ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA ELEKTROTECHNICKÁ

BAKALÁŘSKÁ PRÁCE

1998

Marek Uher

Obsah

Souhlas s použitím výsledků

Souhlasím s tím, aby katedra výpočetní techniky ČVUT mohla použít výsledky a závěry této bakalářské práce.

Marek Uher

V Kladně dne 20.8.1998

Zadání bakalářské práce

Student:

MAREK UHER, skupina 23, ročník IV.

Téma práce:

Zabezpečení podnikové sítě (Intranetu)

Pokyny pro vypracování:

Vytvořte systém zabezpečení intranetové sítě před průniky z Internetu. Systém bude složen z několika vzájemně spolupracujících částí: paketový filtr (Cisco), firewall (GNU/Linux) a autentifikace přístupu do interních databází (běžících v OS Solaris, SCO UNIX a Novell). Systém dále bude zabezpečovat ochranu webového serveru a ERL serveru.

Vedoucí práce:

Ing. Mgr. Petr Zemánek, Csc.

Pracoviště:

Katedra počítačů FEL ČVUT

Poděkování

Rád bych touto cestou poděkoval všem, kteří mi pomáhali s mou bakalářskou prací. Především bych rád poděkoval panu Ing. Ivo Musilovi z firmy Corpus, který mě obeznámil s hlubší problematikou síťové bezpečnosti. Jeho rady a nápady znatelně ovlivnily mou práci při budování firewallu.

Dále bych chtěl poděkovat Ing. Jaroslavu Mejstříkovi z České národní banky a Ing. Jiřímu Přibylovi z katedry telekomunikační techniky ČVUT v Praze za poskytnuté konzultace v otázkách bezpečnostní politiky a její tvorby. Jejich rady mi pomohly při vytváření bezpečnostního modelu zabezpečení počítačové sítě.

Zvláštní poděkování patří ekonomicko-technickému náměstkovi Ústavu hematologie a krevní transfuze panu Ing. Vladimíru M. Keřkovi, který mi poskytl podporu a prostředky pro realizaci firewallu.

Také bych rád poděkoval pracovnicím ze Střediska vědeckých lékařských informací Ústavu hematologie a krevní transfuze paní Ing. Marii Horníkové a paní Ing. Mileně Pohlové.

Nakonec bych chtěl poděkovat vedoucímu oddělení Správy počítačového informačního systému Ústavu hematologie a krevní transfuze panu Bc. Janu Vycudilíkovi za jeho rady spojené se samotnou realizací firewallu.

1 Úvod do síťové bezpečnosti

1.1 Problematika síťové bezpečnosti

Bezpečnost počítačových sítí je komplexním problémem. Je zřejmé, že tato problematika nemůže být řešena zcela izolovaně od ostatních oblastí bezpečnosti, jako jsou zabezpečení přístupu vnitřních uživatelů k interním serverům, správa lokálních uživatelů, monitorování podezřelých událostí v interní síti nebo administrace a správa informačních systémů. Na druhou stranu můžeme říci, že vzájemná ochrana sítí by měla být navržena tak kvalitně, aby byla nezávislá na technologiích použitých uvnitř jednotlivých sítí a komunikace mezi těmito sítěmi byla zcela řízena ochrannými prvky, které tak izolují potencionální bezpečnostní problémy v jedné z připojených sítí od sítí ostatních.

Mezi různými bezpečnostními projekty je typizovaným dílčím úkolem bezpečné připojení lokální sítě do veřejné sítě Internet a následná komunikace dvou a více subjektů (sítí, uživatelů,...) přes tuto veřejnou síť s využitím mechanizmů autorizovaného přístupu popřípadě šifrované komunikace.

V dobách, kdy nebyly počítače zapojeny do sítě, se bezpečnost zajišťovala fyzickými prostředky. K fyzickým kontrolním prostředkům patří zámky na dveřích, dozorčí u vchodů, záložní kopie důležitého softwaru a dat a fyzické prostory s výpočetní technikou volené s ohledem na minimalizaci škod způsobených případnými živelnými pohromami. Některá opatření spadající mezi výše uvedené najdou uplatnění i dnes. Přesto jsou někdy jednoduché fyzické kontroly opomíjeny, zatímco náročnější a dražší přístupy jsou propagovány, i když často přinesou z hlediska bezpečnosti znatelně menší efekt než jednoduchá fyzická opatření.

Cílem moderní informační bezpečnosti je zavádění kontrolních opatření zajišťujících současně ***diskrétnost*** (utajení), ***integritu*** (celistvost) a ***dostupnost*** (použitelnost).

Mezi kontrolní prostředky lze zařadit šifrování, kontroly softwaru (vývojové kontroly, kontroly operačního systému, kontroly spustitelných programů,...), kontroly hardware a konečně administrativní, legislativní a etické kontroly.

Počítače připojené k síti, zejména pak k Internetu, jsou vystaveny většímu ohrožení bezpečnosti, než systémy izolované. Zabezpečení takového systému pak slouží zejména ke snížení rizik souvisejících právě s připojením počítačů do sítě. Tím ale vzniká dilema - ze své podstaty stojí připojení k síti a počítačová bezpečnost obecně proti sobě. Funkcí sítě je zvýšení možnosti přístupu k dalším počítačovým systémům (službám, informacím, atd.), zatímco bezpečnost se snaží tento přístup omezit. Z toho vyplývá, že zajištění síťové bezpečnosti představuje kompromis mezi otevřeným přístupem a absolutní zabezpečením.

1.2 Internet a bezpečnost

Internet je fenomén, který ovládá nejenom počítačový průmysl, ale stále více se dotýká každého z nás, ať již pracovně nebo v soukromém životě. Proto, aby každá společnost mohla využít obrovský potenciál této sítě a technologie s ní související, je důležité si uvědomit fakt, že Internet je sítí veřejnou. To přináší řadu výhod, od možnosti výběru nejvhodnějšího lokálního poskytovatele (ISP – Internet Service Provider), přes možnost efektivního propojení sítě poboček až po snadnou komunikaci se zahraničním partnerem. Zajímavá je také vysoká dostupnost veřejných dat na Internetu a naopak nízké náklady na publikování vlastních informací. Tato otevřenost Internetu však současně znamená, že pro připojení se k němu je nezbytné zavést mechanismy ochrany vnitřní sítě - ***Intranetu*** a zajistit případné utajení přenášených dat a soukromých informací uložených v interních databázích.

Každá instituce nebo firma, která se rozhodne v jakékoliv míře využívat služeb sítě Internet, je postavena před otázku síťové bezpečnosti. To, jakým způsobem se s ní vypořádá, do velké míry ovlivní přínosy a případné škody způsobené podceněním rizik, která sebou tato velká datová síť přináší.

Využití sítě Internet, ale také množství jiných datových zdrojů, jako jsou například virtuální privátní sítě, které plánuje v budoucnu realizovat Ministerstvo zdravotnictví, je nezbytné řešit komplexně tak, aby interní síť byla maximálně zabezpečena. Otázka bezpečnosti patří při propojování sítí mezi klíčové, a je proto nezbytné jí věnovat maximální pozornost.

1.3 Koncepce bezpečnostního modelu

Každé realizaci bezpečného připojení musí předcházet návrh bezpečnostní koncepce. Jedná se o komplexní problematiku, kdy zanedbání jednoho prvku může zmařit vynaložené náklady a současně ohrozit cenná data.

Stejně jako chybná konfigurace nákladného ochranného systému je i volba nevyzrálého operačního systému na kritické pozici styčného místa s veřejnou sítí ohrožením bezpečnosti interní sítě [16].

Na počátku každého bezpečnostního projektu je návrh topologie jednotlivých síťových prvků. Nejprve je nutno vytvořit seznam síťových služeb, které hodlá organizace uvažující o připojení do Internetu využívat. V následujícím kroku se provede specifikace síťových serverů. Jejich seznam by měl zahrnovat systém firewallu, proxy server, interní jmenný server (DNS), webové a aplikační servery, poštovní server a další servery podle konkrétních požadavků. Tento krok je úzce provázán se specifikací koncových uživatelských stanic (např. jejich přibližný počet, použité operační systémy, použitá kabeláž,...). Takto získané informace se použijí při konečném návrhu topologie interní sítě a při realizaci připojení této sítě do Internetu. Z toho vyplývá, že koncepce připojení interní sítě do sítě Internet musí optimálně řešit dvě základní body:

- bezpečné zpřístupnění externích zdrojů (serverů) ve veřejných sítích uživatelům chráněných sítí
- bezpečné vystavení vlastních zdrojů do externích sítí a to buď všem uživatelům nebo pouze vybraným uživatelům (sítím) při použití příslušných mechanismů autorizovaného přístupu

1.4 Firewally

Jedním z nejdůležitějších článků v řetězci síťových bezpečnostních opatření je ***firewall***. Firewall je způsob jak zabezpečit spojení mezi Intranetem a Internetem. Nejčastěji se firewall umisťuje na místo s nejvyšším potencionálním rizikem - do místa, kde se interní síť propojuje s Internetem. Zřízení firewallu může velmi redukovat případy napadení, kdy se externí útočníci snaží proniknout do vnitřního systému a sítí. Při absenci firewallu hrozí také reálné nebezpečí spočívající v možnosti zkompromitování diskrétních informací (nezašifrovaných hesel, citlivých dat,...) nechtěně zaslaných interními uživateli do Internetu.

Přesná definice firewallu neexistuje, lze použít pouze volnější výklad: firewall je pojmenování celého systému skládajícího se z filtru paketů na IP úrovni, systému proxy serverů a dalších bezpečnostních mechanismů. Pokusíme-li se o přesnější technický popis, lze firewall popsat jako ucelený systém softwaru a hardwaru, jehož hlavním úkolem je provádět filtraci paketů na síťové úrovni a podle definovaných pravidel řídit komunikaci. Dnešní moderní firewally (např. *Check Point FireWall-1* [20]) výrazně překračují rámec této základní definice, neboť poskytují mnohem více služeb určených pro zajištění bezpečnosti interní sítě.

2 Zabezpečení Intranetu

2.1 Základní bezpečnostní principy

Při návrhu komplexních bezpečnostních opatření je velmi důležité si dopředu rozmyslet, co a jak bude chráněno. Je také potřeba si uvědomit základní bezpečnostní principy. Je možno také vycházet z některých formálních kritérií bezpečnosti (např. ITSEC, TCSEC, ITSEM a další, viz. [1] a [2]), ale tato kritéria vycházejí z názoru, že bezpečnost produktu, resp. systému, je měřitelná počtem a rozsahem ochranných mechanizmů zavedených během návrhu a vývoje.

V praxi však bezpečnost není měřitelná pouze existencí nebo počtem bezpečnostních mechanizmů, ale spíše jejich správným nasazením a používáním. Je proto daleko lepší se při návrhu bezpečnostních opatření týkajících se počítačové sítě řídit principy, která prověřila praxe. V následujících odstavcích se pokusím shrnout základní bezpečnostní principy.

- ***Co není povolené, je zakázané***

Tento princip (v anglické literatuře [7] označovaný jako „*default to deny principle*") je základním principem při návrhu a tvorbě rozsáhlých kombinací přístupových práv většího počtu oprávněných uživatelů systému. Tento princip zajišťuje již v samotném základě vysokou bezpečnost navrhovaných bezpečnostních opatření. V případě omylu jsou totiž oprávněnému uživateli obvykle přidělena menší privilegia, než jaká potřebuje pro svou práci. Dá se očekávat, že takový omyl bude poměrně rychle objeven a napraven. Důsledkem tohoto omylu bude omezení činnosti uživatele, protože uživatel nebude schopen využívat služby systému v předpokládaném rozsahu.

- ***Nejmenší privilegia***

Princip (v anglické literatuře [7] označovaný jako „*least privileges principle*"), který stanovuje následující bezpečnostní pravidlo: „oprávněnému uživateli systému mají být přidělena jen taková privilegia, jaká nutně potřebuje pro svou činnost, a ne větší“.

Hlavním důvodem zavádění tohoto pravidla je minimalizace možné škody, a to jak zaviněné chybou nebo omylem oprávněného uživatele systému, tak i v případě jeho pokusů o zneužití přidělených oprávnění.

- ***Obecné bezpečnostní principy***

Do této kategorie spadají ostatní bezpečnostní principy. Bližší specifikace těchto principů již přímo nesouvisí s mojí bakalářskou prací. Případné zájemce mohu odkázat na literaturu [1], [2] a [8]. Do této skupiny například náleží: rozdělení povinností (výkonná, kontrolní a schvalovací funkce je rozdělena mezi více subjektů), zachování bezpečnosti systému při havárii a při obnovení jeho provozu, vyloučení existence slabého bodu (nutnost odstranění jediné, nezálohovatelné anebo jinak nechráněné komponenty systému, na níž v plné míře závisí správný a bezporuchový chod systému), zajištění pravidelné revize bezpečnostních principů a pravidel.

2.2 Plánování bezpečnosti

Druhým a patrně nejdůležitějším krokem při návrhu zabezpečení sítě je vytvoření ***síťové bezpečnostní politiky***. Tato činnost patří k nejméně oblíbeným krokům v celém postupu návrhu zabezpečení. Téměř všichni pracovníci z počítačové komunity se vždy snaží nalézt pro každý problém technické řešení. V tomto případě je ale potřeba sestavit dohromady vysvětlující text na úrovni znalostí běžného zaměstnance dané společnosti o bezpečnostní politice a postupech. Je ale třeba vzít v úvahu, že dobře promyšlený bezpečnostní plán usnadní rozhodování o tom, co se má chránit, kolik se má do ochrany investovat a kdo bude za jednotlivé ochranné postupy zodpovědný. V příloze 6.4 je uveden výčet citlivých míst interní sítě Ústavu hematologie a krevní transfuze (dále jen ÚHKT) v Praze. Bohužel se mi nepodařilo sestavit úplnou bezpečnostní politiku, neboť každé oddělení ÚHKT má svou specifickou bezpečnostní politiku. Sjednocení těchto různorodých politik do obecné koncepce je nad rámec této bakalářské práce. Například konečné znění bezpečnostní politiky na klinickém a transfuzním úseku není zcela vyřešeno. Jeho finální podoba je předmětem rozsáhlé diskuse mezi lékaři a Správou počítačového informačního systému ÚHKT.

Řešení tohoto problému je dlouhodobá záležitost. Pracovníkům Správy počítačového informačního systému se podařilo vytvořit Provozní řád počítačové sítě ÚHKT, kde je alespoň částečně vyřešena problematika síťové bezpečnostní politiky.

2.3 Riziková analýza

Plánování bezpečnostních opatření začíná rizikovou analýzou. V procesu rizikové analýzy se vymezují rizika a jejich možné důsledky. Nejprve se vymezí všechna možná rizika, která by mohla ohrozit počítačovou síť nebo informační systém. Ve druhém kroku se navrhnou možná protiopatření včetně jejich ceny. Riziková analýza vede k plánu návrhu bezpečnostních opatření, který vymezuje odpovědnosti za realizaci určitých kroků směřujících ke zvýšení bezpečnosti.

Hlavní kroky rizikové analýzy jsou tyto:

- vymezení hodnot prvků systému
- stanovení zranitelnosti hodnot systému
- odhad pravděpodobnosti zneužití zranitelných míst
- výčet odhadu ročních ztrát
- výčet použitelných bezpečnostních opatření a jejich ceny
- plán ročních úspor dosažených v důsledku zavedených bezpečnostních opatření

Pro realizaci prvních dvou kroků jsem sestavil přehlednou tabulku, (tab. č. 1) ze které je již na první pohled patrný obsah návrhu zmíněných bodů. Tato tabulka dává obecnou představu o tom, co se s užitnými hodnotami systému v případě napadení může stát.

U dané instalace je třeba specifikovat možnosti konkrétních změn hardwaru, softwaru, datových položek a dalších hodnot. Tabulka slouží k lepšímu pochopení hlavních cílů ochrany počítačových systémů, mezi které patří zajištění integrity, diskrétnosti a dostupnosti. Zranitelnost představuje každou situaci, která může vést ke ztrátě některé z těchto základních vlastností. Místa zranitelnosti informačního systému nebo počítačové sítě lze určit analýzou situací, které mohou vést k ohrožení těchto základních vlastností.

Prvek	Utajení	Integrita	Dostupnost
Hardware	zcizení, zneužití	přetížení, zničení, narušení (úmyslné či náhodné), hardwarová chyba	ztracení, zcizení, zničení, nedostupnost (úmyslná či náhodná)
Software	zcizení, kopírování, zneužití	modifikace, narušení, trojský kůň, viry, softwarová chyba	vymazání, nesprávné založení, ukončení užívacího práva
Data	odhalení, přístup vnějšího narušitele	poškození chybou: softwaru, hardwaru nebo uživatele	vymazání, nesprávné založení, zničení
Personál	únos, vydírání, korupce	záměrné nebo nezáměrné poškození či zničení neznalostí obsluhy	výpověď, odchod na dovolenou
Dokumentace	zcizení, kopírování	falšování, nesprávné a matoucí informace	ztráta, zcizení, poškození
Materiál	zcizení, zneužití	zničení	ztráta, zcizení, poškození

Tab. č.1 Užitné hodnoty a způsoby napadení

Tabulka byla sestavena podle pokynů uvedených v [2]. Informace obsažené v tabulce mohou sloužit k širším úvahám o možnostech napadení systému. Formu tabulky lze proto podle potřeby modifikovat a tím přizpůsobit tabulku konkrétním požadavkům. V tabulce nejsou uvedeny všechny možné situace vedoucí ke ztrátě základních vlastností, neboť je nelze beze zbytku vyjmenovat. Uvedl jsem pouze ty nejznámější nebo nejčastěji vyskytující se způsoby ohrožení základních vlastností informačního systému.

Dalším, v pořadí již třetím krokem, je odhad pravděpodobnosti vzniku nežádoucích situací. Tento krok určuje četnost výskytu nežádoucích situací. Pravděpodobnost vzniku takových situací závisí na přísnosti přijatých bezpečnostních opatření a na pravděpodobnosti toho, že někdo nebo něco naruší tato opatření. Odhad pravděpodobnosti výskytu některých jevů je za určitých okolností nemožný. Nicméně existují zdroje informací a metody, pomocí kterých lze pravděpodobnost výskytu takových jevů přibližně určit. V odborné literatuře [2] jsem vyhledal tabulku (tab. č. 2), která uvádí četnost výskytu náhodných jevů. Tato tabulka byla získána analýzou několika odlišných přístupů pro odhad pravděpodobnosti vzniku nežádoucích situací. Pro sestavení této tabulky byl v konečné fázi použit matematický aparát pro výpočet pravděpodobnosti náhodného jevu. Takto získané hodnoty jsou korigovány s ohledem na statisticky získaná data.

Čtvrtým krokem rizikové analýzy je odhad finančních ztrát vyvolaných výskytem nežádoucích jevů. Některé finanční částky lze stanovit snadno, jako například cenu za výměnu hardwarového dílu. Stejně tak i cenu za výměnu části softwaru lze poměrně snadno odhadnout z jeho pořizovací ceny. Nicméně cenu za nedostupnost části hardwaru nebo softwaru, nebo za kompromitaci části dat lze stanovit jen velmi těžko. Zpracování důkladné analýzy rizik vyžaduje vyčíslení těchto cen.

Protože nejsem odborníkem v otázkách finančního managementu, tuto část rizikové analýzy jsem do svého projektu nezahrnul. Důležitost tohoto kroku však spočívá v tom, že realistické odhady potenciálních škod mohou zvýšit zájem o bezpečnost počítačové sítě a systému informatiky obecně. Pomohou tak vymezit oblasti, kterým by měla být věnována zvýšená pozornost.

Četnost	Kategorie
Častěji než jednou denně	10
Jednou denně	9
Jednou za tři dny	8
Jednou za týden	7
Jednou za čtrnáct dní	6
Jednou za měsíc	5
Jednou za čtyři měsíce	4
Jednou za rok	3
Jednou za tři roky	2
Méně než jednou za tři roky	1

Tab. č.2 Kategorizace četnosti výskytu náhodných jevů

V dalším kroku je třeba vytvořit přehled současných bezpečnostních opatření. Protože jsem nezahrnul do svého projektu předchozí bod (odhad finančních ztrát), předpokládám, že ztráty způsobené napadením nebo zneužitím budou nepřípustně velké. Do dnešní doby byla v ÚHKT otázce síťové bezpečnosti věnována relativně malá pozornost. Proto bylo třeba nadefinovat bezpečnostní opatření zcela nově, bez vazeb na předchozí bezpečnostní opatření. Jedna cesta k určení bezpečnostních opatření vede přes rizikové faktory. Tak například riziko ztráty dat lze potlačit periodickým zálohováním, náhradními paměťovými médii, kontrolami přístupu znemožňujícími neautorizovaný přístup, fyzickou ochranou zabraňující průniku do počítačového sálu a zcizení hardwaru. Některá rizika spojená se zneužitím informací uložených v interních databázích ÚHKT však nelze ani vyčíslit. V databázích ÚHKT jsou uložena data finančního účetnictví, informace o zaměstnancích a zejména informace o pacientech. Posledně jmenované informace (mezi kterými jsou i informace o dárcích krve s diagnózou AIDS) jsou velmi citlivé. Jejich prozrazení či zcizení by mělo zcela jistě vážné důsledky. Proto je cena zneužití těchto informací zvláště vysoká.

Účinnost každého bezpečnostního opatření, potlačujícího výše zmíněná rizika, se hodnotí. K výběru vhodných bezpečnostních opatření pro potlačení konkrétního rizika může napomoci rozbor všech možných bezpečnostních aspektů chráněného systému.

V posledním kroku rizikové analýzy se vyčíslí skutečné náklady a úspory spojené se zavedením nových bezpečnostních opatření. Efektivní náklady jsou reprezentovány cenou bezpečnostních opatření sníženou o předpokládanou redukci roční ztráty v důsledku zavedených kontrol. Skutečný výnos bezpečnostních opatření může být dokonce negativní, jestliže náklady na snížení rizika budou nižší, než cena bezpečnostních opatření.

Následující tabulky obsahují analýzu nákladů a úspor pro zvolenou realizaci ochrany sítě ÚHKT. Je potřeba zdůraznit, že uváděné finanční částky jsou pouze přibližné, protože jsem neměl k dispozici odhad ročních finančních ztrát vyvolaných výskytem nežádoucího jevu podle čtvrtého bodu rizikové analýzy. Uvedené částky je proto potřeba brát pouze jako orientační. Tento bod rizikové analýzy bude v budoucnu podroben přesnému vyčíslení finančních částek v součinnosti s ekonomickým oddělením ÚHKT. Takto získané skutečné finanční částky by patrně vedly k vyčlenění větších částek na bezpečnost a tím i k celkovému lepšímu zabezpečení počítačové sítě a informačního systému ÚHKT. Nejdůležitější informace, které můžeme z uvedených tabulek získat jsou celkové finanční částky očekávaných ročních nákladů a úspor, které vznikly se zavedením bezpečnostních opatření.

Tabulka č.3a ukazuje rozdělení rizik spojených s ohrožením objemem vykázané zdravotní péče pro zdravotní pojišťovny. Měsíční objem zdravotních dávek pro pojišťovny je zhruba 20 miliónů korun. Na serveru, na kterém se provádí toto vykazování, jsou k dispozici vždy údaje pro aktuální kalendářní měsíc a záloha dat za předešlé tři měsíce. V případě napadení tohoto serveru může tedy útočník zničit či modifikovat data v celkové hodnotě až 80 miliónů korun. Zdravotní pojišťovny zasílají kontrolu vykázané zdravotní péče nejpozději do tří měsíců po obdržení uzavřených a odeslaných dávek z ÚHKT.

Vezmu-li v úvahu tuto skutečnost, tak za zpracování nesprávných dat bude ztráta ÚHKT činit zhruba 40 miliónů korun (je nepravděpodobné, že se útočníkovi podaří modifikovat všechna data na serveru). V případě odhalení dalších citlivých dat (mzdové účetnictví, osobní údaje zaměstnanců, údaje o pacientech,...) vznikne ÚHKT ztráta přibližně 10 miliónů korun. Tabulka č.3b ukazuje možná bezpečnostní opatření a očekávané úspory plynoucí z těchto opatření.

Riziko	Cena prostředků [tis. Kč]	Pravděpodobnost výskytu rizika / rok [%]	Cena rizika [tis. Kč]
• odhalení citlivých dat ústavu	10 000	10	1 000
• počítačové zpracování nesprávných dat	40 000	10	4 000
			celkem: 5 000

Tab. č.3a Vyčíslení ztrát

Bezpečnostní opatření	Cena opatření [tis. Kč]	Účinnost opatření [%]	Očekávané úspory [tis. Kč]
• Software pro zabezpečení přístupu	20	60	***celkem: 3 000***

Tab. č.3b Vyčíslení úspor

Tabulka č.4a popisuje rizika spojená s neautorizovaným přístupem k datům a programům. S těmito riziky souvisí i další ohrožení - neautorizované využívání výpočetní techniky. Uživatelé si na interní servery v počítačové síti ÚHKT ukládají osobní data, která z nějakého důvodu nemohou mít uloženy na svém lokálním počítači (např. nedostatek vlastních diskových prostorů, větší bezpečnost a možnost centrálního zálohování dat na serveru, atd.).

V případě útoku na vnitřní síť může útočník tyto data znehodnotit nebo odcizit. V jiném případě může útočník využívat diskové prostory a výkon počítače určený lokálním uživatelům pro své vlastní účely. Stejně tak bude omezovat lokální uživatele v činnosti, která vyžaduje přístup pevnou linkou do Internetu. Útočník má možnost se například do interní sítě připojit přes svého lokálního provozovatele pomocí modemu. Po průniku do sítě ÚHKT se přihlásí na unixový server (pomocí odposlechnutého uživatelského jména a hesla), spustí složitý a časově náročný výpočet a pak ukončí interaktivní sezení. Po určité době se vrátí pro výsledky své činnosti. Tím zneužije výpočetní prostředky určené lokálním uživatelům sítě ÚHKT. Tabulka č.4b ukazuje možné bezpečnostní opatření chránící síť ÚHKT před těmito riziky.

Riziko	**Cena prostředků [tis. Kč]**	**Pravděpodobnost výskytu rizika / rok [%]**	**Cena rizika [tis. Kč]**
• neautorizovaný přístup k datům a programům	3 000	10	300
• neautorizované využívání výpočetních prostředků	500	40	200
			celkem: 500

Tab. č.4a Vyčíslení ztrát

Bezpečnostní opatření	**Cena opatření [tis. Kč]**	**Účinnost opatření [%]**	**Očekávané úspory [tis. Kč]**
• síťové kontroly:			
▪ hardware (s 5-ti letou autorizací)	20 (z toho za rok 4)		
▪ software (s 5-ti letou autorizací)	2 (z toho za rok 0.4)		
	celkem: 4.4	95	***celkem: 475***

Tab. č.4b Vyčíslení úspor

Uvedené celkové výsledky v tabulce č.5 ukazují, že riziková analýza může sloužit k vyčíslení skutečných nákladů na zavedení navrhovaných bezpečnostních opatření a že může být chápána jako neocenitelný nástroj plánování. Tato analýza může kvantitativně hodnotit efektivnost různých kontrol a při opakovaném použití přispívá k výběru optimálního souboru bezpečnostních opatření.

Očekávané celkové roční	**Výpočet [tis. Kč]**
Ztráty:	1. (z tab. č.3): 5 000.0 - 3 000.0 + 20.0 = 2 020.0 2. (z tab. č.4): 500.0 - 475.0 + 4.4 = 29.4 ***Celkem: 2 049.4***
Úspory:	1. (z tab. č.3): 5 000.0 - 2 020.0 = 2 980.0 2. (z tab. č.4): 500.0 - 29.4 = 470.6 ***Celkem: 3 450.4***

Tab. č.5 Celkové roční ztráty a úspory

Z tabulky č.5 jednoznačně vyplývá, že i v první aproximaci je výnos ze zavedení bezpečnostních opatření relativně velmi vysoký (cca 1,5 mil. Kč), což svědčí o velké potřebnosti nasazení firewallu pro ochranu sítě.

2.4 Realizace bezpečnostních opatření

Při zavádění bezpečnostních opatření je nutno ujasnit si, co budou bezpečnostní opatření chránit. Při připojení interní sítě ÚHKT k Internetu jsou potenciálnímu nebezpečí vystavena:

- ústavní důvěrná a citlivá data, uložená na serverech vnitřní sítě
- výpočetní zdroje (počítače, strojový čas, diskové prostory,atd.)
- v neposlední řadě též pověst ústavu

V kapitole 1.1 o ochraně počítačových sítí jsem uvedl, že u dat uložených v počítačích zapojených do sítě je nutno zajistit diskrétnost, integritu a dostupnost. Tyto tři vlastnosti je třeba zachovávat jako celek. Nelze se zaměřit pouze na jednu vlastnost a ostatní opomíjet, neboť všechny tři vlastnosti jsou mezi sebou úzce propojeny.

Pokud vetřelci nejde o data, tak ve většině případů mu jde o bezplatné využívání výpočetních zdrojů. V tomto případě se nejčastěji jedná o ty, kteří sami nedisponují dostatečným výpočetním výkonem nebo diskovou kapacitou a tak využívají zdrojů, které jim poskytne napadená síť. Pokud útočníkovi nejde o přímé využívání výpočetních zdrojů, tak zcela jistě se pokusí napadenou síť použít k dalším výbojům v Internetu.

Nebezpečí popsané v předešlém odstavci souvisí i s posledním druhem zneužití napadené sítě. Vetřelec se může na Internetu prezentovat s identitou napadené sítě. To může vést až k finančním postihům nebo trestním oznámením na ÚHKT.

2.5 Typy útočníků

V současné době vznikají nové studie (viz. [2], [4] a [5]), které studují vlastnosti lidí páchající počítačovou trestnou činnost. Tyto studie mají napomoci při typování potenciálních pachatelů a preventivně potlačovat kriminalitu. V následujícím výčtu uvedu pouze některé typy lidí páchající počítačovou trestnou činnost:

- ***amatéři*** - lidé využívající náhodně objevenou bezpečnostní slabinu informačního systému. Využívají napadené počítače pro osobní zájmy
- ***hakeři, krakeři a studenti*** - obvykle středoškolští nebo vysokoškolští studenti, kteří se snaží získat přístup k zabezpečeným výpočetním prostředkům

- ***joyriders*** - nudící se lidé, kteří hledají zábavu. Většinou napadají informační systémy ze zvědavosti
- ***vandalové*** - lidé, které baví ničit věci, nebo lidé, kteří nemají v lásce vlastníky napadeného systému (typicky propuštěný zaměstnanec)
- ***score keepers*** - lidé napadající systém z důvodu zvýšení si vlastního sebevědomí. Snaží se napadat známé nebo výjimečné, dobře zajištěné systémy
- ***profesionálové*** - lidé, kteří jdou systematicky za svým cílem. Nejčastěji do této kategorie spadají tzv. průmysloví špioni

2.6 Typy útoků

Stejně, jako existuje mnoho typů útočníků, existuje i velké množství typů útoků. Útočník může napadnout hardware (týká se obvykle vlastního výpočetního centra - krádež, ničení počítačů střelbou, nebo ostrými předměty, ničení počítačových sálů výbušninami, ohněm, atd.), software (úmyslná modifikace, mazání, chybná instalace, krádež,...) a zejména data (zcizení, zničení a modifikace).

Mezi nejčastější druhy útoků patří:

- ***vniknutí*** - vetřelec využívá systém jako legitimní uživatel
- ***znemožnění služby*** - jeden z možných způsobů zaměřený na zabránění v běžném využívání počítače
- ***krádež informace*** - získání důvěrných dat bez přímého použití chráněného počítače (nejčastěji odposlechem síťové komunikace)

2.7 Implementace bezpečnostních opatření

Hlavním cílem, který jsem si vytyčil, je zabezpečení připojení vnitřní sítě ÚHKT do Internetu. Realizace tohoto zabezpečení spočívá ve vybudování a zprovoznění firewallu. Firewall je nejefektivnějším typem síťové bezpečnosti.

Na tomto místě ještě jednou shrnu nejpodstatnější rysy a účely firewallu. Firewall slouží k zabránění rozšiřování nebezpečí z Internetu do interní sítě. Je vystavěn tak, aby co nejlépe plnil následující účely:

- důkladně kontroluje vstupující uživatele při vstupu do Intranetu
- zabraňuje útočníkům v bližším kontaktu s dalšími (interními) ochranami
- kontroluje odchozí uživatele při vstupu do Internetu

Instalace firewallu se provádí v místě připojení interní sítě do Internetu. Všechen provoz přicházející z Internetu, nebo jdoucí ven z Intranetu prochází přes firewall. Firewall sleduje provoz mezi interní a externí sítí a na základě bezpečnostní politiky aplikuje omezující pravidla. To znamená, že firewall funguje jako oddělovač, omezovač a analyzátor.

Firewall má též určité nevýhody. Jeho vytvoření vyžaduje značné výdaje, námahu a omezení, která jsou kladena na vnitřní stranu sítě. Je nutné si na začátku výstavby firewallu uvědomit, co může a nemůže firewall zajistit.

Firewall je hlavním místem pro aplikaci bezpečnostních rozhodnutí. Všechen provoz dovnitř a ven musí projít tímto jedním úzkým kontrolním místem. Firewall je také jedním z nejdůležitějších prvků, které si vynucují určitou bezpečnostní taktiku. Většina veřejných Internetových služeb je z hlediska síťové bezpečnosti nebezpečných. To znamená, že firewall povoluje používat pouze relativně bezpečné služby. Služby, které s sebou nesou potenciální rizika je nutné vyřadit bez ohledu na to, jaký systém je zkouší spustit, nebo který uživatel je vyžaduje. Další možností, jak využít firewall, je zaznamenávání provozu mezi Intranetem a Internetem. Vzhledem k tomu, že veškerý provoz prochází skrze firewall, poskytuje dobré místo pro kumulaci informací o používání systému a sítě.

Firewall taktéž omezuje vystavované služby do Internetu. Ve většině případů je žádoucí, aby uživatelům Internetu byly poskytovány pouze vybrané, přesně specifikované služby. Pro tyto služby jsou zřízeny speciální služby v takzvané ***demilitarizované zóně*** (*DMZ*). DMZ je chráněná oblast oddělená od veřejné i interní sítě, která slouží k umísťování veřejně přístupných serverů, proxy serverů a podobně. Lepší představu o funkci firewallu a DMZ můžeme získat z obrázku č.1 uvedeného v příloze 6.1.

Jsou ale i problémy, které firewall nemůže ošetřit. To je zapříčiněno tím, že firewall není kompletním bezpečnostním řešením. Nemůže uchránit před vetřelci, kteří jsou již uvnitř. Firewall je také zcela bezbranný proti zlomyslným interním uživatelům. To znamená, že zcela jistě nemůže zabránit například ve vědomém poslání důvěrných dat elektronickou poštou mimo společnost lokálním uživatelem. Firewall je taktéž zcela bezmocný vůči spojením s vnějším světem, která přes něj neprochází. Typickým příkladem je modemový přístup na počítač umístěný ve vnitřní síti.

Firewall je též bezbranný vůči zcela novým hrozbám. To vyplývá z toho, že firewall je vystaven tak, aby čelil známým hrozbám. V poslední řadě firewall není schopen odolávat napadení vnitřní sítě způsobenými počítačovými viry. Nicméně, tento problém se dá v některých případech částečně obejít (viz. [12], [13] a [20]). Je to ale spíše otázka kombinace různých typů bezpečnostních opatření, než otázka samotného firewallu. Firewall nejlépe pracuje, jestliže je zkombinován s další interní ochranou.

3 Realizace firewallu

3.1 Návrh firewallu

Při návrhu konkrétního firewallu pro zabezpečení interní sítě ÚHKT jsem mohl vybírat ze dvou základních implementačních variant:

- ***Paketový filtr*** - jedná se v podstatě o klasický router, který na základě určitých, předem jasně definovaných tabulek pravidel rozhoduje, zda příchozí nebo odchozí paket propustí či nikoliv. Paketový filtr může současně fungovat jako prostředek pro záznam informací o přenesených datech, tzn. poskytuje službu pro účtování dat. Paketový filtr provádí kontrolu na úrovni síťové vrstvy.

- ***Proxy systém*** - ten na rozdíl od předcházející varianty pakety zásadně nesměruje. Místo toho nabízí zprostředkování vybraných služeb. Spojení z externí i interní sítě je směrováno výhradně na proxy server a z něho teprve dovnitř nebo ven. Proxy systém provádí kontrolu na úrovni aplikační vrstvy.

Systém používající filtrování paketů má patrně největší výhodu v tom, že jeden dobře umístěný router pro filtrování paketů může zabezpečit celou síť.

Síť ÚHKT je do Internetu připojena přes jeden směrovač a tím vlastně vzniká nejlepší místo pro instalaci firewallu tohoto typu. Další výhodou firewallu implementovaného na bázi filtrování paketů je, že nevyžaduje žádný další uživatelský software nebo dodatečnou konfiguraci na koncových stanicích. Tato vlastnost je velkou výhodou, neboť si koncový uživatelé ani neuvědomí instalaci nového bezpečnostního opatření, které je téměř neovlivňuje v jejich každodenní práci. Pro administrátora rozsáhlé sítě je to velká výhoda, protože celou instalaci firewallu může provést i bez vědomí uživatelů. Stejný přínos vzniká i pro uživatele - nemusí se učit cokoliv nového.

Tento systém však sebou bohužel přináší i určité nevýhody. Hlavní nevýhodou při implementaci paketového filtru je velká obtížnost vytváření filtrovacích pravidel. Když se podaří překlenout tento úvodní problém a pravidla jsou sestavena, je těžké je otestovat a přesně prověřit, zda neobsahují nějakou bezpečnostní díru. Možnosti filtrace paketů (konkrétně na systému GNU/Linux s jádrem řady 2.0.x nebo 2.2.x při použití nástroje ***ipfwadm***, viz. kapitola 3.2) jsou neúplné, což činilo nastavení firewallu obtížným.

Chyba, kterou zaviní administrátor špatným nastavením paketového filtru je zpravidla fatální a znamená velké ohrožení interní sítě.

Firewally založené na proxy systémech mají řadu předností. Jmenujme například výhody při zvláště efektivním zaznamenávání. Na rozdíl od paketového filtru, kdy je zaznamenáváno pouze množství přenesených dat, zaznamenává proxy systém pouze příkazy a obdržené odpovědi. Výsledkem je pak mnohem menší a užitečnější logovací soubor. Další výhodou je odolnost vůči špatné konfiguraci. Pokud administrátor provede špatné nastavení proxy serveru, většinou to znamená pouze nefunkčnost špatně nastavené služby.

Proxy systémy také ale oplývají mnoha nectnostmi. Pro služby provozované přes proxy server velmi vzrůstá prodleva odezvy. Ve většině případů je zpomalení komunikace přes proxy server větší, než při použití paketového filtru. Další nevýhodou je to, že pro téměř každou službu je potřeba jiná zástupná aplikace. Pro některé nové síťové služby chybí zcela.

Nedostupnost důležitých zástupných aplikací mě v konečném výběru architektury firewallu vedla k tomu, že jsem zvolil variantu paketového filtru. Hlavním důvodem tohoto rozhodnutí je skutečnost, že proxy servery neumí zpracovat některé konkrétní služby využívané v ÚHKT. Patrně nejvíce používanou službou v interní síti ÚHKT, pro kterou neexistuje zástupná aplikace, je aplikace *MedLine* firmy SilverLine. Jedná se o aplikaci klient - server. V budoucnosti se uvažuje o možnosti zpřístupnění této aplikace jiným zdravotnickým zařízením, nebo uživatelům ÚHKT používajícím modemový přístup z domácího počítače. Další problematickou aplikací je *RealPage*. Tato aplikace slouží pro on-line prohlížení literatury na Internetu.

Spojuje v sobě vlastnosti webového prohlížeče a textového editoru (umožňuje snadnou manipulaci s textem, změnu fontů, tisk, atd.). Pro tuto aplikaci již byla zkonvertována velká řada odborné lékařské literatury. V některých případech představuje tato aplikace pro uživatele jedinou cestu k dosažení těžko dostupné odborné zahraniční literatury.

Nicméně jsou zde i další nevýhody, které jsou velkou překážkou použití. Proxy servery vyžadují úpravy klientů. Tyto úpravy vedou k tomu, že uživatelé nemohou vždy snadno používat nástroje, se kterými umí zacházet. Použití proxy serveru klade na administrátora rozsáhlé úkoly. Administrátor je nucen instalovat a konfigurovat velkou řadu nových klientů. V heterogenní síti s velkým počtem operačních systémů a typů počítačů (mezi které patří i počítačová síť ÚHKT) je to nerealizovatelný problém.

3.2 Implementace paketového filtru

Při budování firewallu je prvním krokem výběr počítače a operačního systému. Jako nosnou architekturu jsem zvolil GNU/Linux na platformě Intel. GNU/Linux poskytuje velkou flexibilitu co do výběru hardwarových komponent, poskytuje spolehlivé síťové služby, multiuživatelské a multiprocesové prostředí. Je pro něj k dispozici mnoho nástrojů pro správu a zabezpečení sítě. Další výhodou pro mne byla znalost tohoto systému. Používám ho několik let a proto vím o kolik je stabilnější a robustnější než například MS Windows NT, které jsem měl nějaký čas možnost instalovat a spravovat. Zájemce o problematiku zabývající se porovnáním vlastností operačních systémů UNIX a MS Windows NT odkazuji na velmi zajímavý článek [16]. Pokud bych měl k dispozici větší finanční zdroje, patrně bych zvolil některé z dostupných komerčních řešení - například *FireWall-1* firmy *Check Point* [20] v kombinaci s některým se serverů firmy Sun Microsystems s operačním systémem *Trusted Solaris* [13]. Pro hardwarovou realizaci jsem vybral osobní počítač typu PC, vybavený dvěma síťovými rozhraními. Bližší popis hardwarové a softwarové konfigurace je uveden v příloze 6.2.1 a 6.2.2.

Počítač sloužící jako firewall by neměl být výkonným počítačem. Je lepší, když má menší výpočetní výkon, protože služby které poskytuje, nejsou výpočetně náročné. Při výběru dílů jsem spoléhal na osvědčené druhy hardwarových komponent, ověřené delším používáním v počítačích zapojených do sítě ÚHKT. Nevolil jsem žádné neotestované díly od neznámých firem. Dalším faktorem při výběru dílů byla finanční částka vyčleněná na realizaci firewallu, neboť ÚHKT je státním zdravotnickým zařízením s limitovaným finančním rozpočtem.

Mezi distribucemi operačního systému GNU/Linux jsem zvolil komerční distribuci ***Caldera OpenLinux 1.1*** [31]. Výhodou této distribuce je, že výrobce poskytuje záruku do výše ceny produktu a bezplatnou měsíční technickou a konzultační podporu. Další výhodou této distribuce je (podle informací mých konzultantů) to, že je certifikována podle norem ***POSIX 1*** (FIPS 152-2), ***Single UNIX Specification APIs*** a certifikátu ***X-Open***, což ji řadí do skupiny certifikovaných operačních systémů typu UNIX. Nevýhodu této distribuce shledávám v tom, že stále nepoužívá GNU C knihovny glibc, která nabízí vyšší výkon, podporu pro lokalizaci a thready. Tato vlastnost stěžuje například aktualizaci jádra operačního systému. Jeho kompilace a sestavení musí probíhat na firewallu. Na druhou stranu je knihovna glibc relativně nová a není zcela bez chyb.

Dalším mým krokem bylo umístění firewallu v rámci sítě. Zde byla volba velmi jednoduchá. Síť ÚHKT je do Internetu napojena pouze v jednom místě pevnou linkou o přenosové kapacitě 64kb/s. Nicméně, do interní sítě je umožněn přístup i na dalších místech:

- Pomocí modemového připojení. Počítač poskytující toto připojení však nepoužívá protokol TCP/IP. Počítač je obsluhován speciálním programem v operačním systému DOS (konkrétně *Caldera DR-DOS 7.1*) a jeho připojení do sítě je realizováno pomocí protokolu společnosti Novell IPX/SPX. Komunikace přes tento kanál je šifrována a je použita spolehlivá autentifikace. Toto spojení je výhradně určeno ke sběru medicínských dat z vnějších zdravotnických zařízení. Všechny vnější, řádně registrované pobočky jsou zaneseny v interní databázi. Pokud příchozí volání nesouhlasí se záznamem v databázi, je okamžitě ukončeno.

- Dalším vstupem do interní sítě je propojení s III. interní klinikou Všeobecné fakultní nemocnice na Karlově náměstí. Toto spojení opět slouží ke sběru medicínských dat. Je realizováno pomocí jednoduchého serveru disponujícího dvěma síťovými rozhraními. Tento server je obsluhován operačním systémem GNU/Linux (konkrétně se jedná o distribuce Debian GNU/Linux). Počítač je nakonfigurován tak, aby nesměroval pakety z interní sítě ven a naopak. Komunikace se sítí III. interní kliniky je realizována opět pomocí protokolu IPX/SPX. Propojovací počítač se přihlásí na Novell server III. interní kliniky, vyzvedne si data a ta předá na disk lokálního Novell serveru. Veškerý další síťový přenos je blokován.

- V nejbližší době se bude realizovat další modemové připojení, které bude sloužit lokálním uživatelům pro čtení pošty z domova. Jeho zřízení si vyžádá dodatečné zabezpečení.

Po upřesnění přístupových míst byl v další fázi realizace firewallu proveden výběr služeb, jejichž provoz bude přes firewall povolen. Jejich výčet je uveden v tabulce č. 6 i s odpovídajícími čísly portů protokolu TCP/IP.

Povolení nebo zakázání příchozích nebo odchozích spojení pro jednotlivé služby je možno vysledovat ze souboru ***rules.list*** v adresáři */firewall/rules* na přiložené disketě. Tento soubor obsahuje aktuální nastavení pravidel pro filtrování paketů. Jeho obsah se pravidelně aktualizuje, a proto jsem ho do zprávy nepřikládal v tištěné podobě. Soubor je opatřen velkým množstvím komentářů a je snadno přehledný.

Mezi další služby, které nejsou uvedeny v tabulce č.6 a jsou používány v síti ÚHKT, jsou služby postavené na protokolu ICMP (např. aplikace ping, traceroute a další nástroje pro kontrolu sítě). Tyto služby jsou určeny spíše správcům sítě než řadovým uživatelům. Další tabulka (tab. č. 7) obsahuje přehled vybraných ICMP zpráv. Průchod zpráv uvedených v tabulce by měl být přes firewall povolen.

Služba	Číslo portu / protokol	Komentář
FTP (data)	20 / TCP	datový kanál protokolu pro přenos souborů
FTP	21 / TCP	příkazový kanál protokolu pro přenos souborů
SSH	22 / TCP	terminálová aplikace se šifrovaným přenosem
TELNET	23 / TCP	služba vzdáleného terminálu
SMTP	25 / TCP	protokol pro přenos elektronické pošty
WHOIS	43 / TCP	informační služba
DNS	53 / TCP, UDP	jmenná služba
GOPHER	70 / TCP	textová informační služba
FINGER	79 / TCP	služba poskytující informace o uživatelích
HTTP	80 / TCP	webové služba
POP3	110 / TCP	jednoduchý protokol pro přenos elektronické pošty
AUTH	113 / TCP	autentifikace uživatele
NNTP	119 / TCP	elektronické konference
NTP	123 / UDP	protokol pro synchronizaci času
SNMP	161 / UDP	protokol pro správu sítě
SNMP (trap)	162 / UDP	protokol pro sledování sítě - události
IMAP4	585 / TCP, UDP	rozšířený protokol pro přístup k elektronické poště
RLOGIN	513 / TCP	vzdálený přístup na počítač
PROXY HTTP	3128 / TCP	zástupná aplikace pro www
PROXY ICP	3130 / UDP	zástupná aplikace pro www (výměna informací mezi proxy servery)
X11	6000 + n / TCP	X-Window protokol

Tab. č.6 Přehled používaných služeb protokolu TCP/IP v ÚHKT

Typ zprávy	Komentář
0	*echo replay* (odezva na ping)
3	*destination unreachable* (použito pro traceroute) - hostitel, síť či port není dostupný
4	*source quench* - pokyn pro zpomalení komunikace
5	*redirect* - změna trasy spojení
8	*echo request* - (žádost o ping)
11	*time exceeded* - oznámení o možném zacyklení paketu
12	*parametr problem* - problém s hlavičkou paketu

Tab. č.7 vybrané zprávy protokolu ICMP

Dá se zcela logicky očekávat, že v budoucnu zcela jistě přibudou další služby, které nejsou dnes tak intenzivně používány a proto jsem je nezahrnul do tabulky. Jejich používání je tak z důvodu síťové bezpečnosti zakázáno (viz. kapitola 2.1).

Po výběru služeb a vyhledání patřičných portů a protokolů se kterými se dané služby pojí jsem provedl opatření v souvislosti se zvýšením bezpečnosti v samotném operačním systému. Zrušil jsem všechny uživatelské účty a ponechal jsem funkční pouze dva - účet administrátora systému *root* a uživatele dohlížejícího na bezpečnost s právem modifikovat určitá nastavení na firewallu s účtem *security*. Na samotný firewall je možné se přihlásit pouze na konzoli.

Po této redukci uživatelských účtů jsem podrobil stejnému postupu i další části systému. Při instalaci systému jsem použil volbu, která zajišťovala nainstalování minimálního počtu nejnutnějších softwarových balíků (systém se instaluje pomocí nástroje *rpm*). Po dokončení této instalace jsem ještě provedl manuální kontrolu a odinstaloval nepotřebný software. Ponechal jsem pouze nezbytně potřebné součásti operačního systému.

Po té jsem provedl aktualizaci jádra Linux na verzi 2.0.35. Jedná se o jádro ze stabilní řady. Dále jsem nainstaloval všechny doporučené opravy operačního systému.

Opravy jsem plánoval podle doporučení firmy Caldera [31] a použil jsem i alternativní informační zdroje na Internetu [17], [18], [22] a [23]. Následujícím krokem byla konfigurace systémových logovacích démonů.

Firma Caldera je známa svou pečlivostí při nastavování konfigurace systému a proto jsem pouze doladil připravené konfigurační soubory. Pro údržbu logovacích souborů nepoužívám žádné speciální nástroje. Jejich záloha probíhá manuálně na přenosná média podle potřeby (nejméně však dvakrát týdně).

V následujícím kroku jsem provedl redukci síťových a systémových služeb používaných na firewallu. Tento krok obnášel přehodnocení démonů a služeb, které jsou nezbytné pro chod firewallu. Přetřídil jsem startovací skripty systému a zrušil jsem všechny síťové služby spouštěné přes démona inetd z důvodu minimalizace možností přístupu na firewall. Z tohoto důvodu na firewallu neběží žádní síťový démoni (telnet démon, ssh démon). Na firewall se lze přihlásit pouze z lokální konzole (heslo administrátora nikdy nebude posíláno přes síť a tím se zamezí jeho odposlechu). Počítač sloužící jako firewall je určen výlučně k ochraně, proto na něm nesmí běžet žádné jiné aplikace. V příloze 6.2.4 je uveden výpis běžících procesů na firewallu získaných pomocí příkazu *ps*. Samozřejmostí je použití balíku TCP Wrapper (tcpd) pro sledování provozu a kontrolu síťových aktivit.

V posledním kroku konfigurace systému jsem se rozhodl připojit souborové systémy v režimu pouze pro čtení. Zapisovat lze pouze do svazků pro ukládání logovacích souborů */var*, */tmp*, domácích adresářů a odkládacího prostoru na pevném disku.

Nejdůležitější část podpory pro paketový filtr je v jádře operačního systému GNU/Linux, kde se řeší směrování. Při překladu jádra je potřeba v sekci ***Networking options*** zapnout volby *IP forwarding* a zároveň *IP firewalling*, popřípadě *IP accounting*. Kromě toho je potřeba mít v systému nainstalované rozhraní, kterým je možné příslušné datové struktury v jádře prohlížet a manipulovat s nimi. Pro řízení paketového filtru slouží v GNU/Linuxu nástroje ***ipfw***, ***ipfwadm*** nebo ***ipchains***.

Všechny nástroje pracují přibližně stejně, avšak *ipchains* na rozdíl od prvních dvou nástrojů vyžaduje úpravu jádra operačního systému. Tato úprava (patch) není součástí distribuce zdrojových kódů stabilní řady linuxového jádra 2.0.x. Z tohoto důvodu jsem tento nástroj nepoužil, i když jeho možnosti tvorby filtrovacích pravidel silně překračují možnosti zbylých dvou nástrojů. Konfigurace paketového filtru pomocí *ipchains* je jednodušší a přehlednější, ale nutnost nestandardních úprav jádra může ohrozit bezpečnost celého systému.

Nástroj *ipfwadm* poskytuje širší možnosti než *ipfw*. Z tohoto důvodu jsem si ho také vybral pro realizaci paketového filtru. V následujících několika řádcích shrnu základní vlastnosti nástroje *ipfwadm*, který jsem použil pro realizaci firewallu.

Nástroj *ipfwadm* je charakterizován následujícími body:

- provádí filtrování podle služby
- neudržuje tabulku otevřených spojení
- rozpoznává ACK bit v TCP paketech
- neumožňuje účinné filtrování UDP paketů
- efektivně filtruje ICMP pakety
- umožňuje jednoduchou specifikaci pravidel
- pravidla aplikuje v uvedeném pořadí
- umožňuje aplikovat pravidla odděleně na příchozí a odchozí pakety
- rozeznává síťová rozhraní
- umožňuje zaznamenávání přijatých paketů
- neumožňuje dostatečnou kontrolu a prověření nastavených pravidel

3.3 Grafické nadstavby pro konfiguraci paketového filtru

Pro vytváření pravidel existují pro *ipfwadm* různé grafické nadstavby. Mezi nejznámější patrně patří modul se stejným názvem (tedy *ipfwadm*) pro aplikaci ***dotfile***. Její rozhraní je znázorněno na obrázku č.2 a č.3 v příloze 6.1. Aplikace *dotfile* je naprogramována pro rozhraní X-Window. Její ovládání je snadné, nicméně nedovoluje nastavování složitějších pravidel. Další nevýhodou této aplikace je, že ji lze spustit pouze v prostředí X-Window. X-Window je samo o sobě nebezpečné, protože obsahuje velmi mnoho neřešených bezpečnostních problémů. Proto není možné používat tento nástroj přímo na firewallu. Je nutno ho instalovat na jiném počítači s prostředím X-Window a s operačním systémem GNU/Linux. Zde se potom provede konfigurace a nastavení. V následujícím kroku se vygenerují příslušná filtrovací pravidla. Tato pravidla se přenesou na firewall, kde se provede jejich instalace do systému.

Dalším grafickým nástrojem pro konfiguraci nástroje *ipfwadm* je aplikace ***fwconfig***. Jedná se o sadu webových stránek a CGI skriptů. Celá konfigurace je řízena pomocí vyplňování formulářů. Aplikace *fwconfig* opět běží pod X-Window. Pro její používání je navíc potřeba grafický webový prohlížeč. Aby se dala tato aplikace využívat, je nutná instalace systém X-Window na samotný firewall, což si vyžádá nejen velkou část diskové kapacity a výkonu procesoru, ale přinese to sebou i bezpečnostní rizika. Druhou možností je instalace pouze aplikace *fwconfig*, webového prohlížeče a sdílených knihoven, které používají.

V tomto případě je ale nutno aplikaci zobrazovat po síti na vzdálený X-server, což opět přináší řadu bezpečnostních problémů (například odposlech), neboť jak jsem již zdůraznil, X-Window nemají dořešeny některé základní bezpečnostní principy.

Z těchto důvodů jsem si naprogramoval vlastní aplikaci, kterou jsem pojmenoval ***firewall***. Jedná se o sadu skriptů v příkazovém interpretu (konkrétně *tcsh*). Tato aplikace je pro zvýšení přehlednosti rozdělena do modulů. Každý modul ošetřuje a nastavuje určitou skupinu problémů (např. síť, pravidla, atd.). Popis celé aplikace, včetně funkce jednotlivých modulů je uveden v příloze 6.3.

Na tomto místě se ještě zmíním o tom, že moje aplikace umožňuje na rozdíl od aplikací *dotfile* a *fwconfig* jednoduché logování událostí během chodu aplikace a instalace pravidel. To zjednodušuje ladění nadefinovaných pravidel a jejich testování.

Výpis celého kódu aplikace neuvádím, protože je příliš obsáhlý. Pro realizaci aplikace jsem zvolil příkazový interpretr tcsh, protože je relativně bezpečný a jeho provoz na firewallu si nevyžádá dodatečné nastavení ani instalaci dalších knihoven. Kdybych použil například jazyk Perl (jehož instalace by musela být z tohoto důvodu provedena na firewallu), poskytl bych tak potenciálnímu útočníkovi, který by pronikl až na samotný firewall, mocný nástroj pro jeho další činnost.

3.4 Realizace paketového filtru

Pro další popis paketového filtru je potřeba si uvědomit, jak zachází GNU/Linux s datagramy. Odtud pak snadno odvodíme činnost jednotlivých součástí paketového filtru. GNU/Linux s příchozím datagramem provádí následující akce:

- datagram se zaúčtuje pro vstupní rozhraní
- datagram se podrobí vstupním pravidlům pro vstupní rozhraní
- datagram se podrobí výstupním pravidlům pro vstupní rozhraní
- datagram se podrobí vstupním pravidlům pro výstupní rozhraní
- datagram se podrobí výstupním pravidlům pro výstupní rozhraní
- datagram se zaúčtuje pro výstupní rozhraní

Nástroj *ipfwadm* umožňuje filtrování TCP, UDP a ICMP paketů. Na rozdíl například od systému *FireWall-1* [20] neudržuje *ipfwadm* informace o navázaných spojeních. U některých paketových filtrů nové konstrukce je k dispozici tabulka otevřených spojení.

To znamená, že filtrovací systém má neustále k dispozici informace o všech právě realizovaných spojeních. Nástroj *ipfwadm* tento nedostatek částečně kompenzuje možností testování ACK bitu v TCP paketech.

TCP (*Transmission Control Protocol*) protokol je označován jako spolehlivý. To znamená že zaručuje doručení paketů v tom pořadí, v jakém byly odeslány, dále, že místo určení obdrží veškerá aplikační data a že se žádná data nebudou opakovat dvakrát. Protokol TCP je obousměrný, to znamená, že jakmile je spojení jednou navázáno, může server klientovi odpovídat na základě téhož spojení. Není nutné zřizovat jedno spojení od klienta k serveru pro dotazy nebo příkazy a druhé spojení od severu zpět ke klientovi pro odpovědi.

Chceme-li zablokovat TCP spojení, stačí prostě pozastavit první paket navazující spojení. Bez prvního paketu (který nese informace o spojení, které se má navázat) nemohou být pozdější data příjemcem sestavena do datového proudu a spojení se nikdy neuskuteční.

Tento první paket se pozná podle toho, že je v jeho TCP záhlaví nastaven ACK bit na nulu. Každý další paket v daném spojení, bez ohledu na směr, má ACK bit nastaven na jedničku. Rozpoznání zahajovacích TCP paketů umožňuje uplatnit politiku, která dovoluje interním uživatelům připojení k externím serverům, ale brání externím narušitelům v připojení na interní počítače. Toho lze dosáhnout tak, že se povolí jen zahajovací TCP pakety směřující směrem ven. Zahajovací pakety tak budou propuštěny pouze z interních počítačů na externí servery, nikoliv však z externích počítačů na počítače zapojené v interní síti. Útočník nemůže tento přístup zfalšovat tím, že by nastavil ACK bit ve svých zahajovacích paketech, protože absence ACK bitu je tím, co identifikuje tyto pakety jako zahajovací. Nástroj *ipfwadm* je schopen rozpoznat nastavení ACK bitu a tím umožňuje poměrně efektivně filtrovat TCP pakety.

Dalším druhem paketů, který může *ipfwadm* filtrovat, jsou UDP (*User Datagram Protocol*) pakety. Na rozdíl od TCP paketů neposkytuje žádnou spolehlivou záruku doručení, pořadí a zamezení duplicity. Každý UDP paket je nezávislý, to znamená, že UDP pakety nejsou součástí žádného virtuálního kanálu jako TCP pakety. UDP pakety se svou strukturou velmi podobají TCP paketům.Na

rozdíl od TCP paketů ale neexistuje v záhlaví UDP paketu ACK bit. ACK bit je součástí TCP mechanismu zajišťujícího spolehlivé doručení dat. Jelikož UDP žádné takové záruky neposkytuje, nepotřebuje ACK bit. Z toho vyplývá, že paketový filtr není schopen žádným způsobem zjistit, zda se jedná o první paket od externího počítače k počítači zapojenému v interní síti, nebo o odpověď od externího počítače směřující do interní sítě.

Na rozdíl od *ipfwadm* uchovává systém *FireWall-1* [13], [20] tabulku otevřených spojení. Do této tabulky se ukládá informace o všech odcházejících UDP paketech. Následně tak může filtrovací mechanismus propustit jen pakety nesoucí pouze odpovídající odpovědi. Aby byl paket považován za odpověď, musí pocházet z počítače a portu, na který byl odcházející paket odeslán, a musí být směrován na interní počítač a port, který původní UDP paket s žádostí odeslal. Tato schopnost je často označována termínem ***dynamické filtrování paketů***. *FireWall-1* podstatně upravuje pravidla pro filtrování za chodu, aby je přizpůsobil vracejícím se paketům. Pravidla vytvořená za účelem propuštění odpovědí jsou časově limitována, po několika sekundách či minutách vyprší.

Dynamické filtrování paketů je výhodné použít i v situaci, kdy se pravidla pro filtrování paketů mění, aniž by někdo explicitně změnil konfiguraci. Nástroj *ipfwadm* bohužel dynamické filtrování nepodporuje a tím je podstatně omezen.

Posledním typem paketů, které může nástroj *ipfwadm* filtrovat jsou ICMP (*Internet Control Message Protocol*) pakety. Tento protokol je součástí síťové vrstvy a využívá schopnosti doručení IP datagramů k předávání vlastních zpráv. ICMP posílá zprávy, zajišťující řízení přenosu, detekci nedosažitelných cílů, přesměrování trasy a kontrolu vzdálených hostů. Na rozdíl od TCP nebo UDP protokolů nemá ICMP protokol zdrojové ani cílové porty a nad ním již není žádná další vrstva. Místo toho obsahuje sadu definovaných kódů s typy ICMP zpráv (viz. tabulka č.7). Konkrétní použitý kód tak určuje způsob interpretace zbytku ICMP paketu. Nástroj *ipfwadm* umožňuje filtrovat ICMP pakety v závislosti na poli nesoucí typ ICMP zprávy. Tím je dosaženo stejně efektivního filtrování jako v případě TCP paketů.

Původně jsem chtěl zkombinovat systém pro filtrování paketů ze dvou částí - z paketového filtru *ipfwadm* pod operačním systémem GNU/Linux a z paketového filtru který poskytuje router Cisco 1601. Paketový filtr zabudovaný do routeru Cisco však poskytuje pouze možnost filtrování podle adres. Filtrování tímto způsobem dovoluje omezit tok paketů v závislosti na zdrojové nebo cílové adrese paketů bez nutnosti testování použitých protokolů. Tento filtrovací mechanismus poskytuje i nástroj *ipfwadm*, který navíc umožňuje i filtrování podle služeb.

Kdybych se spoléhal pouze na paketový filtr zabudovaný do routeru Cisco, nebylo by možno zabránit nebezpečí napadení interní sítě metodou podvržení IP adres (tzv. IP spoofing).

I v případě použití nástroje *ipfwadm* není nebezpečí tohoto útoku zcela eliminováno. Tento bezpečnostní problém efektivně neřeší většina nástrojů pro filtrování paketů (KarlBridge, SecureConnect Router a mnohé další). Z těchto důvodů jsem nakonec upustil od kombinace paketového filtru v GNU/Linuxu s paketovým filtrem Cisco routeru. Pro realizaci paketového filtru jsem použil pouze nástroj *ipfwadm*.

Na závěr této části uvedu příklad (převzatý z [4]), jakým způsobem se zachází s nástrojem *ipfwadm*. Na ukázku jsem si vybral službu WWW (World Wide Web), která používá protokol HTTP (Hyper Text Transfer Protocol) používající přenosový protokol TCP. Pravidla pro filtrování WWW jsou uvedena v následující tabulce č. 8.

Podobnou tabulku jsem si vytvořil pro každou službu, jejíž provoz jsem chtěl přes firewall povolit. Na základě těchto tabulek již nebyl problém vytvořit pravidla pro nástroj na filtrování paketů *ipfwadm*.

Směr	Zdrojová adresa	Cílová adresa	Protokol	Zdrojový port	Cílový port	ACK bit	Komentář
dovnitř	externí	interní	TCP	větší než 1023	80	*	příchozí žádost
ven	interní	externí	TCP	80	větší než 1023	nastaven	odpověď na žádost
ven	interní	externí	TCP	větší než 1023	80	*	výstupní žádost
dovnitř	externí	interní	TCP	80	větší než 1023	nastaven	odpověď na žádost

Tab. č.8 Pravidla filtrování služby WWW

* ACK bit nebude nastaven u prvního paketu (paket navazující spojení), zbylé pakety jej nastaven mít budou

V uvedeném případě budou filtrovací pravidla vypadat následovně (pro jednoduchost uvedu část skriptu pro tcsh) :

```
#!/bin/tcsh

#  /*  Filtrovací pravidla pro ipfwadm          */
#  /*  (c) 1998 Marek Uher, uher@uhkt.cz   */

#  /*  Definice proměnných   */
set  HTTP                       =  80
set  TCP                        =  „-P tcp“
set  ACCEPT                     =  „-a accept“
set   DENY                      =  „-p deny“
set  ANYWHERE                   =  „0.0.0.0/0“
set  INTERNAL_NETWORK           =  „193.84.143.0/24“
set  HI_PORTS                   =  „1024:65535“

#  /*  Definice maker  */
alias FW_SET_POLICY             'ipfwadm -I \!*; ipfwadm -O \!*'
alias FW_SET_RULES              'ipfwadm -I \!*; ipfwadm -O \!*'
alias FW_FLUSH                  'ipfwadm -I -f; ipfwadm -O -f '

#  /*  Vyprázdnění seznamu pravidel  */
FW_FLUSH

#  /*  Nastavení implicitní politiky na deny pro vstupní i výstupní rozhraní  */
FW_SET_POLICI  $DENY
```

```
#  /*  Vytvoř pravidlo podle prvního řádku tabulky č.1  */
FW_SET_RULES $TCP -S $ANYWHERE  $HI_PORTS  \
        -D $INTERNAL_NETWORK  $HTTP  $ACCEPT

#  /* Vytvoř pravidlo podle druhého řádku tabulky č.2  */
FW_SET_RULES  $TCP  -S  $INTERNAL_NETWORK  $HTTP \
        -D  $ANYWHERE  $HI_PORTS  $ACK  $ACCEPT

#  /*  Vytvoř pravidlo podle třetího řádku tabulky č.3  */
FW_SET_RULES $TCP -S $INTERNAL_NETWORK $HI_PORTS  \
        -D $ANYWHERE  $HTTP  $ACCEPT

#  /* Vytvoř pravidlo podle čtvrtého řádku tabulky č.4  */
FW_SET_RULES  $TCP  -S  $ANYWHERE  $HTTP \
        -D  $ INTERNAL_NETWORK $HI_PORTS  $ACK  $ACCEPT

# /* konec příkladu */
```

4 Závěr

Podařilo se mi vybudovat a zprovoznit firewall fungující jako paketový filtr. Během budování firewallu jsem narazil na vážnější problémy při výběru a konfiguraci vhodného nástroje pro filtrování paketů v operačním systému GNU/Linux. Pro tento operační systém existuje několik paketových filtrů, ale žádný z nich není pro tuto činnost optimální, o nevýhodách těchto nástrojů jsem se zmínil v kapitole 3.2. Během práce na budovaném firewallu jsem měl možnost srovnání s komerční implementací firewallu firmy Check Point *FireWall-1* [20].

Všechny volně šiřitelné aktuální distribuce paketových filtrů neumožňují například dynamické filtrování, což je velmi výkonný a efektivní nástroj pro filtrování paketů. Konfigurace a vytváření pravidel pro linuxové nástroje je sice jednoduchá, ale velmi nepřehledná. Z tohoto důvodu se hotový seznam filtrovacích pravidel velmi špatně testuje a prakticky neexistuje možnost úplného otestování všech filtrovacích pravidel. Částečně lze filtrovací pravidla prověřit přímo nástrojem ipfwadm, ale toto testování není kompletní.

Pro prověření všech možných způsobů napadení interní sítě, nebo firewallu, bych musel provést velký počet různorodých testů. To však není reálné, neboť nikdy nemohu do těchto testů zahrnout všechny možné způsoby napadení interní sítě. Proto jsem pro testování velkého seznamu pravidel použil metodu pokusu a omylu - provedl jsem simulaci určitého počtu možných reálných ohrožení. Testování a doladění velké sady pravidel je dlouhodobá záležitost. Během této doby se interní síť vystavuje potenciálně velkému riziku napadení a průniku.

Při testování jsem musel velmi často používat pomocné nástroje. Například řádkově orientovaný nástroj *tcpdump* (dodávaný s většinou distribucí GNU/Linux) nebo grafickou aplikaci X^{ni} firmy Fastlane (příloha 6.1). Aplikace X^{ni} je určena pro komplexní analýzu vnitřní sítě. Poskytuje přehlednou formou všechny důležité informace o síti a všech jejích problémech.

I přes problémy s testováním pravidel je firewall funkční a poskytuje určitou úroveň ochrany vnitřní sítě ÚHKT. V budoucnu je možno po aktualizaci firmware routeru Cisco 1601 z dnešní verze IP na verzi IP+ propojit paketový filtr v GNU/Linuxu s novým paketovým filtrem na routeru Cisco. Nový software IP+ poskytuje znatelně lepší možnosti nastavení pravidel než stávající verze firmwaru a tím dává možnost dokonalejšího filtrování paketů.

Pro efektivnější zabezpečení sítě ÚHKT je potřeba spolupráce uživatelů a vedení ústavu na zavádění dalších bezpečnostních opatření. Typickým problémem je nedostatečná znalost základních bezpečnostních principů. Uživatelé si nejsou často vědomi ani nejzákladnějších bezpečnostních pravidel pro práci se svými účty a hesly. Proto je nutné v co nejkratší době vytvořit skutečně fungující bezpečnostní politiku, která by uživatele obeznámila se základními bezpečnostními principy.

Po zprovoznění firewallu se budu zabývat propojením jeho činnosti na další interní bezpečnostní opatření. Jedná se například o výměnu uživatelského softwaru pro přístup k unixovým serverům. Stávající aplikace, které se využívá dnes, komunikují po síti otevřeným kanálem. Proto prosazuji zavedení aplikací, které používají pro komunikaci po síti šifrovaný přenos dat (například SSL telnet nebo ssh). Tyto aplikace snižují riziko odposlechu hesel a celé komunikace mezi klientem a serverem. Bohužel nejsou k dispozici klienti pro nejrozšířenější operační systém na ÚHKT - MS Windows. To velmi ztěžuje změnu bezpečnostních pravidel pro komunikaci v počítačové síti.

Velkou pozornost bude nutno věnovat na další seznámení uživatelů s bezpečnostními principy pro práci v počítačové síti. Je známo, že 80% všech útoků je provedeno z vnitřní sítě umístěné za firewallem [12]. Již dnes probíhají na danou problematiku rozsáhlé diskuse mezi vedením ústavu, správou počítačové sítě a uživateli. Zprovoznění firewallu přineslo první praktické výsledky. Uživatelům bylo zabráněno v používání některých nebezpečných síťových aplikací (např. ICQ). Toto omezení činnosti uživatelů vyvolalo velkou diskusi na dané téma a tím se naskytla dobrá možnost pro obeznámení uživatelů s bezpečnostními principy pro práci v počítačové síti.

V budoucnu bude nutné zavést ještě přísnější bezpečnostní pravidla platná pro práci uživatelů v interní síť. Zvýšení bezpečnosti na firewallu si nevyžádá žádné další finanční náklady (kromě možné aktualizace firmwaru pro router Cisco). Hrubý odhad finančních úspor (chyba odhadu se pohybuje řádově ve sto tisících korun), který jsem provedl v kapitole 2.3, jasně ukázal, že vybudování systému bezpečnostních opatření je vysoce účinné a přineslo očekávaný efekt.

5 Použitá literatura

[1] ***Kritéria hodnocení zabezpečených počítačových systémů***
(Trusted Computer System Evaluation Criteria CSC-STD-001-83, Orange Book), český překlad (c)1994 Nakladatelství Ben

[2] ***Ochrana dat v informatice***
Ing. J. Přibyl, Ing. J. Kodl, (c)1996 Vydavatelství ČVUT

[3] ***Konfigurace a správa sítí TCP/IP***
C. Hunt, (c)1992 O'Reilly, český překlad (c)1997 Computer Press

[4] ***Firewally - principy budování a udržování***
D.B. Chapman, E.D. Zwicky, (c)1995 O'Reilly, český překlad (c)1998 Computer Press

[5] ***Server v Internetu***
L. Lhotka, (c)1996 Nakladatelství KOPP

[6] ***LINUX - Internet server*** (2. upravené vydání)
P.Satrapa, J.A. Randus, (c)1996, 1998 Neokortex

[7] ***UNIX Security***
SysAdmin editors, (c)1997 R&D Books

[8] Časopis ***Data security management***,
II.ročník (1998)

[9] Časopis ***SysAdmin***,
ročník 1998, články věnované bezpečnosti

[10] Časopis ***SUNEXPERT***,
ročník 1997/98, rubrika *System administration*

[11] Časopis ***Performance Computing***,
ročník 1998, rubrika *Daemons & dragons*

[12] Materiály firmy ***Corpus, s.r.o***.

[13] Materiály firmy ***Sun Microsystems, s.r.o.***

[14] ***Sbírka zákonů České republiky***,
č.148/98 - Zákon o ochraně utajovaných skutečností

[15] ***Manuálové stránky*** operačního systému Linux

[16] Článek porovnávající vlastnosti OS ***UNIX*** a ***MS Windows NT***
http://www.pdas.cz/~had/unix-nt.html

[17] Server ***Root Shell,*** věnující se bezpečnostním problémům
http://www.rootshell.com/

[18] Domácí stránka ***Stokely Consulting***
http://www.stokely.com/

[19] Domácí stránka ***Unix Guru Universe***
http://www.ugu.com/ugu/

[20] Domácí stránka firmy ***CHECKPOINT***
http://www.checkpoint.com/

[21] Domácí stránka firmy ***Cisco***
http://www.cisco.com/

[22] Domácí stránka projektu ***Linux Security***
http://www.ecst.csuchico.edu/~jtmurphy/

[23] ***Linux Security Archive***
http://www.sonic.net:80/hypermail/security/mbox/

[24] Domácí stránka firmy ***FishNet***
http://www.kcfishnet.com/

[25] Popis vybraných firewallů
http://education.isinc.com/gtc/security/firewall_products.html

[26] Výběr některých komerčních řešení pro ochranu sítě
http://ipw.internet.com/firewall/index.html

[27] Domácí stránka firmy ***Zeuros***
http://www.zeuros.co.uk/firewall/

[28] Domácí stránka časopisu ***SysAdmin***
http://www.samag.com/

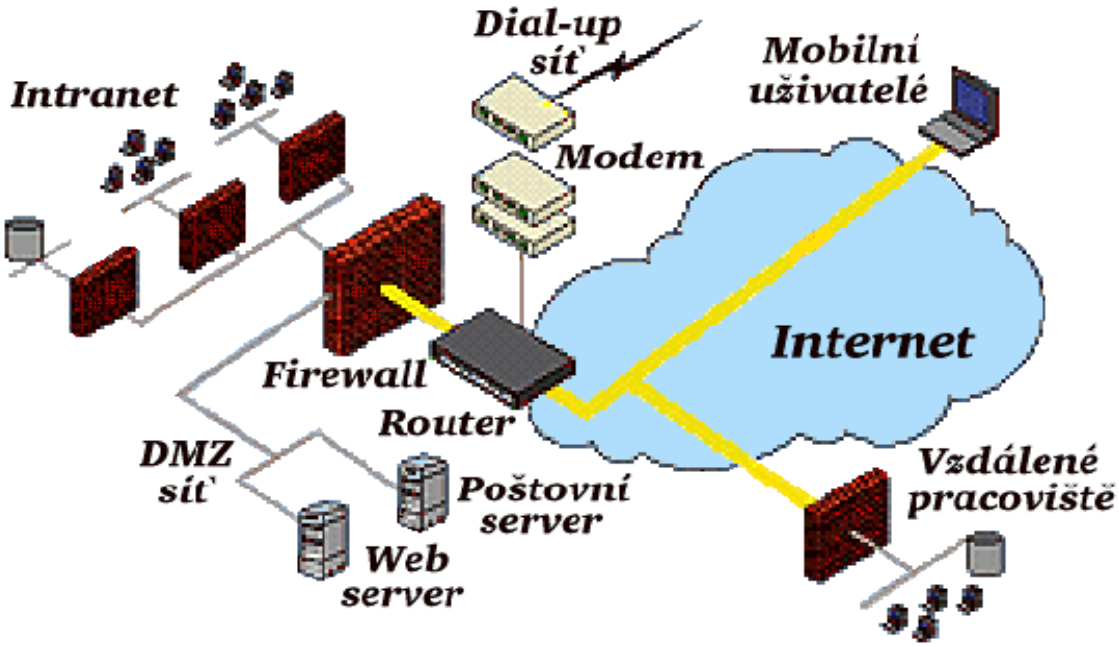
[29] Stránky věnované administrátorům systému
http://www.sysadmin.com/

[30] Stránky věnované operačnímu systému Linux v ČR
http://www.linux.cz/

[31] Domácí stránka firmy ***Caldera***
http://www.caldera.com/

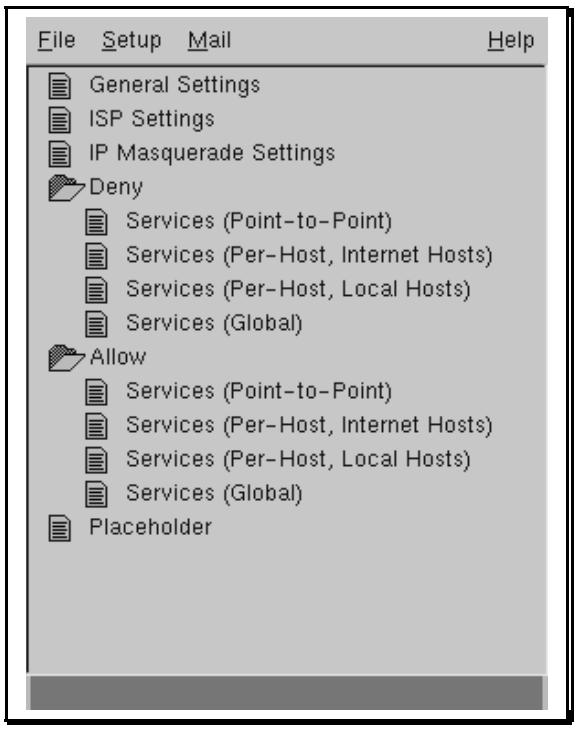
6 Přílohy

6.1 Obrazová dokumentace

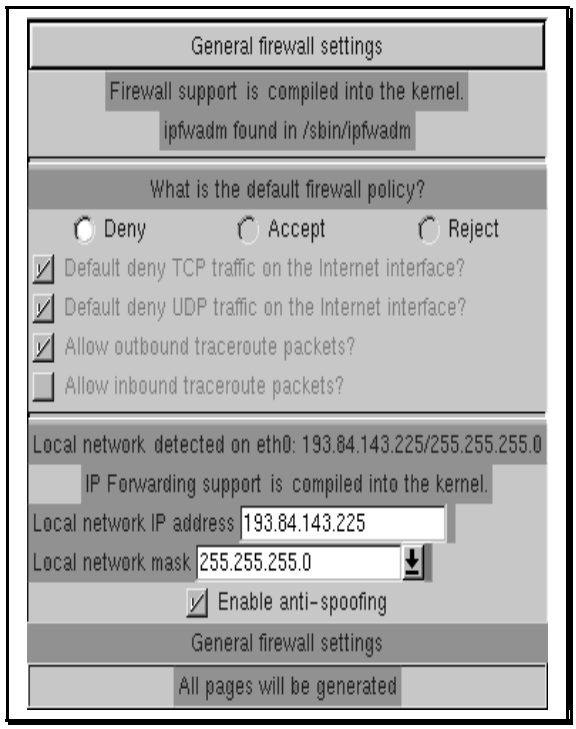


Obrázek č. 1

Obrázek č.1 ukazuje použití kombinace různých technik a technologií použitých při výstavbě bezpečnostních síťových opatření. Při budování firewallu lze jen zřídkakdy vystačit pouze s použitím jedné techniky. Některé protokoly (např. telnet, SMTP) mohou být mnohem účiněji zvládnuty pomocí ***filtrování paketů***. Pro jiné protokoly (např. FTP, WWW, gopher) je mnohem účinnější nasadit techniku ***proxy služeb***. Proto většina firewallů používá kombinaci proxy služeb a filtrování paketů. Proxy služby bývají často umísťovány v tzv. ***DMZ***, jejíž definice je uvedena v textu. I když ve své práci popisuji budování jednoduchého firewallu, smysl může mít i kombinace několika firewallů, jak je ukázáno na výše uvedeném obrázku. Důvody pro takovéto uspořádání jsou různé - zahrnují výkon, redundanci a potřebu oddělit data nebo servery.



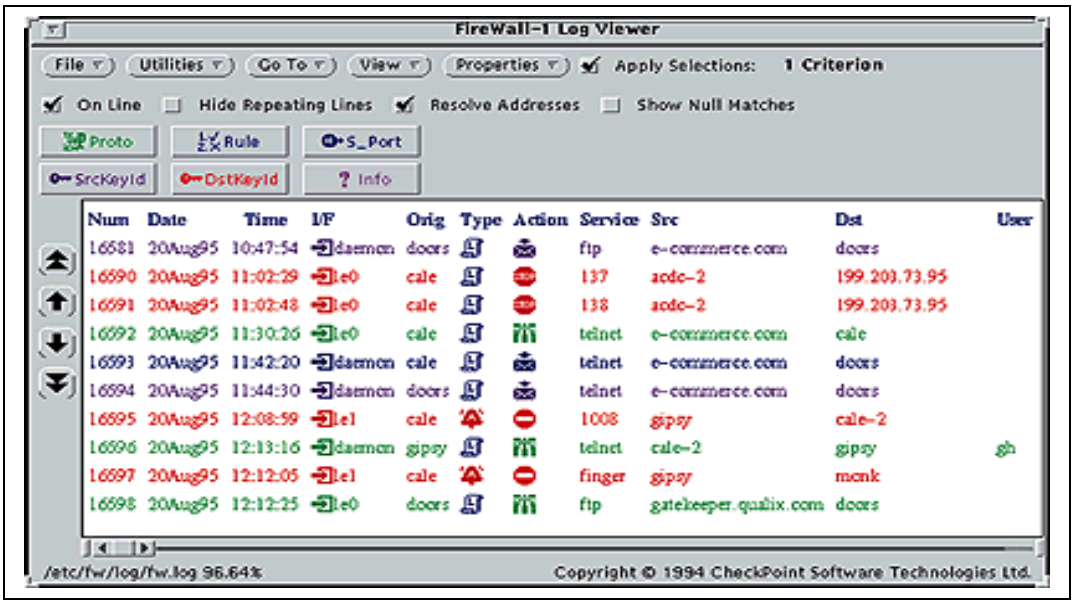
Obrázek č. 2



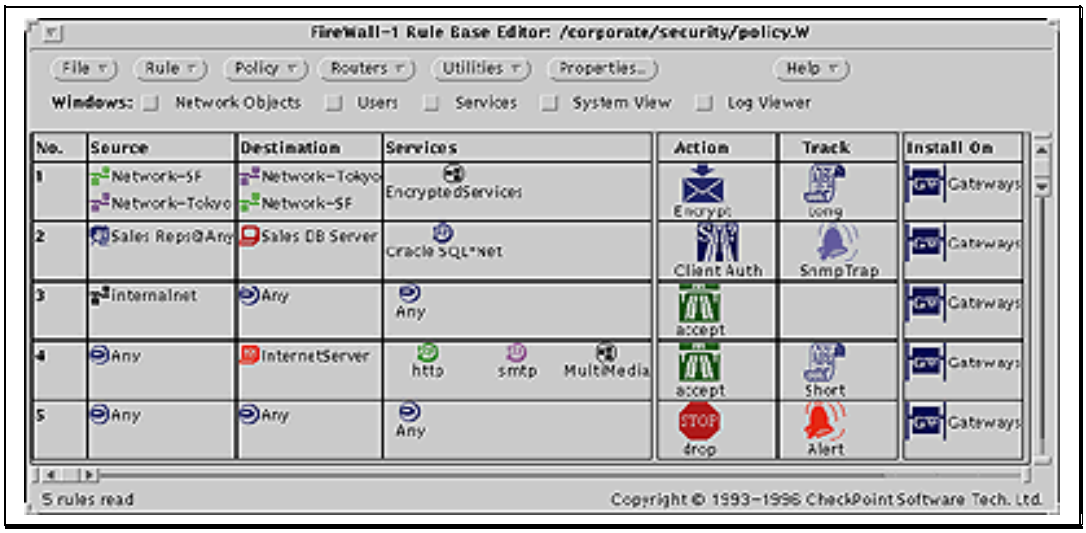
Obrázek č. 3

Obrázek č.2 zobrazuje jeden z mnoha grafických nástrojů pro konfiguraci paketového filtru operačního systému Linux - *ipfwadm*. Jedná se o aplikaci ***dotfile*** napsanou pro grafické uživatelské rozhraní X-Window, které je dodávané s většinou moderních systémů založených na OS UNIX. Zvláštní modul ***ipfwadm*** pro aplikaci *dotfile* umožňuje velmi komfortní nastavování pravidel pro filtrování paketů. Na obrázku č.3 je zobrazena sekce pro nastavení *bezpečnostní politiky*. Lze vybrat ze tří typů bezpečnostní politiky: *accept*, *deny* nebo *reject*.

Jaké důsledky má nastavení jednotlivých bezpečnostních politik v souvislosti s bezpečnostním síťovým modelem je podrobně popsáno v textu zprávy. Velkou nevýhodou tohoto nástroje je, že ho lze používat pouze v prostředí X-Window, které samo o sobě má velmi mnoho nevyřešených bezpečnostních problémů. Aplikaci *dotfile* zde uvádím spíše pro ilustraci, osobně ho pro praktické používání nedoporučuji právě pro jeho „nebezpečné“ uživatelské rozhraní.



Obrázek č.4

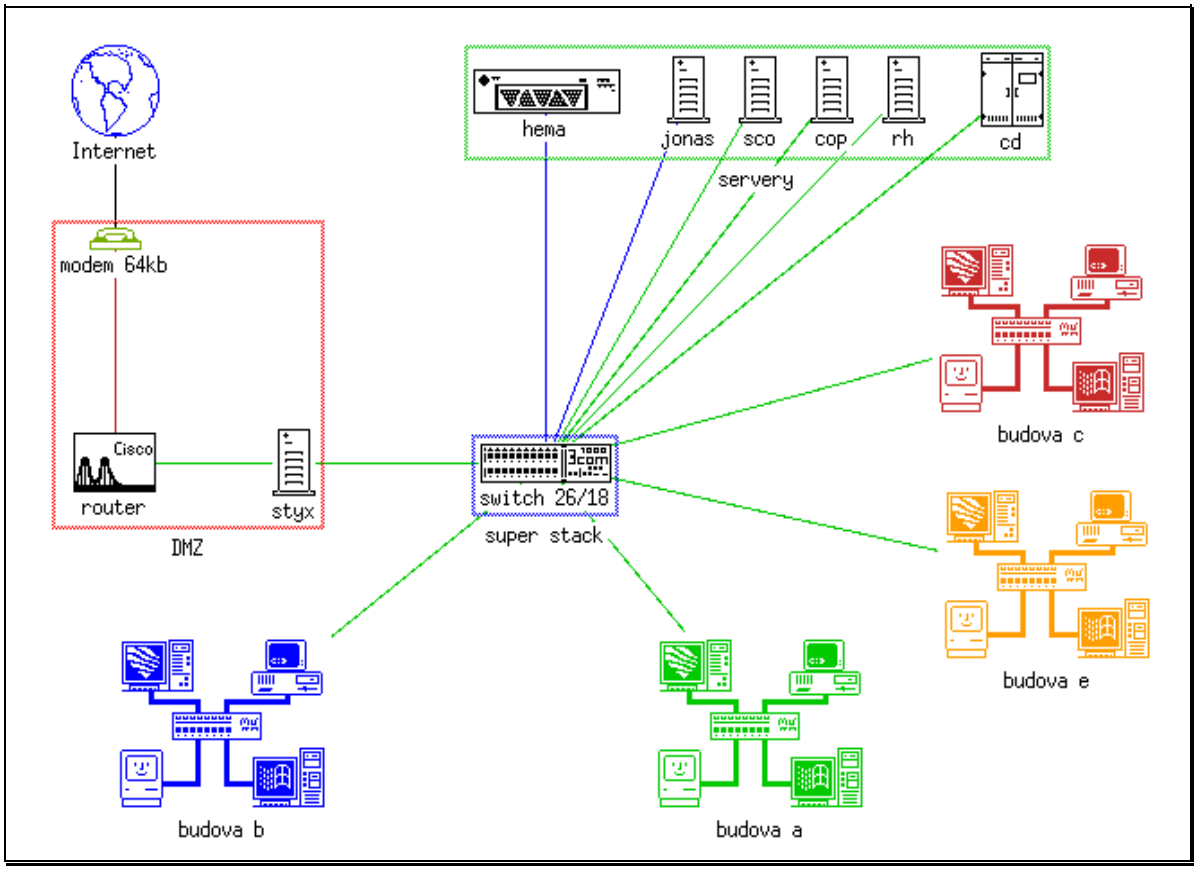


Obrázek č.5

Obrázky č.4 a č.5 ukazují grafické rozhraní komerčního produktu ***FireWall-1*** firmy ***Check Point***. Tento softwarový produkt je kombinován se speciálně upravenými servery společnosti ***Sun Microsystems***. Jedná se patrně o nejlepší systém poskytující maximální ochranu počítačové sítě, který je v současné době dostupný na trhu bezpečnostních technologií.

Obrázek č.6

Na obrázku č.6 je zobrazen software ***X**ni* firmy *Fastlane* pro analýzu sítě. Tento systém je určen pro operační systém UNIX požívající rozhraní X-Window. Nepoužívá se přímo na firewallu, ale slouží k analýze interní sítě umístěné za firewallem. Poskytuje přesný obraz toho, co a kdo právě v daný okamžik v síti dělá. Jsou k dispozici podrobné informace o používaných protokolech, službách, portech, využívání a zatížení sítě a serverů. Tento produkt pokrývá i protokoly mimo rámec rodiny protokolů TCP/IP (např. SPX/IPX a další). Tuto aplikaci jsem měl možnost otestovat a mohu jí vřele doporučit. Je to opravdu velmi silný a výkonný nástroj.



Obrázek č.7

Na obrázku č.7 je vyobrazen zjednodušený model sítě Ústavu hematologie a krevní transfuze v Praze. Síť má hvězdicovou topologii. Centrálním prvkem sítě je přepínač *Super Stack II 1000* firmy *3com*. Nejdůležitější částí z pohledu mé bakalářské práce je demilitarizovaná zóna (DMZ), která se skládá z firewallu (server *Styx*), routeru (*Cisco 1601*) a modemu (*RAD ASM 31, 0.6 - 128kbps*). Do DMZ ještě patří server *Cop*, který poskytuje web proxy službu pouze pro interní uživatele. Funkce jednotlivých serverů je podrobně popsána v příloze B. Zde je také okomentovaná topologie interní sítě, včetně výčtu jejích výhod a nevýhod.

6.2 informace o firewallu

Tato příloha obsahuje podrobné informace týkající se počítače, jenž vykonává funkci firewallu v počítačové síti ÚHKT. V příloze je uvedena hardwarová a softwarová konfigurace počítače. Dále je zde uveden výpis některých důležitých systémových konfiguračních skriptů a obsah důležitých adresářů. Dále je zde uveden okomentovaný výčet finančních limitujících faktorů omezujících realizaci firewallu.

6.2.1 Hardwarová konfigurace

CPU:	AMD K5 133 MHz
RAM:	32MB EDO
HDD:	1.2 GB EIDE
Grafická karta:	512kB
Monitor:	14 ” mono VGA
Síťová rozhraní:	3COM EtherLink 3C905 PCI 100 Mbps
	SMC WD 8013 10 Mbps

Zbývající díly jsou vybrány tak, aby celková cena sestavy nepřesáhla částku 20 000,- Kč. Tuto částku jsem měl k dispozici na zakoupení hardware potřebného na stavbu firewallu.

6.2.2 Softwarová konfigurace

Operační systém: Caldera OpenLinux 1.1

Jedná se o komerční distribuci firmy Caldera, Inc. z USA. Produkty firmy Caldera u nás distribuuje firma IPEX s.r.o. Cena distribuce je přibližně 18 500,- Kč (počítáno podle aktuálního kurzu amerického dolaru). Dodávka obsahuje sadu 3 CD, manuály a registrační kartu opravňující jejího držitele k měsíční bezplatné podpoře firmy Caldera. Během tohoto měsíce jsou k dispozici bezplatné aktualizace operačního systému. Po skončení této měsíční lhůty si lze zhruba za 13 000,- Kč zakoupit roční servis (obsahuje mimo jiné bezplatné aktualizace na novou verzi operačního systému OpenLinux a další produkty dodávané s touto distribucí). Firma Caldera zřídila svým zákazníkům přehledný anonymní FTP server, na kterém jsou k dispozici opravy operačního systému. Na domácí webové stránce firmy Caldera jsou průběžně publikovány články obsahující informace o bezpečnostních problémech distribuce OpenLinux.

6.2.3 Nastavení systému

Výpis systémových skriptů uložených v adresáři ***/etc/rc.d/rc3.d***, které se startují při přechodu do úrovně číslo 3:

S15inet → ../init.d/inet

S25syslog → ../init.d/syslog

S30amd → ../init.d/amd

S40cron → ../init.d/cron

S41atd → ../init.d/atd

S75keytable → ../init.d/keytable

S98local → ../init.d/local

S99rmnologin → ../init.d/rmnologin

S99skipped → ../init.d/skipped

6.2.4 Výpis běžících procesů

styx # ps -ax

PID	TTY	STAT	TIME	COMMAD
1	?	S	0:02	init
2	?	SW	0:00	(kflushd)
3	?	SW<	0:00	(kswapd)
34	?	S	0:00	(bdflush)
93	?	S	0:01	syslogd
95	?	S	0:00	klogd
103	?	S	0:00	cron
612	3	S	0:00	/sbin/getty tty3 VC linux
613	4	S	0:00	/sbin/getty tty4 VC linux
614	5	S	0:00	/sbin/getty tty5 VC linux
615	6	S	0:00	/sbin/getty tty6 VC linux
959	2	S	0:00	login root
980	1	S	0:00	/sbin/getty tty1 VC linux
1019	2	S	0:00	-tcsh
1510	2	R	0:00	ps ax
107	?	S	0:00	atd

Z výpisu získaného pomocí příkazu ps je vidět minimální zátěž počítače sloužícího jako firewall. Na to bylo pamatováno i při jeho konstrukci. Firewall by měl potenciálním útočníkům nabízet malý výpočetní výkon, což jim v případě průniku znesnadní jejich další činnost.

6.2.5 Nastavení síťových služeb

Na firewallu jsou zrušeny všechny síťové služby spouštěné pomocí démona inetd. Tento démon je vyřazen již při startu počítače. Navíc jsou pravidla pro filtrování paketů nastavena tak, aby znemožnila ostatní síťové služby z a na firewall. Tím je splněno jedno ze základních pravidel pro zabezpečení firewallu (viz. kapitola 3.2).

Více informací o konfiguraci síťových služeb lze získat z následujícího výpisu, který je získán pomocí příkazu netstat:

```
styx # netstat -a
Active Internet connections (including servers)
Proto  Recv-Q      Send-Q      Local Address      Foreign Address State
udp    0           0           *:syslog           *:*
raw    0           0           *:1                *:*
Active UNIX domain sockets (including servers)
Proto  RefCnt Flags   Type      State              I-Node   Path
unix   1      [ACC]   STREAM    LISTENING          245      /dev/log
unix   2      [ ]     STREAM    CONNECTED          266
unix   2      [ ]     STREAM                       267      /dev/log
unix   2      [ ]     STREAM    CONNECTED          297
unix   2      [ ]     STREAM                       321      /dev/log
unix   2      [ ]     STREAM    CONNECTED          17076
unix   2      [ ]     STREAM                       17077    /dev/log
```

6.3 Aplikace firewall

Tato příloha popisuje aplikaci ***firewall***, kterou jsem naprogramoval pro zjednodušení nastavování pravidel pro paketový filtr ***ipfwadm***. Aplikace je naprogramována v příkazovém interpretu tcsh, který je dodáván standardně s většinou distribucí Linuxu. Aplikace se instaluje do adresáře ***/etc/security***. Zde se po rozbalení distribuce *firewall.tgz* vytvoří podadresář firewall obsahující samotnou aplikaci. Pro větší přehlednost jsou vytvořeny během instalace další podadresáře. Adresář ***/etc/security/firewall*** obsahuje následující strom podadresářů:

/accounting

/bin

/config

/modules

/policies

/rules

Popis obsahu a funkce jednotlivých adresářů následuje dále. Adresář ***accounting*** obsahuje jediný spustitelný soubor ***accounting-all***. Tento scénář nastavuje účtovací pravidla, je nutné ho spouštět až po instalaci filtrovacích pravidel. Nastavení filtrovacích pravidel se provádí pomocí skriptu ***firewall***, který je uložen v adresáři ***bin***. Tento skript tvoří jádro mé aplikace. Řídí veškerou činnost související s nastavováním paketového filtru. V adresáři ***bin*** jsou uloženy ještě dva spustitelné skripty: ***fwlog*** (slouží jako jednoduchý logovací nástroj pro skript ***firewall***) a ***fwclear*** který vypíná na firewallu paketový filtr.

V adresáři ***config*** se nacházejí dva centrální konfigurační soubory. První z nich ***firewall.cfg*** slouží pro konfiguraci aplikace firewall. Po instalaci aplikace lze v tomto souboru doladit určitá nastavení. Druhý soubor ***fwlog.cfg*** slouží k nastavení vlastností popřípadě formátu logovaných událostí pomocí nástroje ***fwlog***. I tento soubor si možná vynutí dodatečné nastavení.

Adresář ***modules*** obsahuje několik modulů, které jejichž obsah a nastavení se budou na každém systému zcela určitě lišit (na rozdíl od centrálních konfiguračních souborů ***firewall.cfg*** a ***fwlog.cfg***, které mohou zůstat beze změny s implicitním nastavením). Obsah a funkci těchto modulů lze snadno odvodit od jejich názvů. Tyto soubory je nutno ručně editovat, neboť obsahují informace o nastavení sítě. Nahrávání jednotlivých modulů je definováno v souboru ***firewall.cfg***. Pořadí, v jakém jsou moduly nahrávány je důležité, neboť mezi moduly existuje závislost. V případě vytvoření nového modulu je nejlepší ho připojit až na konec seznamu modulů. Standardně jsou s aplikací firewall dodávány následující moduly:

module.debug

module.errors

module.messages

module.misc

module.network

module.servers

Další podadresář s názvem ***policies*** obsahuje definici pravidel pro nastavení implicitní bezpečnostní politiky. Výběr bezpečnostní politiky se provádí v konfiguračním souboru ***firewall.cfg*** (implicitně je nastavena na ***deny***, viz. kapitola 2.1). Soubory v tomto adresáři není nutné editovat. Veškeré nastavení se provádí ve výše zmíněném souboru ***firewall.cfg***. Adresář obsahuje následující soubory:

policy.in.accept

policy.in.deny

policy.in.reject

policy.out.accept

policy.out.deny

policy.out.reject

Poslední a patrně nejdůležitější podadresář ***rules*** obsahuje jediný soubor ***rules.list***. V tomto souboru je uložen seznam pravidel pro filtrování paketů. Z hlediska mé bakalářské práce je to nejdůležitější část celé aplikace firewall. Jeho obsah ovlivňuje bezpečnost celé interní sítě a vlastní funkčnost firewallu. Pořadí pravidel uvedených v souboru ***rules.list*** je důležité. Při vkládání nového pravidla je třeba dát velký pozor na jeho umístění. Jedno špatně umístěné pravidlo může zcela vyřadit z činnosti celý firewall.

Všechny soubory aplikace firewall jsou důkladně okomentovány. Proto doufám že informace, které čtenář postrádá v tomto textu najde zcela určitě v doprovodných komentářích v jednotlivých souborech.

Pro aktivaci firewallu již při startu systému doporučuji přidat do startovacích skriptů systému následující řádek:

/etc/security/firewall/bin/firewall

Popřípadě pro účtování přenesených dat řádek:

/etc/security/firewall/accounting/accounting-all

Tím se zaručí automatické spouštění firewallu již během startu počítače a následná ochrana interní sítě bez nutnosti zásahu administrátora.

6.4 Citlivé objekty počítačové sítě ÚHKT

Tato příloha obsahuje výčet tzv. citlivých objektů počítačové sítě ÚHKT. Jsou zde uvedeny všechny servery a důležité aplikace a služby, které poskytují.

- ***Server hema:***

  Hardware: Sun Netra i 1/170 (model 1175), UltraSPARC 167 Mhz, 192 MB RAM, 1 x 2.1 GB interní Fast/Wide SCSI disk, 3 x 9.1 GB externí Fast/Wide SCSI disk, FastEthernet 10/100 Mbps

  OS: Sun Solaris 2.6

  Software: Netra Internet Software 3.1, Netscape Enterprise FastTrack server, ERL server MedLine

  Aplikace: ERL databázový server obsluhující 13 GB dat lékařských informací, podnikový informační systém VEMA (mzdové údaje, osobní údaje zaměstnanců), primární NFS server, poštovní server, WWW server

- ***Server sco:***

  Hardware: Pentium 100 MHz, 32 MB RAM, 1 x 1.6 GB EIDE interní disk, 10 Mbps Ethernet card

  OS: SCO UNIX System V Release 3.2

  Software: Databázový server SuperNOVA

  Aplikace: Databáze zdravotní pojišťovny (obsahuje informace o pacientech, vyšetřeních, diagnózách, lécích). Slouží jako podklad pro vykazování zdravotním pojišťovnám.

- ***Server cd:***

  Hardware: Control Data 4330, MIPS 3030 33 MHz , 24 MB RAM, 2 x 1.2 GB SCSI 2 interní disk, 10 Mbps Ethernet card

  OS: EP/IX 1.4.3 (UNIX System V Release 3)

  Aplikace: Zálohovací server

- ***Server rh:***

  Hardware: Pentium 166 MHz, 32 MB RAM, 1 x 2.1 GB interní disk EIDE, 10 Mbps Ethernet card

  OS: Debian GNU/Linux 2.0 (hamm)

  Aplikace: Slouží jako sekundární bootp a dhcp server, centrálně řídí zálohování ostatních serverů

- ***Server cop:***

  Hardware: Pentium 150 MHz, 64 MB RAM, 1 x 2.1 GB interní EIDE disk, 10 Mbps Ethernet card

  OS: Debian GNU/Linux 2.0 (hamm)

  Aplikace: web proxy server, primární bootp a dhcp server

- ***Server novell:***

  Hardware: Pentium II 233 MHz, 128 MB RAM, 2 x 9.1 GB interní Fast SCSI disk, 100 Mbps Ethernet Card

  OS: Novell NetWare 4.11 (licence pro 250 uživatelů)

  Aplikace: Lékařská data pro klinický úsek (databáze hospitalizovaných pacientů), aplikace TransNet (registr dárců krve včetně dárců vzácných krevních skupin a vyřazených dárců - např. s diagnózou AIDS), informační systém transfuzní stanice, lékařský informační systém (systém pro evidenci lékařských zpráv a vyšetření), finanční účetnictví ÚHKT