Uživatelský manuál

Kerio Personal Firewall 2.1

Datum vydání: 4. února 2002

Kerio Technologies Inc.

Sedláčkova 16

301 11 PLZEŇ

Česká Republika

Tel.: +420-19-7338901

E-Mail: support@kerio.cz

WWW: http://www.kerio.cz

Obsah

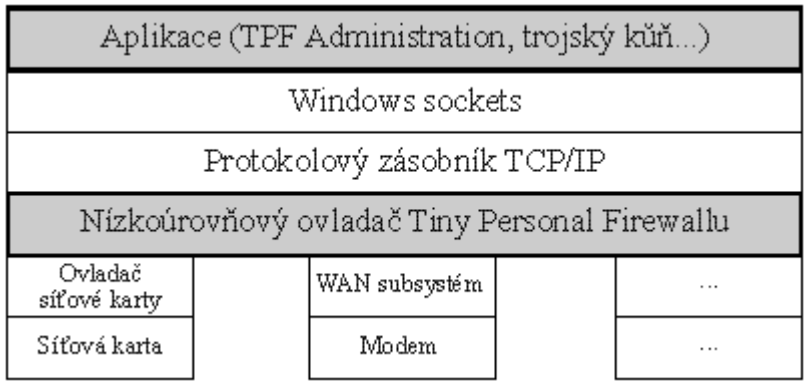
KAPITOLA 1

Úvod

Kerio Personal Firewall

Kerio Personal Firewall je malý snadno použitelný systém pro ochranu osobního počítače proti napadení hackerem a úniku dat. Je založen na bezpečnostní technologii použité ve firewallu WinRoute Pro a certifikované organizací ICSA.

Vlastní firewall běží jako služba na pozadí, který využívá speciální nízkoúrovňový ovladač zavedený do jádra systému. Tento ovladač je umístěn na nejnižší možné úrovni - přímo nad ovladači síťových zařízení. Díky tomu má absolutní kontrolu nad všemi procházejícími pakety a může tak zajistit dokonalou ochranu počítače, na němž je nainstalován.



Systémové požadavky

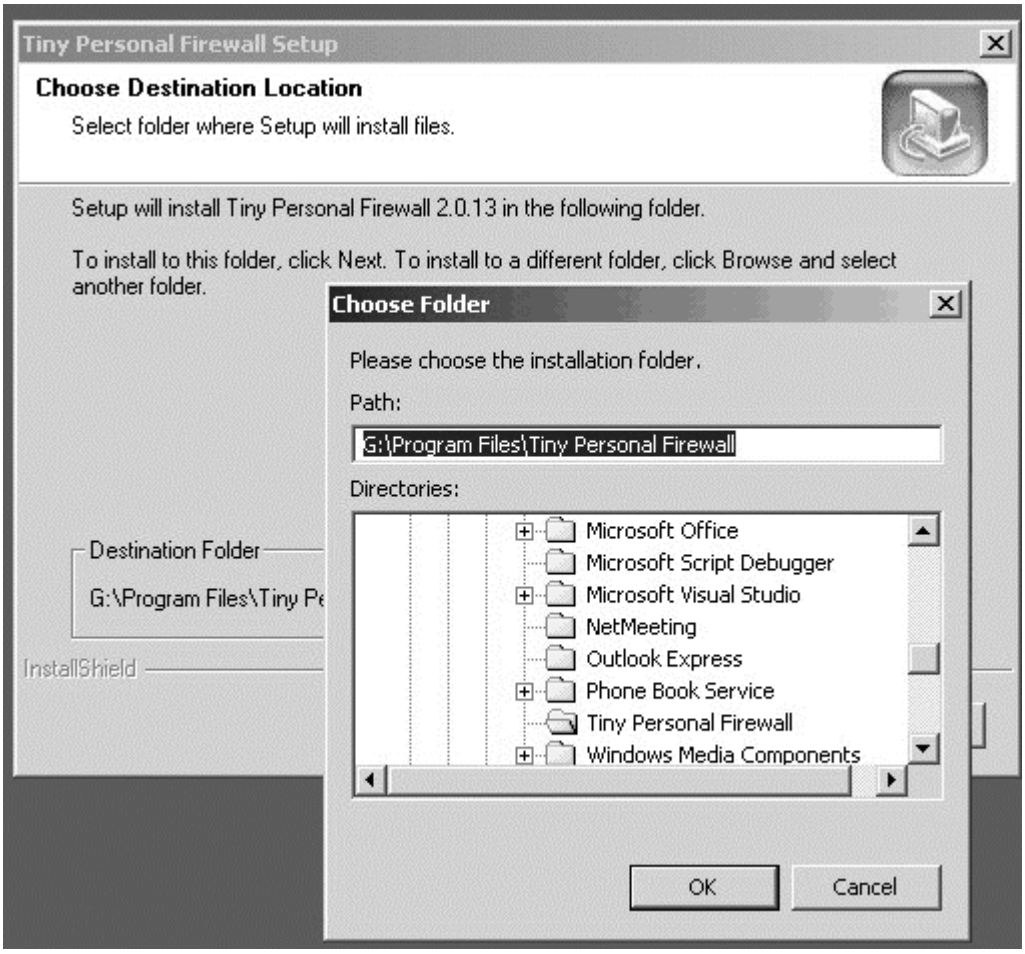
Pro instalaci produktu Kerio Personal Firewall je doporučena následující minimální konfigurace:

- CPU Intel Pentium a kompatibilní
- 16MB RAM
- cca 3MB místa na disku (pro instalaci; dále doporučujeme rezervovat alespoň 10MB pro záznamy)
- Windows 9x / Me / NT4.0 / 2000

Kerio Personal Firewall je určen pro ochranu počítačů, na nichž neběží WinRoute Pro nebo WinRoute Lite. Tyto produkty používají stejnou technologii zabezpečení a vykazují s Kerio Personal Firewallem konflikty.

Instalace

Instalace se provede jednoduše spuštěním instalačního archívu (typicky pfw2en.exe). V instalačním programu je možno vybrat adresář, kam mám být Kerio Personal Firewall nainstalován, nebo ponechat standardní adresář (C:\Program Files\Kerio\Personal Firewall). Po instalaci je třeba restartovat počítač, aby mohl být zaveden nízkoúrovňový ovladač firewallu.

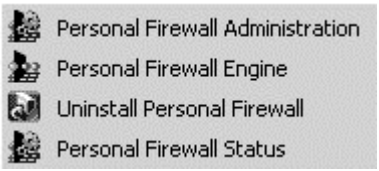


KAPITOLA 2

Administrace

Komponenty Kerio Personal Firewallu

Kerio Personal Firewall je tvořen třemi programy: Personal Firewall Engine, Pesonal Firewall Administration a Personal Firewall Status Window.



Personal Firewall Engine je vlastní výkonný program, který zajišťuje všechny funkce Personal Firewallu. Běží skrytě na pozadí (příp. jako služba ve Windows NT/2000) a zobrazuje se pouze jako ikonka na liště (v System Tray).

Při kliknutí pravým tlačítkem na ikonku se zobrazí menu, v němž je možno spustit aplikaci Administration nebo Status Window, zjistit informace o verzi programu (About) nebo ukončit Personal Firewall Engine (Exit). Při ukončení Engine se samozřejmě vypínají veškeré bezpečnostní funkce.

Dvojitým kliknutím levým tlačítkem je možno přímo spustit program Personal Firewall Administration.

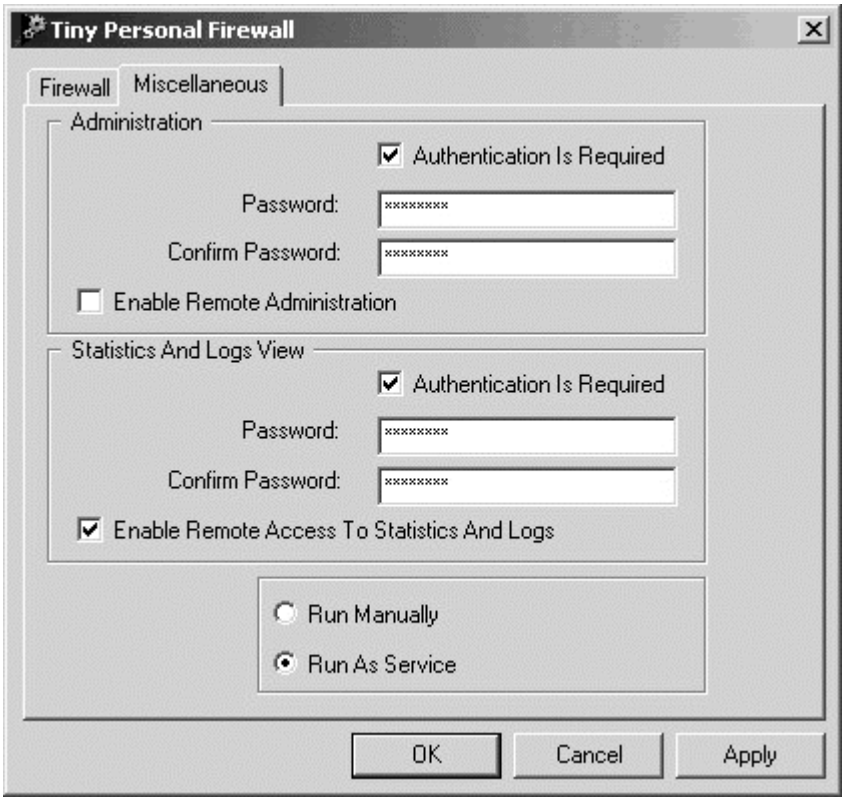
Personal Firewall Administration slouží ke konfiguraci Personal Firewall Engine. Jednotlivá nastavení budou popsána v následujících kapitolách tohoto manuálu.

Personal Firewall Status Window zobrazuje informace o všech běžících aplikacích komunikujících prostřednictvím TCP/IP. Jeho popisu je věnována samostatná kapitola.

Komunikace mezi Personal Firewall Engine a ostatními komponentami je chráněna silným šifrováním. Tím je zajištěno, že přenášená data nemohu být odposlechnuta a zneužita k napadení vašeho počítače.

Zabezpečení přístupu k administraci

Pro zajištění optimální bezpečnosti je třeba, aby Personal Firewall běžel po celou dobu běhu počítače, a také aby neoprávněná osoba nemohla zasahovat do jeho konfigurace. Tato nastavení lze provést v programu Personal Firewall Administration, záložka Miscellaneous.



Sekce Administration

Volba Authentication Is Required znamená, že program Personal Firewall Administration bude při svém spuštění vyžadovat heslo. Po zapnutí této volby jsopu přístupná pole pro zadání a potvrzení hesla (Password, Confirm Password). Volba Enable Remote Administration umožňuje, aby konfigurace Personal Firewallu byla prováděna z jiného počítače než z lokálního.

Sekce Statistics And Logs View

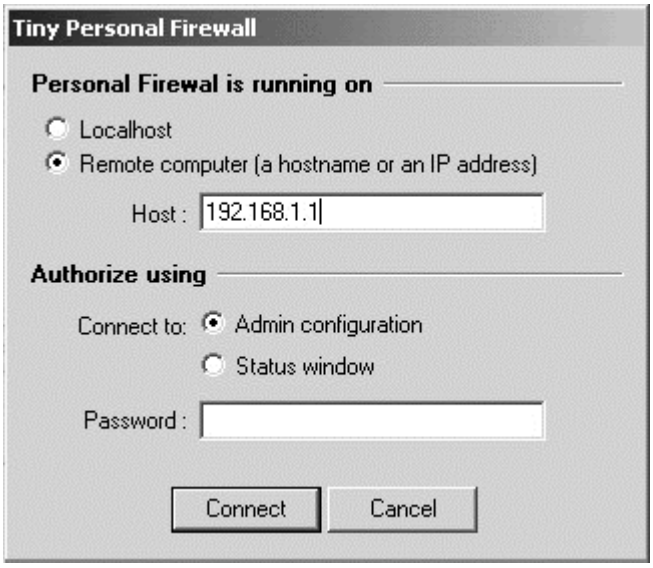
Zde se provádějí nastavení přístupu a vzdáleného přístupu k záznamům a statistikám. Volby jsou shodné jako v předchozí sekci. Tím, že je možno je nastavit odděleně, lze definovat dvě různé úrovně přístupu - k prohlížení záznamů a k plné administraci.

Run Manually / Run As Service

Volba, zda má být Personal Firewall spouštěn ručně, anebo automaticky při startu systému jako služba (resp. aplikace na pozadí ve Windows 9x/Me). Aby byla zaručena úplná bezpečnost, je bezpodmínečně nutné, aby byl Personal Firewall spouštěn jako služba a běžel po celou dobu běhu systému!

Přihlášení k administraci

Chcete-li spravovat Kerio Personal Firewall nebo prohlížet záznamy přímo na počítači, kde Personal Firewall běží, a není-li přístup k administraci nebo záznamům zabezpečen heslem, je možno přímo spustit aplikaci Personal Firewall Administration, resp. Personal Firewall Status Window. V ostatních případech se po spuštění libovolné z těchto aplikací nejprve zobrazí přihlašovací dialog.



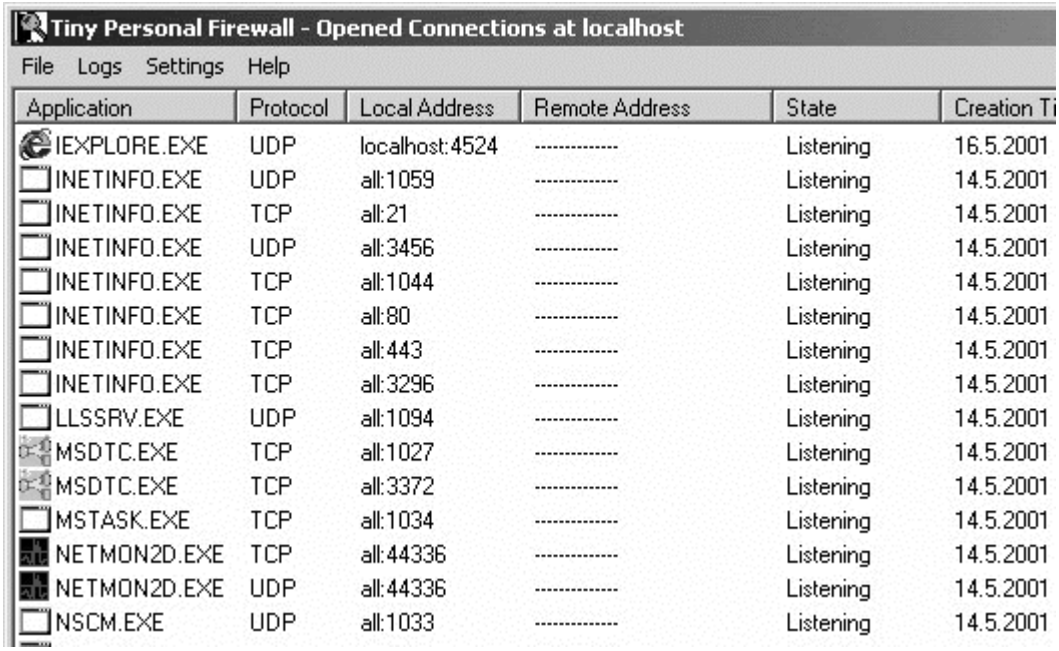
Zde je možno zvolit, zda se chcete připojit k Personal Firewallu běžícímu přímo na lokálním počítači (Localhost) nebo na jiném počítači (Remote computer) zadaném DNS jménem nebo IP adresou. Dále lze vybrat, zda se chcete otevřít program Personal Firewall Administration (volba Admin configuration) nebo Personal Firewall Status Window (volba Status Window). Do položky Password zadejte příslušné heslo (je-li nastaveno).

Personal Firewall Status Window

Aplikace Personal Firewall Status Window slouží k monitorování veškerých TCP/IP aktivit v operačním systému. Zobrazuje podrobné informace aplikace, které se účastní komunikace (a jimž je komunikace povolena bezpečnostními pravidly).

Základní okno

Základní okno zobrazuje na každé řádce informace o jednom lokálním koncovém bodu (koncový bod je určen IP adresou, portem a protokolem). Lokální koncový bod může vždy náležet pouze jedné aplikaci, naopak jedna aplikace může mít více lokálních koncových bodů (např. FTP server čeká na příchozí spojení na portech 20 a 21). Jednotlivé sloupce pak zobrazují informace o tomto koncovém bodu.



Application	Protocol	Local Address	Remote Address	State	Creation Ti
IEXPLORE.EXE	UDP	localhost:4524	----------	Listening	16.5.2001
INETINFO.EXE	UDP	all:1059	----------	Listening	14.5.2001
INETINFO.EXE	TCP	all:21	----------	Listening	14.5.2001
INETINFO.EXE	UDP	all:3456	----------	Listening	14.5.2001
INETINFO.EXE	TCP	all:1044	----------	Listening	14.5.2001
INETINFO.EXE	TCP	all:80	----------	Listening	14.5.2001
INETINFO.EXE	TCP	all:443	----------	Listening	14.5.2001
INETINFO.EXE	TCP	all:3296	----------	Listening	14.5.2001
LLSSRV.EXE	UDP	all:1094	----------	Listening	14.5.2001
MSDTC.EXE	TCP	all:1027	----------	Listening	14.5.2001
MSDTC.EXE	TCP	all:3372	----------	Listening	14.5.2001
MSTASK.EXE	TCP	all:1034	----------	Listening	14.5.2001
NETMON2D.EXE	TCP	all:44336	----------	Listening	14.5.2001
NETMON2D.EXE	UDP	all:44336	----------	Listening	14.5.2001
NSCM.EXE	UDP	all:1033	----------	Listening	14.5.2001

- Application - jméno spustitelného souboru aplikace, která vlastní daný koncový bod. Jméno může být zobrazeno i s plnou cestou zapnutím volby Settings / Don't Cut Pathnames
- Protocol - komunikační protokol (buď TCP - spojovaný protokol, nebo UDP - nespojovaný datagramový protokol)
- Local Address - lokální IP adresa a port (zobrazováno ve tvaru "adresa:port"). Volbami v menu Settings lze místo IP adres zobrazovat DNS jména a místo (standardních) portů názvy služeb.
- Remote Address - vzdálená IP adresa a port (nezobrazuje se, pokud není navázáno spojení)
- State - stav lokálního koncového bodu: Listening - čeká na příchozí spojení, Connected In - spojení navázáno zvenčí (vzdáleným klientem), Connected Out - spojení navázáno směrem ven (lokálním klientem)
- Creation Time - čas, kdy bylo spojení navázáno, nebo kdy daná aplikace začala přijímat na daném portu příchozí spojení
- Rx [Bytes] - objem přijatých dat daným koncovým bodem (resp. spojením) v bytech
- Rx Speed [kB/s] - průměrná rychlost příjmu dat (v kilobytech za sekundu)
- Tx, Tx Speed - totéž pro vyslaná data

Hlavní menu

- Nabídka File

  Volba Connect... umožňuje připojit se k Personal Firewall Engine (na lokálním či vzdáleném počítači). Volba Exit ukončuje program Personal Firewall Status Window.

- Nabídka Logs

  Umožňuje zobrazit záznamové okno (Firewall Log) nebo statistiky přenesených a filtrovaných dat (Statistics).

- Nabídka Settings

  Slouží k detailnímu nastavení, které informace a jakým způsobem se mají zobrazovat.

  Hide Listening Sockets - nezobrazí se koncové body, které jsou ve stavu "Listening" - tj. na nichž není navázáno spojení

  Hide Local Connections - nezobrazí se spojení, které jsou navázána pouze v rámci lokálního systému (na zpětnovazební rozhraní)

Hide Admin-Firewall Connection - nezobrazí se spojení navázaná mezi jednotlivými komponentami Personal Firewallu

Don't Resolve Domain Names - IP adresy počítačů nebudou převáděny na DNS jména

Don't Cut Pathnames - jména aplikací budou zobrazována včetně plné cesty

Update Frequency - jak často se mají informace v okně obnovovat. Lze zvolit jednu z těchto variant: Slowest (5 sec), Slower (3 sec), Normal (1 sec) a Fast (0.5 sec).

- Help

  Nápověda a informace o výrobci a verzi programu.

KAPITOLA 3

Nastavení zabezpečení

Úvod do TCP/IP

Pro správné nastavení Kerio Personal Firewallu a využití všech jeho možností je nutné porozumět, jak funguje komunikace protokoly sady TCP/IP. Zkušení uživatelé mohou tuto kapitolu přeskočit, začátečníkům naopak doporučujeme si ji důkladně prostudovat.

TCP/IP je souhrnné označení pro protokoly používané pro komunikaci v síti Internet. V rámci každého protokolu jsou data dělena na datové jednotky, nazývané pakety. Každý paket se skládá z hlavičky a datové části, přičemž hlavička obsahuje systémové informace (např. zdrojovou a cílovou adresu) a datová část vlastní přenášená data.

Protokolová sada je rozdělena na několik tzv. úrovní. Přitom platí, že pakety protokolů nižších úrovní obsahují (zapouzdřují) ve své datové části pakety protokolů vyšších úrovní (př. pakety protokolu TCP jsou neseny v IP paketech).

IP (Internet Protocol) je protokol, ktery nese ve své datové části všechny ostatní protokoly (kromě ICMP). Nejdůležitější informací v jeho hlavičce je zdrojová a cílová **IP adresa**, tedy kým (jakým počítačem) byl paket vyslán a komu je určen.

ICMP (Internet Control Message Protocol) je protokol pro přenos řídicích zpráv. Těchto zpráv existuje několik typů, např. informace, že cílový počítač je nedostupný, žádost o přesměrování nebo žádost o odezvu (použito v příkazu PING).

TCP slouží pro spolehlivý přenos dat tzv. virtuálním kanálem (spojením). Je používán jako nosný protokol pro většinu aplikačních protokolů, např. SMTP, POP3, HTTP, FTP, Telnet atd.

UDP je tzv. nespojovaný prototokol, tzn. nevytváří žádný kanál a data jsou přenášena v jednotlivých zprávách (tzv. datagramech). UDP nezaručuje spolehlivé doručení dat (datagram se může při přenosu sítí ztratit). Ve srovnání s protokolem TCP má ale mnohem nižší režii (odpadá vytváření a rušení spojení, potvrzování atd.). Protokol UDP se typicky používá např. pro přenos DNS dotazů, zvuku, videa apod.

Nejdůležitější informací v hlavičce TCP a UDP paketu je zdrojový a cílový **port**. Zatímco IP adresa určuje počítač v Internetu, port určuje aplikaci běžící na tomto počítači. Porty 1-1023 jsou rezervovány pro standardní služby a operační systém, porty 1024-65535 mohou být použity libovolnou aplikací. Při typické komunikaci klient-server je zpravidla znám cílový port (na něj se navazuje spojení nebo posílá UDP datagram), zdrojový port je naopak přidělován automaticky operačním systémem.

Aplikační protokoly jsou neseny v paketech protokolu TCP, příp. UDP, a slouží přímo k přenosu uživatelských (aplikačních) dat. Existuje mnoho standardních aplikačních protokolů (např. SMTP, POP3, HTTP, FTP apod.), programátor aplikace si však může navrhnout libovolný vlastní (nestandardní) způsob komunikace.

Jak funguje Kerio Personal Firewall?

Veškerá komunikace v síti Internet probíhá protokoly sady TCP/IP. Tyto protokoly jsou převážně používány i pro komunikaci v lokálních sítích. Základním (nosným) protokokolem je IP (Internet Protocol), jehož pakety nesou veškeré další informace (zapouzdřují v sobě ostatní protokoly). Opravdový firewall (jímž Kerio Personal Firewall bezesporu je) musí mít tedy stoprocentní kontrolu nad veškerými IP pakety - tzn. musí být schopen je zachytit, zjistit z nich potřebné informace a poté je propustit nebo filtrovat. Samozřejmostí je také vytváření záznamů o všech prováděných akcích, detekovaných útocích apod.

Základním principem činnosti Kerio Personal Firewallu je tzv. stavová inspekce. To znamená, že o každém paketu odcházejícím z vašeho počítače je vytvořen záznam, a zpět je propuštěn pouze paket odpovídající tomuto záznamu (odpověď na odeslaný paket). Ostatní pakety jsou zahazovány. Tím je zaručeno, že Personal Firewall propustí pouze komunikaci, která je zahájena z vnitřní sítě.

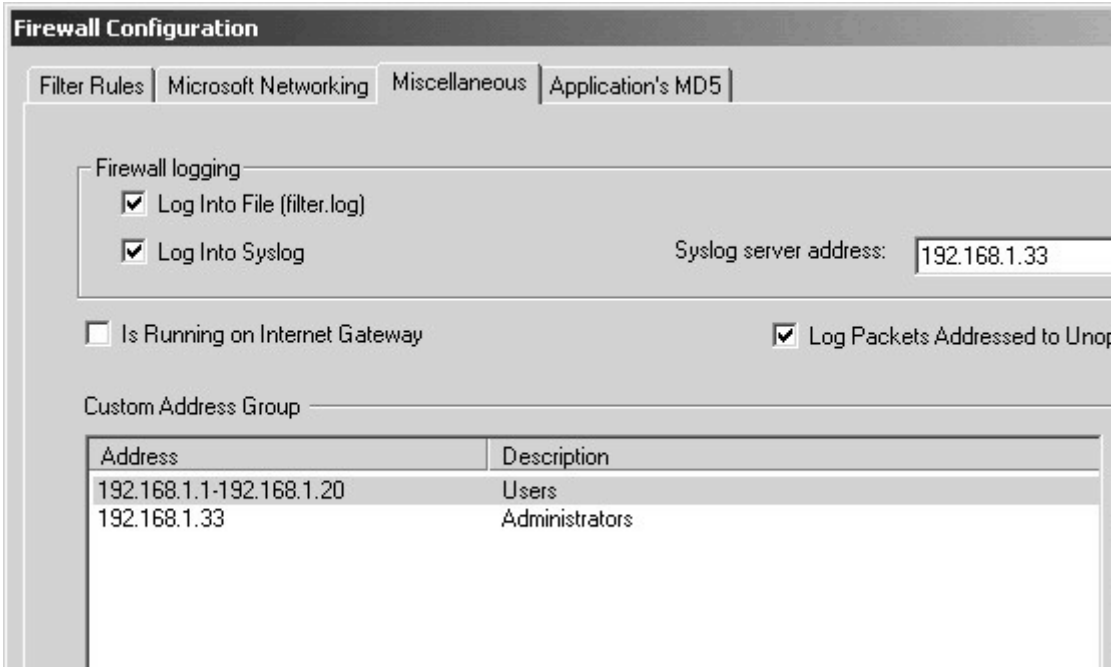
Filtrovacími pravidly může uživatel (resp. administrátor) specifikovat další podmínky pro filtrování a propouštění paketů. Vždy jsou ale propuštěny jen takové pakety, které vyhovují definovaným kritériím.

Skupiny IP adres

Při vytváření filtračních pravidel zakazujících nebo naopak povolujících určitou komunikaci může nastat situace, že má stejné pravidlo platit pro určitou skupinu IP adres (např. několik počítačů ve vaší lokální síti). Pak by bylo nutné definovat totéž pravidlo vícekrát (pro různé IP adresy či rozsahy adres).

Kerio Personal Firewall umožňuje vytvořit pro tento účel skupinu IP adress, kterou lze pak jednoduše použít v definici pravidla. Skupina přitom může obsahovat libovolný počet IP adres, rozsahů IP adres nebo subsítí.

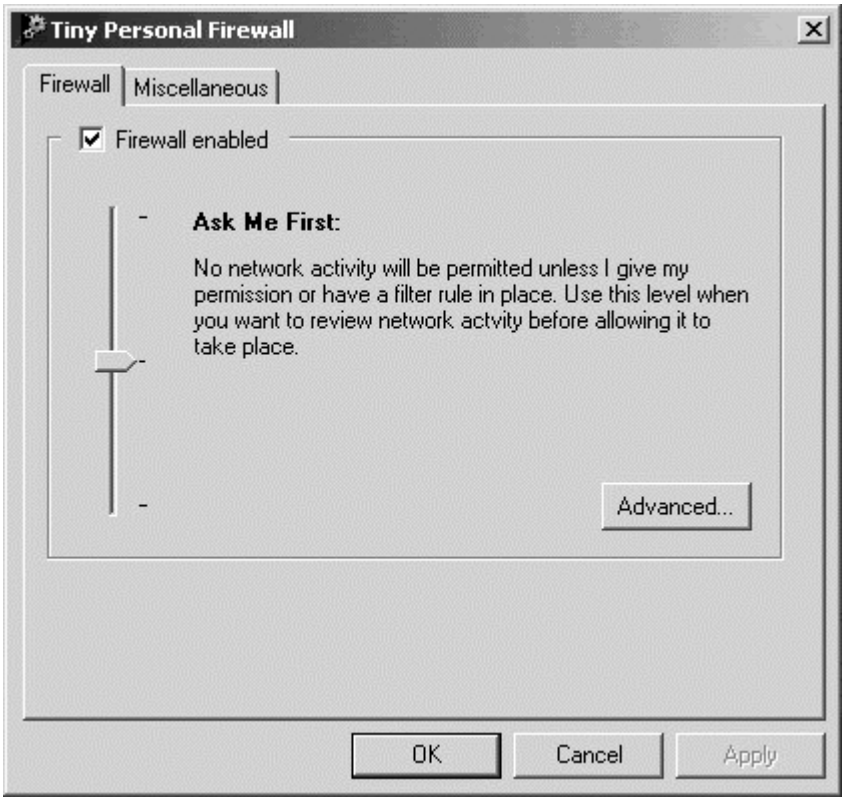
K definici uživatelské skupiny adres slouží sekce Custom Address Group v záložce Miscellaneous.



Tlačítkem Add... lze do skupiny přidat jednu IP adresu (Single address), rozsah IP adres (Network / Range) nebo subsíť (Network / Mask). Tlačítky Edit... a Del pak lze jednotlivé položky upravit, resp. smazat. Skupinu adres může být i prázdná (pak ale její použití nemá smysl).

Úrovně zabezpečení

Kerio Personal Firewall umožňuje nastavit 3 základní úrovně zabezpečení:



Don't Bother Me (neobtěžuj mě)

Minimální zabezpečení. Personal Firewall povoluje libovolnou komunikaci, kromě takové, která je filtrovacími pravidly explicitně zakázána. Nejsou-li nastavena žádná pravidla, Personal Firewall se chová transparentně (tj. jako kdyby nebyl vůbec spuštěn).

Ask Me First (nejdříve se mě zeptej)

V této úrovni je veškerá komunikace implicitně zakázána. Pokouší-li se nějaká aplikace komunikovat, nebo chce někdo zvenčí navázat spojení na tento počítač, Personal Firewall požadavek pozastaví a zobrazí dialogové okno, kde může uživatel komunikaci povolit či zakázat (jednorázově nebo trvale).

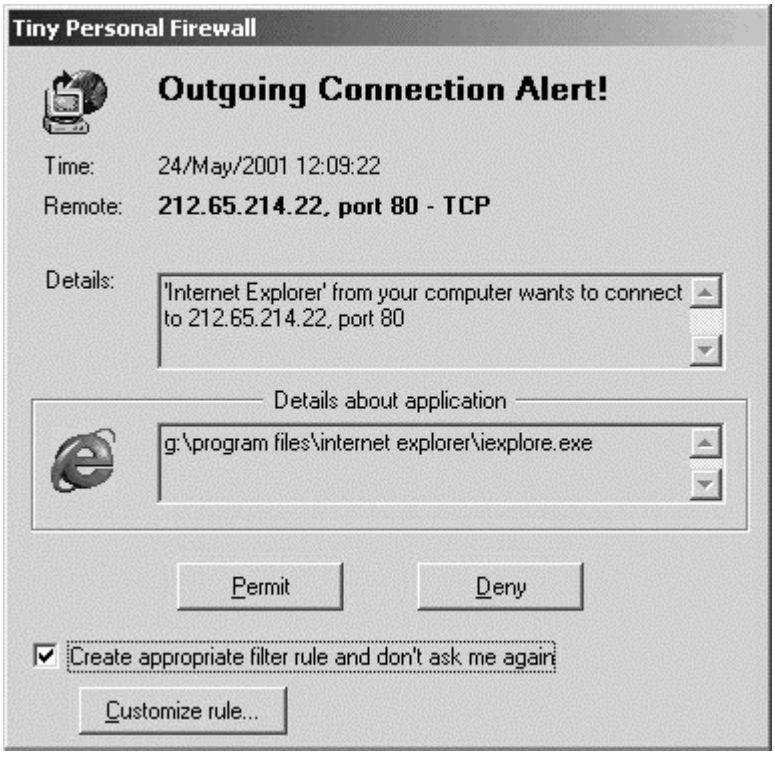
Cut Me Off (odřízni mě)

Zakáže veškerou síťovou komunikaci (bez ohledu na nastavená filtrovací pravidla). Tento režim bývá také označován jako tzv. síťový zámek a je ekvivalentní fyzickému odpojení počítače od sítě.

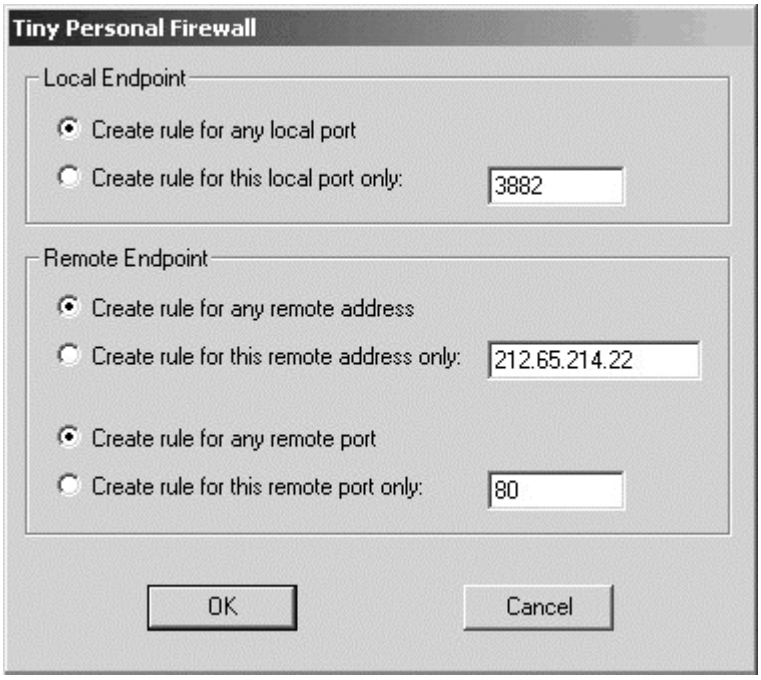
Interakce s uživatelem

Je-li nastavena úroveň zabezpečení "Ask me first", Personal Firewall propouští automaticky pouze komunikaci povolenou nastavenými filtrovacími pravidly. Je-li zachycen paket, který nevyhovuje žádnému pravidlu, předpokládá se, že uživatel počítače spustil novou aplikaci, kterou dosud nepoužíval, a zobrazí dialog, kde může uživatel komunikaci povolit nebo zakázat, a to buď jednorázově nebo trvale (vytvořením příslušného pravidla). Stejná situace nastává i v případě, že je zachycen příchozí paket zvenčí.

Dialogové okno obsahuje následující informace:



- Incoming Connection Alert / Outgoing Connection Alert - zda bylo detekováno příchozí nebo odchozí spojení
- Time - přesný údaj o datu a čase, kdy událost nastala
- Remote - informace o vzdáleném koncovém bodu (IP adresa, port a komunikační protokol)
- Details - podrobné informace o zachycené události
- Details about application - detaily o lokální aplikaci, která se účastní komunikace (v roli klienta nebo server)
- Permit - povolit zachycený paket
- Deny - zakázat (odfiltrovat) zachycený paket
- Create appropriate filter rule and don't ask me again - je-li zapnuta tato volba, pak se se stiskem tlačítka Permit nebo Deny automaticky vytvoří filtrovací pravdidlo, a příští paket tohoto typu bude již automaticky propouštěn nebo filtrován. Toho lze z výhodou využít zejména při počáteční konfiguraci firewallu - uživatel nemusí složitě definovat pravidla, pouze postupně spustí aplikace, které hodlá používat. Když Personal Firewall komunikaci zachytí, nechá automaticky vytvořit příslušná pravidla.
- Customize rule - stiskem tohoto tlačítka může zkušený uživatel upravit automaticky vytvořené pravidlo.



Filtrovací pravidlo vytvoření tímto způsobem je vždy platné pro konkrétní aplikaci, která vyslala nebo jíž byl určen zachycený paket (viz informační pole Details about application). Této aplikaci je vždy zároveň vytvořen tzv. MD5 podpis, aby mohla být v budoucnu ověřována její pravost (tzn. aby nemohl být spustitelný soubor aplikace nahrazen jiným programem stejného názvu). Podrobnosti naleznete v kapitole MD5 podpisy aplikací.

Standardně je filtrovací pravidlo pro konkrétní aplikaci vytvářeno tak, že aplikace může komunikovat na libovolném lokálním portu (any local port) s libovolným počítačem v Internetu (any remote address) a rovněž na libovolném portu (any remote port). Předpokládá se totiž, že pokud uživatel aplikaci jednou povolí, považuje ji za důvěryhodnou a nebude ji v komunikaci dále omezovat. To však nemusí být vždy zcela pravda, a proto má uživatel možnost pravidlo upravit (vytvořené pravidlo lze samozřejmě upravit i kdykoliv později, případně odstranit).

Jak správně (ne)upravit vytvářené pravidlo?

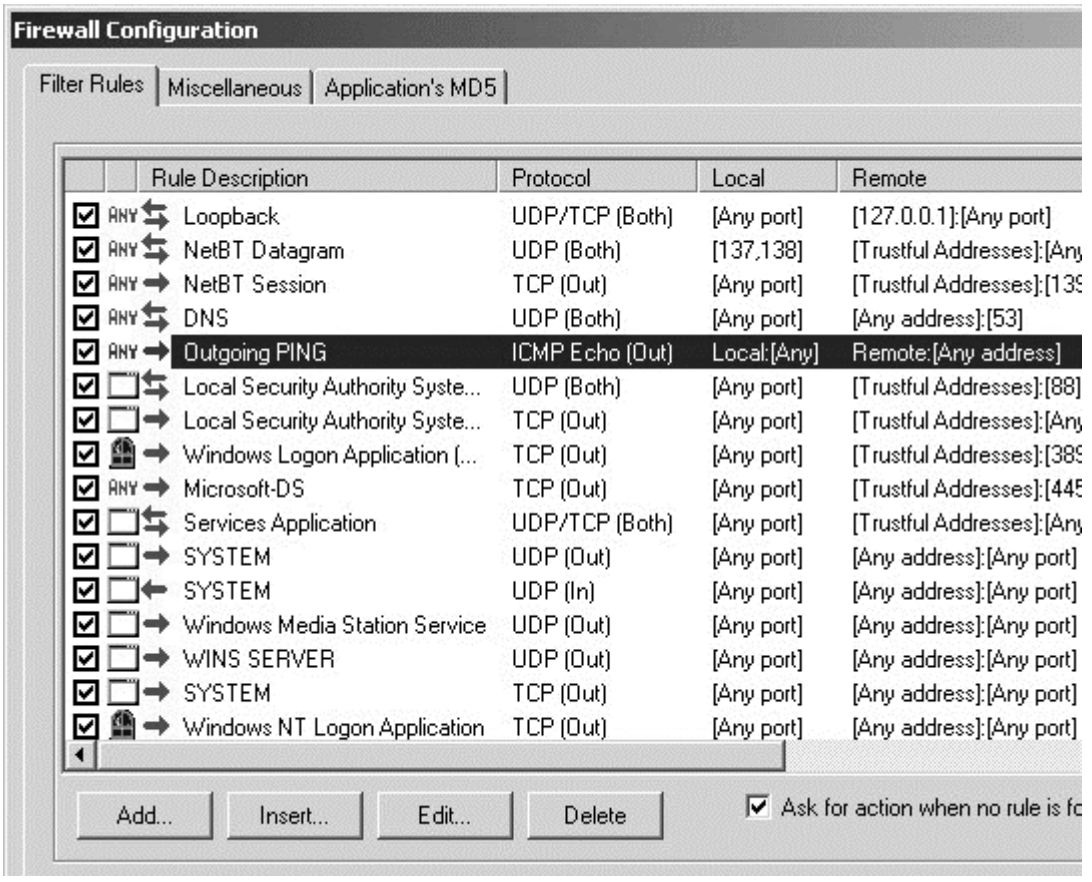
Detailní nastavení filtračního pravidla vždy závisí na konkrétní situaci, zejména aplikaci, jíž má být komunikace povolena nebo zakázána. Uveďme alespoň několik obecných zásad:

- Upravovat nastavení pravidel doporučujeme pouze uživatelům, kteří ovládají alespoň základy TCP/IP komunikace (viz kap. Úvod do TCP/IP).
- Nedoporučuje se nastavovat lokální port, pokud se jedná o klientskou aplikaci (např. WWW prohlížeč). Klientský lokální port je totiž přidělován operačním systémem a ve většině případů tedy není předem znám.
- Totéž platí pro vzdálený port, jedná-li se o serverovou aplikaci (např. WWW server), kdy je naopak klient s náhodně přidělovaným portem umístěn na vzdáleném konci.

Pravidla pro filtrování paketů

Filtrovací pravidla slouží k přesné definici, který paket má být propuštěn a který naopak filtrován. Bez těchto pravidel by fungoval Kerio Personal Firewall jen ve dvou módech: všechna komunikace povolena nebo naopak veškerá komunikace zakázána.

Existují dva způsoby, jak filtrovací pravidla vytvářet: buď "automaticky" při detekci neznámého paketu (jestliže uživatel paket odmítne nebo potvrdí - viz kap. Interakce s uživatelem) nebo ručně v programu Personal Firewall Administration. Zde je možno pravidla nejen vytvářet, ale také upravovat, mazat nebo řadit podle priority zpracování.
Definovaná filtrovací pravidla se zobrazují v záložce Filter Rules (po stisku tlačítka Advanced v hlavním okně Personal Firewall Administration).


Firewall Configuration
Filter Rules
Miscellaneous
Application's MD5
Rule Description
Protocol
Local
Remote
Loopback
UDP/TCP (Both)
[Any port]
[127.0.0.1]:[Any port]
NetBT Datagram
UDP (Both)
[137,138]
[Trustful Addresses]:[Any
NetBT Session
TCP (Out)
[Any port]
[Trustful Addresses]:[139
DNS
UDP (Both)
[Any port]
[Any address]:[53]
Outgoing PING
ICMP Echo (Out)
Local:[Any]
Remote:[Any address]
Local Security Authority Syste...
UDP (Both)
[Any port]
[Trustful Addresses]:[88]
Local Security Authority Syste...
TCP (Out)
[Any port]
[Trustful Addresses]:[Any
Windows Logon Application (...
TCP (Out)
[Any port]
[Trustful Addresses]:[389
Microsoft-DS
TCP (Out)
[Any port]
[Trustful Addresses]:[445
Services Application
UDP/TCP (Both)
[Any port]
[Trustful Addresses]:[Any
SYSTEM
UDP (Out)
[Any port]
[Any address]:[Any port]
SYSTEM
UDP (In)
[Any port]
[Any address]:[Any port]
Windows Media Station Service
UDP (Out)
[Any port]
[Any address]:[Any port]
WINS SERVER
UDP (Out)
[Any port]
[Any address]:[Any port]
SYSTEM
TCP (Out)
[Any port]
[Any address]:[Any port]
Windows NT Logon Application
TCP (Out)
[Any port]
[Any address]:[Any port]
Add...
Insert...
Edit...
Delete
Ask for action when no rule is fo

Seznam filtrovacích pravidel

Pravidla jsou zobrazována v tabulce, kde každý řádek představuje jedno pravidlo. Jednotlivé sloupce mají následující význam:

- Checkbox (zaškrtávací políčko) - zda je pravidlo aktivní či nikoliv. Kliknutím lze jednoduše pravidlo vypnout (deaktivovat), aniž by bylo nutno jej mazat a případně znovu přidávat
- Ikona aplikace - zobrazuje ikonu lokální aplikace, k níž se pravidlo vztahuje. Jedná-li se o pravidlo platné pro všechny aplikace, zobrazí se speciální zelená ikona s nápisem "ANY".
- Rule Description - směr a popis pravidla. Symboly pro směr jsou následující: šipka vpravo (odchozí paket), šipka vpravo (příchozí paket) a dvojitá šipka (pravidlo platí pro odchozí i příchozí pakety). Popis pravidla může být libovolný uživatelem zadaný řetězec, u automaticky vytvářených pravidel se zde objeví název lokální aplikace.
- Protocol - použitý komunikační protokol (TCP, UDP, ICMP...). Za názvem protokolu se v kulatých závorkách rovněž zobrazuje směr komunikace (In - dovnitř, Out - ven, Both - oba směry)
- Local - lokální port
- Remote - vzdálená IP adresa a port (odděleno dvojtečkou)
- Application - spustitelný soubor lokální aplikace včetně plné cesty. Jedná-li se o službu operačního systému, zobrazí se zde jméno "SYSTEM".

Klávesové zkratky

V seznamu filtrovacích pravidel lze použít následující klávesové zkratky:

- Enter - Edit
- Ins - Insert
- Del - Delete

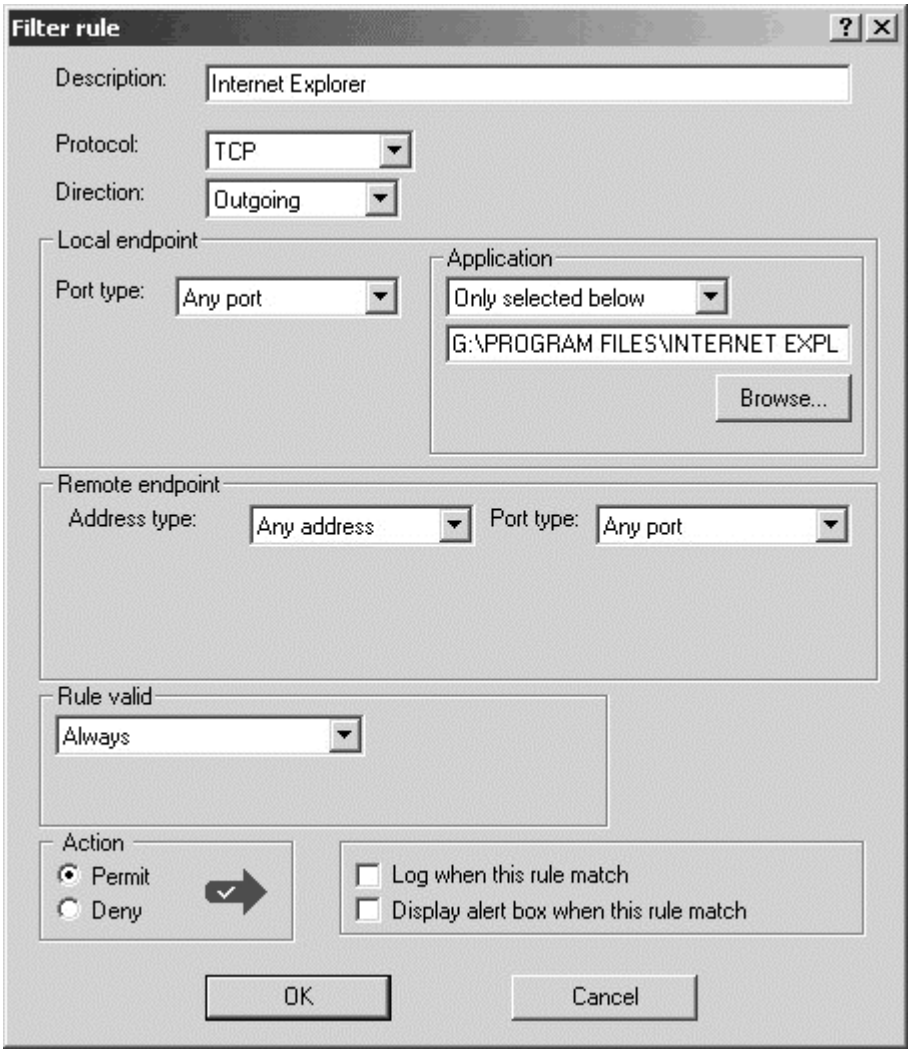
Ovládací prvky

- Add... - přidání nového pravidla na konec seznamu
- Insert... - vložení nového pravidla nad označené pravidlo. Tato funkce ušetří přesouvání nového pravidla v seznamu, protože jej umožní vložit přímo na požadované místo.
- Edit... - umožňuje změnit vybrané pravidlo
- Delete - smaže vybrané pravidlo

- Ask for action when no rule is found - zda má být při detekci neznámého paketu zobrazen dialog (viz kap. Interakce s uživatelem). Je-li tato volba vypnuta, pak jsou pakety, které nevyhovují žádnému pravidlu, automaticky zahazovány (tzn. je povolena pouze taková komunikace, pro niž bylo ručně vytvořeno pravidlo).
- Tlačítka se šipkami (vpravo vedle seznamu pravidel) - umožňují přesun vybraného pravidla v seznamu. Tak lze stanovit prioritu provádění pravidel (jsou zpracovávána směrem shora dolů).

Přidání nebo změna pravidla

Po stisku tlačítka Add, Insert nebo Edit se zobrazí dialog pro definici filtrovacího pravidla.


Filter rule
Description:
Internet Explorer
Protocol:
TCP
Direction:
Outgoing
Local endpoint
Port type:
Any port
Application
Only selected below
G:\PROGRAM FILES\INTERNET EXPL
Browse...
Remote endpoint
Address type:
Any address
Port type:
Any port
Rule valid
Always
Action
Permit
Deny
Log when this rule match
Display alert box when this rule match
OK
Cancel

- Description - pravidlu je možno přiřadit libovolný textový popis (název). Doporučujeme všechna definovaná pravidla důsledně pojmenovávat podle toho, k čemu jsou určena. Ušetří vám to mnoho komplikací při pozdějších změnách pravidel a odstraňování problémů.
- Protocol - komunikační protokol, na nějž se pravidlo vztahuje. Lze zvolit protokol TCP, UDP, TCP a UDP, ICMP nebo libovolný jiný (volba Other) - pak je protokol nutno specifikovat číslem protokolu v hlavičce IP paketu. Speciální volba Any znamená libovolný protokol, čili všechny IP pakety.

  Je-li vybrán protokol ICMP, zobrazí se navíc tlačítko Set ICMP..., po jehož stisknutí lze vybrat, na které typy ICMP zpráv se má definované pravidlo vztahovat. Vybrané ICP typy jsou pak vypsány do speciálního textového pole.

- Direction - směr, ve kterém mají být pakety zachycovány (Outgoing - odchozí, Incoming - příchozí, Both Directions - oba směry)

Sekce Local Endpoint - popisuje lokální koncový bod

- Port type - port (pouze je-li zvolen protokol TCP a/nebo UDP). Lze zvolit: Any (libovolný port), Single Port (jeden port), Port Range (rozsah portů) a List of ports (seznam čísel portů, oddělených čárkami).
- Application - zda se má pravidlo vztahovat na všechny pakety (Any application) nebo pouze na pakety vysílané / přijímané určitou aplikací (Only selected below). Spustitelný soubor aplikace by měl být uveden včetně plné cesty, a je možné jej buď zadat ručně, anebo tlačítkem Browse nalézt na disku.

Sekce Remote Endpoint - vzdálený koncový bod

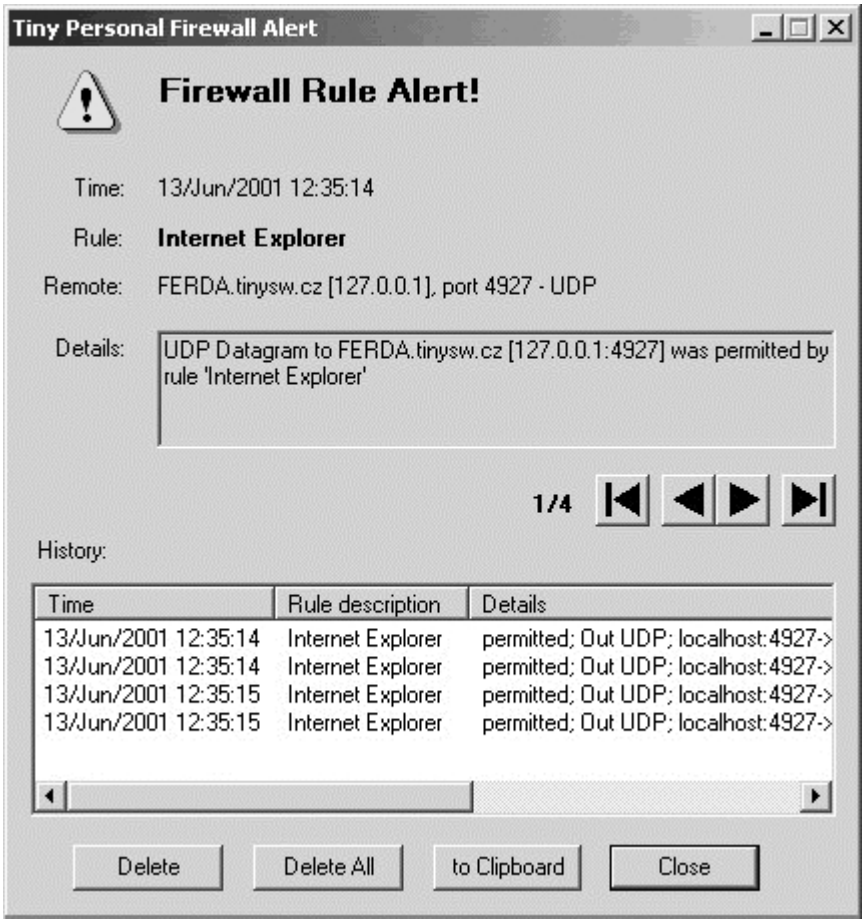
- Address type - IP adresa vzdáleného počítače. Může být specifikována jako libovolná adresa (Any address), adresa konkrétního počítače (Single address), subsíť zadaná adresou sítě a maskou (Network/Mask), rozsah IP adres (Network/Range) nebo uživatelem definovaná skupina IP adres (Trustful Addresses).
- Port type - vzdálený port. Možnosti jsou stejné jako při definici lokálního portu.

Další parametry

- Rule valid - zda je pravidlo platné vždy (Alvays) nebo jen v určité době (At this time interval only).Ve druhém případě lze pak tlačítkem Set.. nastavit dobu platnosti pravidla (počáteční a koncový čas a příslušné dny v týdnu). Použití časových intervalů samozřejmě vyžaduje správné nastavení systémového času!
- Action - akce, která se má provést - zda má být paket vyhovující definovaným podmínkám povolen (Permit) či zakázán (Deny).
- Log when this rule match - jestliže zachycený paket vyhovuje tomuto pravidlu, bude zaznamenán (viz nastavení záznamů v záložce Miscellaneous).
- Display alert box when this rule match - jestliže paket vyhovuje tomuto pravidlu, zobrazí se informační okno (Firewall Rule Alert) se detailním popisem paketu a informací, zda byl propuštěn nebo filtrován.

Informační okno Rule Alert

Toto okno se zobrazí, jestliže byl zachycen paket vyhovující pravidlu, u něhož je zapnuta volba Display alert box when this rule match.



Dialog zobrazuje následující informace:

- Time - čas, kdy k události došlo (kdy byl paket zachycen)
- Rule - název pravidla, které bylo použito
- Remote - informace o vzdáleném koncovém bodu - IP adresa (případně DNS jméno počítače), port a komunikační protokol
- Details - detailní popis paketu včetně informace, zda byl povolen nebo zakázán
- History - seznam všech událostí dosud zachycených na základě tohoto pravidla. Jsou řazeny od nejstarších k nejnovějším, kliknutím na pole "Time" lze řazení obrátit.

Ovládací prvky:

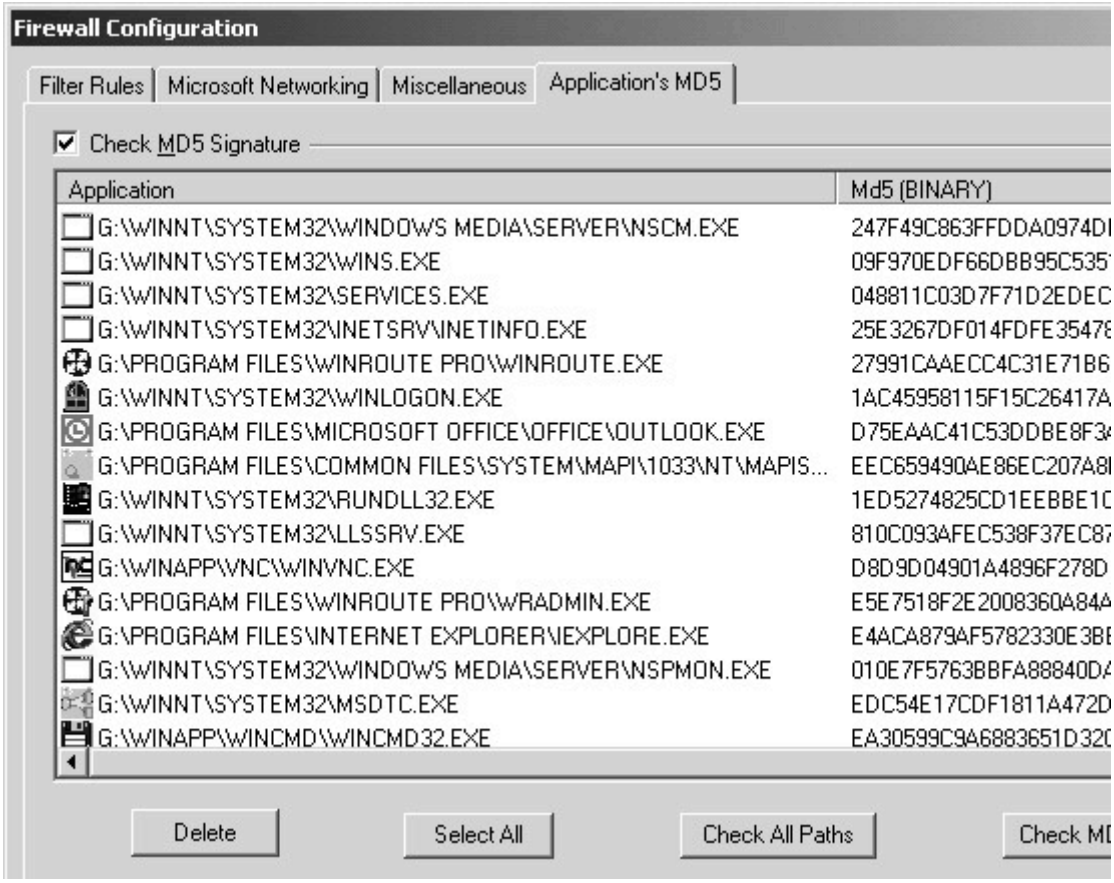
- Tlačítka "přehrávače" - umožňují pohyb po zaznamenaných událostech (první záznam, předchozí záznam, následující záznam, poslední záznam). V horní části okna se vždy zobrazují detailní informace o té události, která byla těmito tlačítky vybrána.
- Delete - vymazání vybrané události
- Delete All - smazání všech zaznamenaných událostí
- To Clipboard - přenesení informací o vybrané události do schránky
- Close - ukončení dialogu. Historie zachycených paketů zůstává zachována.

MD5 podpisy aplikací

Kromě kontroly příchozích a odchozích paketů umí Kerio Personal Firewall také zjišťovat, zda jsou povolené pakety vysílány pouze oprávněnými aplikacemi. Do vašeho počítače se totiž může infiltrovat aplikace (např. mailem, z diskety apod.), která se vydává za nějaký běžný program (tj. přepíše jeho originální spustitelný soubor) a snaží se odeslat z vašeho počítače vaše privátní data. Tyto aplikace se nazývají trojské koně. Většinou je lze odhalit při antivirové kontrole, ale to už samozřejmě může být pozdě.

Kerio Personal Firewall používá metodu vytváření a kontroly MD5 podpisů aplikací. Zjednodušeně lze říci, že MD5 podpis je kontrolní součet spustitelného souboru aplikace. Při prvním použití aplikace (resp. při prvním pokusu této aplikace o síťovou komunikaci) Personal Firewall zobrazuje dialog, kde uživatel může komunikaci povolit nebo zakázat. Je-li komunikace uživatelem povolena, Personal Firewall vytvoří a zaznamená MD5 podpis této aplikace. Při každém dalším pokusu o komunikaci je pak MD5 podpis kontrolován. Došlo-li ve spustitelném souboru aplikace ke změně (např. infikace virem nebo záměna za jiný program), Personal Firewall komunikaci nepovolí a zobrazí varovné hlášení s dotazem, zda má být změna akceptována (např. v případě upgrade aplikace na novější verzi) či nikoliv.

MD5 podpisy lze prohlížet a mazat v záložce Application's MD5 (vytvářeny mohou být pouze automaticky).

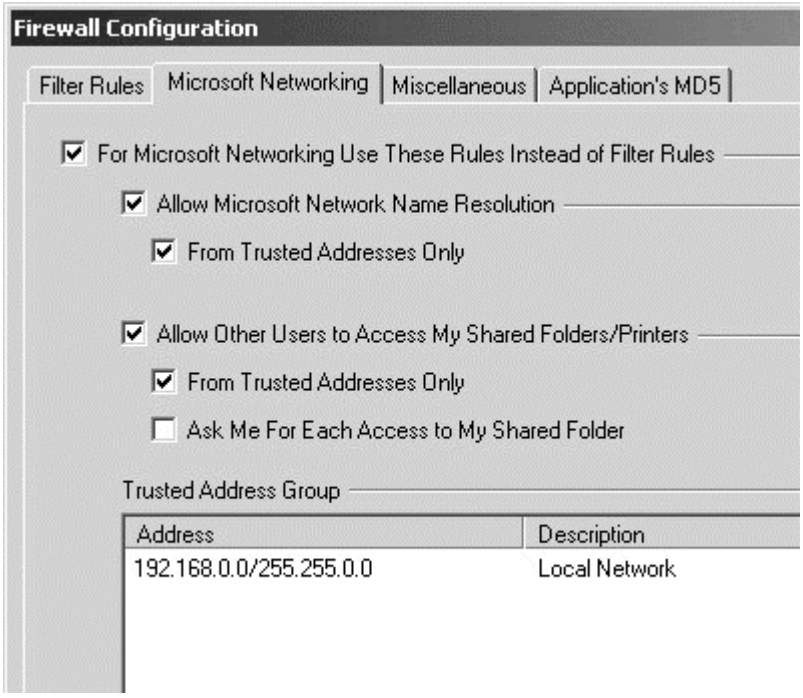

Firewall Configuration
Filter Rules
Microsoft Networking
Miscellaneous
Application's MD5
Check MD5 Signature
Application
Md5 (BINARY)
G:\WINNT\SYSTEM32\WINDOWS MEDIA\SERVER\NSCM.EXE
247F49C863FFDDA0974D
G:\WINNT\SYSTEM32\WINS.EXE
09F970EDF66DBB95C535
G:\WINNT\SYSTEM32\SERVICES.EXE
048811C03D7F71D2EDEC
G:\WINNT\SYSTEM32\INETSRV\INETINFO.EXE
25E3267DF014FDFE3547
G:\PROGRAM FILES\WINROUTE PRO\WINROUTE.EXE
27991CAAECC4C31E71B6
G:\WINNT\SYSTEM32\WINLOGON.EXE
1AC45958115F15C26417A
G:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\OUTLOOK.EXE
D75EAAC41C53DDBE8F3
G:\PROGRAM FILES\COMMON FILES\SYSTEM\MAPI\1033\NT\MAPIS...
EEC659490AE86EC207A8
G:\WINNT\SYSTEM32\RUNDLL32.EXE
1ED5274825CD1EEBBE1C
G:\WINNT\SYSTEM32\LLSSRV.EXE
810C093AFEC538F37EC87
G:\WINAPP\VNC\WINVNC.EXE
D8D9D04901A4896F278D
G:\PROGRAM FILES\WINROUTE PRO\WRADMIN.EXE
E5E7518F2E2008360A84A
G:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE
E4ACA879AF5782330E3BE
G:\WINNT\SYSTEM32\WINDOWS MEDIA\SERVER\NSPMON.EXE
010E7F5763BBFA88840DA
G:\WINNT\SYSTEM32\MSDTC.EXE
EDC54E17CDF1811A472D
G:\WINAPP\WINCMD\WINCMD32.EXE
EA30599C9A6883651D320
Delete
Select All
Check All Paths
Check MD

- Check MD5 signature - tato volba zapíná a vypíná vytváření a kontrolu MD5 podpisů aplikací.
- Delete - smaže MD5 podpis vybrané aplikace.
- Select All - vybere všechny záznamy v okně.
- Check All Paths - zkontroluje všechny aplikace, zda v dané cestě spustitelný soubor skutečně leží. Pokud ne (např. po deinstalaci aplikace), je uživatel dotázán, zda má být MD5 podpis odstraněn.
- Check MD5 Now - zkontroluje, zda jsou MD5 podpisy vybraných aplikací platné. Aplikaci lze označit myší, více aplikací s přidržením klávesy Ctrl nebo Alt. Všechny aplikace v seznamu lze označit kombinací kláves Ctrl+A. Je-li podpis neplatný, zobrazí se varovné hlášení, v opačném případě zpráva, že kontrola MD5 podpisů byla dokončena.

Síť Microsoft Network

Velmi častým případem je, že je počítač s operačním systémem Windows zapojen do lokální sítě Microsoft Network, kde se využívá sdílení souborů a tiskáren. Při komunikaci v této síti se využívá několik různých služeb a optimální nastavení Personal Firewallu není v tomto případě právě triviální záležitost.

Z výše uvedených důvodů umožňuje Kerio Personal Firewall oddělené nastavení pravidel pro Microsoft Network. Tato nastavení se provádějí po stisku tlačítka Advanced v záložce Microsoft Networking.



- For Microsoft Networking Use These Rules Instead Of Filter Rules - tato volba určuje, že se pro Microsoft Network mají používat speciální pravidla definovaná v této záložce.
- Allow Microsoft Network Name Resolutions - povolí zjištění IP adresy počítače z jeho NetBIOS jména (službou NetBIOS).
- From Trusted Addresses Only - převod NetBIOS jména na IP adresu je povolen pouze ze skupiny důvěryhodných adres (viz níže)
- Allow Other Users to Access My Shared Folders / Printers - povolí přístup ke sdíleným adresářům a tiskárnám
- From Trusted Addresses Only - přístup je povolen pouze z níže definovaných důvěryhodných adres
- Ask Me For Each Access to My Shared Folders - Personal Firewall se bude při každém přístupu ke sdílenému adresáři dotazovat, zda má být přístup povolen či nikoliv.
- Trusted Address Group - skupina IP adres, které jsou považovány za důvěryhodné. Tlačítky Add, Edit a Del lze přidat, změnit nebo odebrat IP adresu, rozsah IP adres nebo subsíť. Platnost této skupiny je omezena pouze na záložku Microsoft Networking, nelze ji tedy použít při definici pravidel.

Příklady optimálního nastavení

- Máte-li samostatný počítač, který není zapojen do lokální sítě (např. notebook připojený přes modem do Internetu), zapněte pouze volbu For Microsoft Networking Use These Rules Instead Of Filter Rules. Ostatní volby ponechte vypnuté. Tak zajistíte, že komunikace v síti Microsoft bude zcela zakázána.
- Je-li váš počítač připojen do lokální sítě, kde svým kolegům důvěřujete a chcete všem zpřístupnit své sdílené adresáře a tiskárny, zapněte všechny volby kromě Ask Me For Each Access to My Shared Folders. V poli Trusted Address Group definujte vaši lokální síť (např. jako subsíť s příslušnou maskou nebo jako rozsah IP adres).
- Chcete-li zpřístupnit své sdílené prostředky a mít přitom úplnou kontrolu nad tím, kdo na ně přistupuje, postupujte jako v předchozím případě, ale zapněte také volbu Ask Me For Each Access to My Shared Folders.

Poznámka: Oddělené nastavení pro Microsoft Networking je implementováno ve verzi 2.0.15 a vyšších.

Ochrana internetové brány

Kerio Personal Firewall může být rozvěž použit k ochraně internetové brány, tj. počítače, který umožňuje přístup do Internetu pro lokální síť (jako směrovač nebo směrovač s překladem IP adres). Typické použití je společně s aplikací Microsoft Internet Connection Sharing (Sdílení internetového připojení, zkr. ICS), což je komponenta operačních systémů Windows 98 SE, ME a 2000. ICS umožní všem počítačům přístup do Internetu přes jedinou veřejnou IP adresu, nezajišťuje ale žádnou ochranu proti útoku zvenčí. V kombinaci s programem Personal Firewall získáte bezpečné sdílené připojení do Internetu.

Personal Firewall je navržen k ochraně jednoho počítače. Přes internetovou bránu (směrovač) ale samozřejmě prochází velké množství paketů, které nejsou určeny přímo aplikacím na tomto počítači. Aby nebylo nutno pro tento případ definovat složité paketové filtry, je možné Personal Firewall přepnout do speciálního módu pro internetové brány. To se provede v rozšířených nastaveních (po stisku tlačítka Advanced) v záložce Miscellaneous zapnutím volby "Is running on Internet gateway".

POZNÁMKA: Nezapínejte tuto volbu, jestliže Personal Firewall skutečně neběží na internetové bráně. Degradujete tím úroveň zabezpečení svého počítače.

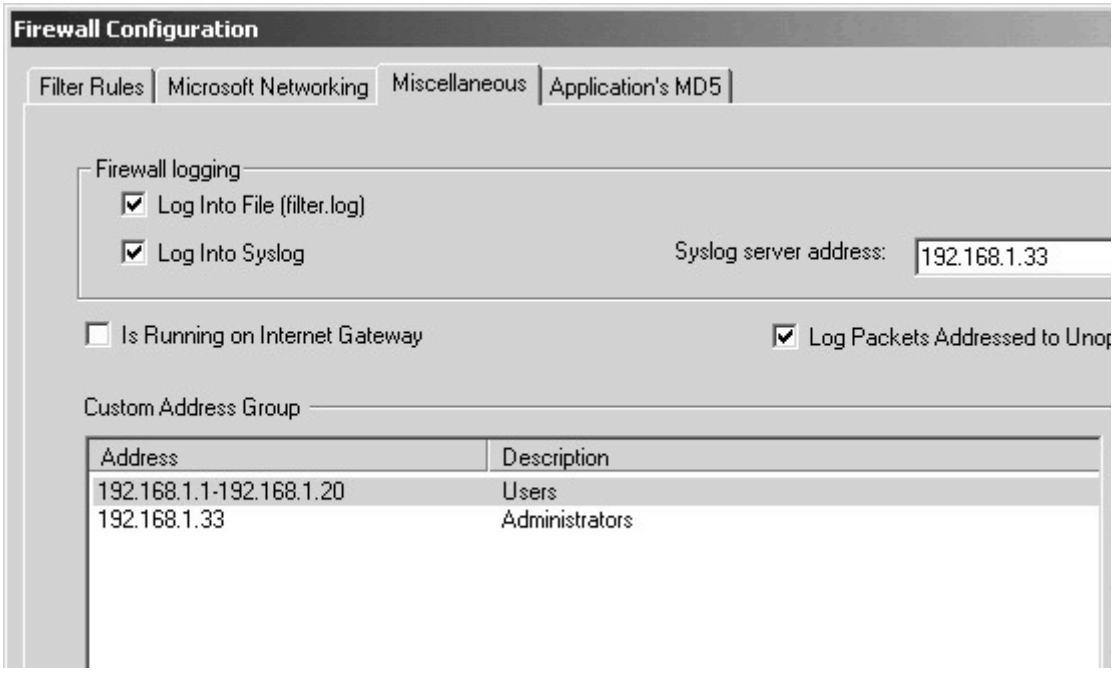
KAPITOLA 4

Záznamy a analýza paketů

Základní informace

Kerio Personal Firewall umožňuje vytvářet detailní záznamy o průchozích a filtrovaných paketech. Uživatel (resp. správce) má poměrně široké možnosti nastavení, co a kam má být zaznamenáváno. Záznamy mohou být buď ukládány do souboru (má název "filter.log" a je uložen v adresáři, kde je Personal Firewall nainstalován) nebo odesílány na Syslog server.

Základní nastavení záznamů se provádí v rozšířených nastaveních (po stisku tlačítka Advanced) v záložce Miscellaneous v sekci Firewall Logging.



- Log Into File (filter.log) - záznamy budou ukládány do souboru filter.log (v adresáři, kde je Personal Firewall nainstalován). Velikost tohoto souboru je omezena pouze dostupným místem na disku.
- Log Into Syslog - záznamy budou posílány na Syslog server běžící na zadané IP adrese
- Log packets addressed to unopened ports - zapne zaznamenávání paketů, které jsou směrovány na porty, na nichž neběží žádná aplikace (typicky útok typu "portscanning").

Soubor filter.log

Soubor "filter.log" slouží k ukládání záznamů Kerio Personal Firewallu na lokálním počítači. Vytváří se v adresáři, kde je Personal Firewall nainstalován (typicky "\Program Files\Kerio\Personal Firewall"), a to až v okamžiku zapsání prvního záznamu.

"filter.log" je textový soubor, v němž každý záznam je uložen na samostatném řádku. Formát každého řádku je následující:

```
1,[08/Jun/2001 16:52:09] Rule 'Internet Information Services': Blocked: In TCP, richard.kerio.cz [192.168.2.38:3772]->localhost:25, Owner: G:\WINNT\SYSTEM32\INETSRV\INETINFO.EXE
```

- 1 - typ pravidla (1 = zakazující, 2 = povolující)
- [08/Jun/2001 16:52:09] - datum a čas, kdy byl paket zachycen (doporučujeme zkontrolovat správné nastavení systémového data a času na vašem počítači!)
- Rule "Internet Information Services" - název pravidla, které bylo aplikováno (z pole Description)
- "Blocked:" / "Permitted:" - zda byl paket blokován či propuštěn (koresponduje s číslem na začátku řádku)
- "In" / "Out" - zda se jedná o příchozí či odchozí paket
- "IP" / "TCP" / "UDP" / "ICMP" atd. - komunikační protokol (pro nějž bylo pravidlo definováno)
- richard.kerio.cz [192.168.2.38:3772] - DNS jméno počítače, který paket vyslal, v hranatých závorkách pak jeho IP adresa a za dvojtečkou zdrojový port
- locahost:25 - cílová IP adresa a port (localhost = tento počítač)
- Owner: název lokální aplikace, jíž je paket určen (včetně plné cesty). Jedná-li se o systémou službu, je zde uvedeno "SYSTEM".

Společně se souborem "filter.log" se vytváří také indexový soubor "filter.log.idx". Chcete-li smazat soubor "filter.log" (záznamy v něm jsou již pro vás nevýznamné), smažte také tento soubor, jinak nebude zaznamenávání fungovat správně.

Rejstřík