Síťová bezpečnost v Microsoft Windows

Network security in Microsoft Windows

Martin Macháč

Bakalářská práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin MACHÁČ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Síťová bezpečnost v Microsoft Windows**

Zásady pro vypracování:

Vypracujte literární rešerši na zadané téma.
Nainstalujte a nakonfigurujte nejméně 3 zvolené softwarové firewally.
Firewally testujte postupně.
Popište možnosti jejich nastavení, funkčnost v plné (placené) verzi a rozdíly mezi verzí poskytovanou zdarma.
Firewally otestujte podle zvolených kritérií, vzájemně je porovnejte.
Navrhněte nejvhodnější firewall pro běžného a zkušeného uživatele. Své doporučení zdůvodněte.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

Košťál, D., Staudek, J.: Firewally, bezpečnostní oddělovací uzly.
Osterloh, H.: TCP/IP – kompletní průvodce. SoftPress, 2003.
Simmons, C., Causey, J.: Mistrovství v sítích Microsoft Windows XP. ComputerPress, 2005.
Dostálek, L.: Velký průvodce protokoly TCP/IP: Bezpečnost. ComputerPress, 2003.

Vedoucí bakalářské práce: **Ing. Martin Sysel, Ph.D.**
Ústav aplikované informatiky

Datum zadání bakalářské práce: **13. února 2007**

Termín odevzdání bakalářské práce: **24. května 2007**

Ve Zlíně dne 13. února 2007

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.
①

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce se zabývá síťovou bezpečností v operačních systémech Microsoft Windows, konkrétně pak se zaměřením na osobní firewally a jejich konfiguraci. Teoretická část pojednává o základních principech počítačové sítě, její skladbě a funkci. Probrána je i bezpečnost počítačových sítí, nejčastější síťové útoky a ochrana proti nim. Praktická část zahrnuje instalaci a nastavení každého firewallu. Všechny firewally jsou také testovány a vzájemně porovnány, a to především s ohledem na zabezpečení počítače.

Klíčová slova: počítačová síť, síťová bezpečnost, osobní firewall, leak-testy

ABSTRACT

This bachelor thesis deals with network security in Microsoft Windows operating systems, specifically personal firewalls and their configuration is highlighted. The theoretical part of this document refers about elementary principles of computer network, its structure and function. The security of computer networks, the most frequent network attacks and protection against them are explained too. The practical part includes installation and settings of each firewall. All the firewalls are also tested and compared each other, especially with respect to the security of computer.

Keywords: the computer network, the network security, the personal firewall, leak-tests

Tímto bych chtěl poděkovat vedoucímu bakalářské práce Ing. Martinu Syslovi, Ph.D., za cenné připomínky a čas, který mi věnoval při přípravě této práce.

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD

Práce na samostatném počítači patří již v dnešní době k základní počítačové gramotnosti a s rozvojem potřeby on-line komunikace se samostatný počítač, nepřipojený do počítačové sítě, stává výrazně omezený z hlediska možného použití. Každý z nás využívá širokých možností sítě Internet, a proto je kladen hlavní důraz na bezpečnost a ochranu dat i celých počítačových sítí. A to nejenom velkých a rozsáhlých systémů, ale i zcela malých, byť by se jednalo pouze o dva mezi sebou propojené počítače se společným přístupem na Internet. Ruku v ruce s rozmachem síťové komunikace se ale bohužel vyvíjí také mechanizmy určené k napadnutí její bezpečnosti. Takzvaní hackeři se k tomu snaží tvořit specializované nástroje se snahou získat důvěrná data nebo si jen sami sobě dokázat, že jsou schopni dané zabezpečení prolomit. Proto je velmi důležité jim tuto činnost maximálně ztížit (ne-li znemožnit) a soustředit se na zkvalitnění bezpečnosti počítačových sítí.

Cílem této práce ale není popsat princip zabezpečení sítí do hloubky. V úvodu práce je čtenář seznámen se základními poznatky, které se bezpečnosti počítačových sítí bezprostředně týkají. Pozornost je věnována především osobním firewallům. Druhá část obsahuje testování pěti předem zvolených firewallů. Podrobně je rozebírána instalace a zvláště pak konfigurace každého firewallu. Produkty jsou zkoušeny také leak-testy, které prověří firewally proti útokům zaměřených na odchozí komunikaci.

Tato práce se snaží nastínit funkce a možnosti daných osobních firewallů, aby bylo možno porovnat jejich kvalitu a úspěšnost ve schopnosti zabezpečit počítač připojený k síti.

I. TEORETICKÁ ČÁST

1 TEORIE POČÍTAČOVÝCH SÍTÍ

1.1 Počítačová síť, komunikace mezi počítači

Počítačové sítě existují již od počátku vzniku výpočetní techniky. Důležitost práce v síti byla zřejmá i v době, kdy se počítače skládaly z vakuových elektronek a vyplňovaly celé místnosti. Definice počítačové sítě se liší podle perspektivy. Síť může představovat způsob získávání a sdílení informací, být prostředkem centrální správy počítačů a uživatelů, umožňovat jednoduchým způsobem komunikaci mezi účastníky nebo i sloužit k zábavě ve formě hraní her po síti a podobně. Je vidět, že přesná a jediná definice počítačové sítě neexistuje. Každý člověk ji vnímá podle svého a využívá k svým vlastním potřebám. Dalo by se tedy říci, že síť je skupina propojených počítačů a používá se ke sdílení informací mezi lidmi a správě prostředků a zabezpečení.

Při vývoji prvních sítí byla komunikace mezi počítači delikátní záležitostí (70. léta). Ve většině případů mohl počítač komunikovat výhradně s jiným počítačem od téhož výrobce. Počítače tedy pracovaly v homogenních sítích. V roce 1978 představil mezinárodní standardizační úřad ISO (International Organization for Standardization) referenční model OSI (Open Systems Interconnection). Pomocí vrstveného přístupu model definuje, jak musí síťový hardware a software fungovat a jak je zapotřebí zpracovávat a řídit data. Díky tomu lze do sítí spojovat počítače od různých výrobců, podmínkou je ovšem dodržení referenčního modelu OSI. Referenční model OSI je obecný model vytvářející obecný rámec pro navrhování a budování počítačových sítí, bez konkrétních mechanismů fungování. Proto je tedy nazýván referenční.

1.2 Síťové protokoly

Počítače v počítačových sítích používají pro vzájemnou komunikaci síťové protokoly. Síťovým protokolem rozumíme soustavu předpisů definující pravidla pro vzájemnou spolupráci dvou sítí. Síťových protokolů existuje celá řada. V Internetu se používají síťové protokoly TCP/IP (Transmission Control Protocol / Internet Protocol), které tvoří rozsáhlou soustavu protokolů. Znalost základních myšlenek TCP/IP je nezbytná pro správné pochopení konfigurace, zavádění a řešení problémů vzniklých v sítích nejen se systémy Microsoft Windows, které tyto protokoly používají.

TCP/IP je v dnešní době standardní sada protokolů určená pro propojení a komunikaci rozlehlých sítí WAN. Byla vyvinuta v roce 1969 americkou agenturou DARPA (Defense Advanced Research Projects Agency) jako výsledek experimentu se sdílením prostředků nazvaného ARPANET (Advanced Research Projects Agency Network). Od osmdesátých let se ARPANET rozrostl do celosvětové společnosti sítí známé jako Internet [1].

1.3 Standardy a normy

Standardy pro TCP/IP jsou zveřejněny v řadě dokumentů nazývaných RFC (Request For Comments). Tyto dokumenty popisují vnitřní stavbu Internetu. Mají formu mnoha technických zpráv, které popisují síťové služby nebo protokoly a jejich implementaci, zatímco ostatní shrnují důležité zásady. TCP/IP standardy jsou vždy uveřejňovány jako dokumenty RFC (ne všechny dokumenty RFC jsou ale standardy, jedná se například o doporučení). Dokumentace RFC je volně přístupná například na www stránkách http://www.faqs.org/rfcs.

TCP/IP standardy byly vyvinuty na základě mnoha dohod, protože dokument určený ke zveřejnění jako RFC může dodat kdokoli. Dokumenty zkontroluje vydavatel RFC a přiřadí jim určený typ. Tento typ potom určuje, zda je dokument pokládán za standard či nikoli. Dokumenty RFC jsou vydávány v chronologickém pořadí. Při publikaci je dokumentu přiřazeno tzv. RFC číslo. Revidované dokumenty nahrazují původní, ale je jim přiřazeno číslo novější.

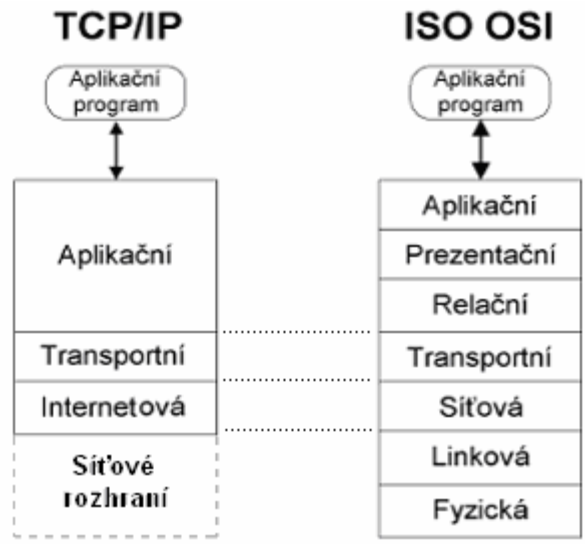
V této práci bude často odkazováno na dokumenty RFC (kupříkladu RFC 2045 a podobně), kde lze nalézt hlubší vysvětlení daného tématu.

Pozn.: Další organizací vydávající normy v oblasti komunikací je ITU (International Telecommunication Union) se sídlem v Ženevě, dříve CCITT (Comité Consultativ International Téléphonique et Télégraphique - nejstarší celosvětová organizace vůbec, založena 1865). Setkat se lze i s normami vydanými organizací IEEE (Institute of Electrical and Electronics Engineers). Běžný uživatel má však přístup pouze k normám RFC, protože ostatní organizace neposkytují své normy zdarma [2].

1.4 Síťové modely

Komunikace mezi počítači je vždy rozdělena do více vrstev. Počet vrstev závisí na tom, jakou soustavu síťových protokolů použijeme. Místo o soustavě síťových protokolů někdy též mluvíme o tzv. síťovém modelu.

Takový síťový model představuje referenční model OSI. V dnešní době se setkáváme s modelem, který používá Internet. Tento model se nazývá rodinou protokolů TCP/IP (někdy též model DARPA) a má v sobě implementovány konkrétní protokoly. Rodina protokolů TCP/IP využívá čtyři vrstvy, referenční model OSI používá vrstev sedm. Každá vrstva modelu TCP/IP odpovídá jedné nebo více vrstvám sedmiúrovňového referenčního modelu OSI.



Obr. 1. Porovnání vrstev síťového modelu TCP/IP a referenčního modelu ISO OSI.

Hlavní odlišnosti mezi oběma modely vyplývají především z rozdílných výchozích předpokladů a postojů jejich tvůrců. Referenční model OSI počítá se soustředěním co možná nejvíce funkcí, včetně zajištění spolehlivosti přenosů, již do komunikační podsítě, která v důsledku toho bude muset být poměrně složitá. Tvůrci protokolů TCP/IP naopak vycházeli z předpokladu, že zajištění spolehlivosti je problémem koncových účastníků komunikace, a mělo by tedy být řešeno až na úrovni transportní vrstvy [3]. Hlavně díky tomuto flexibilnějšímu přístupu se model TCP/IP prosadil v Internetu.

Každá skupina má vlastní definici svých vrstev i protokolů jednotlivých vrstev. Proto jsou protokoly obou síťových modelů obecně nesouměřitelné. Soustavy síťových protokolů

TCP/IP a referenčního modelu OSI jsou tedy vzájemně neporovnatelné. Z obrázku (Obr. 1) je však patrné, že na síťové a transportní vrstvě jsou si velmi blízké[2].

1.4.1 Referenční model OSI

Referenční model OSI využívá hierarchii vrstev. Zadává také, jak musejí položky fungující v jedné vrstvě spolupracovat s položkami v přilehlých vrstvách. Celkově obsahuje tento model sedm oddělených vrstev. Každá definuje, jak musí specifická část komunikace probíhat. Platí, že každá vrstva komunikuje pouze s odpovídající vrstvou na vzdáleném počítači.

Vrstvy referenčního modelu OSI:

Fyzická	Popisuje elektrické či optické signály používané při komunikaci mezi počítači.
Linková	Zajišťuje převod znaků nebo slov počítače na posloupnost bitů a naopak.
Síťová	Zabezpečuje přenos dat mezi vzdálenými počítači WAN.
Transportní	Vytváří transportní spoje, které zajišťují výměnu dat mezi dvěma účastníky síťové komunikace.
Relační	Zabezpečuje výměnu dat mezi aplikacemi.
Prezentační	Je zodpovědná za reprezentaci a zabezpečení dat.
Aplikační	Předepisuje, v jakém formátu a jakým způsobem mají být data přebírána (předávána) od aplikačních programů.

1.4.2 Model TCP/IP

Protokoly TCP/IP jsou založeny na čtyřvrstvém koncepčním modelu známém též jako model DARPA. Rodina síťových protokolů TCP/IP neřeší (až na výjimky) linkovou a fyzickou vrstvu, proto se lze v Internetu setkat s linkovými a fyzickými protokoly referenčního modelu OSI.

1.4.2.1 Vrstva síťového rozhraní

Vrstva síťového rozhraní zodpovídá za předávání TCP/IP paketů síťovému médiu a přijímání TCP/IP paketů z tohoto média. TCP/IP bylo navrženo tak, že je nezávislé na metodě přístupu k síti, použitém formátu rámce a médiu. Tak může být TCP/IP použit při propojování různých typů sítí, včetně technologií LAN a technologií WAN. Nezávislost na určité síťové technologii poskytuje TCP/IP schopnost adaptace na nové technologie, mezi které patří například ATM (Asynchronous Transfer Mode) [1].

Vrstva síťového rozhraní zahrnuje linkovou a fyzickou vrstvu referenčního modelu OSI.

1.4.2.2 Internetová vrstva

Internetová vrstva je zodpovědná za adresaci, balení dat a směrovací funkce. Základním protokolem této vrstvy je IP ve spolupráci s protokoly ARP, RARP, ICMP a IGMP:

- Protokol IP (Internet Protocol) je směrovatelný protokol odpovědný za adresaci, směrování, rozdělování a opětovné skládání paketů.
  IP je definován v RFC 791.
- Protokol ARP (Address Resolution Protocol) je odpovědný za překlad adres internetové vrstvy (IP adres) na adresy pro vrstvu síťového rozhraní, jako jsou hardwarové adresy MAC. Opačnou funkci zajišťuje protokol RARP (Reverse ARP).
  ARP je definován v RFC 826, RARP v RFC 2390.
- Protokol ICMP (Internet Control Message Protocol) je odpovědný za poskytování diagnostických funkcí a hlášení o problémech s doručením IP paketů.
  ICMP je definován v RFC 792.
- Protokol IGMP (Internet Group Management Protocol) je odpovědný za správu skupin pro vícesměrové vysílání. [1]
  IGMP je definován v RFC 2236.

1.4.2.3 Transportní vrstva

Transportní vrstva (nazývaná též transportní vrstva hostitel-hostitel) je jakýmsi jádrem celé soustavy TCP/IP. Zodpovídá za zpřístupnění poskytování komunikačních služeb relací a datagramu.

Hlavními protokoly transportní vrstvy jsou TCP a UDP:

- Protokol TCP (Transmission Control Protocol) poskytuje spolehlivé komunikační služby pro dvoubodové spojení. TCP odpovídá za ustavení TCP spojení, seřazení a potvrzení posílaných paketů a obnovení paketů ztracených během přenosu.
  TCP je definován v RFC 793.
- Protokol UDP (User Datagram Protocol) poskytuje nespolehlivé komunikační služby pro dvou či vícebodové spojení. Rychlost přenosu paketu je vyšší, spolehlivost doručování není ovšem zaručena. [1]
  UDP je definován v RFC 768.

1.4.2.4 Aplikační vrstva

Aplikační vrstva umožňuje aplikacím přístup ke službám jiných vrstev a definuje protokoly používané aplikacemi k výměně dat. Existuje mnoho protokolů aplikační vrstvy. Nejznámější protokoly aplikační vrstvy jsou protokoly používané k výměně uživatelských informací:

- Protokol HTTP (Hyper Text Transfer Protocol) se používá k přenosu souborů tvořících webové stránky na Internetu. Viz RFC 2616.
- Protokol FTP (File Transfer Protocol) se používá k interaktivnímu přenosu souborů. Viz RFC 959.
- Protokol SMTP (Simple Mail Transfer Protocol) se používá k přenosu poštovních zpráv a příloh. Viz RFC 2821.
- Protokol Telnet (Telnet Protocol) emuluje terminál a používá se ke vzdálenému přístupu k hostitelům v sítích. Viz RFC 854.

Navíc používání a správu TCP/IP sítí pomáhají ulehčit tyto protokoly aplikační vrstvy:

- Protokol DNS (Domain Name System) se používá k překladu doménových názvů na konkrétní IP adresy, které se používají k adresaci v Internetu. Viz RFC 1034 a 1035.
- Protokol RIP (Routing Information Protocol) je požíván směrovači k výměně směrovacích informací. Viz RFC 2453.

- Protokol SNMP (Simple Network Management Protocol) se používá mezi konzolí pro správu sítě a síťovými zařízeními (směrovače, mosty, inteligentní rozbočovače) ke sběru a výměně informací o stavu sítě. Viz RFC 1157. [1]

1.4.3 Protokoly TCP/IP

Komponenty TCP/IP jsou sadou vzájemně propojených protokolů, tzv. základních (hlavních) protokolů TCP/IP. Všechny ostatní aplikace a další protokoly v TCP/IP jsou na těchto základních službách poskytovaných protokoly TCP, UDP a IP závislé.

1.4.3.1 TCP

Protokol TCP je spolehlivá doručovací spojovaná služba pro dvoubodové spojení pracující na úrovni transportní vrstvy. Data jsou přenášena v segmentech. „Spojovaná služba“ znamená, že před výměnou dat mezi hostiteli musí být ustaveno spojení. Spolehlivost je dosažena přiřazením pořadového čísla každému přenášenému segmentu, přičemž přijetí všech segmentů dalším hostitelem se ověřuje potvrzením jejich přijetí. U každého odeslaného segmentu musí během určité doby přijímající hostitel vrátit potvrzení přijatých bajtů (ACK). Nedojde-li potvrzení, jsou data přenesena znovu. [1]

1.4.3.2 UDP

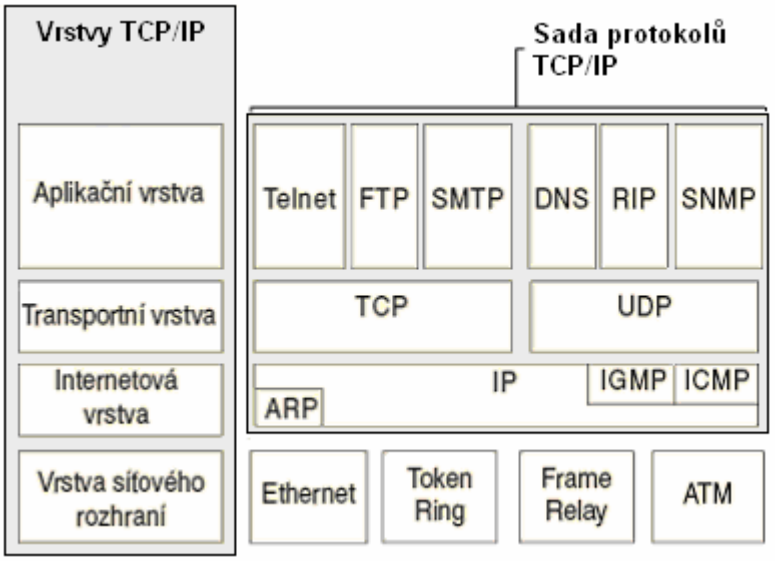
Protokol UDP je jednoduchou alternativou protokolu TCP. UDP je na rozdíl od protokolu TCP nespojovaná služba, tj. že nenavazuje spojení mezi 2 komunikujícími zařízeními. Odesílatel odešle UDP datagramy příjemci a nestará se o jejich úspěšné dodání ani o správné pořadí doručených paketů. O to se musí postarat protokoly vyšších vrstev. UDP se používá v případě, že aplikace nebo protokoly v horní vrstvě zaručují spolehlivé doručení, v případě nežádoucího ustavení nákladného TCP spojení nebo při přenosu pouze malého množství dat (využívají jej například datagramové služby NetBIOS a SNMP).

1.4.3.3 IP

Protokol IP je nespojovaný, nespolehlivý datagramový protokol pracující na úrovni internetové vrstvy. Není tedy garantováno doručení paketů. Registrace doručených paketů a obnova ztracených paketů náleží protokolu ve vyšší vrstvě, například TCP. Od nadřazených protokolů transportní vrstvy obdrží IP datové segmenty s požadavkem na odeslání. K nim připojí vlastní hlavičku a vytvoří tak IP-datagram. Každý datagram ve

svém záhlaví nese mimo jiné IP adresu příjemce, čili síť může přenášet každý IP-datagram samostatně. Ty tak mohou k adresátovi dorazit v jiném pořadí než byly odeslány [2].

V hlavičce jsou uloženy kromě cílové adrese také informace, jako jsou zdrojová IP adresa, protokol, kontrolní součet CRC (Cyclic Redundancy Check) a jiné.



Obr. 2. Sada protokolů síťového modelu TCP/IP.

1.4.3.4 Porty

Adresování na úrovni transportní vrstvy (protokoly TCP a UDP) tvoří kombinace IP adresy daného počítače a portu. Tato kombinace je nazývána socket. Port je číslo z intervalu 1-65536, používané pro identifikaci služeb (a jejich prostřednictvím aplikací) na určitém počítači. Na jednom počítači může běžet více aplikací současně. Každá aplikace je pak jednoznačně identifikována číslem portu. Není možné, aby stejný port používalo několik aplikací. Pro přidělování čísel portu platí závazná pravidla původně vypracována organizací IANA (Internet Assigned Numbers Authority). Od března roku 2001 je touto funkcí pověřena organizace ICANN (Internet Corporation for Assigned Names and Numbers).

Porty jsou rozděleny do tří skupin. Pro nejběžnější služby jsou vyhrazené porty v rozsahu 0-1023, označované jako „well known ports“ (dobře známé porty). Porty v rozsahu 1024-49151 by měly být registrovány organizací ICANN. Ostatní porty (49152-65535) jsou přidělovány dynamicky a náhodně a jsou určeny pro soukromé využití. IP adresa klienta a jeho port tvoří spolu s IP adresou a portem serveru tzv. pár socketů. Pár socketů je spojení

mezi dvěma koncovými procesy (aplikacemi) a jednoznačně tak identifikuje komunikaci mezi dvěma zařízeními.

UDP porty jsou odlišné a oddělené od TCP portů, i když některé z nich používají stejná čísla. Přehled nejčastěji používaných portů je uveden v příloze P I. Úplný seznam přiřazených TCP a UDP portů je k nalezení například na internetových stránkách organizace IANA http://www.iana.org/assignments/port-numbers.

2 SÍŤOVÁ BEZPEČNOST

2.1 Bezpečnost počítačových sítí

Bezpečnost počítačových sítí a aplikací je v současnosti jedním z nejdiskutovanějších problémů. V dnešní době, kdy je internet využíván jako hlavní komunikační prostředek pro přenosy dat i k obchodním transakcím, je stále důležitější data a jejich přenosy maximálně zabezpečit. Bezpečnost sítě má mnoho stránek a různých úhlů pohledu. V prvé řadě záleží na tom, jakým potenciálním útokům a hrozbám je síť vystavena.

2.2 Typy útoků

Útoků na počítače v sítích, respektive v Internetu, existuje v dnešní době nepřeberné množství. Samotné útoky mohou být vedeny na hardware, na software i jinými způsoby. Mezi dobře známé a hojně využívané typy útoků na stanice běžných uživatelů patří falšování IP adres, odposlech paketů a útoky s odepřením služeb.

2.2.1 Falšování IP adres (IP spoofing)

Tento typ útoku znamená, že útočník (zvaný hacker) zfalšuje zdrojovou IP adresu a nastaví ji na jinou. Vezme tak na sebe totožnost důvěryhodného hostitele, který s cílovou stanicí komunikuje bez vzbuzení jakéhokoliv podezření. Změněná IP adresa je často volena z lokální sítě LAN, ve které pracuje počítač oběti, a proto se k útočníkovi nemusí dostat odpovědi z cílového systému. Nezjistí tak, zda byl úspěšný či nikoliv. Může však zvolený počítač určitým způsobem napadnout.

2.2.2 Odposlech paketů (Packet sniffing)

Nástroje pro odposlech paketů zachycují pakety, které v síti procházejí místem jejich připojení. Tyto nástroje (Sniffers) mohou být jak softwarové tak hardwarové na specializovaném počítači. Dokonalejší typy odposlechových nástrojů umí i dekódovat data z paketů, což lze využít k dalšímu postupu útoku. Útočník musí být při odposlechu „napíchnutý“ do sledované sítě. Takovéto nebezpečí vzniká především v bezdrátových sítích. [4]

2.2.3 Útoky s odepřením služeb (Denial of Services)

Jedná se o nebezpečné a v dnešní době hojně používané typy útoků, které dovolují zahltit linku oběti, i když má větší kapacitu než vaše linka. Tyto útoky se snaží znepřístupnit určitou službu, počítač, nebo dokonce síť [5]. Základním principem je přetížení sítě množstvím požadavků a docílení zpomalení provozu na síti nebo jeho úplného zastavení. Může dojít i k velkému vytížení systému napadeného počítače a následně k jeho havárii.

Útoky s odepřením služeb (neboli DoS útoky) můžeme dělit podle mnoha parametrů. Jsou to například útoky lokální a vzdálené. Lokální DoS útok znamená, že pro provedení tohoto útoku musíme mít přístup k počítači, na který chceme útočit. To, že chyba umožňuje vzdálený útok, znamená, že není potřeba mít přístup k počítači, na který útočíme, ale můžeme jej napadnout vzdáleně [5]. DDoS je zkratka pro distribuované DoS útoky, což znamená, že se útoku účastní více počítačů současně. Tyto útoky jsou v poslední době na vzestupu. Reflektivní a záplavové útoky se snaží zahltit linku, při zesilujících útocích zase útočník rozesílá data o určité velikosti a k oběti přicházejí data o velikosti větší (pakety ICMP - příkaz ping, pakety TCP s příznakem SYN, IP pakety se změněnou hodnotou TTL a podobně).

DoS útoky jsou ve své podstatě jednoduché, ovšem patří k jedním z nejnebezpečnějších. Je to dáno tím, že tyto útoky zneužívají provoz, který se na sítích běžně vyskytuje. Proto je obrana proti této technologii obtížná.

2.3 Ochrana a její druhy

V současné době, kdy je používání Internetu běžnou záležitostí pro každého, musí uživatel připojený k síti klást vysoký důraz na bezpečnost. Stále rostoucí množství útoků v rámci počítačových sítí, a to jak z vnějšku, tak i z vnitřního síťového prostředí, zvyšuje nároky na zabezpečení.

2.3.1 Překlad síťových adres

Překlad síťových adres - NAT (Network Address Translation), se zavádí a provozuje na vhodném zařízení umístěném mezi vnitřní sítí s privátními IP adresami a vnějším Internetem s veřejnými IP adresami. Zmíněné zařízení pak provádí překlady mezi těmito adresami. Kromě toho, že NAT pomáhá řešit nedostatek veřejných IP adres ve vnitřních sítích (mapuje více privátních IP adres na jednu veřejnou), patří také k základní úrovni

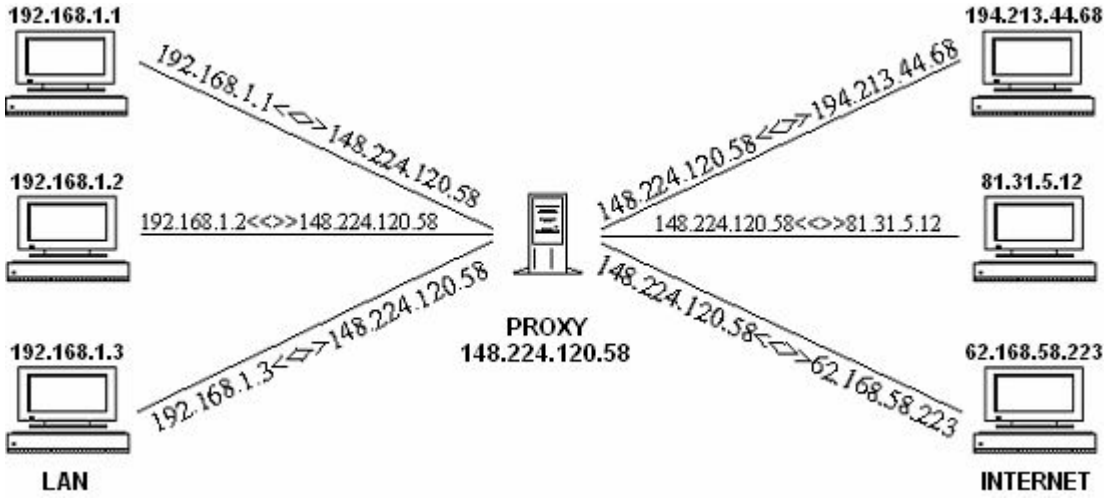
zabezpečení sítě. NAT útočníkovi velmi výrazně ztěžuje například zjištění počtu provozovaných systémů v síti, mapování topologie cílové sítě, vedení různých útoků typu DoS a podobně.

NAT může být různorodý podle způsobu převodu - SNAT (statický), DNAT (dynamický), NAPT (překlad síťové adresy a portu), PAT (překlad pouze adresy portu) atd. NAT je definován v RFC 1631.

2.3.2 Proxy

Proxy je program, který pracuje na aplikační úrovni. Skládá se ze dvou částí. Na jedné straně pracuje jako server a na druhé straně jako klient. Serverová část proxy přijímá požadavky od klientů a předává je klientské části proxy, která jménem původního klienta předává požadavky na originální server [6]. Počítače klientů tedy ve skutečnosti posílají své požadavky na IP adresu proxy, ta je následně nasměruje na požadovanou cílovou IP adresu. Pro cílový server je klientem proxy server a nikoliv původní klient. To má za následek, že cílovému serveru není známa IP adresa původního klienta. Zejména u webových proxy ale toto opatření není stoprocentní, protože některé z nich adresu klienta přidávají do upraveného požadavku.

Za pomocí proxy lze i analyzovat obsah komunikace a zjišťovat přítomnost například virů. Dále může procházející požadavky také šifrovat a dešifrovat. Proxy se používá zejména na rozhraní dvou sítí, kde se chová jako oddělovač. Může se jednat jak o hardwarový, tak i softwarový produkt.



Obr. 3. Příklad jednoduché proxy.

2.3.3 IDS (Intrusion Detection System)

IDS sleduje datové toky a hledá v nich pokusy o útok na konkrétní aplikace. Jedná se o pasivní zařízení, které provoz sítě pouze sleduje, ale nezasahuje. Prostřednictvím upozornění (alertů) a statistik poskytuje obsluze informace o útocích.

2.3.4 IPS (Intrusion Prevention System)

IPS nejen detekuje pokusy o útok, ale zároveň je schopno dle nastavené konfigurace aktivně reagovat a útoku zabránit. To znamená, že zařízení IPS umí nejen analyzovat datový tok až na aplikační vrstvu, ale musí umět datový tok patřičně modifikovat. Takové zařízení se instaluje přímo do cesty datového toku. [7]

2.3.5 Inspekce paketů

Různé druhy ochrany v sítích jsou založeny na pozorování paketů síťového provozu. Jsou to zejména filtrování paketů a stavová inspekce paketů.

2.3.5.1 Filtrace paketů

Filtrování paketů (Packet filtering) je jedním z nejstarších a zároveň nejběžnějších typů dostupných technologií pro inspekci paketů pohybujících se v sítích. Paketové filtry tvoří často první obrannou linii a kombinují se s jinými technologiemi ochrany sítě. Dnes jejich nejběžnější implementaci představují takzvané přístupové seznamy, které pracují ve směrovačích na obvodu sítě. Filtrací rozumíme kontrolu procházejících paketů síťovým zařízením a následné rozhodnutí na základě jejich obsahu a definovaných pravidel, může-li být paket puštěn dále nebo ne. Samotný filtr nemění na rozdíl od jiných technologií obsah datových parketů.

Filtrování paketů není samo o sobě nijak kvalitním mechanismem zabezpečení, jako jedna z vrstev zabezpečení má ale svůj smysl.

2.3.5.2 Stavová inspekce paketů

Stavová inspekce paketů (Statefull packet inspection) je pokročilejší metoda inspekce paketů a pracuje ve většině případů na firewallu, který je umístěn hned za směrovačem při vstupu do sítě. Ve spolupráci s filtrováním paketů na směrovači se už získá hodnotně zabezpečená síť. Mechanismus stavové inspekce paketů se spustí s prvními pakety, které

zahajují komunikaci ve spojení. Při inspekci spojení se vytvoří záznam a další pakety se propustí jen tehdy, pokud náleží k již povolenému, existujícímu spojení (jako například odpověď na dotaz).

2.3.6 Firewall

Termínem firewall označujeme zařízení (nebo na něm pracující software), jímž je oddělena lokální síť od Internetu. Chrání PC nebo LAN především před přístupem z Internetu. Firewallů a jejich funkcí je velké množství. Základní dělení firewallů je na hardwarové a softwarové. Další dělení podle toho, jak firewall pracuje, je dělení na paketové filtry, stavové filtry a aplikační brány. Jiné dělení (podle oblasti, kterou má firewall chránit) je na osobní a síťové firewally, popřípadě podle toho, na které vrstvě síťového modelu pracuje a podobně.

2.3.6.1 Osobní firewall

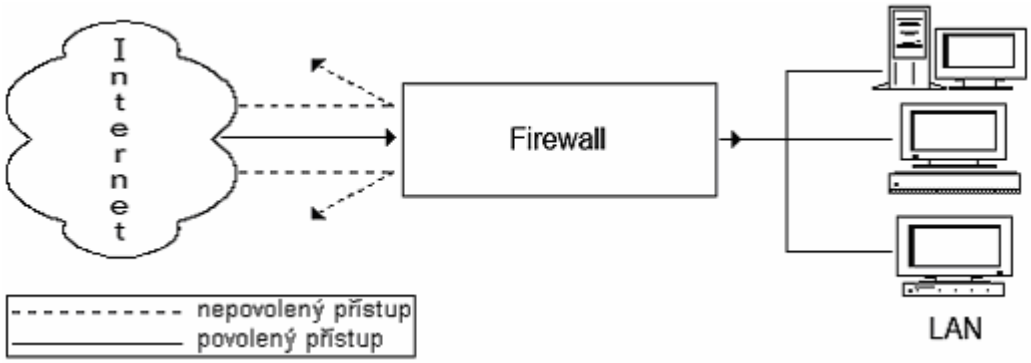
Pro běžné uživatele bývají nejdostupnější softwarové osobní firewally (Personal firewalls). Hlavní úlohou firewallu jako programu je zabránění cílenému útoku na konkrétní počítač či síť. Neexistuje totiž jen nebezpečí, které vyplývá z napadení viry a nejrůznějším spywarem, za které si ve velkém měřítku mohou sami uživatelé. Hrozí také mnohem větší nebezpečí přímého napadení a posléze i ovládnutí daného počítače připojeného na síť.

Firewall se usadí na nejnižší vrstvě operačního systému a zkoumá všechen síťový provoz. Jak na Internetu, tak také po místní síti LAN. Jestliže nějaká aplikace chce s někým navázat kontakt, firewall to oznámí (zobrazí název aplikace, kam volá, po jakém portu a protokolu) a dá na výběr akci. Uživatel to pak může povolit nebo zakázat [8], popřípadě nadefinovat pravidlo, aby tuto volbu provedl příště firewall automaticky. Firewall také zkoumá všechny pakety, které přicházejí z Internetu. Navíc zabraňuje útočníkům získat kontrolu nad počítačem tím, že ošetřuje některé známé chyby v programech. Firewall není schopen prohlížet obsah paketů na vyšších vrstvách. Mnoho moderních útoků probíhá na aplikační vrstvě. Firewall jim tedy nemůže zabránit. V takových případech je potřeba nasadit jiný typ ochrany, jako je IDS nebo IPS.

Jako vždy v oblasti bezpečnosti, tak i tady platí, že prostředek je jedna věc, ale jeho nastavení a používání věc druhá a zpravidla rozhodující [9]. Nesprávně nakonfigurovaný nebo nedostatečně vybavený firewall může být v některých případech dokonce horší, než kdybychom neměli firewall vůbec žádný.

Základem firewallu bývá NAT. Kromě toho většinou zvládá filtrování paketů TCP/IP, povolování služeb (otevírání portů TCP/IP), chová se jako proxy server a jiné funkce. Některé navíc disponují i dalšími službami, jako je blokování reklamních oken, antivirová a antispywarová ochrana a podobně. Jednoduchý firewall by měl síťový provoz řídit následujícím způsobem (není-li explicitně určeno uživatelem jinak):

- do lokální sítě nevpouštět žádné pakety přicházející z Internetu
- dovolit navázat spojení z LAN do Internetu
- přichází-li z Internetu odpověď vyvolaná dříve navázaným spojením (z LAN ven), tuto odpověď vpustit



Obr. 4. Schéma funkce firewallu.

Osobních firewallů lze na Internetu nalézt hned několik, většinou je výrobci nabízejí zdarma jako „odlehčenou“ variantu svých dalších produktů, a můžete je využít pro osobní potřebu, tj. domácí použití. Osobní firewally nalézají uplatnění zpravidla v domácnostech uživatelů rozličné počítačové gramotnosti. Protože se tím pádem nejedná o produkt zaměřený na úzkou cílovou skupinu, měl by nabízet funkce pro všechny - jednoduchou obsluhu a intuitivní nastavení pravidel pro uživatele nepříliš znalé, pokročilou skupinu pak uspokojí detailním nastavením portů, protokolů, důvěryhodných počítačů a podobně. V tomto směru hraje nemalou roli také nápověda, která by kromě popisu nastavení měla přiblížit i technologické pozadí firewallů [10].

II. PRAKTICKÁ ČÁST

3 ZPŮSOB TESTOVÁNÍ

Každý uživatel si může nejen na Internetu otestovat svůj osobní firewall pomocí různých nástrojů k tomu určených. Existuje řada možností, jak provést kontrolu konfigurace firewallu a jeho úspěšnosti v ochraně počítače. Důležitou vizitkou každého firewallu je i náročnost jeho ovládání, přívětivost k uživateli nebo míra zatížení systému.

3.1 Test otevřenosti portů

K základním mechanismům patří ověření otevřenosti portů, které zkoumá napadnutelnost počítače z Internetu. Kontrolují se především porty nejpoužívanějších a nejzneužívanějších služeb, jako například ftp, telnet, smtp, pop3, www a jiné. Tento způsob vzdáleně otestuje, je-li příslušný port otevřen (a tím pádem i napadnutelný) nebo znepřístupněn.

Testování otevřenosti portů může přinést ale zkreslené nebo nepravdivé výsledky. Pokud je IP adresa, která se kontroluje, veřejná (tj. viditelná z Internetu), test ukáže skutečný výsledek. Problém nastává v tom případě, když je IP adresa testovaného počítače skrytá za routerem nebo firewallem poskytovatele internetového připojení (například díky službě NAT nebo proxy). Takovýchto případů se obecně vyskytuje velké množství, nevyjímaje provozu níže testovaných firewallů. Proto kontrolu otevřenosti portů při použití příslušných firewallů tato práce neobsahuje.

3.2 Leak-testy

Další velmi významnou pomůckou pro testování osobního firewallu jsou takzvané Leak-testy. To jsou malé, neškodné programky vytvořené odborníky přes síťovou bezpečnost. Tyto programy se snaží obejít režii firewallu a to každý odlišným způsobem. Leak-testy prověřují zdatnost firewallu detekovat neoprávněnou odchozí komunikaci do Internetu a tím napomáhají odhalit napadnutelnost počítače „zevnitř“ (kupříkladu nevědomé odesílání důvěrných informací trojskými koni, sledování stisků kláves a podobně).

Leak-testů existuje velké množství. K nalezení jsou například na internetových stránkách http://www.matousec.com a http://www.firewallleaktester.com. K testování firewallu bylo vybráno 20 leak-testů:

- AWFT Atelier Web Firewall Tester obsahuje 6 různých efektivních leak-testů a hodnotí výsledek testu maximálním skóre 10 bodů. Používá

mechanismů jako jsou DLL (Dynamic Link Library) injekce, procesní injekce nebo paměťové substituce.

- BITStester — Pokusí se využít BITS (Background Intelligent Transfer Service) služby systému Windows XP ke stažení souboru ze vzdáleného serveru.
- Breakout — Zneužívá zprávy systému Windows k ovládnutí internetového prohlížeče. Maximální skóre jsou 2 body (test prohlížeče Internet Explorer a jeho zneužití pomocí Windows Active Desktop).
- Coat — Pomocí substituce o sobě mění informace a poté se snaží navázat internetové spojení.
- CopyCat — Používá konkrétní službu Windows API (Advanced Program Interface) k převzetí kontroly nad vláknem procesu, který je povolen v nastavení firewallu.
- CPIL — Comodo Parent Injection Leak testovací souprava obsahuje 3 testy k obelhání firewallu pomocí manipulace se spouštěcím souborem prohlížeče explorer.exe. Maximální skóre je tedy 3.
- DNStester — Zkouší využít Windows DNS API a odeslat DNS požadavek na Internet.
- FireHole — Tento test se pokusí o procesní injekci internetového prohlížeče.
- FPR — Fake Protection Revealer pomáhá odhalit falešnou anti-leakovou ochranu firewallu. Tímto způsobem se dá zjistit, zda firewall nedává uživateli zdánlivý pocit bezpečí.
- Ghost — Snaží ze zmást firewall tím, že restartuje svůj proces a tím i svůj identifikátor (PID).
- Jumper — Pokusí se infikovat soubor prohlížeče svým vlastním kódem a po násilném restartu prohlížeče se načte do systému a zkusí odeslat informace na Internet.
- LeakTest — Jeden z nejstarších leak-testů, který zaměňuje název spuštěného procesu.

- OSfwbypass Zkusí načíst HTML stránku s Java skriptem, který přesměruje prohlížeč na vzdálený server.
- PCAudit Klasicky infikuje ve firewallu povolený proces DLL injekcí čímž zajistí přístup k Internetu bez vzbuzení pozornosti.
- PCFlank Pomocí OLE (Object Linking and Embedding) mechanizmů zkusí ovládnout běžící vlákna prohlížeče.
- Runner Zkusí nabourat integritu spouštěcího souboru prohlížeče.
- Surfer Vytvoří skrytou plochu a spustí na ní prohlížeč. Pak použije DDE (Direct Data Exchange) k ovládnutí jeho chování.
- TooLeaky Spustí skrytě prohlížeč s parametry příkazového řádku.
- WallBreaker Obsahuje 4 samostatné testy. Jejich cílem je různými způsoby spustit originál nebo kopii spouštěcího souboru prohlížeče.
- Yalta Pošle specifický UDP paket na konkrétní IP adresu a port, které firewally často propouštějí (DNS služby a podobně).

3.3 Zatížení systému

V neposlední řadě je také dobré znát systémové nároky firewallu a jeho kompatibilitu s provozovaným operačním systémem. Zatížení systému a spotřeba systémových prostředků již není takovým problémem, protože dnešní hardwarové vybavení osobních počítačů je už na vysoké úrovni a poskytuje dostatečné prostředky k bezproblémovému provozu firewallu. Je ale užitečné mít o takových informacích přehled, a proto jsou také součástí této práce. Důležitá je také technická a uživatelská podpora každého produktu, jako jsou aktualizace, opravné záplaty, rozšíření programu, komplexní nápověda, online výpomoc nebo diskusní fóra. I tyto aspekty budou zhodnoceny u každého produktu.

V dnešní době podporují osobní firewally nejrozšířenější operační systémy, což jsou Microsoft Windows a také linuxové distribuce. Všechny testované firewally byly provozovány na sestavě s čistou instalací operačního systému Microsoft Windows XP Professional s aktualizací Service Pack 2 (SP2).

4 TESTOVÁNÍ FIREWALLŮ

Po dohodě s vedoucím této práce byly k testování a porovnání zvoleny následující firewally:

- ZoneAlarm Pro (verze 7.0.302.000)
- Sunbelt Kerio Personal Firewall (verze 4.3.635.0)
- Outpost Firewall Pro (verze 4.0.1007.7323)
- Comodo Firewall Pro (verze 2.4.18.184)
- Brána firewall systému Windows

Tyto produkty patří k nejpoužívanějším v kategorii osobních firewallů. Instalovány byly komerční verze těchto firewallů, které ovšem slouží uživateli po omezenou dobu (několik dní na vyzkoušení). Po uplynutí této lhůty je zpravidla požadována registrace a zaplacení licence k dalšímu provozování firewallu. Není-li toto učiněno, firewall nelze nadále používat anebo jsou znepřístupněny některé jeho původní funkce. Přesnější změny mezi verzemi popřípadě jejich omezení budou popsány samostatně u každého firewallu.

Ke srovnání také otestuji bránu firewall systému Windows. Tento mechanismus je jednoduchý a funguje na základě filtrace paketů. Ve srovnání bude patrný velký rozdíl oproti zbylým čtyřem firewallům, nicméně tento produkt je určen k základnímu zabezpečení sítě v operačním systému Windows XP a je k němu zdarma dostupný. Brána firewall systému Windows byla ovšem při používání ostatních firewallů deaktivována.

4.1 ZoneAlarm Pro

K testování byl použit ZoneAlarm Pro verze 7.0.302.000.

Testovaná verze byla vydána 15. ledna 2007.

4.1.1 O produktu

Americká společnost ZoneLabs (http://www.zonelabs.com), která vyvíjí řadu zabezpečovacích programů pro obchodní organizace i pro soukromé použití, patří na trhu internetové bezpečnosti ke světové špičce. Ze svých produktů nabízí nejen produkty zaměřené na firewallovou ochranu, ale i samostatné aplikace zaměřující se na virovou, spywarovou nebo komunikační bezpečnost.

Vizitkou společnosti ZoneLabs je řada ocenění, která obdržela za vynikající výsledky při testování jejich produktů nezávislými organizacemi v USA i v Evropě.

4.1.2 Instalace

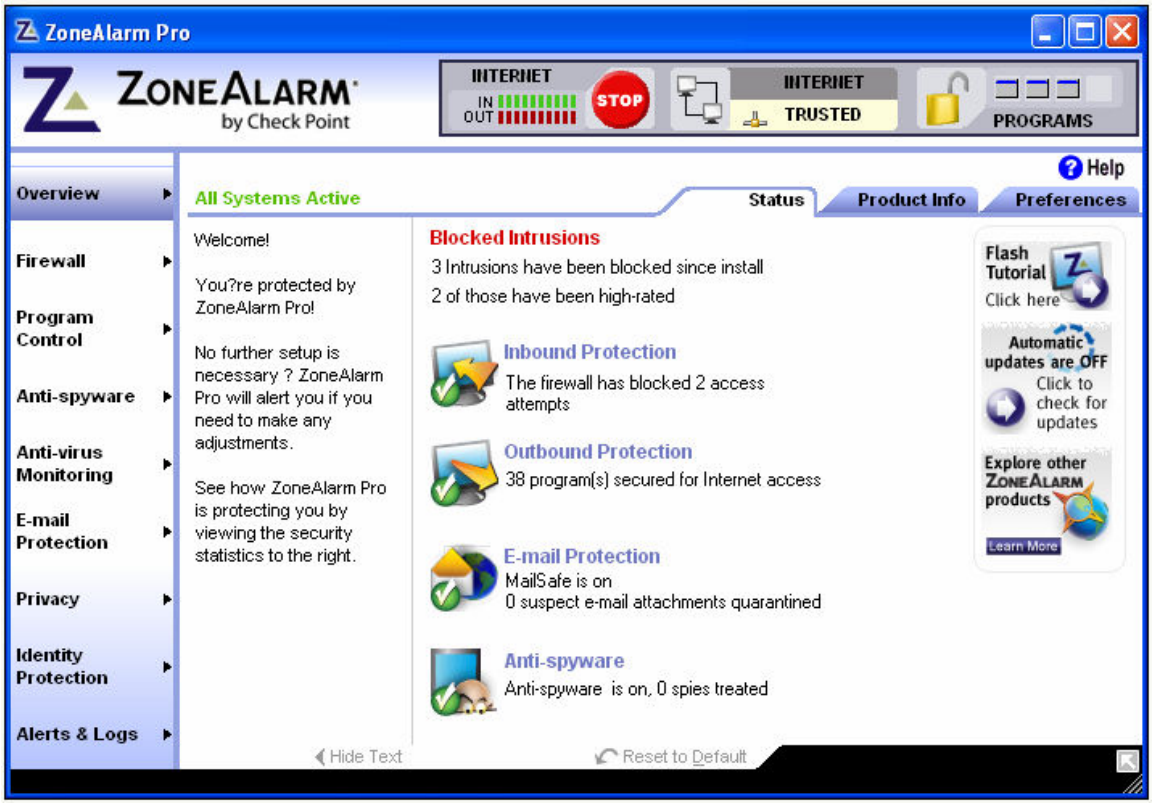
Vlastní instalace programu je velmi rychlá a snadná, řešená grafickým konfiguračním průvodcem. Jazykem instalace je Angličtina. Pomocí dotazů sleduje průvodce v pár krocích uživatelovy volby a sám se přitom automaticky nastavuje podle jeho odpovědí. Po krátkém nepovinném dotazníku týkajícího se zkušeností uživatele s nežádoucím softwarem se průvodce ptá pouze na nastavení manuálního nebo automatického rozhodování o programech zachycených firewallem. O tom rozhoduje zabudovaný rádce SmartDefense Advisor. Je také možnost začlenit se do společnosti DefenseNet uživatelů ZoneAlarmu a sdílet své bezpečnostní zkušenosti pro lepší boj s internetovými útočníky. Také je nabízena kontrola systému k identifikaci standardních procesů přistupujících k Internetu a jejich začlenění do pravidel firewallu.

4.1.3 Vzhled a konfigurace

Ihned po instalaci programu a nutného restartu počítače je tento automaticky chráněn. To je signalizováno ikonou ZoneAlarmu Pro v taskbaru. Ikona může měnit svoji podobu podle toho, co právě firewall provádí. Informuje tak o provozu ZoneAlarmu.

Při prvním spuštění je žádoucí zadat heslo pro zabezpečení firewallu. Pak je chráněn kompletně celý program před změnami jeho nastavení a funkcí od případného útočníka.

ZoneAlarm Pro je na první pohled přehledný a uživatelsky příjemný program. Grafické uživatelské rozhraní (GUI - Graphical User Interface) působí přehledně a texty jsou zobrazovány v anglickém jazyce. Úvodní obrazovka obsahuje menu s kartami základních komponent firewallu umístěné na levé straně okna. Nahoře se nachází přehledná lišta, kde je vidět síťový provoz, programy momentálně připojené k Internetu a tlačítko STOP, kterým je možno okamžitě zastavit veškerý síťový provoz. Celé okno lze skrýt a nechat tak zobrazit jen kompaktní lištu. Nechybí ani ikona nápovědy.



Obr. 5. Vzhled uživatelského rozhraní ZoneAlarmu Pro.

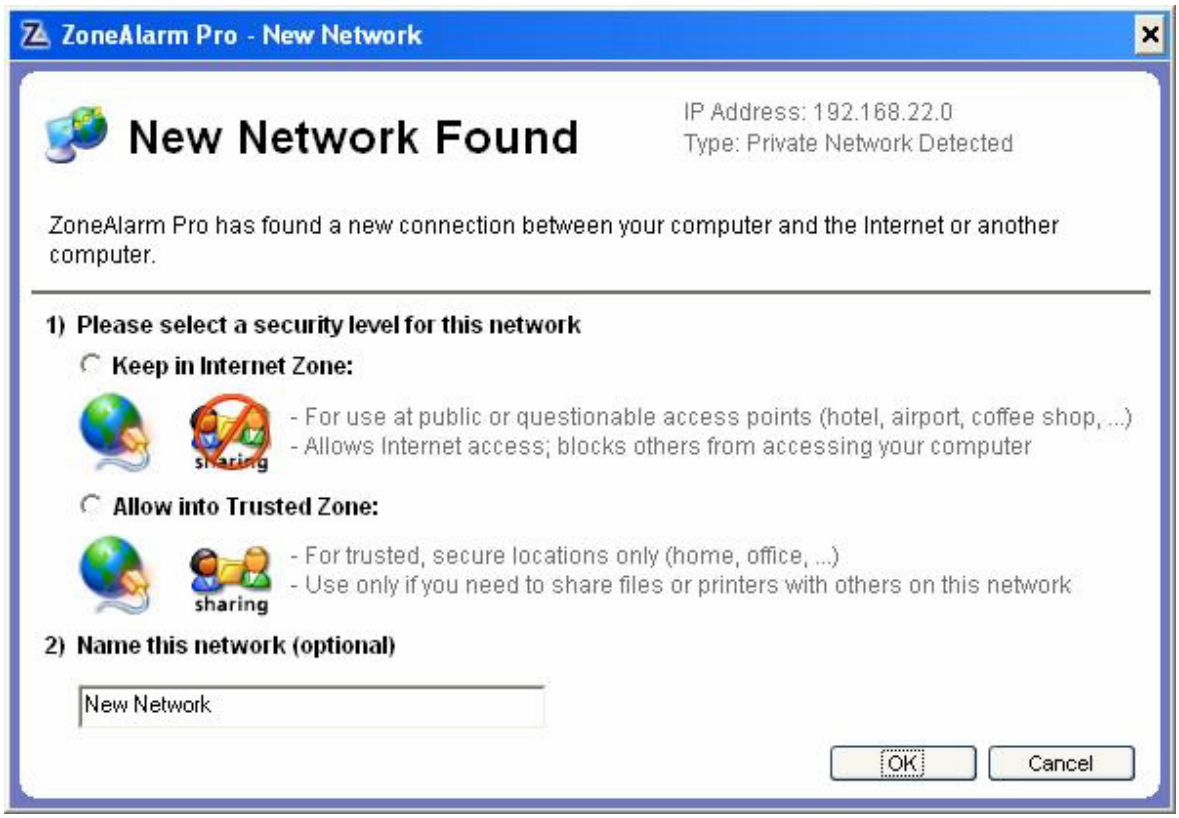
Každá karta z postranního menu zobrazuje po kliknutí příslušné informace a své nastavení v okně. Pomocí záložek lze ještě přepínat mezi podkategoriemi dané karty. Kliknutím na titulek *Reset to Default* přidělíme příslušné kartě standardní nastavení.

Karta první (*Overview*) zobrazuje statistiku již uplynulého firewallového provozu. Je také vidět, která z komponent je aktivní. Na zbylých záložkách jsou k dispozici údaje o produktu a také základní nastavení. To je například aktualizace firewallu, změna vzhledu, administrátorské heslo, záloha nastavení programu nebo možnost aktivace proxy.

Karta *Firewall* je velmi důležitá, protože se zde nastavuje citlivost a chování firewallové ochrany. ZoneAlarm Pro klasifikuje počítače nebo sítě, s nimiž je navázáno spojení, podle zóny, ve které je zařazen. Standardně jsou to 3 zóny. *Internet Zone* (internetová) je „neznámá“. Všechny stanice a sítě na Internetu patří do této zóny. *Trusted Zone* (důvěryhodná) je bezpečná zóna a obsahuje počítače a sítě, které určí uživatel za důvěrné a spolehlivé. Jen v této zóně je povoleno sdílení prostředků s jinými počítači. V *Blocked Zone* (blokující) jsou umístěny nedůvěryhodné nebo nebezpečné počítače a sítě. S nimi je komunikace zakázána.

Zóny *Trusted* a *Internet* lze nastavit na 2 úrovně zabezpečení - *High* (vysoká) a *Medium* (střední). Při vysoké úrovni zabezpečení je počítač ve skrytém režimu a je tak na Internetu neviditelný. Sdílení prostředků je zakázáno. Povoleno je pouze odchozí DNS, odchozí DHCP a broadcast (všesměrové vysílání v daném segmentu sítě), takže je možno surfovat Internetem. Toto nastavení je doporučeno pro *Internet Zone*. Při střední úrovni zabezpečení ZoneAlarm Pro poznává komponenty nejčastěji komunikujících programů a zapamatovává si tyto údaje. Sdílení souborů a tiskáren je umožněno a všechny protokoly a porty jsou povoleny. Počítač je viditelný z Internetu - tato úroveň zabezpečení je proto doporučena jen pro *Trusted Zone*.

Na záložce *Zones* jsou zobrazeny sítě a jejich zařazení. Při identifikaci nové sítě nabídne ZoneAlarm Pro možnost začlenit ji do jedné ze zón. Mezi přiřazenými zónami lze poté libovolně přepínat.



Obr. 6. Upozornění při rozpoznání nové sítě.

Každé zóně lze samozřejmě manuálně upřesnit nastavení o povolení/blokování provozu. Pro detailní nastavení slouží záložka *Expert*, kde je možnost povolení nebo blokování uživatelsky definované komunikace (zdroj spojení, cíl spojení, použitý protokol a port, konkrétní čas komunikace, její priorita atd.).

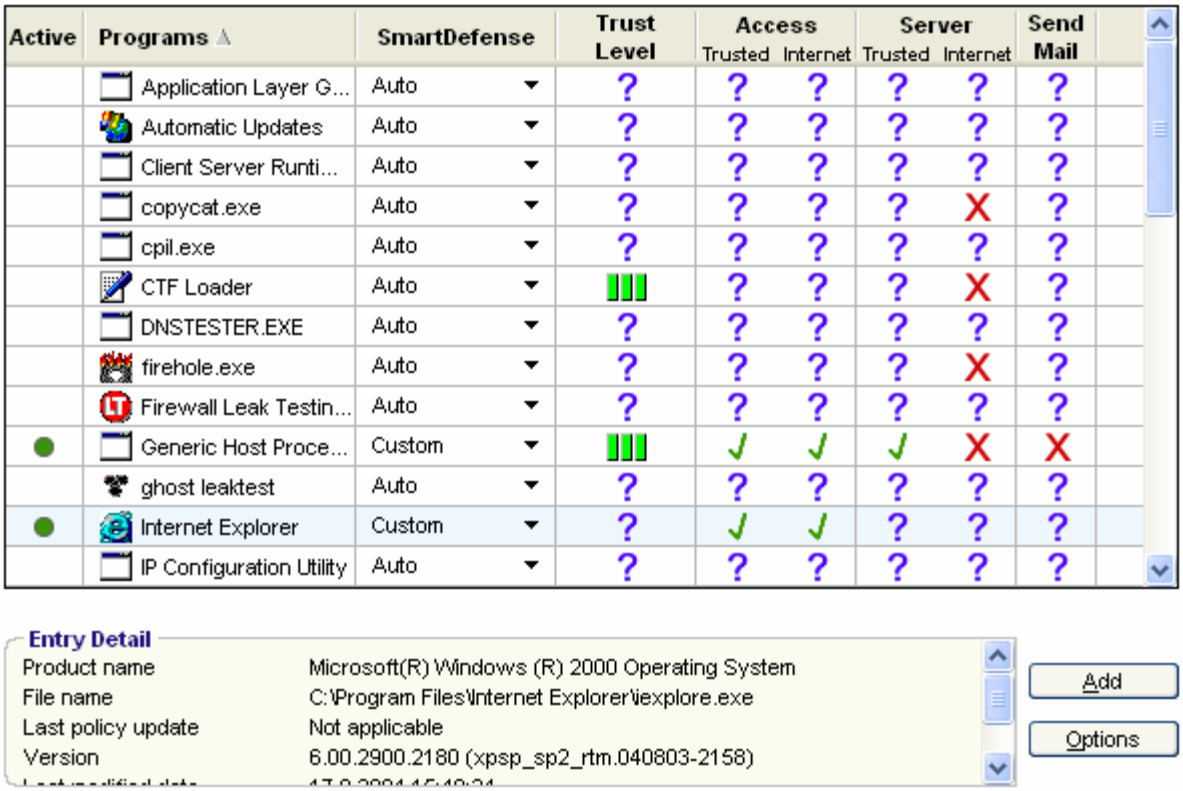
Karta *Program Control* je neméně důležitou součástí firewallu. Na tomto místě se nastavuje především citlivost kontroly programů (*High*, *Medium*, *Low*, *Off*) a firewallový rádce SmartDefense Advisor (*Auto*, *Manual*, *Off*). V rámci programové kontroly lze aktivovat i pokročilou kontrolu programů, kontrolu interakcí aplikací, kontrolu komponent programů a OSfirewall protekci (hlídání nastavení operačního systému). Při zapnutí některých z těchto funkcí ovšem bude firewall zasypávat uživatele mnoha převážně zbytečnými upozorněními a dotazy pro povolení daných komunikací. Proto je standardně přednastavený *Medium* režim. Díky němu se musí programy ptát pro povolení síťové komunikace, pokročilé detekce jsou ovšem deaktivovány, v provozu je jen OSfirewall.

SmartDefense Advisor je původně nastaven na automat. Sám tak rozhoduje (podle porovnání s online databází) o povolení či blokování programů. V režimu manuál musí uživatel sám vyhodnocovat situace, Advisor mu však zobrazuje svá doporučení.

V rozšířené volbě se nastavuje defaultní chování programů (povolit, zakázat, ptát se) při automatické režii firewallu.

Na záložce *Programs* se navíc můžou měnit a upřesňovat práva programů pro přístup. Pole *Access* znamená, že program může přistupovat z počítače ven. Pole *Server* znamená povolení přístupu zvenčí na počítač. To vše lze nastavit pro *Trusted* i *Internet* zónu. Hodnota *Trust Level* udává míru přístupových práv programu. Pozorovatelný je i stav *SmartDefense Advisoru* pro každou aplikaci (*Auto*, *Custom*) a to, provozuje-li právě aplikace nějakou síťovou komunikaci (vyjádřeno symbolem zeleného puntíku).

Záložka *Components* obsahuje seznam programových komponent. Programové komponenty jsou soubory, jejichž obsah je běžně využíván jinými aplikacemi, které je načítají do své paměti. V tom případě získají komponenty tytéž práva jako aplikace, jíž jsou součástí.



Obr. 7. Nastavení pravidel jednotlivým programům.

Karta *Anti-spyware* informuje o spyware protekci. Lze také přímo zkontrolovat systém na škodlivé objekty, popřípadě nastavit automatickou léčbu. Karta *Anti-virus Monitoring* pouze monitoruje přítomnost a stav antivirového programu nainstalovaného v počítači. Karta *E-mail Protection* zajišťuje pomocí technologie MailSafe ochranu proti virům v příchozích (a)nebo odchozích e-mailových zprávách. Podporované protokoly jsou http, pop3 (příchozí), smtp (odchozí) a imap4. Kontrolují se i e-mailové přílohy.

Karta *Privacy* umožňuje nastavit blokování různorodých cookies, webových reklam, vyskakujících popup oken nebo nebezpečných skriptů (Java, ActiveX a podobně). Záložka *Site List* pak ukazuje přehledný seznam rozpoznaných webových serverů a nastavení jejich práv. Jednotlivým serverům lze tak upravit konkrétní pravidla.

Na kartě *Identity Protection* můžeme po zadání osobních informací nastavit úroveň zabezpečení pro jejich přenos Internetem. Jsou to kupříkladu jméno, adresa, telefon, e-mail, ale i různá hesla, čísla bankovních účtů nebo licenční kódy. Tuto ochranu zajišťuje technologie MyVAULT.

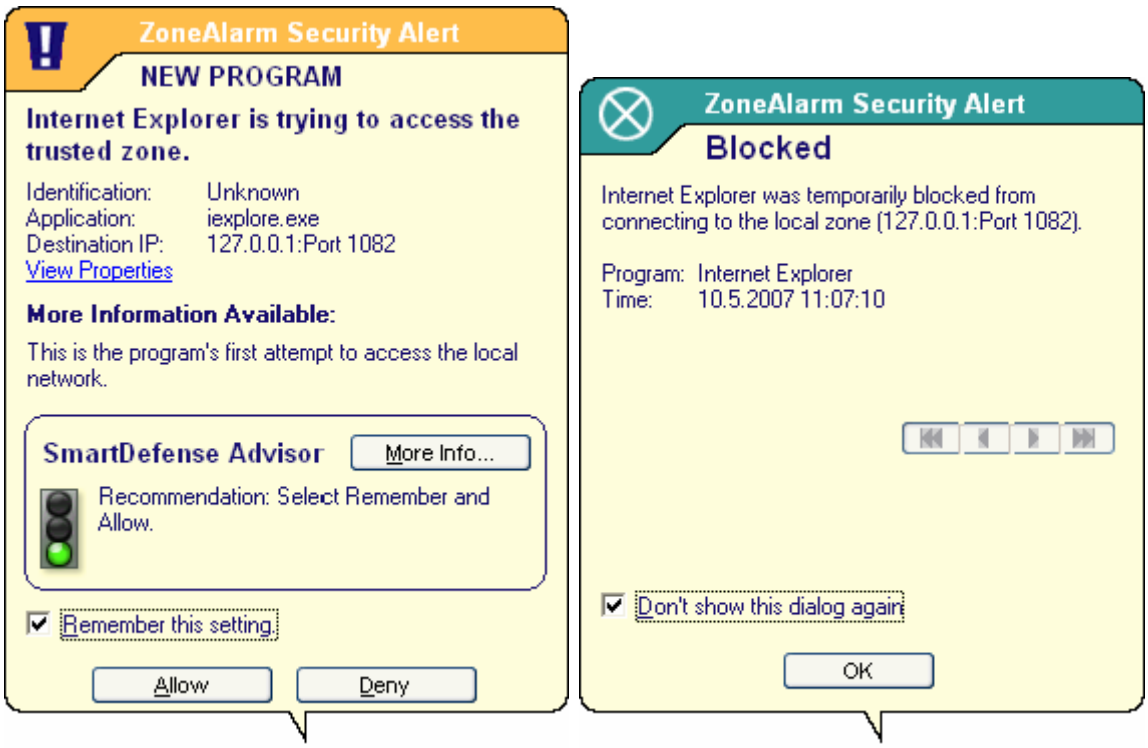
Pod kartou *Alerts & Logs* jsou k dispozici nastavení pro programová upozornění (alerty) a pro archivaci firewallového provozu (logy). Tady je možno definovat množství a druhy

zobrazovaných alertů a prohlížet si již proběhlé události. Celý log se ukládá do textového souboru na disku pro pozdější potřebu.

4.1.4 Běh programu

Pokud je nastaven firewall na manuální režim, bude se ptát, zda má každému konkrétnímu programu povolit přístup do sítě či povolit přístup ze sítě na takový program. Vždy se zobrazí popup okno (alert) s informacemi o tom, jaký program hodlá přistupovat a kam (na jakou IP adresu a port) hodlá přistupovat. Uživatel může akci povolit volbou Allow nebo zakázat volbou Deny. Zatržítkem lze firewallu určit, že si má tuto odpověď pamatovat a příště se již nedotazovat. Pokud je SmartDefense Advisor aktivní, zobrazuje doporučený postup.

Upozornění mohou být vyvolána v souvislosti s firewallovou i programovou ochranou.



Obr. 8. Upozornění při detekci a zablokování programu.

Firewall lze přes kontextové menu ze systémové lišty uvést i do tzv. herního módu (Game mode) a nastavit jej tak, aby povolil nebo blokoval veškerou komunikaci bez upozorňování. To se využívá například při hraní on-line her.

4.1.5 Výsledky leak-testů

Testování firewallu leak zkouškami bylo prováděno dvakrát - pro standardní nastavení a pro konfiguraci s vysokou citlivostí. ZoneAlarm Pro dopadl v tomto testu zejména s citlivým nastavením výborně. Zjištěné skutečnosti jsou uvedeny v tabulkách (Tab. 4, Tab. 5) v závěrečném souhrnu všech firewallů.

4.1.6 Rozdíly mezi verzemi

Po vypršení 15-ti denní lhůty na vyzkoušení je nutno zakoupit licenci pro pokračování provozování ZoneAlarmu Pro (cena licence na 1 rok je 39.95 $). Nestane-li se tak, provoz programu je zastaven. Alternativou je pořízení verze ZoneAlarm, která je zdarma dostupná pro osobní využití. Tím ovšem zaniknou některé důležité funkce původního programu. Přehled změn je uveden v tabulce (Tab. 1).

Tab. 1. Srovnání komerční a neplacené verze ZoneAlarmu.

ZoneAlarm Pro	**ZoneAlarm**
firewall + Expert nastavení	firewall
programová kontrola + SmartDefense Advisor	omezená programová kontrola
OSfirewall	-
ochrana soukromí	-
ochrana identity	-
e-mailová kontrola	omezená kontrola e-mailů
anti-spyware	-
anti-virus monitoring	anti-virus monitoring

Součástí ZoneAlarmu Pro je velmi podrobná nápověda s možností vyhledávání, rejstříkem a slovníkem pojmů. Pro základní seznámení s firewallem je k dispozici animovaný tutoriál přístupný z hlavního okna programu. Online podpora je také dostupná, a to v Angličtině, Francouzštině, Němčině a Španělštině. Zajímavé postřehy ostatních uživatelů ZoneAlarmu lze objevit především na on-line diskusním fóru http://forums.zonealarm.com.

Více informací o programu ZoneAlarm Pro je k nalezení na oficiálních www stránkách produktu http://www.zonealarm.com a na internetovém blogu http://blog.zonealarm.com.

4.2 Sunbelt Kerio Personal Firewall

K testování byl použit Sunbelt Kerio personal firewall verze 4.3.635.0.

Testovaná verze byla vydána v 21.února 2007.

4.2.1 O produktu

Společnost Kerio Technologies (http://www.kerio.com) obohacuje trh se softwarovými nástroji na zabezpečení internetové komunikace již od roku 1997. Tato společnost sídlí v USA a má pobočky ve Velké Británii a České republice. Prvním komerčním firewallem byl WinRoute Pro, který byl později nahrazen Kerio WinRoute Firewallem. V roce 2002 byl vydán Kerio Personal Firewall, což je osobní firewall určený pro širokou veřejnost. V prosinci roku 2005 přebrala vývoj tohoto firewallu společnost Sunbelt Software (http://www.sunbelt-software.com) a produkt byl přejmenován na Sunbelt Kerio Personal Firewall. Americká společnost Sunbelt Software byla založena v roce 1994 a jejím hlavním cílem byla zpočátku anti-spamová a anti-spywarová ochrana. Převedením osobního firewallu se okruh působnosti v síťovém zabezpečení společnosti Sunbelt Software ještě rozšířil.

4.2.2 Instalace

Instalace programu je prováděna pomocí grafického průvodce a celá se odehrává v Angličtině. Průběh instalace je zcela jednoduchý, rychlý a bezproblémový. Po uvítací obrazovce se objeví okno s licenční smlouvou, kterou je nutné před pokračováním instalace odsouhlasit. Následuje výběr adresáře na disku, kam se má celý program nainstalovat. Posledním krokem je výběr základního chování firewallu. K dispozici je volba *Simple (No popup mode)*, což je výchozí nastavení pro většinu uživatel a představuje mód firewallu bez dotazování uživatele (veškerá odchozí komunikace je povolena, veškerá příchozí blokována). Alternativou je položka *Advanced (Learning mode)* doporučená pro zkušenější uživatele. V tomto módu se firewall při pokusu neznámé aplikace o síťovou komunikaci dotáže uživatele, zda ji může povolit anebo blokovat. Výběr jedné z možností

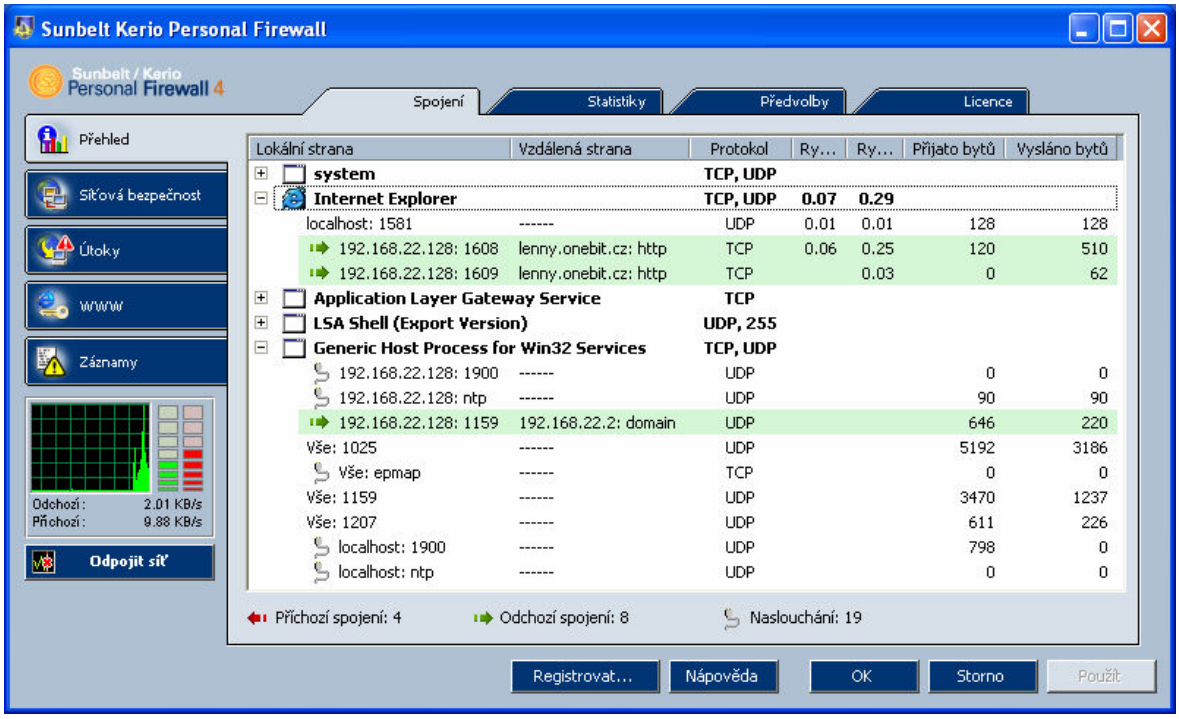
lze později změnit v samotném programu. Po tomto kroku vyzve průvodce k restartu počítače, aby jej bylo možno začít chránit firewallem.

Po znovunačtení operačního systému nastala situace, kdy programové služby běžely na pozadí, nicméně žádným způsobem se nedalo zobrazit uživatelské rozhraní firewallu. Na Internetu se tento problém řešil v několika diskuzích. Po jejich prostudování se manuálně nastavilo spuštění programu do příkazu *Po spuštění* v systému Windows a tím se problém podařilo odstranit.

4.2.3 Vzhled a konfigurace

Základem je grafické uživatelské rozhraní s podporou českého jazyka. Orientace je velmi snadná a intuitivní. GUI je tvořeno centrálním oknem s hlavním menu na levé straně. Každá karta z menu má dostupné podrobnější nastavení v listech, které jsou umístěny nad celým oknem. Pod hlavním menu se zobrazuje přehledná statistika příchozí a odchozí síťové komunikace ve formě grafu. Tlačítko *Odpojit síť* slouží k okamžitému zastavení síťového provozu.

Základní karta po zobrazení GUI je *Přehled*. Její první list *Spojení* obsahuje seznam aktuálně připojených procesů. Rozbalením daného procesu se zobrazí podrobnosti o jeho komunikaci.



Obr. 9. Uživatelské rozhraní Sunbelt Kerio Personal Firewallu.

Na listu *Statistiky* jsou přehledně shrnuty souhrnné informace o blokování všech událostí, které je schopen firewall detekovat. Přes list *Předvolby* je k dispozici nejzákladnější nastavení programu, jako je ochrana konfigurace heslem, vzdálená správa počítače, import a export nastavení firewallu nebo výběr jazyka. List *Licence* obsahuje detaily o licenci.

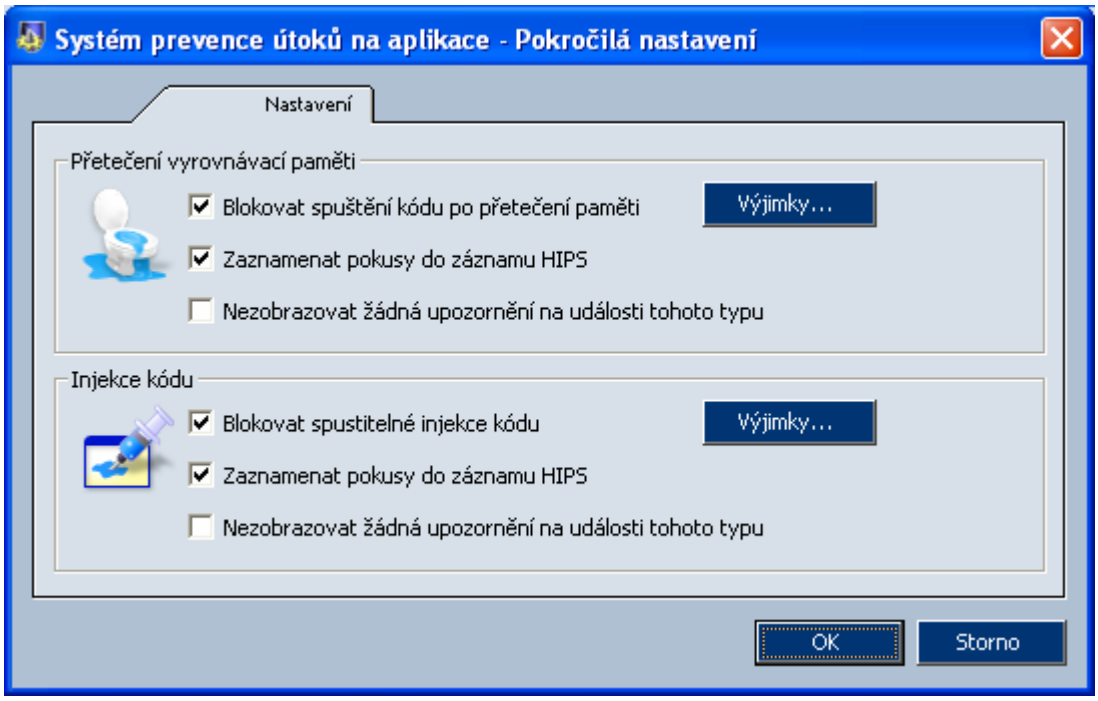
Karta *Síťová bezpečnost* sdružuje stěžejní nastavení chování firewallu. Na listu *Aplikace* se nachází seznam dříve rozpoznaných aplikací. Každé jsou přiřazena pravidla pro příchozí a odchozí komunikaci v důvěryhodné síti i v Internetu. K dispozici jsou volby povolit, zakázat a ptát se. Zajímavá je poslední položka v seznamu - *Libovolná jiná aplikace*. Jejím nastavením se ovlivňuje chování firewallu (zda nově detekovanou aplikaci automaticky vyhodnotit podle předvolby anebo dát uživateli na výběr o jejím rozhodnutí). Komunikaci každé aplikace lze také zapisovat do logu a zobrazovat upozornění uživateli. Detailnější nastavení aplikací (a nejen jich samotných) se provádí pod tlačítkem *Paketový filtr*, jenž je umístěno v pravém spodním rohu okna. Pravidla pro obecný síťový provoz v internetové i důvěryhodné zóně jsou uvedena pod listem *Předdefinované*. Pravidla aplikací i sítě lze také jednoduše deaktivovat. Na listu *Důvěryhodné* je možno nadefinovat libovolnou síť a přiřadit jí status důvěryhodnosti. Poslední list této karty se nazývá *Pokročilé* a umožňuje nastavit například režim internetové brány nebo blokování příchozího spojení při startu a ukončování operačního systému.

Popis	Důvěryhodné		Internet		Zaznamenat	Upozornit
	Příchozí	Odchozí	Příchozí	Odchozí		
rapimgr	zaká…	povolit	zaká…	ptát se		
wcesmgr	zaká…	povolit	zaká…	ptát se		
wcescomm	zaká…	povolit	zaká…	ptát se		
Windows NT Logon Application	zaká…	povolit	zaká…	povolit		
Userinit Logon Application	zaká…	povolit	zaká…	povolit		
Internet Explorer	zaká…	povolit	zaká…	povolit		
Generic Host Process for Win32 …	zaká…	povolit	zaká…	povolit		
ceappmgr	zaká…	povolit	zaká…	povolit		
LSA Shell (Export Version)	zaká…	povolit	zaká…	povolit		
Microsoft File and Printer Sharing	povolit	povolit	zaká…	zaká…		
Libovolná jiná aplikace	ptát se	ptát se	ptát se	ptát se		

Obr. 10. Přiřazení pravidel jednotlivým aplikacím.

Karta *Útoky* obsahuje správu položek NIPS (systém prevence síťových útoků), HIPS (systém prevence útoků na hostitelský operační systém) a blokování chování aplikací. NIPS ochrana spočívá v tom, že prohlíží síťovou komunikaci a blokuje rozpoznané útoky založené na databázi signatur známých útoků. Ochrana HIPS zabezpečuje hlídání

nelegitimního chování aplikací napadených určitým druhem útoku. Mezi základní položky patří kontrola přetečení vyrovnávací paměti a kontrola aplikačního kódu proti injekcím. Blokování chování aplikací umožňuje hlouběji sledovat chování programů. Jedná se o spouštění aplikace aplikací či o spuštění aplikace po její modifikaci.



Obr. 11. Detailní nastavení HIPS ochrany.

Karta *WWW* zabezpečuje filtrování obsahu www stránek (blokování reklam, popup oken, aktivního obsahu, cookies nebo ochranu soukromých informací). Zajímavou funkcí je položka *Referer*, což znamená zákaz serverům trasovat pohyb po webu.

Údaje o všech činnostech firewallu se nachází ve formě logu pod kartou *Záznamy*. Tady je možno si záznamy nejen prohlédnout, ale také upravit jejich ukládání. Zatrhnutím pole *Syslog server* lze docílit odesílání navolených událostí na vzdálený server společnosti Sunbelt.

4.2.4 Běh programu

Má-li aplikace pokoušející se navázat spojení nastaven v pravidlech příznak *Ptát se* anebo je-li firewall v learning módu a detekuje neznámou aplikaci, objeví se nové okno s dotazem na uživatele. Ten následně rozhodne o povolení nebo zablokování komunikace. Zatržítkem lze firewallu sdělit, aby pro danou aplikaci vytvořil pravidlo a příště se již

netázal. Tlačítkem *Podrobnosti* lze navíc rozbalit podokno s detailními informacemi o probíhané komunikaci.

Obr. 12. Detekce komunikace nové aplikace.

Aplikaci je možno nastavit také příznak *Upozornit*. V takovém případě se při každé síťové komunikaci aplikace objeví ve spodním rohu obrazovky okno s informacemi o tomto spojení.

Obr. 13. Upozornění na probíhající komunikaci.

4.2.5 Výsledky leak-testů

Sunbelt Kerio Personal Firewall byl testován dvakrát. V prvním případě byla testována konfigurace *Simple*, která byla zvolena při instalaci programu (standardní doporučené nastavení). Výsledky byly dosti špatné, protože firewall nekontroloval téměř žádnou odchozí komunikaci. Druhé testy byly aplikovány na pokročilé nastavení firewallu s důrazem na maximální bezpečnost. Tentokrát byl firewall mnohem úspěšnější. Závěry z testování jsou uvedeny v tabulkách (Tab. 4, Tab. 5) v závěrečném souhrnu všech firewallů.

4.2.6 Rozdíly mezi verzemi

Doba na vyzkoušení plné verze je 30 dní. Jakmile tato lhůta vyprší, Sunbelt Kerio Personal Firewall nabídne možnost zakoupit licenci anebo přejít na verzi Free a bezplatně ji nadále provozovat. Tím se ovšem některé funkce programu deaktivují nebo omezí. Výčet nejdůležitějších změn je uveden v tabulce (Tab. 2).

Poplatek za používání plné verze programu činí 19.95 $ na 1 rok.

Tab. 2. Rozdíly obou verzí Sunbelt Kerio Personal Firewallu.

Sunbelt Kerio Personal Firewall (plná verze)	**Sunbelt Kerio Personal Firewall (Free verze)**
neomezené využití	jen nekomerční využití
heslem chráněná konfigurace	-
vzdálená správa firewallu	-
NIPS, HIPS, blokování chování aplikací	NIPS, blokování chování aplikací
filtr obsahu webu	-
použití i jako internetová brána	-
Syslog	-

Sunbelt Kerio Personal Firewall je uživatelsky přívětivý program, jenž se může chlubit řadou nezávislých ocenění. Jeho nespornou výhodou pro uživatele České Republiky je podpora Češtiny. Česky je psána i nápověda k produktu. Uživatelský manuál je však kompletně v Angličtině. Technická podpora je dostatečně široká a je k dispozici prostřednictvím online výpomoci (rozbor nejčastěji kladených otázek, vědomostní základna a podobně) nebo telefonní komunikace. Hodně užitečných informací je k nalezení i na českém uživatelském fóru http://forums.kerio.cz.

4.3 Outpost Firewall Pro

K testování byl použit Outpost Firewall Pro verze 4.0.1007.7323.

Testovaná verze byla vydána 25.ledna 2007.

4.3.1 O produktu

Outpost Firewall Pro vyvíjí společnost Agnitum (http://www.agnitum.com). Tato organizace byla založena v Petrohradu v únoru roku 1999. Jejím cílem bylo prosadit ve světě software zaměřující se na bezpečnost, a to nejen pro firemní využití. Důraz měl být kladen především na efektivitu programu a na snadné použití. Dnes má společnost Agnitum řadu poboček v Evropě a od roku 2005 též v USA.

Kromě osobního firewallu nabízí Agnitum i komplexnější Outpost Network Security určený zejména pro obchodní sítě.

4.3.2 Instalace

Outpost Firewall Pro je moderní osobní firewall, který nabízí řadu základních, ale i specializovaných funkcí k ochraně počítače. Tyto funkce zajišťují takzvané moduly Plug-In, což jsou samostatné nezávislé aplikace zaměřující se na různorodé síťové útoky. Moduly Plug-In lze do Outpost Firewallu Pro snadno implementovat a rozšířit tím rozsah zabezpečení počítače.

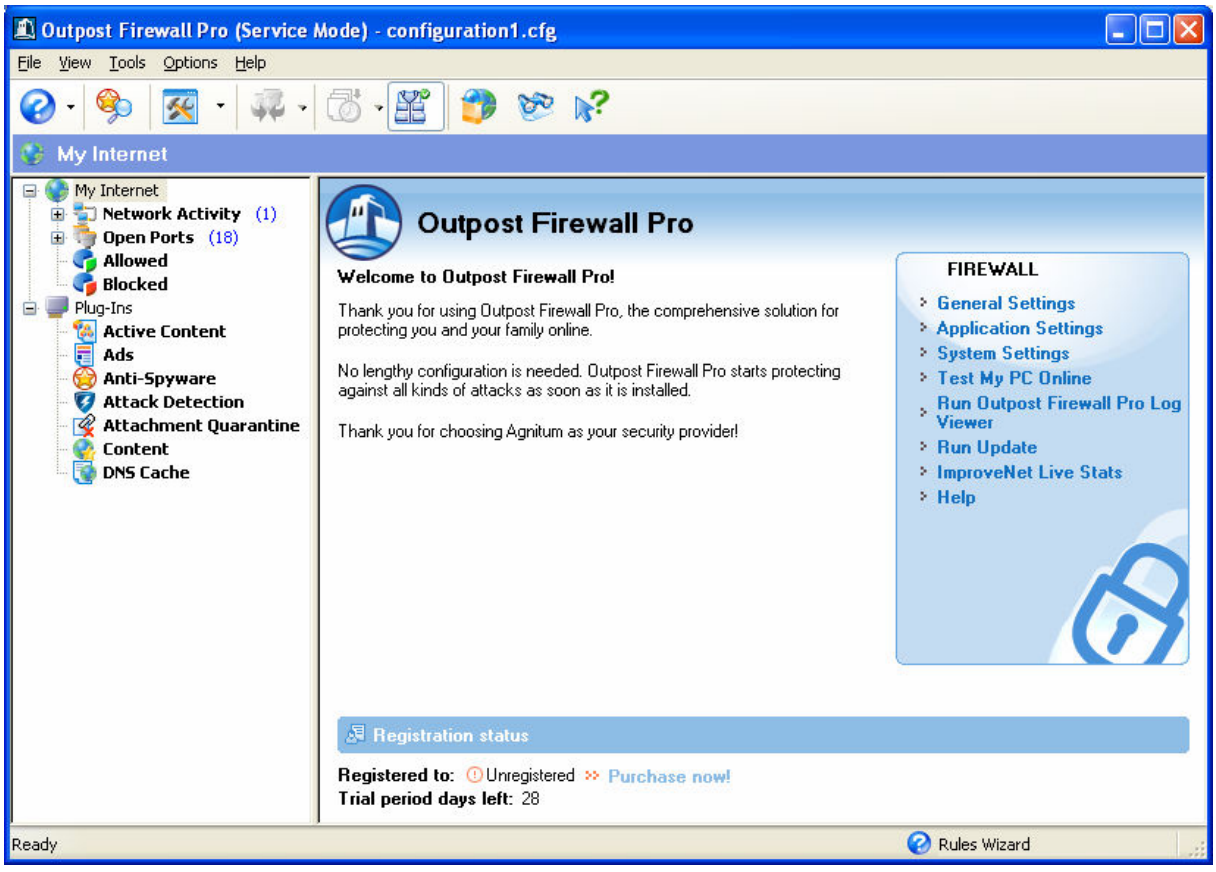
Instalací programu provází grafický průvodce. Postup instalace probíhá standardním způsobem. Po volbě jazyka instalace (Angličtina, Němčina, Španělština, Francouzština, Ruština) následuje potvrzení souhlasu s licenčním ujednáním a výběr cesty pro umístění programu na disk. Nejdůležitějším krokem je nastavení úrovně zabezpečení, kde jsou k dispozici 3 možnosti - *Advanced security* (pokročilá úroveň), *Normal security* (standardní) anebo *Custom configuration* (vlastní nastavení). Následně se firewall sám nakonfiguruje podle varianty zvolené v předchozím kroku. V závěru instalace je nabídnuta možnost anonymně sdílet informace s komunitou ImproveNet pro výpomoc v boji především se spywarem. Posledním krokem je výběr tvorby pravidel při detekci nové aplikace. Na výběr je tvorba automatická (firewall obsahuje databázi předdefinovaných pravidel pro nejpoužívanější aplikace) nebo manuální. Po ukončení instalačního průvodce se konfigurace Outpost Firewallu Pro dokončí detekcí sítí, do kterých je PC připojen a vytvořením databáze komponent nejznámějších aplikací. Po nutném restartu počítače má

ještě uživatel možnost aktivovat Anti-Spyware Plug-In a integraci Qiuck Tune Plug-Inu do Internet Exploreru (blokování grafických reklamních bannerů, cookies, vyskakujících oken a podobně). Jiné internetové prohlížeče bohužel podporovány nejsou.

K dispozici je i polská, maďarská, portugalská a italská verze programu.

4.3.3 Vzhled a konfigurace

Grafické uživatelské rozhraní je jednoduché, avšak není příliš přehledné. Jazyk je možno zvolit jako při instalaci programu. K zobrazení nashromážděných informací v GUI používá Outpost Firewall Pro dvou panelů. Levý panel obsahuje seznam nejdůležitějších kategorií firewallu. Velký informační panel potom ukazuje specifická data každé kategorie zvolené v levém panelu.



Obr. 14. Uživatelské rozhraní Outpost Firewallu Pro.

Menu na levé straně okna obsahuje dvě hlavní položky - *My Internet* a *Plug-Ins*.

Výběrem položky *My Internet* se v hlavním panelu zobrazí uvítací obrazovka s rychlým přístupem k nejpoužívanějším funkcím a také informace o licenci a doby do vypršení zkušební verze. Po rozbalení oddílu *My Internet* jsou vidět další položky s údaji o síťové

komunikaci. *Network Activity* zobrazuje velmi podrobné a užitečné informace o právě probíhající komunikaci (název souboru, dobu trvání komunikace, používaný protokol a port, rychlost přenosu dat, množství přijatých a odeslaných bytů a jiné). Po kliknutí na položku *Open Ports* se na hlavním panelu zobrazí seznam aktuálně otevřených portů ve formě aplikací, které tyto porty používají, a také celkový čas, po který je příslušný port otevřen. Zbývající dvě položky *Allowed* a *Blocked* podávají především statistické informace o povolené, respektive blokované komunikaci s možností náhledu na detailnější výpis (například velikost přijatých a odeslaných TCP a UDP paketů v bytech, jejich celková velikost, počet příchozích a odchozích TCP spojení, počet přijatých a odeslaných UDP datagramů a podobně).

Oddíl *Plug-Ins* shrnuje nainstalované moduly Plug-In a jejich stručný popis. Po instalaci Outpost Firewallu Pro jsou k dispozici Plug-Iny:

- Active Content — Správa aktivního obsahu webových stránek.
- Ads — Blokování reklamních bannerů.
- Anti-Spyware — Ochrana před spywarovými útoky.
- Attack Detection — Detekce útoků na počítač nebo síť, v níž je zapojen.
- Attachment Quarantine — Kontrola e-mailových příloh.
- Content — Blokace zobrazovaného obsahu či celých www stránek.
- DNS Cache — Správa a nastavení služby DNS.
- Quick Tune — Integrovaný panel v prohlížeči s funkcí blokování obsahu.

Po výběru některého z modulů Plug-In se zobrazí informace o jeho aktuálním stavu na hlavním panelu. Z něj je možno příslušný Plug-In také nakonfigurovat podle požadavků každého uživatele (funkčnost *Quick Tune* se nastavuje samostatně přímo v panelu umístěného v levé straně okna internetového prohlížeče). Z webových stránek společnosti Agnitum lze zdarma stáhnout množství dalších modulů Plug-In, které jsou neustále vyvíjeny.

Kromě dvou zmíněných panelů najdeme na hlavním okně programu nahoře i programové menu se záložkami *File* (soubor), *View* (zobrazení), *Tools* (nástroje), *Options* (nastavení) a *Help* (pomoc). Pomocí tohoto menu lze Outpost Firewall Pro podrobněji nakonfigurovat.

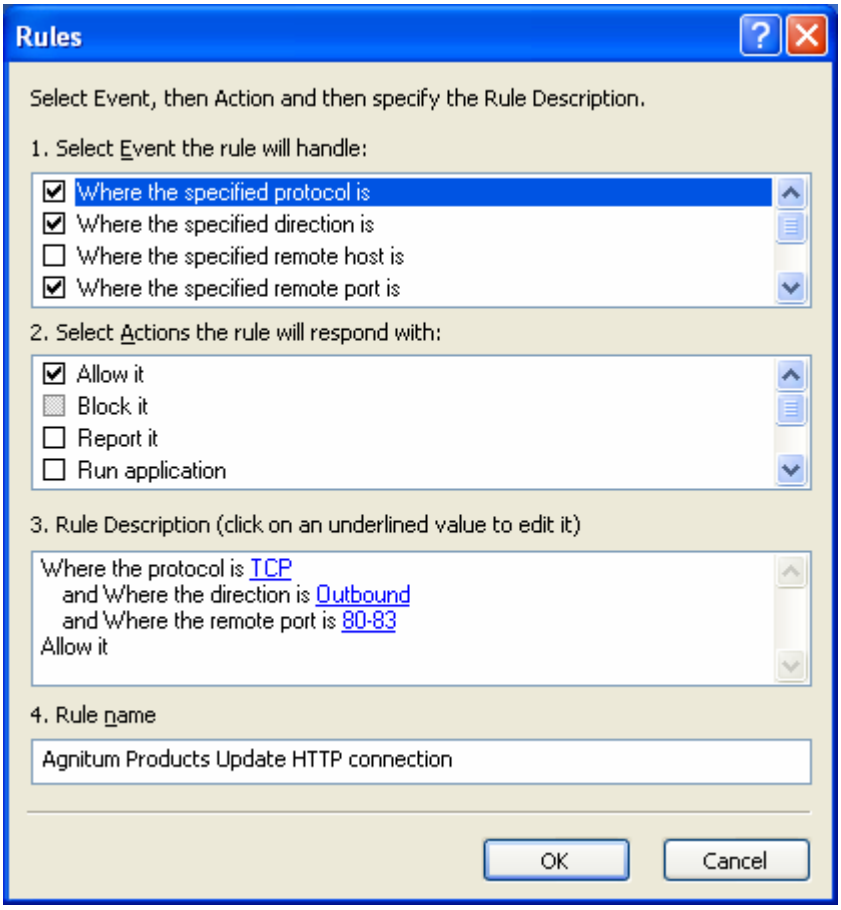
Pro rychlý přístup k vybraným funkcím slouží nástrojová lišta s ikonami umístěná pod programovým menu.

Pod položkou *File* je k dispozici uložení a obnova schématu nastavení firewallu nebo jeho nového sestavení. Odtud lze také celý program ukončit. Pomocí záložky *View* lze seskupovat položky v panelech různými způsoby, případně je dle určitých kritérií seřazovat (podle času a podobně). Také umožňuje zvolit jiný jazyk programu. K dispozici je mimo Angličtinu i Francouzština, Němčina, Ruština a Španělština. Menu *Tools* soustřeďuje odkazy k programovým nástrojům. K dispozici je zde především možnost upgradu programu, systémová kontrola proti spywaru, aktivace zápisu (logu) událostí s odkazem na jejich prohlížení (*Log viewer*), (de)aktivace Plug-Inu Quick Tune či (de)aktivace programové sebeobrany *Self-protection mode*. Tato funkce hlídá soubory firewallu proti modifikaci jinými aplikacemi. Položka *Help* umožňuje přístup k nápovědě, registraci atd.

Options je nejdůležitější záložka. Přes ni se lze dostat k jednotlivým nastavením firewallu:

Na kartě *General* (obecné) je k dispozici volba módu firewallu po spuštění systému. Na výběr jsou módy *Normal* (normální), *Background* (na pozadí) anebo *Disabled* (vypnuto). Mód *Background* se používá při celoobrazovkových aplikacích (hraní her, sledování filmu atd.), aby nepřerušoval práci uživatele zobrazováním upozornění. Proto má svá vlastní pravidla. Na tomto místě je možno také nastavit heslo pro ochranu nastavení firewallu.

Karta *Application* (aplikace) obsahuje seznam blokovaných (blocked), částečně povolených (partially allowed) a důvěryhodných (trusted) aplikací. Do jedné z těchto sekcí je zařazena každá aplikace, kterou firewall detekuje a vytvoří pro ni příslušné pravidlo. Tyto pravidla lze modifikovat právě zde pomocí tlačítka *Edit* a volby *Modify Rules*. Aplikacím jde nastavit povolení/blokování příchozí/odchozí komunikace specifikované podle protokolu(ů) a portu(ů), které ke komunikaci používají.



Obr. 15. Úprava pravidel jednotlivých aplikací.

V pravém dolním rohu karty se ještě nachází tlačítko *Anti-Leak* a *Components*. Pomocí nich se dá aktivovat ochrana systému proti mechanismům, které využívají programy útočící pomocí odchozí komunikace a také nastavit úroveň sledování programových komponent.

Na kartě *System* (systémové) se nastavují vlastnosti sítě LAN, kde je možnost zvolit důvěryhodnost sítě a povolení NetBIOS komunikace, která se uplatňuje při sdílení prostředků. V tomto místě se také upravuje tolerování ICMP paketů nebo aktivuje skrytý mód firewallu (tj. neposkytování žádné odezvy na dotazy z Internetu). Posledním oddílem na této kartě je definice globálních pravidel pro všechny aplikace. Tato pravidla mají nižší prioritu než konkrétní pravidla dané aplikace. Aplikují se na obecnou komunikaci jako je povolení služby DHCP nebo DNS.

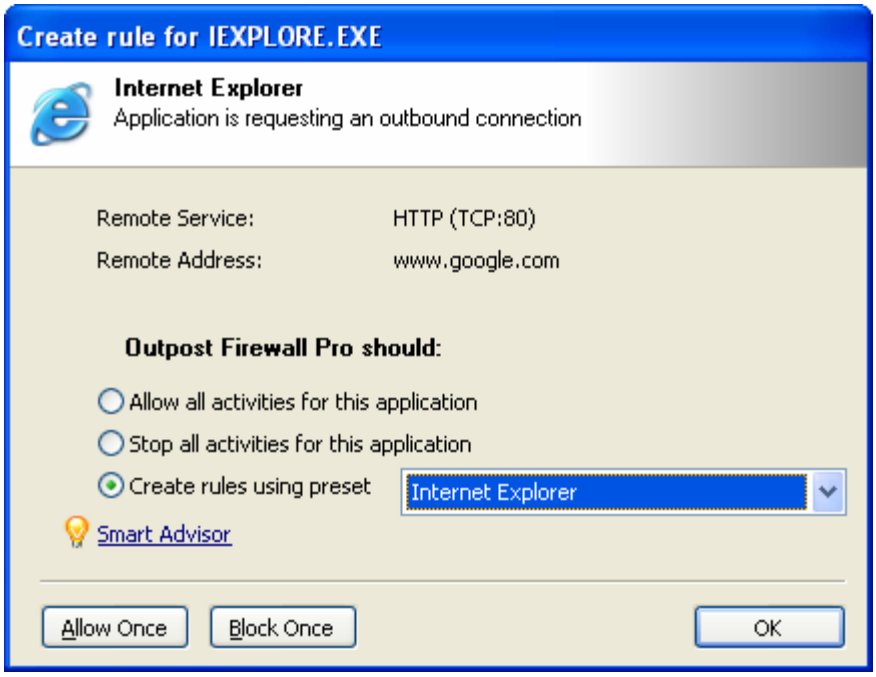
Karta *Policy* (politika) obsahuje pět alternativ nastavení politiky firewallu, a to *Disable mode* (firewall vypnut), *Allow most* (povolit většinu), *Rules Wizard* (volba pravidel), *Block most* (blokovat většinu) a *Stop All mode* (zastavení veškeré komunikace). Zvolením

příslušné možnosti se zobrazí její symbol v systémové liště pro snazší přehled o aktuální režii firewallu. V pokročilém nastavení se definují samostatná pravidla pro background (respektive entertainment) mód a taktéž se zde nachází volba z automatické anebo manuální tvorby pravidel.

Karta *Plug-Ins* (plug-iny) umožňuje správu jednotlivých nainstalovaných modulů Plug-In.

4.3.4 Běh programu

Pokusí-li se nějaká aplikace o síťovou komunikaci (příchozí či odchozí) a pokud je firewall v módu pravidel, objeví se na obrazovce okno s možnostmi tuto komunikaci trvale povolit, zakázat nebo pro ni vytvořit pravidlo. Pravidlo je možno vytvořit podle předdefinované šablony, ale i uživatelsky definované. Tlačítky *Allow Once* a *Block Once* lze programu komunikaci v dané situaci jednorázově povolit, respektive zablokovat. Kliknutím na Smart Advisor lze zobrazit doporučený postup, pokud je k dispozici.



Obr. 16. Detekce aplikace vyžadující síťovou komunikaci.

Pokud je firewall v režimu automaticky definovaných pravidel pro aplikace, zobrazí se pouze malé upozornění o této akci v pravém spodním rohu obrazovky.

Obr. 17. Upozornění firewallu při automatickém vytvoření pravidla.

Většina událostí souvisejících s činností programu je zaznamenávána do logu. Tento log si lze kdykoliv prohlédnout pomocí samostatného nástroje *Log viewer* (rychlý přístup je přes klávesu F7). Uchovávaný log je velmi podrobný a členitý. Obsahuje informace nejen z běhu firewallu jako takového, ale i od všech modulů Plug-In.

4.3.5 Výsledky leak-testů

Outpost Firewall Pro byl podroben leak-testům jak ve své standardní konfiguraci, tak i v nejvyšší úrovni zabezpečení. V druhém případě byl firewall v testování úspěšný na 100%. Toho bylo docíleno aktivní anti-leakovou ochranou. Test na odhalení falešné ochrany však dopadl velmi špatně. Z toho lze usuzovat, že firewall použité leak-testy sice odhalí, avšak většinu metod, které používají jiné nástroje k útokům, detekovat nedokáže. To je jasně pozorovatelné v prvním testu (anti-leaková ochrana zde byla deaktivována), kdy firewall dopadl o poznání hůře než v druhé konfiguraci.

Výsledky toho, jak Outpost Firewall Pro obstál v leak-testech, jsou zobrazeny v tabulkách (Tab. 4, Tab. 5) v závěrečném souhrnu všech firewallů.

4.3.6 Rozdíly mezi verzemi

Cena licence k provozování Outpost Firewallu Pro činí 39.95 $ na 1 rok. Licenci je potřeba zakoupit po uplynutí zkušební lhůty firewallu, což je 30 dní od instalace softwaru. Pokud není platnost licence prodloužena, stává se z firewallu neplacená verze Outpost Firewall Free. V tabulce (Tab. 3) je uveden výčet změn mezi komerční a neplacenou verzí.

Tab. 3. Hlavní odlišnosti Outpost Firewallu mezi verzí Pro a Free.

Outpost Firewall Pro	Outpost Firewall Free
kompletní firewall	omezený firewall
globální a systémová pravidla	-

Outpost Firewall Pro	Outpost Firewall Free
anti-leak ochrana	omezená anti-leak ochrana
automatická tvorba pravidel	jen manuálně tvořená pravidla
kompletní log	stručnější log
záloha konfigurací	jedna konfigurace

Outpost Firewall Pro disponuje kvalitní uživatelskou podporou. Nápověda i dokumentace k programu jsou velmi rozsáhlé a podrobné. Dokumentace je přístupná k instalaci programu, jeho nastavením i ke všem modulům Plug-In. Příručka pro začátečníky pomůže s prvními kroky užívání firewallu. K dispozici je i animovaný průvodce, online podpora v 5 světových jazycích (Angličtina, Francouzština, Němčina, Ruština a Španělština) nebo internetové fórum http://www.outpostfirewall.com.

4.4 Comodo Firewall Pro

K testování byl použit Comodo Firewall Pro verze 2.4.18.184.

Testovaná verze byla vydána 16.února 2007.

4.4.1 O produktu

Společnost Comodo (http://www.comodo.com) sídlící v USA patří ve světě k vedoucím organizacím, které se zabývají poskytováním zabezpečovacích služeb na Internetu. Mezi ně patří především ověřování totožnosti, inteligentní zabezpečování a další služby potřebné k zajištění bezpečnosti on-line transakcí. Díky výsledkům výzkumného centra Digital Trust Lab zaujímá Comodo čelní příčky mezi poskytovateli certifikátů zabezpečení. Společnost Comodo má generální pobočky i v Anglii, Ukrajině a Indii.

Comodo nabízí také uživatelské produkty týkající se internetové bezpečnosti, jako jsou osobní firewall, anti-virus, anti-spam, e-mailové zabezpečení a jiné. Je také k podivu, že nástroj Comodo Firewall Pro je dostupný zdarma a lze jej provozovat bezplatně. Společnost Comodo tím ale k sobě přitahuje pozornost nejen mezi uživateli pohybující se v odvětví síťové bezpečnosti a tím si zajišťuje kvalitní reklamu.

4.4.2 Instalace

Instalací Comodo Firewallu Pro provází grafický průvodce (v Angličtině), který pomáhá uživateli s jejím průběhem. Po standardním zobrazení licenčního ujednání, jeho odsouhlasení a zvolení adresáře pro umístění programu nabídne instalátor dalšího průvodce. Ten vypomůže se základní konfigurací firewallu. Možnost registrace do komunity Comodo a aktivace produktu je dobrovolná, poté je ale nutno zvolit způsob konfigurace. Doporučená je automatická konfigurace, alternativou je manuální nastavení firewallu určené pro zkušenější uživatele. V témže okně lze také aktivovat ochranu Windows DEP (Data Execution Protection), což je systém hlídaní útoků proti přetečení zásobníku paměti. Po restartu počítače je firewall připraven chránit systém.

4.4.3 Vzhled a konfigurace

Comodo Firewall Pro používá ke komunikaci s uživatelem povedené GUI v Angličtině, na webových stránkách produktu (http://www.personalfirewall.comodo.com) lze ovšem stáhnout až 14 jazykových verzí programu. Úvodní okno GUI obsahuje graficky rozlišený přehled základních informací. K těm patří mimo jiné signalizace nastavení jednotlivých složek firewallu, grafické znázornění aplikací účastnících se síťové komunikace nebo údaje o dostupných síťových adaptérech a jejich nastavení. V levém spodním rohu je umístěn posuvník určený k rychlé změně režie firewallu. Po výběru možnosti *Block All* blokuje firewall veškerou komunikaci, zvolením možnosti *Custom* funguje podle nadefinovaných pravidel a konečně v režimu *Allow All* všechnu komunikaci povoluje. Pro lepší orientaci přiřadí každý režim jinou barvu programové ikoně v systémové liště. Ikona nad posuvníkem umožňuje nechat otestovat firewall on-line na internetových stránkách http://www.hackerguardian.com (nutná registrace).

Mezi podokny GUI lze přepínat pomocí tří záložek *Summary*, *Security* a *Activity* situovaných nad obsahem okna (první záložka *Summary* zastupuje úvodní okno).

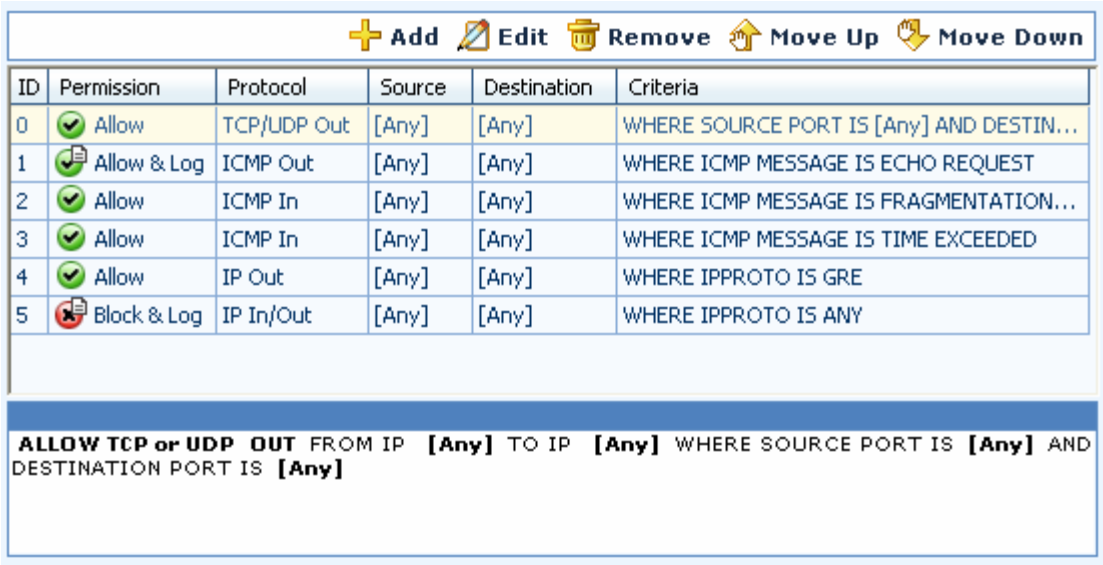
Obr. 18. Vzhled uživatelského rozhraní Comodo Firewallu Pro.

Přes druhou záložku *Security* se lze dostat ke všem nastavením firewallu.

Karta *Tasks* nabízí běžné úkony související s funkcí firewallu a také dva průvodce pro specifikování důvěryhodné sítě a pro vyhledání známých aplikací v systému (interní databáze obsahuje totiž jen malé množství nejběžnějších aplikací). Mezi nástroje této karty patří definice nové důvěryhodné nebo zakázané aplikace. Comodo Firewall Pro odlišuje jednotlivé aplikace také podle toho, která jiná aplikace vyvolala její běh (takzvaná mateřská aplikace). Proto může být definována v pravidlech tatáž aplikace vícekrát, pokaždé ale s jinou mateřskou aplikací. Ostatní položky této karty umožňují nadefinovat konkrétní síť (zónu), kterou lze poté průvodcem nastavit jako důvěryhodnou (například pro umožnění sdílení prostředků), dostat se odkazem na uživatelské fórum, vyhledat aktualizace softwaru nebo zaslat neznámé soubory k analýze společnosti Comodo.

Na kartě *Application Monitor* jsou uvedena pravidla rozpoznaných aplikací. Tyto definice obsahují mimo jiné název aplikace a její mateřské aplikace, cílovou IP adresu s portem (popřípadě jakýkoliv cíl, rozsah IP adres nebo zónu), použitý protokol (TCP, UDP, ICMP

atd.), směr komunikace a přiřazení povolení nebo blokádu komunikace. Karta *Component Monitor* je seznamem programových komponent s jejich popisem a příznakem. Velmi důležitá je karta *Network Monitor*, která definuje stěžejní pravidla síťového provozu. Funguje na principu filtrace paketů. Jednotlivá pravidla mají svůj identifikátor (ID) přiřazený podle jeho priority. Platí, že čím nižší ID, tím vyšší priorita (maximální prioritu zastupuje ID číslo 0). Všechny tři nástroje *Monitor* lze snadno deaktivovat a vyhnout se tak případným potížím se síťovým provozem.

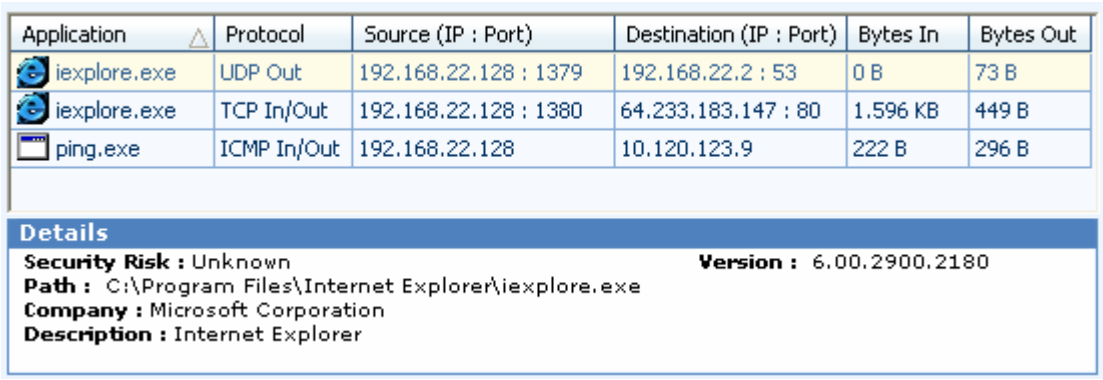


Obr. 19. Síťová pravidla pro všeobecnou komunikaci.

Karta *Advanced* obsahuje pokročilé nástroje detekce síťových útoků a také ostatní nastavení týkající se firewallu. Pokud je aktivní nástroj *Application Behavior Analysis*, analyzuje firewall vnitřní chování aplikací (včetně mateřských), jako jsou interní paměťové modifikace, DLL injekce, OLE mechanismy a další. Nástroj *Advanced Attack Detection and Prevention* zase chrání počítač před DoS/DDoS útoky, kdy lze určit například maximální propustnost paketů (TCP, UDP, ICMP), aby nedošlo k zahlcení počítače prostřednictvím záplavových útoků. V rozšířené volbě se nastavují související funkce, což je blokování odchozí komunikace při načítání operačního systému, blokování fragmentovaných IP datagramů, analyzování komunikačních protokolů a podobně.

Poslední nastavení je k dispozici pod záložkou *Miscellaneous*. Zde se posuvníkem konfiguruje množství upozornění generovaných firewallem, popřípadě jejich vypnutí. K ostatním položkám patří aktivace programových aktualizací, způsob startu firewallu anebo ochrana jeho registračních klíčů a důležitých souborů před neoprávněnou modifikací. Zabezpečení programu heslem však bohužel chybí.

Třetí záložka *Activity* obsahuje dvě karty. Karta *Connections* zobrazuje informace o síťové aktivitě, respektive o aplikacích, které se této komunikace účastní. Popsány jsou používaný protokol, zdrojová a cílová IP adresa s použitým portem a velikost bytů přijatých/odeslaných aplikací. Další detaily o aplikaci jsou vyobrazeny pod celým seznamem.



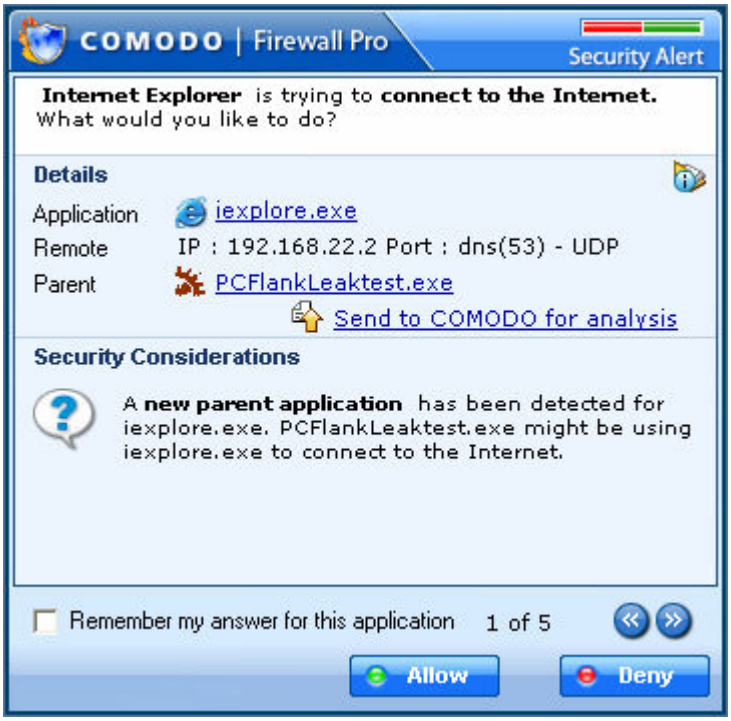
Obr. 20. Informace o síťové aktivitě.

Karta *Logs* slouží k prohlížení událostí zaznamenaných firewallem. Každá událost má status *High* (velké) nebo *Medium* (střední), což značí úroveň potenciální nebezpečnosti. Je také vidět, který nástroj firewallu danou událost vyhodnotil a jak s ní vynaložil (povolení, blokování, oznámení a jiné). K dispozici jsou i informace o zdrojové a cílové IP adrese s portem, čas výskytu události nebo ID síťového pravidla, které tato událost podléhá.

4.4.4 Běh programu

Firewall upozorňuje uživatele na jednotlivé události prostřednictvím vyskakujících oken. Jejich obsahem je zejména název aplikace pokoušející se navázat spojení, cílová IP adresa s portem a protokolem a také mateřská aplikace. Pokud firewall aplikaci nezná, je možno ji poslat společnosti Comodo na analýzu. V opačném případě se zobrazí doporučený postup.

V rohu okna symbolizuje ukazatel graficky míru bezpečnosti detekované komunikace množstvím zeleného zabarvení. Konečně lze tuto komunikaci povolit tlačítkem *Allow* nebo zablokovat tlačítkem *Deny*. Zatržením volby *Remember* si firewall naši volbu zapamatuje.



Obr. 21. Rozpoznání komunikující aplikace.

Kliknutím na symbol malého *i* v kroužku se zobrazí detailní informace o dané aplikaci, popřípadě o aplikaci mateřské, jako je například verze aplikace, její autor a jiné. Viz obrázek (Obr. 22).

Obr. 22. Detaily o mateřské aplikaci.

4.4.5 Výsledky leak-testů

Program byl nejprve testován v standardní konfiguraci (zvolené při instalaci programu) a posléze v režimu maximálního zabezpečení počítače. Firewall si počínal výborně zejména v druhém případě, nicméně v standardním nastavení dopadl také dobře.

Úspěšnost Comodo Firewallu Pro v testování je zobrazena v tabulkách (Tab. 4, Tab. 5) v závěru práce, kde jsou porovnány výsledky všech firewallů.

4.4.6 Informace o verzi

Comodo Firewall Pro je poskytován zcela zdarma, a to z důvodu popsaného výše. Při instalaci programu je doporučena registrace u společnosti Comodo, povinná ovšem není. Comodo Firewall Pro klade důraz zejména na kvalitní síťovou ochranu definovanou snadným uživatelským ovládáním. Z používání firewallu je patrné, že se mu tento cíl poměrně vydařil.

Programová a uživatelská podpora má širokou základnu. K produktu je nabízen uživatelský manuál a v případě nejasností je k dispozici e-mailová výpomoc. Řadu užitečných informací obsahuje i on-line uživatelské fórum http://forums.comodo.com nebo vědomostní základna http://support.comodo.com s nejčastějšími dotazy týkajících se firewallu Comodo.

4.5 Brána firewall systému Windows

4.5.1 O produktu

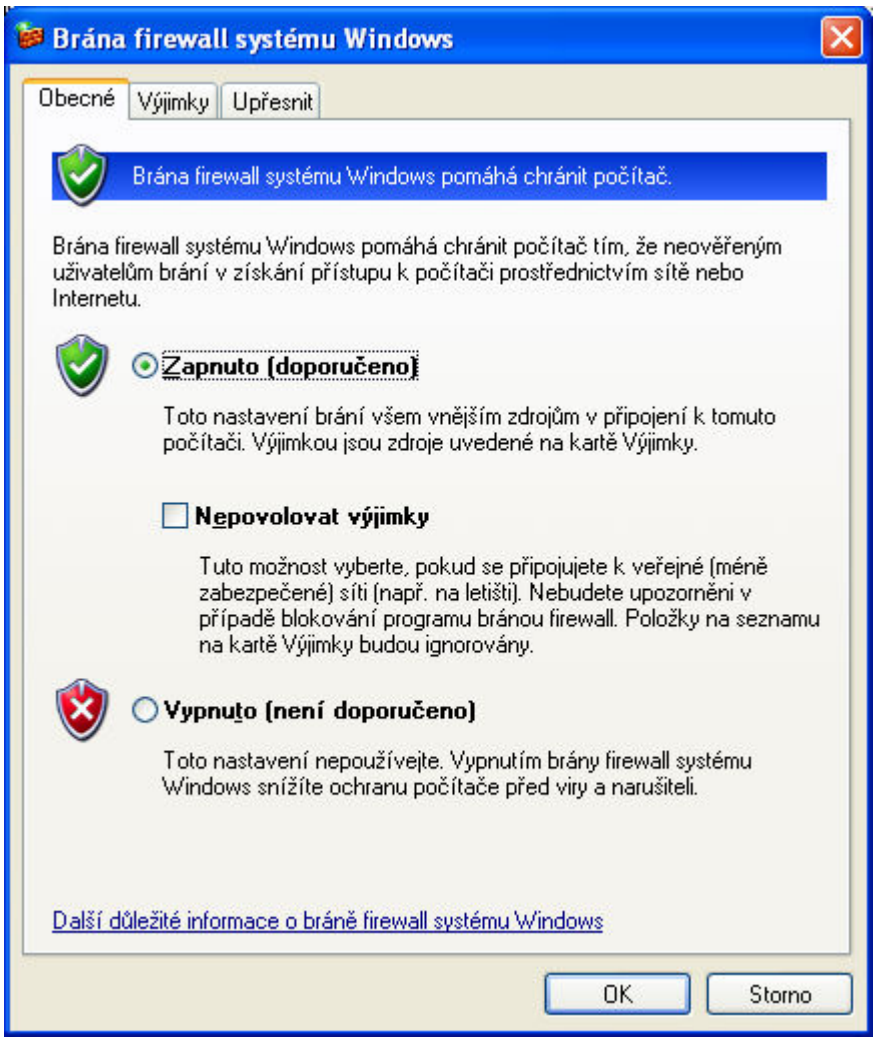
Společnost Microsoft (http://www.microsoft.com) asi není třeba příliš představovat. Tento americký gigant založili v roce 1975 Bill Gates a Paul Allen a v dnešní době stále ještě ovládá převážnou většinu trhu s operačními systémy. Systém Microsoft Windows byl vyvíjen od verze Windows 3 (nadstavba MS-DOSu) až po současnou, 64-bitovou verzi Windows Vista. Zpočátku nebyl kladen příliš velký důraz na bezpečnost práce v systému Windows, postupně se ovšem ukazovalo, že implementace alespoň základního zabezpečení bude nezbytná. Proto Microsoft začal poskytovat bránu firewall v operačních systémech Windows XP.

Pro kvalitní zabezpečení počítače je ale v první řadě potřeba pravidelně stahovat opravné záplaty a aktualizace operačního systému Microsoft Windows. Teprve potom se může pozornost uživatele obrátit na samostatný nástroj určený k ochraně počítače před síťovými útoky, jako je osobní firewall a podobně.

4.5.2 Vzhled a konfigurace

Brána firewall je součástí systémů Windows XP Home Edition a Windows XP Professional s aktualizací Service Pack 2. Brána je určena pro jednoduchou filtraci paketů, a to pouze pro komunikaci příchozí ze sítě do počítače. Proto by měla sloužit jen jako nouzové řešení.

Brána je implementována přímo do prostředí operačního systému, tudíž nemá svoje vlastní uživatelské rozhraní (konfiguruje se klasicky prostřednictvím oken). Používaný jazyk je stejný jako jazyková verze operačního systému. Přístup k bráně je možný přes *Ovládací panely* a položku *Brána firewall systému Windows*.

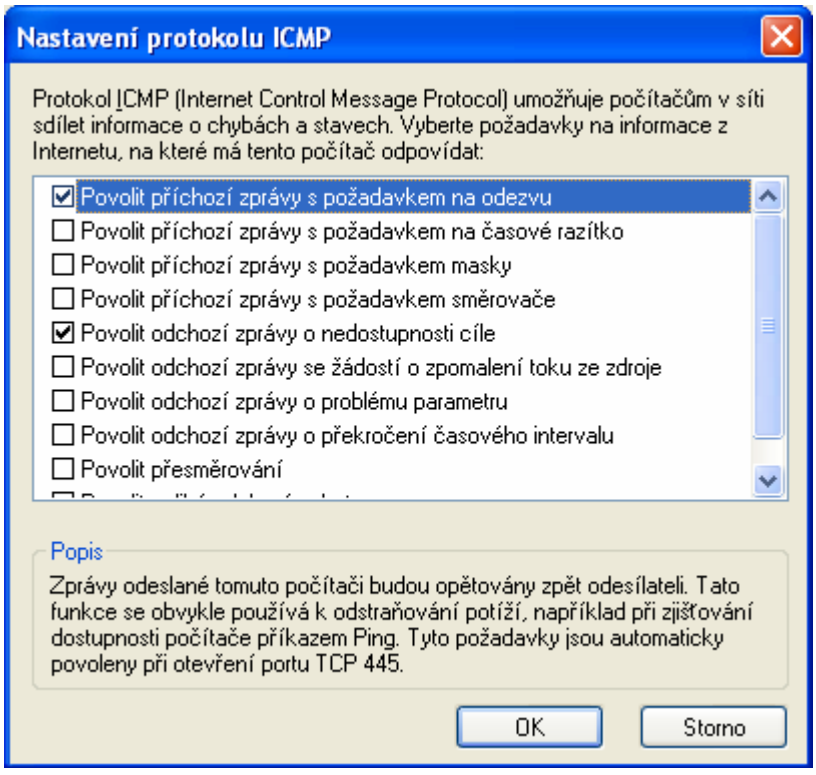


Obr. 23. Aktivace brány firewall systému Windows.

Okno má k dispozici tři záložky. Záložka *Obecné* umožňuje pouze dvěma volbami aktivovat resp. deaktivovat bránu. Nachází se zde i možnost nepovolovat žádné výjimky.

Záložka *Výjimky* obsahuje seznam programů a služeb, které brána ignoruje při jejich komunikaci. Každá tuto položka lze zapnout, vypnout i upravit. Měnit se dá především skupina, které je toto pravidlo určeno, a to tlačítkem *Změnit obor*. Na výběr je kterýkoliv počítač, pouze vnitřní síť anebo vlastní seznam IP adres (sítí). Službám je možno navíc upravovat porty (pouze TCP nebo UDP) a označovat je za otevřené nebo uzavřené. Dalšími dvěma tlačítky lze do seznamu výjimek přidat konkrétní program nebo port. Zatržítkem vespod okna lze zajistit, aby při blokování brána generovala upozornění.

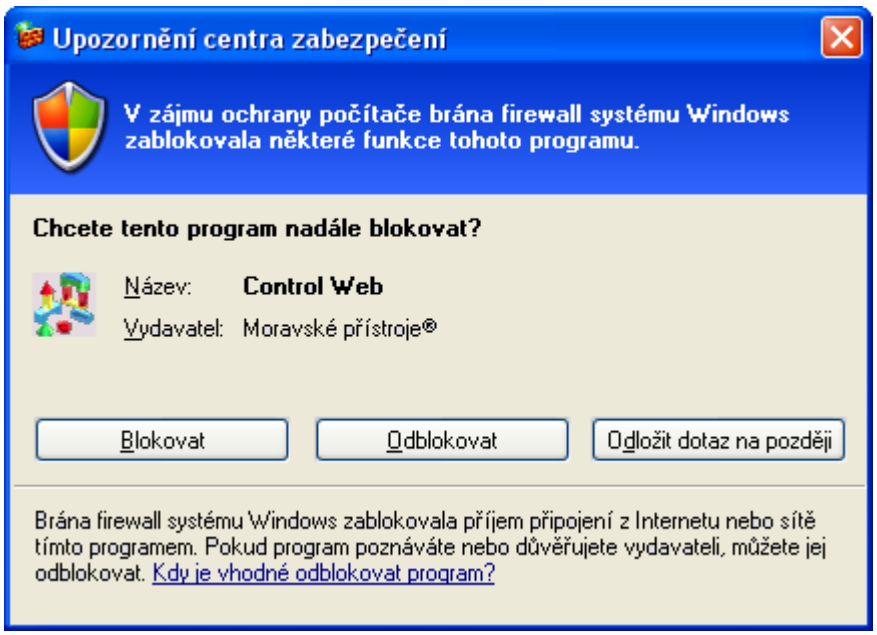
Poslední záložka *Upřesnit* umožňuje nastavit, které připojení (ze všech dostupných) má podléhat bráně firewall a také jej podrobněji nakonfigurovat. Určují se hlavně služby běžící v síti, které mohou používat uživatelé Internetu a také ICMP zprávy, na které má počítač odpovídat. Položka *Protokolování zabezpečení* slouží k nastavení logování událostí. Změnit jde například velikost zálohovaného log souboru a jeho umístění nebo pár možností, co konkrétně má brána do protokolu zaznamenávat. Brána dokáže také detekovat některé ICMP pakety. K jejich konfiguraci je určena položka *Protokol ICMP*. Seznam deseti předdefinovaných druhů zpráv může být opět označen jako aktivní nebo neaktivní, podrobnější nastavení však k dispozici není. Konečně tlačítkem *Obnovit výchozí* se nastavuje konfigurace brány do výchozího stavu.



Obr. 24. Nastavení protokolu ICMP.

4.5.3 Běh programu

Brána firewall pracuje ve dvou režimech. Buďto provádí přednastavené úkony v tichosti anebo generuje upozornění při detekci příchozí komunikace (pokud je nastaven příznak generování upozornění). V tom případě nabídne možnost komunikaci povolit, zablokovat, případně odložit dotaz na později. Na okně je uveden pouze název aplikace (služby) a její vydavatel, vespod okna jsou zobrazeny informace o dané komunikaci.



Obr. 25. Upozornění při detekci příchozí komunikace.

4.5.4 Výsledky leak-testů

Jak již bylo zmíněno, nekontroluje brána firewall žádnou odchozí komunikaci. Proto dopadlo testování leak-testy velmi špatně. Všechny testy bez problémů detekci brány obešly. Nicméně její výsledky jsou pro porovnání také zahrnuty v tabulkách (Tab. 4, Tab. 5) souhrnu všech firewallů v závěru práce.

5 VYHODNOCENÍ TESTŮ

Výsledky testování firewallů přinesly zajímavé závěry. Některé firewally si vedly v leak-testech výborně, jiné obstály hůře. Za povšimnutí stojí také úspěšnost firewallů v testování při jejich standardní (výrobcem doporučené) konfiguraci. V některých případech se výsledky testování s detailní konfigurací firewallu poměrně shodovaly, jindy se zase výrazně rozcházely. Překvapující jsou také výsledky leak-testu FPR, který dokázal odhalit klamnou ochranu daného firewallu. Firewall v tomto případě dokáže rozpoznat a zablokovat konkrétní leak-test, jiné nástroje založené na stejném principu by však nebyl schopen detekovat.

5.1 Porovnání firewallů

Všechny zjištěné skutečnosti z průběhu práce jsou vyobrazeny v tabulkách shrnujících úspěšnost firewallů v leak-testech. První tabulka (Tab. 4) obsahuje výsledky leak-testů při standardním nastavení daného firewallu, tabulka druhá (Tab. 5) zobrazuje výsledky testů při nastavení firewallu na maximální citlivost. Symbolika, která je v tabulkách použita, má následující význam:

- ✓ Firewall úspěšně zablokoval daný leak-test.
- ✗ Firewallu se nepodařilo daný leak-test zablokovat.
- **X/MAX** Firewall úspěšně zablokoval **X** testů z maximálního počtu **MAX** dané sestavy leak-testu.

Pro bezproblémový chod firewallu je také důležité znát jeho nároky na systém a minimální konfiguraci, při které je schopen normálně fungovat. Tyto aspekty jsou uvedeny v tabulce minimálních konfigurací potřebných k chodu firewallů (Tab. 6). Skutečné využití systémových prostředků je pak orientačně znázorněno v tabulce míry zatížení operačního systému každého z firewallů (Tab. 7). Brána firewall systému Windows je do operačního systému přímo integrovaná a tudíž nelze její nároky a míru zatížení systému přesně stanovit.

Tab. 4. Vyhodnocení leak-testů při standardní konfiguraci firewallů.

	ZoneAlarm Pro	Sunbelt Kerio Personal Firewall	Outpost Firewall Pro	Comodo Firewall Pro	Brána firewall systému Windows
AWFT	**8/10**	**10/10**	**10/10**	**10/10**	**0/10**
BITStester	✗	✗	✗	✓	✗
Breakout	**2/2**	**0/2**	**0/2**	**2/2**	**0/2**
Coat	✓	✗	✓	✓	✗
CopyCat	✓	✗	✓	✓	✗
CPIL	**1/3**	**0/3**	**3/3**	**3/3**	**0/3**
DNStester	✓	✗	✗	✓	✗
FireHole	✓	✓	✓	✓	✗
FPR	✓	✓	✗	✓	✗
Ghost	✓	✗	✗	✓	✗
Jumper	✗	✗	✓	✓	✗
LeakTest	✓	✗	✓	✓	✗
OSfwbypass	✗	✗	✗	✓	✗
PCAudit	✓	✓	✗	✓	✗
PCFlank	✗	✗	✗	✓	✗
Runner	✓	✗	✓	✓	✗
Surfer	✓	✗	✗	✓	✗
TooLeaky	✓	✓	✗	✓	✗
WallBreaker	**3/4**	**0/4**	**0/4**	**1/4**	**0/4**
Yalta	✓	✗	✓	✓	✗

Tab. 5. Vyhodnocení leak-testů při maximální citlivosti firewallů.

	ZoneAlarm Pro	Sunbelt Kerio Personal Firewall	Outpost Firewall Pro	Comodo Firewall Pro	Brána firewall systému Windows
AWFT	**10/10**	**10/10**	**10/10**	**10/10**	**0/10**
BITStester	✓	✓	✓	✓	✗
Breakout	**2/2**	**1/2**	**2/2**	**2/2**	**0/2**
Coat	✓	✓	✓	✓	✗
CopyCat	✓	✓	✓	✓	✗
CPIL	**3/3**	**1/3**	**3/3**	**3/3**	**0/3**
DNStester	✓	✗	✓	✓	✗
FireHole	✓	✓	✓	✓	✗
FPR	✓	✗	✗	✓	✗
Ghost	✓	✓	✓	✓	✗
Jumper	✗	✗	✓	✓	✗
LeakTest	✓	✓	✓	✓	✗
OSfwbypass	✓	✗	✓	✓	✗
PCAudit	✓	✓	✓	✓	✗
PCFlank	✓	✗	✓	✓	✗
Runner	✓	✓	✓	✓	✗
Surfer	✓	✓	✓	✓	✗
TooLeaky	✓	✓	✓	✓	✗
WallBreaker	**4/4**	**4/4**	**4/4**	**4/4**	**0/4**
Yalta	✓	✓	✓	✓	✗

Tab. 6. Minimální konfigurace potřebná pro chod firewallů.

	ZoneAlarm Pro	Sunbelt Kerio Personal Firewall	Outpost Firewall Pro	Comodo Firewall Pro	Brána firewall systému Windows
Operační systém	Win 2000 Pro/XP	Win 2000, XP	Win 98 /2000, XP	Win 2000, XP	Win XP (SP2)
Procesor [MHz]	450	300	450	300	-
Operační paměť [MB]	64/128	64	64/128	64	-
Místo na disku [MB]	50	10	50	32	-
Podpora 64-bit operačního systému	Ne	Ne	Ano	Ne	Ano

Tab. 7. Zatížení systému jednotlivými firewally.

	ZoneAlarm Pro	Sunbelt Kerio Personal Firewall	Outpost Firewall Pro	Comodo Firewall Pro	Brána firewall systému Windows
Místo na disku [MB]	30	14	45	16	-
Průměrná spotřeba operační paměti [MB]	29	24	14	17	-
Maximální spotřeba operační paměti [MB]	35	41	40	37	-

ZÁVĚR

Cílem této práce bylo porovnat vybrané osobní firewally a detailně prozkoumat jejich nastavení a přístupnost uživateli. To je podrobně popsáno u jednotlivých firewallů. Z hlediska síťové bezpečnosti má však větší význam zabývat se způsobem ochrany počítače firewallem a jeho úspěšností v leak-testech.

ZoneAlarm Pro spolu s Comodo Firewallem Pro obstály v testování nejlépe. Zejména Comodo Firewall Pro dopadl výborně, a to jak v přednastavené konfiguraci, tak i v citlivé. Může se zdát, že Outpost Firewall Pro byl v testech nejúspěšnější, nicméně jeho anti-leaková ochrana je ve velké míře ovlivněna detekcí známých leak-testů, čímž dává uživateli zdánlivý pocit bezpečí. Sunbelt Kerio Personal Firewall v testování nedopadl dobře zejména ve standardní konfiguraci. Při testování citlivějšího nastavení byly výsledky uspokojivější. Jeho výhodou pro mnohé místní uživatele však může být podpora českého jazyka. Brána firewall systému Windows neodhalila ani jeden leak-test, což se dalo očekávat, protože v podstatě nekontroluje žádnou odchozí komunikaci.

Pokud bych měl osobně doporučit osobní firewall z testovaných produktů, přiklonil bych se ke dvěma z nich. Comodo Firewall Pro má velmi příjemné uživatelské prostředí a lze jej poměrně snadno konfigurovat. Nenabízí sice více detailního nastavování, zato v testování si vedl ze všech firewallů nejlépe, a to i ve standardní konfiguraci. Proto je vhodný pro běžné, nenáročné uživatele, kteří nemají čas případně chuť zabývat se konfigurací firewallu do hloubky. ZoneAlarm Pro je na druhou stranu robustní a komplexní osobní firewall. Po instalaci firewall generuje spoustu upozornění, postupem času si však nejpoužívanější události zapamatovává a míra alertů tím klesá. Vzhledem k jeho slušné úspěšnosti v leak-testech a v možnosti detailního nastavení implementovaných funkcí tento produkt uspokojí i náročnější uživatele, kteří chtějí mít dokonalejší kontrolu nad svým počítačem.

ZÁVĚR V ANGLIČTINĚ

The goal of this paper work was to compare selected personal firewalls and investigate in detail their settings and accessibility to the user. This is closely described by each individual firewall. But in term of the network security the method of computer protection offered by firewalls and their successfulness in leak-tests have a major importance.

ZoneAlarm Pro along with Comodo Firewall Pro gained the best results in testing. Especially Comodo Firewall Pro fell out excellently both in the standard and in the thoroughgoing configuration. It may seem that Outpost Firewall Pro was the winner in leak-tests, but its anti-leaks protection is high impressed with detection of known leak-tests and thus gives users an illusive sense of safety. Sunbelt Kerio Personal Firewall did not fare well mainly with the preset parameters in testing. While testing with its deeper settings the results were more satisfactory. The advantage of this product can be its support of Czech language for local users. Windows firewall revealed not one in leak-tests, which was expected because of its impossibility to detect outbound communication.

If I ought to recommend a personal firewall from the tested products, I would tend towards two of them. Comodo Firewall Pro has a very pleasant user interface and it is possible to configure it easily. Firewall does not offer more detailed configuration, on the other hand its results of leak-testing were the best even in its standard settings. That is why it is suitable for common unassuming users who have not so much time or a fancy for the deeper settings of the firewall. Over against ZoneAlarm Pro is robust and complex personal firewall. After the installation the firewall generates a lot of alerts but the number of them decreases over time when firewall memorizes the most used events. In view of its fair successfulness in leak-tests and of possibility to configure its implemented functions in detail, this product satisfies also more exacting users who wants to hold a better control over their computers.

SEZNAM POUŽITÉ LITERATURY

[1] Microsoft Corporation. *Microsoft Windows 2000 Server : Sítě TCP/IP*. Překlad P. Kocanová, M. Kocan. 1. vyd. Praha : Computer Press, 2000. xxxviii, 824 s. ISBN 80-7226-291-2.

[2] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualiz. vyd. Praha : Computer Press, 2000. 435 s. ISBN 80-7226-323-4.

[3] PETERKA, Jiří. Co je čím ... v počítačových sítích : Síťový model TCP/IP. *E-archiv Jiřího Peterky* [online]. 1992 [cit. 2007-03-15]. Dostupný z WWW: <http://www.earchiv.cz/a92/a231c110.php3>.

[4] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí.* 1. vyd. Brno : Computer Press, 2005. 338 s. ISBN 80-251-0417-6.

[5] HALLER, Martin. Denial of Service (DoS) útoky : úvod. *Lupa.cz* [online]. 2006 [cit. 2007-03-20]. Dostupný z WWW:

<http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/>. ISSN 1213-0702.

[6] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP : bezpečnost* [online]. c2002 [cit. 2007-04-02]. Vybrané kapitoly. Dostupný z WWW: <http://www.cpress.cz/knihy/tcp-ip-bezp/5.htm>.

[7] Atlantis Telecom & Datacom. *Bezpečnost sítí* [online]. Version V0.909c. c2006 , 9.2.2007 [cit. 2007-03-22]. Kódováno v UTF-8. Dostupný z WWW: <http://www.atlantis.cz/Ips.aspx>.

[8] WEIDA, Petr. Firewall - data v bezpečí. *Pcsvět.cz* [online]. 2002 [cit. 2007-04-05]. Dostupný z WWW: <http://www.pcsvet.cz/art/article.php?id=1896>. ISSN 1213-6042.

[9] DYMÁČEK, Jan. Bezpečnost firewallů - zabezpečení stanic. *Lupa.cz* [online]. 2003 [cit. 2007-04-05]. Dostupný z WWW:

<http://www.lupa.cz/clanky/bezpecnost-firewallu-zabezpeceni-stanic/>. ISSN 1213-0702.

[10] BITTO, Ondřej. Vybíráme osobní firewall (1.). *Lupa.cz* [online]. 2005 [cit. 2007-03-20]. Dostupný z WWW:

<http://www.lupa.cz/clanky/vybirame-osobni-firewall-1/>. ISSN 1213-0702.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DHCP	Dynamické přidělovaní síťových zdrojů
DNS	Systém doménových názvů
DoS	Odepření služeb
GUI	Grafické uživatelské rozhraní
IDS	Systém detekce průniku
IPS	Systém prevence průniku
LAN	Lokální počítačová síť
NAT	Překlad síťových adres
PC	Osobní počítač
SYN	Synchronizace
TTL	Doba životnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PŘEHLED NEJČASTĚJI POUŽÍVANÝCH PORTŮ

Číslo portu	Protokol	Název služby	Vysvětlení
7	TCP/UDP	Echo	Služba Echo
20	TCP/UDP	FTP (data)	File Transfer Protocol
21	TCP/UDP	FTP	File Transfer Protocol
22	TCP/UDP	SSH	Secure Shell
23	TCP/UDP	Telnet	Protokol Telnet
25	TCP/UDP	SMTP	Simple Mail Transfer Protocol
43	TCP/UDP	Whois	Služba Who Is
53	TCP/UDP	DNS	Domain Name System
67	TCP/UDP	DHCP (server)	Dynamic Host Configuration Protocol
68	TCP/UDP	DHCP (klient)	Dynamic Host Configuration Protocol
69	TCP/UDP	TFTP	Trivial FTP
70	TCP/UDP	Gopher	Služba Gopher
79	TCP/UDP	Finger	Služba Finger
80	TCP/UDP	HTTP	Hyper Text Transfer Protocol
88	TCP/UDP	Kerberos	Protokol Kerberos
110	TCP/UDP	POP3	Post Office Protocol version 3
113	TCP/UDP	Auth	Ověřovací služba
115	TCP/UDP	SFTP	Simple FTP
119	TCP/UDP	NNTP	Network News Transfer Protocol
123	TCP/UDP	NTP	Network Time Protocol
137	TCP/UDP	NB (name)	Názvová služba NetBIOS
138	TCP/UDP	NB (datagram)	Datagramová služba NetBIOS
139	TCP/UDP	NB (session)	Relační služba NetBIOS
143	TCP/UDP	IMAP	Internet Message Access Protocol
161	TCP/UDP	SNMP	Simple Network Management Protocol
179	TCP/UDP	BGP	Border Gateway Protocol
194	TCP/UDP	IRC	Protokol Internet Relay Chat
213	TCP/UDP	IPX	Internetwork Packet Exchange
389	TCP/UDP	LDAP	Lightweight Directory Access Protocol
411-414	TCP/UDP	DC++	P2P (Peer To Peer) - DC++
443	TCP/UDP	HTTPS	Zabezpečený HTTP

Číslo portu	Protokol	Název služby	Vysvětlení
445	TCP/UDP	SMB	Server Message Block (NetBIOS nad TCP)
513	TCP	Login	Vzdálené přihlášení
514	UDP	Syslog	Služba Syslog
520	UDP	RIP	Routing Information Protocol
530	TCP/UDP	RPC	Remote Procedure Call
540	TCP/UDP	UUCP	Unix to Unix CoPy
554	TCP/UDP	RTSP	Real Time Streaming Protocol
563	TCP/UDP	NNTP (SSL)	NNTP Secure Sockets Layer (Zabezpečený)
636	TCP/UDP	LDAP (SSL)	Zabezpečený LDAP
992	TCP/UDP	Telnet (SSL)	Zabezpečený Telnet
993	TCP/UDP	IMAP (SSL)	Zabezpečený IMAP
994	TCP/UDP	IRC (SSL)	Zabezpečený IRC
995	TCP/UDP	POP3 (SSL)	Zabezpečený POP3
1214	TCP/UDP	Fasttrack	P2P - Kazaa apod.
1433	TCP/UDP	MSSQL (server)	Microsoft SQL
1512	TCP/UDP	WINS	Windows Internet Name Service
1863	TCP/UDP	MSN	MSN Messenger
3306	TCP/UDP	MySQL	MySQL databáze
3389	TCP	RDP	Remote Desktop Protocol (vzdálená plocha)
4661-4665	TCP/UDP	eDonkey	P2P - eDonkey
5190	TCP	IM	Instant Messenger (AOL, ICQ apod.)
5222	TCP	Jabber	Protokol Jabber
5223	TCP	Jabber (SSL)	Zabezpečený Jabber
5900	TCP/UDP	VNC	Virtual Network Computing
6000-6063	TCP/UDP	X11	X Window System
6345-6349	TCP/UDP	Gnutella	P2P - Bearshare apod.
6699	TCP/UDP	Napster	P2P - Napster
6881-6999	TCP	BitTorrent	P2P - BitTorrent
8080	TCP	HTTP	Alternativní HTTP