správa uživatelů. Příklad správy uživatelů můžete vidět na *obrázku 5.2.* První tabulka obsahuje výpis všech aktuálních uživatelů systému. Administrátor může jednotlivé uživatele mazat nebo editovat jejich údaje po stisku tlačítka Delete, respektive Edit. Při vytváření uživatelského účtu je zapotřebí zadat login, heslo a rozsah IP adres uživatele v podobě masky. Právě rozsah IP adres určuje uživatelovi práva, jelikož právě podle této položky jsou filtrovány statistiky. E-mail je nepovinná položka.



Obr. 5.2.: Správa uživatelů

5.6 Skript pro automatické odesílání

Mimo samotné uživatelské rozhraní aplikace obsahuje skript, který je spouštěn periodicky, ve zvoleném intervalu, v našem případě je to každý den v 8 hodin ráno. Tento skript prohledá uložená nastavení v XML konfiguračním souboru a v případě shody v datu, odešle dotaz na uživatelem vybranou statistiku, poté z výstupu z nástroje NfDump vygeneruje graf a tabulku, které vloží do dokumentu formátu PDF. Nakonec odešle tento dokument na uživatelem nastavenou e-mailovou adresu a ukončí se. Ještě před tím než se ukončí, smaže všechny dočasné soubory.

5.7 Chybová hlášení

Existuje stará pravda, že člověk není tvor neomylný. Z toho je nutné vycházet i při tvorbě webového portálu. Je tedy nutné kontrolovat možné chyby uživatele, případně snažit se jim předejít. V této práci existují dva druhy chybových hlášení, jedná se o hlášení přímo v HTML a hlášení pomocí Javascriptu. Výhodou posledně jmenovaného je, že k zachycení chyby dojde již před odesláním na server. Tímto způsobem tedy není nutné aktuální stránky znovu načítat a zrychluje se tak práce s aplikací.

5.8 Zabezpečení

V dnešní době je nutné, aby každá webová aplikace byla dobře zabezpečena proti případným útočníkům. Jedná se o prvek, který je nutné neustále zdokonalovat a aktualizovat. Zabezpečení na vysoké úrovni by měly obsahovat především portály a systémy s obsahem velmi citlivých dat, jako jsou bankovní systémy, lékařské systémy, ale také třeba školní systémy. Stejně tak je tomu i v případě tohoto portálu. Zabezpečení aplikace je na současné poměry standardní.

Při přihlašování uživatelů do systému a při manipulaci s hesly byl použit šifrovací algoritmus MD5 a HMAC_MD5. Tento algoritmus nejenom šifruje hesla ještě před odesláním na server, ale také používá kontrolní řetězec, který se pošle spolu s daty na server, kde proběhne jeho verifikace společně s heslem poslaným a heslem v souboru. Kontrolní řetězec se vytváří pomocí algoritmu HMAC_MD5 zašifrováním a zřetězením hesla náhodně generovaného klíče. V našem případě se jedná o UNIX datum.

Pro případ možného zneužití informací uložených v Sessions se při přihlášení uživatele do systému vygeneruje řetězec, v našem případě počet sekund od roku 1.1.1970 (UNIX datum), ten se zašifruje použitím MD5 algoritmu a uloží do souboru na server a do Sessions. Při každém načtení skriptu dochází ke kontrole řetězce v souboru a v Sessions, pokud nesouhlasí, je uživatel odhlášen. Zároveň je kontrolována doba nečinnosti uživatele na portálu. Pokud doba nečinnosti dosáhne určité hodnoty (specifikováno v *config.php*), je uživatel odhlášen.

Hlavním prvkem zabezpečení tohoto portálu je komunikace přes protokol HTTPS. Jedná se o protokol, který využívá šifrování SSL. Tento způsob zabezpečené komunikace přináší vyšší bezpečnost před odposloucháváním dat nebo před jejich podvržením.

5.9 Statistiky

Práce se statistikami je jednou z hlavních náplní tohoto portálu. V této práci jsou rozlišeny dva typy statistik. Jedná se předdefinované statistiky a o volitelné statistiky. Všechny výsledné statistiky jsou filtrovány pouze na IP adresy, kterými daný uživatel disponuje. To samozřejmě neplatí o administrátorovi.

Předdefinované statistiky jsou statistiky souhrnné a často používané, není zde pro uživatele nutné nic zadávat. Mezi tyto statistiky patří například Top N stahovačů dat, Top N uživatelů s největším přístupem na ICQ nebo Top uživatelů, kteří využívají WWW stránky. Mezí další statistiky patří detekce DoS útoků a potencionálně zavirovaných počítačů. Detekce DoS útoků se provádí pomocí filtrování statistik pouze na toky přes protokol TCP s příznakem SYN a bez následného příznaku ACK či FIN.

Naopak volitelné statistiky jsou určeny převážně pro pokročilejší uživatele, jedná se o mnohem více flexibilnější statistiky, jelikož si je může uživatel značně upravit a v podstatě umožňují vytvoření vlastní statistiky, která daného uživatele zajímá. Uživatel musí zadat klíč statistiky a klíč pro seřazení a pokud chce, tak je k dispozici i možnost zadání filtru. Tato možnost je tedy určena převážně pokročilejším uživatelům.

5.10 Ovládání

Ovládání portálu je velice intuitivní a poměrně dosti jednoduché. Nemělo by činit problém nikomu, kdo je alespoň trochu znalý v oblasti webových stránek a internetu obecně. O něco složitější to již bude s pochopením obsahu a funkcí tohoto portálu. Portál je převážně určen pro správce sítě, tedy pro uživatele, kteří se dobře vyznají v oblastí sítí, přesto i mírně pokročilí by neměli mít s pochopením problém. Pro případ jakýchkoliv nejasností či problémů obsahuje tento portál i jednoduchý systém nápovědy, případně nahlédněte do souboru README, který je přiložen k této zprávě.

5.11 Nápověda

Kromě portálu a této zprávy obsahuje tato práce také jednoduchý systém nápovědy pro uživatele portálu. Nápověda lze spustit přímo ze souboru index.html, který se nachází ve složce help nebo kliknutím na odkaz, který je umístěn přímo v hlavní nabídce portálu. Nápověda je vytvořená v jazyce HTML a obsahuje základní informace potřebné pro práci s portálem. Jedná se především o popis

instalace, ovládání a funkcí portálu, dále informace o autorovi a také často kladené otázky, neboli FAQ.

5.12 Struktura XML

```
<Data>
  <Id>2</Id>
  <Statistic>1:1</Statistic>
  <Setting>3</Setting>
  <Date>9-01-2008</Date>
  <Belongs>admin</Belongs>
</Data>
```

6 Testování a instalace

Samotnou implementací tvorba aplikace nekončí. Ještě před tím než můžeme aplikaci zprovoznit pro uživatele, je nutné, aby prošla důkladným testováním. Při testování se snažíme odchytit co nejvíce chyb aplikace, bohužel je často nemožné odchytit chyby všechny. Je velice důležité, abychom při testování vyzkoušeli aplikaci za různých situací a vymysleli jsme co nejvíce možných akcí, které budou uživatelé s aplikací provádět. Konfigurace, na kterých byl portál testován, naleznete níže.

Server:

- Operační systém: Linux ela 2.6.15-26-amd64-generic #1
- Server: Apache 2.0
- PHP 5.1.2.
- NfDump 1.53

Klient

- Operační systém: Microsoft Windows XP SP2
- Prohlížeč: Mozilla Firefox 2.0, Internet Explorer 7.0

6.1 Požadavky

6.1.1 Na straně serveru

- Nainstalované PHP, ideálně verze 5 a výš.
- Nainstalovaný NfDump a přístupné NetFlow datové záznamy.
- Doinstalované potřebné knihovny.

6.1.2 Na straně klienta

Není zapotřebí ničeho jiného, nežli připojení k internetu, internetového prohlížeče, např. Mozilla Firefox a prohlížeč dokumentů PDF, např. Acrobat Reader.

6.2 Instalace na server

Pokud sever odpovídá minimálním požadavkům je možné zahájit instalaci na server. Instalace je poměrně jednoduchá, stačí pouze nakopírovat jednotlivé soubory do adresáře na serveru. Umožnit nejen čtení, ale i zápis u konfiguračních souborů a podle potřeby změnit konstanty ve skriptu config.php a dále ve skriptech, kde se používají další knihovny. Posledním krokem je přidání spouštění automatického skriptu do crontabu. Nyní by mělo být vše připravené a funkční. Podrobnější popis instalace portálu i potřebných knihoven se nachází v souboru INSTALL, který je přiložen k této práci.

7 Možná rozšíření

7.1 Bezpečnost

Jak již bylo v této práci zmíněno, je nutné neustále zdokonalovat a aktualizovat zabezpečení webových aplikací a systémů obecně. To, že dnes je aplikace dobře zabezpečená, nemusí zítra již platit. Mezi možné úpravy zabezpečení lze zahrnout použití lepšího šifrování, například šifrování s 512bitovým klíčem. Dále také šifrování dat přenášených přímo v URL před jejich odesláním a jejich následné rozšifrování po přenesení.

7.2 Archivace reportů

Hned na začátku této práce v kapitole Úvod, jsme se seznámili s možnostmi využití tohoto portálu. Mezi tyto možnosti patří i analýza získaných dat a statistik pro následné využití při zdokonalování služeb, jak co se kvality týče, tak i finančně. Právě pro tyto účely je vhodným rozšířením archivace jednotlivých reportů na straně serveru a administrátora. Portál by po implementaci této funkce mohl automaticky archivovat jednotlivé reporty podle nastavení uživatele.

7.3 Rozšíření statistik

Nástroj Nfdump skýtá mnoho možností, co se statistik týče. Možnosti implementované v této práci jsou pouze ukázkou toho, co tento nástroj dokáže. Proto jedno z hlavních možných rozšíření je právě rozšíření počtu statistik. Jednou z možností je propracování filtrování dat. V této práci lze data filtrovat pomocí ip adres a pomocí portů. Do budoucna by se tento portál mohl rozšířit o filtrování dat pomocí protokolů, zařízení, příznaků či bps nebo pps.

Rozšíření by mohla dostát i forma reportů a statistik. V současné době portál generuje reporty obsahující tabulky a ‚koláčové' grafy. To by se dalo rozšířit o celou řadu dalších typů grafů a nejen to, údaje by mohly být vyjádřeny procentuálně, například uveďme jako příklad procentuální využití kapacity linky. Ale nemusí to být jen procentuální vyjádření, může se jednat i o maximální, minimální či průměrné hodnoty některých údajů.

7.4 Další vylepšení uživatelského rozhraní

Vývoj v oblasti internetu a webových stránek jde neustále dopředu a s ním různorodost a kvalita stylového a grafického pojetí webových stránek a aplikací. V této práci byl kladen důraz na jednoduché a přehledné grafické prostředí. Proto lze toto prostředí do budoucna rozšířit a aktualizovat o nové grafické prvky a také celkový vzhled a styl stránek zdokonalit a zmodernizovat. S tímto spojené mohou být i zdokonalení, co se ovládání a přehlednosti týče.

7.5 Profily

V aktuální podobě je možné na portálu pracovat s přednastavenými a volitelnými statistikami. Pokud uživatel nenajde požadovanou statistiku mezi vybranými, je nucen si tuto statistiku nadefinovat sám. Proto je do budoucna možné přidat profily, které by tuto činnost pro uživatele značně zjednodušily. Každý uživatel by si po nakonfigurování své vlastní statistiky, mohl toto nastavení uložit, tedy vytvořit nový profil a tím statistiku přidat mezi předdefinované. Zároveň by systém umožňoval správu těchto profilů.

8 Závěr

Náplní této bakalářské práce bylo seznámení se s prostředky pro tvorbu webových systémů a s technologií NetFlow pro monitorování provozu na síti. Analýza možnosti tvorby grafů, tabulek a reportů o síťovém provozu. Návrh modelu systému, který by takové reporty generoval a jeho následná implementace. Všechny tyto prvky zadání byly bez výjimky splněny, přesto však se nedá říct, že by výsledný systém byl definitivní či dokonalý v jakémkoliv ohledu. Je stále ještě mnoho možných funkcí, které je možno do systému přidat a tím systém rozšířit, stejně tak teprve plné nasazení portálu do užívání ukáže, jak kvalitní doopravdy je a co je potřeba upravit či přidat.

Při vývoji tohoto portálu jsme prošli několika fázemi. Nejprve specifikací a analýzou požadavků. Seznámili jsme se s možnostmi modelovacích jazyků a s návrhem modelu systému obecně. Poté jsme samotný model implementovali za použití různých implementačních prostředků a nakonec jsme systém důkladně testovali a ladili.

Při práci na tomto portálu jsem si mohl vyzkoušet řadu znalostí, nabytých studiem na této fakultě. V samotné práci byly využity poznatky z několika předmětů. Při modelování a návrhu, ale i při specifikaci a analýze zadání se mně velice hodily znalosti z předmětu IUS. Při samotné implementaci jsem často využíval skripta z předmětů IIS a ITW. Ale to nejsou jediné předměty, ze kterých jsem čerpal, dále také určitě z předmětů IPK, ITU či ISA. Celkově asi největším přínosem pro mne byla samotná implementace, kdy jsem si prakticky vyzkoušel programování v jazyce PHP, HTML, CSS či JavaScript.

V rámci této práce byl specifikován, analyzován, navržen a implementován systém pro generování zpráv o síťovém provozu. Tento systém skýtá mnoho možností využití a obsahuje mnoho užitečných funkcí a možností. Výhodou tohoto systému je zejména možnost jednoduchého, přehledného a účinného monitoringu a také analýzy síťové komunikace a celkového provozu na síti. Velice užitečná je i možnost detekce útoků a virů, která těmto nebezpečím pomáhá předejít. Za velmi pozitivní považuji fakt, že se nejedná pouze o školní projekt, ale že tato práce má i reálné využití a je schopná okamžitého nasazení do praktického užití. Z celkového hlediska bych náplň a podstatu této práce zhodnotil velice kladně. Jedná se kompaktní celek, vhodný pro praktické užití v oblasti správy sítě s širokou škálou možných rozšíření a vylepšení.

Literatura

[1] *Wikipedie* [online]. 2001- 2008. [cit.2007-12-28].
Dostupný z WWW: <http://en.wikipedia.org/wiki/>.

[2] ACHOUR, Mehdi. *PHP manual* [online]: 1997- . [cit.2007-12-12].
Dostupný z WWW: <http://php.net/>.

[3] CISCO SYSTEMS Inc. *Cisco IOS NetFlow*. 2003- 2008. [cit.2008-1-8].
Elektronický dokument dostupný na <http://www.cisco.com/go/netflow>.

[4] HAAG, P. *Nfdump*. 2004- . [cit.2007-12-17].
Elektronická dokumentace dostupná na <http://sourceforge.net/projects/nfdump>.

[5] HRUŠKA, Tomáš. *Informační systémy 2006 : Programování serveru (PHP)* [online]. 2007. [cit.2007-12-19].
Dostupný z WWW: <https://www.fit.vutbr.cz/study/courses/WAP/private/opory/>.

[6] HRUŠKA, Tomáš. *Informační systémy 2006 : Programování klienta (Javascript)* [online]. 2007. [cit.2007-12-19].
Dostupný z WWW: <https://www.fit.vutbr.cz/study/courses/WAP/private/opory/>.

[7] JANOVSKÝ, Dušan. *Jak psát web* [online]. 2001. [cit.2007-12-18].
Dostupný z WWW: <http://www.jakpsatweb.cz/>.

[8] ZAJÍC, Petr. *Seriál o PHP* [online]. 2004. [cit.2007-12-18].
Dostupný z WWW: <http://www.linuxsoft.cz/php/>.

[9] *WWW Consortium* [online]. 1991-2008. [cit.2008-1-9].
Dostupný z WWW: <http://www.w3.org/>.

[10] ŽÁDNÍK, Martin. *Síťové aplikace a správa sítí 2007 : NetFlow* [online]. 2007. [cit.2008-1-18].
Dostupný z WWW: <https://wis.fit.vutbr.cz/FIT/st/course-files-st.php/course/ISA-IT/lectures>.

Seznam příloh

Příloha 1. Manuály readme a install obsahující popis instalace i základní funkce a ovládání aplikace.

Příloha 2. Jednoduchý systém nápovědy.

Příloha 3. CD/DVD obsahující zdrojové soubory k portálu i tuto zprávu ve formátu PDF.