ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
PROVOZNĚ EKONOMICKÁ FAKULTA
Studijní obor Informatika

Bakalářská práce

Síťová bezpečnost - Firewall na iptables

Autor: Miroslav Šimek
Vedoucí práce: Ing. Martin Papík
Akademický rok: 2008/2009

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci „Síťová bezpečnost - Firewall na iptables“ vypracoval samostatně a uvedl v seznamu literatury všechny použité zdroje.

V Praze dne 30.4.2009

.....

Miroslav Šimek

Poděkování

Děkuji vedoucímu práce panu Ing. Martinu Papíkovi za cenné rady a podněty při zpracování této práce.

Název

Síťová bezpečnost - Firewall na iptables

Title

Network security - Firewall on iptables

Souhrn

Tato bakalářská práce se zabývá síťovou bezpečností se zaměřením na firewall na iptables. V teoretické části mapuje uvedenou problematiku, v praktické části jsou uvedeny ukázky z konfigurace. Práce se věnuje různým funkcím firewallu, variantním řešením a možnostem doplnění dalšími bezpečnostními prvky. Obsahuje také zhodnocení jejich výhod a nevýhod a z toho plynoucí praktická doporučení.

Klíčová slova

- Síť
- Firewall
- Proxy
- Iptables
- Klient
- FrontEnd
- Server
- Filtrace

Summary

This bachelor work concerns about network security and is focused on Firewall based on iptables. In its theoretical part it maps over above mentioned area and its practical part contains configuration examples. This work attends various Firewall functions, variations, possibilities of completion with other security components. This work also involves evaluation of component advantages and disadvantages and resulting practical recommendations.

Keywords

- Network
- Firewall
- Proxy
- Iptables
- Client
- FrontEnd
- Server
- Filtering

Obsah

Obsah 3
1 Úvod 4
2 Cíl práce a metodika 5
2.1 Cíl práce 5
2.2 Metodika 5
3 Síťová bezpečnost 6
3.1 Obecné zásady 6
3.2 Bezpečnostní prvky 6
3.3 Firewall 7
3.3.1 Obecná charakteristika 7
3.3.2 Výběr firewallu 8
3.3.3 Funkce firewallu 9
3.3.4 Extranet 9
3.3.5 Filtrace 10
3.3.6 Wrappery 11
3.3.7 Proxy 13
3.3.8 SOCKS 14
3.4 Internetový FrontEnd 16
4 Iptables 17
4.1 Obecná charakteristika 17
4.2 Pravidla 17
4.3 IP maškaráda 19
5 Konfigurace iptables 20
5.1 Syntaxe 20
5.2 Konfigurace 22
6 Závěr 25
6.1 Shrnutí 25
6.2 Problémy 26
6.3 Zhodnocení práce 28
7 Seznam literatury 29
8 Přílohy 31
8.1 Seznam zkratek 31
8.2 Seznam obrázků 32

1 Úvod

V této práci se zabývám síťovou bezpečností se zaměřením na firewall na iptables. Jde o problematiku, která nabývá stále na významu, a to jak z důvodu masového rozšíření připojení počítačů k sítím, tak i z důvodu velkého množství bezpečnostních rizik, které připojení k sítím vedle nepochybných pozitivních efektů také přináší.

Roste počet soukromých uživatelů (domácností), které disponují přístupem k Internetu a aktivně ho využívají, a také obchodní společnosti či jiné právnické osoby, státní správa a další subjekty si dnes už těžko dovedou své fungování představit bez vnitřních sítí (LAN) a bez připojení k veřejným sítím (Internetu).

Počítač připojený k síti je vystaven různým druhům rizik, jako jsou například napadení útočníky, použití škodlivých kódů (trojští koně, spyware apod.), které mohou způsobit velké škody. Prostředky ochrany proti nim je nezbytné volit jak v oblasti hardware, tak i software.

Ve své práci se zaměřuji na softwarovou ochranu, konkrétně na firewally, které mohou sloužit jak k ochraně jednotlivého počítače (např. v domácnosti), tak i na ochranu celé vlastní (důvěryhodné) sítě (např. v rámci podniku) před veřejnou sítí. Vedle této hlavní mohou firewally zahrnovat také další funkce ke zpříjemnění práce v síti, jako jsou blokování pop-up oken, filtrace reklamních bannerů apod.

Iptables jsem si ke konfiguraci firewallu vybral z více důvodů. Jsou rozšířené, dobře prakticky využitelné, jejich užití včetně modifikací je umožněno bezplatně díky GNU General Public License, licenci pro Linux typické.

Tématika je podle mého názoru velmi zajímavá a domnívám se, že síťová bezpečnost bude v budoucnu nadále patřit mezi intenzivně rozvíjené oblasti.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je zmapovat problematiku síťové bezpečnosti se zaměřením na firewall na iptables a navrhnout konfiguraci, zdrojový text obsahující příkazy, na základě kterých dojde k nastavení firewallu pro ochranu jednotlivého počítače připojeného k veřejné síti.

V kapitole 3 si kladu za cíl podat přehled o smyslu síťové bezpečnosti, firewallu jako prostředku jejího zajištění v odpovídající míře a alternativám, resp. možnostem doplnění firewallu dalšími softwarovými prostředky. V kapitole 4 potom předložím souhrn poznatků o iptables v teoretické rovině.

V kapitole 5 této práce je mým cílem popsat některé příkazy a postupy při konfiguraci firewallu pro uživatele nacházejícího se v malé síti, která bude připojena k Internetu.

Tato práce bude zveřejněna v systému Moodle ČZU jako součást dobrovolného semináře bezpečnosti, který pořádá katedra informačního inženýrství.

2.2 Metodika

Pro zpracování této práce jsem volil následující pracovní postup: Po shromáždění dostupných podkladů k tématu jsem provedl rozbor existujících poznatků a problematiku popsal. Následně jsem vše znovu analyzoval a doplnil o vlastní názor na některé řešené otázky, někde jsem se pokusil o předpověď budoucího vývoje.

Pro praktickou část práce jsem si opatřil následující software: Fedora Linux, FW Builder, Nessus a seznámil jsem se se základy práce s nimi.

3 Síťová bezpečnost

3.1 Obecné zásady

Problematika síťové bezpečnosti se řeší již od samého počátku vzniku sítí, který se datuje do 60. let minulého století. Sítí se při tom rozumí technické prostředky umožňující komunikaci mezi počítači. Sítě můžeme klasifikovat z různých hledisek, nejběžnější je jejich dělení na vnitřní (chráněnou) síť a vnější síť (Internet), dalším kritériem může být rozsáhlost sítě. Pro různé sítě jsou potom vhodné různé formy zabezpečení v závislosti na typu a velikosti sítě, nárocích na úroveň zabezpečení atd. Jejich účelem je zejména zajistit bezpečné uložení a přenos dat a ochranu před neoprávněnou manipulací s daty.

Při sestavování bezpečnostní strategie je také třeba vždy přihlížet k poměru mezi výší nákladů vynaložených na zabezpečení a výší případné škody, která by mohla vzniknout při jejím nezavedení. Kromě výdajů spojených s pořízením prvků bezpečnosti je totiž nutno počítat s dalšími budoucími výdaji, které budou souviset s provozem a údržbou a které mohou původní pořizovací náklady výrazně převyšovat.

Je rovněž nezbytné si vždy uvědomit, že útok nemusí přijít jen z vnější sítě (útočník, škodlivý kód), ale může proběhnout i přímo z vnitřní sítě (zlovolný pracovník, škodlivý kód). Řešením je kromě obezřetného přijímání pracovníků zejména zásada udělování minimálních přístupových oprávnění, omezených na ta nezbytně nutná k práci konkrétního uživatele. Uživatel tak bude mít zajištěn přístup k aplikacím a datům, která potřebuje, nikoliv však k těm ostatním, u kterých by jeho přístup pouze znamenal riziko jejich zneužití či poškození.

3.2 Bezpečnostní prvky

Zabezpečení počítačové sítě se dociluje pomocí mnoha prvků. Na začátku stojí obvykle zjištění identity uživatele (proces autentizace). „Autentizaci uživatele je možné provést tehdy, pokud: uživatel něco ví (heslo), uživatel něco má (autentizační kalkulátor, čipová karta či v poslední době mobilní telefon), uživatel má nějaké

biometrické vlastnosti (otisky prstů, struktury oční sítnice či duhovky, tvar obličeje, rozpoznávání hlasu a mnohé další vlastnosti ...)“ [1].

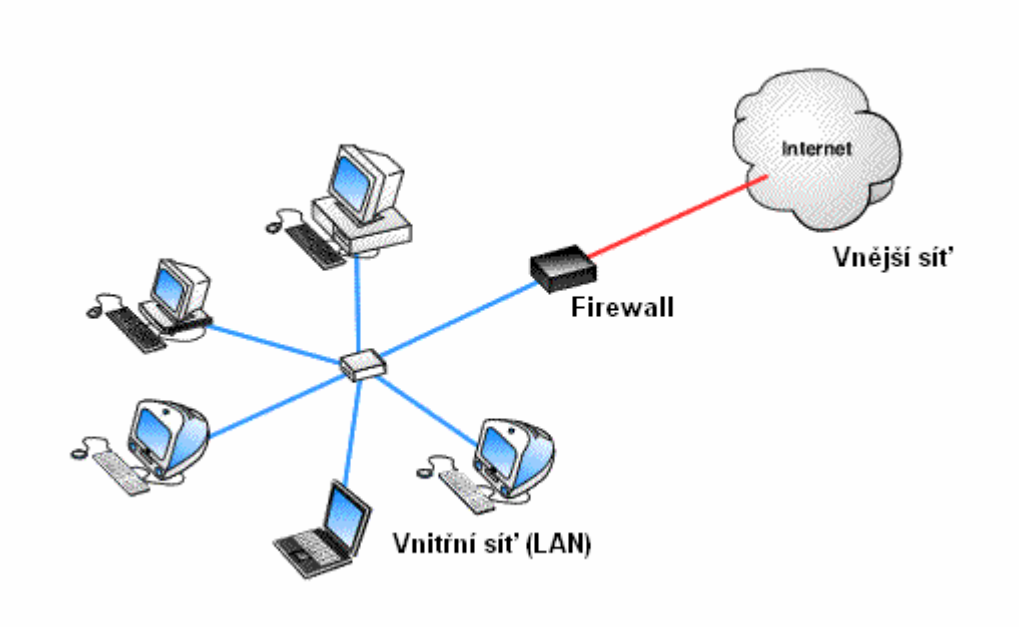
Následuje nastavení přístupových práv, které spolu s autentizací tvoří proces tzv. autorizace. Přístupová práva definují proveditelné úkony, např. čtení, zapisování, spouštění souboru a mohou být zřizována individuálně nebo pro skupinu uživatelů nebo pro ostatní uživatele (mimo skupinu).

Jednotlivým významným prvkům síťové bezpečnosti jsou věnovány následující samostatné subkapitoly. Předmětem zájmu bude zejména firewall.

3.3 Firewall

3.3.1 Obecná charakteristika

Firewall je systém určený k oddělení jednoho počítače nebo vnitřní sítě od Internetu. O přesnou definici pojmu se pokouší dokument RFC-2979 (Behavior of and Requirements for Internet Firewalls, z roku 2000) následovně: Firewall je „agent“, který sleduje datový provoz mezi vnitřní sítí a Internetem, a zjistí-li provoz, který považuje za neodpovídající či nebezpečný, zablokuje jej.



Obrázek 1 - Firewall

Obrázek názorně ukazuje, jak firewall „slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje“ [6].

Firewall je možné umístit přímo na chráněný počítač (domácnost), z praktických důvodů může být vyčleněn na speciálním hardware (podniková síť).

Výhodou firewallu, která ho odlišuje od klasické proxy, je skutečnost, že dokáže rozpoznat, zda paket přichází z vnitřní a nebo z vnější sítě, a nelze ho tak oklamat podvrženou IP-adresou (kdy paket přicházející z Internetu je opatřen IP-adresou vnitřní sítě a naopak).

Vedle vnějšího a vnitřního rozhraní může mít firewall ještě rozhraní pro demilitarizovanou zónu (DMZ). DMZ je samostatná síť oddělená od Internetu i od vnitřní sítě. Znemožňuje přímou komunikaci mezi těmito dvěma sítěmi a používá se pro filtrování protokolů UDP, ICMP, IGMP a dalších. Do demilitarizované zóny se nejčastěji umísťují aplikační, webové a poštovní servery. Z bezpečnostních důvodů se aplikační servery nedotazují databáze běžící na vnitřní síti přímo, ale databáze se replikuje do demilitarizované zóny.

3.3.2 Výběr firewallu

Vlastnímu konfigurování firewallu musí předcházet důkladná analýza potřeb subjektu, pro který je firewall pořizován, tak, aby byl zvolen firewall s nejvhodnějšími vlastnostmi. Firewally totiž dnes mohou nabízet velké množství funkcí, přičemž jednotlivé firewally se od sebe liší.

Z výše uvedené analýzy může ovšem také vyplynout, že z důvodu výskytu utajovaných dat ve vnitřní síti ji nelze vůbec s Internetem propojovat. Bylo by totiž prakticky nemožné zcela zabránit riziku odeslání těchto dat mimo vnitřní síť, ať už z důvodu jejich případného zašifrování nebo i jinak.

Rozhodne-li se nicméně uživatel pro připojení k síti a ochranu firewallem, musí si dále ujasnit, zda jeho potřebám odpovídá některý z dostupných komerčních firewallů, nebo zda jsou jeho požadavky natolik specifické, že je na místě nechat si firewall

navrhnout na míru. V každém případě je třeba předem myslet na v budoucnu potřebné up-date, podporu a údržbu.

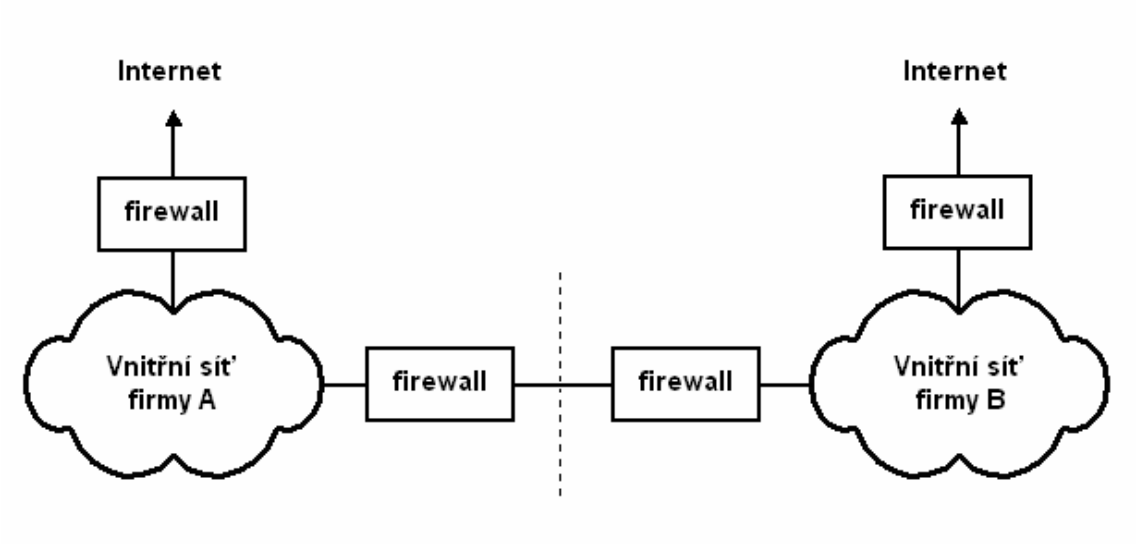
3.3.3 Funkce firewallu

Firewall může v zásadě fungovat buď na principu filtrace nebo proxy, některé ale nabízejí obě funkce a ty jsou pak využívány dle potřeby pro různé aplikace. Zároveň může firewall poskytovat i další funkce. Ty jsou primárně bezpečnostního charakteru, jako je třeba systém detekce a prevence vniknutí, lze ale rovněž říci, že také zpříjemňují a zjednodušují práci uživatelům. Jedná se například o antivirové a antispamové systémy nebo systém filtrování nežádoucího obsahu webových stránek. Práci s webovým prohlížečem zpříjemňuje například blokování reklam.

Výkon těchto funkcí je dán mj. i schopností firewallu ukládat informace o datovém provozu do logů (zvláštní soubory), vytvářet o těchto informacích reporty a podle daných pravidel (jsou-li na konkrétním firewallu stanovena) vyvolat při výskytu určité události definovanou akci. Takovou akcí (alertem) bývá nejčastěji spuštění nebo ukončení nějakého programu. Vhodnost možných alertů v konkrétním případě je třeba posuzovat individuálně. Možnostmi jsou odeslání informace o výskytu události na zadanou adresu, a to buď e-mailem nebo ve formě SMS, zapsání IP-adresy útočníka na černou listinu, ale v úvahu připadá také ukončení práce celého systému a jiné [1].

3.3.4 Extranet

Za určitých okolností je vhodné použít dva firewally za sebou. Jedná se o situaci, kdy je zapotřebí propojit dvě vnitřní sítě mezi sebou (vytvořit extranet), jak ukazuje obrázek. Účelem extranetu je umožnit mezi těmito vnitřními sítěmi efektivní komunikaci oddělenou od komunikace s veřejnou sítí, dvojí firewall ale zároveň dovoluje rozdělit hranici odpovědnosti za bezpečnost komunikace mezi zúčastněnými subjekty, tzn. odlišit, co pro kterou ze sítí tvořících extranet je vnitřní a co vnější síť.

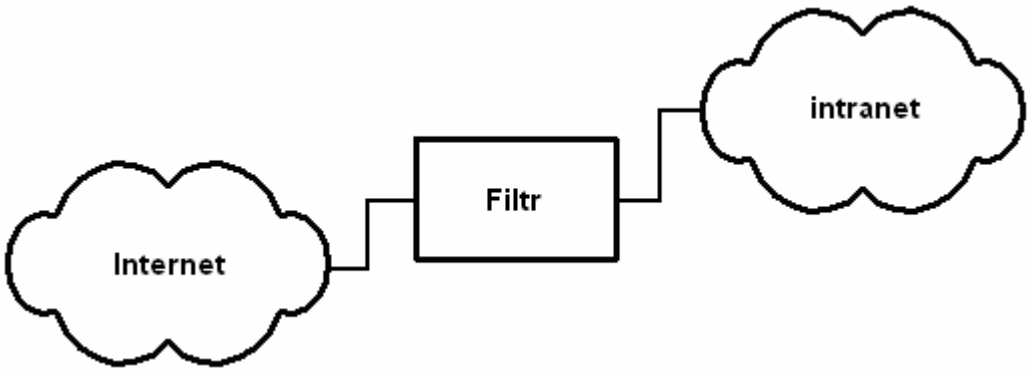


Obrázek 2 - Extranet

Systém firewallu v sobě kromě výše uvedeného může soustřeďovat rovněž funkce popsané v následujících subkapitolách části 3.1 (filtrace, wrappery, proxy, SOCKS). Ty se ovšem mohou aplikovat v rámci bezpečnostní politiky i samostatně, resp. se v různých kombinacích vzájemně doplňovat.

3.3.5 Filtrace

Jednou z podstatných možných schopností firewallu, resp. účinným prvkem síťové bezpečnosti je filtrace.



Obrázek 3 - Filtrace

Pakety procházející aktivním prvkem sítě jsou při filtraci kontrolovány a na základě jejich obsahu je rozhodnuto, zda jsou poslány dále nebo ne. Filtrováním se obsah datových paketů nemění. Hlavním cílem je vytvořit polopropustný filtr, který umožňuje vlastním uživatelům přístup do Internetu, ale zamezuje přístupu cizích uživatelů do vnitřní sítě.

Filtr se umísťuje mezi chráněnou síť a Internet, vždy na to rozhraní, které je blíže k útočníkovi. IP filtrování se provádí na základě údajů, které jsou uvedeny v záhlaví IP-datagramu, zejména IP-adresy odesilatele a příjemce. Udává se tak, které počítače mohou mezi sebou komunikovat, přičemž TCP filtrace rozlišuje přímo jednotlivé aplikace běžící na těchto počítačích. Kombinací filtrace IP a TCP se docílí, že spolu komunikují pouze specifické počítače, a to specifickými aplikacemi.

Rozlišujeme následující přístupy k filtraci:

- Vše se implicitně povolí a poté se pomocí pravidel zakazuje přístup vybraným počítačům na vybrané adresy.
- Vše se implicitně zakáže a poté se povolí pouze to, co je třeba. Tento způsob je považován obecně za bezpečnější.

Vlivem fragmentace paketu vznikají IP-datagramy, z nichž pouze ten první obsahuje i TCP záhlaví. Ostatní fragmenty jsou zejména staršími TCP filtry automaticky propouštěny dál a čekají na sestavení. Pokud se sestavení nepodaří do uplynutí časového limitu, je o tom odesilatel tohoto paketu informován prostřednictvím protokolu ICMP. Aby tato informace nepadla do rukou útočníka, odpověď ICMP se také filtruje.

Filtrace není dostačující, pokud se propojují dvě sítě přes Internet. Útočník nacházející se mezi oběma sítěmi může vydávat svou IP-adresu za IP-adresu patřící jedné ze sítí. V tomto případě je vhodné použít např. VPN.

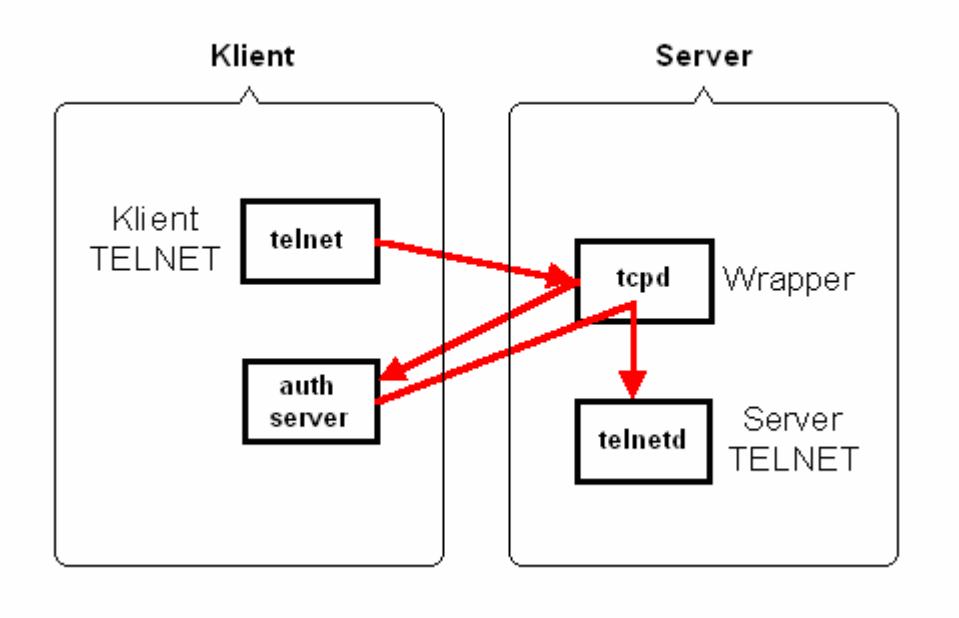
3.3.6 Wrappery

Dalším prvkem ochrany síťové bezpečnosti jsou tzv. wrappery. Jedná se o pojmenování programů, které se automaticky spouštějí před spuštěním samotného

serveru, aby ověřily klienta (program tcpd). K ověření klienta se přitom používají např. jednorázová hesla, čipové karty nebo jiné autentizační pomůcky. Teprve je-li autentizace klienta kladná, je příslušný server spuštěn. Nejjednodušší wrappery provádějí autentizaci dokonce jen sami na základě IP-adresy, resp. zjištění, zda konkrétní IP-adresa je nebo není uvedena v seznamu IP-adres, ze kterých je přístup povolen.

Wrappery se využívají nejčastěji pro zajištění přístupu z Internetu do vnitřní sítě, a to v operačním systému typu UNIX, přičemž se používá protokol TELNET pro servery telnetd, a protokol FTP pro servery ftpd.

Průběh autentizace přibližuje následující obrázek:



Obrázek 4 - Wrapper

Samotná ochrana wrappery není z důvodu relativně snadného podvržení IP-adresy tak dokonalá jako v případě filtrace v rámci proxy, které se věnuji v následující subkapitole, ale v některých případech může stačit.

3.3.7 Proxy

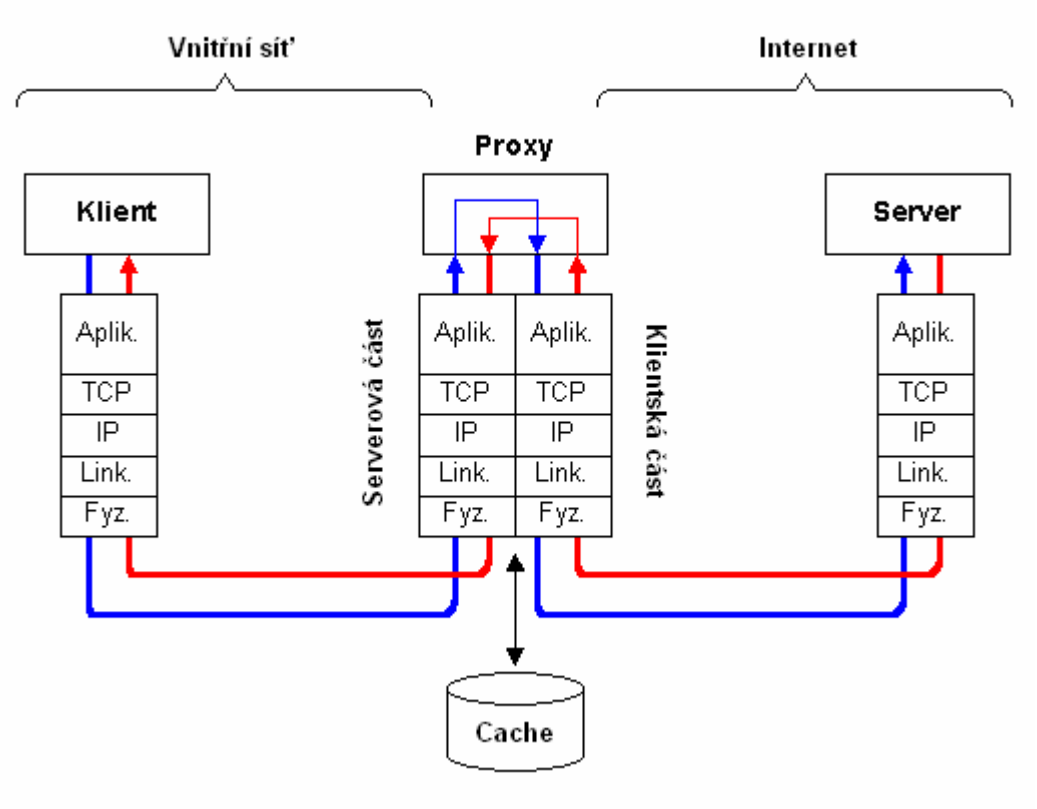
Proxy je program běžící na běžném počítači nebo zvláštním hardware. Zprostředkovává komunikaci mezi klientem a cílovým serverem, a to tak, že se pro klienta tváří jako sám server. „Serverová část proxy přijímá požadavky od klientů a předává je klientské části proxy, která jménem klientů předává požadavky cílovému serveru“ [1]. Je-li požadována rovněž protisměrná komunikace (reverzní proxy), zabezpečuje se propuštění klienta do vnitřní sítě pomocí VPN (např. připojení k poštovnímu serveru umístěnému ve vnitřní síti pracovníkem na dovolené nebo z domova).

Proxy typicky slouží pro připojení více klientů k Internetu. Tito jednotliví klienti nemusejí mít své veřejné IP-adresy, ale vystupují navenek pod jednou společnou IP-adresou.

Komunikace přes proxy může v sobě zahrnovat jen vlastní předávání dat, nebo může realizovat i funkci filtrace nebo cache.

Při předávání dat prostřednictvím proxy se zajistí anonymita klienta, a to tak, že se cílový server nedozví IP-adresu klienta, případně ani informace v podobě cookies či kompletní HTTP hlavičky (referrer). Funkce filtrace dále zajišťuje, že nebude umožněna komunikace se servery umístěnými na černé listině, nebo může být použita i pro detekování virů či pro šifrování a dešifrování procházejících dat apod. Další funkce proxy, kterou bývá cache, zvyšuje efektivitu komunikace. Nejčastěji zpracovávané požadavky jsou ukládány do vyrovnávací paměti na proxy a odtud jsou pak příště zodpovídány klientovi bez nutnosti dalšího kontaktování cílového serveru. Z důvodu častých změn dat na serverech se ale dnes „cachují“ obvykle jen firemní loga.

Tok dat přes proxy je vidět na následujícím obrázku:



Obrázek 5 - Proxy

3.3.8 SOCKS

Posledním prvkem sloužícím k zajištění komunikace klienta, resp. vnitřní sítě s vnější sítí, který je obvykle součástí firewallu, je SOCKS-server. Se SOCKS-serverem mohou komunikovat klienti schopní používat protokol SOCKS.

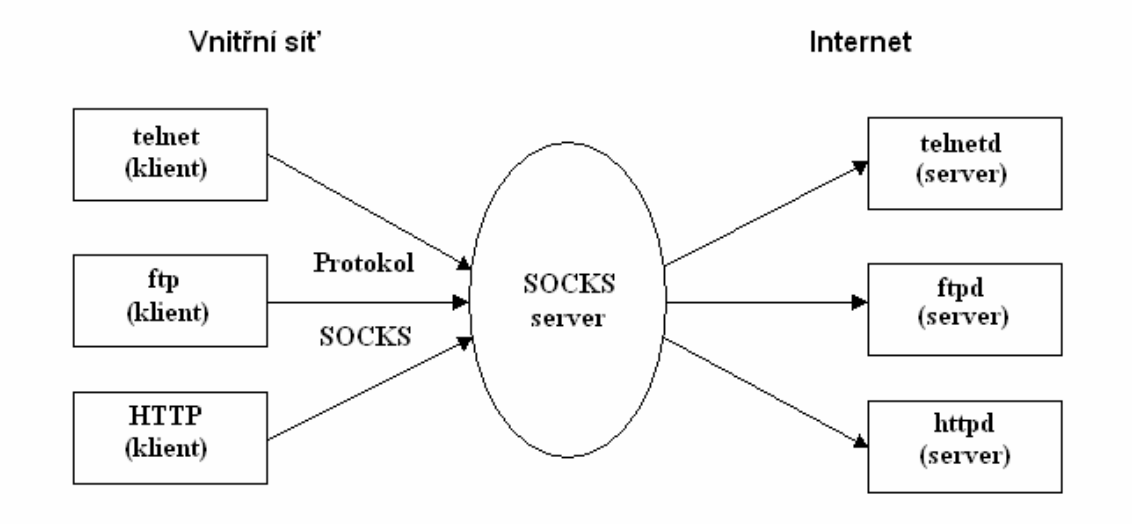
SOCKS-server funguje jako proxy, ale je společný a může přenášet všechny protokoly, a to nejen TELNET, FTP, HTTP, ale i privátní komunikační protokoly či kódovaná data. SOCKS je také nezávislý na použitém operačním systému. Protože ale SOCKS-server s komunikačními protokoly nijak nepracuje, nemůže také do přenášených dat nijak zasahovat; pracuje pouze s IP-pakety.

Komunikace se SOCKS-serverem probíhá formou dialogu, a to následovně: V prvním kroku se klient se SOCKS-serverem dohodnou na autentizační metodě. Poté může následovat buď autentizace bez dialogu (pouze na základě IP-adresy), nebo autentizační dialog, ve kterém se provede autentizace například na základě jména a

hesla uživatele. Ve třetím kroku klient sdělí SOCKS-serveru, na který cílový server se chce připojit a SOCKS-server zřídí pro komunikaci proxy (příkazem CONNECT, BIND nebo ASSOCIATE). Ve čtvrtém kroku pak může dojít k vlastní komunikaci klienta se vzdáleným serverem prostřednictvím zřízené proxy.

Příkazem CONNECT sděluje klient SOCKS-serveru adresu a port cílového serveru, se kterým mu má SOCKS-server navázat spojení. Příkazem BIND se chce klient připravit na příchozí volání. Příkaz ASSOCIATE slouží k předávání UDP-datagramů.

Princip SOCKS-serveru je zjednodušeně znázorněn na následujícím obrázku:



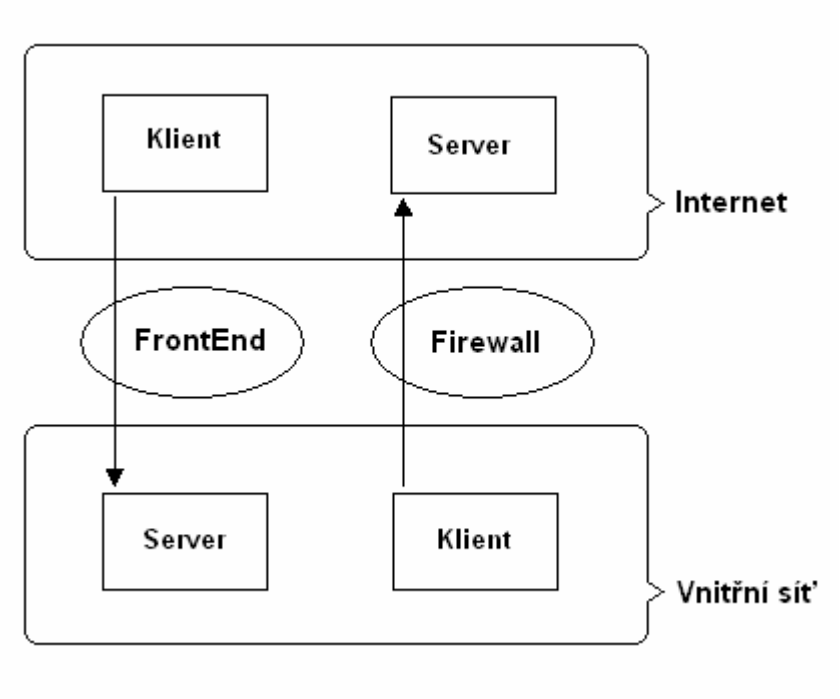
Obrázek 6 - SOCKS

Pouze pro přehlednost a doplnění uvádím, že existuje také systém WIN SOCKS, který ale přes podobnost názvů je řešením od SOCKS odlišným. WIN SOCKS je vyvinut a podporován pouze v prostředí Microsoft a svojí povahou se blíží více firewallu než proxy, protože využívá dvojího rozhraní - pro vnitřní síť a pro veřejnou síť. Ve WIN SOCKS aplikace komunikují se serverem MS Proxy tak, že volají API příslušné knihovny.

3.4 Internetový FrontEnd

Předmětem této práce jsou především otázky přístupu uživatelů z vnitřní sítě na Internet a ochrana vnitřní sítě před bezpečnostními riziky přicházejícími zvnějšku. Chtěl bych tímto ale alespoň zmínit, že existují rovněž situace, kdy je naopak žádoucí poskytnout uživatelům přistupujícím z Internetu bezpečný a pohodlný přístup k aplikacím uvnitř vlastní sítě. Řešením těchto situací je Internetový FrontEnd.

Zjednodušeně je rozdíl mezi komunikací přes firewall a komunikací přes Internetový FrontEnd vidět na následujícím obrázku:



Obrázek 7 - Internetový FrontEnd

Typickým příkladem Internetového FrontEndu je internetové bankovnictví.

4 Iptables

4.1 Obecná charakteristika

Iptables jsou nástroj, který umožňuje linuxovému nebo unixovému systému plně pracovat se síťovou komunikací. Pomocí něj si můžeme postavit firewall nebo sdílení internetu [7].

Iptables jsou součástí linuxové distribuce.

Firewall na iptables je stavový firewall, jehož funkcemi jsou například:

- filtrování paketů
- NAT
- logování
- změny v paketech
- routování
- QoS (protokol řízení datových toků v síti)

4.2 Pravidla

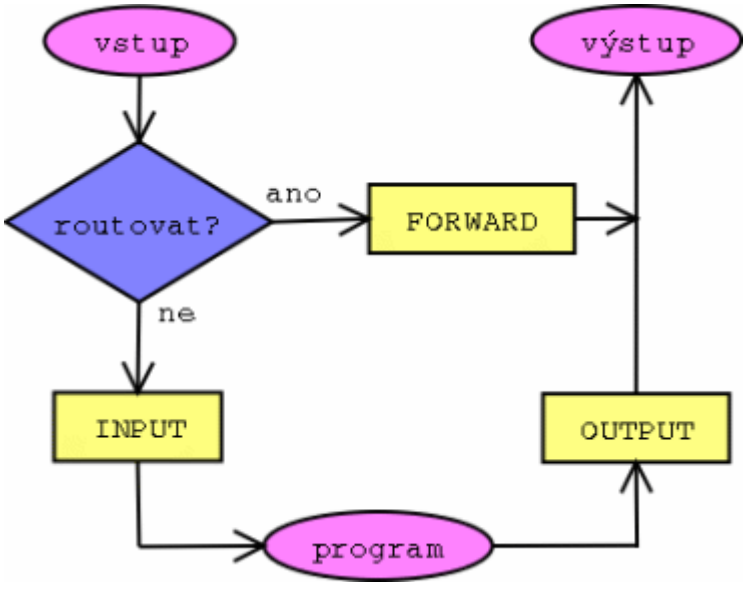
Natavení pravidel pro firewall se označuje jako konfigurace. V iptables se konfigurace zadává textovou formou, k tomu je třeba umět pracovat s příkazovou řádkou. Pro zjednodušení a zpříjemnění práce lze využít i nadstavby, kterou je např. FW Builder, umožňující práci v grafickém rozhraní, což mj. uživatele zbaví nutnosti znát podrobně všechny příkazy příkazové řádky. FW Builder je víceplatformový, použitelný jak pro Linux, tak pro Windows. Stejně jako iptables je i FW Builder distribuován zdarma.

Iptables používají pravidla, podle kterých se paketu buď povolí průchod (ACCEPT), nebo se paket zahodí (DROP), nebo se paket vrátí s chybovým hlášením (RETURN).

Pravidla jsou uspořádána v oddělených řetězcích (chains). Paket prochází řetězcem a narazí-li na pravidlo, které splňuje, je provedena příslušná akce odpovídající pravidlu a procházení paketu řetězcem se ukončí. Z toho vyplývá, že záleží na pořadí pravidel v řetězci. Některá pravidla ale tvoří výjimku a ani v případě, že paket podmínce vyhoví, se procházení řetězce neukončuje. Takovou výjimkou je například logování. V případě, že paket nevyhovuje žádné podmínce, použije se na něj výchozí, tzv. implicitní politika.

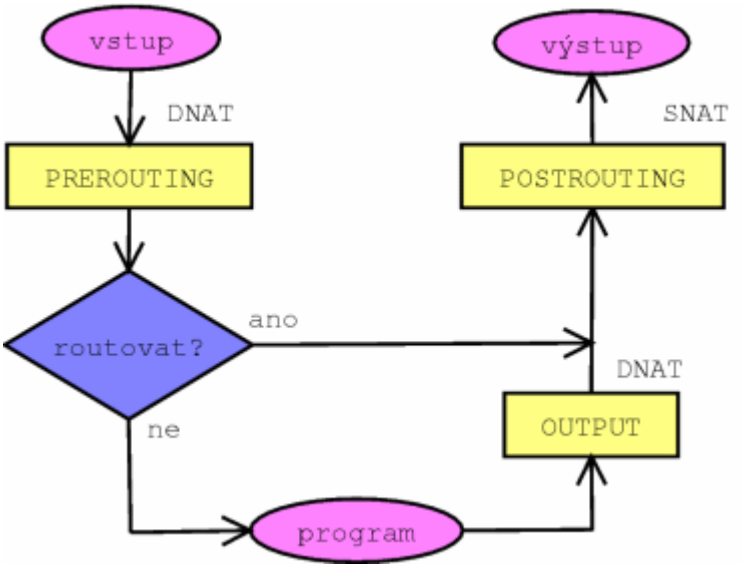
Samotné řetězce jsou uloženy v tabulkách. V tabulce typu filter jsou uloženy řetězce INPUT, OUTPUT a FORWARD. V tabulce typu nat jsou uloženy řetězce PREROUTING, POSTROUTING a OUTPUT. Tabulka typu mangle slouží pro optimalizaci datových cest.

Pravidla z řetězce INPUT se aplikují na pakety, které přicházejí na server. Pravidla pro pakety, které ze serveru odcházejí, obsahuje řetězec OUTPUT. Řetězec FORWARD se týká paketů, které se posílají z vnitřní sítě na vnější a naopak [8].



Obrázek 8 - Struktura filtrovací tabulky [9]

Narozdíl od v předchozím odstavci uvedených řetězců, které posílaly dál celé pakety, řetězce PREROUTING, POSTOUTING a OUTPUT z tabulky nat zasahují do hlavičky paketu, a to tak, že mění jeho zdrojovou IP-adresu a port. Na tomto principu funguje tzv. IP maškaráda.



Obrázek 9 - Struktura tabulky nat [9]

Pokud jde o optimalizaci datových cest, firewall dokáže minimalizovat dobu odezvy nebo maximalizovat propustnost paketů - jedno se děje na úkor druhého.

4.3 IP maškaráda

IP maškaráda je mechanismus, který umožňuje jednomu či více počítačům z vnitřní sítě přístup do Internetu. Funguje tak, že firewall dosadí za privátní IP-adresu počítače ve vnitřní síti svou veřejnou IP-adresu a stejně tak za port počítače ve vnitřní síti dosadí svůj port. Tyto změny si ukládá do tabulky pro další použití.

5 Konfigurace iptables

V této kapitole je vysvětlena syntaxe nutná pro práci s iptables a dále jsou zde uvedeny ukázky z konfigurace firewallu pro zabezpečení malé sítě.

5.1 Syntaxe

Syntaxe iptables nabízí obrovské množství kombinací nastavení. Dále je uveden formální zápis, vysvětlení jeho jednotlivých příkazů včetně možností:

```
iptables [-t table] command chain [N] [match options] [-j target]
  (1)       (2)        (3)      (4)          (5)            (6)
```

1) iptables

Sdělí shellu, že voláme program iptables a následující příkaz tedy bude pravidlem iptables.

2) [-t table]

Nastaví tabulku, pro kterou se pravidlo vztahuje. Při jejím neuvedení se použije výchozí tabulka filter.

- -t filter
- -t nat
- -t mangle

3) command

Značí akci, která se provede s pravidlem.

- -A (add - přidá pravidlo na konec řetězce)
- -D (delete - smaže pravidlo číslo N)
- -F (flush - smaže všechna pravidla v řetězci)

- -P (policy - nastaví výchozí politiku)
- -Z (zero - vynuluje počítadla)
- -R (replace - přepíše pravidlo číslo N)
- -I (insert - přidá pravidlo na pozici N nebo na začátek)
- -L (list - vypíše pravidla)
    - -v (verbose - podrobný výpis)
    - -n (numeric - vypíše IP adresy, porty jako čísla)
    - -x (exact - vypíše počítadla v bytech)

4) chain

Uvede řetězec, tedy umístění pravidla v tabulce.

Řetězce pro tabulku filter:

- INPUT
- OUTPUT
- FORWARD

Řetězce pro tabulku nat:

- PREROUTING
- POSTROUTING
- OUTPUT

Tabulka mangle obsahuje všechny výše zmíněné řetězce.

5) [match options]

Provede vlastní nastavení filtru. Každé pravidlo lze negovat pomocí vykřičníku.

- -p (protocol - TCP, UDP, ICMP)
- -s (source IP - zdrojová IP adresa)
- -d (destination IP - cílová IP adresa)
- -i (incoming interface - příchozí síťová karta)

- -o (outgoing interface - odchozí síťová karta)
- --sport (source port - zdrojový port - TCP/UDP)
- --dport (destination port - cílový port - TCP/UDP)
- --icmp-type (druh ICMP zprávy)
- --tcp-flags (kontrola nastavení flagů)
- --syn (úvodní paket TCP spojení)

6) [-j target]

Cíl, neboli co se provede s paketem, pokud splňuje pravidlo.

- ACCEPT (povolení, ukončí se procházení řetězce)
- DROP (zahození, ukončí se procházení řetězce)
- REJECT (zahození, přičemž se odešle zpráva ICMP o nedostupnosti portu)
- LOG (zalogování hlavičky paketu, procházení řetězce pokračuje)
- DNAT (změna cílové adresy a portu)
- SNAT (změna zdrojové adresy a portu)
- REDIRECT (zvláštní DNAT)
- MASQUERADE (zvláštní SNAT)
- MARK (označení paketu číslem)

5.2 Konfigurace

Nejdříve je třeba zahodit případnou předchozí konfiguraci:

```
iptables -F
iptables -t nat -F
```

Následuje nastavení výchozí politiky. Správnou volbou z hlediska bezpečnosti je zakázat vše, co není povoleno:

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP

iptables -P FORWARD DROP
```

Nyní je možné začít povolovat. Přístup z vnitřní do vnější sítě je volný:

```
iptables -A FORWARD -i eth1 -j ACCEPT
```

Z vnější do vnitřní sítě projdou jen již dříve navázaná spojení:

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

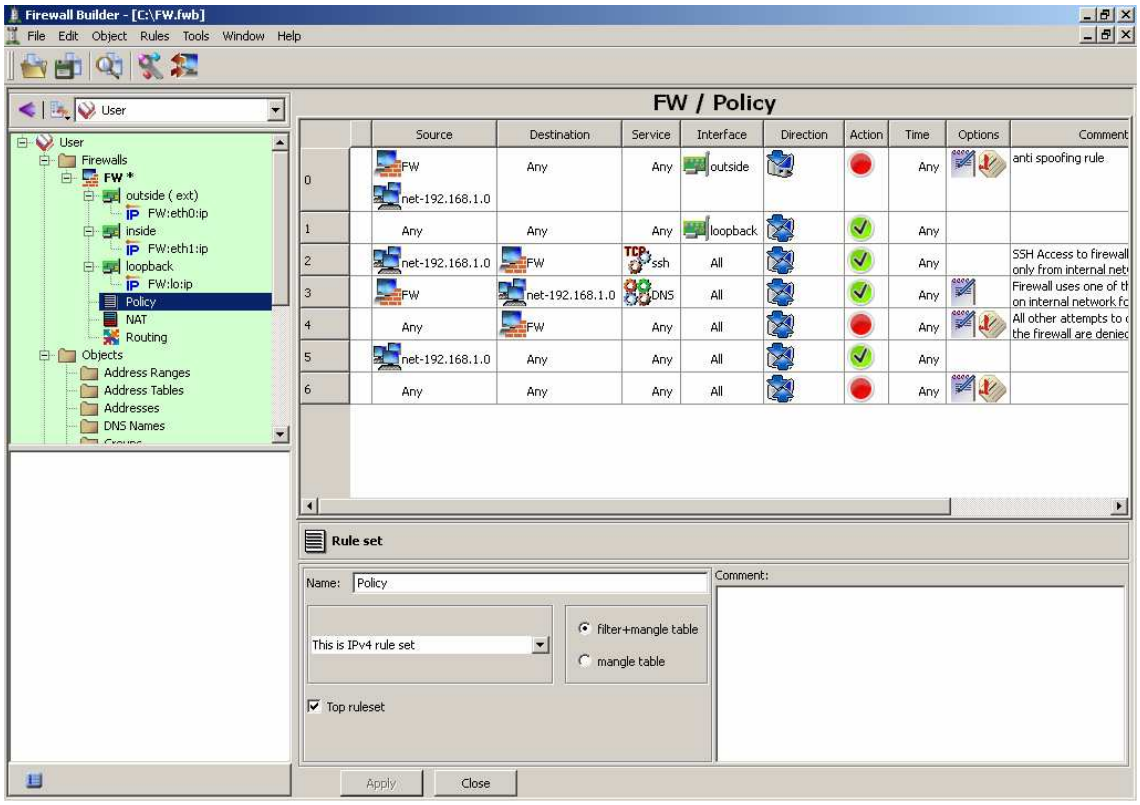
Je třeba ošetřit pakety přicházející na server. Pro běžné a všestranné použití je vhodné povolit port 80 (HTTP), 443 (HTTPS), 21 (FTP), 25 (SMTP), 110 (POP3), 143 (IMAP):

```
iptables -A INPUT -i eth0 -p TCP --dport 80 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP --dport 443 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP --dport 21 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP --dport 25 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP --dport 110 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP --dport 143 -j ACCEPT
```

Odchozí pakety mohou projít jen z našich IP adres:

```
iptables -A OUTPUT -s 127.0.0.1 -j ACCEPT

iptables -A OUTPUT -s 192.168.0.1 -j ACCEPT
```

Výše uvedené ukázky představují zadávání pravidel formou příkazové řádky, zatímco zmiňovaný FW Builder nabízí objektově orientovaný přístup, vlastní nastavování pravidel se provádí myší pomocí jednoduchých operací chytni a táhni.



Obrázek 10 - FW Builder

6 Závěr

6.1 Shrnutí

Na závěr shrnuji hlavní poznatky, které tato práce přinesla:

Protože při komunikaci mezi sítěmi různé úrovně důvěryhodnosti podstupují uživatelé určitá bezpečnostní rizika, je žádoucí tato rizika minimalizovat vhodnou bezpečnostní politikou. Výsledkem bývá sada opatření na hardwarové i softwarové úrovni, které společně přispívají k zajištění síťové bezpečnosti.

Mezi vlastní sítí nebo počítačem a veřejnou sítí může stát systém firewall, jehož funkcím a vlastnostem jsem se v práci věnoval především. Firewall v sobě může kombinovat hardwarová i softwarová opatření.

Firewall umožňuje obousměrnou bezpečnou komunikaci mezi sítěmi, ukládá informace o datovém provozu, rozpoznává výskyt určitých událostí a spouští adekvátní akce. Může tedy fungovat jako proxy, provádět filtraci, zahrnovat v sobě funkci SOCKS-serveru atd.

Iptables jsou nástroj, na kterém je možné postavit firewall s řadou funkcí. Iptables pracují s pravidly, resp. řetězci pravidel, které jsou uloženy v tabulkách v rozdělení dle vlastností. Přístup do Internetu z vnitřní sítě přes takovýto firewall je umožněn mechanismem IP maškaráda.

Závěrem mohu konstatovat, že firewall považuji za optimální prvek síťové bezpečnosti, a to jak v domácnostech, tak i v obchodních společnostech, státní správě a všude, kde je na síťovou bezpečnost kladen důraz. Na firewallech obecně oceňuji jejich velkou variabilitu, díky které je možné výběrem vhodného firewallu a následně jeho optimálním nastavením docílit vysokého stupně zabezpečení při práci s veřejnými sítěmi.

Pokud jde o iptables, považuji je za výborné řešení pro správce sítí a pokročilé uživatele, a to přes určité obtíže, které může způsobovat zvládnutí většího množství potřebných příkazů při konfiguraci firewallu. Jejich nezpochybnitelnou výhodou je fakt, že jako součást Linuxu jsou volně dostupné, lze je pořídit na Internetu. Je také obecně

známo, že komunita uživatelů Linuxu se vyznačuje ochotou svá díla sdílet, tudíž je možná kontrola zdrojových textů dalšími uživateli a dochází tak k odstraňování řady chyb. Jednou nakonfigurované situace je také možné znovu použít pro jiné podmínky.

6.2 Problémy

Při svém výzkumu jsem se setkal také s některými možnými úskalími práce s firewally, resp. iptables. Po formální stránce je jedním z nich nutnost znalosti anglického jazyka, což je ale potřeba společná pro celou oblast informačních technologií. Angličtina je nezbytná pro práci s odbornou literaturou, protože výběr pramenů v češtině je omezený a pro účely hlubšího seznámení s problematikou nemusí být dostatečný. V orientaci v cizojazyčných pramenech pomáhá fakt, že řada odborných pojmů se nepřekládá a i v českém prostředí se používá jejich anglická verze (firewall, server). To může sice někdy vést k jejich komolení v ústním projevu (feature vysl. fíčura, kešovat (ukládat do cache)) nebo komplikacím při dorozumívání s laickými uživateli, nicméně znalost alespoň odborných pojmů práci s cizojazyčnými zdroji informací napomáhá. Dále je angličtina nezbytná při psaní veškerých zdrojových kódů ve všech programovacích jazycích. V praxi také narůstá počet českých uživatelů - právnických osob, kteří z důvodů příslušnosti k nadnárodní skupině nebo s ohledem na zaměstnávané cizince využívají nastavení rozhraní svých počítačů v anglickém jazyce a potřeba znalosti odborného jazyka tak přesahuje potřeby počítačových specialistů a rozšiřuje se i na (nejen) odborné uživatele. Řešením je pouze otázku jazykové vybavenosti nepodcenit a své znalosti angličtiny stále zlepšovat.

Z věcného pohledu je hlavním problémem samotná složitost bezpečnostní politiky týkající se vnitřních sítí. Protože zabezpečení sítě se dociluje často kombinací více bezpečnostních prvků, z nichž některé jsou dodávány na komerční bázi ve finální podobě a jiné jsou předmětem různých úprav či programovány úplně na míru, je třeba věnovat velkou pozornost příslušné dokumentaci o zabezpečení, aby případné personální změny nevedly ke ztrátě zásadního know-how. Je přitom žádoucí, aby byl dodržován jednotný obecně srozumitelný styl společný pro interní IT pracoviště i případné externí programátory.

Citlivá je rovněž problematika vlastního nastavení firewallu, kdy je třeba mít sice hlavně na zřeteli bezpečnostní rizika plynoucí z práce se sítěmi, ale není možné k regulaci komunikace mezi sítěmi přistoupit tak, aby ve výsledku znemožňovala efektivní práci. Nezbytným předpokladem optimálního nastavení firewallu je tedy v praxi znalost potřeb uživatelů, ale zároveň i schopnost vysvětlit a obhájit nutná omezení vyvolaná zájmem na bezpečnosti komunikace. Je nutno si uvědomit, že bez uvědomělého přístupu uživatelů nelze bezpečnost vnitřní sítě zajistit pouze firewallem, resp. kombinací s dalšími prvky bezpečnosti. Uživatelé musejí znát a dodržovat zásady bezpečné práce s Internetem, neotvírat podezřelé e-maily, nepřihlašovat se na podezřelé webové stránky atd. V případě vnitřních sítí, u kterých příslušná bezpečnostní školení zajišťuje zaměstnavatel, který rovněž direktivně stanovuje bezpečnostní politiku, jsou podle mého názoru dobré předpoklady síťové bezpečnosti. Horší situace je podle mých zkušeností v případě soukromých počítačů, např. v domácnostech, kde je síťová bezpečnost i přes pořízení kvalitního firewallu chováním uživatele zejména při práci s e-mailem a Internetem v některých případech až „sabotována“.

Kromě výše uvedených možných komplikací při práci s firewally mohou vzbuzovat pochybnosti také některé právní otázky týkající se iptables. Jde zejména o případné právní důsledky vyplývající ze samotné povahy licence GNU/GPL aplikovatelné na iptables, a skutečnosti, že volné dílo může obsahovat chyby. GNU/GPL například ve svém článku 16. omezuje odpovědnost za případné škody způsobené softwarem v případech, kde to umožňuje národní právní řád, české právo ale právě vyloučení odpovědnosti za škodu neumožňuje. Uplatňování příslušných nároků poškozeného tedy připadá za určitých okolností teoreticky v úvahu, byť mi není žádný takový případ z praxe znám a unést důkazní břemeno by bylo pro eventuálního poškozeného jistě obtížné. Pokud by se ale poškození případných nároků úspěšně domáhali, jistě by to snížilo ochotu autorů volná díla sdílet. Právní otázky nejsou předmětem zájmu této práce, nicméně je třeba k nim brát v praxi zřetel, nejen pokud jde o iptables.

6.3 Zhodnocení práce

Celkově práci hodnotím jako pro mě přínosnou, a to z důvodů splnění cílů, které jsem si v jejím úvodu vytyčil. Podle mého názoru se podařilo shromáždit a analyzovat informace o firewallech na iptables v množství odpovídajícím požadovanému rozsahu práce a logicky je utřídit, z výše uvedeného textu jsou zřejmé klady i zápory možných řešení a vlastní pohled na problémy, které při zpracovávání práce vyvstaly.

Zájemci o síťovou bezpečnost mohou tuto práci nalézt v systému Moodle ČZU jako součást dobrovolného semináře bezpečnosti, který pořádá katedra informačního inženýrství.

Další pokračování práce v oblasti síťové bezpečnosti - firewall na iptables by se mohlo mj. zabývat i zjištěním povědomí uživatelů o zásadách práce v síti, například formou dotazníkové metody, nebo navržením obsahu školení zaměstnanců pracujících se sítí, které by efektivně přispělo ke zlepšení úrovně bezpečnosti příslušné sítě.

V případě pokračování ve studiu bych se k tématu rád vrátil a hlouběji ho rozpracoval ve své diplomové práci. V praxi se s problematikou síťové bezpečnosti a firewallů setkávám již nyní jako zaměstnanec státní správy v oblasti zdravotnictví, kde je otázka zajištění bezpečnosti mimořádně citlivá a aktuální.

7 Seznam literatury

[1] DOSTÁLEK, L., et al. *Velký průvodce protokoly TCP/IP: Bezpečnost*. 2. aktualizované vydání. Praha: Computer Press, 2003. 592 s. ISBN 80-7226-849-X.

[2] DOSTÁLEK, L. - KABELOVÁ, A. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vydání. Praha: Computer Press, 2000. 426 s. ISBN 80-7226-323-4.

[3] CAMERON, R., et al. *Configuring Juniper Networks Netscreen & SSG Firewalls*. Rockland: Syngress Publishing, Inc., 2007. 745 s. ISBN 1-59749-118-7.

[4] ZWICKY, E. D. - COOPER, S. - CHAPMAN, D. B. *Building Internet Firewalls*. 2. vydání. O'Reilly & Associates, 2000. 890 s. ISBN 1-56592-871-7.

[5] MCNAB, C. *Network Security Assessment*. O`Reilly Media, Inc., 2004. 396 s. ISBN 0-596-00611-X.

[6] *Wikipedie, otevřená encyklopedie - Firewall* [online]. 15.03.2009 [cit. 2009-04-17]. <http://cs.wikipedia.org/wiki/Firewall>.

[7] BOTOŠ, Csaba. *Vše o iptables* [online]. 10.1.2006 [cit. 2009-04-19]. <http://www.root.cz/clanky/vse-o-iptables-uvod>.

[8] POLOCH, Radim. *Iptables - stavový firewall* [online]. 15.9.2006 [cit. 2009-04-19]. <http://www.owebu.cz/linux/vypis.php?clanek=880>.

[9] PETŘÍČEK, Miroslav. *Stavíme firewall* [online]. 18.12.2001 [cit. 2009-04-19]. <http://www.root.cz/clanky/stavime-firewall-1>.

[10] *RFC-2979 Behavior of and Requirements for Internet Firewalls* [online] c2000 [cit. 2009-04-17]. <http://www.ietf.org/rfc/rfc2979.txt>.

8 Přílohy

8.1 Seznam zkratek

LAN	Local Area Network
GPL	General Public License
IP	Internet Protocol
TCP	Transmission Control Protocol
ICMP	Internet Control Message Protocol
VPN	Virtual Private Network
UDP	User Datagram Protocol
IGMP	Internet Group Management Protocol
API	Application Programming Interface
DMZ	Demilitarized Zone
SMS	Short Message Service
IT	Information Technology
QoS	Quality of Service

8.2 Seznam obrázků

Obrázek 1 - Firewall
Obrázek 2 - Extranet
Obrázek 3 - Filtrace
Obrázek 4 - Wrapper
Obrázek 5 - Proxy
Obrázek 6 - SOCKS
Obrázek 7 - Internetový FrontEnd
Obrázek 8 - Struktura filtrovací tabulky
Obrázek 9 - Struktura tabulky nat
Obrázek 10 - FW Builder