UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Firewall na OS Linux

Milan Rudolfský

Bakalářská práce
2010

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 26. 07. 2010 Milan Rudolfský

Poděkování

Rád bych touto cestou poděkoval panu Ladislavu Novákovi ze společnosti eBrána s.r.o. za doplňující informace týkající se teoretické části této bakalářské práce. Dále panu Ing. Martinu Semerádovi, rovněž ze společnosti eBrána s.r.o. a Ing. Lukáši Čeganovi Ph.D. z Univerzity Pardubice za čas, ochotu a užitečné rady k řešené problematice.

Anotace

Popis instalace, konfigurace a implementace paketového firewallu IPTABLES, webového a FTP proxy serveru SQUID. Účelem těchto nástrojů je zamezit uživatelům sítě používat komunikační klienty a nastavit blokování určitých URL adres. Tuto problematiku porovnat s technologií MIKROTIK. Vzít v úvahu bezpečnostní opatření proti nepovoleným průnikům.

Klíčová slova

iptables, firewall, proxy, linux, mikrotik

Title

Firewall on OS Linux.

Annotation

Describtion of installation, configuration and implementation of packet firewall IPTABLES, web and ftp proxy server SQUID. Avoid through these tools network users using communication clients and configure block some URL addresses. Compare this issue with MIKROTIK technology. Acknowledge security policy against attacks.

Keywords

iptables, firewall, proxy, linux, mikrotik

Obsah

Seznam zkratek

AOL	American Online Inc.
IP	Internet Protocol
ICQ	I Seek You
QIP	Quiet Internet Pager
IRC	Internet Relay Chat
NAT	Network address translation
DNS	Domain name server
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol security
FTP	File transfer protocol
URL	Uniform Resource locator
TCP	Transmission Control Protocol
GNU	GNU's Not Unix
GPL	General Public License
IM	Instant Messaging

Seznam obrázků

Seznam tabulek

1 Úvod

Jedním z dnešních fenoménů na celosvětové síti Internet je stále oblíbenější používání komunikačních prostředků. Tyto informační zdroje se uživatelé sítě naučili používat velmi rychle, a to nejen pro získávání potřebných a užitečných informací, ale také je velice často využívají jako komunikační kanál mezi svými přáteli. Pro jejich soukromý život je to mnohdy nepostradatelný zdroj komunikace.

Je ale pravdou, že tyto informační toky v pracovním prostředí nejsou oblíbenou zprávou pro zaměstnavatele. Často se stává, že zaměstnanci využívají tuto formu komunikace pro svůj soukromý život i v pracovní době. Tím značnou měrou okrádají firemní aktivitu svojí neloajální činností a produktivita práce ve společnosti je značně snížena.

Zaměstnavateli je často tato skutečnost nepříjemná a produktivitu se snaží samozřejmě co nejvíce zvýšit. Jednou z věcí, kterou lez provést, je finanční sankce zaměstnanců za provozování těchto komunikačních prostředků. Jsou ale tací, kterým ani zpráva o finančních sankcích strach nenažene a prostředky používá nadále. Dalším krokem je oslovení správce počítačové sítě, aby tyto prostředky zakázal užívat.

Z pohledu správce sítě je tento úkol vetšinou poněkud závažnou a naznámou úlohou. Které prostředky zakázat? Jaké síťové porty tyto komunikační služby užívají? Dá se tato služba zakázat nebo nedá? A mnoho dalších otázek se objeví jen při pomyšlení na toto téma. Dále následuje finanční otázka, zda se rozhodnout pro komereční řešení nebo se spoléhat na zkušenosti správce sítě a tím i docílení finančních úspor při užití např. volného software.

Do tohoto úkolu jsem se pustil za použití minimálních investic, a to na platformě Linux, spolu s programy Iptables a proxy server SQUID. Jedná se o jedny z nejlepších programů v oblasti kontroly toku dat na Internetu pro platformu Unix/Linux a nespornou výhodou je jejich cenová stránka. Finanční náklady na tyto programy nejsou žádné, tyto produkty jsou volně dostupné pod licenční politikou GNU/GPL.

V této práci Vás provedu instalací Iptables, proxy serveru SQUID a nastavení těchto produktů pro účely popsané výše tj, omezení komunikačních prostředků především ve firemním prostředí.

2 Komunikační prostředky - teoreticky

2.1 ICQ

Zkratka ICQ znamená I Seek You. Tento komunikační program byl vyvinut izraelskou firmou Mirabilis a později prodán společnosti American Online.

ICQ především komunikuje na svém standartním portu 5190, ale dokáže se připojit přes port služby http 80 a šifrovaný komunikační port https 443.

Tento program se připojuje na nespočet serverů společnosti AOL, tím správcům sítě ztěžuje jeho zablokování ve firemní síti.

ICQ ve starších verzích lze zablokovat na zmíněném portu 5190. Novější verze se umí protunelovat zabezpečeným protokolem https na portu 443 a pouhým blokováním portu 5190 neuspějeme.

Jediným úspěšným řešením, jak tuto službu zakázat, je nastavení firewallu tak, aby nepropouštěl veškerou komunikaci z vnitřní sítě do Internetu na servery společnosti AOL a blokovat port 5190.

Rozsahy IP adres společnosti AOL pro blokování ICQ.

205.188.0.0 – 205.188.255.255

Toto řešení se může mnohým administrátorům zdát ne moc uhlazené, ale je to jediný způsob blokování ICQ. Pokud potřebujeme informační zdroj, který je umístěn na některém ze serveru spol. AOL, tak lze vybranou IP adresu zdroje na firewallu povolit. Obrácený postup je téměř nemožný. Existuje cca 65535 adres, které patří AOL a není v silách administrátorů, aby zakazovali konkrétní adresy pro připojení ICQ do Internetu.

2.2 ICQ2GO

ICQ2GO je online verze komunikačního programu ICQ.

Výhodou ICQ2GO je fakt, že tento program není nutno instalovat do Vašeho počítače. Stačí navštívit webové stránky go.icq.com a na těchto stránkách se přihlásit do sítě ICQ. Mnoho uživatelů se tak domnívá, že obejde zakázané připojení prostřednictvím klasického ICQ programu.

Pro administrátora je zablokování této webové stránky otázkou několika málo úprav v proxy serveru SQUID a šabloně Squirm.patterns programu Squirm.

2.3 QIP

QIP je dalším hojně používaným komunikačním prostředkem.

QIP lze využít pro připojení různých komunikačních kanálů, jako je např. ICQ, QIP.ru, LiveJournal a dalších. V převážné většině se v České Republice využívá jako alternativa programu ICQ.

Pro připojení do sítě ICQ používá QIP následujících adres:

login.icq.com
login.oscar.aol.com
ibucp-vip-d.blue.aol.com
ibucp-vip-m.blue.aol.com
bucp-m08.blue.aol.com
205.188.153.98
205.188.153.97
64.12.161.153

Déle se připojuje skrz porty 5190, 80 a 443.

Zablokování totoho programu je opět poměrně jednoduchým úkolem. Stačí na firewallu opět zablokovat AOL servery 205.188.153.98 a 205.188.153.97 a pomocí proxy serveru SQUID a programu Squirm vložit do šablony Squirm.patterns pravidla pro blokování, případně přesměrování adres login.icq.com, login.oscar.aol.com, ibucp-vip-d.blue.aol.com, ibucp-vip-m.blue.aol.com a bucp-m08.blue.aol.com.

Některým čtenářům by se mohlo zdát, že totéž platí i pro program ICQ, ale toto nastavení pro blokování ICQ použít nelze.

2.4 Miranda IM

Miranda IM je opět komunikačním programem podporující více protokolů, jako např. ICQ, IRC, AIM, MSN, JABBER a dalších.

V mnoha případech se opět využívá pro komunikační protokol ICQ. Miranda lze zablokovat stejným způsoben jako výše popsaný komunikační program QIP.

2.5 IRC

Irc je prvním komunikační protokolem v reálném čase, který se na Internetu objevil. K připojení do sítě užívá port 6667.

K zakázání komunikace IRC stačí na firewallu tento port zakázat.

2.6 FACEBOOK

Největším fenoménem dnešního užívání komunikačních prostředků v síti Internet je bezesporu stále rostoucí společnost Facebook Inc. Webové stránky této firmy jsou známy mnoha lidem komunikujících po Internetu. Ač je tato společnost terčem obrovského množství uživatelů, lze ji vcelku dobře blokovat.

Společnost Facebook, Inc. užívá následující adresní prostory:

69.63.176.0 – 69.63.191.255

66.220.144.0 – 66.220.159.255

K zákazu přístupu na stránky facebook.com stačí pomocí IPTABLES zakázat přístup na tyto IP adresy.

2.7 MEEBO

Společnost Meebo, Inc. je další společností, která pro uživatele Internetu vyvinula webovou aplikaci nahrazující pevně instalované programy jako jsou ICQ, AIM nebo online aplikace FACEBOOK, WINDOWS LIVE a další.

Společnost Meebo, Inc. užívá následujících adresních prostor:

74.114.24.0 – 74.114.31.255

Webová prezentace meebo.com pracuje na IP adrese 74.114.28.10

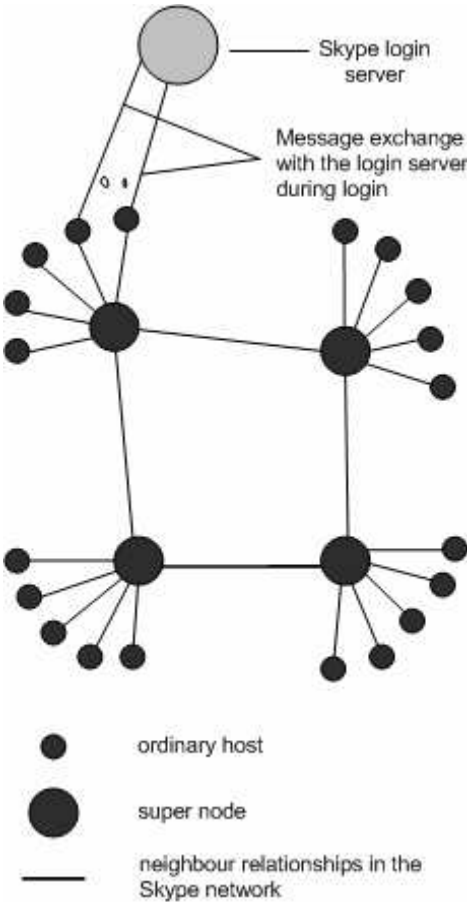
Pro zablokování meebo.com nemůžeme použít celkový rozsah IP adres této společnosti, ale musíme zakázat pouze přístup na adresu webové prezentace. Zákazem celého rozsahu zapříčiníme nefunkčnost např. serveru google.com. Dále doporučuji nastavit proxy server SQUID a Squirm.patterns pro bezpečné blokování této adresy.

2.8 SKYPE

Skype je opět komunikační program, který mimo jiné funkce dovoluje uživateli používat hlasové služby (VoIP) prostřednictvím počítačové sítě. Tento program se dostal do obliby mnoha uživatelů, především možností telefonování po Internetu zdarma a za malý poplatek i do sítí GSM a pevných telefonních sítí.

Program je užitečný pro mnoho uživatelů, ale z pohledu správce počítačové sítě to je dosti složitá záležitost. Zablokování tohoto protokolu je značně složité, ba i nemožné.

Následující obrázek zobrazuje hierarchii serverů Skype pro připojení uživatelů do sítě.



Obrázek 1 – Hiearchie serverů sítě Skype

Skype vlastní pouze login servery, které jsou umístěny na neznámém místě v síti Internet. Pomocí těchto login serverů se ověřují uživatelé sítě Skype, aby jim byl umožněn přístup. Dále pomocí super node serverů může uživatel komunikovat s ostatními účastníky sítě. Super node serverem se může, a to i nevědomě, stát každý počítač, na kterém je nainstalován program Skype a připojení do Internetu je dostatečně rychlé.

Zablokování Skype pomocí zákazu přístupu na login servery není funkční. Z tohoto důvodu se domnívám, že i úlohu login serverů převzaly super node servery. Jak bylo popsáno výše, ani zablokování super node serverů není možné, protože tímto serverem se může stát téměř jakýkoliv počítač v Internetu. Skype pracuje na portech 34586, 80 a 443. Zákázat port 34586 nepomáhá. Po vložení pravidel na zákázání přístupu na stránky Skype do Squirm.patterns pro program Squirm a proxy server Squid se opět projevilo jako neučinné. Zkouškou prošel i program L7-filter, který je nadstavbou IPTABLES a dokáže označkovat pakety pro různé komunikační protokoly. I za pomocí L7-filter programu a IPTABLES nešly zakázat pakety programu Skype. Jedinou funkční možností, která byla objevena, je dosti drastické zablokování celkové komunikace na portu 443 protokolu https. Tímto jediným způsobem se podařilo program Skype zakázat.

3 Balíčky IPTABLES, FWBUILDER, SQUID a SQUIRM popis

3.1 IPTABLES

Iptables je firewall pro systémy Linux/Unix, který dokáže sestavovat obrovské množství pravidel pro komunikaci na počítačové síti. Mezi jeho schopnosti patří řízení přístupu uživatelů do sítě pomocí portů, IP adres, značkování paketů a disponuje i možností překladu adres NAT. Tento nástroj je velice oblíben jak pro svoji malou velikost a tím i nenáročnost na hardware serveru, tak pro dostupnost pod licencí GNU/GPL. Samozřejmostí tohoto softwaru je možnost spravovat veškerou komunikaci pomocí Internet Protokolu verze 6.

3.2 FWBUILDER

Firewall Builder je grafickou nadstavbou pro program IPTABLES. Výhodou tohoto softwaru je možnost připravovat komunikační pravidla pro různé verze operačních systémů, tak i pro odlišné verze IPTABLES. Vytvořené pravidlo můžeme exportovat na vzdálený firewall, kde tyto pravidla lze aplikovat.

Vytvoření pravidel pro komunikaci v síti prostřednictvím samotných IPTABLES je především pro méně zkušené administrátory dosti složitou záležitostí a při větším množství komunikace, které je potřeba sledovat, se značně znepřehledňuje konfigurační script pro IPTABLES. Z tohoto důvodu zde používám grafickou nadstavbu FWBUILDER.

3.3 SQUID

SQUID je kešující proxy server. Tento server má za úkol zprostředkovávat uživatelům potřebné zdroje informací nepřímo. To znamená, že klient odešle požadavek na proxy server, a ten teprve kontaktuje zdroj, ze kterého potřebujeme dané informace získat. Výhodou tohoto nastavení je možnost dočasně ukládat již jednou získané informace do paměti proxy serveru. Klientovi, který opětovně žádá stejná data, je možno tyto data zaslat z paměti a tím ušetřit určitou šířku pásma připojení k Internetu nebo jiné sítě.

Termín transparentní proxy znamená, že uživatel nemusí nastavovat adresu proxy serveru do svých aplikací, ale převážná většina komunikace se automaticky přesměruje na proxy server a ten se tak stává pro uživatele neviditelným.

3.4 SQUIRM

SQUIRM je nadstavbou pro proxy server SQUID. Tento softwar dovoluje pomocí regulárních výrazů a specifických pravidel odfiltrovat nevyžádaný obsah webových stránek. Dále můžeme uživatelsky definované webové adresy směrovat na jiné, případně úplně zakázat

4 Firewall a SQUID server

4.1 Hardwarové prostředky

Pro testování pravidel na zablokování komunikačních prostředků pomocí IPTABLES a proxy serveru SQUID byl použit počítač společnosti DELL s následující hardwarovou konfigurací.

Procesor Intel Pentium 4, frekvence 2.26 GHz

Operační paměť o velikosti 768 MB

Síťové rozhraní (1) Intel 8254OEM Gigabit Ethernet Controler

Síťové rozhraní (2) Realtek RTL-8139/8139C/8139C+

Další hardwarové vybavení je pro podmínky těchto testů nepodstatné.

4.2 Operační systém

Operační systém byl zvolen Linux distribuce Ubuntu s jádrem verze 2.6.32-24-generic. Tento systém jsem vybral pro jeho snadnou ovladatelnost i pro méně zkušené uživatelé Linuxu.

4.3 IPTABLES

IPTABLES je použito ve verzi 1.4.4-2ubuntu2. Níže popsané testy by měly pracovat i na nižších verzích IPTABLES.

4.4 FWBUILDER

Firewall Builder je použit ve verzi 4.0.1. b2950-ubuntu-hardy-1.

4.5 SQUID

Proxy server SQUID je verze 2.7.STABLE7-1ubuntu12.

4.6 SQUIRM

SQUIRM je použito v poslední verzi a to squirm-1.0betaB.

5 Instalace

5.1 IPTABLES

Program IPTABLES je součástí všech dnes nabízených distribucí operačního systému Linux. Případnou instalaci lze provést pomocí zdrojových kódů nebo pomocí správce balíků dané distribuce Linuxu.

Pro distribuci Ubuntu to lze provést následujícím příkazem.

sudo apt-get install iptables

5.2 FWBUILDER

Pro Firewall Builder je nejlepším řešením instalace za použití správce balíku Synaptic v Ubuntu, popřípadě využití apt-get.

Váš systém musí obsahovat následující balíky.

libxml2 v2.4.10 nebo novější

libxslt v1.0.7 nebo novější

ucd-snmp nebo net-snmp

openssl nejlepší v nejnovější verzi

QT 4.3.x nebo QT 4.4.x

Pokud chceme instalovat FWBUILDER pomocí apt-get, musíme do /etc/apt/source.list přidat následující řádek pro hledání balíku v repozitáři.

deb http://www.fwbuilder.org/deb/stable hardy contrib

Pro instalaci stačí sudo apt-get install fwbuilder. Takto nainstalovaný program lze jednoduše spustit z konzole příkazem fwbuilder.

5.3 SQUID

Pro instalaci SQUID je opět nejlepším řešením použít správce balíků Synaptic pro Ubuntu, popřípadě jiný dle distribuce. Samozřejmě lze použít k instalaci zdrojové kódy této aplikace.

Po stažení zdrojových kódů použijeme ke kompilaci a instalaci klasických příkazů, např.

./configure –enable-err-language=Czech –prefix=/usr/local

make

make install

Po kompletní instalaci lze proxy server SQUID spustit příkazem sudo squid.

Pro editaci konfigurace se používá soubor squid.conf uložen v /etc/squid/

SQUID server běží standartně na portu 3128.

5.4 SQUIRM

Pro instalaci programu SQUIRM nelze použít žádný správce balíků. Vše musíme provést ručně v konzoli ze zdrojových kódů.

Nejprve stáhneme balík squirm-1.0betaB.tar

tar xf squirm-1.0betaB.tar

cd regex

./configure

make clean

make

cp –p regex.o regex.h

Nadále se podíváme pod jakým uživatelským jménem a skupinou pracuje náš proxy server SQUID. Například pomocí programu HTOP.

Poté co zjistíme uživatele SQUID serveru, v mém případě je uživatelské jméno i skupyna PROXY, musíme editovat soubor Makefile, kde uživatele squid nahradíme námi zjištěným jménem a skupinou.

make

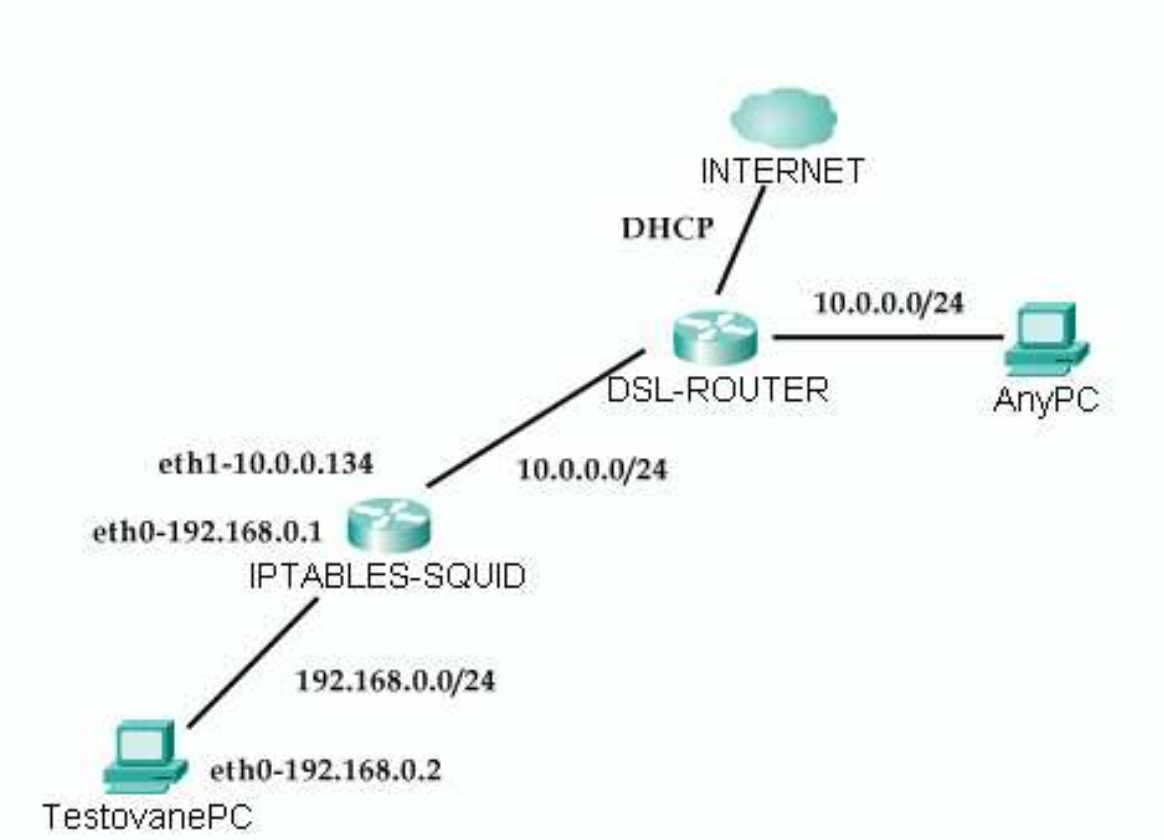
sudo make install

Nyní by měl být program SQUIRM nainstalován.

Spuštění provedeme příkazem sudo /usr/local/squirm/bin/squirm. Šablona pro editování pravidel je umístěna na adrese /usr/local/squirm/etc/squirm.patterns.

6 Vzorová síť

Zde je uvedeno schéma počítačové sítě, které bylo použito pro testování a blokování komunikačních protokolů.



Obrázek 2 – Vzorová síť pro testování

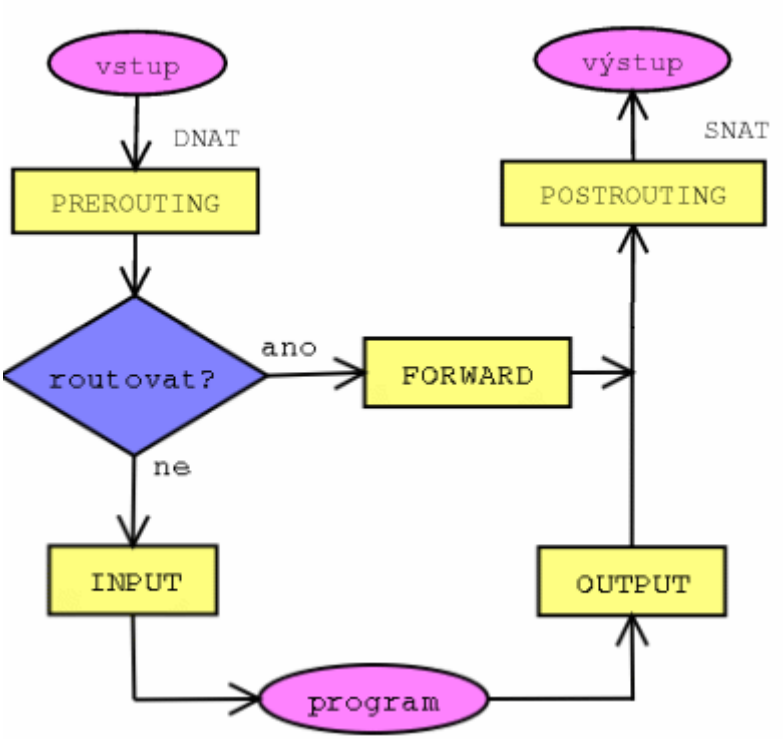
Testovaný počítač je připojen na router s IPTABLES a proxy serverem SQUID. Počítač má nastavenou IP adresu 192.168.0.2/24, brána 192.168.0.1, a DNS servery.

Počítač s IPTABLES a SQUID má nastaveno na rozhraní eth0 IP adresu 192.168.0.1/24 a bránu 192.168.0.1. Druhé rozhraní eth1, které je připojeno do cizí sítě, má IP adresu 10.0.0.134/24, bránu 10.0.0.1 a DNS servery.

Na takto nakonfigurované síti proběhne test komunikačních protokolů.

7 Funkce NAT v IPTABLES

Pro překlad adres funguje IPTABLES dle níže uvedeného obrázku.



Obrázek 3 – Funkce NAT v IPTABLES

Na příchozí paket jsou aplikována pravidla tabulky PREROUTING. Pokud firewall předává paket dále platí pravidla tabulky FORWARD a pokud paked odchází dále, tak platí pravidla v tabulce POSTROUTING.

8 Nastavení NAT a transparentního proxy

8.1 NAT

Pro nastavení překladu adres NAT si do nově vytvořeného dokumentu vložíme následující řádky.

```
#! /bin/bash

/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

/sbin/iptables -A FORWARD -i eth1 -o eth0 -m state --state

RELATED,ESTABLISHED -j ACCEPT

/sbin/iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

Tento skript uložíme např. pod název nat. Jeho spuštěním pomocí příkazu sudo./nat docílíme zapsání těchto pravidel do IPTABLES a následné funkčnosti překladu adres.

8.2 Transparentní proxy

Transparentní proxy zajištuje komunikaci skrze server SQUID, kde se aplikují námi vytvořená pravidla. Aby uživatelé nemuseli zadávat do svých aplikací IP adresu proxy serveru, přidáme následující řádek do našeho souboru nat.

```
/sbin/iptables -t nat -A PREROUTING -p tcp ! --dport 443 -s 192.168.0.0/24 -i eth0

-j REDIRECT --to-port 3128
```

Po uložení a spuštění skriptu se nám veškerá komunikace TCP, vyjma protokolu https, přesměruje na port SQUID proxy serveru 3128.

9 Nastavení SQUID

Konfigurační soubor pro SQUID se nachází v /etc/squid/squid.conf.

Tento soubor obsahuje mnoho možností, jak konfigurovat SQUID. Pro naše potřeby nám bude stačit pozměnit pouze jeho malou část.

Port pro připojení klientů je značen direktivou http_port a je standartně nastaven na 3128. Aby nám SQUID pracoval v transparentním režimu, dopíšeme za port transparent.

http_port 3128 transparent

Pro správnou funkci FTP protokolu skrze proxy server najdeme direktivu označenou jako always_direct. Pod tuto direktivu, která končí direktivou #default zapíšeme tyto dva řádky.

acl FTP proto FTP

always_direct allow FTP

Dále je potřeba zjistit zda v direktivě acl je položka např. acl Safe_ports port 21 #FTP a zda je povolena direktivě http_access např. http_access deny ! Safe_ports.

Pokud je vše splněno, měl by proxy server SQUID plně fungovat pro veškerou komunikaci, kromě šifrovaného spojení https.

První spuštění SQUIDu se provede příkazem sudo squid –z. Tento příkaz spustí SQUID a nastaví odkládací prostor. Po každé změně v konfiguračním souboru se musí provést příkaz sudo squid –k reconfigure, aby se uvedené změny projevily.

10 Omezení komunikačních protokolů prakticky

10.1 Blokování www stránek

Pro blokování www stránek použijeme program SQUIRM. Do šablony squirm.patterns vložíme následující řádky:

regexi .*playboy\.com.* http://www.seznam.cz

regexi ^http://www\.facebook\.com.* http://www.seznam.cz

abort .exe

Tímto nastavením přesměrujeme stránky playboy.com a http://www.facebook.com na adresu http://www.seznam.cz. Dále také zakážeme stahování souborů s příponou exe.

Pomocí regulárních výrazů můžeme vytvářet vlastní pravidla pro potřeby konkrétní situace. Na veškerou komunikaci procházející přes proxy server SQUID budou tyto pravidla uplatněny. Po provedení změn nesmíme zapomenout SQUIRM restartovat.

10.2 Zamezení přístupu ICQ

Pro nastavování firewallu IPTABLES doporučuji pro přehlednost a ulehčení práce používat grafickou nadstavbu FWBUILDER.

Zamezení protokolu ICQ provedeme vložením následujícího pravidla do IPTABLES.

1) Source = any, Destination = any, Service =UDP port 4000 a tuto akci zakážeme.

2) Source = any, Destination = 205.188.0.0 - 205.188.255.255, Service = any zakážeme.

Tímto blokujeme celý adresní prostor společnosti AOL, Inc. Pokud by nastaly problémy s přístupen na stránky, které jsou na serverech AOL, Inc., můžeme tyto IP adresy na firewallu povolit.

10.3 Zamezení přístupu ICQ2GO

Zablokování provedeme pomocí squirm.patterns, kde vložíme tento řádek:

regexi ^http://www\.icq\.com/.* http://www.seznam.cz

Veškerou komunikaci, která probíhá na server www.icq.com, přesměrujeme na adresu www.seznam.cz.

10.4 Zamezení přístupu QIP

QIP zablokujeme pomocí šablony squirm.patterns následujícími řádky:

```
regexi ^login\.icq\.com/.* http://www.seznam.cz

regexi ^login\.oskar\.aol\.com/.* http://www.seznam.cz

regexi ^ibucp-vip-d\.blue\.aol\.com/.* http://www.seznam.cz

regexi ^ibucp-vip-m\.blue\.aol\.com/.* http://www.seznam.cz

regexi ^bucp-m08\.blue\.aol\.com/.* http://www.seznam.cz

regexi ^slogin\.oscar\.aol\.com/.* http://www.seznam.cz
```

Následně zakážeme na firewallu TCP port 5190 a některé servery AOL.

1) Source = any, Destination = any, Service = TCP port 5190 zakázat.
2) Source = any, Destination = 205.188.153.98, Service = any zakázat.
3) Source = any, Destination = 205.188.153.97, Service = any zakázat.
4) Source = any, Destination = 64.12.161.153, Service = any zakázat.

Skript firewallu zkompilujeme a spustíme. Nesmíme zapomenout restartovat SQUIRM.

10.5 Zamezení přístupu MIRANDA

Pro zamezení MIRANDY a protokolu ICQ lze použít stejný postup jako výše zmíněné blokování klienta QIP. Pro protokoly jako je Jabber a IRC vložíme do IPTABLES tyto řádky.

1) Source = any, Destination = any, Service = TCP port 5222 zakázat.
2) Source = any, Destination = any, Service = TCP port 6667 zakázat.

Port 5222 využívá ke své činnosti Jabber a port 6667 IRC.

10.6 Zamezení přístupu IRC

Pomocí firewallu, kde budeme blokovat port TCP 6667, který využívá komunikační protokol IRC. Do IPTABLES vložíme řádek:

Source = any, Destination = any, Service = TCP port 6667 zakázat.

10.7 Zamezení přístupu FACEBOOK

Facebook zablokujeme jak pomocí SQUIRM, tak i IPTABLES. Do šablony squirm.patterns vložíme tento řádek:

regexi ^http://www\.facebook\.com/.* http://www.seznam.cz

Poté pomocí FWBUILDERu vytvoříme následující pravidla:

Source = any, Destination = 69.63.176.0 – 69.63.191.255, Service = any zakázat.

Source = any, Destination = 66.220.144.0 – 66.220.159.255, Service = any zakázat.

Takto jsme přesměrovaly stránky http://www.facebook.com na adresu http://www.seznam.cz a zakázali jsme servery společnosti Facebook, Inc., abychom jsme se nemohli přihlásit pomocí https.

10.8 Zamezení přístupu MEEBO

K zamezení online aplikace meebo.com stačí blokovat IP adresu webového serveru společnosti na níž běží úvodní webová prezentace. Pro lepší funkci můžeme do squirm.patterns zapsat další pravidla.

Pro IPTABLES.

Source = any, Destination = 74.114.28.110, Service = any zakázat.

Pro SQUIRM.

regexi .*\.meebo\.com/.* http://www.seznam.cz

regexi .*\.meebo\.cz/.* http://www.seznam.cz

Všechny stranky meebo.com a meebo.cz budou přesměrovány.

10.9 Zamezení přístupu ostatní

Jelikož v síti Internet je mnoho komunikačních protokolů více či méně známých, je pravděpodobné že budete muset vytvořit vlastní pravidle. Zde je postup.

1) V šabloně squirm.patterns pomocí regulárních výrazů zakázat / přesměrovat přístup na tyto stránky.

2) Zjistit port přes který komunikuje klient a tento port na firewallu zakázat.

3) Pomocí whois informací zjistit adresní rozsahy které se používají pro danou službu a tyto adresy zakázat.

Tímto postupen bychom mohli zakázat většinu komunikačních protokolů.

11 MIKROTIK

11.1 Úvod

Mikrotik je velice zajimavou technologií. V převážné většině případů se používá pro řízení komunikace bezdrátových přenosů dat WiFi na pásmech 2,4 GHz a 5 GHz. Jedná se o operační systém, který je možno nainstalovat na téměř jakýkoliv počítač, ale velkou výhodou je možnost provozu tohoto systému na zařízeních typu RouterBoard. Tento systém má v sobě připravené balíčky s programy na podporu WiFi připojení, firewall, proxy server, DNS, DHCP, routovací protokoly a mnoho dalších. V případě RouterBoardu je nesmírnou výhodou velikost tohoto zařízení, cena a možnosti napájení pomocí PoE. Ovládání systému je možno pomocí ssh, telnet, www prohlížeče a utilitou WinBox.

11.2 Testované zařízení

Pro testování byl použit systém Mikrotik s licencí L4 na RouterBoardu RB443 a pro správu zařízení použita utilita WinBox verze 4.5.

RB433 obsahuje:

1) procesor MIPS 300 MHz
2) operační paměť RAM 64 MB SDRAM
3) 3 x Lan port RJ45 10/100 Mbps
4) seriový port RS-232
5) 3 x miniPCI konektor

11.3 Prvotní nastavení

Prvotní nastavení budeme provádět podle vzorové sítě viz. kapitola 6. Pouze na místo PROXY-SQUID vložíme náš router MIKROTIK.

1) Stáhneme si utilitu WinBox.
2) Pomocí WinBoxu se přihlásíme na náš router.
3) V záložce Interface změníme názvy z eth2 na Internet a z eth3 na Vnitřní síť
4) V IP – Addresses přiřadíme IP adresy našim rozhraní.
5) Pro Internet 10.0.0.134/24
6) Pro Vnitřní síť 192.168.0.1/24

7) Dále IP – Firewall a v záložce NAT přidáme pravidlo, aby nám fungoval překlad adres.

8) Chain = srcnat, Out. Interface = Internet a v Action = masquerade.

9) Přidáme do IP – Routes statickou cestu pro správné směrování.

10) Dst. Address = 0.0.0.0/0, Gateway = Internet.

11) Spustíme proxy server. IP – Web Proxy – Web Proxy Settings nastavíme na Enabled a zkontrolujeme port 8080.

12) V IP – Firewall a záložce NAT přidáme pravidlo, aby komunikace směřovala na náš proxy server.

13) Chain = dsnat, Protocol = tcp, Dst. port = 80, In. Interface = Vnitřní síť a v Action = redirect, To Ports = 8080.

14) V posledním bodě nastavíme DNS servery. Toto provedeme v IP – DNS – Settings. Nezapomeneme zde povolit Allow Remote Requests.

Po takto nastaveném systému by měla veškerá komunikace fungovat. Provoz na portu 80 bude přesměrován na náš proxy server na port 8080.

11.4 Blokování www stránek

Pro zablokování daných stránek se používá oddělení IP – Web Proxy. Na kartě Acces přidáváme pravidla např. pro zákaz přístupu na stránky seznam.cz.

Dst. Host = *.seznam.cz, Action = deny

Veškerá komunikace přes port 80 na adresu seznam.cz bude zakázána. Samozřejmostí je možnost toto pravidlo upřesnit např. podle zdrojové adresy klienta atd.

11.5 Blokování komunikačních klientů

Blokování komunikačních klientů je stejné jako je tomu u IPTABLES a popřípadě proxy serveru SQUID.V systému Mikrotik se jedná o nastavení v IP – Firewall. Zde přidáváme pravidla co povolit a co zakázat. Např. pro zakázání stránek meebo.com prostřednictvím zapezpečeného protokolu https použijeme toto nastavení:

Chain = forward, Dst.Address = 74.114.28.110, Protocol = tcp, In. Interface = Vnitřní síť a v záložce Action = reject.

Po uložení by mělo být pravidlo aplikováno.

Omezení ICQ, QIP, MIRANDy atd. je na stejném principu jako je popsáno v kapitole 10, pouze budeme přidávat pravidla do záložky Filter Rules.

12 IPTABLES vs. MIKROTIK

Porovnání těchto dvou technologií z hlediska autora je uvedeno v následující tabulce:

Tabulka 1 – porovnání technologie MIKROTIK a IPTABLES

	MIKROTIK	IPTABLES
Velikost serveru	**OK**	**X**
Energetická náročnost	**OK**	**X**
Potřebný hardware	**OK**	**X**
Cena zařízení	**OK**	**X**
Škálovatelnost hardware	**X**	**OK**
Instalace nových funkcí	**X**	**OK**
Správa – začátečník	**OK**	**X**
Správa – pokročilý	**OK**	**OK**
Omezení provozu – firewall	**OK**	**OK**
Omezení provozu – proxy	**X**	**OK**
Záloha systému	**OK**	**X**
Spolehlivost např. RAID	**X**	**OK**
Celkové hodnocení	**50 %**	**50 %**

V mém hodnocení podle daných kritérií obdržely obě tyto možnosti jak IPTABLES a proxy server SQUID proti technologii MIKROTIK stejný počet bodů. Osobně bych technologii MIKROTIK doporučil začínajícím správcům počítačové sítě. Po prohloubení znalostí ohledně správy sítě začne být MIKROTIK systémem, jenž nám nebude dostačovat svým omezeným počtem funkcí a přechod na systém Linux s IPTABLES a serverem SQUID bude nevyhnutelný.

13 Nepovolené průniky

Takto sestavená pravidla jak pro firewall IPTABLES a proxy server SQUID by neměly býti napadnutelné. V úvahu neberu kompromitaci serveru jako celku a z tohoto důvodu doporučuji aktualizaci operačního systému a jeho balíčků v prvidelných intervalech. Dále můžeme předpokládat útok DoS který by mohl vyřadit z funkce především proxy server SQUID. Abychom se tomuto typu útoku vyvarovali můžeme pro každáho klienta na síti povolit pouze určitý počet připojení k serveru.

Podstatnou problematikou bezpečnosti tohoto řešení je protokol https. Pokud by si uživatel vnitřní sítě nastavil na svých aplikacích cizí proxy server který podporuje komunikaci https a zkrze tento protokol komunikoval, mohlo by to znamenat průnik blokovaných spojení tímto šifrovaným kanálem. V praxy jsem odzkoušel osmnáct proxy serverů s podoprou https a žádný komunikační klient mi přes toto spojení neprošel.
Z tohoto důvodu je podstatně lepší používat blokování komunikace na firewallu a ne proxy serveru. Řešením této problematiky je povolení nezbytně nutných portů pro komunikaci klientů na vnitřní síti a zákaz veškeré ostatní odcházející komunikace, popřípadě blokování portů vzdálených proxy serverů které nejčastěji pracují na portech 8080, 8085, 3128 a 9415. Vytvoření skriptu který by měl za úkol kontrolu všech proxy serveru v síti Internet je nemožné. Tyto servery vznikají a zanikají každý den a jejich počty nejsou známy.

14 Závěr

Při zpracování této bakalářské práce jsem se naučil mnoha novým zkušenostem. Především jsem prohloubil své znalosti ohledně funkcí komunikačních protokolů jak z hlediska online aplikací tak z pohledu klientských programů. Mezi velmi zajímavou činnost zahrnuji především zkoumání rozsahu IP adres které tyto protokoly využívají ke své funkci a praktickou část kde se tyto aplikace snažíme omezit.

Z hlediska práce na operačním systému Linux a konfigurace nezbytných programových balíčků to byla zkušenost která se nenabízí tak často. Pro tutu práci jsem si musel obnovit znalosti především z instalace potřebného softwaru, užití konfiguračních nástrojů a zdokonalení schopností pro práci s regulárnímy výrazy.

Velkým přínosem pro mé zkušenosti bylo zdokonalení znalostí v konfiguraci IPTABLES a následné aplikaci pravidel. Služba NAT a její nastavení mě překvapilo velice jednoduchým nastavením pro její funkčnost. Nesmírné množství informací jsem nasbíral při práci s proxy serverem SQUID a jeho nadstavbou SQUIRM. Tyto nástroje jsem v praxy užil poprvé a byl jsem mile překvapen jejich funkčností.

Při práci na technologii MIKROTIK jsem byl mile překvapen její snadnou, přehlednou především rychlou konfigurací. Tyto nově nabyté zkušenosti, které mi toto práce dovolila oběvit, jsou pro mě velice užitečné a mohu je aplikovat na počítačoé sítě které spravuji.

Možnosti správy počítačových sítí jak na platformě Linux tak Microsoft je nesmírné množství. Z pohledu začínajícího správce se technologie MIKROTIK a systém Linux mohou zdát dosti nepřehlednými nástroji. Z tohoto důvodu jsou spíše prosazovány komereční aplikace např. společnosti Microsoft. Osobně si myslím že toto řešení není ideální. Při použití např. operačního systému Linux se administrátor tohoto systému dozví nové informace o funkci počítačových sítí jak z pohledu správy tak z pohledu zabezpečení. Vše si odzkouší samostatně a nemá nic předpřipraveno. Dále se naučí mnoha dovednostem které zvíší podvědomí o probírané problematice a tyto zkušenosti posílí rozvoj dalšího bádání a oběvování stále nových možností těchto systémů.

Učit se novým věcem není složitá práce ale chce to mít zkušenost, vytrvalost a odvahu se do toho pustit.

Literatura

Wikipedie: Otevřená encyklopedie: Skype [online]. c2010 [citováno 20. 07. 2010]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Skype&oldid=5398548>

Klement, Vojtěch: Lupa.cz [online]. c2010 [citováno 20. 07. 2010]. Dostupný z WWW: <http://www.lupa.cz/clanky/skype-8211-telefonovani-zadarmo>

Salman A. Baset a Henning Schulzrinne: Columbia University [online]. c2010 [citováno 20. 07. 2010]. Dostupný z WWW: < http://arxiv.org/ftp/cs/papers/0412/0412017.pdf>

Csaba, Botoš: root.cz [online]. c2010 [citováno 21. 07. 2010]. Dostupný z WWW: <http://www.root.cz/clanky/vse-o-iptables-uvod>

Boháč, Jiří: root.cz [online]. c2010 [citováno 21. 07. 2010]. Dostupný z WWW: <http://www.root.cz/clanky/squid-kesujici-proxy-server>

Rajský Lukáš a Pustka Stanislav: vsb.cz [online]. c2010 [citováno 21. 07. 2010]. Dostupný z WWW: <http://www.cs.vsb.cz/grygarek/TPS-0304/projekty0304/ipchains/2/doc/iptables.htm>

Boháč, Jiří: Lupa.cz [online]. c2010 [citováno 21. 07. 2010]. Dostupný z WWW: <http://www.root.cz/clanky/squid-kesujici-proxy-server-2>

Foote, Chris: squirm.foote.com.au [online]. c2010 [citováno 22. 07. 2010]. Dostupný z WWW: <http://squirm.foote.com.au/#download>

Wiles, Frank: revsys.com [online]. c2010 [citováno 21. 07. 2010]. Dostupný z WWW: < http://www.revsys.com/writings/quicktips/nat.html>

Kurland, Vadim:FirewallBuilder [online]. c2010 [citováno 20. 07. 2010]. Dostupný z WWW: < http://www.fwbuilder.org/4.0/docs/firewall_builder_installation.html>

ViSolve Squid Team: visolve.com [online]. c2010 [citováno 20. 07. 2010]. Dostupný z WWW: < http://www.visolve.com/squid/Squid_tutorial.php#Installation_Squid>

Wiki.qipim: wiki.qipim.cz [online]. c2010 [citováno 23. 07. 2010]. Dostupný z WWW: < http://wiki.qipim.cz/index.php?title=Zm%C4%9Bna_p%C5%99ihla%C5%A1ovac%C3%ADho_serveru&oldid=593>

Mikrotik: mikrotik.com [online]. c2010 [citováno 25. 07. 2010]. Dostupný z WWW: <http://www.mikrotik.com/documentation/manual_2.5/IP/Web-proxy.html>

Mikrotik.Tlupa: mikrotik.tlupa.com [online]. c2010 [citováno 25. 07. 2010]. Dostupný z WWW: <http://mikrotik.tlupa.com/?p=38>

Mikrotik: wiki.mikrotik.com [online]. c2010 [citováno 25. 07. 2010]. Dostupný z WWW: <http://wiki.mikrotik.com/wiki/How_to_make_transparent_web_proxy#Howto>

Aspa: wifi.aspa.cz [online]. c2010 [citováno 25. 07. 2010]. Dostupný z WWW: <http://wifi.aspa.cz/rb433-64-mb-ram-300-mhz-3x-minipci-3x-lan-vc-l4-z87398/>

Příloha A – Konfigurační soubor nat

```
#! /bin/bash

/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

/sbin/iptables -A FORWARD -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j
ACCEPT

/sbin/iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

/sbin/iptables -t nat -A PREROUTING -p tcp ! --dport 443 -s 192.168.0.0/24 -i eth0 -j
REDIRECT --to-port 3128
```

Příloha B – Konfigurační soubor squirm.patterns

```
# squirm.patterns.dist
#
# The ordering of lines is this file is critical
# Please see http://www.senet.com.au/squirm/ for examples
#
#block faecbook
regexi ^http://www\.facebook\.com/.* http://www.seznam.cz
#block icq - QIP
regexi ^http://www\.icq\.com/.* http://www.seznam.cz
regexi ^login\.icq\.com/.* http://www.seznam.cz
regexi ^login\.oskar\.aol\.com/.* http://www.seznam.cz
regexi ^ibucp-vip-d\.blue\.aol\.com/.* http://www.seznam.cz
regexi ^ibucp-vip-m\.blue\.aol\.com/.* http://www.seznam.cz
regexi ^bucp-m08\.blue\.aol\.com/.* http://www.seznam.cz
regexi ^slogin\.oscar\.aol\.com/.* http://www.seznam.cz
#block meebo
regexi .*\.meebo\.com/.* http://www.seznam.cz
regexi .*\.meebo\.cz/.* http://www.seznam.cz
#block skype - jen www
$regexi .*skype\.com/.* http://www.seznam.cz
```

Příloha C – Výpis IPTABLES

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state
RELATED,ESTABLISHED
RULE_0     tcp  --  anywhere             anywhere            tcp
multiport dports aol,ircd,xmpp-client
RULE_0     udp  --  anywhere             anywhere            udp dpt:4000
RULE_2     all  --  anywhere             anywhere            state NEW

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state
RELATED,ESTABLISHED
RULE_0     tcp  --  anywhere             anywhere            tcp
multiport dports aol,ircd,xmpp-client
RULE_0     udp  --  anywhere             anywhere            udp dpt:4000
RULE_1     all  --  anywhere             64.12.161.153
RULE_1     all  --  anywhere             69.63.176.0/20
RULE_1     all  --  anywhere             74.114.28.110
RULE_1     all  --  anywhere             202.144.158.192
RULE_1     all  --  anywhere             205.188.0.0/16
RULE_1     all  --  anywhere             205.188.153.97
RULE_1     all  --  anywhere             205.188.153.98
RULE_1     all  --  anywhere             208.81.188.0/22
RULE_2     all  --  anywhere             anywhere            state NEW

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state
RELATED,ESTABLISHED
RULE_0     tcp  --  anywhere             anywhere            tcp
multiport dports aol,ircd,xmpp-client
RULE_0     udp  --  anywhere             anywhere            udp dpt:4000
RULE_1     all  --  anywhere             64.12.161.153
RULE_1     all  --  anywhere             69.63.176.0/20
RULE_1     all  --  anywhere             74.114.28.110
RULE_1     all  --  anywhere             202.144.158.192
RULE_1     all  --  anywhere             205.188.0.0/16
RULE_1     all  --  anywhere             205.188.153.97
RULE_1     all  --  anywhere             205.188.153.98
RULE_1     all  --  anywhere             208.81.188.0/22
RULE_2     all  --  anywhere             anywhere            state NEW

Chain RULE_0 (6 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level
info prefix `RULE 0 -- DENY '
DROP       all  --  anywhere             anywhere

Chain RULE_1 (16 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level
info prefix `RULE 1 -- DENY '
DROP       all  --  anywhere             anywhere

Chain RULE_2 (3 references)
```

```
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level
info prefix `RULE 2 -- ACCEPT '
ACCEPT     all  --  anywhere             anywhere
```