

**Využití open source v prostředí Active Directory  
k řízení a monitoringu internetových aktivit**  
Using Open Source Tools in Active Directory Environment  
for Internet Usage Monitoring

Bc. Michal Prorok

---

Diplomová práce  
2013



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

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

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Michal Prorok**  
Osobní číslo: **A11380**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Využití opensource v prostředí Active Directory  
k řízení a monitoringu internetových aktivit**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Objasněte problematiku využití Internetu na pracovišti z pohledu přínosů, bezpečnostních rizik a legislativy.
3. Nainstalujte Vámi vybranou distribuci Linuxu. Integrujte ji do doménového prostředí Windows Server, zkonfigurujte server tak, aby zajišťoval autentizaci a autorizaci s využitím služeb Kerberos a LDAP systémem Single Sign-On.
4. Publikujte výstupy z proxy serveru s pomocí opensource aplikací s návazností na Active Directory.
5. Navrhněte možnosti pro další rozvoj popsaného řešení.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. SMITH, Roderick W. Linux ve světě Windows: průvodce administrátora heterogenních sítí. 1. vyd. Praha: Grada, 2006, 443 s. ISBN 80-247-1470-1.
2. EISENKOLB, Kerstin. Bezpečnost Windows 2000/XP. 1. vyd. Praha: Computer Press, 2003, 501 s. ISBN 80-7226-789-2.
3. HONTANÓN, Ramón J. Linux: praktická bezpečnost. 1. vyd. Praha: Grada, 2003, 438 s. ISBN 80-247-0652-0.
4. SAINI, Kulbir. Squid Proxy Server 3.1: beginners guide. Birmingham (United Kingdom): Packt Open Source Pub., c2011, 308 p. ISBN 978-1-849513-90-6.
5. WESSELS, Duane. Squid: the definitive guide. 1st ed. Sebastopol (California): OReilly, c2004, 441 p. ISBN 978-0-596-10364-4.
6. DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2. přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.
7. AULDS, Charles. Linux: administrace serveru Apache. 1. vyd. Praha: Grada, 2003, 535 s. ISBN 80-247-0640-7.
8. WELSH, Matt. Používáme Linux. 2. vyd. Praha: Computer Press, 1997, 612 s. ISBN 80-7226-001-4.

Vedoucí diplomové práce:

**Ing. Miroslav Matýsek, Ph.D.**

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

**8. února 2013**

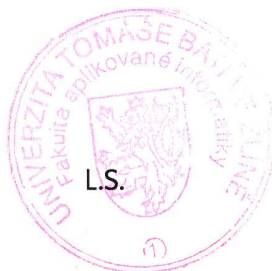
Termín odevzdání diplomové práce:

**3. června 2013**

Ve Zlíně dne 8. února 2013

prof. Ing. Vladimír Vašek, CSc.

*děkan*



doc. RNDr. Vojtěch Křesálek, CSc.

*ředitel ústavu*

## ABSTRAKT

Práce je zaměřena na problematiku monitoringu a řízení přístupu zaměstnanců k Internetu využitím heterogenního řešení v doménovém prostředí s Active Directory. Důraz je kladen na efektivitu správy a informační bezpečnost.

V práci jsou analyzovány přínosy a rizika využití Internetu v organizaci. S přihlédnutím k bezpečnostní politice a platné legislativě jsou formulovány principy, které zajistí účinné, etické a transparentní ošetření internetového provozu v pracovněprávních vztazích. Na jejich základě jsou definovány požadavky na aplikaci, která zajistí řízení a monitoring internetových aktivit. Je navrženo otevřené řešení na linuxové bázi. Použité softwarové komponenty jsou podrobně charakterizovány a je popsána jejich konfigurace. Prostor je věnován také popisu pravidel pro řízení přístupu, výstupům a možnosti zálohování celého řešení z prostředí Microsoft Windows. Jsou zhodnoceny přínosy a úskalí heterogenního řešení v porovnání s komerčními produkty a nastíněny možné oblasti rozvoje řešení.

Klíčová slova:

bezpečnost, proxy, řízení, monitoring, Internet, open source, Linux, Active Directory

## ABSTRACT

The thesis focuses on the problems of monitoring and employee Internet access management using heterogenous solutions in the Active Directory domain environment. Emphasis is being put upon management efficiency and information security.

The author analyses the benefits and risks of using the Internet inside an organization. With respect to security policy and actual legislature, principles are conceived which ensure an effective, ethical and transparent solution to using the Internet within labour-law relations. Based upon these principles, the author presents requirements for an application which provides Internet actions management and monitoring, suggesting a Linux-based open solution. The administered software components and their configuration are described in detail. Moreover, the author sees into the description of rules for access management, outputs and the possibility to backup the whole solution within Microsoft Windows environment. Furthermore, the benefits and disadvantages of such heterogenous solution are assessed as compared to commercial products of similar nature, and the solution's possible fields of development are outlined.

Keywords:

Security, proxy, management, monitoring, Internet, open source, Linux, Active Directory

*„Vyhne se nebezpečí, kdo se má na pozoru, i když je v bezpečí.“*

Publilius Syrus

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>11</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>12</b>
<b>1 ŘÍZENÍ PŘÍSTUPU UŽIVATELŮ K INTERNETU</b> .....	<b>13</b>
1.1 VYUŽITÍ INTERNETU V ORGANIZACI.....	13
1.2 RIZIKA PŘÍSTUPU ZAMĚSTNANCŮ K INTERNETU.....	14
1.3 LEGISLATIVNÍ RÁMEC MONITOROVÁNÍ AKTIVIT ZAMĚSTNANCŮ PROSTŘEDNICTVÍM TELEKOMUNIKAČNÍ TECHNIKY .....	16
1.4 ROLE BEZPEČNOSTNÍ POLITIKY .....	19
<b>II PRAKTICKÁ ČÁST</b> .....	<b>21</b>
<b>2 VÝBĚR SOFTWAREVÉ PLATFORMY</b> .....	<b>22</b>
2.1 PROXY SERVER.....	22
2.1.1 Typy proxy serverů.....	24
2.2 POŽADAVKY NA ŘEŠENÍ.....	25
2.3 NÁKLADY NA KOMERČNÍ ŘEŠENÍ.....	26
2.4 MOŽNOSTI OTEVŘENÉHO SOFTWARE.....	26
2.5 VÝBĚR VHODNÉHO OTEVŘENÉHO ŘEŠENÍ .....	27
2.5.1 Linuxová distribuce pro server.....	28
2.5.2 Výběr proxy serveru .....	29
2.5.3 Systémové požadavky .....	30
<b>3 ZÁKLADNÍ INSTALACE</b> .....	<b>31</b>
3.1 INSTALACE SERVERU .....	31
3.2 NASTAVENÍ SÍŤOVÉ KONFIGURACE .....	32
3.3 NASTAVENÍ DNS RESOLVERŮ .....	32
3.4 VYTVOŘENÍ DNS ZÁZNAMU.....	33
3.5 INSTALACE SSH SERVERU .....	34
3.6 INSTALACE VMWARE TOOLS .....	34
3.7 INSTALACE NETWORK TIME PROTOCOL .....	35
3.7.1 Konfigurace NTP .....	35
<b>4 PŘIPOJENÍ LINUXU K DOMÉNOVÉ STRUKTUŘE ACTIVE     DIRECTORY</b> .....	<b>37</b>
4.1 SAMBA .....	37
4.1.1 Instalace Samby.....	38
4.1.2 Konfigurace Samby.....	38
4.1.3 Úprava host souboru.....	42
4.2 KERBEROS.....	42
4.2.1 Instalace Kerberos .....	46

4.2.2	Konfigurace Kerberos .....	46
4.3	VLOŽENÍ STANICE DO DOMÉNY .....	49
4.4	OTESTOVÁNÍ KERBERA A VYTVOŘENÍ KEYTAB SOUBORU.....	49
4.5	KONFIGURACE NSS.....	50
4.6	KONFIGURACE PAM .....	51
4.6.1	Konfigurace common-account .....	53
4.6.2	Konfigurace common-auth.....	53
4.6.3	Konfigurace common-password.....	54
4.6.4	Konfigurace common-session .....	54
4.6.5	Konfigurace sudo .....	54
4.7	KONFIGURACE SUDOERS.....	55
4.8	TESTOVÁNÍ PROSTŘEDÍ.....	56
4.9	SQUID.....	57
4.9.1	Instalace Squid .....	57
4.9.2	Konfigurace Squid.....	57
<b>5</b>	<b>VÝSTUPY .....</b>	<b>64</b>
5.1	LOGY.....	64
5.2	ÚPRAVA ROTACE LOGŮ .....	65
5.3	INSTALACE LIGHTSQUID.....	66
5.3.1	Konfigurace LightSquid .....	68
5.3.2	Časování spouštění LightSquid.....	68
5.4	INSTALACE SQSTAT.....	69
5.5	INSTALACE APACHE2 .....	70
5.6	PŘÍPRAVA INDEXOVÉHO SOUBORU WEBU .....	71
5.7	KONFIGURACE APACHE.....	71
5.8	PRINCIP OVĚŘENÍ NA SERVERECH APACHE A SQUID Z WEBOVÉHO PROHLÍZEČE.....	75
5.9	ZÁLOHOVÁNÍ SYSTÉMU .....	78
5.9.1	Zálohování konfigurace.....	78
5.9.2	Sdílení adresářů přes Sambu pro použití nástrojů OS Microsoft Windows .....	79
5.10	MOŽNOSTI DALŠÍHO ROZVOJE ŘEŠENÍ.....	79
5.10.1	Antivirová ochrana.....	80
5.10.2	SquidGuard .....	80
5.10.3	Webmin .....	81
5.10.4	NTOP .....	81
5.10.5	Firewall.....	82
	<b>ZÁVĚR .....</b>	<b>83</b>
	<b>CONCLUSION .....</b>	<b>85</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>87</b>

<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>	<b>94</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>98</b>
<b>SEZNAM TABULEK.....</b>	<b>99</b>
<b>SEZNAM PŘÍLOH.....</b>	<b>100</b>

## ÚVOD

Předmětem obchodování moderních firem už nejsou jen výrobky, ale také informace. Informace se staly vzácnou esencí, která má určující vliv na zdraví a prosperitu firem a organizací. To je důvod, proč se ochraně firemních informací začíná věnovat zvýšená pozornost. V této oblasti existuje pestrá paleta dobře definovaných hrozeb. Proti některým z nich se lze snadno a efektivně chránit důsledným zálohováním či použitím prvků na ochranu síťové infrastruktury. Horší je to však s ochranou před riziky interními – nebezpečí postoupení citlivých informací nespokojenými zaměstnanci, možnost využití lidské slabosti a důvěřivosti. Obtížně řešitelný problém v době, kdy ekonomická krize nutí firmy hledat úspory a současně vyvíjet rostoucí tlak na efektivitu lidských zdrojů.

Internet se stal nedílnou součástí všech podnikatelských aktivit. Firmy i organizace musí při budování pravidel informační bezpečnosti věnovat zvýšenou pozornost internetovým aktivitám uživatelů. Ze statistik vyplývá, že brouzdání po Internetu a stahování souborů ohrožuje podnikové sítě nejen virovou nákazou, ale také možností úniku citlivých firemních informací. Nežádoucím průvodním jevem je rovněž snížená produktivita práce zaměstnanců, kteří na Internetu tráví více času, než je nezbytně nutné.

Nejznazší cestou k získání přehledu o aktivitách zaměstnanců je vymezení pravidel pro přístup k Internetu a kontinuální sběr dat o internetovém provozu. Na trhu je dostupná řada komerčních nástrojů, které nabízí komplexní řízení přístupu k Internetu, umožňují aplikovat restriktce, monitorovat a vyhodnocovat činnost uživatelů.

V praxi však bezpečnost vzniká jako kompromis mezi tím, co firma chce a co si může dovolit. Je proto vhodné hledat cesty, které pomohou zajistit požadovanou úroveň bezpečnosti bez nutnosti velkých finančních investic.

## **I. TEORETICKÁ ČÁST**

## 1 ŘÍZENÍ PŘÍSTUPU UŽIVATELŮ K INTERNETU

Internet je dnes platformou pro podnikání, silným komunikačním nástrojem umožňujícím spolupráci organizačních složek geograficky rozsáhlých organizací a prostorem pro získávání příležitostí. Jeho využití však přináší četná rizika. Ve firemním prostředí se proto vytváří systém síťových politik vymezujících práva a povinnosti uživatelů počítačové sítě.

Síťové politiky jsou nástrojem, který snižuje riziko poškození know-how – klíčového aktiva každé organizace. Zaměstnanci mohou vědomě či nevědomě porušovat firemní síťovou politiku a ohrožovat fungování firmy. Proto organizace věnují zvýšenou pozornost ochraně firemní infrastruktury a implementaci nástrojů, kterými mohou chování uživatelů účinně kontrolovat a řídit.

Uživatelé na firemních počítačích často prohlízejí a stahují věci, které nesouvisí s náplní jejich pracovního zařazení. Mohou vlastní aktivitou porušit zákon (nelegální sdílení dat, porušování licencí), zavléct do firmy malware (aplikace určené k vniknutí nebo poškození hostitelského počítačového systému) nebo vynést citlivé údaje [1]. Sdílení dat může v extrémním případě skončit zabavením dostupné techniky pro potřeby vyšetřování, což pro firmu znamená rychlý konec.

### 1.1 Využití internetu v organizaci

Problematice chování zaměstnanců z pohledu využití informačních technologií je věnována řada studií. Z dostupných zdrojů jsou uvedeny ty, jejichž zaměření není striktně marketingové.

Jedním ze zdrojů je rozsáhlá studie firmy Cisco Systems, Inc. zvaná Cisco Connected World Technology Report. Tento dokument obsahuje dvě části. První, věnovanou výzkumu na univerzitních studentech a druhou, zaměřenou na profesionály z praxe mladší 30 let. Celkem bylo dotazováno 1400 respondentů ze 14 zemí světa. Studie ukazuje, že *„Touha po přístupu k informacím je tak hluboce zakořeněna v nastupující generaci zaměstnanců, že mnozí z nich udělají vše pro přístup k Internetu, i když to ohrožuje firemní nebo jejich vlastní bezpečnost“* [2]. Alarmující je také závěr, že 70 % zaměstnanců, kteří jsou obeznámeni s bezpečnostními pravidly, připustilo jejich občasné vědomé porušení. Metodika studie a výsledky jsou publikovány na stránkách společnosti Cisco Systems, Inc. [3].

Zajímavým závěrem práce je fakt, že více než polovina studentů by nepřijala práci bez svobodného přístupu k Internetu a pokud by ji přijala, hledala by cestu, jak toto nařízení obejít. Přístup k Internetu je pro studenty jedním z hledisek ovlivňujících výběr zaměstnání. Má dopad na jejich spokojenost i efektivitu práce. Pro necelou třetinu zaměstnanců jsou podmínky využívání informačních technologií kritériem nástupu na současnou pozici.

Psychologickým aspektům vlivu Internetu na pracovní výkon zaměstnanců se věnují také některé české akademické práce. Z jejich závěrů plyne, že při využití Internetu jako krátké formy aktivního odpočinku během pracovního procesu dochází ke zvýšení efektivitu práce u sledovaných zaměstnanců o 9 %. Autorka práce Psychologické aspekty zneužívání Internetu na pracovišti přišla k závěru, že důvěra a autonomie vlastním zaměstnancům zvyšuje jejich loajalitu a spokojenost. Ze závěrů plyne, že Internet nejčastěji zneužívají zaměstnanci, kteří svoji práci vnímají jako rutinní a nudnou [4].

V práci Monitoring a kontrola zaměstnanců na pracovišti z hlediska etiky zase autorka vyvodila, že otázka kontroly a monitoringu zaměstnanců je velmi citlivé téma. Pro vztah zaměstnavatele a zaměstnance je podle ní klíčová transparentnost nastavených pravidel a kontrolních mechanismů, především ze strany zaměstnavatele. Jen takové jednání lze označit jako etické [5].

## 1.2 Rizika přístupu zaměstnanců k Internetu

Zcela proti výše uvedeným názorovým proudům stojí výzkum společnosti Morse. Jeho autoři se snažili vyčíslit náklady, které zaměstnavatele stojí „internetová pohoda“ zaměstnanců. Výzkum provedený na vzorku 1460 administrativních pracovníků ukázal, že používání Twitteru a dalších sociálních sítí stojí britské firmy značné finanční prostředky. Dotazovaní zaměstnanci odpovídali, že v průměru tráví na sociálních sítích 40 minut týdně. Jejich kolegové však potvrdili, že dotazovaní spolupracovníci tráví na sociálních sítích až hodinu denně. I když byla pro účely studie použita hodnota sdělená respondenty (tj. 40 minut týdně), vyčíslili autoři výzkumu škody na 1,38 miliardy liber [6].

Učinit podobný výpočet pro ČR (Českou republiku) je velmi snadné. Průměrná mzda zaměstnance dosahovala v prvním čtvrtletí 2012 výše 24 126 Kč [7]. Tato hodnota představuje pro zaměstnavatele náklady ve výši 32 330,- Kč [8] na jednoho zaměstnance.

Pokud budeme počítat s osmihodinovou pracovní směnou a průměrnou hodnotou 21 pracovních dní za měsíc, tj. 252 pracovních dní za rok, jednoduše vyčíslíme náklady na internetové kratochvíle uživatele (viz Tab. 1).

Tab. 1. Náklady zaměstnavatele na nepracovní internetové aktivity zaměstnanců.

	<b>Náklady na internetovou aktivitu zaměstnance na internetu při 5 minutách prohlížení za hodinu</b>		
	<b>Denně</b>	<b>Měsíčně</b>	<b>Ročně</b>
<b>Prům. mzda zaměstnance (24 126,- Kč)</b>	96 Kč	2 011 Kč	24 126 Kč
<b>Náklady pro zaměstnavatele (32 330,- Kč)</b>	128 Kč	2 694 Kč	32 330 Kč

Kromě zvýšených nákladů pro zaměstnavatele generuje neřízený přístup na Internet bezpečnostní riziko. Zaměstnanec může snadno vystavit na Internet citlivé dokumenty, předat je elektronickou cestou konkurenci apod. Těmto aktivitám lze zamezit pouze úplným odepřením přístupu na Internet nebo omezením přístupu na explicitně definovaný seznam stránek (i v tomto případě však hrozí ve spolupráci s webmasterem únik dat). Nekontrolovaný přístup na Internet je rizikem také v prostorách, kde dochází k pohybu osob, u kterých není přístup k Internetu žádoucí (např. věznice).

Způsob práce lidí se za poslední desetiletí velmi změnil. Většina administrativních aktivit je zpracovávána na počítači. Proto je třeba síťový provoz a aktivity uživatelů monitorovat. Neproduktivní zaměstnanec, který většinu pracovní doby stráví prohlížením internetových stránek, ubírá motivaci ostatním zaměstnancům. Nežádoucí chování se firmou rychle šíří a ztráty z nečinnosti rostou.

Tisková zpráva American Management Association (AMA) z roku 2007 hovoří o tom, že polovina zaměstnavatelů je schopna dát zaměstnancům výpověď na základě porušení firemních pravidel pro využívání Internetu a e-mailu. Výzkum byl proveden ve spolupráci s organizací The ePolicy Institute ve 304 firmách se 100 a více zaměstnanci [9]. Z výsledků plyne, že zaměstnavatelé, v zájmu zvýšení produktivity, zabezpečení a minimalizace rizika, stále častěji kombinují technologii s firemní politikou. Čtvrtina zaměstnavatelů je schopna rozvázat se zaměstnancem pracovní poměr na základě problémů s využitím elektronické pošty a pro téměř dvě třetiny zaměstnavatelů je porušení pravidel chování na Internetu

důvodem k výpovědi zaměstnance. Nejčastější pochybení, která vedou k rozvázání pracovního poměru jsou v Tab. 2.

Tab. 2. Internetové aktivity, které vedou k rozvázání pracovního poměru [9].

Důvody rozvázání pracovního poměru u zaměstnanců vlivem uživatelské aktivity na Internetu	Zastoupení
Prohlížení, stahování stránek s nevhodným/urážlivým obsahem	84 %
Porušení firemní politiky	48 %
Nadměrné osobní použití	34 %
Jiné důvody	9 %

Podle výzkumu používá 65 % firem software pro blokování připojení k nevhodným webům. V porovnání s rokem 2001 se jedná o 27% nárůst využití tohoto druhu softwaru. Nejčastěji se blokují stránky pro dospělé (96 %), herní servery (61 %), sociální sítě (50 %), zábavní místa (40 %), nákupní a aukční stránky (27 %) a sportovní stránky (21 %).

Firemní data mají tři atributy, jejichž ochranu je nutno zabezpečit [10]:

- **Riziko ohrožení utajení**

Riziko, že k datům společnosti získá přístup neoprávněný subjekt, případně dojde k předčasnému uveřejnění dat, díky čemuž může společnost přijít o značné finanční prostředky.

- **Riziko ohrožení integrity dat**

Toto bezpečnostní riziko zahrnuje riziko napadení databáze dat. Dotýká se internetových aktivit uživatelů pouze okrajově.

- **Riziko ohrožení dostupnosti**

Nedostupné služby znamenají ztráty a snížení produktivity zaměstnanců. Mohou eskalovat až v nedůvěru zákazníků.

### 1.3 Legislativní rámec monitorování aktivit zaměstnanců prostřednictvím telekomunikační techniky

Pracovněprávní předpisy otázku ochrany soukromí zaměstnance, příp. ochranu osobnostních práv zaměstnance v podstatě neřeší. Zákoník práce zaměstnavateli pouze

stanoví povinnost rovného zacházení se všemi zaměstnanci, proto je třeba použít úpravu z jiných zákonů – především občanského zákoníku, který upravuje ochranu osobnosti [11]. Zákon říká: „Každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí.“ (§ 3) a „Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy“ (§ 81) [12].

Soukromí definuje Úřad pro ochranu osobních údajů takto [13]:

*„Pojem soukromí není v českém právu přímo definován. Soukromí můžeme stručně popsat jako osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora. Pojem soukromí obsahuje rovněž hmotný i myšlenkový prostor jednotlivce. Součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.“*

Problematiku monitorování aktivit zaměstnanců ošetřuje zákoník práce v 13. části, hlavě VIII. Tato část je věnovaná ochraně majetkových zájmů zaměstnavatele a ochraně osobních práv zaměstnance. V § 316 tohoto zákona jsou upraveny možnosti preventivně výchovného působení na zaměstnance [14]:

*„(1) Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*

*(2) Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.*

*(3) Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.“*

V komentáři v systému ASPI (Automatizovaný systém prvních informací) je k tomuto paragrafu uvedeno, že naplňování ustanovení § 316 odst. 1 je vhodné ošetřit vnitřním

předpisem, případně sjednat v kolektivní smlouvě. Zaměstnavatel je oprávněn dodržování této povinnosti kontrolovat. Kontrola je však možná jen na základě předchozího oznámení a pouze tam, kde je to nezbytně nutné. Obsah kontroly musí mít jasný a konkrétní cíl.

Problémem je vymezení „přiměřeného způsobu“ kontroly. Na citlivost této problematiky ukazují medializované případy sledování počítačových aktivit zaměstnanců [15] a intervence Rady vlády pro lidská práva [16]. Monitorování pracoviště, např. kamerou nebo použitím keyloggeru, je možné pouze ve výjimečných případech (banky, herny atd.). Odvíjí se od toho, zda jde o specifického zaměstnavatele, nebo zaměstnavatele běžného, který sledování činnosti zaměstnance odůvodňuje pouze tím, že chce mít přehled, co zaměstnanci v pracovní době dělají.

Dle prostudovaných právních výkladů [17], [18] se obvykle za přiměřené pokládá právo kontrolovat:

- dobu strávenou na Internetu a místa pohybu,
- činnost na počítači (např. hraní her),
- obsah paměti svěřeného počítače a externích nosičů dat,
- obsah firemní emailové schránky.

Do nepřiměřeného sledování spadá např. sledování obsahu chatu na ICQ (I Seek You) či Skype.

K výkladu § 316 zákoníku práce uvádí JUDr. Lukáš Jansa toto [18]:

*„O běžném monitoringu přístupu na net a práce s počítačem dle mého názoru zaměstnavatel informovat nemusí. O kontrole pošty doručené na zaměstnancův firemní email ovšem informovat musí. Nicméně bych doporučil, aby firma informovala všechny zaměstnance i o běžném monitorování přístupu, a to z toho důvodu, že zaměstnanci v obavě před touto kontrolou a následky nebudou trávit svou pracovní dobu soukromými aktivitami na Internetu či hraním her. Nicméně zase je třeba z lidského pohledu pochopit, že zaměstnanec (pokud má k dispozici Internet) by měl mít určitou možnost tohoto přístupu, za předpokladu že své pracovní úkoly plní řádně a včas.“*

Pokud by zaměstnavatel překročil mez přiměřenosti kontroly, může se zaměstnanec domáhat dle § 265 zákoníku práce náhrady škody. Při porušení pracovněprávních předpisů hrozí zaměstnavateli uložení pokuty Oblastním inspektorátem práce.

Informace o použití nástrojů monitoringu práce vedou u zaměstnanců k dojmu, že je management sleduje na každém kroku. Tento pocit je však neopodstatněný. Nástroje musí být určeny k monitorování činností a nesmí zasahovat do soukromí uživatele. Výstupem je výčet aktivit s časovým a datovým průběhem. Zpracovávaný obsah však není obsahem kontroly. Softwarové řešení monitoringu internetových aktivit zaměstnanců je mocným nástrojem managementu, který brání nezodpovědnému chování zaměstnanců, identifikuje problémové pracovníky a pomáhá zvýšit jejich efektivitu.

Je zřejmé, že i když Internet hraje v životě lidí a zaměstnanců firem důležitou roli, jeho nadužívání vnímají zaměstnavatelé jako poškozující faktor, který může vést k rozvázání pracovního poměru. Mantinely pravidel a míra tolerance nepracovních aktivit by měly být od začátku známé oběma stranám a být v souladu s pracovněprávní agendou firmy a platnou legislativou.

#### **1.4 Role bezpečnostní politiky**

Krokem, který by měl předcházet úvahám o řešení, je celkové zhodnocení situace a definice požadavků a záměrů realizovat určitá opatření. Bezpečnostní politika by měla vycházet z vedení organizace a měla by vznikat ve spolupráci s pracovníky a uživateli počítačové sítě. Výsledkem musí být posouzení zranitelností, hrozeb a rizik a definice standardů, kterých se chce organizace v této oblasti držet. Rozvaha se musí týkat také nákladů na pořizované zabezpečení. V praxi se vždy jedná o kompromis mezi tím, co organizace chce a co si může dovolit.

Každá organizace by měla mít definovanou bezpečnostní politiku jako základní dokument, který stanovuje požadavky a standardy v oblasti bezpečnosti. Vyústěním komplexní rozvahy je rozšíření provozní bezpečnostní politiky o aspekty týkající se přístupu uživatelů k Internetu. Důležité je, aby si lidé nejprve vše pečlivě promysleli, došli k určitému konsensu, získali pro tento konsensus podporu a vše řádně zdokumentovali [19].

Z předchozího textu je zřejmé, že činnost zaměstnanců ve firmě je třeba kontrolovat, a to jak z bezpečnostního hlediska, tak z pohledu efektivy práce a hospodárneho využívání svěřených zdrojů. Kontrola počítačových a internetových aktivit není porušením požadavku přiměřenosti kontroly, neboť předmětem sběru nejsou osobní data. „*Na tuto*

*kontrolu nemusí být zaměstnanec předem upozorněn, jelikož tyto způsoby kontroly nejsou uvedeny ve výčtu § 316 odst. 2 zákoníku práce“ [18].*

Seznámení zaměstnanců s pravidly musí být prokazatelné, aby mohlo být použito jako důkazní materiál v případném soudním sporu se zaměstnancem. V případě sporu je softwarové řešení jediným zdrojem důkazů o porušování podepsaných smluv.

Pokud jsou nastavená pravidla a použité mechanismy transparentní a v rozsahu zákona, je sledování internetových aktivit zaměstnanců přijatelné jak z etického tak legislativního hlediska. Oblast řízení komunikací je řešena v rámci provozní bezpečnosti také v normě ISO 27 002 (International Organization for Standardization) [20]. Pravidla používání Internetu musí být zakotvena jako nedílná součást podnikové bezpečnosti každé moderní firmy.

## **II. PRAKTICKÁ ČÁST**

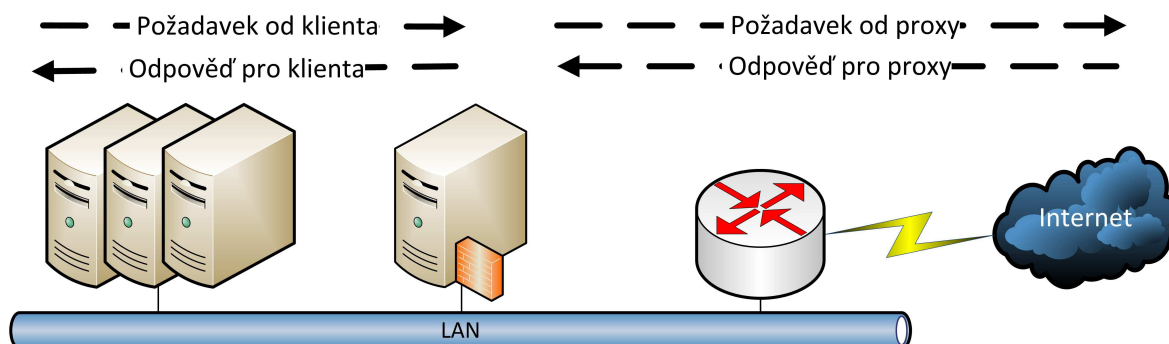
## 2 VÝBĚR SOFTWAREVÉ PLATFORMY

Prvním krokem každého řešení je analýza. V této fázi je nutné specifikovat, co od softwarového řešení očekáváme. Zohledňujeme požadavky na řešení, finanční stránku a celkové možnosti softwaru. Zkušenosti z praxe ukazují, že je vhodné použít co nejflexibilnější řešení, neboť řada požadavků se objeví až následně za provozu.

### 2.1 Proxy server

Nejběžnějším a nejrozšířenějším způsobem kontroly přístupu uživatelů k Internetu je využití proxy serveru. Proxy server, neboli aplikační brána, je přechodový bod, který se postaví mezi uživatele a internetovou sítí. Klienti posílají žádost o přístup ke konkrétní adrese proxy serveru. Ten může provádět rozšířené ověřování, autorizaci a rozsáhlé protokolování informací [10].

Server zjistí, zda má uživatel na požadovanou akci právo, připojí se ke vzdálenému serveru, získá od něj požadovaná data a předá je zpět uživateli. Při tom je schopen zajistit autorizaci a zprostředkovat uživateli požadovaný obsah podle nastavených pravidel, nebo odepřít přístup. Princip fungování proxy serveru ilustruje Obr. 1.



Obr. 1. Princip fungování proxy serveru.

Proxy server bývá též někdy nazýván brána aplikace (application-level gateway), protože funguje jako uzel na aplikační úrovni. Server činí rozhodnutí o přístupu na základě informací obsažených uvnitř paketu - ve všech sedmi vrstvách modelu OSI (Open Systems Interconnection). Poskytuje vyšší úroveň zabezpečení než paketový filtr na firewallu. Činí tak ovšem na úkor transparentnosti. Proxy server je tedy aplikační mezivrstva, která slouží

jako prostředník mezi klientem a cílovým serverem. Vynucenou komunikací přes proxy server je umožněno [19]:

- **Sdílení přístupu k Internetu**

Nahrazení funkce klasického směrovače a sdílení internetové konektivity s využitím proxy serveru.

- **Optimalizování připojení**

Využití proxy serveru může napomáhat efektivnějšímu využití internetové přípojky ve spojení s funkcí cache serveru – viz bod Cacheování. S rostoucí rychlostí internetových přípojek ztrácí tato vlastnost na významu.

- **Filtrování**

Regulace přístupu uživatelů na konkrétní servery a k určitému typu obsahu.

- **Žurnálování**

Evidence přístupů.

- **Řešení problému s IP (Internet Protocol) adresami**

Možnost použití neunikátních IP adres za proxy serverem.

- **Cacheování**

Obsah je z vnějších zdrojů stahován pouze při prvním požadavku. Při opakovaných požadavcích poskytne server lokální kopii zdroje.

S přechodem webu na dynamické stránky ztrácí tato funkce význam, neboť server neví, jak dlouho může uchovat uloženou stránku.

- **Zajištění vyšší bezpečnosti**

Proxy server maskuje identitu klienta. V případě potřeby je možné provést antivirovou kontrolu prohlíženého obsahu dříve, než bude doručen uživateli.

Z uživatelského hlediska vystupuje proxy server jako server, z pohledu serveru, hostujícího požadovaný zdroj, jde však o klienta. Dnes se proxy servery se používají zejména v případech, kdy je vyžadováno filtrování URL (Uniform Resource Locator), antivirová kontrola nebo protokolování přístupů. Protože stanici v LAN (Local Area Network) stačí znát pouze jméno či adresu proxy serveru, je vnitřní síť zcela oddělena od Internetu.

Použití proxy serveru přináší i některá negativa [10]:

- **Nižší výkon**

Každý požadavek uživatele představuje ve skutečnosti dvě samostatná připojení. Jedno mezi uživatelem a bránou, druhé mezi bránou a cílovým hostitelem.

Pro vyřízení požadavku je tedy nutný dvojnásobný počet připojení proti situaci, kdy je použit pouze paketový filtr. Kontrola aplikační mezivrstvy potřebuje více času na zpracování. Aplikace využívající velkou šířku pásma, mohou mít s reakční dobou proxy serveru problémy.

- **Nedostatečnou transparentnost**

Aplikace proxy serveru vyžaduje podporu na straně klienta (na úrovni aplikace).

- **Nutnost použít samostatný proxy server pro každou aplikaci**

Na konkrétní službu je nutné použít server, který danou funkci podporuje.

- **Omezení znalosti aplikací**

Brána musí být schopná rozlišit rozdíl mezi bezpečnými a nebezpečnými funkcemi aplikace. Není-li server schopen rozlišení zajistit, je jeho použitelnost omezena.

### 2.1.1 Typy proxy serverů

Podle způsobu použití můžeme rozlišovat tyto typy serverů:

- **HTTP (Hypertext Transfer Protocol) proxy**

Díky expanzi Internetu je v dnešní době nejrozšířenější.

- **SOCKS (Socket Secure) proxy**

Proxy s rozšířenou funkcionalitou pro libovolné TCP (Transmission Control Protocol) a UDP (User Datagram Protocol) služby. Je nutné, aby aplikace připojení přes SOCKS proxy podporovala.

- **Reverzní proxy**

Funguje na opačném principu než předešlé dva typy. Cílem je rozdělovat požadavky přicházející z Internetu na několik serverů, např. pro účely rozdělování zátěže.

- **Transparentní proxy**

Klient adresuje přímo cílový server. Transparentní proxy akceptuje spojení na cílový server. Z hlediska klienta se transparentní proxy server jeví jako router.

## 2.2 Požadavky na řešení

Před nasazením aplikace je nutné definovat funkce, které má proxy server v počítačové síti zajišťovat. Předpokladem je, že stanice v síti jsou zabezpečeny antivirovou ochranou a není proto nutné řešit tuto funkci v rámci proxy serveru (v případě potřeby je možné řešit volitelně – viz 5.10.1). Rovněž se předpokládá, že proxy server nemusí plnit roli firewallu.

Řešení musí mít tyto vlastnosti:

- nízké pořizovací a provozní náklady,
- plnou vazbu na AD (Active Directory) - z pohledu budování bezpečnosti v organizaci je vhodné respektovat centrální adresářovou strukturu organizace (řízení přístupu uživatelů k Internetu na základě členství v AD skupinách, přístup ke statistikám, zobrazení aktuálního provozu a možnost administrace proxy serveru členům konkrétních AD skupin),
- Single Sign On, tj. přístup k Internetu bez dvojího ověření,
- podporu ověření uživatele na proxy z nejrozšířenějších internetových prohlížečů,
- filtrování prohlíženého obsahu,
- možnost garance přístupu k určitým stránkám všem uživatelům,
- žurnálování přístupu dle požadavků bezpečnostní politiky organizace,
- přehlednou statistiku přístupů,

- možnost jednoduchého zálohování konfigurace z prostředí OS (operačního systému) Microsoft Windows,
- možnost běhu serveru v prostředí 64-bitového VMware ESX,
- podporu předávání požadavků na nadřazený proxy server,
- flexibilitu s možností úpravy pravidel dle požadavků poboček,
- správu a editace pravidel přes webový prohlížeč.

### 2.3 Náklady na komerční řešení

Způsoby připojování jednotlivých uživatelů i celých lokálních sítí k Internetu jsou dobře zvládnutou problematikou, na které profituje řada firem. Na trhu je k dispozici množství produktů, které tuto funkcionalitu zajišťují.

Požadavky na řešení definované v části 2.2 splní např. produkt firmy Kerio Technologies, Inc., která se vývoji řešení věnuje déle než 15 let. Letmá kalkulace pořizovacích nákladů produktu Kerio Control je uvedena v Tab. 3.

Tab. 3. Cena komerčního řešení pro organizaci [21].

Popis	Cena
Cena za server včetně 5 uživatelů	5 300,- Kč
Cena za každého dalšího uživatele	520,- Kč

Je zřejmé, že nákup hotového řešení je pro organizace s větším počtem uživatelů a pobočkovou strukturou velmi nákladný. V ceně přitom není zahrnut roční udržovací poplatek, v rámci kterého je možné průběžně používat poslední verzi softwaru.

### 2.4 Možnosti otevřeného softwaru

Při pohledu na pořizovací cenu komerčního řešení v Tab. 3 se jeví jako ekonomicky výhodné použít otevřené řešení. Svět OSS (Open Source Software) bourá striktní politiku komerčních nástrojů a nabízí aplikace bez licenčních poplatků. Řešení je možné libovolně upravovat a konfigurovat. OSS je cestou k získání řešení bez dodatečné funkcionality. V porovnání s komerčními produkty, které nabízí komplexní řešení, se výčet vlastností

OSS může zdát chabý. V modularitě je však skryta velká síla, která dovoluje zajistit stabilní řešení pro konkrétní potřeby bez nutnosti platit za nadstandardní funkce.

Odpůrci OSS často argumentují množstvím chyb, špatnou dokumentací, nejasnou představou o dalším vývoji aplikace. Otevřený softwarový svět je velmi pestrý, je však nutné uvážlivě vybírat osvědčené řešení s dobrou dokumentací. Většina firem produkujících OSS profituje z technické podpory a konzultačních služeb. Otevřené projekty zpravidla stojí na početné komunitě vývojářů a uživatelů, která je výborným zdrojem informací při řešení problémů.

Podle šetření Českého statistického úřadu používalo v lednu 2011 v ČR alespoň jeden typ OSS 70 % firem [22].

## 2.5 Výběr vhodného otevřeného řešení

Protože hledáme OSS, je nutné začít výběrem vhodného operačního systému. Dobrý a stabilní základ řešení nabízí operační systém Linux. Jedná se o výkonný operační systém, který vznikl jako implementace operačního systému UNIX. Součástí Linuxu jsou obsáhlé repozitáře se softwarovou výbavou. Linux je šířen pod licencí GNU (General Public Licence), která zaručuje, že odvozená díla budou dostupná pod stejnou licencí [23].

Při řešení je žádoucí využít v maximální míře vazbu na Active Directory skupiny a centrální adresářovou strukturu. V případě nasazení řešení, např. na pobočkovou síť spravovanou správci proškolenými na prostředí Microsoft Windows, budou pracovníci schopni používat proxy server jako službu. Odpadá problém s odmítáním alternativní platformy v rámci budování heterogenního řešení. Správcům lze připravit sadu Active Directory skupin s popisem aplikovaných pravidel, metodikou pro přidělování uživatelských práv a přístupů ke statistikám. Administrátoři dostanou volnost v rámci pevných pravidel. Vzniklý stav a pravidla provozní bezpečnosti v oblasti Internetu lze jednoduše zdokumentovat a v případě potřeby kdykoliv centrálně zkontrolovat bez ohledu na velikost organizace.

I přes ekonomické výhody otevřeného softwaru, je třeba pamatovat, že budované heterogenní řešení je navázáno na standardy v rámci uzavřeného produktu. Je proto nutné, aby vedení organizace stanovilo jasná pravidla, nezávisle na produktu, který bude jako proxy server využíván.

Jen tak je možné v případě potřeby realizovat operativní přechod na jiný produkt s podporou Active Directory bez nutnosti zásahů do bezpečnostního modelu.

### 2.5.1 Linuxová distribuce pro server

Hledáme-li řešení určené pro podnikovou sféru, je nutné zvolit takovou distribuci, která zajistí stabilní prostředí a podporu. Oblíbenou softwarovou distribucí pro servery je Debian. Distribuci vytvořil v srpnu 1993 Ian Murdock. Debian je svobodný operační systém určený k provozu na mnoha různých typech počítačů. Obsahuje několik tisíc softwarových balíčků s programy a dokumentací. Jedná se o konzervativní distribuci s dobře organizovanou komunitou vývojářů a uživatelů. Vývoj distribuce probíhá ve třech větvích – „Unstable“, „Testing“ a „Stable“. Balíčky postupují z „Unstable“ do větve „Testing“, kde podléhají intenzivnímu testování. Po odstranění chyb dojde k tzv. zmrazení verze a přesunu do větve „Stable“. Poté se větev „Testing“ odmrazí a začne přebírat další balíčky. Stabilní prostředí pro běh serverů v produkčním prostředí vytváří větev „Stable“, která vykazuje zásahy pouze v rámci bezpečnostních oprav. Vývojový cyklus Debianu trvá přibližně dva roky [24].

Dlouhá doba vývoje Debianu se negativně odráží ve slabší podpoře nejnovějšího hardwaru a starších verzích dostupných balíčků. Systém má fungovat v heterogenním prostředí s vazbou na AD a má být schopen běžet v prostředí virtualizačního hypervisoru VMWare ESX, proto se jako výhodnější jeví např. distribuce Ubuntu.

Ubuntu vychází z Debianu. Jednotlivá vydání balíčků však mají před zařazením do stabilní větve kratší testování. Díky tomu nabízí Ubuntu lepší podporu hardwaru, novější software a je mezi koncovými uživateli rozšířenější. Vývojáři Ubuntu a Debianu úzce spolupracují, proto je možné využívat stejný formát pro instalaci balíčků [25].

Distribuce Ubuntu je vydávána také pro servery. V této řadě se nachází vydání s označením „LTS“. LTS (Long Time Support) verze mají garantovaný pětiletý cyklus podpory. Pro potřeby této práce lze použít aktuální LTS Ubuntu ve verzi 12.04, která vyšla v dubnu 2012. Standardní verze proti tomu vychází každých 6 měsíců a mají pouze 18 měsíční podporu. Díky blízkosti systémů Ubuntu a Debian lze instalační postup v této práci s malými rozdíly použít na obě distribuce.

Důležitým kritériem pro výběr distribuce je použitá architektura. V zadání bylo požadováno, aby řešení fungovalo v prostředí 64-bitového hypervisoru VMware ESX. Při využití procesorů AMD (Advanced Micro Devices) je nutné použít serverové instalační médium verze 12.04 určené pro platformu AMD64.

### 2.5.2 Výběr proxy serveru

Na Internetu je k dispozici řada volně dostupných proxy serverů pro různá vývojová prostředí – viz [26]. V repozitářích Ubuntu se nachází tyto HTTP proxy servery:

- **Micro-proxy**

Základní proxy server v C++. Poskytuje omezenou funkcionalitu pro zabezpečení přístupu k Internetu [27].

- **Privoxy**

Nekešující proxy server s pokročilými možnostmi filtrace a úpravy stránek, který je primárně určen pro zajištění soukromí při pohybu na webu [28].

- **Ziproxy**

Proxy server pro komprimaci obsahu [29].

- **Squid3**

Propracovaný proxy server s množstvím funkcí a pokročilými možnostmi filtrování obsahu [30].

Z repozitáře Ubuntu je nejvhodnější aplikací pro podnikové prostředí proxy server Squid. Squid je vysoce výkonný server, který vznikl z projektu Harvest, zaměřeného na vytvoření vyhledávací služby. Jeho první verze vyšla v roce 1996. Díky dlouhému vývoji je dnes nejrozšířenějším linuxovým serverem.

Nabízí celé spektrum funkcí – podporovány jsou protokoly HTTP, FTP (File Transport Protocol), Gopher. Podporuje jak IPv4 tak IPv6, umí ukládat DNS (Domain Name Service) dotazy a nejpoužívanější objekty do paměti RAM (Random Access Memory). Podporuje SSL (Secure Sockets Layer), tvorbu pravidel pro přístup k URL, zajišťuje detailní logování přístupů. Squid je rovněž možné použít jako reverzní proxy. Aplikace se skládá z hlavního

programu a volitelných modulů, které zajišťují autentizaci, řízení a management klientů [31].

Squid je dostupný na platformě BSD (Berkeley Software Distribution), Linux, UNIX, OS2 a Solaris. V prostředí Cygwin je jej možné provozovat na OS Microsoft Windows. Pro tento OS byl naportován Squid verze 2.7. Vývoj dalších verzí pro Microsoft Windows však dlouhodobě stagnuje [32].

### 2.5.3 Systémové požadavky

Díky oddělení role firewallu a vyřazení antiviru (viz 2.2) stačí proxy serveru jedna síťová karta. Proxy serveru je vhodné přidělit statickou IP adresu z rozsahu vyčleněného pro infrastrukturu dle adresního plánu organizace. Pro komunikaci mezi proxy a Internetem je nezbytné na firewallu hraničního prvku sítě povolit minimálně TCP porty 80 a 443.

Díky dostatečné rychlosti linky není nutné, aby server plnil roli cache. Požadavky na diskový prostor tak generuje pouze potřeba ukádaní logů. V praxi se osvědčil diskový prostor o velikosti 40 GB (gigabyte). Tato velikost postačuje pro dlouhodobý provoz na pobočkách s 250 uživateli při tříměsíční rotaci logu.

Pro server je vhodné dedikovat 1 jádro procesoru na strojích s 2x Quad-Core AMD Opteron 2350. Pro běh bez antiviru postačí 512 MB (megabyte) operační paměti. Větší procesorový výkon by Squid potřeboval v případě antivirové kontroly objektů v cache. V tomto případě rostou také nároky na operační paměť. Souhrn konfigurace uvádí Tab. 4.

Tab. 4. Hardwarová konfigurace pro proxy server.

Komponenta	Hodnota
Název serveru	Prvních 5 znaků z názvu pobočky + SQ01
CPU (Central Processor Unit)	1 jádro CPU Opteron 2350
RAM	512 MB
HDD (Hard Disk Drive)	40 GB
LAN	1 adaptér na 100 Mbit/s nebo 1 Gbit/s

## 3 ZÁKLADNÍ INSTALACE

### 3.1 Instalace serveru

Instalace proběhne pomocí standardního instalátoru Ubuntu. Při dialogových dotazech jsou použity níže uvedené vstupy.

#### Konfigurace instalátoru

Language:	English
Location:	Other/Europe/Czech Republic
Locales:	en_US.UTF-8
Keyboard:	English (US)
Hostname:	squidln01
Full name for new user:	SQUID Administrator
Username:	squidadmin
Password:	squid
Encrypt your home directory?	No
Partitioning method:	Guided and set up LVM
Select disk to partition:	SCSI3 (0,0,0) (sda) 42.9 GB
Write the changes to disks and configure LVM?	Yes
Amount of volume group to use for guided partitioning:	42.7 GB
Write the Changes to disks?	Yes
HTTP Proxy:	No
Do you want to manage upgrades on this system?	No automatic updates
Software selection:	Žádný balíček
Install the GRUB boot loader to MBR?	Yes

Bezpečnostní mechanismus distribuce Ubuntu brání běžným uživatelům provádět operace, které by mohly mít negativní dopad na chod a stabilitu systému. Pokud je nutné upravit

konfiguraci na úrovni systémových komponent, je nutné provádět tyto operace pod právy účtu `root`, který je v hierarchii systému Linux nejvyšším účtem. V distribuci Ubuntu je nutné všem příkazům, vyžadujícím zvýšené oprávnění, předřadit příkaz `sudo`. Běžným uživatelům může být oprávnění používat příkaz `sudo` delegováno [33].

Aby v rámci základní instalace nebylo nutné neustále eskalovat bezpečnostní kontext přihlášeného uživatele, je vhodné použít příkaz č. 1. Všechny příkazy v práci jsou prováděny v kontextu účtu `root` a příkaz `sudo` je ze všech příkazů v textu vynechán. Tím je zaručeno, že popsaný postup je možné využít i na jiných linuxových distribucích.

```
1 sudo -s
```

### 3.2 Nastavení síťové konfigurace

Protože je stroj instalován v produkčním prostředí podnikové sítě, dostává při instalaci přidělenou dynamickou IP adresu ze serveru DHCP (Dynamic Host Configuration Protocol). Proxy server poskytuje službu uživatelům. Proto je vhodné vyčlenit serveru statickou

IP adresu dle adresního plánu organizace. Je rovněž nutné povolit na firewallu přístup na nadřazenou proxy či síťovou bránu, přes kterou bude server komunikovat s Internetem.

Nastavení statické adresy je možné provést úpravou konfiguračního souboru `/etc/network/interfaces`. Je nutné nastavit statickou IP adresu (příkaz č. 6 a 7), síťovou masku (příkaz č. 8) a bránu (příkaz č. 9).

```
2 auto lo
3 iface lo inet loopback
4 # The primary network interface
5 auto eth0
6 iface eth0 inet static
7 address IP_Adresa_Serveru
8 netmask Sitova_Maska
9 gateway IP_Adresa_Brany
```

### 3.3 Nastavení DNS resolverů

Dalším krokem je nastavení DNS serverů, které bude proxy server používat pro překlad jmen. Při základní instalaci byl do systému instalován balíček `resolvconf`. Jelikož není nutné měnit nastavení DNS, je vhodné tento balíček odinstalovat příkazem č. 10.

```
10 apt-get remove resolvconf
```

Dále je nutné zeditovat soubor `/etc/resolv.conf` do tohoto tvaru.

```
11 nameserver IP_Adresa_DNS1
```

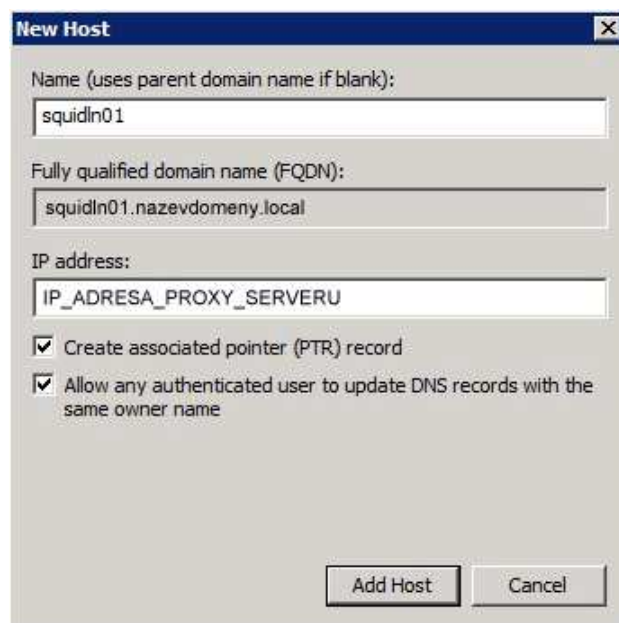
```
12 nameserver IP_Adresa_DNS2
```

```
13 search Nazev_Domeny.local
```

V řádcích č. 11 a 12 stačí vložit IP adresy DNS serverů v síti. Příkaz `search` v řádku 13 určuje seznam domén, které jsou prohledávány pro libovolné hostitelské jméno.

### 3.4 Vytvoření DNS záznamu

Aby byl přístup k serveru flexibilnější a nebylo nutné, např. v případě předadresování sítě, měnit nastavení klientských aplikací, je vhodné používat DNS (Domain Name Service) jména místo IP adres. DNS tvoří nosnou vrstvu protokolu Kerberos a jeho bezchybné fungování je nutnou podmínkou funkčnosti heterogenního řešení v síti s Microsoft Windows.



Obr. 2. Vytvoření DNS záznamu typu A.

V prostředí AD službu DNS obsluhují doménové řadiče. Pro práci s DNS lze použít např. nástroj DNS Manager. Tento nástroj lze vyvolat z prostředí Windows Server 2008 spuštěním modulu `dnsmgmt.msc`. V části `Forward Lookup Zone` je nutné vytvořit nový záznam typu A. Zároveň je vhodné zřídit ukazatel PTR (Pointer Record), který slouží k reverznímu překladi IP adresy (viz Obr. 2).

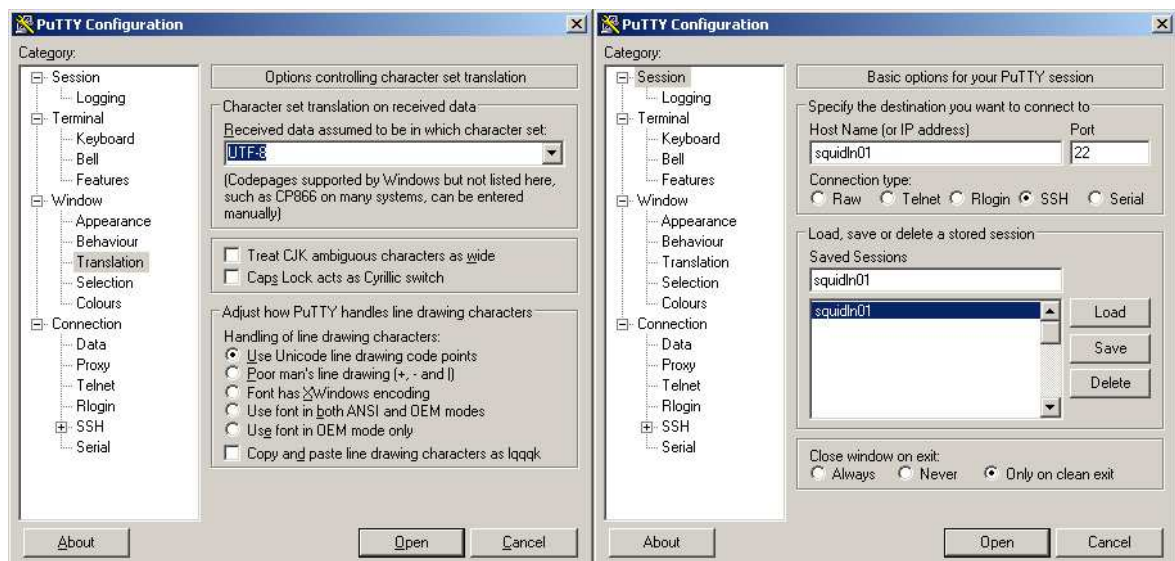
### 3.5 Instalace SSH serveru

V oblasti linuxových řešení se pro efektivní a bezpečnou správu serverů používá protokol SSH (Secure Shell). Před jeho instalací je vhodné provést aktualizaci databáze balíčků (příkaz č. 14) ze zdrojů uvedených v souboru `/etc/apt/sources.list`. Poté lze pokračovat instalací balíčku `open-ssh`.

```
14 apt-get update
```

```
15 apt-get install openssh-server
```

Po dokončení instalace se lze k serveru připojit pomocí protokolu SSH. Protože bude server spravován z prostředí Microsoft Windows, je nutné použít vhodného klienta, např. aplikaci `Putty` (viz Obr. 3). Při instalaci (viz 3.1) byl server zkonfigurován tak, aby pro zobrazení znaků využíval kódování UTF-8 (UCS Transformation Format). Toto kódování je nutné zvolit i v klientské aplikaci při přístupu na server.



Obr. 3. Nastavení aplikace Putty.

### 3.6 Instalace VMware Tools

Pokud je proxy server instalován na fyzický server, je možné tuto část přeskočit. Při instalaci do prostředí virtualizační platformy VMware ESX, je nutné po instalaci systému provést instalaci VMware Tools. Jde o balíček, který zlepšuje chování operačního systému ve virtuálním prostředí a umožňuje jeho plnou integraci pod hypervizor [34].

VMware Tools lze instalovat buď ze souboru, který je součástí instalace každého klienta VMware nebo v případě Linuxu z repozitářů OS. Při souborové instalaci je nutná

kompilace ze zdrojových kódů. Použitelnost obou způsobů instalace je obdobná - u standardní distribuce je vhodnější preferovat instalaci z repozitářů. Zde se projeví přínos distribuce Ubuntu, která je díky kratšímu cyklu schopna nabídnout aktuálnější verzi balíčku.

Použití balíčku z repozitáře má proti ruční kompilaci několik výhod:

- balíček udržuje správce balíčku,
- balíček je vždy aktuální pro použitou verzi linuxového jádra (odpadá nutnost rekompilace při každém upgrade).

VMware Tools jsou vydávány společností VMWare, Inc. jako OSS od roku 2007. V Ubuntu je dostupný balíček `open-vm-tools`. Jeho instalace je velmi snadná.

```
16 sudo apt-get install open-vm-tools
```

Korektně instalované VMware Tools lze poznat podle dostupných voleb „Shutdown Guest“ a „Restart Guest“ u virtuálního hosta v VMware vSphere Client.

### 3.7 Instalace Network Time Protocol

Ověřování uživatelů v prostředí AD je vázáno na časová razítka, proto je nutné zajistit synchronizaci linuxového stroje s časem na DC (Domain Controller).

K synchronizaci času mezi počítači se používá NTP (Network Time Protocol). Balíček je dostupný v repozitáři.

```
17 apt-get install ntp
```

#### 3.7.1 Konfigurace NTP

Při konfiguraci je nutné zadat adresy NTP serverů, se kterými se má klient synchronizovat. Ideální je použít alespoň dva doménové řadiče – řádky 24 a 25. Vhodné je též definovat cestu k adresáři se statistikami (příkaz č. 19), aby bylo možné diagnostikovat činnost služby.

```
18 driftfile /var/lib/ntp/ntp.drift
19 statsdir /var/log/ntpstats/
20 statistics loopstats peerstats clockstats
21 filegen loopstats file loopstats type day enable
22 filegen peerstats file peerstats type day enable
23 filegen clockstats file clockstats type day enable
```

```
24 server Adresa_DC02.Nazev_Domeny.local
25 server Adresa_DC02.Nazev_Domeny.local
26 restrict -4 default kod notrap nomodify nopeer noquery
27 restrict -6 default kod notrap nomodify nopeer noquery
28 restrict 127.0.0.1
29 restrict ::1
```

Po změně konfigurace je nutný restart služby příkazem č. 30.

```
30 service ntp restart
```

V logu je možno příkazem č. 31 ověřit, že synchronizace opravdu probíhá.

```
31 cat /var/log/ntpstats/peerstats
```

## 4 PŘIPOJENÍ LINUXU K DOMÉNOVÉ STRUKTUŘE ACTIVE DIRECTORY

V tento okamžik je provedena základní instalace linuxového stroje. V požadavcích na řešení (viz 2.2) byla definována potřeba podmíněných přístupových pravidel a oprávnění k systému v návaznosti na centrální uživatelskou databázi v AD. Doménové řadiče tak budou nadále jediným nositelem databáze uživatelských účtů. Využití tohoto konceptu v sítích s OS Windows by mělo být z hlediska bezpečnosti prosazováno ve všech oblastech ICT (Information and Communication Technologies).

Autentizační systémy OS Windows a Linux se liší a při práci využívají rozdílné informace. Tato skutečnost komplikuje možnost použití doménového řadiče pro linuxovou autentizaci. Problém lze poměrně elegantně řešit pomocí systému Winbind, který je součástí linuxového balíku Samba. Pokud se podaří provázat server s řadičem domény, mohou všechny služby v OS Linux využívat aktuální databázi uživatelských účtů z DC [35].

### 4.1 Samba

Samba umožňuje linuxovému systému poskytovat souborové služby klientům z OS Microsoft Windows. Jedná se o implementaci síťového protokolu SMB (Server Message Block)/CIFS (Common Internet File System), používaného především ke sdílení souborů v OS Windows. SMB je protokol aplikační vrstvy, sloužící ke sdílení souborů a tiskáren. CIFS zajišťuje stejnou funkcionalitu s využitím TCP/IP. Samba server je dostupný na řadě unixových systémů.

O hlavní funkce Samby se starají tři démoni:

- **Smbd**

Obstarává sdílení tiskáren a souborů, zajišťuje klientům připojení na portech TCP 139 nebo 445.

- **Nmbd**

Zabezpečuje překlady jmen protokolu NetBIOS (Network Basic Input Output System). Démon pracuje na portech UDP 137 a 138.

- **Winbind**

Zajišťuje vazbu mezi DC a linuxovým autentizačním systémem PAM (Pluggable Authentication Modules). Pro správné fungování démona Winbind je nutná Samba, PAM a nástroj NSS (Name Service Switch).

Jak již bylo zmíněno, chybí Linuxu při doménové autentizaci některé informace. Doménový řadič např. neví, jaký interpret příkazů uživatel v OS Linux používá, nezná cestu k lokálnímu linuxovému adresáři uživatele apod. Winbind je službou, která umí operačnímu systému Linux chybějící informace poskytnout.

#### 4.1.1 Instalace Samby

Balíčky Samba a Winbind mají definovanu řadu závislostí. Díky balíčkovacímu systému pro instalaci postačí jen příkaz č. 32. Tímto způsobem dojde k automatické instalaci včetně spouštěcích skriptů.

```
32 apt-get install samba winbind
```

#### 4.1.2 Konfigurace Samby

Konfigurační soubor Samby je rozdělen na několik částí. Při základní konfiguraci postačí upravit jen oddíl `global`. V části 5.9.2 budou do konfiguračního souboru za účelem zálohování linuxového řešení přidány další oddíly.

```
33 [global]
34     log file = /var/log/samba/%m.log
35     max log size = 50
36     log level = 3
37     netbios name = squidln01
38     workgroup = Nazev_Domeny
39     server string = SQUID Proxy
40     restrict anonymous = 2
41     allow trusted domains = yes
42     domain master = no
43     encrypt passwords = yes
44     security = ADS
45     realm = Nazev_Domeny.local
46     password server = Adresa_DC01.Nazev_Domeny.local
47     winbind use default domain = yes
48     winbind separator = +
```

```
49      winbind enum users = yes
50      winbind enum groups = yes
51      winbind nested groups = yes
52      winbind refresh tickets = yes
53      idmap config *: backend = tdb
54      idmap config *: backend = rid
55      idmap config *: range = 500-1000000
56      client use spnego = yes
57      client ntlmv2 auth = yes
58      client use spnego principal = no
59      send spnego principal = no
60      template shell = /bin/bash
61      template homedir = /home/%D/%U
62      smb ports = 139
```

Příkaz č. 34 definuje cestu k logům s využitím proměnné `%m`. Tato proměnná zaručuje, že budou logy nazvány podle NetBIOS jména stanice. Jmenná konvence je užitečná zejména při ladění serveru. Výčet použitelných proměnných uvádí manuálová stránka Samby [36]. Příkazy č. 35 a 36 upravují maximální velikost a podrobnost logů Samby.

NetBIOS jméno nastavené v řádku 37 se musí shodovat se jménem serveru (viz hodnota `hostname` v části 3.1). Tento název je zapsán také v souboru `/etc/hostname`.

V řádku 38 je jako jméno pracovní skupiny použit název domény bez sufixu. Jmenný systém protokolu NetBIOS je plochý, nevyužívá žádnou hierarchii. To je největší rozdíl oproti DNS, neboť NetBIOS je možné použít pouze v rámci jedné organizace. Položka v řádku 39 se v prostředí v OS Microsoft Windows zobrazuje u sdílené složky jako Popis (Description).

Řádek 40 koresponduje s nastavením bezpečnostního modelu OS Microsoft Windows a řídí se doménovou politikou. Hodnota tohoto parametru koresponduje s hodnotou, použitou v systémovém registru OS Microsoft Windows ve větvi `HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous`. Je-li registr nastaven na hodnotu 0 (no), bude informace o uživateli a skupině vrácena na jakýkoliv dotaz. Při hodnotě 1 (yes) budou informace vráceny pouze ověřeným uživatelům. Ideální hodnotou, podporovanou OS Microsoft Windows 2000 a vyšší je 2. Toto nastavení zcela zakazuje přístup neověřeným uživatelům. Příkaz č. 41 omezí přístup ke sdíleným zdrojům pouze z důvěryhodných domén. Příkaz č. 42 zakáže démonu `nmbd` fungovat v módu `domain master`. Není vhodné, aby proxy udržovala seznam služeb pro celou doménu.

Použití hesla v prostém textu lze na OS Microsoft Windows vynutit, jedná se však o zásadní bezpečnostní riziko. Proto všechny novější verze tohoto OS pracují s šifrovanými hesly. Použití šifrovaných hesel vynutí příkaz č. 43.

Tato direktiva souvisí s příkazem č. 44, který vymezuje bezpečnostní režim Samby. Dochází k integraci serveru do prostředí AD, proto je nutné použít režim `Domain` nebo `ADS`. V režimu `Domain` jsou uživatelé autentizováni na řadičích domény. Pokud pracuje Samba režimu `Domain`, musí existovat vztah důvěryhodnosti. Server tedy musí být plnohodnotným členem domény. Autentizační požadavky poté Samba jako členský server předává doménovým řadičům. Při volání používá vzdálené volání procedur RPC (Remote Procedure Call) podporované i ve starších verzích systému NT. Z bezpečnostního hlediska nelze toto nastavení doporučit.

Vhodnější volbou je režim `ADS`. Tento režim vynucuje použití Kerberos protokolu pro autentizaci klientů Samby. Při použití režimu `ADS` je nutné specifikovat Kerberos realm (musí být velkými písmeny) a určit, které doménové řadiče může Samba pro autentizaci uživatelů používat. Při použití režimu `ADS` je doporučenou hodnotou „\*“, tzn., že Samba určí vhodný DC sama. V případě problémů, kdy Samba nezná topologii sítě v AD, je možné na tomto místě použít IP adresu, nebo DNS jméno DC, nebo odkázat Sambu na některý z RODC (Read Only Domain Controller). Jednotlivé DC je nutné oddělit čárkou. Ačkoli se nejedná o doporučený způsob v praxi se osvědčil. Umožňuje totiž Sambu opřít o méně exponované doménové řadiče.

Další příkazy pomáhají Winbindu specifikovat chybějící informace z AD. Příkaz č. 47 způsobí, že pro autentizaci nebude nutné používat název domény. V opačném případě je vyžadováno spojení `Nazev_Domeny+jmenouzivatele`. Budou-li na server přistupovat uživatelé z více domén, je třeba nastavit tento parametr na hodnotu `no` (jedno uživatelské jméno může existovat ve více doménách). Příkaz č. 48 přepisuje výchozí oddělovač uživatelského jména a hesla „\” znakem „+“. Tento znak se lépe používá v sekvencích řídicích znaků (escape sekvence).

Příkazy č. 49 a 50 umožňují získat seznam uživatelů a skupin z AD pomocí standardních linuxových příkazů. Direktiva `winbind nested groups` zapíná podporu vnořených skupin, které se na OS Windows používají pro konsolidaci a snížení nároku na replikace. Příkaz č. 52 říká Winbindu, že má periodicky obnovovat lístky pro Kerbera.

Uživatelské účty v Linuxu používají uživatelská čísla UID (Unique Identifier). V OS Windows se tato čísla nazývají SID (Security Identifier) a GID (Group Identifier). Čísla si navzájem neodpovídají, proto je nutné při spojení obou OS zajistit mapování. Mapování má v Sambě na starost modul `idmap`. Modul je konfigurován v bloku příkazů č. 53-54. Je určeno, že systém bude data uchovávat ve formě TBD souborů (v adresáři `/var/cache/samba`). Příkaz č. 54 definuje, jaký typ mapování má server použít. Mapování `idmap rid` používá jako vstup UID a GID rozsahy a provádí mapování SID podle tohoto algoritmu – např. SID S-1-5-21-34567898-12529001-32973135-**1234**. Při použití UID v rozsahu **500-1000000** (příkaz č. 55) bude výsledné UID **500 + 1234 = 1734**.

Další dva řádky mění bezpečnostní chování Samby. Příkaz č. 56 upravuje chování při vyjednávání o autentizačním mechanismu dle RFC 2478 [37]. Další příkaz vynucuje zabezpečení hesla použitím NTLMv2 (NT LAN Manager verze 2) při vyjednávání o přístupu ke sdíleným prostředkům v síti s OS Microsoft Windows. Direktivu použitou na řádcích 58 a 59 je možné použít od Samby verze 3.6.0. Zvyšuje bezpečnost a kompatibilitu Samby s Microsoft Windows Server 2008.

Jedním ze základních údajů, který v AD databázi linuxový server nenajde je interpret příkazů, který mají všichni linuxoví uživatelé specifikován v souboru `/etc/passwd`. Příkaz č. 60 zajistí, že pro uživatele z AD bude jako interpret použit shell `bash`. Uživatelům z AD je rovněž nutné dát k dispozici jejich domovský adresář. Nastavení zajistí příkaz č. 61. Aby bylo možné odlišit adresáře lokálních a doménových uživatelů, budou doménoví uživatelé přesměrováni do adresáře `/home/domena/jmenouzivatele`.

Po editaci konfiguračního souboru je vhodné provést kontrolu souboru na chyby.

```
63 testparm
```

Pokud je zobrazena chyba `rlimit_max: rlimit_max (1024) below minimum Windows limit (16384)`, je nutné do souboru `/etc/security/limits.conf` přidat řádek

```
64 * - nofile 16384
```

Po úpravě souboru je vyžadován restart serveru. Pokud je vše v pořádku, je možné provést restart služeb.

```
65 service winbind stop
```

```
66 service smbd restart
```

```
67 service winbind start
```

### 4.1.3 Úprava host souboru

Před vložením serveru do doménového prostředí je vhodné zeditovat soubor `/etc/hosts`, aby server věděl, jaké je jeho doménové jméno. Soubor stačí upravit do níže uvedeného tvaru.

```
68 127.0.1.1 squidln01.Nazev_Domeny.local squidln01
```

## 4.2 Kerberos

V části 4.1.2 je uvedeno, že pro plné fungování Samby v režimu ADS, je nutné mít funkční Kerberos. Kerberos je standardní autentizační protokol, využívající symetrickou kryptografii. Od verze Microsoft Server 2000 je používán jako primární autentizační protokol (Kerberos verze 5) [38].

Kerberos zajišťuje [35]:

- **Centrální autentizaci**

Umožňuje autentizovat klienty a ujistit je o identitě služeb, ke kterým se připojují.

- **Ochranu hesel**

Obě strany (klient i server) mohou použít Kerberos pro bezpečnou autentizaci, a v případě potřeby i pro šifrování další komunikace.

- **SSO (Single Sign On) - systém jediného přihlášení**

Jakmile Kerberos jednou ověří uživatele, je klient ověřen pro všechny služby a servery, které Kerberos podporují.

Na operačních systémech rodiny Microsoft Windows Server zajišťuje protokol Kerberos služba, běžící na DC. OS Windows používá pro autentizaci systém IWA (Integrated Windows Authentication), který stojí na protokolech SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism), Kerberos a NTLMSSP (NT LAN Manager Security Support Provider). Protokol SPNEGO vyjednává, zda bude použit Kerberos nebo starší NTLMSSP. IWA umožňuje použít SSO i ve webové aplikaci (je nutná podpora v prohlížeči a webovém serveru).

Klienta ověřeného protokolem Kerberos není nutno ověřovat vůči jednotlivým serverům, které poskytují síťové služby. Jeho důvěryhodnost zajišťuje server KDC (Key Distribution

Center). Použití KDC jako centrálního autentizačního prvku zvyšuje bezpečnost. KDC zná klíče všech svých klientů (uživatelé, servery, aplikace) kteří se vůči němu ověřují. Klient je libovolný počítač, který si od KDC vyžádá autentizační lístek. Obvykle to bývá aplikace spouštěná uživatelem sítě. Lístky (tickety) jsou základem autentizačního mechanismu systému Kerberos. Jde o zašifrovaný blok dat, pomocí kterého se systémy vzájemně autentizují. Posláním Kerbera je autentizace síťových služeb. Na rozdíl od LDAP a NT služeb, které jsou navrženy pro centrální autentizaci uživatelů.

Autentizace protokolem Kerberos v systému Windows probíhá v několika krocích (viz Obr. 4) [39] [40] [35]:

- **Autentizace uživatele a vystavení TGT (Ticket-Granting Ticket)**

Při přihlášení uživatel zadá své přihlašovací údaje.

- KRB AS REQ

Klient vygeneruje pomocí jednosměrné hashovací funkce nad heslem „Password Hash Key“ a odešle jej na AS (Authentication Server), který je součástí KDC, formou žádosti o TGT.

- KRB AS REP

Po přijetí žádosti načte AS z AD uživatelské heslo a vygeneruje z něj hash hodnotu, kterou použije pro dekódování žádosti uživatele. Pokud se podaří žádost dekódovat, vezme z žádosti klienta časové razítko a ověří aktuálnost žádosti.

Po ověření AS pošle klientovi:

- 1) „Client-KDC Session Key“

Klíč určený pro šifrování komunikace mezi klientem a KDC. Klíč je šifrovaný hashem uživatelského hesla.

- 2) TGT

Unikátní klíč, který obsahuje ID (identifikaci) klienta, síťovou adresu, informaci o platnosti ticketu a „Client-KDC Session Key“ (klíč pro budoucí šifrování komunikace mezi KDC a klientem).

TGT je zašifrován klíčem, který zná jen KDC („KDC Secret Key“)

Klient dokáže díky znalosti hashe vlastního hesla rozšifrovat „Client-KDC Session Key“ a je vůči serveru autentizován (vše bez nutnosti odesílat heslo po síti).

TGT dále slouží k identifikaci uživatele - obsahuje jméno klienta, adresu, dobu platnosti a „Client-KDC Session Key“. Klient nedokáže TGT rozšifrovat. TGT má omezenou životnost, ale může probíhat automatická reautentizace (viz řádek 52). Při každém přihlášení se vytváří nový TGT.

Zašifrovaný TGT, „Client-KDC Session Key“ a „Service Ticket“ má klient uloženy dočasně v paměti.

- **Autentizace ke službě**

- **KRB TGS REQ**

Pokud se chceme přihlásit k nějaké službě v síti, aplikace na klientovi použije TGT a požádá TGS (Ticket Granting Service), která je součástí KDC o „Service Ticket“. Žádost tvoří ověření uživatele a je rozdělena do dvou zpráv:

- 1) **TGT**

TGT je zašifrován „KDC Secret Key“. Obsahuje informaci o tom, ke kterému serveru se chce klient připojit, tzv. SPN (Service Principal Name).

- 2) **„Authenticator“**

Složený z identifikace uživatele a časového razítka. Tuto část klient šifruje pomocí „Client-KDC Session Key“.

- **KRB AS REP**

TGS ověří klientův TGT použitím „KDC Secret Key“ a dekoduje „Authenticator“ s využitím „Client-KDC Session Key“. Pokud je vše v pořádku, vystaví a zašifruje „Service Ticket“. Ten je složen ze dvou částí.

- 1) **„Client-to-Server Ticket“**

Serverová část ticketu obsahuje identifikaci uživatele, adresu, časové razítko a „Client-Server Session Key“. Tato část je zašifrovaná klíčem „Service Secret Key“, který zná pouze aplikační server.

2) „Client-Server Session Key“

Slouží pro komunikaci klienta s aplikačním serverem. Tato část je šifrovaná klíčem „Client-KDC Session Key“.

Je zřejmé, že první část nemůže klient dešifrovat, ani pozměnit.

- **Ověření u služby (serveru):**

- KRB\_AP\_REQ

Klient má vše, co potřebuje k autentizaci. Odešle na aplikační server zprávu, složenou ze dvou částí:

- 1) „Client-to-Server Ticket“

Pro šifrování je použit stejný mechanismus jako v části KRB\_AS\_REP.

- 2) „Authenticator“

Šifrovaný „Client-Server Session Key“. Obsahuje ID klienta a časové razítko.

Aplikační server provede rozšifrování první části „Service Ticket“. Z něj získá „Client-Server Session Key“ a pomocí něj rozšifruje „Authenticator“.

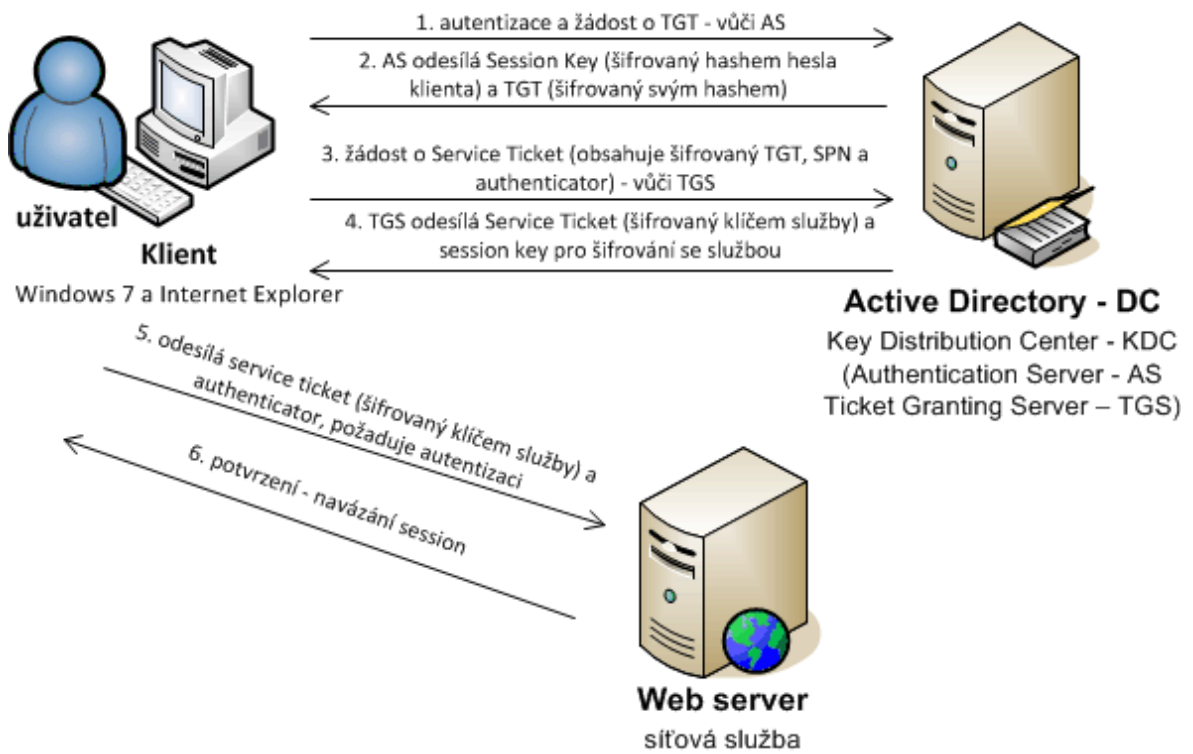
Po úspěšném ověření klienta zvýší server časové razítko z „Authenticator“ o jedničku a odešle serveru zpět potvrzení. Potvrzení je zašifrováno pomocí „Client-Server Session Key“ (zná klient a server).

Klient rozšifruje potvrzení a porovná časovou známku. Pokud je vše v pořádku, je server důvěryhodný pro klienta a komunikace může pokračovat.

Použití protokolu Kerberos umožňuje ověřit nejen klienta na serveru ale i server vůči klientovi. Kerberos zajišťuje pouze autentizaci a není nositelem žádných dalších informací o uživateli. Má-li systém zajišťovat autorizaci, je nutné Kerberos kombinovat s LDAP dotazy. Ty umožňují ověřit, v jakých AD skupinách se úspěšně autentizovaný účet vyskytuje a s využitím těchto informací řídit přístup ke zdrojům.

Z popisu je zřejmé, že důležitou roli pro Kerbera má časové razítko. Synchronizace hodin je zajištěna s pomocí NTP protokolu, jehož nastavení bylo provedeno dříve. Je také nutné, aby všechny servery a služby, u kterých má být Kerberos použit, měly vytvořen DNS záznam typu A (viz 3.4).

Při konfiguraci Samby byl příkazem č. 45 definován parametr `realm`. Jedná se o tzv. kerberovu doménu, tedy oblast spravovanou KDC.



Obr. 4. Princip Kerberos autentizace [40].

#### 4.2.1 Instalace Kerberos

Protože doménové řadiče na OS Microsoft Windows používají Kerberos verze 5, bude prvním krokem instalace balíčků této verze z repozitáře.

```
69 apt-get install krb5-user krb5-doc libpam-krb5
```

Po instalaci je spuštěn průvodce, který v dialogu požaduje vložení `realm`. Dialogové okno je vhodné ukončit a provést ruční konfiguraci.

#### 4.2.2 Konfigurace Kerberos

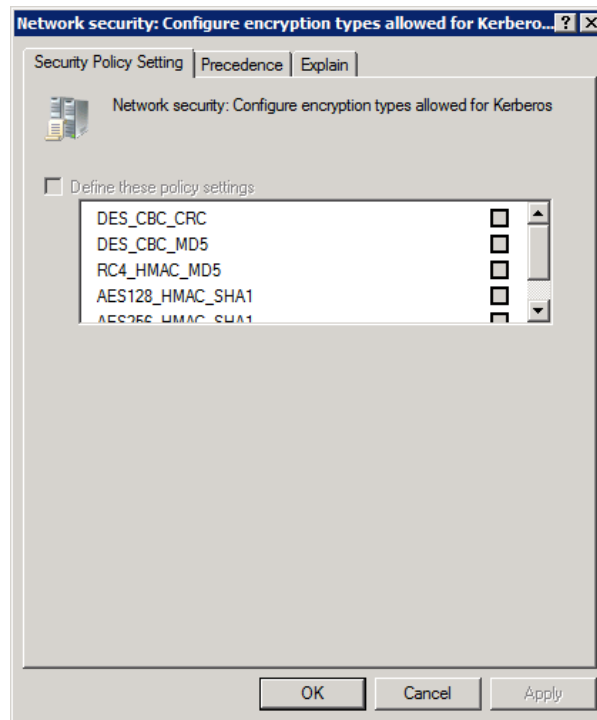
Soubor `/etc/krb5` obsahuje hlavní nastavení Kerbera. Konfigurační soubor je rozdělen na části, stejně jako u Samby. Každý oddíl začíná jménem v hranatých závorkách.

```
70 [logging]
71 default = FILE:/var/log/krb5/default.log
72 kdc = FILE:/var/log/krb5/kdc.log
73 admin_server = FILE:/var/log/krb5/adminsrv.log
74 [libdefaults]
```

```
75 default_realm = NAZEV_DOMENY.LOCAL
76 default_tgs_etypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc
  des-cbc-md5
77 default_tkt_etypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc
  des-cbc-md5
78 permitted_etypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc
  des-cbc-md5
79 kdctimesync = 1
80 ccache_type = 4
81 forwardable = true
82 fcc-mit-ticketflags = true
83 default_keytab_name = FILE:/etc/krb5.keytab
84 clockskew = 300
85 [realms]
86 NAZEVDOMENY.LOCAL = {
87     kdc = Adresa_DC01.Nazev_Domeny.local:88
88     kdc = Adresa_DC02.Nazev_Domeny.local:88
89     admin_server = Adresa_DC01.Nazev_Domeny.local:749
90     default_domain = Nazev_Domeny.local
91 }
92 [domain_realm]
93 .kerberos.server = NAZEV_DOMENY.LOCAL
94 .nazev_domeny.local = NAZEV_DOMENY.LOCAL
```

V části [logging] je řešeno protokolování operací souvisejících s činností serveru. V oddíle [libdefaults] se nastavuje výchozí chování Kerbera. Na řádku 75 je zadána výchozí doména, tedy jméno oblasti spravované KDC. Na řádcích 76-78 jsou specifikovány šifrovací metody pro Kerbera. Je nutné použít šifry podporované Microsoft Windows Server [41]. Definována je nejprve metoda pro šifru (řádek 76), kterou vrací KDC, dále pak šifry, jež mohou být požadovány klientem (řádek 77) a šifry používané pro ochranu klíče (řádek 78). Šifrovací mechanismy lze na Microsoft Windows Serveru upravit s použitím systémových politik v položce Network security: Configure encryption types allowed for Kerberos, která se nachází v části Computer Configuration\Security Settings\Local Policies\Security Options (viz Obr. 5).

Příkaz č. 79 zapíná synchronizaci času klientů s KDC. Aby synchronizace fungovala, je nutné příkazem č. 80 přepnout pověření mezipaměti do režimu 4. V tomto režimu je podporováno použití hlaviček s časovými razítky pro synchronizaci hodin. Uvnitř Kerberos ticketů je zakódována IP adresa klienta, na základě které je klient ověřen KDC.



Obr. 5. Nastavení šifrovacích metod pro Kerbera na Microsoft Windows Server 2008.

Ticket, který byl získán pro jednoho hostitele, nemůže být použit pro jiného. Kerberos verze 5 přidal možnost přeposílání lístků (forwardable tickets). Přeposílání aktivuje příkaz č. 81. Během prvotní žádosti o TGT může klient požádat o lístek s označením „forwardable“. Poté je klientu umožněno žádat o vystavení následného lístku z jiné IP adresy. Příkaz č. 82 určuje, že lístky budou ve formátu, který odpovídá standardu MIT (Massachusetts Institute of Technology). Příkaz č. 83 pak určuje cestu ke `keytab` souboru, který bude vygenerován později.

Řádek 84 zabraňuje útočníkům používat expirované tickety a vymezuje maximální toleranci odchylky systémových hodin serveru a klienta. Bude použita výchozí hodnota 5 minut.

V oddíle `[realms]` jsou definovány kerberovy domény. V konfiguraci je použita jedna doména, která obsahuje dva KDC (DC) a administrativní server. Ten se stará o správu principálů a běží na doménovém řadiči DC01.

V oddílu `[domain realm]` je uveden výčet domén. Je zřejmé, že všechny počítače z domény a subdomén spadají pod doménu `Nazev_Domeny.local`.

### 4.3 Vložení stanice do domény

V tento moment je server připraven stát se členem AD domény. Při vkládání stanice do domény příkazem č. 95 jsou vyžadována zvýšená práva dle nastavení systémových politik. Je tedy nutné použít buď účet z AD skupiny `Domain Admin` nebo účet, který má delegována dostatečná oprávnění.

```
95 sudo net ads join -U Ucet_Domenoveho_Admina
```

System ověří uživatele a vloží stanici do domény. V konzoli se zobrazí hlášení:

```
Joined 'SQUIDLN01' to realm 'Nazev_Domeny.local'.
```

Na pozadí přitom proběhnou tyto kroky:

- je lokalizován doménový řadič, který nabízí služby LDAP a KDC,
- je vytvořen účet počítače v AD,
- je vystaven první TGT pro PC (Personal Computer) a je uložen v dočasné paměti.

V tento moment lze vyzkoušet, že vazba na AD funguje. Pokud vše proběhlo v pořádku, lze pomocí příkazů `wbinfo -u` a `wbinfo -g` vypsat doménové uživatele a skupiny. Stroj je vhodné v AD přesunout z výchozího kontejneru `Computers` do příslušné složky.

### 4.4 Otestování Kerbera a vytvoření keytab souboru

Činnost protokolu Kerberos lze otestovat velmi jednoduše – stačí požádat o vystavení ticketu použitím příkazu `kinit` [42].

```
96 kinit jmenouzivatele
```

System si vyžádá heslo. Po autentizaci je možné pomocí příkazu `klist` zobrazit seznam vystavených ticketů:

```
97 root@squidln01:~# klist
98 Ticket cache: FILE:/tmp/krb5cc_0
99 Default principal: jmeno_uzivatele@NAZEV_DOMENY.LOCAL
100 Valid starting Expires Service principal
101 01/08/2012 14:14 02/08/2012 00:14
krbtgt/NAZEV_DOMENY.LOCAL@NAZEV_DOMENY.LOCAL
102 renew until 02/08/2012 14:14
```

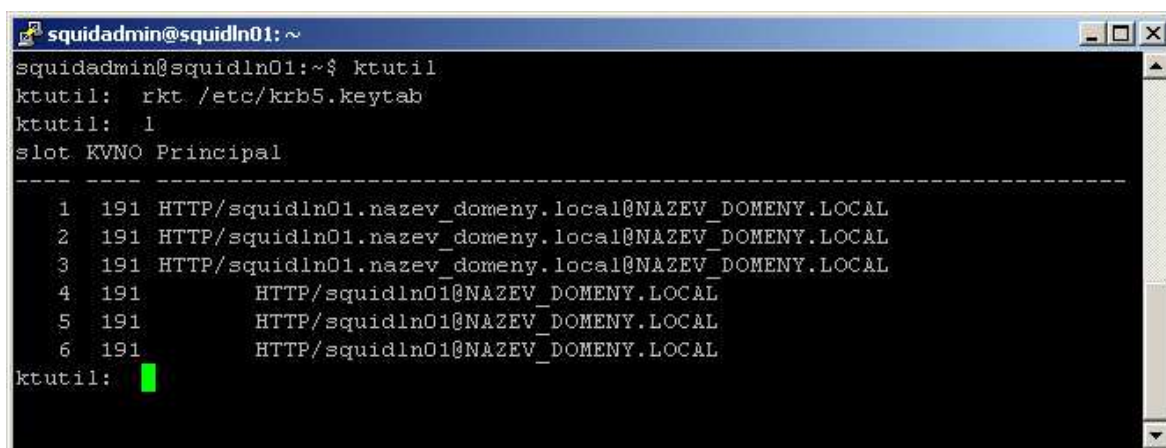
Vystavený lístek je možné zrušit použitím příkazu `kdestroy`.

Při požadavku KRB\_TGS\_REQ se klient odkazuje na požadovanou službu pomocí SPN. Pro aplikace má SPN tvar `service/hostname@REALM`, kde `hostname` odpovídá DNS jménu serveru. Je rovněž nutné vystavit „Service Secret Key“ pro server. Pro službu HTTP má „Principal name“ tvar `HTTP/hostname@REALM`, kde `REALM` je velkými písmeny zapsaný název domény, vůči které se budou uživatelé autentizovat.

Jak bylo uvedeno v popisu fungování protokolu Kerberos, každý server potřebuje tzv. `keytab` soubor. Jedná se o zašifrovaný klíč počítače. Server má již nastavenou Sambu, proto lze soubor `keytab` ihned generovat.

```
103 net ads keytab add HTTP -U Nazev_Domenoveho_Admina
```

Pro kontrolu je možné použít příkaz `ktutil`, který umožňuje manipulaci s klíči. Nejprve je nutné zavolat příkaz `rkt /etc/krb5.keytab` a poté zobrazit písmenem `l` klíče pro služby (viz Obr. 6).



```

squidadmin@squidln01: ~
squidadmin@squidln01:~$ ktutil
ktutil: rkt /etc/krb5.keytab
ktutil: l
slot KVNO Principal
-----
1 191 HTTP/squidln01.nazev_domeny.local@NAZEV_DOMENY.LOCAL
2 191 HTTP/squidln01.nazev_domeny.local@NAZEV_DOMENY.LOCAL
3 191 HTTP/squidln01.nazev_domeny.local@NAZEV_DOMENY.LOCAL
4 191 HTTP/squidln01@NAZEV_DOMENY.LOCAL
5 191 HTTP/squidln01@NAZEV_DOMENY.LOCAL
6 191 HTTP/squidln01@NAZEV_DOMENY.LOCAL
ktutil: █

```

Obr. 6. Obsah `keytab` souboru.

## 4.5 Konfigurace NSS

Aby mohl systém využívat uživatelské účty z AD, je nutné zkonfigurovat systém NSS (Name Switch Service). NSS zajišťuje ověřování jmen pro běžné databáze (např. seznam uživatelů v souboru `/etc/passwd`) a obsahuje i vyhodnocovací mechanismy. NSS umožňuje zjistit, do kterých skupin patří uživatelský účet.

V konfiguračním souboru `/etc/nsswitch.conf` jsou uvedeny databáze, ze kterých systém čerpá data o uživateli. Aby bylo možné čerpat data z AD, je nutné k položkám `passwd` a `group` přidat slovo `winbind`.

```
104 passwd:          compat winbind
105 group:           compat winbind
106 shadow:          compat
107 hosts:           files dns
108 networks:        files
109 protocols:       db files
110 services:        db files
111 ethers:           db files
112 rpc:              db files
113 netgroup:         nis
```

## 4.6 Konfigurace PAM

PAM je sada knihoven, která integruje větší množství nízkourovňových autentizačních mechanismů do jednoho API (Application Programming Interface). Použití API pomáhá oddělit detaily a způsob autentizace od programu, který ji zajišťuje [43]. V zadání byla požadována správa linuxových serverů pomocí účtů z AD. Knihovny PAM lze použít jako vazební článek pro definici práv doménovým uživatelům, kteří mají mít možnost přihlášení na linuxovou konzoli. V organizacích s pobočkami je vhodné v AD vytvořit `Global Security` skupinu, např. `_Domain Linux Admins`, ve které budou uživatelé s právy přihlášení na všechny linuxové servery, a další skupinu `_POB01 Linux Admins` určenou pro správce serveru na pobočce (s oprávněním spravovat vlastní linuxový server).

System PAM je složen ze tří částí:

- knihovna `libpam` (volají programy, které chtějí informace z PAM používat),
- PAM moduly (poskytují konkrétní autentizační mechanismy),
- konfigurace (definuje, které PAM moduly se budou používat při autentizaci).

V adresáři `/etc/pam.d` jsou uloženy jednotlivé soubory, jejichž jméno odpovídá jménu služby, pro kterou jsou určeny. Jednotlivé řádky souborů mají níže uvedený tvar.

```
type control module-path [module-args]
```

Položka **type** udává typ modulu, platné možnosti jsou:

- **account** (modul ověřující platnost účtu – heslo, přístup ke službě),
- **auth** (modul zajišťující ověření identity uživatele, který se snaží přihlásit),
- **password** (modul pro změnu nebo kontrolu přihlašovacích údajů),

- **session** (modul řídící relaci uživatele).

Položka **control** udává chování ověřovacího procesu v závislosti na výsledku modulu.

Obsahem pole mohou být tato slova:

- **Required**

Selháním modulu selže proces ověřování. Provádění však pokračuje dalšími moduly.

- **Requisite**

Selháním modulu selže celý proces a řízení je vráceno aplikaci. K volání dalších modulů nedochází.

- **Sufficient**

Úspěch v modulu zajistí úspěšný výsledek celého ověřování. Pokud nejsou v sekvenci žádné další `required` moduly, provádění se zastaví.

- **Optional**

Úspěch v tomto modulu není podmínkou celkového úspěchu ověřování.

- **Include**

Vloží soubor předaný jako parametr.

Stejně tak je možné použít detailnější nastavení chování v případě různých výsledků. `module-path` je cesta k modulu a `module-args` obsahuje seznam parametrů oddělených mezerou. V Ubuntu jsou konfigurační soubory `pam.d` rozděleny dle oblastí. Každý soubor přitom obsahuje výčet PAM modulů, které mají být použity k provedení zásad přístupu. Zpracování konfiguračního souboru probíhá dle pořadí, ve kterém jsou jednotlivé moduly uvedeny, vyjma případu, kdy je úspěšný modul `sufficient`, nebo selže modul `requisite` [44]. Každý modul může vrátit úspěch nebo skončit s chybou. Výsledky všech modulů jsou sloučeny do jediného výsledku. Sloučení se řídí nastavením položky `control`.

Každá aplikace využívající PAM by měla mít svůj soubor.

#### 4.6.1 Konfigurace common-account

Tento konfigurační soubor slouží pro ověření platnosti použitého uživatelského účtu (platnost hesla, oprávnění přístupu ke službě). Protože mají být použity účty z AD, je nutné na tomto místě zařadit kontrolu modulem `pam_winbind`. Je zřejmé, že úspěšné ověření platnosti účtu modulem postačuje pro přihlášení uživatele. Pokud není úspěšné, je předáno modulu `pam_unix`, který se pokusí o ověření standardní cestou.

```
114 account sufficient      pam_winbind.so
115 account required       pam_unix.so
```

#### 4.6.2 Konfigurace common-auth

Přihlášení má být k dispozici pouze uživatelům, kteří jsou členy vybraných skupin AD. Nejprve je nutné zjistit SID požadovaných AD skupin `_POB01 Linux Admins` a `_POB01 Linux Admins` (použitých v 4.6), které mají mít možnost plného přístupu na linuxový server.

SID lze zjistit pomocí příkazů č. 116 a 117.

```
116 wbinfo -n „_Domain Linux Admins“
117 wbinfo -n „_POB01 Linux Admins“
```

Příkazy vrací dvojici SID, kterou je nutné přidat do konfiguračního souboru jako parametr příkazu `require_membership_of` modulu `pam_winbind.so` na řádce 119.

Parametr `nullok_secure` na řádce 118 potlačuje výchozí chování modulu `pam_unix.so` a povoluje přihlášení i uživateli s prázdným heslem. Zde je vidět jasný rozdíl ve fungování modulu dle použitého volání. Zatímco v kontextu `account` testuje `pam_unix` informace o expiraci účtu, v kontextu `auth` zkoumá uživatelské jméno a heslo. `Pam_unix` umí ověřovat informace o účtech dle konfigurace `nsswitch.conf`. Řádky 120 a 121 jsou pro všechny části PAM stejné a způsobí selhání autentizace v případě, že neuspějí předcházející moduly.

```
118 auth sufficient pam_unix.so nullok_secure
119 auth sufficient pam_winbind.so require_membership_of=SID1,SID2
    use_first_pass
120 auth requisite pam_deny.so
121 auth required pam_permit.so
```

### 4.6.3 Konfigurace common-password

```

122 password      [success=2 default=ignore] pam_unix.so obscure
    use_authok try_first_pass sha512
123 password      [success=1 default=ignore] pam_winbind.so
    use_authok try_first_pass
124 password      requisite pam_deny.so
125 password      required pam_permit.so

```

Soubor řeší možnost změny hesla uživatele. První dva řádky zpracovávají vložené heslo. Parametr `use_authok` zajistí, že modul nastaví nové heslo dle informace z dříve zařazeného modulu. Parametr `try_first_pass` vyžaduje, aby modul použil heslo z dříve zařazeného modulu v kontextu `auth` [45]. Parametr `SHA512` nastavuje hashovací funkci pro heslo. Slovo `obscure` zapíná kontrolu na sílu hesla.

Zajímavou funkci má parametr `success`, který určuje, kolik pravidel má být v zásobníku v případě úspěchu přeskočeno.

### 4.6.4 Konfigurace common-session

V konfiguraci Samby byl uživatelům nastaven domovský adresář. Aby bylo zajištěno jeho vytvoření, je nutné přidat do konfiguračního souboru řádek 127. V momentě, kdy se uživatel přihlásí k systému poprvé, vytvoří modul `pam_mkhome` domovský adresář a naplní jej soubory z `/etc/skel`. Zároveň nastaví k souborům oprávnění `0022`. Příkaz `umask` nastaví masku horní hranice práv na nově vytvářené soubory – tj. `0666 & ~022 = 0644`, tj. `rw-r--r--`.

```

126 session required pam_unix.so
127 session required pam_mkhome.so umask=0022 skel=/etc/skel

```

### 4.6.5 Konfigurace sudo

Jak bylo zmíněno dříve, používají některé distribuce příkaz `sudo`. Aby mohli příkaz používat i uživatelé z AD, je nutné v souboru `/etc/pam.d/sudo` zavést modul `pam_winbind` (řádek 128).

```

128 auth sufficient pam_winbind.so
129 auth sufficient pam_unix.so use_first_pass
130 auth required pam_deny.so
131 @include common-account

```

## 4.7 Konfigurace sudoers

Úprava souboru `/etc/pam.d/sudo` však není jediným krokem. Je nutné modifikovat také soubor `/etc/sudoers`. Editace souboru je nebezpečná. Nevhodný zásah končí odepřením požadavku na eskalaci práv a jedinou cestu k nápravě umožňuje linuxová recovery konzole. Pro editaci souboru je proto vhodné použít příkaz `visudo`.

Díky tomu, že byl v souboru `/etc/pam.d/sudo` (viz 4.6.5) zaveden modul pro `pam_winbind`, je možné v souboru `sudoers` použít názvy AD skupin. Pro zjištění správné syntaxe názvu AD skupiny je vhodné použít příkaz č. 132.

```
132 id jmeno_uzivatele
```

Příkaz vrací seznam skupin, do kterých patří zadaný uživatelský účet ve tvaru `ID skupiny (nazev_skupiny)`. Stejný formát zápisu je nutné použít v souboru `sudoers` – AD skupinu je třeba uvést znakem “%” a místo mezer v názvu je nutné použít znak “\”.

```
133 Defaults          env_reset
134 Defaults
    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin
    :/bin"
135 # User privilege specification
136 root    ALL=(ALL:ALL) ALL
137 # doménové ucty - povolení pro sudo a WinSCP
138 %_Domain\ Linux\ Admins ALL=(ALL)ALL,NOPASSWD:
    /usr/lib/openssh/sftp-server
139 %_POB01\ Linux\ Admins ALL=(ALL)ALL,NOPASSWD: /usr/lib/openssh/sftp-
    server
140 # Members of the admin group may gain root privileges
141 %admin ALL=(ALL) ALL
142 # Allow members of group sudo to execute any command
143 %sudo    ALL=(ALL:ALL) ALL
```

Řádek 0 provádí reset prostředí po přepnutí do kontextu `root` – odstraňuje uživatelské proměnné apod. Řádky 138 a 139 dávají uživatelům z vybraných skupin plná práva na `sudo`. Díky příkazu `NOPASSWD: /usr/lib/openssh/sftp-server` je možné pro doménové účty použít eskalovaná práva při připojení pomocí SCP (Secure Copy Protocol), např. při správě linuxového stroje přes aplikaci WinSCP. Uvedená konfigurace zajistí členům lokálních skupin `root`, `sudo` a `admin` a vyjmenovaných AD skupin právo spouštět cokoliv v kontextu účtu libovolného uživatele.

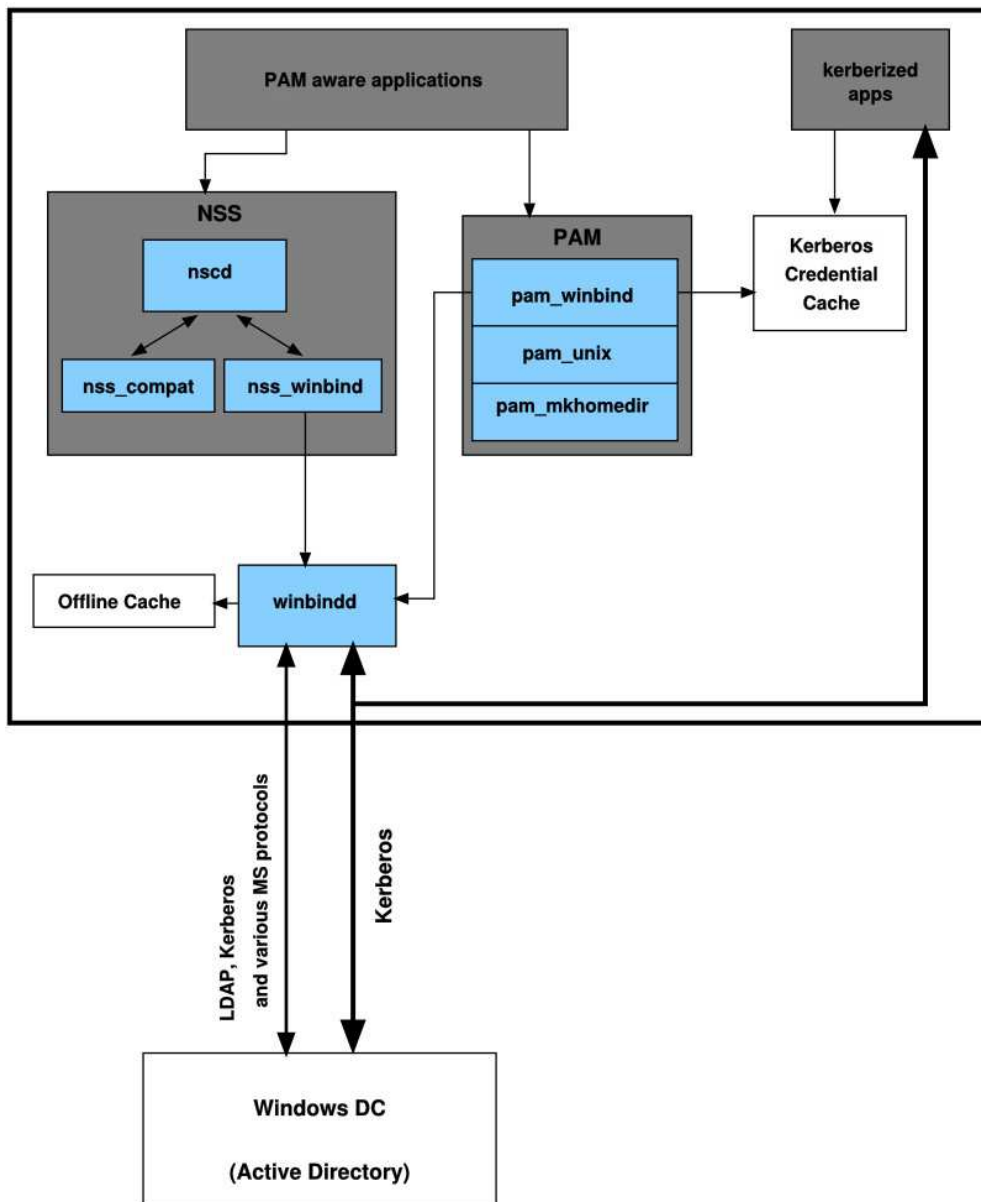
## 4.8 Testování prostředí

V tento okamžik má server zkonfigurován komponenty NSS, PAM, Kerberos a Samba. Linuxový stroj je plně integrován v AD prostředí. Uživatelé z vybraných AD skupin mají možnost přihlášení na konzoli, mají právo na `sudo`. Princip komunikace takto nakonfigurovaného linuxového serveru s doménovým řadičem zobrazuje Obr. 7. Následující příkazy vrací názvy lokálních i doménových skupin.

```
144 getent passwd
```

```
145 getent groups
```

Pokud se systém chová dle popisu, je možné přistoupit k instalaci proxy serveru Squid.



Obr. 7. Možnosti komunikace OS Linux s AD [46].

## 4.9 Squid

Funkci proxy serveru bude zajišťovat aplikace Squid. Ta byla částí 2.5.2 vybrána jako jediná, která dokáže zajistit všechny požadavky, jež jsou na řešení kladeny.

### 4.9.1 Instalace Squid

Po instalaci Squid verze 3 z repozitáře (příkaz č. 146) se aplikace v systému nachází v několika adresářích - viz Tab. 5.

```
146 apt-get install squid3
```

Tab. 5. Umístění aplikace Squid v systému.

Cesta k souboru	Popis
/usr/sbin/squid3	Spustitelný soubor Squid
/etc/squid3	Konfigurační soubory Squid
/usr/lib/squid3	Knihovny volané Squid
/usr/share/squid3	Chybová hlášení Squid
/usr/share/man/man8/squid3.8.gz	Manuálové stránky Squid

### 4.9.2 Konfigurace Squid

Hlavní konfigurační soubor serveru Squid `/etc/squid/squid.conf` obsahuje po instalaci pestrý výčet možností konfigurace proxy. Popis všech variant, které server nabízí, však není předmětem této práce. V dalším textu bude provedena základní konfigurace tak, aby byl Squid schopen zajišťovat funkce v rozsahu zadání.

Prvním krokem je příprava lokalizovaných chybových hlášení pro klienty proxy serveru. Zkušenosti z praxe ukazují, že ačkoliv tento krok není nutný, je chybové hlášení o nestandardní situaci v mateřském jazyce pro uživatele přijatelnější. Šablony chybových hlášení jsou standardně uloženy v adresáři `/usr/share/squid3/errors`. Toto umístění je však z hlediska správy nepraktické a je lépe umístit upravené hlášení do `/etc/squid3/error` tak, aby byly soubory při konfiguraci serveru snadno dostupné. Aby server věděl, kde má soubory hledat, je nutné ve výchozím umístění vytvořit sadu symlinků.

```

147 ln -s /etc/squid3/error/ERR_BLACKLIST
    /usr/share/squid3/errors/templates/ERR_BLACKLIST
148 ln -s /etc/squid3/error/ERR_WWW /usr/share/squid3/errors/templates
    /ERR_WWW
149 ln -s /etc/squid3/error/ERR_BLOCKED_FILES
    /usr/share/squid3/errors/templates/ERR_BLOCKED_FILES

```

Protože bude autentizace proxy serveru a později také Apache fungovat na bázi Kerberos protokolu, je nutné upravit práva na soubor `krb5.keytab`.

```

150 chgrp proxy /etc/krb5.keytab
151 chmod 666 /etc/krb5.keytab

```

Poté je třeba zadat cestu ke `keytab` souboru do inicializačního skriptu Squid serveru `/etc/default/squid3`. Soubor je nutné zeditovat do níže uvedeného tvaru.

```

152 KRB5_KTNAME=/etc/krb5.keytab
153 export KRB5_KTNAME

```

Poté je možné provést základní konfiguraci serveru Squid v souboru `/etc/squid3/squid.conf`.

```

154 #debug_options ALL,1 33,2 28,9
155 #####
156 # Autentizace Kerberos
157 #####
158 auth_param negotiate program /usr/lib/squid3/squid_kerb_auth -d
159 auth_param negotiate children 10
160 auth_param negotiate keep_alive on
161 #####
162 # Autentizace LDAP - pro skupiny
163 #####
164 external_acl_type ADGroup ttl=60 negative_ttl=60 %LOGIN
    /usr/lib/squid3/squid_ldap_group -R -K \
165         -b "DC=Nazev_Domeny,DC=local" \
166         -D "CN=Nazev_Uctu_Pro_Cteni_LDAP,OU=Systemove
    ucty,DC=Nazev_Domeny,DC=local" \
167         -w "Heslo_Uzivatele_Pro_Cteni_LDAP" \
168         -f
    "(&(objectclass=person)(sAMAccountName=%v)(memberof=cn=%a,OU=Skupiny
    ,DC=Nazev_Domeny,DC=local))" \
169         -h IP_Adresa_Domenoveho_Radice
170 #####
171 acl krb5_auth proxy_auth REQUIRED
172 # Zakazane stranky
173 acl zakazsites dstdomain "/etc/squid3/zakaz.sites.acl"
174 # Zakazane pripony souboru

```

```
175 acl zakazfiles urlpath_regex "/etc/squid3/zakaz.files.acl"
176 # Stranky s primym pristupem, které nesmi pres proxy
177 acl bezproxy dstdomain "/etc/squid3/bezproxy.sites.acl"
178 # ACL dle potreb pobočky
179 acl servery src Adresa_Site/Maska_Site
180 acl internet_povoleno Adresa_Site/Maska_Site
181 acl internet_users external ADGroup Internet_Users
182 # Pravidla provozu
183 http_access allow localhost
184 http_access allow servery
185 http_access deny zakazsites
186 http_access deny zakazfiles
187 http_access allow internet_povoleno Internet_Users krb5_auth
188 http_access deny all
189 # Chybove hlaseni pro zakazane pripony
190 deny_info ERR_BLOCKED_FILES zakazfiles
191 # Chybove hlaseni pri pristupu na zakazane weby
192 deny_info ERR_WWW all
193 deny_info ERR_BLACKLIST zakazsites
194 #pristup ke statistikam proxy pro sqstat
195 acl manager proto cache_object
196 http_access allow manager localhost
197 cache_peer Adresa_Nadrazene_Proxy parent Port_Nadrazene_Proxy 0 no-
query no-digest
198 # URL v bezproxy nesmi chodit pres proxy, jinak budou nedostupne
199 never_direct allow all
200 always_direct allow bezproxy
201 http_port 3128
202 shutdown_lifetime 1 seconds
```

První řádek konfiguračního souboru je určen pro ladění. Využít jej lze v případě velkého množství ACL (Access Control List) pravidel, která definují přístup uživatele. Do logu proxy serveru je v debug režimu zaznamenáváno detailní zpracování příchozích požadavků v rámci všech pravidel, takže lze snadno identifikovat, kde problém vzniká.

Squid je modulární systém. K podpoře autentizačních mechanismů používá pomocné „helper“ moduly. Moduly jsou dostupné v rámci repozitářů nebo je možné použít vlastní. Pomocné moduly umí zpracovat přihlašovací údaje z hlavičky Authentication a ověřit je proti konkrétní službě [47]. Každý z autentizačních systémů používaný Squidem má svá specifika:

- **Basic** – nejjednodušší, ale nejméně bezpečný systém. Uživatelská pověření jsou kódována metodou `base64`. Z toho důvodů je určen pouze pro malé, izolované sítě.
- **Digest** – odstraňuje zásadní nedostatek `basic` autentizace, tj. zasílání hesla v otevřené formě. Je bezpečnější, ale také komplikovanější [48]. Klient při `Digest` autentizaci zasílá pouze MD5 kontrolní součet loginu, hesla a řetězce, který obdržel od serveru v rámci požadavku na autentizaci.
- **NTLM** – zajišťuje podporu protokolu NTLM. Microsoft od využití protokolu na nových verzích Windows ustupuje [49], proto byl modul odstraněn ze standardních repozitářů a jeho instalace je volitelná.
- **Negotiate** – funkce určená pro Kerberos ověření do prostředí AD. Je nutné, aby tuto metodu podporoval internetový prohlížeč. V porovnání s NTLM nabízí tento typ ověření vyšší bezpečnost [47].

Pomocné moduly se zavádí prostřednictvím direktivy `auth_param`. Blok příkazů č. 155-160 konfiguruje modul `squid_kerb_auth`. Modul umožní Squid serveru zpracovat Kerberos tickety zasílané prohlížečem v rámci volání `Proxy-Negotiate` (viz popis v 5.8) dle RFC 2478 [37]. Příkaz č. 159 určuje kolik procesů zajišťujících vyřizování požadavků uživatelů, bude na serveru spuštěno. Větší množství spuštěných procesů zkracuje frontu uživatelů, kteří čekají na ověření. Příkaz č. 160 stanovuje, zda má Squid ukončovat připojení při počátečních dotazech prohlížeče na bezpečnostní metody podporované proxy serverem a lze jej použít pro řešení problémů s `PUT/POST` příkazy v rámci `Negotiate` metody.

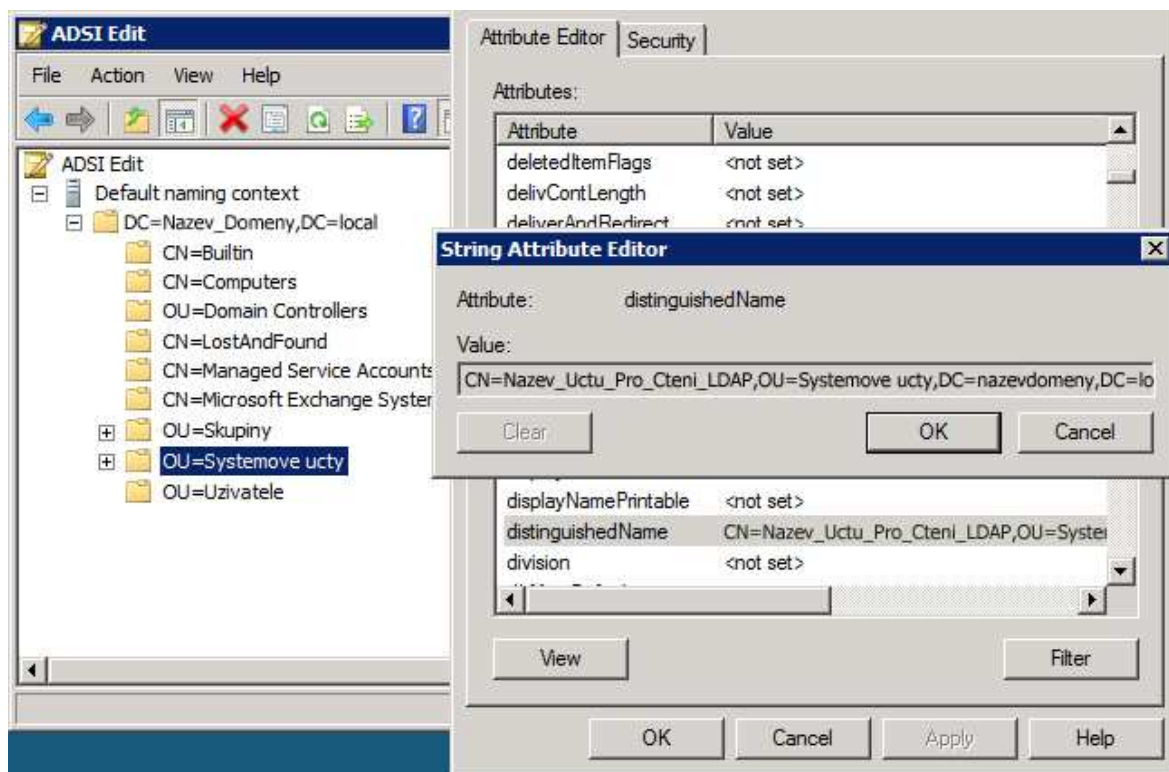
Řízení internetového přístupu má být vázáno na členství uživatele v AD skupině. Proto je nutné použít další pomocný modul, který umožní vytvářet externí ACL na základě LDAP dotazů do centrální databáze uživatelů v AD. Zavedením modulu `squid_ldap_group` (příkaz č. 169) je vytvořen externí ACL s názvem `ADGroup`, který lze využít při tvorbě pravidel. Tvar uživatelského jména, který používá LDAP (`Jmeno_Uzivatele`) je odlišný od jména, které používá Kerberos (`Jmeno_Uzivatele@REALM`). Z toho důvodu je nutné nařídit modulu, aby řetězec upravil.

Hodnoty `TTL` a `NEGATIVE_TTL` určují životnost záznamů (pozitivních i negativních) v cache a vymezují interval, po kterém bude Squid opakovat LDAP dotaz do AD. Parametrem „-R“ je zakázáno sledování „LDAP referrals“, kterými doménový řadič s LDAP dává klientovi

na vědomí, že nemá informace o požadovaném objektu a směruje klienta na server, který informace má. Toto chování není v AD doméně žádoucí.

Modul `squid_ldap_group` je jediným modulem, který umí zajistit práci s AD skupinami. Slabinou modulu v repozitáři je nemožnost práce se vnořenými skupinami – v praxi to znamená, že skupiny v AD, na základě kterých jsou ACL tvořena, musí obsahovat výčet jednotlivých uživatelů a nemohou obsahovat vnořené skupiny. V rozsáhlejší síti je vhodné použít jiný modul, který práci s vnořenými skupinami podporuje (např. [50]). Použití modulu mimo repozitář však znamená ztrátu komfortu a nutnost pravidelné kontroly dostupné verze na webu autora.

Na řádce 165 je definován základní bod, od kterého bude modul v adresářové struktuře hledat uživatele. Při práci s objekty je možné v rámci LDAP používat odkazy na DN (Distinguished Name) nebo CN (Canonical Name) objektu. DN je v LDAP adresářové struktuře jednoznačným identifikátorem objektu, zatímco CN označuje jméno objektu bez jednotlivých kontejnerů a domén. Pro zjišťování CN nebo DN účtu či skupiny z AD je nejvhodnějším nástrojem ADSI Edit. Jeho použití ilustruje Obr. 8.



Obr. 8. Použití aplikace ADSI Edit pro zjištění DN v LDAP struktuře AD.

AD nepodporuje anonymní přihlášení k LDAP, proto je nutné pomocí parametrů 166 a 167 specifikovat AD účet, který bude pro připojení použit. Tento účet musí být ošetřen doménovou politikou tak, aby měl v rámci domény minimální práva. Je vhodné dodržet požadavky na komplexnost hesla dle požadavků bezpečnostní politiky organizace a podobně jako u jiných systémových účtů zakázat expiraci hesla. Filtr na řádku 168 způsobí nahrazení proměnné „%v“ jménem ověřeného uživatele bez Kerberos realmu (parametr „-k“ na řádku 164), které je modulu předáno přes proměnnou „%LOGIN“ v příkazu č. 164. Proměnná „%a“ vkládá jméno skupiny do DN. Parametr 169 určuje, na který server bude modul LDAP dotaz směřovat. Příkaz č. 171 vytváří ACL s názvem `krb5_auth`. Vzniklé ACL bude naplněno úspěšně autentizovanými uživateli.

Další blok příkazů je uveden pro ilustraci. Konkrétní počet ACL a pravidel je závislý na bezpečnostní politice organizace. Jsou uvedeny ukázkové definice ACL se seznamy povolených/zakázaných stránek, příloh a rovněž adresy, na které nesmí být z důvodu dostupnosti přistupováno přes proxy server. Pro vyšší přehlednost je vhodné založit na každý seznam samostatný soubor, který bude načítán do ACL. U zakázaných příloh budou jednotlivé položky vyjmenovány v souboru samostatně formou regulárních výrazů (např. „\\. [Mm] [Pp] 3\$“ pro hudební soubory s koncovkou „mp3“).

Pokud je nutné řídit provoz v organizaci např. podle adresního plánu (minimálně rozdělit provoz pro serverovou infrastrukturu a uživatelské stanice), je možné definovat ACL na bázi adresních rozsahů. Ukázkové ACL pro bloky adres jsou na řádcích 179 a 180. Příkaz č. 181 ilustruje způsob tvorby externího ACL pomocí modulu `squid_ldap_group`. V rámci ukázkového externího ACL je vytvořen seznam členů z AD skupiny `Internet_Users` (dle předchozí konfigurace modulu bude ověřovat členství v LDAP pro cestu `CN=Internet_Users,OU=Skupiny,DC=Nazev_Domeny,DC=local`).

Následují vlastní pravidla pro provoz. Je zřejmé, že pro IP adresu proxy serveru (příkaz č. 183) a adresy z ACL `servery` (příkaz č. 184) není vyžadováno ověření. Na stránky a přípony definované v ACL `zakazsites` a `zakazfiles` je odepřen přístup (řádky 185 a 186).

Zařízení na IP adresách z ACL `internet_povoleno` se na web dostanou jen v případě, kdy z nich bude přistupovat autentizovaný uživatel, který je zároveň členem AD skupiny

„Internet\_Users“. Příkaz č. 188 zajistí, že vše, co nebylo do tohoto okamžiku explicitně povoleno, je zakázáno.

Příkazy č. 189-193 definují chybová hlášení, která se mají uživateli zobrazit v případě, že dojde k chybě nebo se uživatel pokusí přistoupit na zakázaný web. Obsahují názvy dříve vytvořených symlinků.

V zadání (viz 2.2) je požadována možnost zobrazení aktuálního provozu na proxy. Pro tuto funkcionalitu lze použít aplikaci SqStat, jejíž instalace bude popsána později. Aby SqStat mohl pracovat s informacemi o provozu je nutné povolit přístup do cache proxy serveru ACL pravidly č. 195 a 196.

Příkaz č. 197 je možné použít v prostředí s nadřazenou proxy, která zajišťuje centrální filtraci adres či antivirovou kontrolu obsahu. Pokud Squid využívá nadřazenou proxy je nutné zajistit, aby přes ni nesměroval požadavky na intranetové weby. To je možné vyřešit dvěma způsoby.

- Přidat intranetovou adresu do výjimek internetového prohlížeče - nastavení lze realizovat pomocí GPO (Group Policy Object).
- Upravit konfiguraci Squid - server bude umět sám vyhodnotit, zda požadavek směřuje na intranetový server nebo na Internet.

Druhá možnost je univerzálnější, proto je možné příkazem č. 177 definovat ACL `bezproxy`, které obsahuje výčet intranetových adres. Příkaz č. 199 určuje, že žádný požadavek nesmí proxy server předávat přímo na cílový server, s výjimkou ACL `bezproxy` (zajištěno příkazem č. 200). Příkaz č. 202 zkracuje ochranný interval na aktivní spojení při vypínání Squid serveru.

## 5 VÝSTUPY

Důležitou stránkou systému pro řízení a monitorování přístupu uživatelů k Internetu jsou výstupy. Je dobré mít přehled, kam uživatelé chodí a jak moc Internet využívají.

### 5.1 Logy

Jak bylo zmíněno v části 1.4, jsou logy z proxy serveru jediným důkazním materiálem v případě sporu se zaměstnancem. Záznamy v nich jsou velmi podrobné a obsahují informace o přístupech, požadavcích a odezvách serveru. Popis souborů ve výchozí konfiguraci serveru Squid zachycuje Tab. 6.

Tab. 6. Typy logů generovaných Squid3.

Název souboru	Popis
/var/log/squid3/access.log	Obsahuje záznam o všech požadavcích, zasílaných klienty na proxy server
/var/log/squid3/cache.log	Obsahuje ladící informace z běhu aplikace. Užitečná možnost ve spojení s příkazem 154.

Je zřejmé, že klíčovým zdrojem informací je soubor `access.log`. Velikost tohoto logu roste rychlostí úměrnou počtu uživatelů a intenzitě provozu. Příklad záznamu v souboru je uveden níže.

```
1346742920.979      741      192.168.4.14      TCP_MISS/200      59924      GET
http://www.touax.cz/js/yahoo/event.js      uzivatel@REALM
FIRST_UP_PARENT/Adresa_Nadrazene_Proxy application/javascript
```

Formát záznamů má pevnou strukturu. Prvním údajem je informace o datu a čase ve formátu „Unix time“, čas odezvy, IP adresa klienta. Čtvrtá část je tvořena kombinací stavu serveru se stavovým kódem HTTP, následuje velikost objektu včetně HTTP hlaviček. Šestá položkou je typ HTTP požadavku (GET, POST, PUT, DELETE). Sedmou položkou je URL, následovaná jménem uživatele (pokud je uživatel autentizován). Devátá položka udává stav hierarchie proxy serverů a jméno nadřazené proxy. Poslední položkou je typ obsahu.

Unixový formát času je vhodný pro další zpracování, není však příliš uživatelsky přívětivý. Při zobrazování logů je proto vhodné použít příkaz č. 203, který převádí hodnotu do

čitelného formátu. Příkaz lze dále kombinovat se standardními linuxovými příkazy pro zpracování textu (např. `grep`).

```
203 tail -f /var/log/squid3/access.log | perl -p -e 's/^( [0-9]* )/"[" .localtime($1)." ]"/e'
```

## 5.2 Úprava rotace logů

Klíčový význam logů vyvolává potřebu jejich archivace minimálně po dobu ochranného intervalu definovaného v požadavcích provozní bezpečnosti (viz 2.2).

Práci s logy lze ovlivnit úpravou konfiguračního souboru `/etc/logrotate.d/squid3`. Soubor upravuje chování démona `logrotate`, který má na starost veškeré systémové logy. Příkazy č. 215-222 upravují práci se souborem `cache.log`, příkazy č. 204-214 určují pravidla pro ostatní log soubory v adresáři.

Příkaz č. 205 nastavuje denní rotaci logů. Příkaz č. 206 zajistí, že starší logy budou komprimovány. Příkaz č. 207 nařizuje démonu `logrotate` udržovat historii 100 cyklů, tj. 100 dní. Příkaz `missingok` (řádek 208) nařizuje službě, aby při procesu rotace ignorovala případné chybějící soubory [51]. Příkaz č. 209 zaručí, že po provedení rotace logů nebude vznikat automaticky prázdný soubor. Nastavení v řádku 210 je důležité, pokud probíhá současně rotace více souborů vytvářených jedním démonem. Zabezpečí, že se Squid nebude restartovat po rotaci každého z nich a také to, že se blok `postrotate` (příkazy č. 211-213) provede pouze jednou. Příkaz č. 212 provádí vlastní rotaci logu [47]. Blok příkazů č. 215-222 ovlivňuje práci se souborem `cache.log`. Soubor obsahuje diagnostické informace, proto jej není nutné dlouhodobě archivovat.

Konfigurace souboru `/etc/logrotate.d/squid3` je přiložena níže.

```
204 /var/log/squid3/*.log {
205     daily
206     compress
207     rotate 100
208     missingok
209     nocreate
210     sharedscripts
211     postrotate
212         test ! -e /var/run/squid3.pid || /usr/sbin/squid3 -k
           rotate
213     endscript
```

```
214 }
215 /var/log/squid3/cache.log {
216     daily
217     compress
218     rotate 3
219     missingok
220     nocreate
221     sharedscripts
222 }
```

Konfiguraci je možné ověřit příkazem č. 223.

```
223 /usr/sbin/logrotate -d /etc/logrotate.d/squid3
```

Pokud je použita komprese starších logů, je vhodné pro vyhledávání a čtení záznamů použít příkaz č. 224. Ten lze kombinovat s příkazem č. 203.

```
224 sudo gunzip -c /var/log/squid3/access.log.1.gz | grep Hledany_Text
```

### 5.3 Instalace LightSquid

Existuje řada nástrojů pro vyhodnocování uživatelských aktivit z logu Squid serveru. Prakticky byla testována možnost použití skriptu `sarg` [52], který se nachází v repozitářích Ubuntu. Skript lze s úspěchem použít na analýzu souboru `access.log` a generování přehledných statistik. Po několikaměsíčním provozu se však řešení s využitím `sarg` ukázalo jako nepraktické z důvodu vyšších nároků na diskovou kapacitu (na pobočce s 40 uživateli Internetu za půlroku cca 3,1 GB statistik ve formátu HTML).

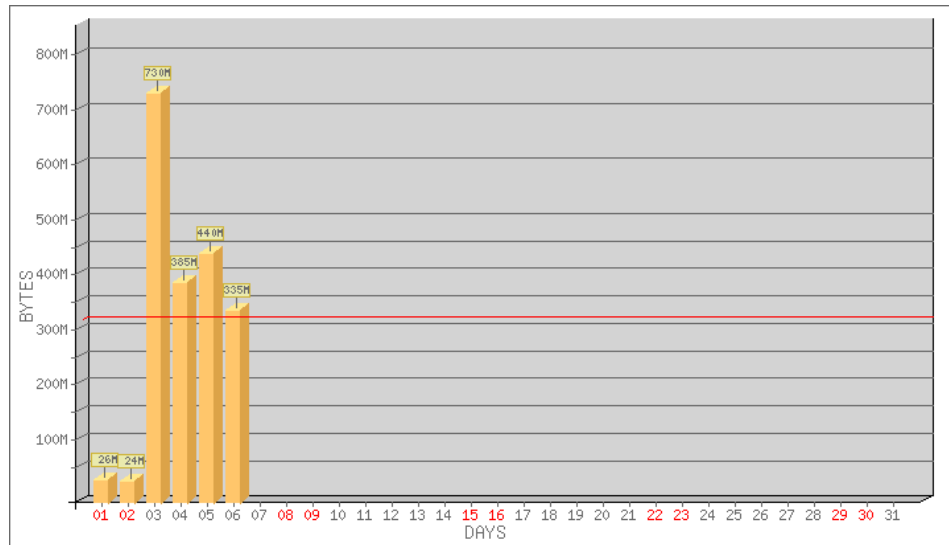
Proto bylo přistoupeno k testování skriptu `LightSquid` [53], který je provozně úspornější a pro praktické použití plně dostačující. Aplikace `LightSquid` umožňuje generovat jednoduché a úsporné statistiky včetně grafických výstupů – viz Obr. 9, Obr. 10 a Obr. 11. Skript používá rychlý parser, podporuje lokalizaci a uživatelské šablony.

Generované statistiky jsou ukládány ve formě agregovaných datových souborů a při přístupu jsou zpracovány pomocí CGI (Common Gateway Interface) skriptu do formy HTML stránky. Díky tomu je aplikace úspornější, než systém `sarg`, který nativně generuje pro každého klienta samostatnou HTML stránku. K prohlížení statistik je nutné instalovat webový server. Standardem na linuxové platformě je v tomto ohledu server Apache.

`LightSquid` je dostupný v repozitářích Ubuntu a instaluje se takto.

```
225 apt-get install lightsquid
```

Výkonná část aplikace je po instalaci umístěna v adresáři /usr/share/light squid.



Obr. 9. Ukázka měsíční statistiky z LightSquid.

**Squid user access report**

Date: 06 Sep 2012 (update :: 13:30 :: 6 Sep 2012)

[Top Sites Report](#)

[Big Files Report](#)

#	Time	User	Real Name	Connect	Bytes	%	Group
1		<a href="#">user35</a>	?	613	80.5 M	24.0%	<a href="#">?</a>
2		<a href="#">user27</a>	?	4 835	66.9 M	19.9%	<a href="#">?</a>
3		<a href="#">user07</a>	?	2 403	35.2 M	10.5%	<a href="#">?</a>
4		<a href="#">user15</a>	?	1 088	18.6 M	5.5%	<a href="#">?</a>
5		<a href="#">user12</a>	?	955	14.1 M	4.2%	<a href="#">?</a>
6		<a href="#">user31</a>	?	485	13.7 M	4.0%	<a href="#">?</a>
7		<a href="#">user01</a>	?	863	12.3 M	3.6%	<a href="#">?</a>
8		<a href="#">user10</a>	?	1 004	11.1 M	3.3%	<a href="#">?</a>
9		<a href="#">user05</a>	?	971	10.7 M	3.1%	<a href="#">?</a>
10		<a href="#">user22</a>	?	962	10.3 M	3.0%	<a href="#">?</a>
11		<a href="#">user06</a>	?	1 011	9.2 M	2.7%	<a href="#">?</a>
12		<a href="#">user16</a>	?	624	8.6 M	2.5%	<a href="#">?</a>
13		<a href="#">user14</a>	?	798	8.5 M	2.5%	<a href="#">?</a>
14		<a href="#">user03</a>	?	334	6.1 M	1.8%	<a href="#">?</a>
15		<a href="#">user18</a>	?	467	5.4 M	1.6%	<a href="#">?</a>
16		<a href="#">user24</a>	?	273	4.7 M	1.3%	<a href="#">?</a>
17		<a href="#">user25</a>	?	251	4.5 M	1.3%	<a href="#">?</a>
18		<a href="#">192.168.10.29</a>	?	131	4.2 M	1.2%	<a href="#">?</a>
19		<a href="#">user40</a>	?	426	3.3 M	0.9%	<a href="#">?</a>
20		<a href="#">user43</a>	?	168	2.0 M	0.6%	<a href="#">?</a>

Obr. 10. Ukázka denní statistiky z LightSquid.

### 5.3.1 Konfigurace LightSquid

Po instalaci není nutné konfiguraci příliš upravovat (konfigurační soubor se nachází v `/etc/lightsquid/lightsquid.conf`). Postačuje drobný zásah do konfigurace webového serveru (viz 5.7).

Přehlednost generovaných statistik je možné zvýšit drobnou úpravou souboru `/usr/share/lightsquid/tools/SiteAggregator/SiteAggregator.pl`. Tento skript umožňuje agregovat domény třetího řádu pod jednu doménu (např. `i1.site.com`, `i2.site.com` a `i3.site.com` pod doménu `site.com`).

Ukázku agregační funkce uvádí Příloha P I. Ve větší organizaci je vhodné pro jednotnou konfiguraci skriptu na pobočkách použít plánovanou úlohu, příp. subversion server. Tyto kroky nebudou v práci dále rozváděny.

### 5.3.2 Časování spouštění LightSquid

Nutným krokem je zaplánování úlohy do služby Cron tak, aby server spouštěl generování statistik v požadovaných intervalech. Cron se řídí nastavením v souboru `/etc/crontab`. Příkazem č. 238 je zajištěno generování statistik každých 30 minut. Příkaz č. 239 provede každou 39. minutu zapsání aktuálního data do log souboru a příkaz č. 240 spustí agregaci doménových záznamů skriptem `SiteAggregator.pl`.

```
226 # /etc/crontab: system-wide crontab
227 # Unlike any other crontab you don't have to run the `crontab'
228 # command to install the new version when you edit this file
229 # and files in /etc/cron.d. These files also have username fields,
230 # that none of the other crontabs do.
231 SHELL=/bin/sh
232 PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
233 # m h dom mon dow user  command
234 17 * * * * root    cd / && run-parts --report /etc/cron.hourly
235 25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-
    parts --report /etc/cron.daily )
236 47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-
    parts --report /etc/cron.weekly )
237 52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-
    parts --report /etc/cron.monthly )
238 */30 * * * * root    /usr/share/lightsquid/lightparser.pl
239 39 * * * * root    date >
    /usr/share/lightsquid/tools/SiteAggregator/SiteAggregator.log
```

```
240 40 * * * * root
usr/share/light squid/tools/SiteAggregator/SiteAggregator.pl >>
usr/share/light squid/tools/SiteAggregator/SiteAggregator.log
```

**Squid user access report**  
 User: **mprorok@navez\_domeny.local**  
 Date: **06 Sep 2012**

#	Accessed site	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Total
	Total	.	.	.	.	.	.	.	12.5	0.1	5.2	0.5	9.4	4.9	2.8	.	.	.	.	.	.	.	.	.	.	17.5 M
1	mt1.google.com	.	.	.	.	.	.	.	.	.	.	.	1.8	.	.	.	.	.	.	.	.	.	.	.	.	1.8 M
2	mt0.google.com	.	.	.	.	.	.	.	.	.	.	.	1.6	.	.	.	.	.	.	.	.	.	.	.	.	1.6 M
3	www.google.cz443	.	.	.	.	.	.	.	.	0.3	0.1	0.6	0.2	0.1	.	.	.	.	.	.	.	.	.	.	.	1.3 M
4	www.blogger.com	.	.	.	.	.	.	.	.	0.6	.	0.7	.	.	.	.	.	.	.	.	.	.	.	.	.	1.3 M
5	ssl.gstatic.com443	.	.	.	.	.	.	.	1.1	.	.	.	0.0	.	.	.	.	.	.	.	.	.	.	.	.	1.1 M
6	a.fsdn.com	.	.	.	.	.	.	.	.	.	.	.	0.8	.	.	.	.	.	.	.	.	.	.	.	.	866 368
7	rt.i.cz443	.	.	.	.	.	.	.	.	.	.	.	0.7	.	.	.	.	.	.	.	.	.	.	.	.	689 164
8	www.google.com	.	.	.	.	.	.	.	.	0.0	0.0	0.6	0.0	0.0	.	.	.	.	.	.	.	.	.	.	.	666 764
9	media.novinky.cz	.	.	.	.	.	.	.	.	0.3	.	0.3	0.0	.	.	.	.	.	.	.	.	.	.	.	.	654 533
10	radar.bourky.cz	.	.	.	.	.	.	.	.	.	.	.	0.6	.	.	.	.	.	.	.	.	.	.	.	.	637 053
11	g.denik.cz	.	.	.	.	.	.	.	0.6	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	618 367
12	mail.google.com443	.	.	.	.	.	.	.	0.4	.	0.2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	589 617
13	i1.blogs.technet.com	.	.	.	.	.	.	.	.	0.5	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	505 560
14	safebrowsing-cache.google.com	.	.	.	.	.	.	.	0.4	.	0.0	0.0	0.0	0.0	0.0	.	.	.	.	.	.	.	.	.	.	504 958
15	www.abclinuxu.cz	.	.	.	.	.	.	.	0.0	0.0	.	0.0	0.0	0.4	0.0	.	.	.	.	.	.	.	.	.	.	445 228
16	sourceforge.net	.	.	.	.	.	.	.	.	.	.	.	0.0	0.4	.	.	.	.	.	.	.	.	.	.	.	435 030
17	www.peetersonline.nl	.	.	.	.	.	.	.	.	0.4	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	417 007
18	forum.broadcom.com	.	.	.	.	.	.	.	.	0.3	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	342 434
19	profile.ak.fbcdn.net	.	.	.	.	.	.	.	0.3	.	.	.	0.0	0.0	.	.	.	.	.	.	.	.	.	.	.	337 144
20	static.sourceforge.net	.	.	.	.	.	.	.	.	.	.	.	.	.	0.3	.	.	.	.	.	.	.	.	.	.	316 943
21	intranet.brecl.vez-shu.justice.cz	.	.	.	.	.	.	0.0	0.0	0.0	.	0.2	.	.	.	.	.	.	.	.	.	.	.	.	.	308 847
22	a4.sphotos.ak.fbcdn.net	.	.	.	.	.	.	0.2	.	.	.	0.1	.	.	.	.	.	.	.	.	.	.	.	.	.	286 573
23	apis.google.com443	.	.	.	.	.	.	0.1	0.1	.	0.0	0.1	.	.	.	.	.	.	.	.	.	.	.	.	.	278 988
24	3.bp.blogspot.com	.	.	.	.	.	.	.	.	0.1	.	0.2	.	.	.	.	.	.	.	.	.	.	.	.	.	265 003
25	lightsquid.sourceforge.net	.	.	.	.	.	.	.	.	.	.	.	0.2	0.0	.	.	.	.	.	.	.	.	.	.	.	262 845
26	www.novinky.cz	.	.	.	.	.	.	.	.	0.1	.	0.1	0.1	.	.	.	.	.	.	.	.	.	.	.	.	251 821
27	img.alza.cz	.	.	.	.	.	.	.	.	.	.	.	0.2	.	.	.	.	.	.	.	.	.	.	.	.	248 173
28	maps.gstatic.com	.	.	.	.	.	.	.	.	.	.	.	0.2	.	.	.	.	.	.	.	.	.	.	.	.	247 163
29	i1-linux.softpedia-static.com	.	.	.	.	.	.	.	.	.	.	.	0.2	.	.	.	.	.	.	.	.	.	.	.	.	243 842
	Total	.	.	.	.	.	.	.	12.5	0.1	5.2	0.5	9.4	4.9	2.8	.	.	.	.	.	.	.	.	.	.	17.5 M

[LightSquid v1.8](#) (c) Sergey Erokhin AKA ESL

Obr. 11. Ukázka podrobného přehledu denní aktivity uživatele z LightSquid.

## 5.4 Instalace SqStat

SqStat je jednoduchý PHP (Hypertext Preprocessor) skript, který dokáže zobrazovat aktivní síťová připojení uživatelů na proxy serveru. Skript zobrazuje formou webového rozhraní IP adresu klienta, jméno ověřeného uživatele, seznam požadovaných URL a rychlost přenosu [54].

Použitím tohoto skriptu lze snadno identifikovat, který zdroj v síti využívá linku. Stejný problém je možné řešit z konzole pomocí utility `iptraf`, která však zobrazuje pouze IP adresu počítače.

Squid RealTime stat for the 127.0.0.1:3128 proxy server (squid/3.1.19).  
 Auto refresh:  sec.   Created at: 02:53:16 06/09/2012

Host	URI	Curr. Speed	Avg. Speed	Size	Time
<b>Total:</b> 1 users and 3 connections @ 152.11/169.58 KB/s (CURR/AVG)					
<b>172.25.47.1</b>					
	http://squidln01.nazevdomeny.local/sqstat/index.php?refresh ....			0 b	
	http://acs.pandasoftware.com/marketing/promo/IS13.exe	152.11 KB/s	169.50 KB/s	2 Mb	15s
	plus.google.com:443		0.08 KB/s	4 Kb	58s
<b>Total:</b>		152.11 KB/s	169.58 KB/s	connections @ 152.11/169.58 KB/s (CURR/AVG)	

© Alex Samorukov, 2006

```
peer=172.25.47.1:7537
me=172.25.44.30:3128
uri=http://acs.pandasoftware.com/marketing/promo/IS13.exe
bytes=2603491
seconds=15
username=mprorok@NAZEV_DOMENY.LOCAL
delay_pool=0
connection=0x7f63b0656ae8
```

Obr. 12. Výstup z aplikace SqStat ilustrující reálný provoz na proxy.

Skript lze stáhnout z domovské stránky programu a provést drobnou úpravu souboru `squid.conf` (příkazy č. 194-196). Výstup z aplikace je zachycen na Obr. 9. Pokud bude aplikace SqStat běžet na stejném serveru jako Squid, lze jej instalovat níže uvedeným způsobem.

```
241 cd /var/www
242 export http_proxy=http://194.213.41.2:8080
243 wget http://samm.kiev.ua/sqstat/sqstat-1.20.zip
244 mv sqstat-1.20 sqstat
245 rm sqstat-1.20.zip
246 mv /var/www/sqstat/config.inc.php.defaults
    /var/www/sqstat/config.inc.php
247 mv /var/www/sqstat/sqstat.php /var/www/sqstat/index.php
```

## 5.5 Instalace Apache2

V tento moment jsou na serveru připraveny dvě aplikace (SqStat a LightSquid), které pro svůj běh vyžadují webový server. Nejvhodnější volbou je Apache server verze 2. Jeho instalaci včetně Kerberos modulu a interpretu PHP lze provést standardním příkazem

```
248 apt-get install apache2 libapache2-mod-auth-kerb libapache2-mod-php5
```

Aby bylo možné zajistit autentizaci pomocí LDAP dotazů, je nutné v Apache zapnout podporu protokolu LDAP.

```
249 a2enmod ldap
250 a2enmod authnz_ldap
```

Poté je nutné provést restart Apache serveru.

```
251 service apache2 restart
```

## 5.6 Příprava indexového souboru webu

V kořenovém adresáři, který Apache používá při publikaci WWW (World Wide Web) stránek, je vhodné založit jednoduchý soubor jako rozcestník pro uživatele, kteří mají do statistik přístup.

```
252 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">
253 <html>
254 <head>
255 <title>Statistiky proxy serveru</title>
256 </head>
257 <body>
258 <h1>Statistiky proxy serveru</h1>
259 <p>- <a href="/lightsquid">lightsquid</a></p>
260 <p>- <a href="/sqstat">sqstat</a></p>
261 </body>
262 </html>
```

## 5.7 Konfigurace Apache

Všechny komponenty pro výstup a vizualizaci dat jsou připraveny. Nyní je nutné nastavit Apache tak, aby zobrazoval statistiky pouze vybraným skupinám uživatelů dle zadání (viz 2.2).

Apache podporuje řadu autentizačních mechanismů. I zde je žádoucí, aby autentizace a autorizace byla zajištěna kombinací Kerberos s LDAP dotazy. V části 4.6 byl přístup na konzoli serveru omezen na AD skupiny `_Domain Linux Admins` a `_POB01 Linux Admins`. Je vhodné, aby členové těchto skupin měli přístup i ke statistikám.

Výchozí konfigurační soubor Apache se nachází v adresáři `/etc/apache2/sites-available/default`.

```
263 LDAPCacheTTL 300
264 LDAPOpCacheTTL 300
265 <VirtualHost *:80>
266     ServerAdmin webmaster@localhost
267     DocumentRoot /var/www
268     <Directory />
269         Options FollowSymLinks
270         AllowOverride None
```

```
271 </Directory>
272 <Directory /var/www/>
273     AuthType Kerberos
274     AuthName "Pouzijte prihlaseni domenovym uctem"
275     KrbMethodNegotiate On
276     KrbMethodK5Passwd On
277     KrbAuthRealms NAZEV_DOMENY.LOCAL
278     Krb5KeyTab /etc/krb5.keytab
279     KrbLocalUserMapping On
280     AuthLDAPURL "ldap://Adresa_DC01.Nazev_Domeny.local
Adresa_DC02.Nazev_Domeny.local/DC=Nazev_Domeny,DC=local?sAMAccountName"
281     AuthLDAPBindDN "CN=Nazev_Uctu_Pro_Cteni_LDAP,OU=Systemove
ucty,DC=Nazev_Domeny,DC=local"
282     AuthLDAPBindPassword Heslo_Uzivatele_Pro_Cteni_LDAP
283     Require ldap-group CN=_Domain Linux
Admins,OU=Skupiny,DC=Nazev_Domeny,DC=local
284     Require ldap-group CN=_POB01 Linux
Admins,OU=Skupiny,DC=Nazev_Domeny,DC=local
285 </Directory>
286 Alias /lightsquid /usr/lib/cgi-bin/lightsquid
287 <Location "/lightsquid/">
288     AddHandler cgi-script .cgi
289     allow from all
290     AuthType Kerberos
291     AuthName "Pouzijte prihlaseni domenovym uctem"
292     KrbMethodNegotiate On
293     KrbMethodK5Passwd On
294     KrbAuthRealms NAZEV_DOMENY.LOCAL
295     Krb5KeyTab /etc/krb5.keytab
296     KrbLocalUserMapping On
297     AuthLDAPURL "ldap://AdresaDC01.Nazev_Domeny.local
Adresa_DC02.Nazev_Domeny.local/DC=Nazev_Domeny,DC=local?sAMAccountName"
298     AuthLDAPBindDN "CN=nazevuctuproctenildap,OU=Systemove
ucty,DC=nazevdomeny,DC=local"
299     AuthLDAPBindPassword Heslo_Uzivatele_Pro_Cteni_LDAP
300     Require ldap-group CN=_Domain Linux
Admins,OU=Skupiny,DC=Nazev_Domeny,DC=local
301     Require ldap-group CN=_POB01 Linux
Admins,OU=Skupiny,DC=Nazev_Domeny,DC=local
302 </Location>
303 ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
304 <Directory "/usr/lib/cgi-bin">
```

```
305     AllowOverride None
306     Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
307     Order allow,deny
308     Allow from all
309 </Directory>
310     ErrorLog ${APACHE_LOG_DIR}/error.log
311     LogLevel warn
312     CustomLog ${APACHE_LOG_DIR}/access.log combined
313 </VirtualHost>
```

LDAP dotazy jsou serverem uchovávány ve vyrovnávací paměti. Aby byla zajištěna provázanost proxy serveru v případě změn v AD, je příkazy č. 263-264 zkrácena doba životnosti záznamů na 5 minut [55]. Po tomto intervalu musí server dotaz na DC opakovat.

Následuje konfigurace virtuálního hostitele. Protože na serveru nebude hostován žádný jiný web, lze místo názvu hostitele použít zástupný symbol „\*“ . Příkaz č. 267 definuje cestu ke kořenovému adresáři virtuálního hostitele. Je následován řadou kontejnerových direktiv, které ovlivňují chování Apache k adresářům. Server Apache zpracovává nastavení adresářů sloučením v tomto pořadí [56]:

1. <Directory> a .htaccess (má přednost před <Directory>),
2. <DirectoryMatch> ,
3. <Files> a <FilesMatch> ,
4. <Location> a <LocationMatch> .

Vyjma <Directory> jsou všechny části zpracovávány dle pořadí v konfiguračních souborech. Pokud konfigurace obsahuje více příkazů <Directory>, jsou tyto příkazy prováděny v pořadí od nejkratší cesty po nejdelší. Je-li na adresář použito více voleb, použije se nejkonkrétnější z nich. Ve výchozím nastavení platí direktiva `Options All` pro všechny adresáře Apache, tzn., že veškeré funkce serveru jsou pro adresáře povoleny [56]. Blok příkazů č. 268-271 určuje konfiguraci Apache pro každý adresář pod `Document Root` (řádek 267). Tím je zaručeno, že adresář (a všechny podadresáře) budou mít ve výchozí konfiguraci povoleno pouze použití symbolických odkazů. Zároveň zakazuje příkazem č. 270 použití všech nastavení z `.htaccess` souboru.

V dalším <Directory> kontejneru jsou definovány přístupy pro adresář `/var/www`, ve kterém je umístěna indexová stránka (viz 5.6) a aplikace `SqStat` (viz 5.4). Příkaz č. 273 vynucuje přihlášení přes Kerberos. Pokud se nepodaří prohlížeči ověření vyjednat, je

vyžadován vstup od uživatele. Při dialogu je zobrazeno hlášení definované příkazem č. 274. Příkaz č. 275 zapíná funkci vyjednávání o Kerberos protokolu. Podpora Kerberos v prohlížeči je nezbytná z hlediska zajištění funkcionality SSO (viz 2.2). Příkaz č. 276 povoluje použití autentizace na bázi hesel pro Kerberos verze 5. Příkaz č. 277 specifikuje Kerberos realm, používaný při autentizaci uživatele. Řádek č. 278 popisuje cestu k souboru `keytab`. Protože je Squid i Apache volán klienty v SPN formátu `HTTP/HOSTNAME`, je nutné použít pro obě aplikace stejný `keytab`. Soubor musí mít dostatečná práva k tomu, aby jej mohl využívat Apache i Squid. Stejně jako při konfiguraci Squid, i zde se objevuje problém s nekompatibilními jmény (Kerberos formát `Jmeno_Uzivatele@realm` versus `Jmeno_Uzivatele` použitý LDAP) a je nutné použít direktivu na řádce 279, která odstraní z uživatelského jména část „`@realm`“.

Při autorizaci je nutné ověřit členství uživatele v AD skupině pomocí LDAP dotazu. Příkaz č. 280 specifikuje adresy DC, na které bude server LDAP dotazy směřovat. I zde je nutné dotazy autentizovat použitím konkrétního AD účtu. Je vhodné použít stejný účet jako u Squidu (viz řádky č. 166 a 167). Uživatelský účet je zadán na řádcích 281 a 282. Příkazy č. 283 a 284 obsahují DN k AD skupinám, jejichž členové mají mít přístup na statistiky.

V kontejneru `<Location>` jsou řešena nastavení a práva pro aplikaci LightSquid. LightSquid (viz 5.3) se po instalaci nachází mimo kořenový adresář webu. Pro jeho zpřístupnění je možné použít direktivu `Alias` (příkaz č. 286). Pro podporu CGI skriptů, které jsou hybnou silou LightSquidu, je nutné zapnout podporu modulu `mod_cgi` příkazem č. 288. Direktiva `AddHandler` říká Apache, jak má nakládat se skripty a jinými dynamickými prostředky. Příkaz č. 288 určuje, že se soubory v adresáři bude zacházeno jako s CGI skripty. Další příkazy definují podmínky ověření pro LightSquid.

Řádky 304-309 obsahují výchozí nastavení Apache pro adresář CGI. Příkaz č. 303 označuje adresář jako kontejner pro CGI skripty pomocí direktivy `ScriptAlias`. Pokud uživatel zavolá požadavek `http://Nazev_Serveru/cgi-bin/example.cgi`, bude Apache hledat soubor s názvem `example.cgi` v adresáři `/usr/lib/cgi-bin`. Přístup k adresářům CGI by měl být zabezpečen. Je zřejmé, že pro adresář je povoleno spouštění CGI skriptů, vypnuta podpora jazykových variant přes MultiViews a zapnuta možnost sledování symbolických odkazů, jejichž cílový soubor nebo adresář je vlastněn uživatelem se stejným ID.

## 5.8 Princip ověření na serverech Apache a Squid z webového prohlížeče

Uživatel se přihlásí k OS Windows doménovým účtem. Dojde k ověření vůči AD a získání TGT. Pokud internetový prohlížeč podporuje Kerberos a uživatel zadá libovolnou internetovou adresu, proběhne další komunikace takto:

1. prohlížeč zašle na proxy server požadavek GET nebo PUT (pokud má nastavený proxy server),
2. proxy server vrátí `Proxy-Authenticate: Negotiate`, čímž dává klientovi najevo, že je vyžadováno ověření,
3. uživatelův počítač vyžádá od KDC na doménovém řadiči „Service Ticket“ pro požadované SPN ve tvaru `HTTP/Adresa_Proxy_Serveru`. Žádost posílá jako `uzivatel@REALM`,
4. server pro PC vystaví „Service Ticket“,
5. počítač předá „Service Ticket“ proxy serveru příkazem `Proxy-Authenticate: Kerberos token` (ve formátu base64),
6. Squid s pomocí `keytab` souboru ověří platnost Kerberos ticketu,
7. proxy může LDAP dotazem zjistit, zda uživatel patří do požadované skupiny a podle toho zprostředkuje/odepře přístup.

Celý průběh ověření zachycený aplikací Wireshark ilustruje Obr. 13. Před ověřením uživatele byly z OS Windows odstraněny vystavené tikety níže uvedeným příkazem.

```
314 klist purge
```

Použitý filtr:

```
((ip.src == IP_Adresa_PC) && (ip.dst == IP_Adresa_DC)) || ((ip.src == IP_Adresa_DC) && (ip.dst == IP_Adresa_PC)) || ((ip.src == IP_Adresa_PC) && (ip.dst == IP_Adresa_Proxy)) || ((ip.src == IP_Adresa_Proxy) && (ip.dst == IP_Adresa_PC)).
```

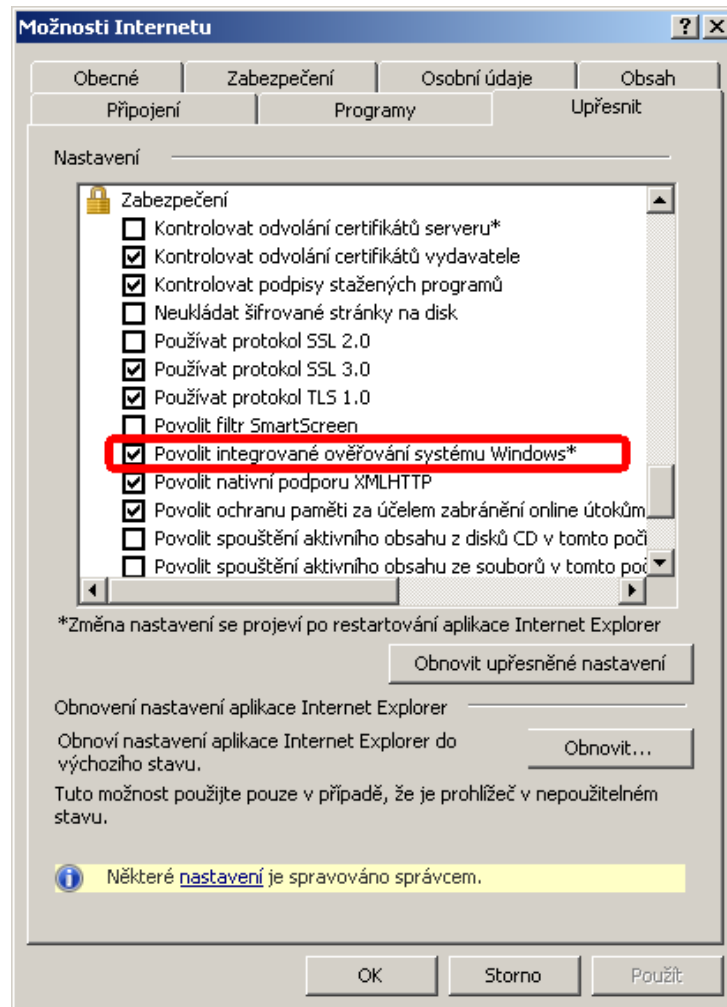
Source	Destination	Protocol	Info
172.25.47.1	172.25.44.30	HTTP	CONNECT www.czebox.cz:443 HTTP/1.1
172.25.44.30	172.25.47.1	TCP	ndl-aas > 8037 [ACK] Seq=1 Ack=90 win=14600
172.25.44.30	172.25.47.1	TCP	[TCP segment of a reassembled PDU]
172.25.44.30	172.25.47.1	TCP	[TCP segment of a reassembled PDU]
172.25.47.1	172.25.44.30	TCP	8037 > ndl-aas [ACK] Seq=90 Ack=2921 win=645
172.25.44.30	172.25.47.1	HTTP	HTTP/1.0 407 Proxy Authentication Required
172.25.47.1	172.25.44.10	TCP	8038 > kerberos [SYN] Seq=0 win=64512 Len=0
172.25.44.10	172.25.47.1	TCP	kerberos > 8038 [SYN, ACK] Seq=0 Ack=1 win=8
172.25.47.1	172.25.44.10	TCP	8038 > kerberos [ACK] Seq=1 Ack=1 win=64512
172.25.47.1	172.25.44.10	TCP	[TCP segment of a reassembled PDU]
172.25.47.1	172.25.44.10	KRB5	TGS-REQ
172.25.44.10	172.25.47.1	TCP	kerberos > 8038 [ACK] Seq=1 Ack=2119 win=642
172.25.44.10	172.25.47.1	TCP	[TCP segment of a reassembled PDU]
172.25.44.10	172.25.47.1	KRB5	TGS-REP
172.25.47.1	172.25.44.10	TCP	8038 > kerberos [ACK] Seq=2119 Ack=2301 win=
172.25.47.1	172.25.44.10	TCP	8038 > kerberos [FIN, ACK] Seq=2119 Ack=2301
172.25.44.10	172.25.47.1	TCP	kerberos > 8038 [ACK] Seq=2301 Ack=2120 win=
172.25.44.10	172.25.47.1	TCP	kerberos > 8038 [RST, ACK] Seq=2301 Ack=2120
172.25.47.1	172.25.44.30	TCP	8039 > ndl-aas [SYN] Seq=0 win=64512 Len=0
172.25.44.30	172.25.47.1	TCP	ndl-aas > 8039 [SYN, ACK] Seq=0 Ack=1 win=14
172.25.47.1	172.25.44.30	TCP	8039 > ndl-aas [ACK] Seq=1 Ack=1 win=64512
172.25.47.1	172.25.44.30	TCP	[TCP segment of a reassembled PDU]
172.25.47.1	172.25.44.30	TCP	[TCP segment of a reassembled PDU]
172.25.44.30	172.25.47.1	TCP	ndl-aas > 8039 [ACK] Seq=1 Ack=2921 win=1752
172.25.47.1	172.25.44.30	HTTP	CONNECT www.czebox.cz:443 HTTP/1.1
172.25.44.30	172.25.47.1	TCP	ndl-aas > 8039 [ACK] Seq=1 Ack=3147 win=2044
172.25.44.30	172.25.47.1	HTTP	HTTP/1.1 200 Connection established
172.25.47.1	172.25.44.30	TLSv1	Client Hello
172.25.44.30	172.25.47.1	TCP	ndl-aas > 8039 [ACK] Seq=40 Ack=3224 win=204
172.25.47.1	172.25.44.30	TCP	8037 > ndl-aas [ACK] Seq=90 Ack=3584 win=638
172.25.44.30	172.25.47.1	TLSv1	server Hello
172.25.44.30	172.25.47.1	TCP	[TCP segment of a reassembled PDU]
172.25.47.1	172.25.44.30	TCP	8039 > ndl-aas [ACK] Seq=3224 Ack=2736 win=6

Obr. 13. Autentizace uživatele na proxy zachycená aplikací Wireshark.

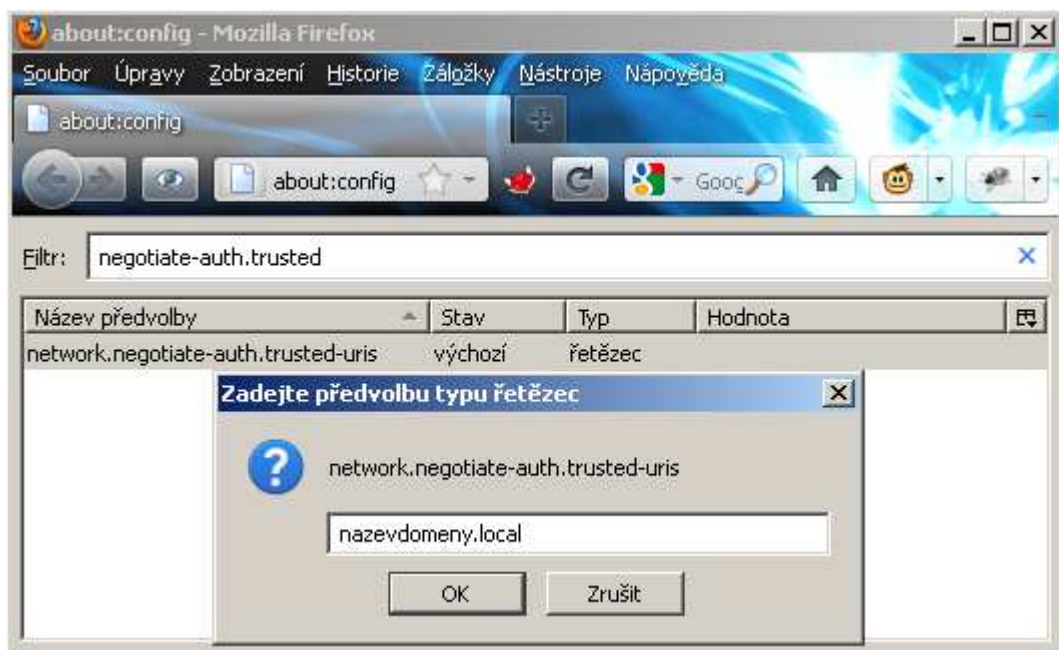
Na stejném principu autentizace funguje Apache. Protože Squid i Apache jsou volány jako služba HTTP, je nutné použít stejný keytab soubor.

Důležité podmínky pro fungování Kerbera:

1. v síti je funkční DNS (nutná podmínka),
2. proxy server má DNS záznam typu A,
3. prohlížeče z klientských stanic používají pro přístup k proxy serveru jeho FQDN (Fully Qualified Domain Name), nikoli IP adresu,
4. internetový prohlížeč podporuje Kerberos a má tuto možnost povolenu – viz Obr. 14 s nastavením Internet Exploreru a Obr. 15 s nastavením položky `network.negotiate-auth.trusted-uris` v prohlížeči Mozilla Firefox.



Obr. 14. Nastavení Internet Exploreru pro Kerberos.



Obr. 15. Nastavení Mozilla Firefoxu pro Kerberos.

## 5.9 Zálohování systému

Proxy server zpravidla není pro organizaci kritickým prvkem infrastruktury, proto postačí zálohovat logy a konfiguraci systému. V rámci práce je předpokládáno nasazení v rámci heterogenního řešení s OS Windows. Je tedy nutné připravit Linux tak, aby pro zálohu serveru bylo možné využít standardní nástroje z OS Windows.

Nejprve bude připraven adresář, kam bude ukládána záloha konfigurace. Poté bude nastaveno sdílení adresářů s využitím Samba serveru. Alternativou je připojení sdíleného adresáře z OS Windows přes `fstab` a kopírování skriptem, příp. instalace zálohovacího agenta komerčního řešení.

Systém i aplikační vybavení distribuce Ubuntu používá pro uložení konfigurace adresář `/etc`, ve kterém jsou v adresářové struktuře uloženy konfigurace jednotlivých služeb ve formě prostého textu. Je proto velmi snadné provést zálohu celého adresáře.

### 5.9.1 Zálohování konfigurace

V kořenu adresářové struktury je třeba vytvořit adresář `/_backup`.

```
315 mkdir /_backup
```

Aby bylo zajištěno, že se záloha provede v denních intervalech, je nutné v adresáři `/etc/cron.daily` vytvořit soubor `etcbbackup.sh` s níže uvedeným obsahem.

```
316 #! /bin/bash
317 echo Backup Started `date` >> /_backup/backuplog
318 mkdir /_backup/`date +%Y%m%d`
319 tar -czf /_backup/`date +%Y%m%d`/etc.tar.gz /etc
320 echo Backup Completed `date` >> /_backup/backuplog
321 for i in `find /_backup/ -maxdepth 1 -type d -mtime +30 -print`; do
    echo -e "Deleting directory $i";rm -rf $i; done
```

Příkazy č. 317 a 320 generují log o činnosti skriptu. Příkaz č. 318 vytvoří podadresář ve formátu „RokMesicDen“, do kterého příkazem č. 319 zálohuje aplikace `tar` obsah adresáře `/etc`. Příkaz č. 321 zajistí periodické čištění záloh starších než 30 dní.

Souboru `/etc/cron.daily/etcbbackup.sh` je nutné nastavit práva pro spouštění.

### 5.9.2 Sdílení adresářů přes Samba pro použití nástrojů OS Microsoft Windows

Nejjednodušší a nejefektivnější formou zálohování je použití standardních nástrojů pro zálohování OS Microsoft Windows (např. Robocopy, Windows Backup apod.).

Adresáře se zálohou konfigurace a logy serveru je vhodné sdílet prostřednictvím služby Samba. Do stávajícího souboru `/etc/samba/smb.conf`, připraveného v části 4.1, je nutno přidat dva oddíly:

```
322 [Backup]
323     comment = Adresar se zalohami
324     path = /_backup
325     read only = yes
326     valid users = @"NAZEV_DOMENY+Nazev_Skupiny"
327 [Squid]
328     comment = Adresar s logy SQUIDA
329     path = /var/log/squid3
330     read only = yes
331     valid users = @"NAZEV_DOMENY+Nazev_Skupiny"
```

Obsah obou bloků je identický, liší se pouze v adresářích, které mají být sdíleny. Příkaz č. 323 nastavuje komentář u adresáře z prostředí OS Windows. Příkaz č. 324 udává cestu ke sdílenému adresáři. Příkaz č. 325 vynucuje sdílení adresáře pouze pro čtení. Výčet uživatelských či skupinových účtů v příkazu č. 326 obsahuje seznam účtů, které budou mít k adresáři povolen přístup. Zde je vhodné použít např. skupinu `Backup Operators`, která se v prostředí OS Microsoft Windows standardně používá pro běh zálohovacích služeb. Zavináč identifikuje doménovou skupinu, použitý oddělovač musí korespondovat s nastavením Samby (viz příkaz č. 48).

Po restartu služby Samba je nutné sdílené adresáře zahrnout do plánu zálohování.

## 5.10 Možnosti dalšího rozvoje řešení

Dosavadními kroky instalace a konfigurace byl získán systém, který zajišťuje plnou funkcionalitu v rámci definovaného zadání. Jediným bodem, který se dosud nepodařilo zajistit, je webová správa. Ta je jedním z rozvojových témat uvedených v této části.

### 5.10.1 Antivirová ochrana

Bude-li organizací požadována antivirová kontrola internetového provozu, je možné na serveru použít příslušnou aplikaci z repozitáře (např. balíček SquidClamav [57], který poskytuje možnost plné kontroly HTTP provozu).

Pokud by měl být server rozšířen o antivirovou aplikaci, je nutné tuto skutečnost zohlednit ve formě vyšších nároků na hardware serveru. V rozsáhlejší síti s více pobočkami je efektivnější, zejména s ohledem na systémové zdroje, řešit ochranu použitím centrálního rodičovského proxy serveru s antivirovým softwarem.

### 5.10.2 SquidGuard

Možnost filtrace dle strukturovaného seznamu nevhodných stránek (blacklist) je skvělou možností, jak funkcionalitu řešení rozšířit. Tento typ ochrany není stoprocentní a může se stát i zdrojem problémů (např. pokud se do seznamu dostane neškodná adresa). Je však mocným nástrojem, který pomůže škálovat pravidla internetového provozu v organizaci.

Z dostupného OSS se nejvíce osvědčila aplikace SquidGuard. V repozitářích Ubuntu 12.04 se nachází SquidGuard verze 1.4, který bohužel neobsahuje podporu LDAP. Funkcionalita je zahrnuta až od verze 1.5. Tato verze SquidGuardu je obsažena v Ubuntu verze 12.10 (Quantal), která je v době vzniku této práce teprve ve vývoji. Také verze 1.5 má jedno zásadní omezení – při použití Kerberos autentizace nelze odstranit z uživatelského jména `realm`, což je nutná podmínka fungování v rámci modelu SSO (nosná myšlenka celého řešení). Problém je možné řešit pomocí patche na zdrojový kód aplikace. Autorem opravy ve formátu `diff` v archivu mailové konference SquidGuard [58] je Mathieu Parent. Pro kompilaci SquidGuard ze zdrojových kódů je nutné nejprve zkompileovat databázové knihovny Berkeley, které bohužel nejsou v repozitáři použité distribuce k dispozici. Po kompilaci je vhodné vytvořit standardní APT balíček, který lze využít k jednoduché instalaci dalších proxy serverů v síti. Oprava rozšiřuje možnosti konfigurace aplikace o parametry `stripntdomain` a `striprealm`. Pomocí těchto parametrů je možné ovlivnit zpracování části `realm` v aplikaci SquidGuard.

Při LDAP dotazech na členství účtů v AD skupinách je v konfiguraci SquidGuardu nutné využívat hexa kódy ASCII znaků v LDAP DN (místo středníku kód `%2c`, místo mezery `%20` apod.). SquidGuard se do Squidu zavádí jako tzv. `url_rewrite_program`. Funguje tak, že

dle nastavených pravidel prochází databázi stránek a pokud najde shodu, nahradí URL jinou adresou dle konfigurace.

Na Internetu je dostupná řada blacklistů. S úspěchem lze použít např. Shalla Blacklist [59], který obsahuje cca 1,7 miliónu URL v desítkách kategorií. Jednoduše lze připravit skript pro pravidelnou aktualizaci blacklistu.

### 5.10.3 Webmin

Zkušenosti z praxe ukazují, že nutnost použití linuxové konzole nese mnoho administrátorů OS Microsoft Windows nelibě. Pokud standardní postupy typu centrální definice pravidel, vytvoření AD skupin a metodika zařazení uživatelů pro implementaci řešení nedostačuje, je možné použít pro správu pravidel aplikaci Webmin [60]. Jedná se o oblíbenou aplikaci, která prostřednictvím webového rozhraní poskytuje možnost plné konfigurace linuxového systému. Webmin obsahuje řadu rozšíření včetně modulů pro Squid, Apache či SquidGuard.

Jeho použití je však diskutabilní. Pro správu je vždy lepší použít standardní cestu editace přes konzoli, která poskytuje plnou kontrolu nad zásahy do konfigurace a lepší podporu při jejím ladění. Použitím softwaru Webmin lze naplnit poslední bod zadání (viz 2.2).

Webmin obsahuje vlastní server. Při integraci do stávajícího řešení je vhodné publikovat interní server Webminu přes server Apache pomocí reverzní proxy. Využití reverzní proxy umožňuje využít podmíněný přístup, podobně jako u statistik a reportů (viz 5.7).

### 5.10.4 NTOP

Pokud bude nahrazen komerční produkt pomocí Squidu, příp. bude role routeru či firewallu přenesena na jiný prvek sítě, mohou správčům chybět podrobnější informace o síťovém provozu.

Chybějící mezeru lze snadno vyplnit použitím aplikace NTOP [61]. Ta umožňuje sbírat data ze síťové karty i okolních zařízení (např. z routeru Mikrotik) a generovat přehledné reporty. Na základě zkušeností z provozu lze subjektivně hodnotit, že generované reporty jsou užitečnější než v případě použití Kerio Winroute.

Také NTOP má vlastní webový server, který je vhodné publikovat přes reverzní proxy a získat tak jednotný nástroj řízení přístupu k rozhraní kombinací Kerberos a LDAP dotazů.

### 5.10.5 Firewall

V zadání bylo určeno, že na proxy serveru nemusí běžet firewall. V případě potřeby je však možné použít proxy server jako firewall (např. jako záložní řešení pro případ výpadku síťového prvku, který tuto roli plní).

Nutným krokem je přidání další síťové karty a konfigurace `iptables` pro Netfilter v jádře OS.

## ZÁVĚR

Je zřejmé, že s využitím otevřeného softwaru lze v prostředí Active Directory vytvořit funkční a účinné řešení k regulaci a zabezpečení internetového provozu v organizaci. V praxi je bezpečnost obvykle řešena jako kompromis mezi tím, co organizace chce a co si může dovolit. Otevřený software nabízí dostupné řešení provozní bezpečnosti v oblasti internetového provozu širokému okruhu firem a organizací.

Pro řešení byla použita otevřená linuxová distribuce s proxy serverem Squid. Linuxový server byl plně integrován s prostředím Active Directory. Kombinací autentizace Kerberos protokolem s autorizací Lightweight Directory Access Protocol (LDAP) bylo docíleno synergického efektu v podobě softwarového řešení s jednoduchou administrací, dostatečnou flexibilitou a přehledným reportingem, včetně možnosti konfigurace a zálohování z prostředí Microsoft Windows.

Podarilo se vytvořit systém, který splňuje všechny parametry zadání. Jako primární zdroj dat je použita databáze Active Directory. Pro správu serveru, řízení přístupu k internetu a reporting lze plně využít víceúrovňový model rolí, založený na doménových skupinách. Při použití internetových prohlížečů podporujících ověření Kerberos, nepředstavuje použití heterogenního řešení dodatečnou zátěž pro uživatele ani správce, neboť vše probíhá s využitím mechanismu Single Sign On.

Server Squid nabízí pokročilé možnosti filtrování. Kombinací s aplikací SquidGuard lze filtrování rozšířit a lépe škálovat definicí konkrétních kategorií internetových stránek. Další rozvoj je možný v oblasti antivirové kontroly obsahu, možnosti webové konfigurace linuxového serveru s použitím aplikace Webmin či sledování síťových toků na aktivních prvcích sítě pomocí aplikace NTOP. Výčet možností využití otevřeného softwaru v doménovém prostředí tím zdaleka nekončí a je zřejmé, že kombinace Linuxu s prostředím Microsoft Windows má v oblasti bezpečnosti co nabídnout, zejména s ohledem na cenu řešení.

Nezbytnou součástí cyklu budování informační bezpečnosti je kontrola. Proto byly v rámci řešení zahrnuty přehledné reporty s možností archivace přístupových logů dle parametrů bezpečnostní politiky organizace. Vše s použitím internetového prohlížeče, příp. standardních nástrojů prostředí Microsoft Windows.

Popsané řešení je stabilní, široce využitelné a snadno přenositelné. Nevyžaduje dodatečné náklady na pořízení a provoz, lze je snadno zdokumentovat a popsat.

Přes nesporné ekonomické výhody je nutno uvážit i slabé stránky – v dotazech do Active Directory není možno používat vnořené skupiny, použití aplikace SquidGuard je možné jen po úpravě zdrojového kódu a kompilaci. Popsané problémy generují vyšší časovou náročnost při nasazení systému, jsou však řešitelné. Neřešitelnou slabinou systému je fakt, že spojení Linuxu a Windows je odkázáno na standardy v rámci uzavřeného produktu. V rámci implementace je proto nutné, aby vedení organizace stanovilo jasná pravidla, nezávisle na produktu, který je jako proxy využíván. Jen tak je možné v případě potřeby realizovat operativní přechod na jiný produkt s podporou Active Directory bez nutnosti zásahů do bezpečnostního modelu.

## CONCLUSION

It is obvious that it is possible to create a dynamic and effective Active Directory environment solution to regulation and security of Internet traffic in a company, making use of open-source software. In practice, Internet security is usually achieved as a compromise between what the company wants, and what it can afford. Open source offers solutions to operational safety available to a wide range of companies and organizations.

The solution makes use of open Linux distribution with proxy server named Squid. The Linux server was fully integrated with the Active Directory environment. A synergic effect in the form of a software solution with simple administration, sufficient flexibility and lucid reporting, including the options to configure and backup from the Microsoft Windows environment, was achieved by combining authentication protocol Kerberos with Lightweight Directory Access Protocol (LDAP) authorization.

The author has managed to create a system that meets all requirement parameters as listed in Chapter 2.2. Active Directory database is used as a primary data source. A multi-level role model based upon domain groups can be used for server administration, Internet access management, and reporting. Using Kerberos authentication supporting web browsers, the heterogenous solution does not involve additional load neither for the user, nor the administrator, as everything runs on the Single Sign On mechanism.

A Squid server provides advanced filtering options. By combining it with the application SquidGuard it is possible to expand and scale filtering, and to define particular web page categories in a more efficient way. Further development is possible in the fields of antivirus content control, web configuration of the Linux server using the application Webmin, or network flow monitoring on networking hardware by means of using the application NTOP. The possibilities provided by using open-source software in a domain environment are very broad and it is apparent that the combination of Linux and Microsoft Windows has a lot to offer, especially considering the price of such solutions.

Another essential part of building an information security is control. Therefore synoptic reports with the option to archive access logs according to an organization's security policy are included in the solution, making use of no more than a web browser or, in case of need, Microsoft Windows environment's standard tools.

The described solutions is steady, broadly usable, and easily portable. It does not require additional purchase or operating costs, and is easy to document and/or render.

In spite of the indisputable economic benefits it is necessary to consider the solution's weak points as well: in Active Directory requests it is impossible to use enumerate groups, the use of SquidGuard is only possible after editing source code and compilation. The above mentioned problems generate lengthier system set-up, yet can be solved. An insoluble weakness of the system is the fact that the integration of Linux and Windows is restricted by the standards within the framework of a closed product. Therefore in the process of implementation it is necessary for the organization's executives to determine detailed rules independently of the type of product used as a proxy. In case of need it is the only way to launch an operative transition to a different Active Directory compatible product without the need to interfere with the security model.

**SEZNAM POUŽITÉ LITERATURY**

- [1] ROITER, Neil. Přichází nová generace firewallů. *Security World: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2011, roč. 2011, č. 4, s. 2-12. ISSN 1802-4505.
- [2] CISCO SYSTEMS. Pravidla pro bezpečnou práci s IT je potřeba uzpůsobit současným potřebám: Studie Cisco. *Cisco Systems, Inc.* [online]. Praha: 2012, 5. ledna 2012 [cit. 2012-06-15]. Dostupné z:  
<http://www.cisco.com/web/CZ/about/news/2012/20120105.html>
- [3] CISCO SYSTEMS. Cisco Connected World Technology Report. *Cisco Systems, Inc.* [online]. San Jose: 2011 [cit. 2012-06-15]. Dostupné z:  
<http://www.cisco.com/en/US/netsol/ns1120/index.html>
- [4] BARTOŠOVÁ, Veronika. *Psychologické aspekty zneužívání internetu na pracovišti*. Praha, 2011. Bakalářská práce. Vysoká škola ekonomická v Praze. Dostupné z: [https://isis.vse.cz/zp/portal\\_zp.pl?podrobnosti=94622](https://isis.vse.cz/zp/portal_zp.pl?podrobnosti=94622)
- [5] MATUŠKOVÁ, Lenka. *Monitoring a kontrola zaměstnanců na pracovišti z hlediska etiky*. Brno, 2011. Bakalářská práce. Masarykova univerzita v Brně. Dostupné z: [http://is.muni.cz/th/251527/ff\\_b/](http://is.muni.cz/th/251527/ff_b/)
- [6] COLINS, Nick. Twitter 'costs British economy £1.38bn'. *The daily telegraph* [online]. 2009, 26 Oct 2009 [cit. 2012-06-15]. ISSN 0307-1235. Dostupné z:  
<http://www.telegraph.co.uk/technology/twitter/6418567/Twitter-costs-British-economy-1.38bn.html>
- [7] ČESKÝ STATISTICKÝ ÚŘAD. Průměrné mzdy - 1. čtvrtletí 2012: Průměrná mzda reálně poklesla o 0,1 %. *Český statistický úřad* [online]. 2012 [cit. 2012-06-27].  
Dostupné z: <http://www.czso.cz/csu/csu.nsf/informace/cpmz060712.doc>
- [8] MAFRA. Kalkulátor čisté mzdy v roce 2012. *IDNES.cz* [online]. 2012 [cit. 2012-06-27].  
Dostupné z: [http://kalkulacky.idnes.cz/cr\\_kalkulator-ciste-mzdy-2012.php](http://kalkulacky.idnes.cz/cr_kalkulator-ciste-mzdy-2012.php)

- [9] AMERICAN MANAGEMENT ASSOCIATION. 2007 Electronic Monitoring & Surveillance Survey: Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse. *AMA – American Management Association* [online]. 2008, February 28, 2008 [cit. 2012-06-18]. Dostupné z: <http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/>
- [10] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. 1. vyd. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.
- [11] ŠTĚDRONĚ, Bohumír a Miroslav LUDVÍK. *Právo v informačních technologiích*. 1. vyd. Kralice na Hané: Computer Media, 2008, 132 s. ISBN 978-808-6686-363.
- [12] ČESKO. Zákon č. 89/2012 Sb.: Občanský zákoník. In: *Sbírka zákonů*. 2012, částka 33.
- [13] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Stanovisko č. 6/2009: Ochrana soukromí při zpracování osobních údajů. *ÚOOÚ: Úřad pro ochranu osobních údajů* [online]. 2009 [cit. 2012-06-21]. Dostupné z: [http://www.uoou.cz/files/stanovisko\\_2009\\_6.pdf](http://www.uoou.cz/files/stanovisko_2009_6.pdf)
- [14] ČESKO. Zákon č. 262/2006 Sb.: Zákoník práce. In: *Sbírka zákonů*. 2006, částka 84.
- [15] KOPECKÝ, Josef. Kvůli šmírování mailů za Dobeše dává odvolaný úředník trestní oznámení. *IDNES.cz* [online]. Praha: MAFRA, 2011, 24. února 2011 [cit. 2012-02-22]. ISSN 1210-1168. Dostupné z: [http://zpravy.idnes.cz/kvuli-smirovani-mailu-za-dobese-dava-odvolany-urednik-trestni-oznameni-1ny-/domaci.aspx?c=A110224\\_114059\\_domaci\\_kop](http://zpravy.idnes.cz/kvuli-smirovani-mailu-za-dobese-dava-odvolany-urednik-trestni-oznameni-1ny-/domaci.aspx?c=A110224_114059_domaci_kop)
- [16] ČESKO. RADA VLÁDY PRO LIDSKÁ PRÁVA. Usnesení Rady vlády pro lidská práva ze dne 18. června 2009: k zajištění respektování odpovídajícího soukromí zaměstnanců na pracovišti. *Vláda ČR: Rada vlády pro lidská práva* [online]. Praha, 2009, 5 s. [cit. 22. 2. 2012]. Usnesení Rady vlády pro lidská práva. Dostupné z: <http://www.vlada.cz/assets/ppov/rlp/cinnost-rady/zasedani-rady/Podnet-k-soukromi-zamestnancu-na-pracovisti.pdf>

- [17] JANSA, Lukáš. Kontrola zaměstnance při výkonu práce s počítačem. *Právo IT* [online]. 2009, 15. 3. 2007 [cit. 2012-02-22]. Dostupné z: <http://www.pravoit.cz/article/kontrola-zamestnance-pri-vykonu-prace-s-pocitacem>
- [18] JANSA, Lukáš. Způsob kontroly zaměstnanců dle nového zákoníku práce. *Právo IT* [online]. 2007, 24. 5. 2007 [cit. 2012-06-20]. Dostupné z: <http://www.pravoit.cz/article/zpusoby-kontroly-zamestnancu-dle-noveho-zakoniku-prace>
- [19] PETERKA, Jiří. Principy firewallů. *eArchiv.cz: archiv článků a přednášek Jiřího Peterky* [online]. 2011 [cit. 2012-06-29]. Dostupné z: <http://www.earchiv.cz/b01/b0100020.php3>
- [20] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2. přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.
- [21] KERIO TECHNOLOGIES. Koupit Kerio Control. *Kerio Technologies*. [online]. 2011 [cit. 2012-07-16]. Dostupné z: <http://www.kerio.cz/cz/control/buy>
- [22] ČESKÝ STATISTICKÝ ÚŘAD. Využívání informačních a komunikačních technologií v podnikatelském sektoru, obsah. *Český statistický úřad* [online]. 2011, 30. 12. 2011 [cit. 2012-07-16]. Dostupné z: <http://www.czso.cz/csu/2011edicniplan.nsf/p/9702-11>
- [23] WELSH, Matt. *Používáme Linux*. 2. vyd. Praha: Computer Press, 1997, 612 s. ISBN 80-7226-001-4.
- [24] ČESKÉ SDRUŽENÍ UŽIVATELŮ OS LINUX. Oficiální stránky o Debianu v České republice. *Debian.cz* [online]. 2012 [cit. 2012-07-20]. Dostupné z: <http://debian.cz/>
- [25] KOZUB, Martin. O Ubuntu. *Ubuntu* [online]. 2012 [cit. 2012-07-20]. Dostupné z: <http://www.iubuntu.cz/index.php?site=5>
- [26] KENNEDY, Alan. A database of open-source HTTP proxies. *Xhaus.com: information technology consultants* [online]. ©2000-2010 [cit. 2012-07-19]. Dostupné z: <http://proxies.xhaus.com/>

- [27] ACME LABORATORIES. Micro\_proxy: really small HTTP/HTTPS proxy. *Acme Laboratories* [online]. 2012 [cit. 2012-07-20]. Dostupné z: [http://www.acme.com/software/micro\\_proxy/](http://www.acme.com/software/micro_proxy/)
- [28] OESTERHELT, Andreas. Privoxy: Home Page. *Privoproxy* [online]. ©2001-2013 [cit. 2012-07-20]. Dostupné z: <http://www.privoxy.org/>
- [29] CABRITA, Daniel. ZipProxy: the HTTP traffic compressor. *Sourceforge* [online]. 2012 [cit. 2012-07-20]. Dostupné z: <http://zipproxy.sourceforge.net/index.html>
- [30] WESSELS, Duane. Squid: Optimising Web Delivery. *Squid-cache.org* [online]. 2012 [cit. 2012-07-20]. Dostupné z: <http://www.squid-cache.org>
- [31] WESSELS, Duane. Squid FAQ: About Squid. *Squid-cache.org* [online]. 2011, 2011-07-05 [cit. 2012-07-20]. Dostupné z: <http://wiki.squid-cache.org/SquidFaq/AboutSquid>
- [32] ACME CONSULTING. Squid 3 for Windows. *Squid 3* [online]. 2009 [cit. 2012-07-20]. Dostupné z: <http://squid.acmeconsulting.it/Squid3.html>
- [33] CANONICAL. Ubuntu: Root sudo. *Ubuntu Česko: Wiki* [online]. 2012 [cit. 2012-07-24]. Dostupné z: <http://wiki.ubuntu.cz/Root%20sudo>
- [34] VMWARE. VMware KB: Overview of VMware Tools. *Vmware* [online]. 2012, 16. 7. 2012 [cit. 2012-07-23].  
Dostupné z:  
[http://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=340](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=340)
- [35] SMITH, Roderick W. *Linux ve světě Windows: průvodce administrátora heterogenních sítí*. 1. vyd. Praha: Grada, 2006, 443 s. ISBN 80-247-1470-1.
- [36] SOFTWARE FREEDOM CONSERVANCY. Smb.conf. *Samba: Opening Windows to a Wider World* [online]. 2012 [cit. 2012-07-30]. Dostupné z: <http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html>
- [37] THE INTERNET ENGINEERING TASK FORCE. The Simple and Protected GSS-API Negotiation Mechanism: Request for Comments: 2478. *The Internet*

- Engineering Task Force* [online]. 1998 [cit. 2012-08-03]. Dostupné z: <http://www.ietf.org/rfc/rfc2478.txt>
- [38] EISENKOLB, Kerstin. *Bezpečnost windows 2000/XP*. 1. vyd. Praha: Computer Press, 2003, 501 s. ISBN 80-7226-789-2.
- [39] MICROSOFT CORPORATION. Microsoft Kerberos (Windows).. *Microsoft Developer Network* [online]. 2012, 20. 7. 2012 [cit. 2012-08-27]. Dostupné z: <http://msdn.microsoft.com/en-us/library/aa378747%28v=vs.85%29>
- [40] BOUŠKA, Petr. Kerberos protokol a Single sign on. *Samuraj-cz.com* [online]. 2010, 15. 09. 2010 [cit. 2012-08-27]. Dostupné z: <http://www.samuraj-cz.com/clanek/kerberos-protokol-a-single-sign-on/>
- [41] MICROSOFT CORPORATION. Changes in Kerberos Authentication: Windows Server. *TechNet: Resources and Tools for IT Professionals* [online]. 2012 [cit. 2012-08-01]. Dostupné z: <http://technet.microsoft.com/cs-cz/library/dd560670%28v=ws.10%29.aspx>
- [42] MASSACHUSETTS INSTITUTE OF TECHNOLOGY. Obtaining Tickets with kinit: Kerberos V5 UNIX User's Guide. *Kerberos V5 UNIX User's Guide* [online]. ©1985-2007 [cit. 2012-08-01]. Dostupné z: <http://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-user/Obtaining-Tickets-with-kinit.html>
- [43] RJ SYSTEMS. PAM configuration guide for Debian. *RJ Systems: Linux System Administration* [online]. 2012, 21. 6. 2012 [cit. 2012-08-07]. Dostupné z: <http://www.rjsystems.nl/en/2100-pam-debian.php#deb6>
- [44] POLLOCK, Wayne. PAM Tutorial: Using PAM to set security policies. *Hillsborough Community College* [online]. 2012, 8. 7. 2012 [cit. 2012-08-07]. Dostupné z: <http://content.hccfl.edu/pollock/AUnix2/PAM-Help.htm>
- [45] HONTAÑÓN, Ramón J. *Linux: praktická bezpečnost*. 1. vyd. Praha: Grada, 2003, 438 s. ISBN 80-247-0652-0.
- [46] NOVELL. Chapter 5: Active Directory Support. *SUSE Linux Enterprise Server Security Guide* [online]. 2012, 25. 7. 2012 [cit. 2012-08-06]. Dostupné z: [http://doc.opensuse.org/products/draft/SLES/SLES-security\\_sd\\_draft/cha.ad.html](http://doc.opensuse.org/products/draft/SLES/SLES-security_sd_draft/cha.ad.html)

- [47] SAINI, Kulbir. *Squid Proxy Server 3.1: beginner's guide*. Birmingham (United Kingdom): Packt Open Source Pub., ©2011, 308 p. ISBN 978-1-849513-90-6.
- [48] WESSELS, Duane. *Squid: the definitive guide*. 1st ed. Sebastopol (California): O'Reilly, ©2004, 441 p. ISBN 978-0-596-10364-4.
- [49] MICROSOFT CORPORATION. Authentication failure from non-Windows NTLM or Kerberos servers. *Technická podpora: Microsoft Online* [online]. 2011 [cit. 2012-08-31]. Dostupné z: <http://support.microsoft.com/kb/976918/en>
- [50] MOELLER, Markus. Squid Kerberos Authentication Helper. *SourceForge.net* [online]. 2012 [cit. 2012-09-03]. Dostupné z: <http://sourceforge.net/projects/squidkerbauth/>
- [51] TURNBULL, James. *Hardening Linux*. New York: Springer-Verlag, ©2005, 552 p. ISBN 15-905-9444-4.
- [52] SARG COMMUNITY. Squid Analysis Report Generator. *Sourceforge* [online]. 2010 [cit. 2012-08-09]. Dostupné z: <http://sarg.sourceforge.net/sarg.php>
- [53] EROKHIN, Sergey. LightSquid. *SourceForge* [online]. 2010 [cit. 2012-08-09]. Dostupné z: <http://sourceforge.net/projects/lightsquid/>
- [54] SAMORUKOV, Alex. SqStat 1.20. *@samm.kiev.ua* [online]. 2012 [cit. 2012-09-07]. Dostupné z: <http://samm.kiev.ua/sqstat/>
- [55] THE APACHE SOFTWARE FOUNDATION. Apache Module mod\_ldap. *Apache: HTTP Server Project* [online]. 2012 [cit. 2012-08-13]. Dostupné z: [http://httpd.apache.org/docs/2.2/mod/mod\\_ldap.html#ldapopcachettl](http://httpd.apache.org/docs/2.2/mod/mod_ldap.html#ldapopcachettl)
- [56] AULDS, Charles. *Linux: administrace serveru Apache*. 1. vyd. Praha: Grada, 2003, 535 s. ISBN 80-247-0640-7.
- [57] DAROLD, Gilles. SquidClamav: Securing Web Delivery. *SquidClamav* [online]. ©2005-2012 [cit. 2012-10-10]. Dostupné z: <http://squidclamav.darold.net/>
- [58] PARENT, Mathieu. Squidguard: Stripping NT domain name or Kerberos Realm from user name. In: *Squidguard Private Archives Mailing List* [online]. 2010 [cit. 2012-10-10]. Dostupné z: <http://www.shalla.de/mailman/private/squidguard/2010-December/001896.html>

- [59] KRONBERG, Christine. Shalla Secure Services. *Shalla's Blacklists* [online]. ©2007-2011 [cit. 2012-10-10]. Dostupné z: <http://www.shallalist.de/>
- [60] CAMERON, Jameson. What is Webmin? *Webmin* [online]. 2012 [cit. 2012-10-10]. Dostupné z: <http://www.webmin.com/>
- [61] DERI, Luca. Ntop: Traffic analysis with NetFlow™ and sFlow™ support. *Ntop*. [online]. 2012 [cit. 2012-11-28]. Dostupné z: <http://www.ntop.org/products/ntop/>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

ACL	Access Control List
AMA	American Management Association
AMD	Advanced Micro Devices, Inc.
API	Application Programming Interface
Apod.	A podobně
AS	Authentication Server
ASPI	Automatizovaný systém prvních informací
BSD	Berkeley Software Distribution
CGI	Common Gateway Interface
CIFS	Common Internet File System
CN	Canonical Name
CPU	Central Processor Unit
Č.	Číslo
ČR	Česká republika
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name Service
E-mail	Elektronická pošta
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
GB	Gigabyte
GID	Group Identifier
GPO	Group Policy Object

---

HDD	Hard Disk Drive
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
ICQ	I Seek You
ICT	Information and Communication Technologies
ID	Identifikátor
Inc.	Incorporated
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Informační technologie
IWA	Integrated Windows Authentication
Kč	Korun českých
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LTS	Long Time Support
MB	Megabyte
MIT	Massachusetts Institute of Technology
Např.	Například
NetBIOS	Network Basic Input Output System
NSS	Name Service Switch
NTLMSSP	NT LAN Manager Security Support Provider
NTLM	NT LAN Manager
NTP	Network Time Protocol
Obr.	Obrázek

---

Odst.	Odstavec
OS	Operační systém
OSS	Open source software
OSI	Open Systems Interconnection
PAM	Pluggable Authentication Modules
PC	Personal Computer, osobní počítač
PHP	Hypertext Preprocessor
Prům.	Průměrná
Příp.	Případně
PTR	Pointer Record
QoS	Quality of Service
RAM	Random Access Memory
RODC	Read only Domain Controller
RPC	Remote Procedure Call
Ř.	Řádek
Sb.	Sbírky
SCP	Secure Copy Protocol
SID	Security Identifier
SMB	Server Message Block
SOCKS	Socket Secure
SPN	Service Principal Name
SPNEGO	Simple and Protected GSSAPI Negotiation Mechanism
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign On

---

Tab.	Tabulka
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TGS	Ticket-Granting Service
TGT	Ticket-Granting Ticket
Tj.	To jest
Tzn.	To znamená
Tzv.	Tak zvaný
UDP	User Datagram Protocol
UID	Unique Identification Number
UID	Unique Identifier
URL	Uniform Resource Locator
Ust.	Ustanovení
UTF	UCS Transformation Format
WAN	Wide Area Network
WWW	World Wide Web

**SEZNAM OBRÁZKŮ**

Obr. 1. Princip fungování proxy serveru.....	22
Obr. 2. Vytvoření DNS záznamu typu A.....	33
Obr. 3. Nastavení aplikace Putty.....	34
Obr. 4. Princip Kerberos autentizace [40]. ....	46
Obr. 6. Obsah keytab souboru.....	50
Obr. 7. Možnosti komunikace OS Linux s AD [46].....	56
Obr. 8. Použití aplikace ADSI Edit pro zjištění DN v LDAP struktuře AD.....	61
Obr. 9. Ukázka měsíční statistiky z LightSquid.....	67
Obr. 10. Ukázka denní statistiky z LightSquid. ....	67
Obr. 11. Ukázka podrobného přehledu denní aktivity uživatele z LightSquid.....	69
Obr. 12. Výstup z aplikace SqStat ilustrující reálný provoz na proxy.....	70
Obr. 13. Autentizace uživatele na proxy zachycená aplikací Wireshark. ....	76
Obr. 14. Nastavení Internet Exploreru pro Kerberos. ....	77
Obr. 15. Nastavení Mozilla Firefoxu pro Kerberos. ....	77

**SEZNAM TABULEK**

Tab. 1. Náklady zaměstnavatele na nepracovní internetové aktivity zaměstnanců. ....	15
Tab. 2. Internetové aktivity, které vedou k rozvázání pracovního poměru [9]. ....	16
Tab. 3. Cena komerčního řešení pro organizaci [21]. ....	26
Tab. 4. Hardwarová konfigurace pro proxy server. ....	30
Tab. 5. Umístění aplikace Squid v systému. ....	57
Tab. 6. Typy logů generovaných Squid3. ....	64

## SEZNAM PŘÍLOH

P I: Ukázka funkce Siteagregator.pl.

P II: Disk CD s konfiguračními soubory a diplomovou prací.

## PI: UKÁZKA FUNKCE SITEAGREGATOR.PL

```
1 sub Aggregate($) {
2   my      $site=shift;
3   if (1) {
4     $site=~ s{kh\d+\.google.com}{maps\.google\.com}o;
5     $site=~ s{kh\d+\.google.com}{maps\.google\.com}o;
6     $site=~ s{mt\d+\.google.com}{maps\.google\.com}o;
7     $site=~ s{tbn\d+\.google.com}{tbn\.google\.com}o;
8     $site=~ s{(.*)\.mapy\.cz}{www\.mapy\.cz}o;
9     $site=~ s{(.*)\.idnes\.cz}{www\.idnes\.cz}o;
10    $site=~ s{(.*)\.gemius\.pl}{www\.gemius\.pl}o;
11    $site=~ s{(.*)\.im\.cz}{www\.im\.cz}o;
12    $site=~ s{kh\d+\.google.cz}{maps\.google\.cz}o;
13    $site=~ s{kh\d+\.google.cz}{maps\.google\.cz}o;
14    $site=~ s{mt\d+\.google.cz}{maps\.google\.cz}o;
15    $site=~ s{tbn\d+\.google.cz}{tbn\.google\.cz}o;
16    $site=~ s{mlt\d+\.google.cz}{mlt\.google\.cz}o;
17    $site=~ s{(.*)\.seznam\.cz}{www\.seznam\.cz}o;
18    $site=~ s{(.*)\.allegroimg\.pl}{www\.allegroimg\.pl}o;
19    $site=~ s{(.*)\.bbmedia.cz}{www\.bbmedia\.cz}o;
20    $site=~
21    s{(.*)\.semnicneposilejte\.cz}{www\.semnicneposilejte\.cz}o;
22    $site=~ s{(.*)\.fler\.cz}{www\.fler\.cz}o;
23    $site=~ s{(.*)\.googleadservices\.com}{www\.google\.com}o;
24    $site=~ s{(.*)\.googlesyndication\.com}{www\.google\.com}o;
25    $site=~ s{(.*)\.googleusercontent\.com}{www\.google\.com}o;
26    $site=~ s{(.*)\.google-analytics\.com}{www\.google\.com}o;
27    $site=~ s{(.*)\.centrum\.cz}{www\.centrum\.cz}o;
28    $site=~ s{(.*)\.novinky\.cz}{www\.novinky\.cz}o;
29    $site=~ s{(.*)\.mapy\.cz}{www\.mapy\.cz}o;
30    $site=~ s{(.*)\.google\.cz}{www\.google\.cz}o;
31    $site=~ s{(.*)\.google\.com}{www\.google\.com}o;
32    $site=~ s{(.*)\.mozilla\.org}{www\.mozilla\.org}o;
33    $site=~ s{(.*)\.chmi\.cz}{www\.chmi\.cz}o;
34    $site=~ s{(.*)\.ebay\.com}{www\.ebay\.com}o;
35    $site=~ s{(.*)\.odletime\.cz}{www\.odletime\.cz}o;
36  }
37  return $site;
38 }
```