Způsoby ochrany počítačových sítí a samostatných počítačů pomocí technologie firewallů

Protection of computer networks and personal computers using firewalls

Jaroslav Krajča

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jaroslav KRAJČA**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Způsoby ochrany počítačových sítí a samostatných počítačů pomocí technologie firewallů**

Zásady pro vypracování:

1. **Proveďte průzkum informačních zdrojů a literární rešerši z oblasti bezpečnosti ICT zaměřenou na technologii firewallů.**
2. **Analyzujte současný stav a porovnejte různá řešení (využijte metodiku SWOT).**
3. **Navrhněte vhodné řešení pro zvolené oblasti formou projektu.**
4. **Zvolená řešení prakticky realizujte a diskutujte jejich pozitiva a negativa.**
5. **Stanovte závěry k dané problematice včetně dalších doporučení.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **STREBE, Mathew, PERKINS, Charles. Firewally a proxy-servery. Lenka Hendrychová. [s.l.] : Computer Press, 2003. 473 s. ISBN 80-722-6983-6.**
2. **KRÁL , Mojmír. Bezpečnost domácího počítače. [s.l.] : Grada, 2006. 336 s. ISBN 80-247-1408-6.**
3. **THOMAS M., Thomas. Zabezpečení počítačových sítí. [s.l.] : Computer Press, 2005. 344 s. ISBN 80-251-0417-6.**
4. **BITTO, Ondřej. Jak zabezpečit domácí a malou síť Windows XP : Účty, práva, firewally, antiviry a další nástroje. [s.l.] : Computer Press, 2006. 216 s. ISBN 80-251-1098-2.**
5. **LOCKHART, Andrew. Bezpečnost sítí na maximum : 100 tipů a opatření pro okamžité zvýšení bezpečnosti vašeho serveru a sítě. [s.l.] : Computer Press, 2005. 280 s. ISBN 80-251-0805-8.**

Vedoucí bakalářské práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav aplikované informatiky

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je poskytnout čtenáři základní pohled na problematiku firewallů, jeho technologii a funkci. Tato práce ukazuje charakteristické prvky, ze kterých se firewall skládá a jejich princip funkce. Praktická část se pak zabývá problematikou zabezpečení osobního počítače a sítě malé a střední firmy pomocí dostupných firewallů.

Klíčová slova:

Firewall, síťová bezpečnost, paketový filtr, proxy, NAT, VPN

ABSTRACT

The aim of this work is to provide the reader with a basic view of the firewalls, and its technology function. This work shows the characteristic features of which consist firewall and operating principles. The practical part deals with the security of personal computers and networks of small and medium-sized businesses using firewalls.

Keywords:

Firewall, network security, packet filter, proxy, NAT, VPN

Chtěl bych poděkovat především vedoucímu mé bakalářské práce doc. Mgr. Romanu Jaškovi, Ph.D. za cenné připomínky a rady při řešení problémů související s bakalářskou prací.

Prohlašuji, že

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

Prohlašuji,

že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Internet se za několik posledních let rozšířil obrovskou rychlosti a setkáváme se s ním každý den. Je to obrovský zdroj informací, výborný komunikační prostředek a sbližuje mnoho lidí. Nese s sebou ale také mnoho záporů. Působí zde mnoho hackerů a škodlivého softwaru.

Časy, kdy jediným problémem pro počítač byla zavirovaná disketa vašeho známého, jsou nenávratně za námi. Nebezpečí dnes nepředstavují pouze viry, ale také problémy týkající se osobních údajů uživatele, jako jsou hesla, důležitá data a podobně. Každou chvíli je ohromné množství počítačů a počítačových sítí napadáno nebezpečnými programy a jsou vydávány na pospas útočníkům.

Vedle kvalitního antivirové programu a antispyware programu je tedy firewall jedním z nejdůležitějších nástrojů pro zabezpečení našeho počítače nebo počítačové sítě. Používání firewallu při práci s internetem je nezbytností. Lidé, kteří ho nepoužívají, posílají pozvánku virům, spywaru a jiným nežádoucímu softwaru.

Stejně jako každý z nás chrání svůj byt či dům před zloději, musí i každá společnost chránit svou počítačovou síť. Dnes již nezáleží na velikosti nebo na počtu samotných počítačů připojených k internetu, je nutné chránit síť jako celek, včetně ochrany klíčových serverů, na nichž běží aplikace typu mailserver, fileserver, databázový server a další. Pomocí firewallů můžeme tak dosáhnout nejbezpečnějšího možného připojení k internetu.

I. TEORETICKÁ ČÁST

1 CHARAKTERISTIKA FIREWALLU

Firewall je síťové zařízení, které 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. Tato pravidla historicky vždy zahrnovala identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port, což je však pro dnešní firewally už poměrně nedostatečné – modernější firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS.

1.1 Prvky firewallů

Pomocí firewallů lze dosáhnout nejbezpečnější možné připojení k Internetu. Firewally kontrolují a poté schvalují nebo zamítají jednotlivé pokusy o připojení mezi interní sítí a externími sítěmi jako je např. Internet. Robustní firewally chrání síť na všech vrstvách od linkové až po aplikační.

Firewally jsou umístěny na hranicích sítě a jsou přímo připojeny k okruhům, které poskytují přístup k jiným sítím. Z tohoto důvodu se jim často říká zabezpečení hranic. Pojem zabezpečení vnějších hranic je důležitý - bez tohoto konceptu by každý hostitelský počítač v rámci sítě musel provádět funkce firewallů sám, zbytečně by zatěžoval své prostředky a zdroje, a tak by v lokálních, velmi rychlých sítích zvyšoval dobu potřebnou k připojení, autentizaci a zašifrování dat. Použitím firewallu lze soustředit veškeré externí služby zabezpečení do optimálního zařízení, vyhrazeného přímo k tomuto účelu. Kontrola provozu na hraničních bránách má dále také tu výhodu, že zamezuje, aby provoz, který byl napaden hackerským útokem, využíval kapacitu interní sítě.

Ze své podstaty vytvářejí firewally mezi interními a externími sítěmi úzká místa, protože veškerý provoz, který putuje mezi interní sítí a externím prostředím, musí projít jediným bodem. To je ale nízká cena, kterou je nutné za zabezpečení zaplatit. Externí připojení pomocí pronajatých linek je v porovnání s rychlostí moderních počítačů relativně pomalé, takže čekací doba způsobená firewally může být zcela transparentní. Pro většinu uživatelů se standardním připojením k Internetu typu TI postačí i relativně levné firewally. Pro podniky a ISP, jejichž internetový provoz je mnohem obsáhlejší, byl vyvinut zcela nový druh extrémně rychlých (a také velmi nákladných) firewallu, které se vyrovnají i s těmi nej-

náročnějšími privátními sítěmi. Některé země dokonce pomocí vysokorychlostních firewallu cenzurují Internet.

Firewally fungují primárně na základě tří metod:

- **Filtrování paketů**

  Odmítá pakety TCP/IP od neautorizovaných uživatelů a odmítá pokusy o připojení k neautorizovaným službám.

- **Překládání síťových adres (NAT)**

  Překládá IP adresy interních hostitelských počítačů a skrývaje před monitorováním zvenčí. Funkci NAT se někdy také říká maskování adres IP.

- **Služby proxy**

  Vytváří na základě požadavků interních hostitelských počítačů připojení na aplikační vrstvě. Tím úplně ruší propojení mezi interními a externími hostiteli na síťové vrstvě.

Je možné použít i zařízení nebo servery, jež provádí pouze jednu z výše uvedených funkcí; můžete mít třeba směrovač, který provádí filtrování paketů, a pak ve zvláštním zařízení proxy server. Paketový filtr pak musí buď přenášet provoz na proxy server anebo je nutné umístit proxy mimo síť (bez ochrany prostřednictvím filtrování paketů). Obě tato řešení jsou však méně bezpečná než použití jednoho firewallu se všemi funkcemi. Většina firewallu také provádí dvě další důležité služby zabezpečení:

- **Šifrovaná autentizace**

  Umožňuje uživatelům veřejných sítí prokazovat firewallu svou totožnost, a získávat tak přístup k privátní síti z externích lokalit.

- **Propojování virtuálních privátních sítí**

  Ustavuje bezpečné propojení mezi dvěma privátními sítěmi přes veřejné prostředí, např. Internet. Fyzicky oddělené sítě tak mohou ke komunikaci místo pronajatých linek používat Internet. VPN se také říká zašifrované tunely.

Některé firewally také nabízejí dodatečné služby, které se nevztahují přímo k zabezpečení, ale jež mnoho uživatelů ocení:

- **Skenování virů**

  Prohledává příchozí datový toky a zjišťuje, zda neobsahuje signatury virů. Chcete-li mít k dispozici nejaktuálnější signatury, musíte si objednat službu aktualizace virů, kterou poskytuje dodavatel firewallu.

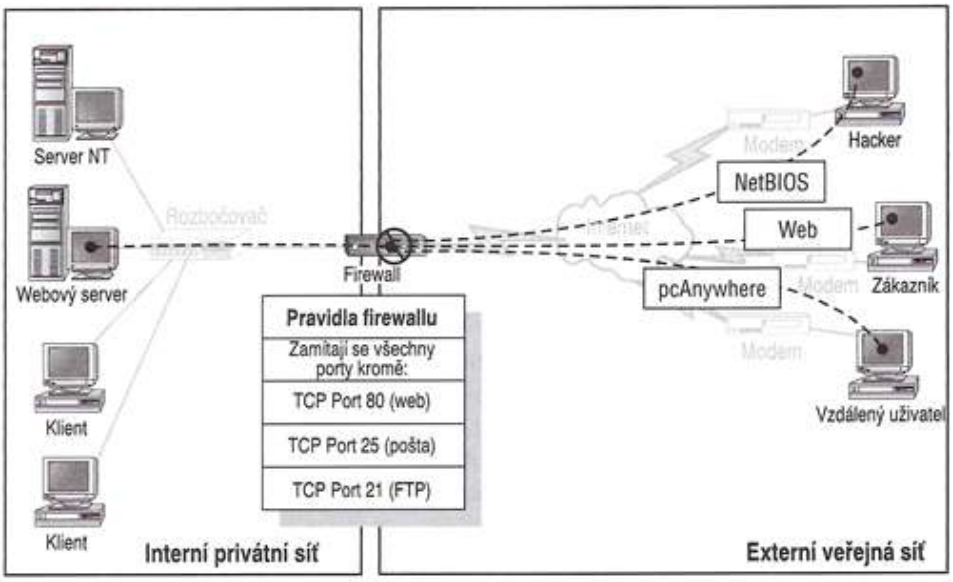
- **Filtrování obsahu**

  Umožňuje blokovat interním uživatelům přístup k určitým typům obsahu podle kategorií, např. pornografie, propaganda rasistických organizací, a informace o hackerství. Aktualizace seznamů blokovaných webových stránek pro určitou kategorii je k dispozici také pouze po registraci služby.

Téměř všechny firewally využívají k zabezpečení sítí tyto základní metody. Na trhu jsou v současnosti k dispozici doslova stovky firewallů a všechny se snaží vymámit ze zákazníků dolary za řešení zabezpečení. Většina firewallů jsou velmi solidní výrobky, které se liší pouze v povrchních maličkostech.

1.1.1 Paketové filtry

První internetové firewally byly jednoduché paketové filtry a filtrování paketů zůstává i nadále jednou z klíčových funkcí dnešních firewallů. Filtry porovnávají síťové protokoly (jako např. IP) a pakety transportních protokolů (např. TCP) s databází pravidel a propouštějí pouze ty pakety, které vyhovují kritériím uvedeným v databázi pravidel. Filtry mohou být implementovány buď ve směrovacích nebo v implementaci TCP/IP protokolů na serverech .



Obrázek 1: Filtrované připojení k Internetu blokuje nažádoucí provoz

Filtry instalované ve směrovacích nepropouštějí podezřelý provoz do cílové sítě. Filtrovací moduly v implementaci TCP/IP protokolů na serverech pouze brání tomu, aby konkrétní zařízení na podezřelý provoz reagovalo. Provoz i přesto dorazí do sítě a mohl by si v rámci této sítě za cíl zvolit jakékoliv zařízení. Směrovače s filtry chrání před podezřelým provozem všechna zařízení v cílové síti. Proto by se mělo filtrování v implementaci TCP/IP protokolů na serverech (jako např. filtrování ve Windows NT) používat pouze jako doplnění filtrování pomocí směrovače a ne místo něj.

Ve filtrech jsou obvykle nastavena tato pravidla:

- Zablokuj pokusy o připojení zvenčí, ale povol pokusy o připojení zevnitř sítě.
- Nepropouštěj pakety TCP určené portům, které by neměly být k dispozici na Internetu (např. port pro relace NetBIOS), ale propouštěj pakety, které by měly být k dispozici (jako např. SMTP). Ve většině filtrů lze přesně uvést, na jaký server by ten který druh provozu měl směřovat - např. provoz SMTP na portu 25 by měl směřovat výhradně na IP adresu poštovního serveru.
- Omez příchozí přístup na určité rozsahy IP.

Kvalitnější filtry zkoumají stav všech připojení, které přes ně procházejí, sledují příznaky naznačující hackování, jako např. přímé směrování, přesměrování ICMP a falšování IP adres (IP spoofing). Připojení, která vykazují výše uvedené charakteristiky, se přeruší.

Omezení filtrování paketů

Filtrování neřeší problém zabezpečení připojení k Internetu beze zbytku. Především je nutné zmínit, že odchozí provoz obsahuje IP adresy počítačů za filtrem. Je tedy celkem snadné zjistit typ a počet hostitelských počítačů připojených k Internetu za filtrem a směrovat útoky proti těmto adresám. Filtrování neskrývá totožnost hostitelů umístěných za filtrem.

U protokolů vyšší úrovně jako jsou hlavičky TCP nejsou navíc filtry schopny kontrolovat všechny fragmenty zprávy IP, protože hlavička je přítomná pouze v prvním fragmentu. Další fragmenty neobsahují ve své hlavičce žádné informace a lze je porovnávat pouze s pravidly na úrovni IP, která jsou většinou volnější, aby přes filtr nějaký provoz propustila. V tomto případě lze zneužít chyb v implementaci IP na cílových počítačích a také by v takovém případě mohlo v rámci sítě docházet ke komunikacím s nainstalovanými trojskými koni. Modernější firewally podporují opětovné sestavování fragmentovaných paketů a následně použití pravidel firewallu na tyto pakety.

Filtry navíc nejsou ani tak inteligentní, aby v rámci paketů síťové vrstvy kontrolovaly legitimitu protokolů. Například nekontrolují pakety HTTP v paketech TCP a nemohou tedy zjistit, jestli tyto pakety neobsahují programy na napadání bezpečnostních chyb (exploity), které pak mohou napadnout webový prohlížeč nebo webový server na vaší straně připojení. Většina moderních útoků hackerů je založena na zneužívání těchto náročnějších služeb, protože kromě útoků, které způsobují nepříjemné odepření služeb, firewally téměř úplně vyloučily úspěšné útoky na síťové vrstvě.

Při ochraně sítě se není dobré spoléhat výhradně na vestavěné filtrování operačního systému. Pomocí operačního systému by se měly nastavit filtry tak, aby propouštěly pouze protokoly, které se mají obsluhovat. Zamezí se tak tomu, aby software pracoval jinak, než je žádoucí a trojské koně nebudou fungovat, ani kdyby se nainstalovaly. Při základním filtrování operačním systémem lze na základě níže uvedených parametrů nadefinovat u jednotlivých síťových adaptérů v počítači pro příchozí připojení následující kritéria přijetí:

- Číslo protokolu IP
- Číslo portu TCP
- Číslo portu UDP

Filtrování se obvykle neuplatňuje na odchozí připojení (tj. připojení, které se zahajuje na serveru) a definuje se zvlášť pro jednotlivé adaptéry v systému.

U standardních serverů jsou služby nastavené tak, aby poslouchaly na následujících portech. Uvedené služby budou fungovat správně jenom když se porty prostřednictvím filtru otevřou.

Jednoduché služby TCP/IP obvykle poslouchají na těchto portech:

Port	Služba PCP/IP
7	Echo
9	Discard
13	Daytime
17	Quote of the day
19	Charakter generator

Tabulka 1: Obvyklé porty služeb TCP/IP

Internetové servery většinou poslouchají na těchto portech:

Port	Server
21	File Transfer Protocol (FTP)
22	Secure Shell
23	Telnet
70	Gopher
80	World Wide Web (HTTP)
119	Net News (NNTP)
443	Secure HTTP (HTTPS)

Tabulka 2: Obvyklé porty internetových serverů

Souborové servery obvykle poslouchají na těchto portech:

Port	Služba
53	DNS (Domain Name Service) (služba DNS v případě, že je nainstalovaná)
135	RPC Locator Service (pouze u Windows NT)
137	NetBIOS Name Service (pouze servery WINS)
139	NetBIOS Session Service (pouze síťové servery založené na Windows a SMB/CIFS)
515	LPR používá služba tisku TCP/IP v případě, že je nainstalovaná
530	RPC (Remote Procedure Call)
3389	Na tomto portu přijímá připojení Windows Terminal Services pomocí protokolu RDP

Tabulka 3: Obvyklé porty souborových serverů

Poštovní servery jsou obvykle nastaveny, aby poslouchaly na těchto portech:

Port	Služba
25	SMTP (Simple Mail Transfer Protocol) (poštovní server na ústředny serverů)
110	POP (Post Office Protocol) verze 3 (server na poštovní ústředny klienta)
143	IMAP (Internet Mail Access Protocol) (přístup klienta na poštovní server)

Tabulka 4: Obvyklé porty poštovních serverů

Pokud se v síti nainstaluje nová služba, je nutné zkontrolovat, jestli je filtr na serveru nastaven tak, aby poslouchal na portech, které služba vyžaduje - jinak nebude služba fungovat. Zjistěte si u výrobce softwaru, které porty se pro danou službu vyžadují. Uvedené informace se netýkají hraničních firewallů, které by se měly nastavit, aby propouštěly službu pouze v případě, že ji hodláte poskytovat veřejnosti.

Všeobecná pravidla pro filtrování paketů

K zabezpečení je možno přistupovat dvěma základními způsoby: pesimisticky, kdy se deaktivuje veškerý přístup kromě přístupu, který je podle názoru administrátora nezbytný. A optimisticky, kdy se povolí všechen provoz kromě provozu, který je zaručeně škodlivý. K zabezpečení by se mělo vždy přistupovat pesimisticky, protože optimistický přístup předpokládá, že administrátor zná všechny hrozby předem, což není prakticky možné. Při filtrování paketů je třeba vzít v úvahu tato všeobecná pravidla:

- V původním nastavení deaktivujte všechny protokoly a adresy a pak výslovně povolte služby a hostitele, které si přejete podporovat.
- Deaktivujte všechny pokusy o připojení k hostitelům v síti. Kdybyste povolili příchozí připojení, umožníte hackerům, aby se připojovali k trojským koním nebo zneužívali chyby v softwaru pro služby.
- Odfiltrujte zprávy s přesměrováním ICMP a zprávy typu „ozvěna" (ping) a neodpovídejte na ně. Blokujte všechny pakety, které využívají přímé směrování TCP. Přímé směrování se používá pro legitimní účely jen málokdy.
- Blokujte všechny aktualizace externích směrovacích protokolů (RIP, OSPF), které jsou určeny interním směrovačům. Vně interní sítě by nikdo neměl přenášet aktualizace protokolů RIP.

- Zvažte deaktivaci fragmentů po nultém fragmentu. Tato funkce je většinou už zastaralá a často přes ni dochází k napadení.
- Pro hostitelské počítače, které obsahují veřejné služby, jako jsou webové servery a servery SMTP, neotevírejte průchody paketovými filtry. Umístěte je raději před paketové filtry.
- Nespoléhejte se při ochraně sítě pouze na filtrování paketů.

1.1.2 Překládání síťových adres

Překládání síťových adres (Network Address Translation - NAT) řeší problém skrývání interních hostitelů. Funkce NAT je v podstatě proxy na síťové vrstvě: požadavky jménem všech interních hostitelů provádí jediný hostitelský počítač, takže totožnost interních hostitelských počítačů je před veřejnou sítí skryta. Windows 2000 a XP, Linux a mnohé moderní operační systémy UNIX tuto funkci poskytují v distribuci operačního systému. Windows NT tuto funkci nemají.

Funkce NAT skrývá interní IP adresy tak, že všechny adresy interních hostitelů zkonvertuje na adresu firewallu. Firewall potom pomocí čísla portu TCP přepošle datovou část z interního hostitelského počítače z jeho vlastní adresy. Tím monitoruje, jaká připojení z veřejné sítě se přiřazují ke kterým hostitelům v privátní síti. Pro Internet se jeví, že veškerý provoz v interní síti pochází od jednoho velmi zaneprázdněného počítače.

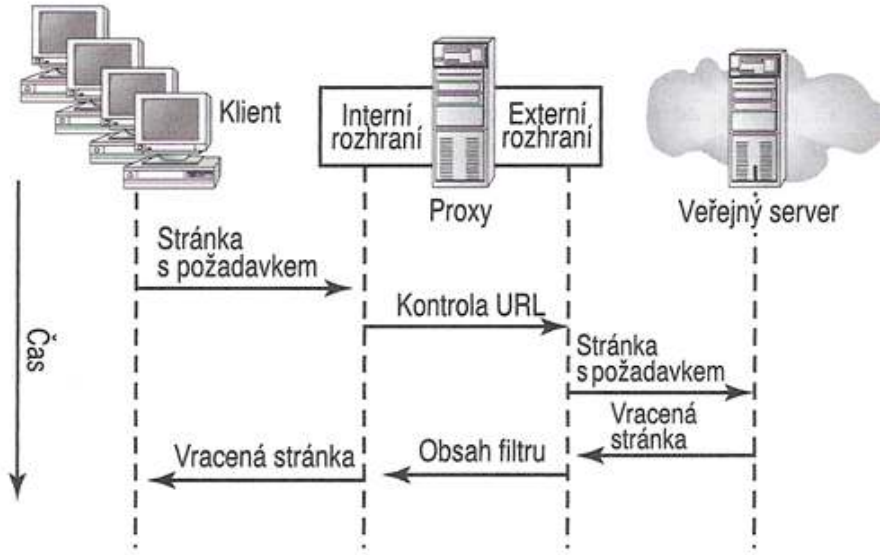
Funkce NAT účinně skrývá veškeré informace o interních hostitelských počítačích na úrovni TCP/IP před zvědavýma očima na Internetu. Funkce překládání adres dále umožňuje používat v rámci interní sítě jakýkoliv rozsah IP adres i v tom případě, že se tyto adresy používají už jinde na Internetu. Nemusíte tedy ARIN žádat o velký rozsah IP adres ani měnit síťová čísla, která jste aktivovali, když jste připojovali síť k Internetu.

Pomocí NAT lze z jedné veřejné IP adresy vysílat více zpráv do celé sítě. Mnoho malých společností se spoléhá na služby upstream ISP. Tito ISP nepřidělují ochotně větší rozsahy IP adres, protože mají sami omezenou kapacitu. Možná budete chtít sdílet jednu adresu s vytáčeným nebo kabelovým připojením, aniž byste o tom svého ISP informovali. Při použití překládání síťových adres jsou všechna tato řešení možná.

1.1.3 Proxy

NAT řeší mnoho problémů spojených s přímým připojením k Internetu, ale přesto neblokuje tok paketů přes firewall úplně. Někdo se zařízením pro monitorování síťového provozu (network monitor) může monitorovat provoz, který přichází z firewallu a zjistit, že firewall překládá adresy pro jiná zařízení. Pak je tedy možné, aby hacker zpětně provedl únos připojení TCP nebo zfalšoval připojení přes firewall.

Tyto problémy řeší proxy na aplikační úrovni. Umožňují prostřednictvím firewallu úplně přerušit tok protokolů na síťové úrovni a omezit provoz pouze na protokoly vyšší úrovně - HTTP, FTP a SMTP. Proxy na aplikační úrovni je kombinace serveru a klienta pro uvedený protokol. Například webový proxy je kombinace webového serveru a webového klienta. Protokolový server na proxy přijímá připojení od klientů v interní síti a protokolový klient na proxy se připojuje k veřejnému serveru. Jakmile přijme protokolový klient proxy z veřejného serveru data, server proxy zašle data konečnému internímu klientovi.



Obrázek 2: Servery proxy přijímají požadavky v privátní síti a znovu je generuji na veřejné síti

Proxy fungují na hranicích mezi dvěma sítěmi, které nejsou propojeny pomocí směrovačů. Jakmile provede klient v chráněné síti připojení na server ve veřejné síti, obdrží proxy žádost o připojení a připojí se jménem chráněného klienta. Pak proxy postoupí požadavek z

veřejného serveru do interní sítě. Proxy v podstatě provádějí jakožto prostředníci neškodné útoky a jsou dobrým příkladem toho, jak by mohl libovolný systém, který funguje jako prostředník mezi vámi a jiným koncovým bodem systému, případně provádět škodlivější zpracování dat bez vašeho svolení.

Aplikační proxy (jako je např. Microsoft Proxy Server) se od překladačů síťových adres a filtrů liší v tom, že s proxy většinou komunikuje aplikace internetového klienta (obvykle). Sdělíte například Internet Exploreru adresu webového proxy a Internet Explorer pak neprovede rozpoznání IP adresy a nepřipojí se přímo, ale zasílá všechny požadavky z Internetu na tento proxy server.

Aplikační proxy nemusí být nainstalovány na firewallech. Roli proxy může provádět jakýkoliv server, buď v rámci interní sítě nebo mimo ni. Bez firewallu nemáte stále k dispozici žádné skutečné zabezpečení, takže potřebujete oba komponenty. Server proxy musí být před útoky na síťové vrstvě, které způsobují odepření služby (jako např. nechvalně známý „ping of death"), chráněn alespoň nějakým typem paketového filtru. A pokud není proxy nainstalován na firewallu, je nutné nějak otevřít průchod firewallem. Ideálním řešením je, aby firewall prováděl funkce proxy. Tak znemožníte propouštění paketů z veřejného prostředí přes firewall.

1.1.4 Virtuální privátní sítě (VPN)

Virtuální privátní sítě (VPN), kterým se také říká zašifrované tunely, umožňují bezpečné propojení dvou fyzicky oddělených sítí prostřednictvím Internetu, aniž by byla přenášená data odhalována neautorizovaným subjektům. V okamžiku, kdy se vytváří tunel, mohlo by ve vlastních VPN docházet k pokusům o přesměrování, ustavování zfalšovaných připojení a všem možným hackerským útokům. Pokud se ale privátní síť implementuje jako nedílná součást firewallu, mohou napadání VPN během vytváření tunelu zabránit autentizace firewallu a služby zabezpečení.

Jakmile je síť VPN ustavena, odolává po dobu, kdy je zabezpečena šifrováním, napadení. A protože firewally jsou umístěny na hranicích Internetu, fungují jako skvělé koncové body na obou koncích tunelu. Privátní sítě mohou v podstatě přenášet provoz, jako kdyby to byly dvě dílčí sítě ve stejné doméně.

Při využití sítě VPN také mohou uživatelé přímo kontaktovat vzdálené interní hostitele prostřednictvím skrytých IP adres; pokud by přišel pokus o připojení přímo z Internetu, překladače síťových adres a paketové filtry by mu zabránily.

Jsou-li výhodnější z hlediska nákladů, je dobré místo VPN vždy použít pronajaté linky. V případě, že nejsou pronajaté linky k dispozici nebo jsou z hlediska nákladů neúnosné, měla by se pro veškerou komunikaci přes Internet mezi jednotkami organizace použít síť VPN. Při využití VPN jako primární metody komunikace mezi jednotkami organizace lze dosáhnout mnohem vyššího výkonu, když se bude ve všech lokalitách používat stejný ISP, protože provoz VPN nebude nutné směrovat přes zahlcené komerční Internetové ústředny. Nikdy neposílejte privátní informace mezi jednotkami v rámci organizace přes Internet bez nějaké formy šifrování. Nezašifrované hlavičky paketů obsahují cenné informace o struktuře interní sítě.

1.1.5 Šifrovaná autentizace

Šifrovaná autentizace umožňuje externím uživatelům na Internetu prokázat firewallu, že jsou autorizovaní uživatelé a že tedy mají oprávnění provést připojení k interní síti přes firewall. Šifrovaná autentizace může využívat jakéhokoliv množství bezpečných autentizačních protokolů. Jakmile je spojení ustaveno, může nebo nemusí být zašifrováno, v závislosti na tom, jaký firewall se používá a zda byl na klientovi nainstalován dodatečný software, který podporuje vytváření tunelů.

Využití šifrované autentizace je výhodné, protože k němu dochází na transportní úrovni mezi softwarem klienta a firewallem. Jakmile se ustaví připojení, spustí se standardní aplikační software a software pro přihlašování k operačnímu systému zcela transparentně. Nemusíte tedy mít žádný zvláštní software, který podporuje konkrétní nainstalované firewally.

Šifrovaná autentizace ale bohužel snižuje zabezpečení firewallu. Svou podstatou vyvolává tyto problémy:

- Firewall musí na nějakém portu reagovat, protože naslouchá pokusům o připojení. Hackeři se tak mohou dozvědět, že firewall existuje.
- Připojení může být po ustavení pomocí ICMP přesměrováno, obzvláště pokud není zašifrované.

- Hacker, který by sledoval ustavení připojení, může zfalšovat adresu autorizovaného klienta, a získat tak přístup do sítě, aniž by musel stávající připojení přesměrovávat.
- Přístup do sítě lze získat zneužitím ukradeného laptopu s příslušnými klíči.
- Zaměstnanci, kteří pracují doma, se mohou stát cílem napadení, protože jejich počítače mají přístup do privátní sítě.
- Postup autentizace může obsahovat mnoho chyb nebo nemusí být úplně bezpečný, takže kdokoliv na Internetu má možnost otevřít průchody přes firewall.

Ke všem těmto rizikům ve skutečností dochází pouze velmi zřídka. Administrátoři prostředí se středním nebo minimálním rizikem by se neměli ostýchat použít šifrovanou autentizaci, pokud je připojení po celou dobu svého trvání zašifrované.

2. TECHNOLOGIE FIREWALLŮ

2.1 TCP/IP

Pro lepší představu o funkci firewallů je potřeba zmínit, jak vlastně funguje komunikace na internetu a síti. Rodina protokolů TCP/IP obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet. Komunikační protokol je množina pravidel, které určují syntaxi a význam jednotlivých zpráv při komunikaci.

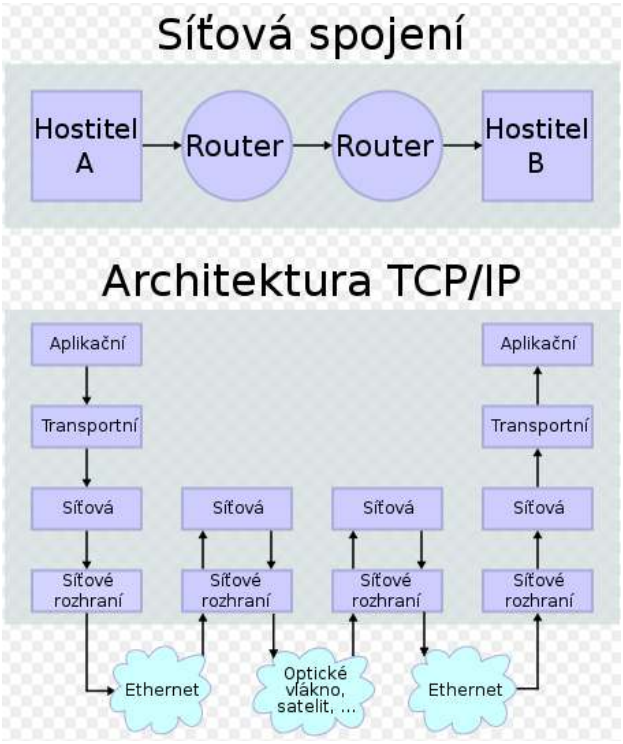
Architektura TCP/IP

Vzhledem ke složitosti problémů je síťová komunikace rozdělena do tzv. vrstev, které znázorňují hierarchii činností. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší. Celý význam slova TCP/IP je Transmission Control Protocol/Internet Protocol (česky primární transportní protokol - TCP/protokol síťové vrstvy - IP).

Komunikace mezi stejnými vrstvami dvou různých systémů je řízena komunikačním protokolem za použití spojení vytvořeného sousední nižší vrstvou. Architektura umožňuje výměnu protokolů jedné vrstvy bez dopadu na ostatní. Příkladem může být možnost komunikace po různých fyzických médiích - ethernet, token ring, sériová linka.

Architektura TCP/IP je členěna do čtyř vrstev (na rozdíl od referenčního modelu OSI se sedmi vrstvami):

- aplikační vrstva (application layer)
- transportní vrstva (transport layer)
- síťová vrstva (network layer)
- vrstva síťového rozhraní (network interface)



Obrázek 3: Vrstvy TCP/IP zajišťující přenos mezi dvěma hostiteli prostřednictvím dvou routerů.

Vrstva síťového rozhraní

Nejnižší vrstva umožňuje přístup k fyzickému přenosovému médiu. Je specifická pro každou síť v závislosti na její implementaci. Příklady sítí: Ethernet, Token ring, FDDI, X.25, SMDS.

Síťová vrstva

Vrstva zajišťuje především síťovou adresaci, směrování a předávání datagramů. Protokoly: IP, ARP, RARP, ICMP, IGMP, IGRP, IPSEC. Je implementována ve všech prvcích sítě - směrovačích i koncových zařízeních.

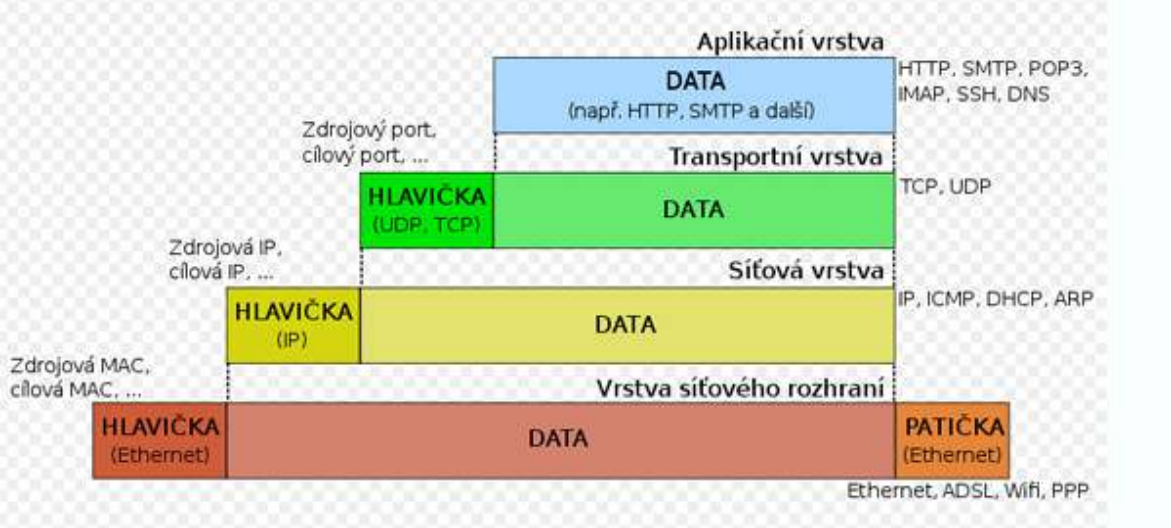
Transportní vrstva

Transportní vrstva je implementována až v koncových zařízeních (počítačích) a umožňuje proto přizpůsobit chování sítě potřebám aplikace. Poskytuje spojované (protokol TCP, spolehlivý) či nespojované (UDP, nespolehlivý) transportní služby.

Aplikační vrstva

Vrstva aplikací. To jsou programy (procesy), které využívají přenosu dat po síti ke konkrétním službám pro uživatele. Příklady: Telnet, FTP, HTTP, DHCP, DNS.

Aplikační protokoly používají vždy jednu ze dvou základních služeb transportní vrstvy: TCP nebo UDP, případně obě dvě (např. DNS). Pro rozlišení aplikačních protokolů se používají tzv. porty, což jsou domluvená číselná označení aplikací. Každé síťové spojení aplikace je jednoznačně určeno číslem portu a transportním protokolem (a samozřejmě adresou počítače).



Obrázek 4: Schéma zapouzdření aplikačních dat na vrstvách TCP/IP.

2.2 Filtrování paketů

Prvními firewally byly paketové filtry. První pokusy o zabezpečení TCP/IP vycházely z předpokladu, že směrovač umí poměrně dobře kontrolovat hlavičky paketů TCP/IP a pakety, které nejsou v souladu se zavedenými specifikacemi, prostě zahazuje. Paketové filtry obsahují nedostatky, kvůli nimž samy o sobě na zajištění úplného zabezpečení interní sítě nestačí. V současnosti se filtry kombinují se servery proxy a překladači síťových adres, a tím se uvedené nedostatky řeší.

Servery proxy původně sloužily k urychlení přístupu k datům z Internetu. Překladače síťových adres původně rozšiřovaly adresový prostor, který měly k dispozici soukromé

organizace a řešily problémy s využitím čísel pro adresy IP, k nimž docházelo v důsledku připojování privátních sítí TCP/IP k Internetu. Nečekané a příjemné výhody obou těchto funkcí pro zabezpečení se spojily s filtrováním paketů a technologiemi pro šifrování a společně položily základ moderním, účinným firewallům.

Ani servery proxy, ani překladače síťových adres nelze dostatečně zabezpečit bez paketového filtru. Paketový filtr zároveň není s to poskytnout celkové zabezpečení bez služeb serveru proxy nebo překladače síťových adres. Uvedené služby jsou účinné pouze v případě, že se sloučí do jediné, konzistentní funkce zabezpečení, takže ke skutečnému zabezpečení sítě by se měly použít firewally, které využívají všechny tři uvedené metody.

Existují dva hlavní typy filtrování paketů:

- Původní, neboli „bezstavové" filtrování paketů, které často používají směrovače a operační systémy.
- Filtrování paketů s kontrolou stavu (stateful inspection), které využívají všechny moderní firewally.

2.2.1 Bezstavové paketové filtry

Paketové filtry jsou hraniční, které posilují zabezpečení tím, že určují, zda paket na základě informací v hlavičce každého jednotlivého paketu přeposlat anebo nikoliv. Teoreticky mohou filtry tuto skutečnost určovat na základě jakékoliv části hlavičky protokolu, ale většinu filtrů lze nastavit, aby filtrovaly pouze nejužitečnější datová pole:

- Typ protokolu
- Adresa IP
- Port TCP/IP
- Číslo fragmentu
- Informace o přímém směrování

Filtrování protokolů

Filtrování protokolů filtruje pakety na základě údajů v poli Protokol IP paketu. Podle údajů v poli Protokol lze také od sebe odlišit sady služeb, např.:

- UDP

- TCP
- ICMP
- IGMP

Například pokud je v síti jednoúčelový server, který poskytuje služby založené na TCP (např. HTTP), bylo by možno odfiltrovat všechny služby UDP. Bohužel, pole protokol je tak obecné (k filtrování jsou k dispozici pouze čtyři běžné protokoly), že většina serverů a směrovačů musí ponechat všechny otevřené.

Filtrování adres IP

Filtrováním adres IP lze omezit připojení na konkrétní hostitelské počítače a sítě (nebo z nich) na základě jejich adres IP. U většiny filtrů lze buď zakázat přístup ke všem hostitelským počítačům kromě počítačů uvedených na seznamu povolených nebo povolit přístup všem hostitelským počítačům kromě počítačů uvedených na seznamu zakázaných.

Zablokování konkrétních určitých hostitelských počítačů je téměř úplně zbytečné, protože by se musela vést evidence o všech hackerech, kteří kdy síť napadli a bylo by nutné předpokládat, že nemají jinou možnost získat informace z jiné adresy IP, což ale nikdy není pravda. Zablokování konkrétního přístupu neustavuje solidní bezpečnostní politiku. Ale obzvláště silné zabezpečení zajišťuje metoda povolení přístupu pouze konkrétním adresám hostitelských počítačů. Je to nejsilnější forma zabezpečení, kterou mohou bezstavové filtry poskytnout. Blokování přístupu ke všem hostitelským počítačům kromě seznamu známých adres IP zajistí, že se ke směrovačům dostanou pouze zařízení nebo sítě s adresami IP, které jsou síti známé. Na seznamu by mohly být i další sítě v organizaci, sítě zákazníků nebo sítě uživatelů, kteří pracují doma. Zablokování přístupu všem ostatním adresám IP téměř hackerovi znemožní, aby síť napadl. Aby se mohl do sítě vlámat, musel by mít přístup k seznamu povolených adres IP.

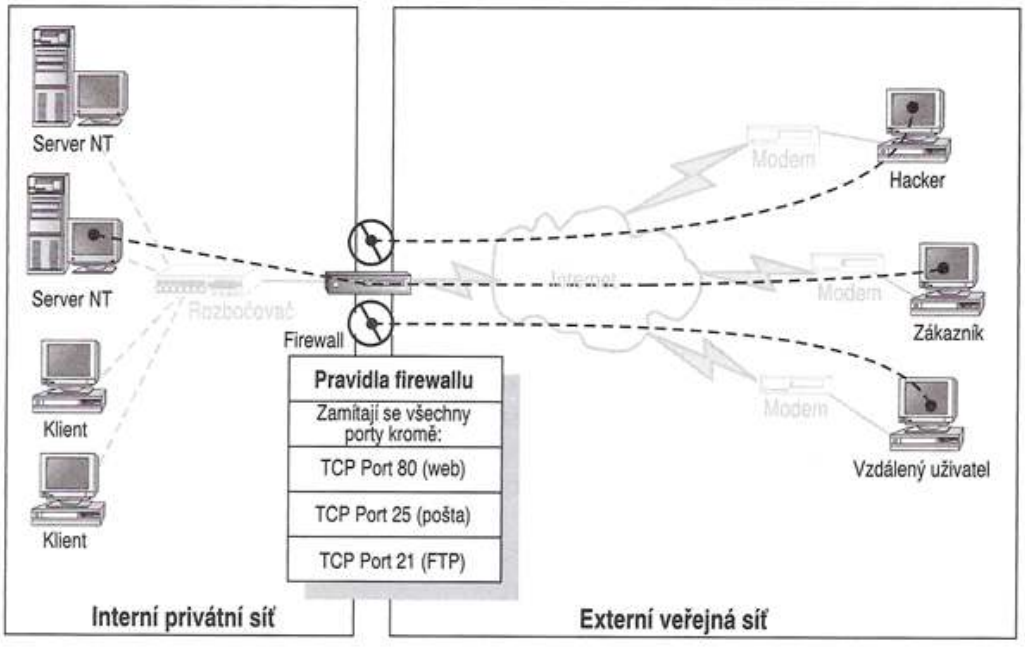
Hacker může adresu IP „vyslídit" pomocí přímého směrování. Při přímém směrování může hacker do paketu umístit povolenou adresu a pak zachytit zpětný provoz tak, že nadefinuje, aby se odpovědi směrovaly na jeho počítač. Z toho důvodu by paketové filtry měly být vždy nastaveny tak, aby zahazovaly pakety s přímým směrováním.

U kvalitních paketových filtrů lze definovat přístup hostitelských počítačů na základě jednotlivých protokolů, takže (například) jde povolit přístup všem hostitelským počítačům přes TCP na portu 80 pro služby HTTP, ale přístup přes TCP na portu 23 (Telnet) povolit pouze počítačům z podnikové sítě. Nejjednodušší filtry nemají seznamy povolených hostitelských počítačů pro jednotlivé protokoly, umožňují pouze vytvořit jeden seznam hostitelských počítačů pro všechny protokoly.

Je důležité mít na paměti, že filtr může omezovat adresy pouze na základě obsahu pole Adresa IP (přičemž údaje v tomto poli se mohou od skutečného zdrojového hostitelského počítače lišit). Hackeři umí u paketu pole s adresou IP zfalšovat, takže určitě mohou paket dostat přes paketový filtr, pokud znají adresu, kterou filtr povoluje. To může být pro hackery užitečné v případech, kdy není nutná zpáteční cesta, např. u útoků s odepřením služby nebo v případech, kde je zpáteční adresa protokolu uvedena v datové části paketu i v hlavičce (např. u FTP).

Porty TCP/UDP

Informace, na základě nichž se nejčastěji provádí filtrování, jsou informace o portech TCP nebo UDP, protože toto datové pole nejpřesněji uvádí, k čemu uvedený paket slouží. Filtrování portů se také běžně označuje jako filtrování protokolů, protože číslo portu TCP nebo UDP identifikuje protokoly na vyšší úrovni.



Obrázek 5: Paketový filtr odmítá nechtěný provoz

Mezi běžné protokoly, které lze filtrovat na základě pole s portem TCP nebo UDP, patří:

Daytime	DNS	Relace NetBIOS
Echo	HTTP	IMAP
Quote	Gopher	NFS
FTP	POP	Whois
Telnet	SNMP	RSH
SMTP	NNTP	

Stejně jako u adres IP umožňuje většina paketových filtrů buď povolit všechny protokoly kromě seznamu zakázaných anebo všechny protokoly kromě seznamu povolených blokovat a stejně jako u adres IP je blokování všech protokolů kromě seznamu povolených bezpečnější. Na rozdíl od filtrování adres IP je ale blokování určitých portů i tak užitečné, protože většina hackerských útoků si jako cíl vybírá pouze několik konkrétních protokolů. Mezi hlavní protokoly, které by se měly blokovat, patří:

- **Telnet**

  Pokud se tento port na hostitelském počítači ponechá otevřený, hackeři mohou získat přístup k příkazovému řádku, který jim může poskytnout kontrolu nad zařízením.

- **Relace NetBIOS**

  Pokud je tento port pro Internet na serverech Windows nebo SMB otevřen, hackeři se budou moci připojovat k souborovým serverům, jako kdyby byli lokální klientské počítače.

- **POP**

  Pro vzdálené klientské počítače, které chtějí mít přístup k poštovním schránkám, by se měla implementovat připojení prostřednictvím VPN, protože POP poskytuje přístup pomocí nezašifrovaných hesel, což hackerům umožňuje monitorovat uživatelská hesla ze sítě.

- **NFS**

  Klientské počítače na Unixu by měly zablokovat přístup k portům NFS ze stejného důvodu jako by klientské počítače na Windows měly blokovat přístup k portům NetBIOS.

- **X Windows**

  Spuštění klientských X aplikací (v prostředích X mají výrazy „klient" a „server" opačný význam než obvykle), způsobí zranitelnost vašeho serveru vůči útokům.

- **Windows Terminal Services**

  Vystavení Windows Terminal Services na Internetu znamená, že terminálový server je chráněn pouze prostřednictvím uživatelského jména a hesla. Informace od klientských počítačů na síti lze získat mnoha metodami.

Tyto porty jsou obzvláště citlivé vůči útokům, protože útočníkovi nabízejí vysokou míru kontroly nad funkcemi systému. Další porty, jako je DNS, lze využít k poškození určitých, konkrétních informací, ale služba sama není dostatečně „bohatá", aby mohla zařízení přímo řídit a tedy není pro útočníka tak zajímavá (samozřejmě všechny služby, které naslouchají, lze potenciálně napadnout útoky s přetečením vyrovnávací paměti a souvisejícími hrozbami).

Mezi další porty, které by se měly blokovat, patří všechny druhy softwaru pro vzdálený přístup nebo kontrolu jako pcAnywhere nebo VNC.

Filtrování dalších informací

Kromě standardních polí obsahují hlavičky i další informace, na jejichž základě lze rozhodnout, zda paket povolit či nikoliv.

Protokol IP podporuje dvě metody, které jsou zastaralé a hackeři je často zneužívají. Jedná se o přímé směrování a fragmentaci. U většiny paketových filtrů lze pakety, u kterých došlo k přímému směrování nebo fragmentaci, zahazovat.

Přímé směrování

Přímé směrování je postup určování přesné trasy, kterou musí paket projít mezi dvěma hostitelskými počítači v propojení přes IP. Směrování zdrojů se původně používalo k odstraňování chyb a testování, ale v současnosti tuto metodu často používají hackeři. Do

pole Zdroj vloží hacker libovolnou adresu, ale přesto zajistí, aby se k němu paket vrátil, protože do volby přímé směrování paketu IP zadá svou vlastní adresu.

Existují tyto dva typy směrování zdrojů:

- Volné přímé směrování, které uvádí jeden nebo více hostitelských počítačů, přes které musí paket projít, ale nikoliv jejich úplný výčet.
- Přísné přímé směrování, které uvádí přesnou trasu, po níž musí paket mezi dvěma počítači projít.

Z těchto dvou typů používají hackeři častěji volné přímé směrování, protože při něm stačí, aby nastavili do pole zdrojová adresa libovolnou adresu IP, adresu IP svého zařízení zadali do pole voleb přímého směrování a paket se jim vrátí za jakýchkoliv podmínek.

Pokud síť přímé směrování nepoužívá, filtry by měly všechny pakety s volbou přímé směrování zahazovat. Přímé směrování nepožadují žádné protokoly ani ISP.

Fragmentace

Fragmentace původně sloužila jako pomoc při přenosu velkých paketů IP přes směrovače. Ty je nemohly kvůli omezením velikosti rámců, která se v některých sítích v minulosti používala, předávat dál. Pomocí fragmentace mohl každý směrovač mezi dvěma hostitelskými počítači rozsekat příchozí paket IP do více menších paketů a pak fragmenty do sítí, které velikost omezovaly, poslat po jednom. Systém příjemce pak prostě vyčkal na všechny fragmenty paketu a pak paket z těchto fragmentů složil do původní podoby.

Problém s fragmentací spočívá v tom, že nejužitečnější údaje pro filtrování, tj. čísla portů TCP nebo UDP, se udávají pouze na začátku paketu IP, takže jsou pouze ve fragmentu 0. Fragmenty 1 a další nelze podle informací o portech filtrovat, protože žádné informace o portech neobsahují. Takže většina prvních filtrů prostě předávala všechny následující fragmenty s tím, že pokud byl zahozen 0. fragment, byly všechny následující fragmenty bezcenné.

Ale není tomu tak vždy. Mnoho závadných verzí protokolů TCP/IP, které jsou nainstalovány na interních hostitelských počítačích, umí paket i tak znovu sestavit a v případě, že pakety 1 až re obsahují platný paket TCP, protokol nebude váhat a použije ho. Hacker tedy může upravit svůj zásobník IP tak, že všechna čísla fragmentů budou začínat od 1 a v podstatě tedy filtr úplně obejdou.

2.2.2 Paketové filtry s kontrolou stavu

Standardní paketové filtry mají mnoho nedostatků, přičemž všechny vycházejí ze skutečnosti, že jednotlivý paket v rámci komunikace neobsahuje dostatek informací k určení toho, zda by měl být paket zahozen či nikoliv, protože tento paket je součástí rozsáhlejší komunikace. Paketové filtry s kontrolou stavu tento problém řeší, protože uchovávají stav celé komunikace, která prochází přes firewall, v paměti a na základě tohoto zapamatovaného stavu pak určují, zda by měly být jednotlivé pakety zahozeny či nikoliv. Zařízení s kontrolou stavu filtrují celé komunikační toky, nikoliv pouze pakety.

Stavové filtry si pamatují stav připojení na síťové a relační vrstvě, protože zaznamenávají informace o ustavení relace, které procházejí přes bránu filtru. Na základě těchto informací pak odlišují platné zpětné pakety od neplatných pokusů o připojení nebo hacker-ských pokusů.

Většina bezstavových paketových filtrů jednoduše povoluje přes firewall všechny porty nad 1 024, protože tyto porty se používají pro zpětné sokety připojení ustavených za fire-wallem z interní sítě. Toto zabezpečení je nesmírně slabé - nic nebrání trojským koním, aby na interní síti vyčkávaly na portu služby nad 1 024, takže bezstavové paketové filtry nemohou tomuto druhu proniknutí zabránit.

Stavové paketové filtry naopak nepropouštějí přes firewall žádné služby, kromě služeb, u nichž mají nastavené povolení, a kromě připojení, která už mají ve svých stavových tabulkách.

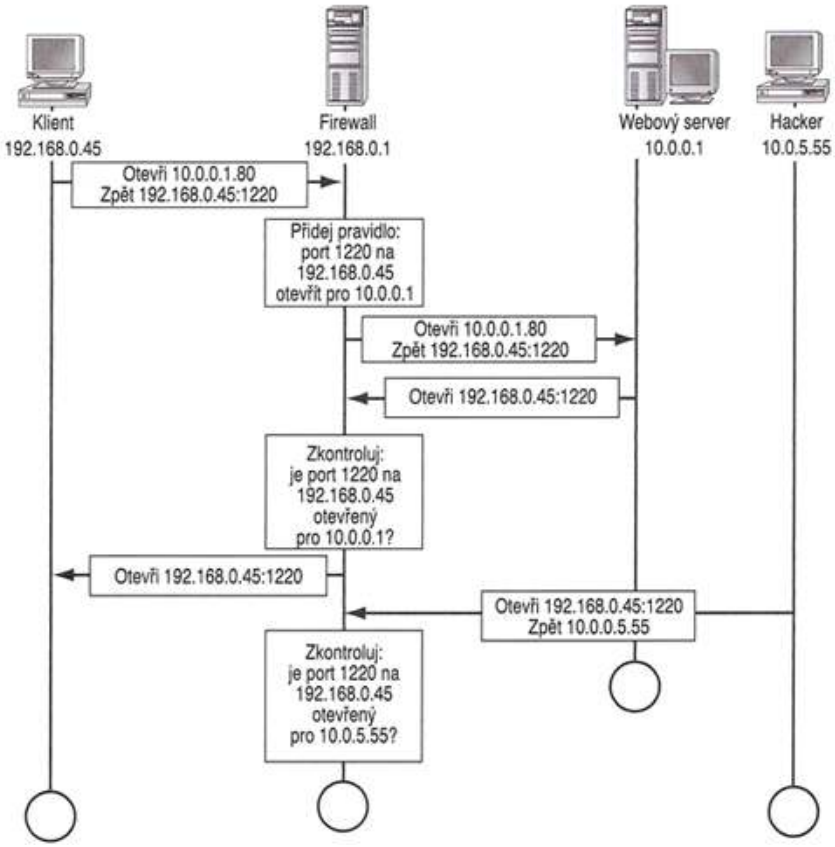
Když se k soketu TCP na externím nedůvěryhodném hostitelském počítači připojí důvěryhodný interní hostitelský počítač, vyšle spolu s paketem o synchronizaci připojení (SYN) soket (adresu IP a port), na němž očekává přijetí odpovědi. Při průchodu paketu SYN přes filtr s kontrolou stavu vloží filtr do stavové tabulky položku, ve které je uveden cílový soket a soket, na kterém se bude odpovídat, a pak paket předá na nedůvěryhodnou síť. Jakmile dorazí odpověď, filtr ve své stavové tabulce vyhledá zdroj paketu a cílový soket a zjistí, zda se shodují s očekávanou odpovědí a paket propustí. Pokud v tabulce žádná položka není, paket se zahodí, protože nebyl vyžádán zvnitřku sítě. Na obrázku 6.2 je znázorněna fáze ustavení spojení na stavovém filtru.

Jakmile přes filtr projdou pakety obsahující dohodu o ukončení relace TCP nebo po určité prodlevě, která obvykle trvá několik minut, filtr ze stavové tabulky položky odstraní. To

zajišťuje, že zahozená připojení nezanechávají ve stavové tabulce otevřené „průchody". Na obrázku 6.3 je znázorněno, jak filtr odstraňuje z tabulky položku, která umožňuje zpětný tok dat z připojení.

U stavových filtrů se pak nastavují pravidla (většinou se jim říká politiky), která toto základní chování upravují. Politiky většinou obsahují pravidla pro pakety, které se vždy zahazují, pro pakety, jež se nezahazují nikdy, pro služby, které se propouštějí zvnějšku na určité konkrétní hostitelské počítače v síti a tak dále. Na multifunkčních firewallech politiky dále upravují překládání síťových adres a používání proxy a obvykle abstrahují adresy IP, sítě a porty do objektů, oblastí a služeb, takže místo blokování portu 80 ze sítě 192.168.12.0 se blokuje „webová služba" z „účetnictví".

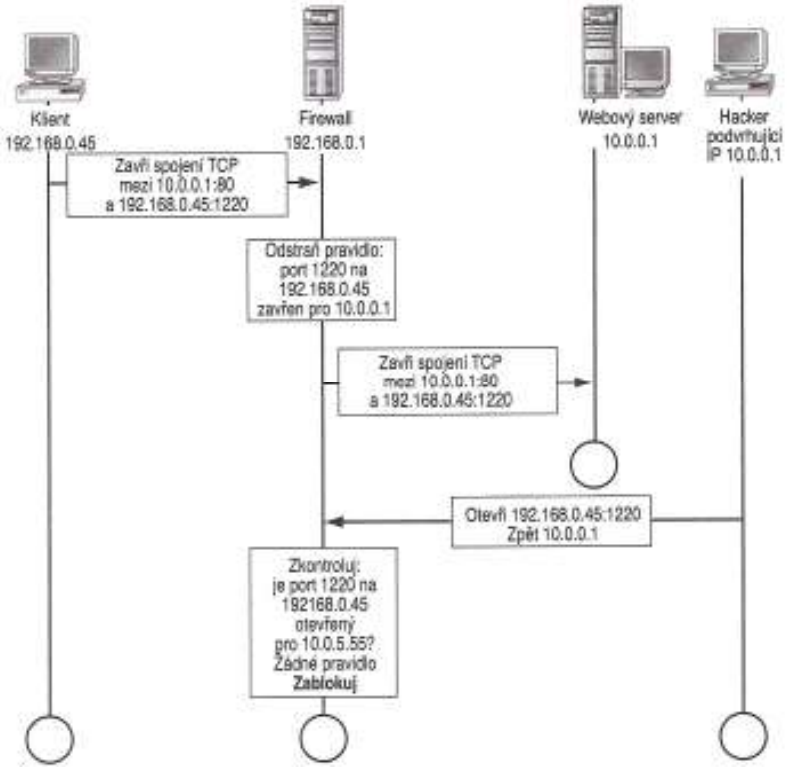
Protože stavové filtry filtrují všechny informace, jež filtrují i bezstavové filtry, a navíc mohou filtrovat fragmenty, informace o tom, z které strany firewallů se ustavuje připojení a další složitější informace, jsou stavové filtry výrazně bezpečnější.



Obrázek 6: Paketový filtr s prohlídkou stavu povoluje zpětná data

Bezstavové paketové filtry ale stále neřeší problém analýzy interních protokolů pro protokoly vyšší úrovně jako jsou HTTP nebo FTP. Dražší, kvalitnější firewally, např.

Firewall-1, ale pro běžné protokoly, např. HTTP, FTP a SMTP, poskytují službu filtrace na vyšších vrstvách podobnou fungování proxy. I když je toto řešení mnohem bezpečnější než absence jakékoliv inspekce na vyšší úrovni, stejně se neregenerují všechny pakety tak, jako je tomu u serverů proxy, takže i nadále existuje možnost, že by přes filtr mohla na cíl uvnitř sítě projít zákeřně zmodifikovaná původní data.



Obrázek 7: Filtr s prohlídkou stavu nechává otevřené „průchody" pouze v nezbytně nutných případech

2.3 Překládání síťových adres

Pomocí překládání síťových adres (NAT) se převádějí privátní adresy IP v privátní síti na jedinečné veřejné adresy IP, které lze použít na Internetu. Ačkoliv NAT se původně implementovalo jako hackerská metoda, která sloužila k uvolnění více adres IP na privátní sítí, má v sobě také neočekávaný a příjemný aspekt bezpečnosti, jenž je stejně významný - skrývání interních hostitelských počítačů.

Překládání síťových adres účinně skrývá všechny informace o interních hostitelských počítačích na úrovni TCP/IP před hackery na Internetu. Veškerý provoz vypadá, jako kdyby pocházel z jediné adresy IP. Při zavedení funkce NAT lze také na interní síti použít libovolný interval adres IP. (I v případě, že se uvedené adresy již používají jinde na Internetu. Ale v takovém případě nelze veřejné servery na veřejném Internetu, které jsou v intervalu adres na privátním Internetu, kontaktovat.) Není tedy třeba si u ARIN nebo ISP registrovat velký, drahý blok ani měnit čísla, která byla přidělena při prvním připojení sítě na Internet.

Když pakety procházejí přes firewall, NAT převádí všechny adresy interních hostitelských počítačů na adresu firewallu (nebo na adresu, na které firewall odpovídá). Postupně tak skryje všechny interní adresy IP. Pomocí překladové tabulky pak pošle datovou část interního hostitelského počítače znovu, ze své vlastní adresy a eviduje všechny sokety na externím rozhraní, které přísluší soketům na interním rozhraní. Internetu se všechen provoz na síti jeví, jako kdyby pocházel z jednoho velmi zaneprázdněného počítače.

Funkce NAT je vlastně jednoduchý server proxy. Požadavky provádí jediný hostitelský počítač jménem všech interních hostitelských počítačů, takže před veřejnou sítí skrývá jejich totožnost. Systém Windows NT tuto funkci neobsahoval, ale Windows 2000 a pozdější operační systémy Microsoft počítačům, které se přes ně připojují k externím sítím (a k Internetu), překládání síťových adres umožňují. Mnoho verzí Unixu obsahuje veřejně dostupný software na maskování adres IP anebo tento software může používat. NAT obsahují i všechny moderní firewally.

Funkce NAT se implementuje pouze na transportní vrstvě. To znamená, že informace skryté v datové části provozu TCP/IP lze zaslat na službu vyšší úrovně a tam jejich prostřednictvím napadnout její nedostatky, anebo ustavit komunikaci s trojským koněm. Pokud se tedy má zabránit porušení zabezpečení služeb vyšší úrovně, je nutné použít i lepší vybavení, např. proxy.

2.3.1 Princip funkce NAT

Firewally mají pro překládání síťových adres k dispozici tabulku obsahující interní sokety přiřazené k externím soketům. Když interní klientský počítač ustaví spojení s externím hostitelským počítačem, firewall změní zdrojový soket na jeden z externích soketů a do

překladové tabulky vloží novou položku, ve které uvede skutečný zdrojový soket, cílový soket a soket spárovaný na firewallů.

Jakmile externí hostitelský počítač pošle data zpět na soket interního hostitelského počítače, firewall provede reverzní překlad. V případě, že v překladové tabulce není pro zkontaktovaný soket žádná položka anebo v případě, že se adresa IP zdroje liší od adresy, kterou firewall očekává, paket se zahodí.

Nejjednodušeji lze fungování NAT vysvětlit na příkladu. Řekněme, že interní hostitelský počítač 192.168.1.9 chce ustavit relaci na Internetu s externím hostitelským počítačem 10.50.23.11. Pomocí prvního volného portu 1 234 vyšle paket TCP na 10.50.23.11:80.

Paket dorazí na směrovač/firewall (interní adresa 192.168.1.1, externí adresa 10.0.30.2) a ten do své překladové tabulky zapíše tento záznam:

Zdroj	192.168.1.9:1234
Veřejný hostitelský počítač	10.50.23.11:80
Překlad	10.0.30.2:15465

Pak vyšle paket na Internet z přeložené adresy IP a přeloženého čísla portu, takže 10.50.23.11:80 (veřejný hostitelský počítač) obdrží pokus o připojení, který pochází z 10.0.30.2:15465 (externí adresa firewallů). Jakmile zašle veřejný hostitelský počítač data zpět, odpoví zdroji, o němž se domnívá, že je původcem požadavku: 10.0.30.2:15465 (externí adresa firewallů).

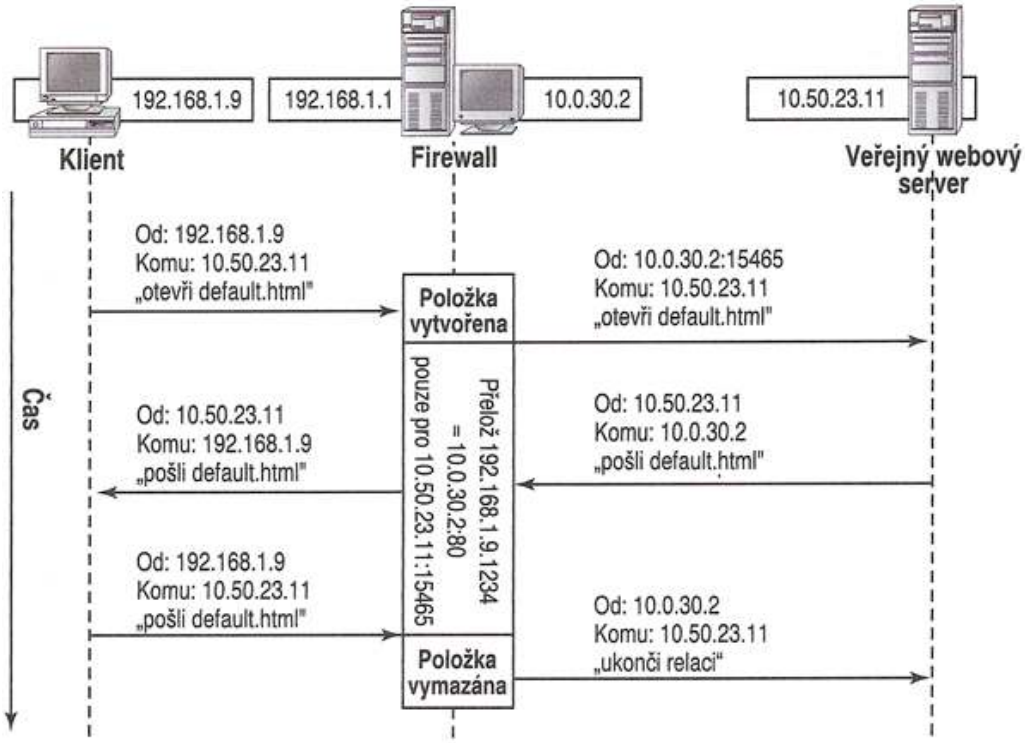
Firewall paket obdrží a vyhledá v překladové tabulce odpovídající soket. Pak ověří, zda se zdroj paketu shoduje s veřejným hostitelským počítačem uvedeným v překladové tabulce při tvorbě položky. Přítomnost položky v tabulce potvrzuje, že si paket vyžádal interní hostitelský počítač - pokud by nebyl paket vyžádán, nebyla by v překladové tabulce žádná položka, která by odpovídala jak přeloženému soketu, tak i zaznamenanému soketu veřejného hostitelského počítače. V případě, že se odpovídající položka nenajde, firewall paket zahodí a událost zaznamená.

Firewall pak do paketu přidá číslo soketu interního zdrojového klienta a předá ho interní síti, aby ho zaslala klientskému počítači - příjemci.

Na straně veřejného hostitelského počítače se NAT také používá v režimu „přesměrování portů". Webový server v tomto případě chrání jiná implementace NAT, která je nastavena,

aby přijímala připojení na své veřejné adrese IP a překládala je pro interní síť. Na rozdíl od NAT na připojení prohlížeče není toto nastavení automatické. Administrátor musí výslovně nastavit zařízení NAT, aby uvedené překládání provádělo.

V uvedeném příkladu zařízení NAT přijme připojení HTTP na 10.50.23.11:80. Prozkoumá svoje překladové tabulky portů a zjistí, že port 80 se přiřazuje k internímu hostitelskému počítači 192.168.0.5:80. Takže překladač přepíše adresu IP z 10.50.23.11:80 na 192.168.0.5:80 a paket přesměruje. Na zpětném toku provede inverzní překlad, takže paket poslaný na 10.0.30.2:1234 (veřejná adresa IP zařízení NAT v prohlížeči) od 192.168.0.5:80 přepíše jeho zařízení NAT na 10.50.23.11:80.



Obrázek 8: Překládání síťových adres

Protože NAT mění adresu IP v paketu, je téměř vždy nutné vkládat do směrovacích tabulek nové položky, aby přeložené pakety dorazily do svého správného místa určení v síti.

V případě přesměrování portů není nutné žádnou „dynamickou" položku vytvářet či ukládat - přepisování adres IP je stejné na odchodu i na příchodu pro každý hostitelský počítač. Přesměrování portů je tedy trochu jednodušší a nevyžaduje na zařízení NAT obsáhlou kapacitu paměti RAM.

Protože při překládání síťových adres dochází ke změně obsahu hlavičky IP, systémy, které se spoléhají na neměnnost těchto dat (např. autentizované hlavičky v IPSec, což je sada protokolů Internet Protocol Security), přes NAT nefungují. Dalším problémem u IPSec je, že překladače síťových adres nesnadno třídí provoz IPSec od více interních klientů. Takže firewally, které provádějí funkci passthrough u IPSec, většinou pouze umožňují, aby se v určitém okamžiku na umístění mimo síť připojoval pomocí tunelů IPSec jenom jeden interní klient.

2.3.2 Režimy překládání

Různé firewally podporují různé typy překládání síťových adres. Uvádíme zde čtyři nejdůležitější funkce NAT na firewallů v pořadí jejich oblíbenosti a dostupnosti:

Dynamické překládání (také se mu říká NAPT nebo maskování adres IP)

Používá se v prostředí, kde interní klienti sdílí jednu interní adresu IP nebo skupinu adres, aby skryli svou totožnost nebo rozšířili adresový prostor v interní síti. Porty na jedné veřejné adrese IP lze přesměrovat na určené privátní adresy IP.

Statické překládání

Používá se v prostředí, kde se staticky překládá blok veřejných adres na blok privátních adres o stejné velikostí. V tomto režimu má interní zařízení v síti (zpravidla server) fixní překládání, které se nikdy nemění.

Překládání s vyrovnáváním zatížení

Používá se v prostředí, kde se překládá jedna adresa IP a port na několik stejně nakonfigurovaných serverů, takže jednu veřejnou adresu může obsluhovat několik serverů.

Překládání s redundancí v síti

Používá se v prostředí, kde je několik připojení k Internetu připojeno k jednomu firewallů s NAT, přičemž volba a využívání těchto spojení probíhá na základě přenosové kapacity, přetížení v síti a dostupnosti.

2.4 Aplikační proxy

Původně proxy poskytovaly počítačům za běžným připojením k Internetu služby ukládání často navštěvovaných internetových stránek do vyrovnávací paměti. V začátcích Internetu

byla propojení v sítích WAN velmi pomalá, Internet byl poměrně malý a stránky na něm byly statické. Celou síť tvořilo jen několik tisíc stránek pro vědecké pracovníky a akademiky. Kdykoliv se na nějaké stránce objevila nějaká nová zpráva, navštívil uvedenou stránku v rámci jedné organizace velký počet vědců (kolikrát jste už u vás ve firmě přeposílali odkaz?). Uložením stránky do vyrovnávací paměti na lokálním serveru minimalizovaly proxy zbytečné připojování k Internetu a opakované stahování stejné stránky. Takže původně byly proxy velmi účinné nástroje na ukládání stránek do vyrovnávací paměti.

Když se z Internetu stala supernova, funkce ukládání do vyrovnávací paměti, kterou proxy zajišťovaly, výrazně ustoupila. Internet je rozsáhlý, stránky jsou často dynamické (tj. vyprší, jakmile se pošlou) a uživatelé v jedné organizaci si mohou mezi návštěvou jedné a té samé stránky prohlížet miliony dalších stránek. Všechny tyto faktory byly samozřejmě pro ukládání do vyrovnávací paměti negativní a proxy se v tomto ohledu vesměs neosvědčily, kromě opravdu velkých organizací nebo ISP. I když všechny standardní prohlížeče měly zabudovanou podporu proxy, kolem roku 1996 se proxy využívaly jen zřídka.

Ale nový Internet má také svou stinnější stránku a v této souvislosti se u serverů proxy objevil neočekávaný a příjemný postranní účinek: umí skrýt všechny uživatele sítě za jediné zařízení, umí filtrovat URL a také umí zahazovat podezřelý nebo nelegální obsah. Takže ačkoliv původně sloužily jako vyrovnávací paměti a ne přímo pro zabezpečení, nyní se prvořadým účelem většiny serverů proxy stává funkce firewallu.

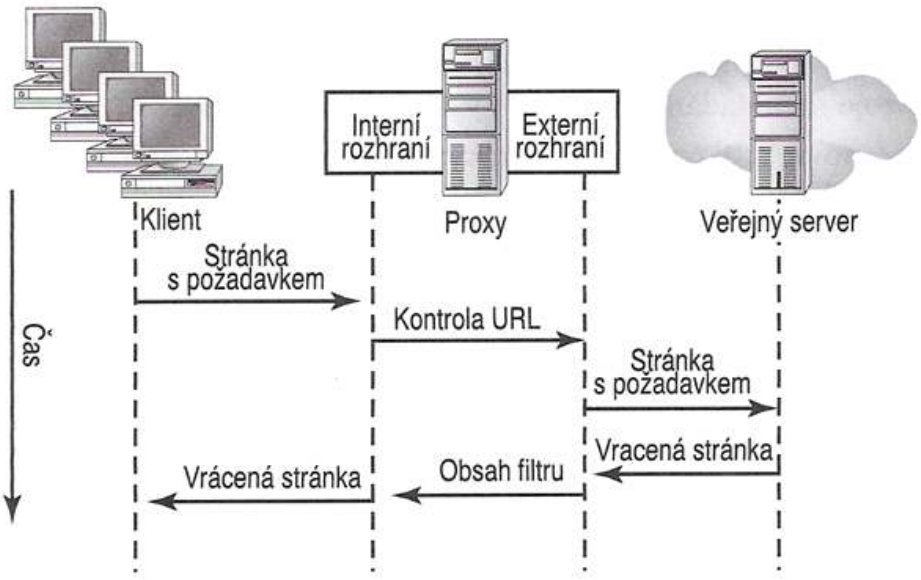
Proxy znovu generují požadavky o služby vyšší úrovně na externí síti jménem klientských počítačů z privátní sítě. Účinně tak před externí sítí skrývají totožnost a počet klientů na interní síti. Proxy jsou umístěny mezi několika interními klientskými počítači a veřejnými servery, takže mohou také do vyrovnávací paměti ukládat často navštěvovaný obsah z veřejné sítě, čímž snižují potřebu přístupu k veřejné síti přes drahá propojení sítí WAN.

Pro lepší pochopení věnujeme tuto kapitolu pouze „čistým" proxy - tj. těm, které fungují na principu forwardování protokolů služeb. Většina skutečných instalací bezpečnostních proxy obsahuje i služby filtrování paketů a překládání síťových adres, takže tvoří kompletní firewall. Kombinací uvedených metod s proxy lze zamezit některým druhům útoků, k nímž jsou čisté proxy náchylné.

Na trhu je spousta různých druhů proxy, od filtrů na aplikační vrstvě ve skutečných, kvalitních firewallech (např. Firewall-1 od Checkpointu), přes aplikace typu „pouze proxy" pro všeobecné použití (příkladem může být WinGate), až po jednoduché proxy s jedinou službou jako Jigsaw pro HTTP. Čisté proxy trpí celou řadou nedostatků, z nichž většina je způsobena tím, že software proxy nechrání základní operační systém před útoky založenými na principu odepření služby a napadáním dalších služeb nainstalovaných na serveru. Proxy se nejčastěji kombinují s internetovou službou HTTP, protože původně byly pro tuto službu vytvořeny. Od té doby se ale funkce proxy začaly využívat i pro většinu ostatních běžných internetových služeb. V příkladech v této části knihy budeme používat službu HTTP, ale funkce jsou z velké části podobné i u dalších služeb.

2.4.1 Princip funkce proxy

Proxy fungují tak, že naslouchají požadavkům o služby od interních klientů a pak je předávají na externí síť jako kdyby byl klientem - původcem samotný server proxy. Jakmile obdrží proxy od veřejného serveru odpověď, vrátí tuto odpověď původnímu internímu klientskému počítači, jako kdyby byl sám původním veřejným serverem.



Obrázek 9: Proxy pro služby

2.4.2 Výhody pro zabezpečení při využití proxy

Opětovné generování požadavků a skutečnost, že proxy je umístěn mezi externí a interní sítí, poskytují pro zabezpečení mnoho výhod:

- Proxy skrývají privátní klienty před veřejným vystavením.
- Proxy mohou blokovat nebezpečné URL.
- Proxy mohou filtrovat nebezpečný obsah, než ho propustí ke klientským počítačům, např. viry a trojské koně.
- Proxy mohou eliminovat směrování na transportní vrstvě mezi sítěmi.
- Proxy poskytují jediný bod přístupu, řízení a přihlašování.

Skrývání klientů

Nejvýznamnější vlastností serverů proxy při zabezpečení je skrývání klientských počítačů. Podobně jako u překládání síťových adres mohou i při využití proxy vypadat celé interní sítě z pohledu Internetu jako jedno zařízení, protože to posílá požadavky na Internet. Jako překladače síťových adres brání i proxy externím hostitelským počítačům, aby se připojovaly ke službám na interních zařízeních. V případě použití proxy neexistuje ke klientským počítačům žádná cesta, protože domény adres interních a externích sítí nemusí být kompatibilní a protože mezi uvedenými sítěmi nedochází ke směrování na transportní vrstvě.

Tato funkce proxy spočívá v tom, že u požadavků na úrovni služeb nedochází pouze ke změně a přepočítání hlavičky adres, ale požadavky se znovu úplně generují. Například když podá požadavek přes server proxy webový klient, proxy požadavek přijme, jako kdyby byl cílový webový server na interní sítí. Pak požadavek znovu vygeneruje na externí síti, jako kdyby byl standardní webový prohlížeč. Když proxy obdrží od skutečného webového serveru odpověď, předá tuto odpověď svému internímu klientovi. Přes proxy prochází pouze HTTP, nikoliv TCP nebo IP. TCP/IP (a další protokoly na nižší úrovni) proxy generuje znovu. Pokud tedy není proxy špatně nastavený, TCP/IP přes proxy neprochází.

Blokování URL

Blokování URL umožňuje administrátorům, aby deaktivovali poskytování určitých stránek na základě jejich URL. Teoreticky vzato tak lze zaměstnancům zabránit v prohlížení stránek, k nimž nechcete povolit přístup. Instalace této funkce je velmi snadná. Proxy prostě před tím, než znovu požadavek vygeneruje, porovná všechny požadavky na určitou

stránku (nebo jinou URL služby) se seznamem zakázaných stránek. Je-li URL stránky blokovaná, proxy stránku nevyžádá ani ji nepošle jako odpověď na požadavek. Blokování URL lze ale snadno obejít, protože stránku lze vyhledat i pomocí její adresy IP anebo dokonce i jako adresu v podobě celého čísla. Stejnou stránku lze do vyhledávače zadat v těchto podobách:

http://www.gamehound.com/default.html

http://192.168.13.12/default.html

http://3232238860/default.html

Závažným nedostatkem, se kterým se musí síťoví administrátoři při blokování URL vyrovnat, je mít aktuální přehled o stránkách, které se mají blokovat. Problematické stránky (např. úložiště pirátského softwaru a hackerských nástrojů, pornografické stránky a stránky s hazardními hrami) mají jepicí život - objevují se a mizí stejně rychle. Většina lidí, kteří se zajímají o témata uvedená na těchto stránkách, používá vyhledávače nebo seznamy Usenet a tam hledají, kam se jejich oblíbené stránky přesunuly. S tím nebudete s to udržet krok.

Filtrování obsahu

Protože proxy přeposílají datové části všech protokolů a fungují vždy pro konkrétní protokoly, lze jejich prostřednictvím datové části zkoumat a zjišťovat, zda neobsahují podezřelý obsah. Službu HTTP na proxy lze nastavit, aby odstraňovala ovládací prvky ActiveX, aplety jazyka Java nebo dokonce objemné obrázky, pokud by mohly být pro zabezpečení rizikové. Z SMTP na proxy se zase mohou odstraňovat přílohy se spustitelnými soubory programů a archivované zazipované soubory, pokud by mohly ohrožovat zabezpečení. Díky filtrům obsahu lze také kontrolovat, zda webové stránky neobsahují určitá slova nebo slovní spojení (např. ochranné známky konkurence nebo určité zprávy).

Filtrovat by se měly ovládací prvky ActiveX na webových stránkách, aplety jazyka Java a spustitelné soubory v e-mailech, protože pomocí nich lze v síti nainstalovat trojské koně. Pokud nějaký uživatel potřebuje poslat spustitelný soubor, ať ho pošle jako zazipovaný soubor nebo použije BinHex nebo jiný kodér a pošle ho v textovém formátu. Pak bude obtížné soubor dekódovat, takže se zabrání náhodnému přenesení trojského koně nebo viru do sítě.

Kontrola kompatibility

Při kontrole kompatibility se kontroluje obsah protokolu a ověřuje se, že obsah je pro uvedený protokol smysluplný. Kontrola kompatibility zaručí, že slabiny v zabezpečení v interní síti nebude možné napadnout cíleně zdeformovanými typy obsahu.

Blokování trasy

Pakety na transportní vrstvě nelze směrovat, protože požadavek se opět znovu celý generuje. To vylučuje, aby na transportní vrstvě docházelo k útokům ve formě přímého směrování, fragmentace a dalším různým útokům s odepřením služby. Pokud se deaktivuje směrování, lze také zajistit, že na veřejnou síť nelze povolit protokoly, pro které nebyly ustaveny služby proxy.

Blokování trasy je zřejmě největší výhodou serverů proxy. Protože mezi interní a externí sítí vlastně neputují žádné pakety TCP/IP, je vyloučeno velmi mnoho útoků s odepřením služby a zneužitím chyb v implementaci TCP/IP.

Bohužel, blokování trasy se nevyužívá dostatečně často. Protože pro mnoho protokolů nejsou k dispozici dostatečně kvalitní služby proxy, správci musí často na serveru proxy směrování aktivovat, což úplně vylučuje výhody zabezpečení prostřednictvím odpojení trasy. Pokud je to možné, nepropouštějte síťové pakety na nižší úrovni přes server proxy. Většina softwaru pro servery proxy umožňuje vytvářet generické TCP proxy pro libovolný port např. pomocí proxy SOCKS nebo utility redi r z Unixu. Tyto generické proxy neumí filtrovat obsah, ale i přesto znemožňují přenášení paketů TCP/IP mezi sítěmi.

Zaznamenávání a upozorňování

Poslední výhodou proxy jsou funkce zaznamenávání a upozorňování. Při využití proxy protéká veškerý obsah jediným bodem, takže je k dispozici kontrolní bod pro síťová data. Většina programů pro proxy zaznamenává použití proxy jednotlivými uživateli a lze je nastavit, aby měly k dispozici seznam stránek, které uživatelé navštíví. Vznikne-li podezření, že došlo k nelegální nebo neetické činnosti, je pak u jednotlivých uživatelů možné znovu vyvolat jejich webové relace.

Funkce upozorňování, kterou některé proxy poskytují, může upozornit na probíhající útoky, i když proxy na serveru není obecně řečeno vůči útokům náchylné. Zařízení ale

může upozornit na pokusy o připojení k proxy z externího rozhraní, která hackeři často napadají, když si chtějí „vyprat" svá vlastní připojení.

3 ANALÝZA POUŽÍVANÝCH METOD

Jak už bylo řečeno v předchozích kapitolách, firewally fungují primárně na základě metody paketových filtrů, NAT a proxy. Tato část práce se věnuje jejich analýze. Cílem je porovnat řešení, které nám nabízí dnešní firewally.

Paketové filtry	
Silné stránky	**Slabé Stránky**
Vysoká rychlost zpracování. Nízké hardwarové nároky. Jednoduché a transparentní řešení.	Neumí kontrolovat datovou část paketů. Nižší úroveň zabezpečení než proxy. Bezstavové paketové filtry neuchovávají stav spojení.
Příležitosti	**Hrozby**
Možnost kombinace s dalšími řešeními. Rozšíření důvodů ceny, která je spojená s malými nároky.	TCP lze filtrovat pouze v 0. Segmentu. Filtry povolují a blokují nižší porty. Veřejné služby je nutné propouštět. Filtrování může být potlačeno interními překladači síťových adres.

Tabulka 5: SWOT analýza paketových filtrů

NAT	
Silné stránky	**Slabé Stránky**
Neviditelnost počítače z vnější sítě – zvýšení zabezpečení. Umožňuje připojit více počítačů na jednu veřejnou IP adresu.	Několik protokolů nelze ve spojení s NAT použít.
Příležitosti	**Hrozby**

Další možnost řešení problému nedostatku přidělených veřejných IP adres.	Statické překládání nechrání interní hostitelský počítač. Když klient ustaví připojení, existuje i zpětné připojení. Pokud lze připojení zachytit nebo ho vystavit útoku z pozice prostředníka, pak je prostředník koncovým bodem. Pokud je implementace NAT na firewallu závadná, lze ji napadnout.

Tabulka 6: SWOT analýza NAT

Aplikační proxy	
Silné stránky	**Slabé Stránky**
Skrývají privátní klienty před veřejným vystavením. Mohou blokovat nebezpečné URL. Mohou filtrovat nebezpečný obsah, než ho propustí ke klientským počítačům. Mohou eliminovat směrování na transportní vrstvě mezi sítěmi. Poskytují jediný bod přístupu, řízení a přihlašování.	Vytvářejí jediný bod selhání. Klientský software musí být často nastaven, aby uměl pracovat s proxy. Pro každou službu je nutné mít jeden proxy. Nechrání základní operační systém.
Příležitosti	**Hrozby**
Rozšíření z důvodu vysoké úrovně zabezpečení.	Hrozby spojené s původní konfigurací, která je často nastavená na ideální výkon, nikoliv na nejlepší zabezpečení.

Tabulka 7: SWOT analýza aplikační proxy

II. PRAKTICKÁ ČÁST

4 NÁVRH ŘEŠENÍ ZABEZPEČENÍ SAMOTNÉHO POČÍTAČE

Zabezpečit počítač firewallem v době, kdy je téměř každé PC připojené k internetu je naprostá nutnost. Pro zabezpečení samotného PC máme k dispozici řadu personálních firewallů, které nám po správné instalaci a nastavení zajistí dobrou ochranu před viry a útoky z internetu.

4.1 Výběr vhodného produktu

Jaký si tedy správně vybrat? Já jsem postupoval podle doporučeného návodu a vybral si firewall, který si drží jednu z prvních pozic v žebříčku leak testů. Dalším důvodem byl také fakt, že výrobce nabízí program jako freeware.

Product	Product score	Level reached	Protection level	Recommendation
Online Armor Personal Firewall 3.5.0.14	99%	10+	Excellent	GET IT NOW!
Comodo Internet Security 3.8.65951.477 FREE	96%	10+	Excellent	GET IT NOW!
Outpost Firewall Free 2009 6.5.2724.381.0687.328 FREE	94%	10+	Excellent	GET IT NOW!
Outpost Security Suite Pro 2009 6.5.2514.381.0685	93%	9	Excellent	GET IT NOW!
Jetico Personal Firewall 2.0.2.8.2327	89%	10+	Very good	N/A
Privatefirewall 6.0.20.14	88%	10+	Very good	GET IT NOW!
Malware Defender 2.0.5	87%	10	Very good	GET IT NOW!
PC Tools Firewall Plus 5.0.0.36 FREE	86%	10	Very good	GET IT NOW!
Online Armor Personal Firewall 3.0.0.190 Free FREE	86%	10+	Very good	GET IT NOW!
Netchina S3 2008 3.5.5.1 FREE	85%	9	Very good	N/A
Kaspersky Internet Security 2009 8.0.0.506	83%	9	Very good	GET IT NOW!
ZoneAlarm Pro 8.0.059.000	72%	9	Good	Not recommended
Norton Internet Security 2009 16.2.0.7	66%	8	Good	Not recommended
Webroot Desktop Firewall 5.8.0.25 FREE	54%	7	Poor	Not recommended
BitDefender Internet Security 2009 12.0.12.0	12%	2	None	Not recommended
ZoneAlarm Free Firewall 8.0.298.000 FREE	11%	2	None	Not recommended
CA Internet Security Suite Plus 2009 5.0.0.581	5%	1	None	Not recommended
Sunbelt Personal Firewall 4.6.1861.0	5%	1	None	Not recommended
ThreatFire Free 4.1.0.25 FREE	5%	1	None	Not recommended

Obrázek 10: Žebříček leak testů

Kritériím výběru nejvíce vyhovoval personální firewall, který je součástí programu Comodo Internet Security.

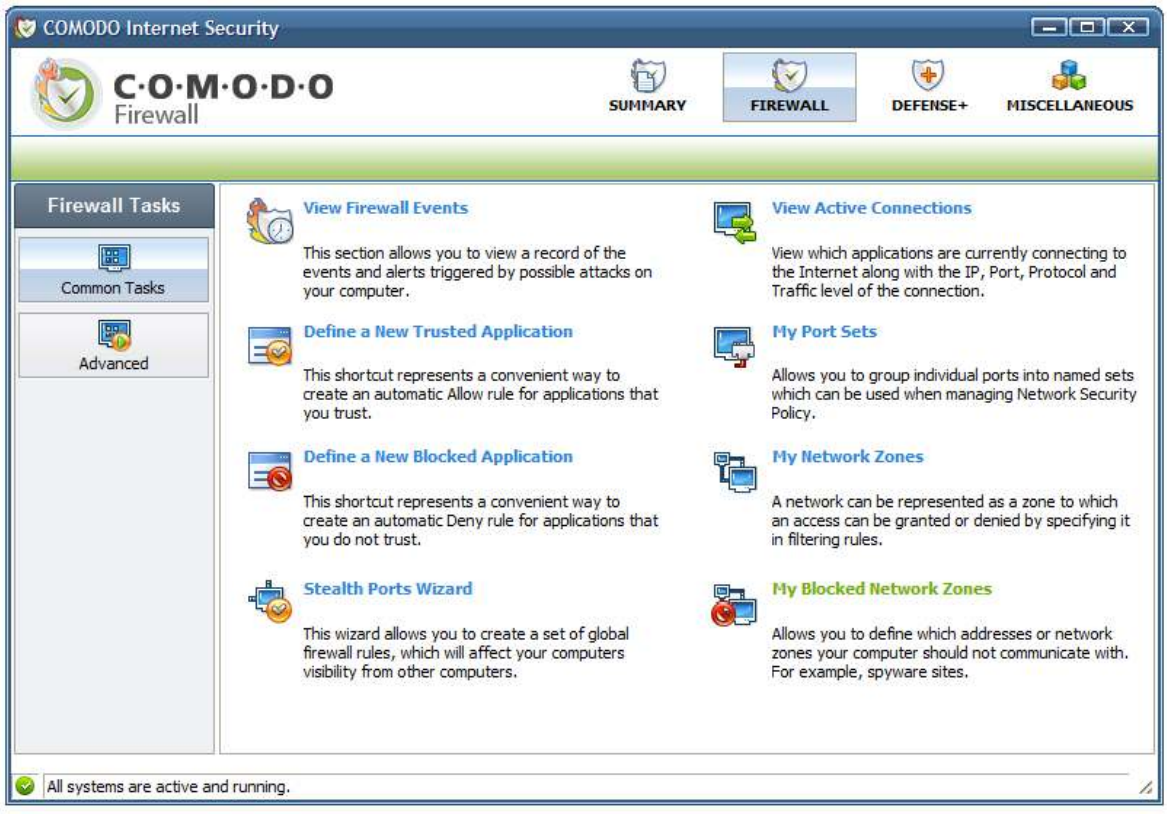
4.2 Instalace, nastavení a popis programu

Program je volně ke stažení na adrese http://www.slunecnice.cz/sw/comodo-internet-security/. Na internetových stránkách www.viry.cz je možné stáhnout českou nápovědu. Po instalaci proběhne automatická aktualizace programu. Dále je nutné restartovat počítač a můžeme nadefinovat chod a pravidla firewallu.

Centrum úloh firewallu umožňuje konfigurovat všechny možnosti nastavení firewallu. Nastavení je rozděleno do dvou sekcí: Panel úloh a Pokročilé úlohy

Panel úloh

Panel úloh umožňuje vytvořit pravidlo pro aplikace a síťová spojení pomocí řady zkratek a průvodců.



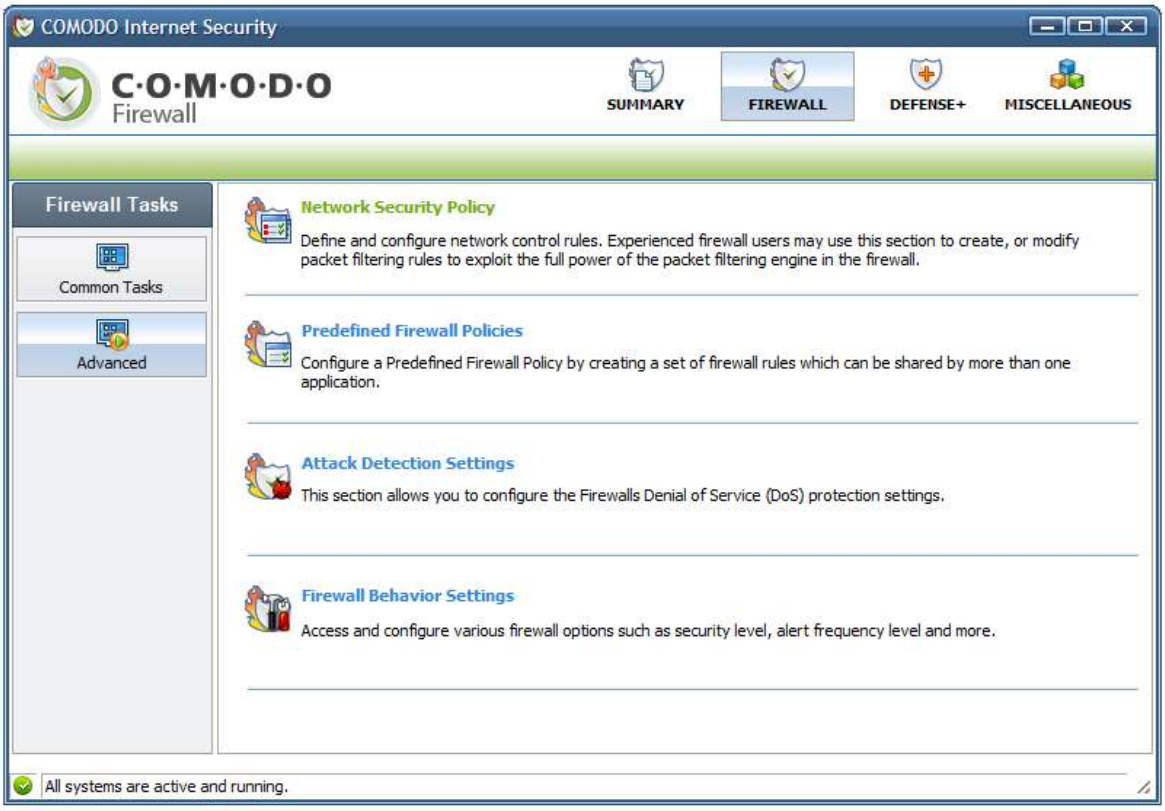
Obrázek 11: Panel úloh Comodo Firewallu

Panel úloh obsahuje:

- Zobrazení záznamů firewallu
- Rozpoznání nové důvěryhodné aplikace
- Rozpoznání nové blokované aplikace

- Průvodce zabezpečením portů
- Zobrazení aktivních spojení
- Nastavení portů
- Síťové zóny
- Blokované síťové zóny

Pokročilé úlohy



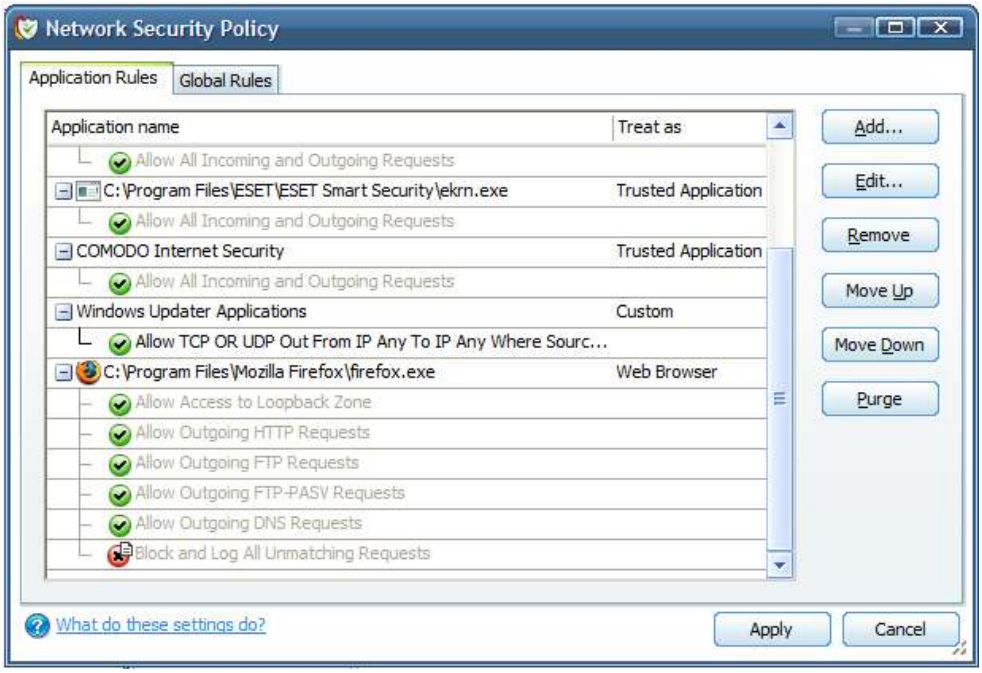
Obrázek 12: Pokročilé úlohy Comodo firewallu

Pokročilé úlohy umožňují zkušeným uživatelům, aby definovali ve firewallu vlastní nastavení všech úrovni. Obsahují:

- Síťová pravidla zabezpečení
- Předdefinovaná pravidla firewallu
- Nastavení detekce útoků

- Nastavení zabezpečení firewallu

Pomocí uvedených nástrojů jsem tedy provedl nastavení funkce firewallu, pravidel, nadefinování aplikací a podobně.



Obrázek 13: Nastavení síťových pravidel zabezpečení

4.3 Testování funkce

4.3.1 Leak testy

Pro testování správné funkce firewallu bývá často využíváno leak testů. Jedná se o malé a jednoduché programy které testují schopnost firewallu zamezovat odchozí komunikaci. Program je nainstalován na počítač a zkouší se spojit s internetovým serverem. Pokud se mu to nepodaří, tak firewall funguje správně. Pro testování firewallů, které jsou uvedeny v této práci, jsem použil program Firewall Leakage Tester v. 1.2.

Obrázek 14: Rozdílné výsledky leak testů

Na obrázků vpravo můžeme vidět výsledek testu před nadefinováním pravidel. Testu se podařilo navázat spojení se serverem grc.com, na kterém je test možné stáhnout. Pokud tedy neprovedeme správné nastavení firewallu, nezaručí nám potřebnou ochranu. Po nastavení všech pravidel byl ale výsledek opačný. Firewall tedy obstál.

4.3.2 Testovací servery

Další možnost testování nabízí internetové testovací servery. Jejich úkolem je zjistit, zda je počítač chráněn před útokem z internetu. Většinou se je o skenování otevřenosti portů. Máme možnost vyhledat celou řadu podobných stránek. Já jsem pro testování použil:

- www.paranoia.cz/test
- www.pcflank.com
- test.bezpecnosti.cz

Port	Služba	Bezpečnostní význam	Stav
21	FTP	Veřejný FTP server. Slouží ke kopírování dat. Hackeři jej často používají ke stahování dat a zakódovaných databází hesel.	Zabezpečeno nebo vypnuto
23	Telnet	Nekódované terminálové spojení --- dá se odposlouchávat. Máte pravděpodobně FIREWALL. Váš správce nechal velkou bezpečnostní díru do systému. Přes terminál se může někdo pokoušet připojit k serveru...	Zabezpečeno nebo vypnuto
25	SMTP pošta	Služba pro příjem pošty. Pokud je špatně nastavena, umožní z vašeho počítače jednoduše udělat zdroj spamů (nevyžádaných e-mailů). Pokud máte poštovní server bez posledních aktualizací, je zde možnost i server ovládnout!	Zabezpečeno nebo vypnuto
80	WWW server	Na vašem počítači, popř. serveru, běží veřejný internetový server. Vaše linka do Internetu je sdílena s uživateli vašich stránek. Pokud není webový server dobře nastaven a aktualizován, lze jej napadnout. Je to hackery nejvíc napadaná služba.	Zabezpečeno nebo vypnuto
110	POP3 pošta	Služba pro stahování pošty. Lze odposlouchávat nebo provést slovníkový útok nebo útok brutální silou, v případě úspěchu má útočník přístup k vaší poště. V případě, že váš účet slouží i ke vzdálenému přístupu k firemní síti, jde o velký bezpečnostní incident.	Zabezpečeno nebo vypnuto

Obrázek 15: Ukázka části testu na test.bezpecnosti.cz

Při všech uvedených testováních byl firewall vyhodnocen jako bezpečný.

4.4 Zhodnocení

Tento produkt hodnotím pozitivně. Instalace a nastavení programu působilo přehledně a bylo srozumitelné. Také provedené zkoušky dopadly dobře. To se ale předpokládalo už při výběru, protože program měl výborné hodnocení v žebříčku leaktestů. Další kladem je jeho free licence, kterou využije celá řada uživatelů PC.

Snad jedinou nevýhodu je fakt, že program není k dispozici v češtině. Jak už ale bylo uvedeno výše, na internetu je volně dostupná česká nápověda.

5 NÁVRH ŘEŠENÍ ZABEZPEČENÍ SÍTĚ MALÉ A STŘEDNÍ FIRMY

Sítě malých a střeních podniků, které obvykle vlastní zhruba desítku až několik desítek počítačů, mají často vyhrazeny počítače pro službu souborů a tiskáren a v mnoha případech vyhrané připojení k internetu. I když firewally vlastní jen poskrovnu malých firem, všechny tyto společnosti by je mít měly. Možná ztráta dat a obchodní produktivity v důsledku vniknutí do sítě ospravedlňuje vynaložení nákladů na jeden počítač navíc a na zakoupení programového vybavení.

Hlavní cíle pro zabezpečení sítě malé a střední firmy tedy jsou:

- Zajistit obranu sítě před hackery, zhroucením, viry a spamy.
- Umožnit bezpečný přístup k nástrojům, které potřebují všichni pracovníci ve firmě.
- Chránit informace o zákaznících, společnosti a dodavatelích.

5.1 Výběr vhodného produktu

Pro zabezpečení sítě malého a středního podniku jsem zvolil Kerio Winroute Firewall 6. Firma Kerio se pohybuje na trhu problematiky firewallů už řadu let a její produkty jsou zpravila hodnoceny velice příznivě. Kerio Winroute Firewall navíc získal certifikát ICSA Labs (uznávaná nezávislá autorita definující standardy kvality produktů pro zabezpečení informací), který vypovídá o jeho kvalitách. Dalším důvodem byl fakt, že Kerio Technologies nabízí třicetidenní zkušební lhůtu na všechny své produkty, takže jsem měl možnost si program bezplatně vyzkoušet a seznámit se s jeho vlastnostmi a možnostmi.

5.2 Instalace, nastavení a popis programu

Zkušební verze Kerio Winroute Firewall 6 je volně ke stažení na adrese http://www.kerio.cz/kwf_firewall.html. Ze stejného zdroje je také možnost si stáhnout manuál k programu, který podrobně popisuje instalaci a nastavení programu pro bezproblémovou funkci. Po stažení programu můžeme přejít k samotné instalaci, ve které je potřeba zadat údaje, které budou dále potřebné pro přihlášení ke správě firewallu.

Komponenty firewallu

WinRoute sestává z následujících tří částí:

- **WinRoute Firewall Engine**

  Vlastní výkonný program, který realizuje všechny služby a funkce. Běží jako služba operačního systému (služba má název *Kerio WinRoute Firewall* a ve výchozím nastavení je spouštěna automaticky pod systémovým účtem).

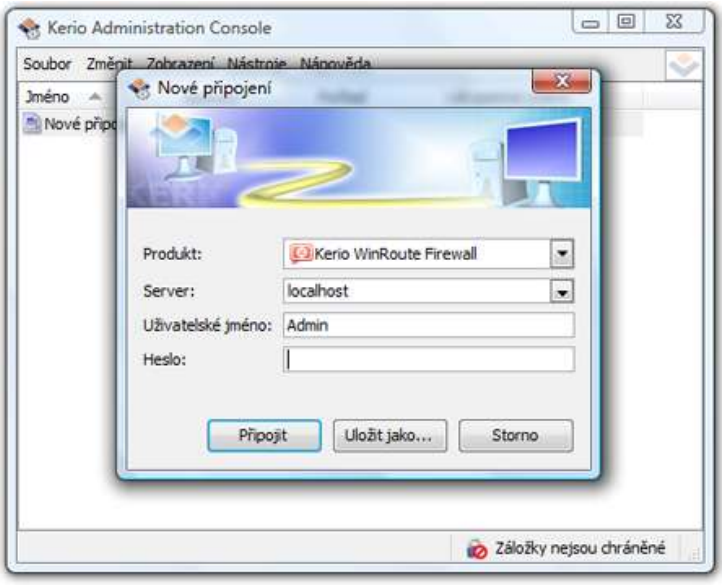
- **WinRoute Engine Monitor**

  Slouží k monitorování a změně stavu Engine (zastaven / spuštěn), nastavení spouštěcích preferencí (tj. zda se má Engine nebo Monitor sám spouštět automaticky při startu systému) a snadnému spuštění administrační konzole.

  Poznámka: WinRoute Firewall Engine je zcela nezávislý na aplikaci WinRoute Engine Monitor. Engine tedy může být spuštěn, i když se na liště právě nezobrazuje ikona.

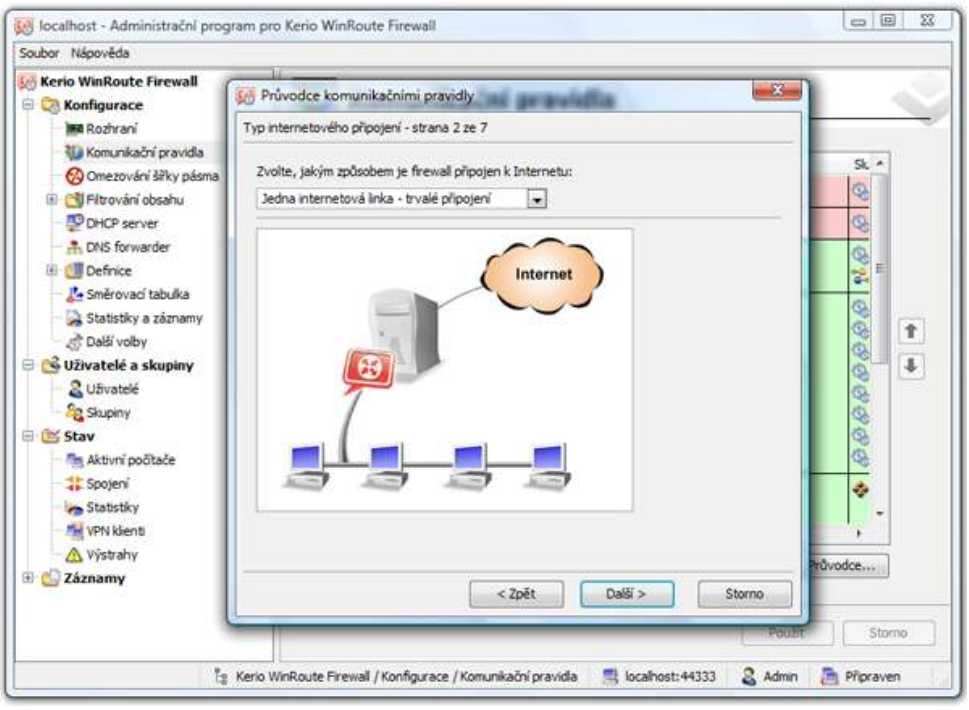
- **Kerio Administration Console**

  Univerzální program pro lokální či vzdálenou správu serverových produktů firmy Kerio Technologies. Pro připojení k určité aplikaci je třeba modul obsahující specifické rozhraní pro tuto aplikaci. Při instalaci WinRoute je Kerio Administration Console nainstalována s příslušným modulem.

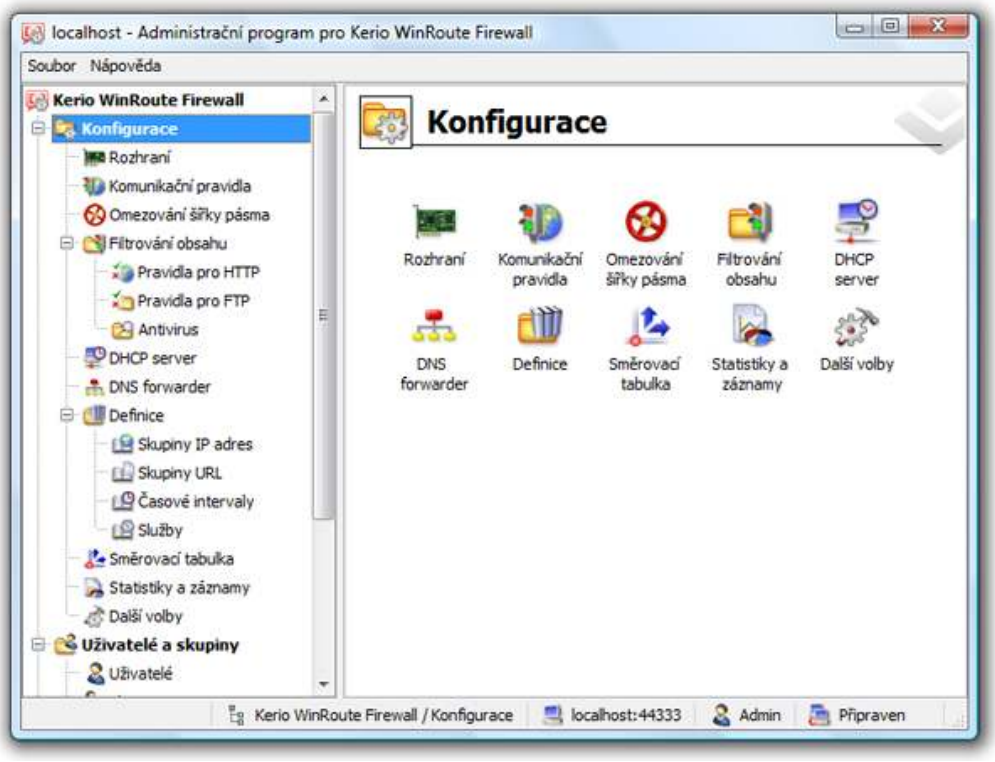


Obrázek 16: Přihlášení do administračního programu

Po prvním spuštění administračního programu můžeme použit průvodce komunikačními pravidly, který nám pomůže jednoduše nastavit všechna potřebná komunikační pravidla.



Obrázek 17: Průvodce komunikačními pravidly Kerio Winroute firewallu



Obrázek 18: Nástroje pro konfiguraci KWF

Nástroje pro konfiguraci KWF:

- **Rozhraní**

  WinRoute je síťový firewall. To znamená, že tvoří bránu mezi dvěma nebo více sítěmi (typicky mezi lokální sítí a Internetem) a obsluhuje komunikaci procházející přes síťová rozhraní (Ethernet, WiFi, vytáčené linky atd.), která jsou do těchto sítí připojena.

  WinRoute v principu pracuje jako IP směrovač nad všemi síťovými rozhraními, která jsou v systému instalována. Základem konfigurace firewallu je proto správné nastavení síťových rozhraní.

- **Komunikační pravidla**

  Komunikační pravidla (Traffic Policy) jsou základem konfigurace. V jediné tabulce je integrováno nastavení zabezpečení, překladu IP adres, zpřístupnění serverů, řízení přístupu lokálních uživatelů do internetu.

- **Omezování šířky pásma**

Modul omezování šířky pásma nabízí řešení nejčastějších problémů s přetížením sdílené internetové linky. Tento modul dokáže rozpoznat spojení, kterými se přenáší velké objemy dat, a vyhradit pro ně určitou část kapacity linky.

- **Filtrování obsahu**

  WinRoute poskytuje velmi rozsáhlé možnosti filtrování komunikace protokoly HTTP a FTP.

- **DHCP server**

  DHCP (Dynamic Host Configuration Protocol) slouží ke snadné konfiguraci TCP/IP na počítačích v síti.

- **DNS server**

  Modul DNS forwarder slouží ve ke zjednodušení konfigurace DNS na počítačích v lokální síti a pro zrychlení odpovědí na opakované DNS dotazy.

- **Definice**

  Obsahuje nastavení pro skupiny IP adres, časové intervaly, služby a skupiny URL

- **Směrovací tabulka**

  Zde lze zobrazit a upravovat směrovací tabulku počítače, na němž je WinRoute nainstalován. Toto je velmi užitečné zejména při odstraňování problémů či úpravě konfigurace na dálku.

- **Statistiky a záznamy**

  Sledování statistik může za určitých okolností zpomalovat činnost programu a rychlost internetového připojení. Tato záložka proto umožňuje nastavit parametry statistik tak, aby byla shromažďována jen taková data a vytvářeny jen takové statistiky, které nás skutečně zajímají.

- **Další volby**

  V této nabídce můžeme nastavit volby, které nelze definovat bezpečnostními pravidly.

Pomocí těchto nástrojů byly nastaveny všechny pravidla a vlastnosti firewallu.

5.3 Testování fuknce

Pro testování Kerio Winroute Firewallu 6 byly použity stejné nástroje jako v předchozím případě. Testovalo se tedy opět pomocí progamu Firewall Leakage Tester v. 1.2 a testovacích serverů, které jsou uvedeny v předchozím návrhu. V obou případech byly testy úspěšné a firewall tedy splnil očekávání.

Port:	Status	Service	Description
21	stealthed	FTP	File Transfer Protocol is used to transfer files between computers
23	stealthed	TELNET	Telnet is used to remotely create a shell (dos prompt)
80	stealthed	HTTP	HTTP web services publish web pages
135	stealthed	RPC	Remote Procedure Call (RPC) is used in client/server applications based on MS Windows operating systems
137	stealthed	NETBIOS Name Service	NetBios is used to share files through your Network Neighborhood
138	stealthed	NETBIOS Datagram Service	NetBios is used to share files through your Network Neighborhood

Obrázek 19: Ukázka části testu na www.pcflank.com

5.4 Zhodnocení

Kerio Winroute Firewallu 6 v prováděných testech uspěl a je tedy podle mě vhodným řešením pro zabezpečení malých a středních firem. Instalace proběhla bez problémů a je přehledná a jednoduchá. Program pro administraci je přehledný a umožňuje snadno nastavit všechna pravidla pro bezproblémovou funkci. Na internetových stránkách výrobce lze navíc stáhnout detailní manuál pro nastavení, který významně usnadňuje konfiguraci. Příjemná je také skutečnost, že je program k dostání v české verzi.

ZÁVĚR

Cílem této bakalářské práce bylo podat čtenáři informace o principu funkce firewallů, možnostech jejich použití a vlastnostech, které jsou důležité z hlediska datové bezpečnosti. Dalším důvodem pro sepsání práce bylo přesvědčit uživatele PC o důležitosti a významu firewallu pro bezpečnost počítačů a sítí.

Pro porozumění principu firewallu je nutné vysvětlil metody, pomocí kterých je dosaženo stanovených cílů. V první části práce jsou proto detailně popsány prvky, které realizují správnou funkci a jejich technologie. Paketové filtry, NAT a služby, které poskytují proxy, jsou základními stavebními kameny firewallování. Pro zajištění požadované bezpečnosti je často nutné uvedené metody kombinovat. Je také důležité uvést jaké mají tato řešení silné stránky a slabiny, aby bylo jasné s jakými hrozbami se můžeme setkat v případě jejich použití. Další část se proto věnuje jejich analýze.

V praktické části je uvedena konkrétní možnost pro zabezpečení dané oblasti a vysvětlen důvod zvoleného řešení. V dnešní době máme možnost si vybrat z obrovského množství nabízených produktů, je proto důležité vědět, jakým způsobem se rozhodnou o optimálním řešení a jaký produkt zvolit. V práci je proto popsáno podle jakých kritérií jsem vybíral já a jaký způsob tedy doporučuji.

Je potřeba vysvětlit, že ani ty nejlepší firewally nám nezaručí dokonalou ochranu před útoky hackerů, viry. Pro nejlepší možné zabezpečení musím být firewally doplněny antivirovými a antispywarovými programy. Dále je nutné udržovat software na počítačích aktualizovaný a stahovat tedy pravidelně nabízené aktualizace , aby bylo možné reagovat na nové hrozby. Toto jsou tedy možnosti, které nám by nám měly přinést optimální zabezpečení pro náš osobní počítač nebo síť.

ZÁVĚR V ANGLIČTINĚ

The aim of this work was to give readers information about the principle functions of firewalls, their use and characteristics that are important in terms of data security. Another reason for the drafting work was to convince PC users on the importance and significance of the firewall for security of computers and networks.

For understanding the principle of the firewall, it is necessary to explain the methods by which it achieved its objectives. In the first part of the work are described in detail the elements that implement proper functionality and technology. Packet filters, NAT, and services provided by proxy, are the building blocks of firewalls. To ensure the safety it is often necessary to combine these methods. It is also important to note what these solutions have strengths and weaknesses, make it clear what threats we can see if their use. Another part is therefore devoted to the analysis.

In the practical part is given a specific option for securing the area and explained the reason for the solution. Today we can choose from a huge quantity of products offered, it is important to know how to decide on the optimal solution and what product to choose. The work is thus described according to what criteria I select and how I therefore recommend.

There is a need to explain that even the best firewalls we guarantee full protection against hacker attacks, viruses. For the best possible security must be accompanied by firewalls and antivirus programs antispywarovými. It is also necessary to maintain the software on computers to download and therefore updated regularly offered updates to respond to new threats. This are the options that we should provide optimum security for our personal computer or network.

SEZNAM POUŽITÉ LITERATURY

[1] STREBE, Matthew, PERKINS, Charles. *Firewally a proxy-servery : Praktický průvodce*. Libor Pácl; Lenka Hendrychová, Jakub Mikuláštík. 1. vyd. Brno : Vydavatelství a nakladatelství Computer Press, 2003. 442 s. ISBN 80-7226-983-6.

[2] THOMAS M., Thomas. *Zabezpečení počítačových sítí bez předchozích znalostí* . Miroslav Hausknecht; David Krásenský. 1. vyd. Brno 635 00 : Computer Press, 2005. 341 s. ISBN 80-251-0417-6.

[3] LOCKHART, Andrew. *Bezpečnost sítí na maximum : 100 tipů a opatření pro okamžité zvýšení bezpečnosti vašeho serveru a sítě.* [s.l.] : Computer Press, 2005. 280 s. ISBN 80-251-0805-8.

[4] *Wikipedie, firewall* [online]. 15.3.2009 [cit. 2009-04-02]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Firewall>.

[5] *Wikipedie, TCP/IP* [online]. 2005 [cit. 2009-04-02]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/TCP/IP>.

[6] *Proactive Security Challenge* [online]. 2008 [cit. 2009-04-05]. Dostupný z WWW: <http://www.matousec.com/projects/proactive-security-challenge/results.php>.

[7] *Internetem bezpečněji* [online]. 2007 [cit. 2009-04-04]. Dostupný z WWW: <http://tutorialy.lupa.cz/jak-zabezpecit-pocitac-s-windows/internetem-bezpecneji/>.

[8] *Bezplatné firewally* [online]. 10.11.2008 [cit. 2009-04-01]. Dostupný z WWW: <http://www.chip.cz/cs/testy/bezplatne-firewally.html>.

[9] *Bezpečnost firewallů - zabezpečení firemních sítí* [online]. 2003 [cit. 2009-04-04]. Dostupný z WWW: <http://www.lupa.cz/clanky/bezpecnost-firewallu-zabezpeceni-firemnich-siti/>.

[10] *Malé a střední firmy Zabezpečení* [online]. 2008 [cit. 2009-02-22]. Dostupný z WWW: <http://www.cisco.com/web/CZ/solutions/smb/security/index.html>.

[11] *Kerio Technologies* [online]. 2007 [cit. 2009-04-20]. Dostupný z WWW: <http://www.kerio.cz/kwf_home.html>.

[12] *Firewally* [online]. 2007 [cit. 2009-05-03]. Dostupný z WWW: <http://www.fi.muni.cz/~kas/p090/referaty/2008-podzim/st/firewally.html>.

[13] *Aplikační firewall se neomezuje na porty a protokoly* [online]. 2008 [cit. 2009-04-23]. Dostupný z WWW: <http://securityworld.cz/securityworld/aplikacni-firewall-se-neomezuje-na-porty-a-protokoly-99>.

[14] *I malou firmu musíme chránit* [online]. 2006 [cit. 2009-04-23]. Dostupný z WWW: <http://securityworld.cz/securityworld/i-malou-firmu-musime-chranit-1211>.

[15] *PC Flank* [online]. 2008 [cit. 2009-05-03]. Dostupný z WWW: <http://www.pcflank.com/scanner1.htm>.

[16] *Test bezpečnosti* [online]. 2008 [cit. 2009-05-03]. Dostupný z WWW: <http://test.bezpecnosti.cz/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IDS	Intrusion detection system
TCP/IP	Transmission Control Protocol/Internet Protocol
NAT	Network Address Translation
SMTP	Simple Mail Transfer Protocol
VPN	Virtual Private Network
URL	Uniform Resource Locator
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
LPR	Line Printer Daemon protocol
NNTP	Network News Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
DNS	Domain Name System
RPC	Remote procedure call
SMB/CIFS	The Server Message Block/ Common Internet File Systém
SMTP	Simple Mail Transfer Protocol
POP	Post Office Protocol
IMAP	Internet Message Access Protocol
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
ISP	Internet service provider
NFS	Net File System
RSH	remote shell

NNTP	Network News Transfer Protocol
LAN	Local Area Network
WAN	Wide Area Network
KWF	Kerio Winroute Firewall

SEZNAM OBRÁZKŮ

SEZNAM TABULEK