Kerio Personal Firewall 4™

Uživatelský manuál

Kerio Technologies

Datum vydání: 24. listopadu 2003

Aktuální verze produktu: *Kerio Personal Firewall 4.0.8*. Změny vyhrazeny.

Obsah

Kapitola 1

Úvod

1.1 Kerio Personal Firewall 4.0

Kerio Personal Firewall je aplikace určená k ochraně osobního počítače před útoky ze sítě (typicky z Internetu), viry a únikem dat. Tyto bezpečnostní funkce zajišťují čtyři hlavní moduly:

Síťová bezpečnost Tento modul sleduje veškerou síťovou (resp. TCP/IP) komunikaci počítače, na kterém je *Kerio Personal Firewall* nainstalován. Pro síťovou komunikaci může uživatel definovat dva typy pravidel:

- pravidla pro aplikace — pro každou aplikaci lze povolit nebo zakázat síťovou komunikaci, případně nastavit, aby se *Kerio Personal Firewall* dotázal uživatele.
- pravidla paketového filtru — zkušenější uživatelé mohou definovat detailní pravidla pro síťovou komunikaci (specifikace IP adres, protokolů, portů atd.). Tato pravidla mohou platit pro konkrétní aplikaci nebo obecně (pro libovolnou aplikaci).

Kerio Personal Firewall obsahuje také sadu předdefinovaných pravidel pro síťovou komunikaci (např. pro DNS, DHCP apod.). Tato pravidla jsou oddělená od uživatelsky definovaných pravidel a lze je jednoduše aktivovat či vyřadit.

Jestliže *Kerio Personal Firewall* zachytí komunikaci, pro kterou neexistuje odpovídající pravidlo, dotáže se uživatele, zda tuto komunikaci povolí či zakáže. Na základě odpovědi uživatele může být automaticky vytvořeno pravidlo pro aplikaci nebo pravidlo paketového filtru.

Bezpečnost systému Modul *Bezpečnost systému* kontroluje spouštění aplikací v operačním systému. Sledovány jsou tři typy událostí:

- spuštění aplikace
- změna ve spustitelném souboru aplikace od posledního spuštění (záměna aplikace)
- spuštění jiné aplikace běžící aplikací

Podobně jako v případě síťové komunikace lze definovat pravidla pro jednotlivé aplikace, která příslušnou akci povolují nebo zakazují, případně vyžadují reakci uživatele. Pokud neexistuje odpovídající pravidlo, *Kerio Personal Firewall* se dotáže uživatele, zda spuštění aplikace povolí či zakáže.

Poznámka: Kerio Personal Firewall 4.0 (narozdíl od starších verzí) kontroluje spouštění všech aplikací, bez ohledu na to, zda se účastní síťové komunikace. V případě infikace virem reaguje spolehlivěji než antivirový program (jedná-li se o nový virus, který dosud není ve virové databázi, antivirus jej nezachytí — *Kerio Personal Firewall* však vždy pozná, že došlo ke změně spustitelného souboru a upozorní uživatele).

Detekce útoků Systém detekce útoků (*IDS — Intrusion Detection System*) dokáže rozpoznat, blokovat a zaznamenat známé typy útoků. K tomuto účelu má *Kerio Personal Firewall* databázi známých útoků, která je pravidelně aktualizována (aktualizace je vždy začleněna do nové verze produktu).

Filtrování obsahu WWW stránek Modul pro filtrování obsahu umožňuje:

- blokování reklam (dle pravidel pro URL), skriptů a dalších prvků WWW stránek
- blokování pop-up oken
- blokování skriptů (*JavaScript*, *VB Script*)
- ochranu před ukládáním nežádoucích cookies a odesíláním privátních dat

Pro důvěryhodné servery či případy, kdy filtrování způsobí nefunkčnost určitých stránek, je možno definovat výjimky (specifická nastavení).

Mezi další významné funkce a vlastnosti *Kerio Personal Firewallu* patří:

Blokování veškeré komunikace *Kerio Personal Firewall* umožňuje jedním tlačítkem (resp. volbou z menu) zablokovat síťovou komunikaci počítače, na kterém je nainstalován (tzv. síťový zámek). Tuto funkci lze použít při zjištění podezřelé či nežádoucí síťové aktivity — po provedení příslušných opatření může být komunikace opět povolena.

Logování Každý z modulů firewallu vytváří vlastní záznam (log), který se ukládá jako soubor v textovém formátu. Záznamy lze prohlížet přímo v konfiguračním okně *Kerio Personal Firewallu*. Volitelně je možno záznamy také odesílat na *Syslog* server.

Přehled spojení a statistiky Přehled spojení dává uživateli informaci o navázaných spojeních a portech otevřených jednotlivými aplikacemi. U spojení se rovněž zobrazuje aktuální přenosová rychlost a celkový objem přenesených dat v každém směru. Seznam je automaticky obnovován v pravidelných intervalech.

Statistiky informují uživatele o počtu objektů blokovaných WWW filtrem, počtu zachycených privátních informací a počtu detekovaných útoků za zvolené časové období.

Automatická aktualizace *Kerio Personal Firewall* pravidelně kontroluje, zda není k dispozici novější verze, a pokud ano, nabídne uživateli její stažení a instalaci. Kontrolu nové verze lze také kdykoliv provést ručně.

Upozornění: Žádná z verzí tohoto produktu nemůže být provozována na operačních systémech serverového typu (tj. Windows NT Server, Windows 2000 Server a Windows Server 2003).

1.2 Plná a volně šiřitelná verze

Kerio Personal Firewall je k dispozici ve dvou verzích: plné (placené) a volně šiřitelné.

Instalační balík je pro obě verze společný. Po instalaci se produkt chová jako demoverze (tj. plná verze s časovým omezením na 30 dnů). Pokud nebude produkt během této doby zaregistrován, stává se z něj volně šiřitelná verze. Zakoupením licence a registrací produktu se z instalované demoverze nebo volně šiřitelné verze stává plná verze (podrobnosti viz kapitola 2.3).

Volně šiřitelná verze má oproti plné verzi tato omezení:

- Může být použita pouze pro osobní a/nebo nekomerční účely.
- Není funkční filtrování obsahu WWW stránek, včetně příslušných záznamů a statistik (viz kapitola 9).
- Nemůže být použita na internetové bráně (viz kapitola 4.3).
- Záznamy nelze odesílat na *Syslog* server (viz kapitola 11.3).
- Konfiguraci nelze ochránit heslem a není možná vzdálená správa.

Technická podpora

Na produkt *Kerio Personal Firewall* je standardně poskytována pouze e-mailová technická podpora. Majitelé licence pro více než 1 počítač (multilicence) mají rovněž nárok na telefonickou technickou podporu. Kontakt naleznete na WWW stránkách `http://www.kerio.com/`.

1.3 Systémové požadavky

Pro instalaci aplikace *Kerio Personal Firewall* je požadováno:

- CPU Intel Pentium nebo 100% kompatibilní
- 64 MB RAM
- 8 MB místa na disku (pouze pro instalaci; doporučujeme dalších minimálně 10 MB pro soubory záznamů)
- operační systém Windows 98 / Me / NT 4.0 / 2000 / XP

1.4 Konfliktní software

Kerio Personal Firewall vykazuje konflikty s určitými druhy aplikací, které používají stejné nebo podobné technologie. Při kombinaci s níže uvedenými aplikacemi nezaručujeme správnou funkci *Kerio Personal Firewallu* ani operačního systému.

Neinstalujte *Kerio Personal Firewall* na tentýž operační systém společně s těmito aplikacemi:

Personální firewally Osobní firewally (např. *Internet Connection Firewall* — součást Windows XP, *Zone Alarm*, *Sygate Personal Firewall*, *Norton Personal Firewall* apod.) poskytují obdobnou funkčnost jako *Kerio Personal Firewall*. Rozhodnete-li se používat *Kerio Personal Firewall*, nekombinujte jej s dalšími firewally.

Síťové firewally Síťový firewall (např. *Kerio WinRoute Firewall*, *Kerio WinRoute Pro*, *Kerio WinRoute Lite*, *Microsoft ISA Server*, *CheckPoint Firewall-1*, *WinProxy* firmy Ositis, *Sygate Office Network* a *Sygate Home Network* atd.) sám chrání také počítač, na kterém je nainstalován, a proto není třeba jej doplňovat personálním firewallem.

Poznámka: Kerio Personal Firewall může být kombinován se směrovačem, se směrovačem provádějícím překlad IP adres (NAT) nebo proxy serverem — např. *Internet Connection Sharing* (*Sdílené internetového připojení* — součást novějších verzí operačního systému Windows) za účelem vytvoření jednoduchého síťového firewallu. Podrobné informace naleznete v kapitole 4.3.

1.5 Instalace, upgrade a odinstalování

Instalace

Instalaci provedete jednoduše spuštěním instalačního programu (např. `kerio-pf-4.0.0-en-win.exe`). Během instalace můžete vybrat adresář, do kterého bude aplikace *Kerio Personal Firewall* nainstalována

(standardně `C:\Program Files\Kerio\Personal Firewall 4`).

Po instalaci je třeba systém restartovat, aby byl zaveden nízkoúrovňový ovladač *Kerio Personal Firewallu*.

Poznámka: V operačních systémech Windows 98, Me, NT 4.0 a 2000 může být vyžadována aktualizace systémového instalátoru (*Windows Installer*), pokud již nebyl aktualizován dříve (např. při instalaci jiné aplikace). Velikost této aktualizace je cca 1.8 MB. Aktualizaci instalátoru je třeba stáhnout a nainstalovat, jinak nelze v instalaci aplikace *Kerio Personal Firewall* pokračovat!

Poznámka:

Při instalaci se v operačních systémech typu Windows NT zapíná vytváření výpisu paměti v případě havárie systému. Výpis paměti může uživatel odeslat do firmy *Kerio Technologies* — jeho analýza může pomoci k nalezení a odstranění chyby, která havárii operačního systému způsobila.

Po zaškrtnutí příslušné volby (viz kapitola 4.3) se v operačním systému nastaví generování výpisu paměti.

Upgrade

Instalace nové verze, resp. oprava stávající instalace se provádí stejným způsobem jako nová instalace (viz výše). Spuštěné komponenty aplikace není třeba ukončovat — instalační program je zastaví sám.

Poznámka: Kerio Personal Firewall má vestavěný mechanismus pro automatickou kontrolu a stahování nových verzí (podrobnosti viz kapitola 1.6).

Odinstalování

Kerio Personal Firewall lze odinstalovat pomocí nástroje *Přidat nebo odebrat programy* (*Add / Remove programs*) v *Ovládacích panelech* (*Control Panel*). Při odinstalování nebudou smazány soubory, které vznikly až za běhu aplikace (tj. konfigurační soubory,

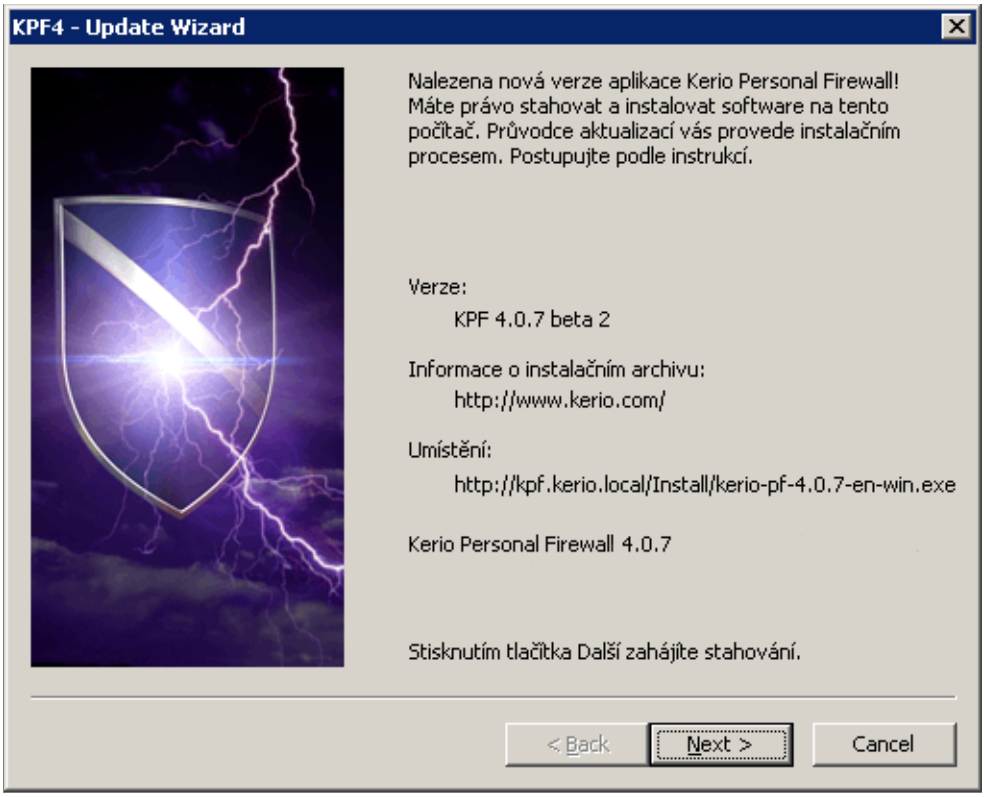
záznamy atd.). Ty je třeba smazat ručně, případně mohou zůstat uchovány pro další instalaci.

1.6 Kontrola nových verzí

Kerio Personal Firewall automaticky kontroluje, zda je k dispozici novější verze, a pokud ano, nabídne ji uživateli ke stažení. Kontrola nové verze se provádí při každém spuštění *Personal Firewall Engine* a pak pravidelně v intervalu 24 hodin.

Kontrolu nové verze lze také kdykoliv spustit ručně tlačítkem *Zjistit teď* v sekci *Přehled / Předvolby* konfiguračního okna *Kerio Personal Firewallu* (podrobnosti viz kapitola 4.3).

Je-li verze *Kerio Personal Firewallu* na vašem počítači aktuální, spojení se serverem se ukončí a naplánuje se příští kontrola nové verze. V opačném případě je zobrazen dialog s informacemi o nové verzi.



Stisknutím tlačítka *Další* se zahájí stahování nové verze. *Kerio Personal Firewall* vždy kontroluje signaturu staženého souboru — tím je zajištěno, že stažený soubor je skutečně originální (nejedná se o podvrh, není napaden virem, poškozen atd.).

Po stažení nové verze se spustí instalační program. Po instalaci je třeba počítač restartovat.

Tlačítkem *Storno* lze stahování, resp. instalaci nové verze zrušit. V takovém případě nebude tato aktualizace znovu automaticky nabízena — lze ji však kdykoliv spustit ručně. Při nalezení další nové verze *Kerio Personal Firewall* opět nabídne aktualizaci automaticky.

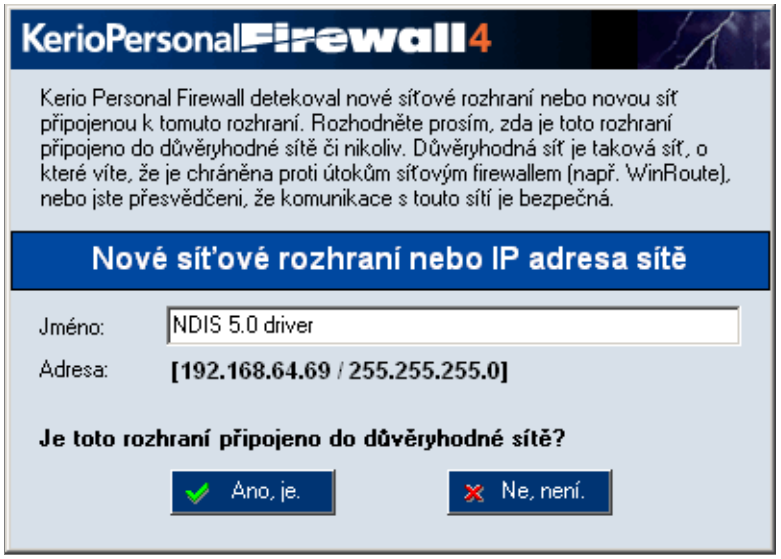
Podrobnosti o instalaci aplikace *Kerio Personal Firewall* naleznete v kapitole 1.5.

Poznámka: Kerio Personal Firewall má speciální interní pravidla, která vždy povolují přístup na server pro aktualizaci a registraci produktu. Uživatel tedy nemůže nevhodným nastavením firewallu automatickou aktualizaci zablokovat.

1.7 Počáteční konfigurace

Při prvním spuštění (tj. po instalaci) detekuje *Kerio Personal Firewall* aktivní síťová rozhraní počítače, na kterém je nainstalován. Pro každé rozhraní zobrazí dotaz, zda je toto rozhraní připojeno do důvěryhodné sítě či nikoliv.

Důvěryhodná síť je taková síť, o které uživatel předpokládá, že komunikace s počítači v ní je bezpečná. Typicky se jedná o lokální síť, která je proti průniku z Internetu chráněna síťovým firewallem. *Kerio Personal Firewall* umožňuje definovat různé akce pro důvěryhodnou síť a pro zbytek Internetu (podrobnosti viz kapitola 5.4).



V poli *Jméno* je uveden název příslušného síťového adaptéru, v položce *Adresa* jeho IP adresa a maska subsítě, do které je připojen.

Stisknutím tlačítka *Ano, je* se subsíť, do níž je rozhraní připojeno, zařadí do skupiny důvěryhodných IP adres (*Důvěryhodná zóna*). Tlačítko *Ne, není* způsobí, že tato subsíť bude považována za součást Internetu.

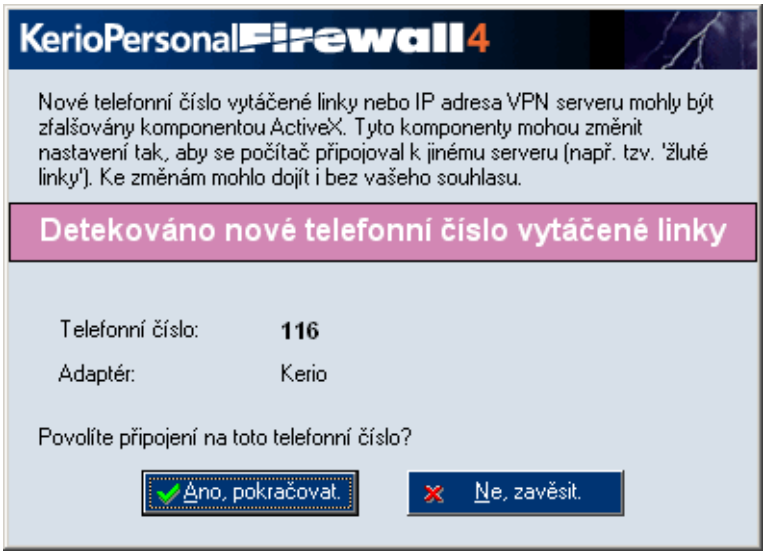
Poznámky:

1. Nastavení skupiny důvěryhodných IP adres lze kdykoliv pozměnit (detailní informace naleznete v kapitole 5.4).

2. Je-li kdykoliv později přidáno či aktivováno další rozhraní nebo je rozhraní přepojeno do jiné subsítě, *Kerio Personal Firewall* jej rovněž automaticky detekuje a zobrazí výše popsaný dialog.

3. V případě vytáčené linky se také kontroluje, zda od posledního vytočení nedošlo ke změně telefonního čísla. Jestliže *Kerio Personal Firewall* detekuje změnu čísla, dotáže se uživatele, zda tuto změnu akceptuje. Toto je ochrana proti nežádoucí změně parametrů telefonického připojení (např. ActiveX objektem na WWW stránce).

   Upozornění na nové telefonní číslo (nové telefonické připojení):



   Upozornění na změnu telefonního čísla již existujícího telefonického připojení:

   V poli *Telefonní číslo* je uvedeno nové telefonní číslo (tzn. telefonní číslo, které je nyní v příslušném telefonickém připojení nastaveno). Pole *Adaptér* zobrazuje název telefonického připojení.

   Po stisknutí tlačítka *Ano, pokračovat* *Kerio Personal Firewall* změnu čísla akceptuje a povolí vytočení linky. Tlačítko *Ne, zavěsit* znamená zamítnutí změny — linka bude zavěšena.


KerioPersonalFirewall4
Telefonní číslo vytáčené linky nebo IP adresa VPN serveru mohly být zfalšovány komponentou ActiveX. Tyto komponenty mohou změnit nastavení připojení tak, aby se počítač připojoval k jinému serveru (např. tzv. 'žluté linky'). Ke změnám mohlo dojít i bez vašeho souhlasu.
Telefonní číslo vytáčené linky bylo změněno
Telefonní číslo: 116
Adaptér: Kerio
Povolíte připojení na toto telefonní číslo?
Ano, pokračovat.
Ne, zavěsit.

Kapitola 2

Komponenty firewallu a základní ovládání

2.1 Komponenty aplikace Kerio Personal Firewall

Nízkoúrovňový ovladač Zavádí se do jádra operačního systému při jeho startu. Je umístěn mezi ovladači síťových rozhraní a TCP/IP subsystémem a zachytává a zpracovává veškerou přijatou či vysílanou IP komunikaci.

Nízkoúrovňový ovladač je uložen v systémovém adresáři Windows:

- v operačních systémech Windows NT a Windows 2000 typicky v adresáři

  `C:\WINNT\system32\drivers` (soubor `fwdrv.sys`)

- v operačním systému Windows XP typicky v adresáři

  `C:\WINDOWS\system32\drivers` (soubor `fwdrv.sys`)

- v operačních systémech Windows 98 a Windows Me typicky v adresáři

  `C:\WINDOWS\system` (soubor `fwdrv.vxd`)

Personal Firewall Engine Vlastní výkonné jádro *Kerio Personal Firewallu*. Běží jako služba nebo jako skrytá aplikace (Windows 98 a Me).

Služba *Personal Firewall Engine* je uložena v souboru `kpf4ss.exe` v instalačním adresáři aplikace *Kerio Personal Firewall*. Součástí *Personal Firewall Engine* je také tzv. rozhraní ovladače, které je uloženo v samostatném souboru `kfe.dll`.

Personal Firewall GUI Uživatelské rozhraní aplikace *Kerio Personal Firewall* (*GUI — Graphical User Interface*).

Komponentu *Personal Firewall GUI* spouští automaticky služba *Personal Firewall Engine* (při svém startu a dále v každém okamžiku, kdy detekuje, že uživatelské rozhraní neběží). Po spuštění se *Personal Firewall GUI* zobrazuje jako ikona tvaru štítu v pravé části nástrojové lišty (System Tray).

Pomocí ikony v System Tray lze otevřít konfigurační okno aplikace *Kerio Personal Firewall*, případně vyvolat některé další funkce (zablokování síťové komunikace, deaktivace firewallu atd.). Podrobnosti naleznete v kapitole 2.2.

Komponenta *Personal Firewall GUI* je reprezentována souborem `kpf4gui.exe` v instalačním adresáři aplikace *Kerio Personal Firewall*.

Modul pro obsluhu horkých kláves Tento modul je zodpovědný za dočasné vypínání filtru pop-up oken pomocí horké klávesy (viz kapitola 9.1). Jedná se o soubor `gkh.dll`.

Nástroj pro odesílání výpisů paměti Asistenční nástroj, který zajišťuje odeslání výpisu paměti při pádu aplikace *Kerio Personal Firewall* do firmy *Kerio Technologies*. Nachází se v souboru `assist.exe`.

Podpora rychlého přepínání uživatelů

Kerio Personal Firewall má vestavěnou podporu pro tzv. rychlé přepínání uživatelů ve Windows XP (*Fast User Switching*).

Personal Firewall GUI může běžet ve více instancích. *Personal Firewall Engine* vždy komunikuje s tou instancí, která náleží aktivnímu uživateli..

Po startu operačního systému a služby *Personal Firewall Engine* se spustí první instance, která běží pod systémovým účtem (resp. pod účtem, pod kterým se spouští služba *Personal Firewall Engine*). Při přihlášení uživatele se spustí nová instance *Personal Firewall GUI*, která běží s právy tohoto uživatele. Tato instance je aktivní až do odhlášení uživatele (v tom případě je ukončena), případně do přepnutí uživatelů (pak je pouze deaktivována).

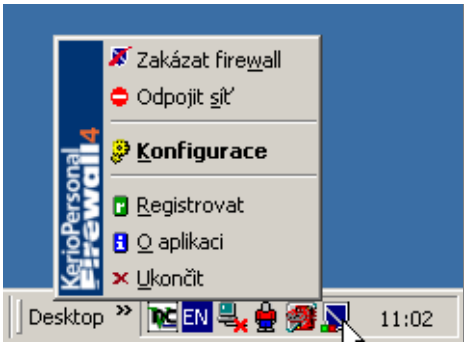
2.2 Ikona na nástrojové liště

Ikona aplikace *Kerio Personal Firewall* v pravé části nástrojové lišty (System Tray) je zobrazena vždy, když běží komponenta *Personal Firewall GUI*. Tuto komponentu spouští automaticky služba *Personal Firewall Engine*.

Ikona *Kerio Personal Firewallu* zobrazuje také síťovou aktivitu počítače, na kterém je firewall nainstalován. Síťová aktivita je zobrazována barevnými sloupci v dolní části ikony:

- zelený sloupec — odchozí (vysílaná) komunikace
- červený sloupec — příchozí (přijímaná) komunikace

Dvojitým kliknutím na ikonu levým tlačítkem myši se otevře konfigurační okno aplikace *Kerio Personal Firewall* (nastavení firewallu bude podrobně popsáno v kapitole 4). Po kliknutí na ikonu pravým tlačítkem myši se zobrazí menu s těmito funkcemi:



Zakázat firewall Deaktivace firewallu. Tato funkce vypíná všechny moduly *Kerio Personal Firewallu* — tj. filtrování síťové komunikace, sledování spouštěných aplikací, detekci útoků a filtrování obsahu WWW stránek.

Volba *Zakázat firewall* je určena pro krátkodobé vyřazení firewallu, typicky pro účely testování či odstraňování problémů (např. nefunkčnost síťového připojení). Nedoporučujeme ponechávat volbu *Disable Firewall* trvale zapnutou — firewall je pak neúčinný a váš počítač není chráněn.

Je-li *Kerio Personal Firewall* deaktivován, ikona na nástrojové liště je červeně přeškrtnutá.

Výběrem funkce *Zakázat firewall* se volba v menu se změní na *Povolit firewall* — výběrem této volby dojde k opětovné aktivaci firewallu.

Odpojit síť Zablokování veškeré síťové komunikace (tzv. síťový zámek).

Blokování síťové komunikace je signalizováno symbolem „jednosměrná ulice“ na ikoně *Kerio Personal Firewallu*.

Po aktivaci funkce *Odpojit síť* se volba v menu změní na *Zapojit síť* — výběrem této volby dojde k opětovnému povolení komunikace dle aktuálního nastavení firewallu.

TIP: Funkce *Odpojit síť* může být užitečná např. v případě, kdy omylem došlo k povolení síťové komunikace, která měla být zakázána. Volba *Odpojit síť* pozastaví aktuální spojení a zabrání navázání dalších spojení. Bylo-li vytvořeno komunikační pravidlo (tj. zaškrtnuta volba *Vytvořit pravidlo pro tuto komunikaci*), můžete jej smazat (viz kapitola 5.2, resp. 6) a poté komunikaci opět povolit.

Poznámka: Při startu služby *Personal Firewall Engine* se volby *Zakázat firewall* a *Odpojit síť* vždy nastaví do výchozího stavu. Z bezpečnostních důvodů není žádoucí, aby byl firewall po startu neaktivní. Blokování veškeré komunikace by mohlo způsobit problémy např. s přihlašováním uživatelů.

Konfigurace Tato volba otevírá konfigurační okno aplikace *Kerio Personal Firewall*. Konfigurace firewallu je detailně popsána v kapitole 4.

Registrovat Spuštění průvodce registrací produktu (podrobnosti viz kapitola 2.3). Je-li *Kerio Personal Firewall* již registrován, tato položka se v menu nezobrazuje.

O aplikaci Okno s informacemi o verzích jednotlivých komponent *Kerio Personal Firewallu* a licenci, případně datu skončení funkčnosti časově omezené verze.

Ukončit Ukončení aplikace. Tato volba zastaví službu *Personal Firewall Engine* a ukončí všechny instance *Personal Firewall GUI* (tzn. uzavřou se všechna otevřená okna aplikace a skryje se ikona na nástrojové liště). Je-li v tomto okamžiku zobrazen alespoň jeden dialog (např. *Upozornění na spojení*), čeká se na jeho potvrzení uživatelem.

Upozornění: Ukončením aplikace *Kerio Personal Firewall* přestává být váš počítač chráněn! *Kerio Personal Firewall* lze znovu aktivovat spuštěním služby v ovládacím panelu *Nástroje pro správu / Služby* (*Administrative Tools / Services*).

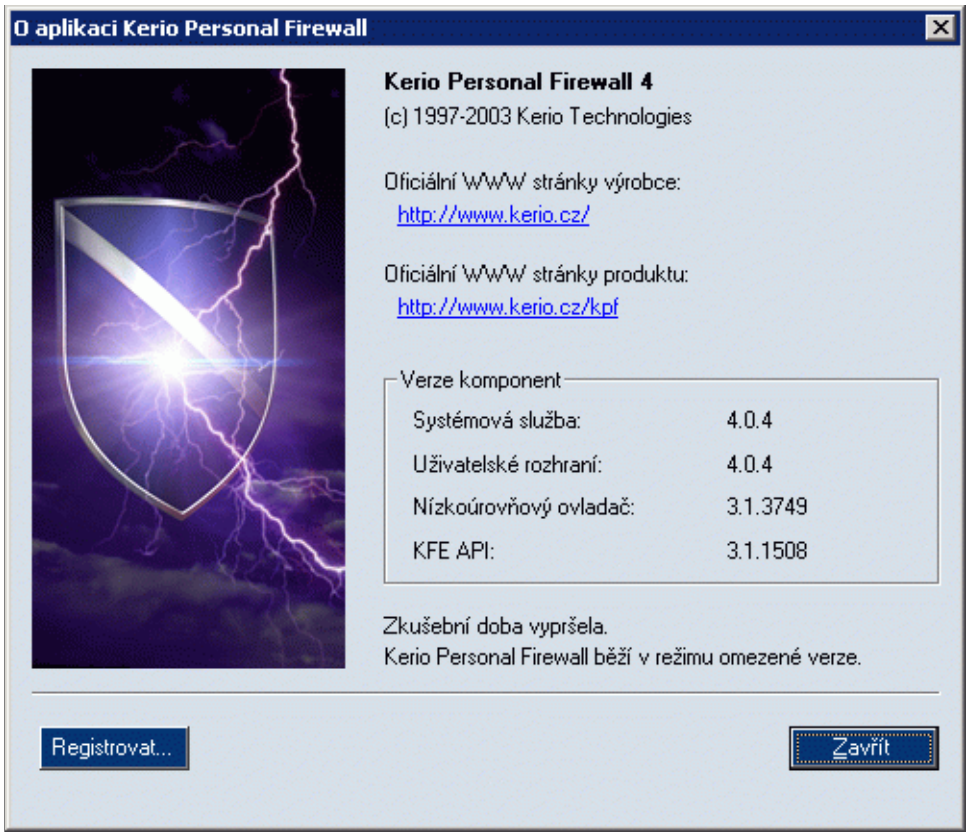
Je-li přístup ke správě firewallu chráněn heslem a uživatel je přihlášen, pak je kontextové menu rozšířeno o položku *Odhlásit*. Podrobné informace naleznete v kapitole 4.2.

2.3 Registrace produktu

Zakoupenou licenci produktu *Kerio Personal Firewall* je třeba registrovat. Registrací se aktivují funkce, které nejsou ve volně šiřitelné verzi dostupné (viz kapitola 1.2).

Poznámka: Produkt *Kerio Personal Firewall* je poskytován zdarma pro osobní a nekomerční použití. V takovém případě není nutné registraci provádět. Po uplynutí 30 dnů od instalace se však *Kerio Personal Firewall* začne chovat jako omezená verze — viz kapitola 1.2

Registraci *Kerio Personal Firewallu* lze provést pomocí *Průvodce registrací*. Průvodce se spustí volbou *Registrovat* z kontextového menu ikony na nástrojové liště (viz kapitola 2.2), stisknutím tlačítka *Registrovat...* v konfiguračním okně nebo v dialogu *O aplikaci Kerio Personal Firewall* (tento dialog se otevírá volbou *O aplikaci* z výše uvedeného menu).

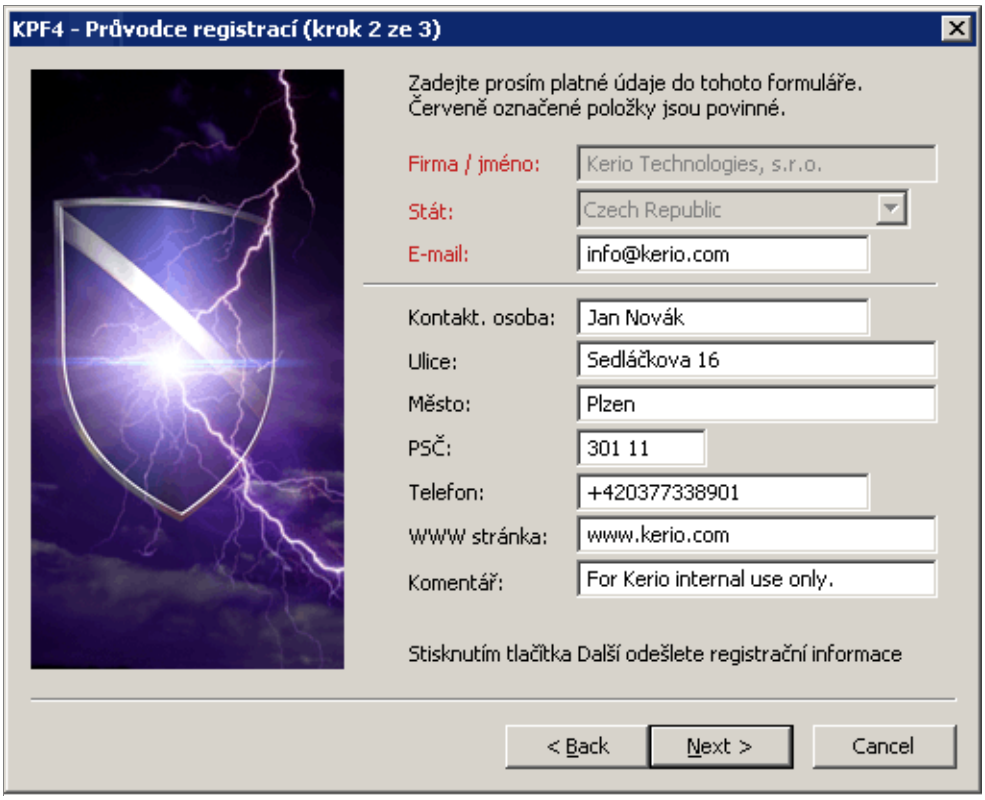


V prvním kroku průvodce je třeba vyplnit registrační číslo získané při zakoupení produktu (*Registrační klíč*).

Ve druhém kroku jsou požadovány informace o společnosti nebo osobě, na kterou je produkt registrován.

Položky *Firma / jméno* (název společnosti nebo jméno osoby),

Stát a *E-mail* (kontaktní e-mailová adresa) jsou povinné, tzn. musejí být vyplněny. Ostatní položky jsou volitelné.



Po stisknutí tlačítka *Další* naváže *Kerio Personal Firewall* spojení s registračním serverem, ověří správnost zadaných údajů a automaticky stáhne licenční klíč (digitální certifikát).

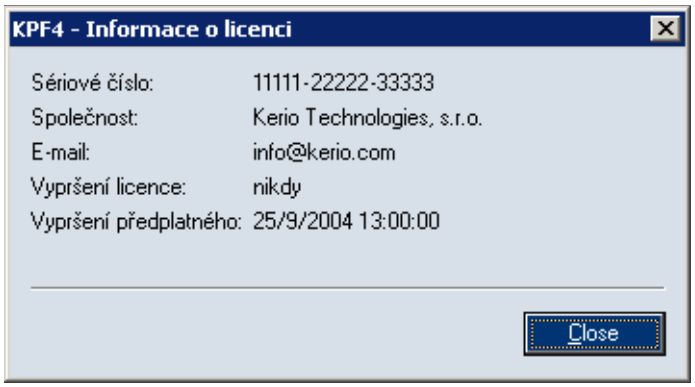
Ve třetím kroku průvodce se zobrazí informace o výsledku registrace.

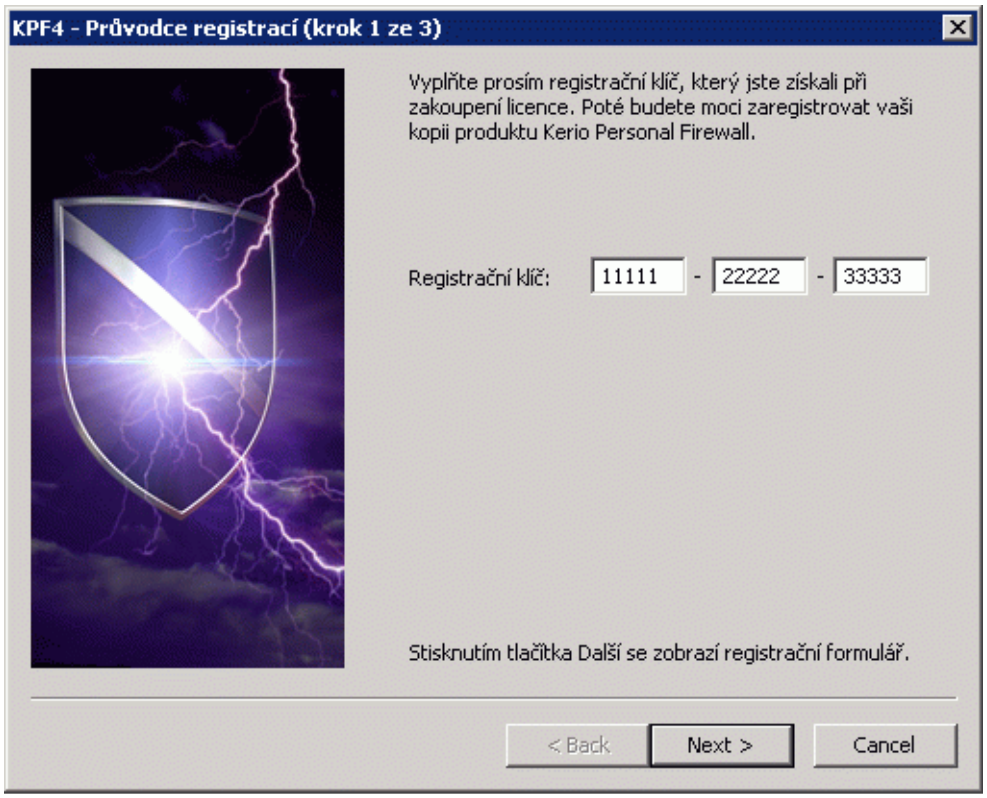
Jedná-li se o časově omezenou licenci, zobrazí se datum skončení platnosti licence (*Vypršení licence*) a skončení předplatného (*Vypršení předplatného*) — tj. nároku na bezplatné aktualizace produktu.

Stisknutím tlačítka *Dokončit* se průvodce ukončí.

Poznámka: Při dalším otevření dialogu *O aplikaci Kerio Personal Firewall* se v levém dolním rohu okna namísto tlačítka *Registrovat...* zobrazí tlačítko *Licence...*, které otevírá okno s informacemi o licenci:

- *Sériové číslo* — sériové číslo produktu
- *Společnost* — společnost, na kterou je produkt registrován
- *E-mail* — kontaktní e-mailová adresa





- *Vypršení licence* — datum skočení platnosti licence (*nikdy* = platnost licence není časově omezena)
- *Vypršení předplatného* — datum skončení platnosti předplatného, tj. nároku na bezplatné automatické aktualizace produktu

Kapitola 3

Chování firewallu a interakce s uživatelem

3.1 Chování firewallu

Při komunikaci v síti Internet se používají protokoly sady TCP/IP. Tyto protokoly jsou převážně používány i pro komunikaci v lokálních sítích. Základním (nosným) protokolem je IP (Internet Protocol), jehož pakety nesou veškeré další informace (zapouzdřují v sobě ostatní protokoly). *Kerio Personal Firewall* má úplnou kontrolu nad všemi IP pakety — tzn. je schopen je zachytit, zjistit z nich potřebné informace a poté je propustit nebo filtrovat. Samozřejmostí je také vytváření záznamů o prováděných akcích, detekovaných útocích apod.

Základním principem činnosti *Kerio Personal Firewallu* je tzv. stavová inspekce. Probíhá-li komunikace protokolem TCP, pak je o každém povoleném spojení vytvořen záznam, a firewall propustí pouze pakety patřící do tohoto spojení.

Kerio Personal Firewall pracuje v tzv. samoučícím režimu. Při zachycení dosud neznámé síťové komunikace se zobrazí dialogové okno, ve kterém může uživatel příslušnou komunikaci povolit či zakázat, a to jednorázově nebo trvale. Pro trvale povolenou či zakázanou komunikaci se automaticky vytvoří odpovídající pravidlo a při příštím zachycení této komunikace se již *Kerio Personal Firewall* uživatele nedotazuje. Detaily naleznete v kapitolách 3.2 a 6.

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

Obdobným způsobem *Kerio Personal Firewall* postupuje také při kontrole spouštěných aplikací (podrobnosti viz kapitola 7.1).

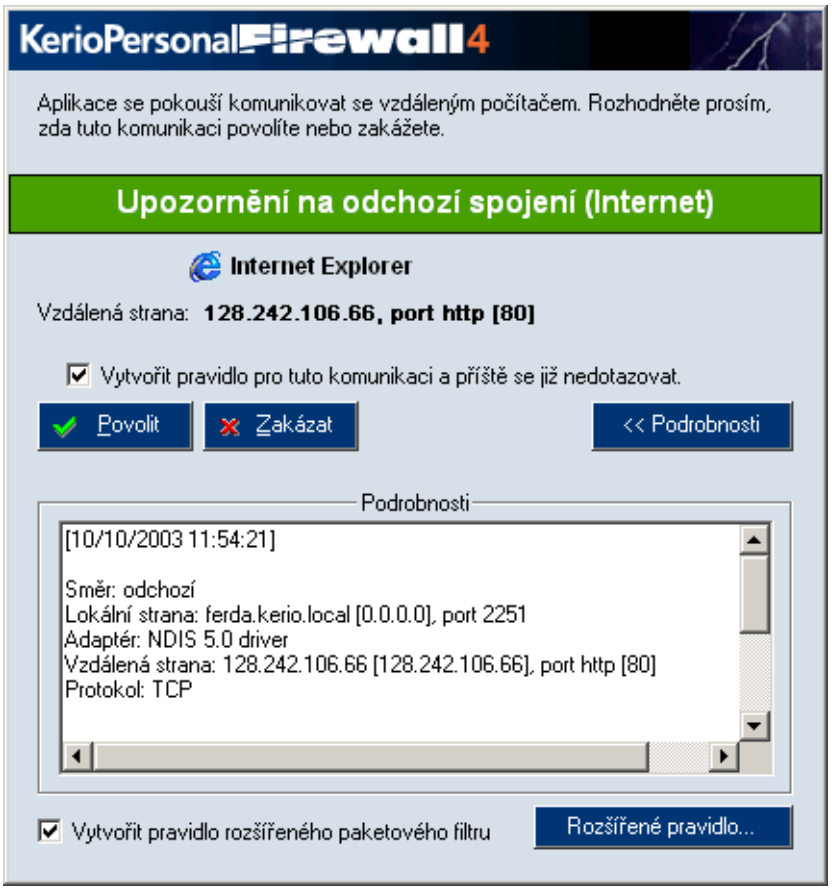
3.2 Dialog Upozornění na spojení (zachycení neznámé komunikace)

Dialog *Upozornění na spojení* (dotaz na povolení či zákaz komunikace) informuje uživatele o tom, že *Kerio Personal Firewall* zachytil dosud neznámou komunikaci a očekává jeho rozhodnutí, zda tuto komunikaci povolit či zakázat, případně vytvořit odpovídající komunikační pravidlo.

Poznámka: Chování *Kerio Personal Firewallu* při zachycení síťové komunikace určují volby a pravidla v sekci *Síťová bezpečnost* (viz kapitoly 5.2 a 5.3). Dialog *Upozornění na*

spojení se zobrazuje v případech, kdy neexistuje odpovídající pravidlo nebo pravidlo explicitně vyžaduje dotázat se uživatele.

Tento dialog je zobrazen vždy nad okny ostatních aplikací („Always on Top“). Je-li zachyceno více událostí (tj. více pokusů o navázání spojení nebo spuštění aplikací — viz kapitola 3.3) současně, pak se tyto události řadí do fronty — teprve po potvrzení jednoho dialogu se zobrazí další; nikdy se nezobrazuje více dialogů *Upozornění na spojení* současně.



Dialog *Upozornění na spojení* obsahuje následující informace a volby:

Směr komunikace a zóna Barevný pruh v horní části dialogu informuje uživatele o směru komunikace (příchozí nebo odchozí) a zóně, do které patří vzdálený počítač (důvěryhodné IP adresy nebo Internet).

Barva pruhu a text před závorkou určuje směr navazovaného spojení:

- *Upozornění na odchozí spojení* — odchozí spojení (tzn. navazované z lokálního počítače na vzdálený).

  Odchozí spojení je signalizováno zelenou barvou.

- *Upozornění na příchozí spojení* — příchozí spojení (tzn. navazované ze vzdáleného počítače na lokální).

  Příchozí spojení je signalizováno červenou barvou.

V závorce je uvedena zóna, do které patří IP adresa vzdáleného počítače:

- *Důvěryhodná zóna* — skupina důvěryhodných IP adres (podrobnosti viz kapitola 5.4)

- *Internet* — „zbytek světa“ (tj. libovolná IP adresa, která nepatří do skupiny *Důvěryhodná zóna*)

Lokální aplikace a vzdálený konec spojení Pod barevným pruhem s informací o směru komunikace jsou uvedeny stručné informace o navazovaném spojení:

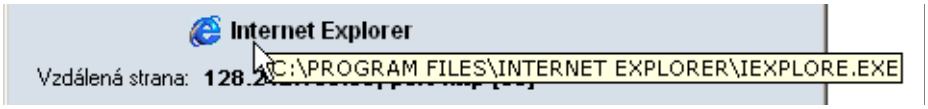
- ikona a popis aplikace na lokálním počítači. Není-li popis k dispozici, zobrazí se jméno spustitelného souboru aplikace. Nemá-li aplikace svoji ikonu, použije se standardní systémová ikona pro spustitelné soubory.

- DNS jméno vzdáleného počítače a jeho IP adresa (v hranatých závorkách).

  Poznámka: DNS jména počítačů se zjišťují dotazováním DNS. V závislosti na rychlosti odezvy může být po nějakou dobu zobrazena pouze IP adresa daného počítače. Pokud neexistuje odpovídající DNS záznam, zůstane trvale zobrazena pouze IP adresa. Převod IP adres na DNS jména lze globálně vypnout/zapnout např. v kontextovém menu okna *Overview / Connections* (viz kapitola 10.1)

- vzdálený port (jedná-li se o standardní službu, zobrazí se její jméno a číslo portu v hranatých závorkách; jinak číslo portu bez závorek)

Při umístění kurzoru myši na popis aplikace se jako nápovědný text (tooltip) zobrazí úplná cesta k spustitelnému souboru aplikace.



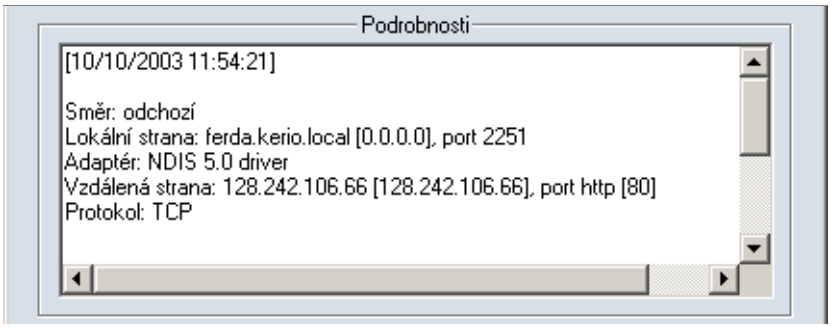
Volba akce Nejdůležitější částí dialogu je volba akce, tedy povolení či zakázání příslušné komunikace.

- Tlačítko *Povolit* povolí danou komunikaci.
- Tlačítko *Zakázat* zakáže danou komunikaci.
- Volba *Vytvořit pravidlo pro tuto komunikaci a příště se již nedotazovat* způsobí vytvoření komunikačního pravidla na základě zachycené komunikace. Akce v pravidle bude nastavena podle toho, které tlačítko bylo stisknuto (*Povolit* nebo *Zakázat*). Při příštím zachycení stejné komunikace se již *Kerio Personal Firewall* nebude dotazovat uživatele, ale provede akci dle vytvořeného komunikačního pravidla.

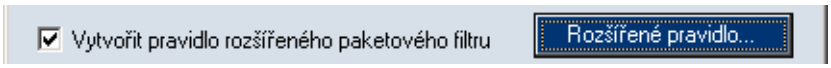
  Poznámka: Vytvořené komunikační pravidlo lze kdykoliv později upravit nebo odstranit v konfiguračním okně *Kerio Personal Firewallu* v sekci *Síťová bezpečnost*, záložka *Aplikace*. Podrobnosti naleznete v kapitole 5.2.
- Tlačítko *Podrobnosti* zobrazí pole s podrobnými informacemi o navazovaném spojení a lokální aplikaci. Opětovným stisknutím tohoto tlačítka se podrobné informace skryjí.

Následující části dialogu se zobrazí po stisknutí tlačítka *Podrobnosti*.

Detailní informace o spojení a lokální aplikaci V poli *Podrobnosti* jsou uvedeny podrobné informace o spojení (směr, protokol, lokální a vzdálená IP adresa, lokální a vzdálený port) a lokální aplikaci, která se komunikace účastní (jméno spustitelného souboru aplikace včetně plné cesty, popis aplikace, datum vytvoření, poslední změny a posledního čtení spustitelného souboru).



Vytvoření rozšířeného pravidla



Zaškrtnutím volby *Vytvořit pravidlo rozšířeného paketového filtru* bude namísto standardního pravidla pro aplikaci (viz kapitola 5.2) vytvořeno pravidlo paketového filtru, umožňující detailně nastavit parametry komunikace (IP adresy, porty atd.), lokální aplikaci, časovou platnost atd.

Tlačítko *Rozšířené pravidlo...* otevírá dialog pro definici pravidla paketového filtru, ve kterém lze pravidlo upravit (upřesnit) dle požadavků uživatele. Rozšířené pravidlo lze kdykoliv změnit nebo odstranit v konfiguračním okně *Kerio Personal Firewallu* (sekce

Síťová bezpečnost, záložka *Aplikace*, tlačítko *Paketový filtr*).

Podrobnosti o rozšířených komunikačních pravidlech naleznete v kapitole 6.

Poznámka: Po dobu, kdy je zobrazen dialog *Upozornění na spojení*, je příslušná komunikace „pozastavena“ (již přijatá či vyslaná data uchovává *Kerio Personal Firewall* ve své vyrovnávací paměti). Není-li reakce uživatele dostatečně rychlá, může vysílající aplikace po určité době (zpravidla několik desítek sekund) tento stav vyhodnotit jako síťovou chybu (cílový počítač nedostupný).

3.3 Dialog Spouštění/Záměna/Spouštění jiné aplikace

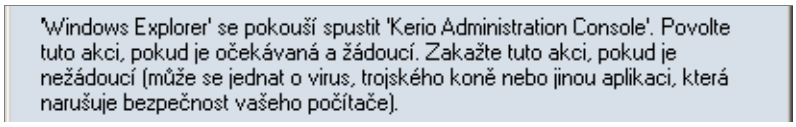
Dialog *Spouštění/Záměna/Spouštění jiné aplikace* informuje uživatele o tom, že *Kerio Personal Firewall* detekoval pokus o spuštění aplikace a očekává jeho rozhodnutí, zda tuto akci povolit či zakázat, případně vytvořit odpovídající pravidlo. Aplikace bude spuštěna až v okamžiku, kdy to uživatel povolí.

Poznámka: Chování *Kerio Personal Firewallu* při spouštění aplikací určují volby a pravidla v sekci *Bezpečnost systému* (viz kapitola 7). Dialog *Spouštění/Záměna/Spouštění jiné aplikace* se zobrazuje v případech, kdy neexistuje odpovídající pravidlo nebo pravidlo explicitně vyžaduje dotázat se uživatele.

Tento dialog je zobrazen vždy nad okny ostatních aplikací („Always on Top“). Je-li zachyceno více událostí (tj. více pokusů o spuštění aplikací nebo o síťovou komunikaci — viz kapitola 3.2) současně, pak se tyto události řadí do fronty — teprve po potvrzení jednoho dialogu se zobrazí další. Nikdy se tedy nezobrazuje více dialogů *Spouštění/Záměna/Spouštění jiné aplikace* a/nebo *Upozornění na spojení* současně.

Dialog obsahuje tyto informace:

Popis události V záhlaví dialogového okna je uveden slovní popis zachycené události a obecné doporučení, jakou akci by měl uživatel zvolit.

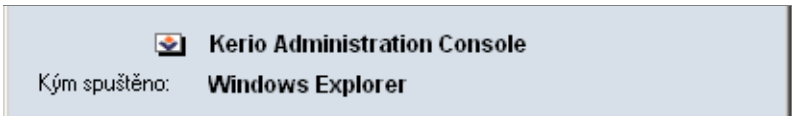


Název události Barevný pruh obsahuje informaci o tom, jaká událost byla zachycena:

- *Spouštění aplikace*
- *Záměna aplikace* — změna ve spustitelném souboru aplikace
- *Aplikace spouští jinou aplikaci* — běžící aplikace se pokouší spustit jinou aplikaci

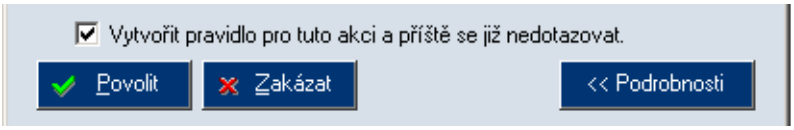
Ikona a popis aplikace Pod informací o typu události je zobrazen popis a ikona spouštěné aplikace. Není-li popis k dispozici, zobrazí se jméno spustitelného souboru aplikace. Nemá-li aplikace svoji ikonu, použije se standardní systémová ikona pro spustitelné soubory.

Pokud byla aplikace spuštěna jinou aplikací, zobrazí se ve druhém řádku (*Kým spuštěno*) popis této aplikace.



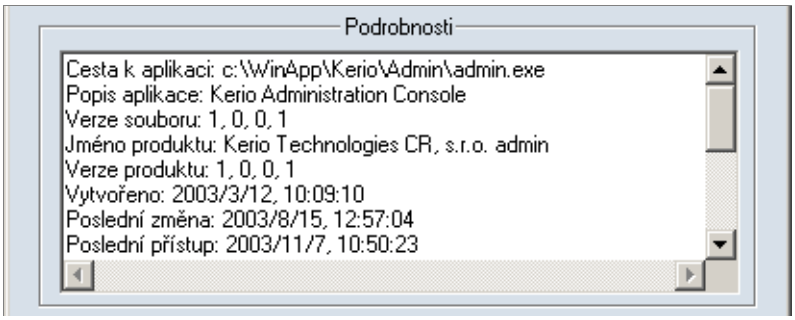
Při umístění kurzoru myši na popis aplikace (v prvním řádku) nebo na popis aplikace, která ji spouští (ve druhém řádku) se jako nápovědný text (tooltip) zobrazí úplná cesta k spustitelnému souboru aplikace.

Volba akce Nejdůležitější částí dialogu je volba akce — tedy povolení či zakázání spuštění příslušné aplikace.



- Tlačítko *Povolit* povolí spuštění aplikace.
- Tlačítko *Zakázat* zakáže spuštění aplikace.
- Volba *Vytvořit pravidlo pro tuto akci a příště se již nedotazovat* způsobí vytvoření pravidla pro tuto událost (v sekci *Bezpečnost systému / Aplikace*). Při příštím zachycení události stejného typu se již firewall uživatele nedotazuje a provede akci definovanou uživatelem.
- Tlačítko *Podrobnosti* zapíná/vypíná zobrazení podrobnosti o spouštěné aplikaci (případně také o aplikaci, která ji spouští)

Podrobnosti o aplikacích Sekce *Podrobnosti* obsahuje podrobné informace o spouštěné aplikaci, případně o aplikaci, která se ji pokouší spustit (úplná cesta k spustitelnému souboru, popis aplikace, číslo verze, datum vytvoření, poslední změny a posledního přístupu k souboru atd.).

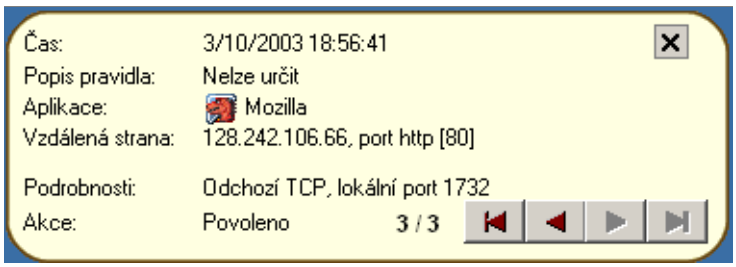


3.4 Upozornění na událost

V pravidlech *Kerio Personal Firewallu* může být nastaveno zobrazení upozornění při zachycení komunikace vyhovující tomuto pravidlu, resp. při spuštění odpovídající aplikace. Jestliže *Kerio Personal Firewall* zaznamená takovou událost, zobrazí v pravém dolním rohu obrazovky okno s detailními informacemi. Nastanou-li další události tohoto typu dříve, než uživatel informační okno zavře, řadí se informace do fronty, kterou lze procházet oběma směry (použitím tlačítek se šipkami v pravém dolním rohu okna).

Poznámka: Uzavřením okna s upozorněním (kliknutím na křížek v pravém horním rohu nebo kombinací kláves *Alt+F4*) dojde k vymazání všech zpráv z fronty, bez ohledu na to, zda byly zobrazeny či nikoliv!

Příklad upozornění na síťovou komunikaci



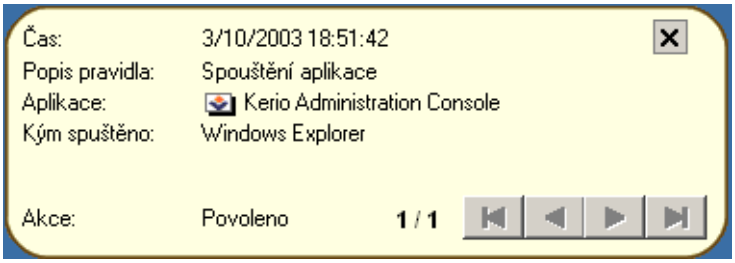
Upozornění uživateli obsahuje tyto položky:

- *Čas* — datum a čas, kdy událost nastala
- *Popis pravidla* — popis (název) pravidla rozšířeného paketového filtru, které bylo uplatněno (pokud bylo použito pravidlo pro aplikaci, zobrazuje se zde *Nelze určit*)
- *Aplikace* — ikona a název lokální aplikace, která se komunikace účastní (nemá-li aplikace ikonu, použije se standardní systémová ikona; není-li k dispozici název aplikace, zobrazí se jméno spustitelného souboru bez přípony)

- *Vzdálená strana* — IP adresa a port vzdáleného počítače (pokud lze z DNS zjistit jeho jméno, zobrazuje se namísto IP adresy; jedná-li se o standardní službu, zobrazí se před číslem portu její název)
- *Podrobnosti* — podrobnosti o spojení: směr (*Odchozí* nebo *Příchozí*), protokol a lokální port
- *Akce* — akce, která byla provedena (*Povoleno* — komunikace povolena, *Zakázáno* — komunikace zakázána)
- pořadí zprávy ve frontě a celkový počet zpráv ve frontě (celkový počet zpráv může narůstat, jestliže v době zobrazení okna s upozorněním generuje *Kerio Personal Firewall* další zprávy)

Podrobné informace o pravidlech pro síťovou komunikaci aplikací naleznete v kapitole 5.2.

Příklad upozornění na spouštění aplikace



Upozornění uživateli obsahuje tyto položky:

- *Čas* — datum a čas, kdy událost nastala
- *Popis pravidla* — popis události, která byla zachycena:
  - *Spouštění aplikace*
  - *Záměna aplikace* (změna spustitelného souboru aplikace)
  - *Aplikace spouští jinou aplikaci*
- *Aplikace* — ikona a název spouštěné aplikace (nemá-li aplikace ikonu, použije se standardní systémová ikona; není-li k dispozici název aplikace, zobrazí se jméno spustitelného souboru bez přípony)

- *Kým spuštěno* — název (popis) aplikace, která danou aplikaci spouští
- *Akce* — akce, která byla provedena na základě odpovídajícího pravidla (*Povoleno* — spuštění aplikace povoleno, *Zakázáno* — spuštění aplikace zamítnuto).

Podrobné informace o pravidlech pro spouštění aplikací naleznete v kapitole 7.1.

Kapitola 4

Konfigurace firewallu

4.1 Konfigurační okno

K nastavení *Kerio Personal Firewallu* a sledování stavových informací a záznamů slouží tzv. konfigurační okno. Toto okno lze otevřít následujícími způsoby:

- dvojitým kliknutím *levým* tlačítkem na ikonu *Kerio Personal Firewallu* na nástrojové liště
- kliknutím pravým tlačítkem na tuto ikonu a volbou *Konfigurace* z kontextového menu

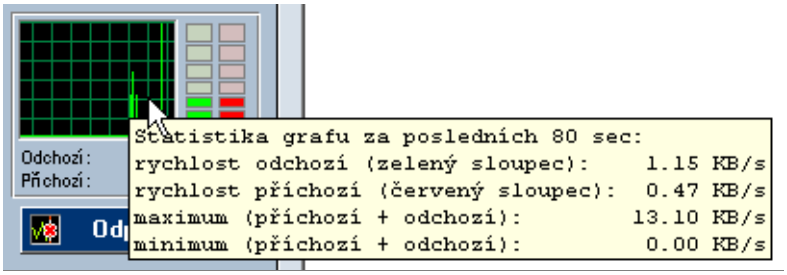
Záložky v levé části okna slouží k přepínání jednotlivých sekcí:

- *Přehled* — přehled aktivních spojení a otevřených portů (viz kapitola 10.1), statistiky (viz kapitola 10.2) a uživatelské preference (viz kapitola 4.3).
- *Síťová bezpečnost* — pravidla pro síťovou komunikaci aplikací, paketový filtr, definice důvěryhodné zóny (viz kapitola 5)
- *Bezpečnost systému* — pravidla pro spouštění aplikací (viz kapitola 7)
- *Útoky* — nastavení detekce známých typů útoků (viz kapitola 8)
- *WWW* — pravidla pro WWW stránky — blokování pop-up oken, URL filtr, blokování objektů, kontrola nad odesílanými daty (viz kapitola 9)
- *Záznamy* — prohlížení a nastavení záznamů (viz kapitola 11)

Graf v levé dolní části okna zobrazuje časový průběh zatížení síťového rozhraní. Zelený sloupec vedle grafu zobrazuje aktuální (okamžitou) rychlost odchozí komunikace, červený sloupec rychlost příchozí komunikace.

Kliknutím levým tlačítkem myši na graf se přepíná zobrazení — čárový graf nebo sloupcový graf.

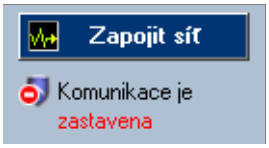
Při umístění kurzoru myši nad graf se zobrazí nápovědný text (tooltip) se statistikou síťové komunikace:



- *rychlost odchozí (zelený sloupec)* — aktuální rychlost odchozí komunikace
- *rychlost příchozí (červený sloupec)* — aktuální rychlost příchozí komunikace
- *maximum (příchozí + odchozí)* — nejvyšší zaznamenaná rychlost (součet odchozí a příchozí komunikace za posledních 80 sekund)
- *minimum (příchozí + odchozí)* — nejnižší zaznamenaná rychlost (součet odchozí a příchozí komunikace za posledních 80 sekund)

Tlačítko *Odpojit síť* pod grafem slouží k zablokování veškeré síťové komunikace (všechna otevřená spojení budou pozastavena). Tato funkce může být užitečná např. v případě, kdy omylem povolíme komunikaci, která měla být zakázána. Po stisknutí změní toto tlačítko popis na *Zapojit síť*.

Je-li komunikace zastavena, je tento stav signalizován ikonou a textem pod tlačítkem *Zapojit síť*.

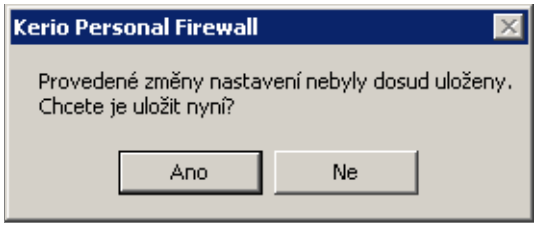


Poznámka: Volba *Odpojit síť / Zapojit síť* je dostupná také z kontextového menu ikony *Kerio Personal Firewallu* na nástrojové liště (viz kapitola 2.2).

Tlačítka na spodním okraji okna mají standardní funkce:

- *OK* — uložení provedených změn a zavření konfiguračního okna
- *Storno* — zavření okna bez uložení změn
- *Použít* — uložení (akceptování) provedených změn, okno zůstává otevřené
- *Nápověda* — otevření nápovědy pro aktuální sekci/záložku

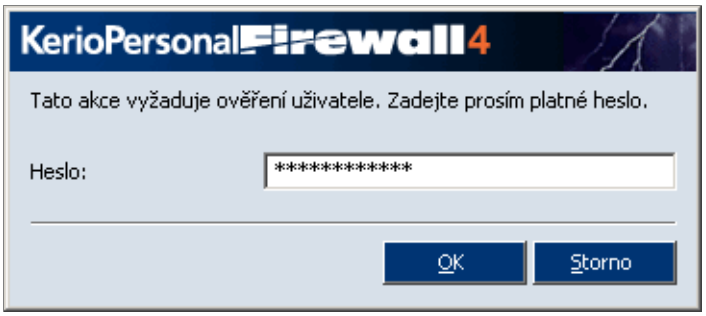
Poznámka: Změny konfigurace lze provádět současně pouze v jedné záložce jedné sekce. Při přechodu do jiné záložky, resp. jiné sekce, se kontroluje, zda v aktuálním zobrazení nebyly provedeny dosud neuložené změny. Pokud ano, *Kerio Personal Firewall* se dotáže, zda má tyto změny akceptovat nebo stornovat.



Ochrana konfigurace heslem

Přístup ke konfiguraci *Kerio Personal Firewallu* může být chráněn heslem (změny v konfiguraci pak může provádět pouze oprávněný uživatel). Heslo lze nastavit v sekci *Přehled / Předvolby* (viz kapitola 4.3).

Je-li konfigurace chráněna heslem, může neověřený uživatel nastavení v konfiguračním okně pouze prohlížet. Při prvním pokusu o provedení změny bude vyžadováno zadání hesla.



Po zadání platného hesla dojde k přihlášení uživatele — uživatel bude mít právo provádět změny v konfiguraci.

Po provedení všech konfiguračních změn by se uživatel měl odhlásit, aby nemohlo dojít k zásahu do konfigurace neoprávněnou osobou. Odhlášení lze provést volbou *Odhlásit* z kontextového menu ikony na nástrojové liště (viz kapitola 2.2), případně tlačítkem *Odhlásit* v sekci *Přehled / Předvolby*. Pokud se uživatel neodhlásí, je přihlášení platné až do ukončení běhu služby *Personal Firewall Engine*.

4.2 Vzdálená správa

Kerio Personal Firewall může být spravován i vzdáleně, tj. z jiného počítače, než na kterém běží služba *Personal Firewall Engine*. Vzdálený přístup je možný na dvou úrovních:

- přístup ke konfiguraci — ze vzdáleného počítače lze provádět všechna nastavení a akce, které jsou dostupné v konfiguračním okně. Dialogy při událostech (spouštění aplikací, síťová komunikace) a upozornění na události budou zobrazovány na počítači, kde běží *Personal Firewall Engine*.
- přesměrování relace — na vzdálený počítač budou přesměrovány také všechny dialogy a upozornění uživateli.

Připojení ze vzdáleného počítače

Pro připojení k *Personal Firewall Engine* z jiného počítače je třeba provést tyto kroky:

1. Nastavení hesla pro přístup ke správě

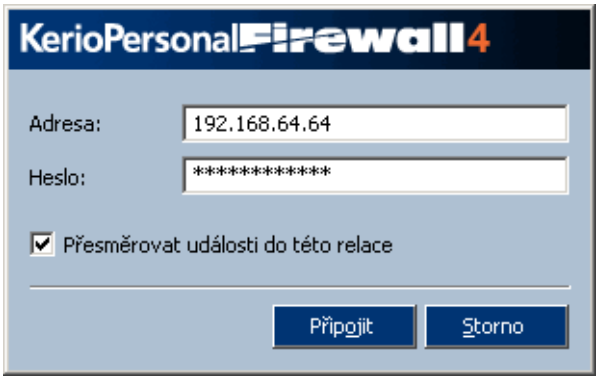
   Vzdálené připojení k *Personal Firewall Engine* je možné pouze na základě ověření uživatele heslem. V sekci *Přehled / Předvolby* zapněte volbu *Povolit ochranu heslem*, případně nastavte heslo, pokud nebylo dosud definováno. Podrobnosti naleznete v kapitole 4.3.

2. Spouštění *Personal Firewall GUI* na vzdáleném počítači

- Je-li na vzdáleném počítači nainstalován *Kerio Personal Firewall 4.x*, spusťte komponentu *Remote Firewall Administration* z programové skupiny *Kerio*.
- Není-li na vzdáleném počítači *Kerio Personal Firewall* nainstalován, zkopírujte z lokálního počítače (typicky adresář `C:\Program Files\Kerio\Personal Firewall 4`) na vzdálený počítač soubor `kpf4gui.exe` a podadresář `trans`. Na vzdáleném počítači spusťte aplikaci `kpf4gui.exe`.

3. Přihlášení k *Personal Firewall Engine*

   Při spuštění *Personal Firewall GUI* jedním z výše popsaných způsobů se zobrazí dialog pro přihlášení k *Personal Firewall Engine*.



Adresa DNS jméno nebo IP adresa počítače, na kterém běží *Personal Firewall Engine*. . Po přihlášení bude toto jméno nebo IP adresa zobrazena:

- v záhlaví konfiguračního okna

- v nápovědném textu (tooltip) ikony na nástrojové liště

Heslo Heslo pro přístup ke správě (viz bod 1.)

Přesměrovat události do této relace Tato volba zapíná/vypíná přesměrování všech dialogů a upozornění na vzdálený počítač.

Zapněte tuto volbu, chcete-li *Kerio Personal Firewall* kompletně sledovat a ovládat ze vzdáleného počítače. Pokud chcete provést pouze jednorázovou úpravu konfigurace, doporučujeme tuto volbu nezapínat.

Po stisknutí tlačítka *Připojit* se naváže spojení se vzdáleným počítačem.

Poznámka: Připojení vzdálené správy je povoleno interními pravidly *Kerio Personal Firewallu*. Pro vzdálenou správu tedy není třeba definovat speciální pravidla síťové bezpečnosti.

Po úspěšném navázání spojení s *Personal Firewall Engine* se na nástrojové liště zobrazí (v poli System Tray) ikona *Kerio Personal Firewallu* se symbolem vzdáleného připojení (*R* = remote = vzdálený). Kontextové menu této ikony obsahuje následující funkce:

Zakázat firewall Deaktivace firewallu (vypnutí všech bezpečnostních funkcí).

Konfigurace Tato volba otevírá konfigurační okno, ve kterém lze provádět všechny konfigurační úkony stejně jako na lokálním počítači (s výjimkou zastavení síťové komunikace). Podrobnosti viz kapitola 4.1.

O aplikaci Okno s informacemi o verzích jednotlivých komponent *Kerio Personal Firewallu* a licenci, případně datu omezení funkčnosti zkušební verze. Informace v tomto okně jsou stejné jako v případě lokálního připojení).

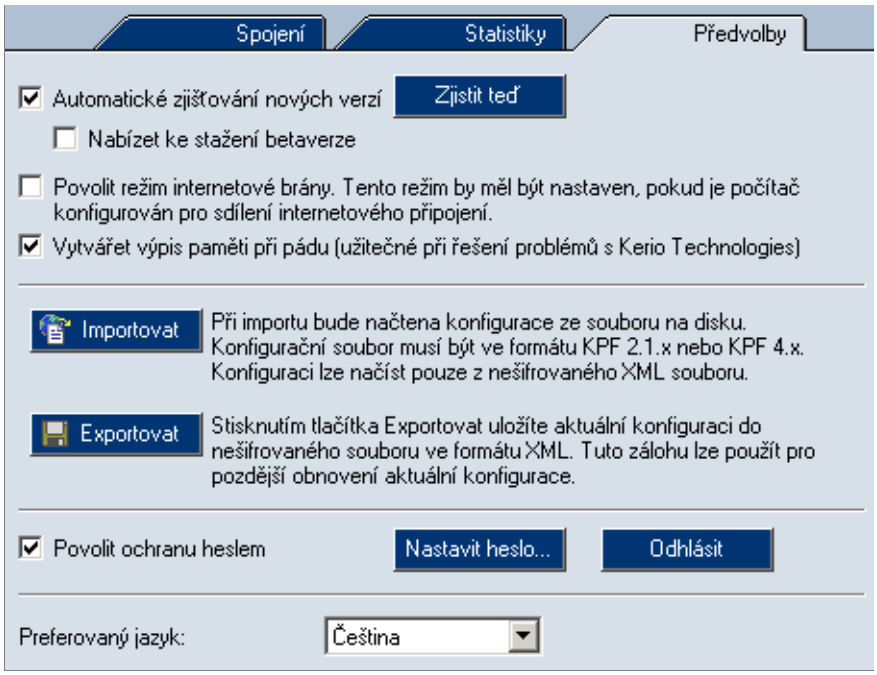
Odpojit Odpojení od vzdálené služby *Personal Firewall Engine* a ukončení *Personal Firewall GUI* na počítači, ze kterého byla vzdálená správa prováděna.

Poznámka: Narozdíl od lokální správy nejsou při vzdáleném připojení v kontextovém menu dostupné tyto funkce:

- *Odpojit síť* (zablokování síťové komunikace by přerušilo také spojení mezi *Personal Firewall Engine* a *Personal Firewall GUI* na vzdáleném počítači)
- *Odhlásit* (při vzdálené správě musí být uživatel ověřen, odhlášení se de facto provede při odpojení od *Personal Firewall Engine*)
- *Ukončit* (službu *Personal Firewall Engine* nelze vzdáleně ukončit; *Personal Firewall GUI* na vzdáleném počítači se ukončí volbou *Odpojit*)

4.3 Předvolby

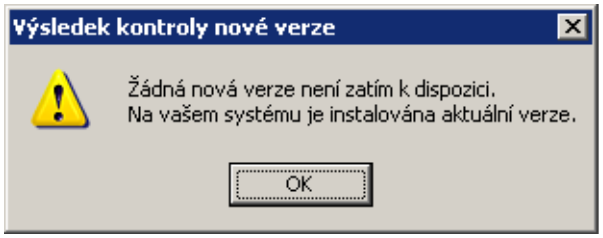
Sekce *Přehled / Předvolby* slouží k nastavení uživatelských preferencí a upřesňujících parametrů firewallu.



Automatické zjišťování nových verzí Zapnutí/vypnutí automatické kontroly nových verzí programu. Pro zajištění maximální bezpečnosti doporučujeme ponechat tuto volbu zapnutou (nové verze obsahují aktualizace databáze známých útoků, opravy případných chyb atd.).

Podrobnosti o automatické kontrole a instalaci nové verze naleznete v kapitole 1.6.

Zjistit teď Toto tlačítko spouští okamžitou kontrolu existence nové verze *Kerio Personal Firewallu*. Je-li na aktualizačním serveru nalezena novější verze, pak je uživateli nabídnuto její stažení a instalace (podrobnosti viz kapitola 1.6). V opačném případě se zobrazí informace o tom, že novější verze není k dispozici (instalovaná verze je aktuální).



Nabízet ke stažení betaverze Zapnutím této volby budou při kontrole nových verzí uživateli nabízeny také zveřejněné betaverze. Betaverze jsou nové verze ve stádiu vývoje — není zaručena jejich plná funkčnost a mohou obsahovat chyby.

Volbu *Nabízet ke stažení betaverze* použijte v případě, jestliže se chcete účastnit testování betaverzí (podrobnosti viz `http://www.kerio.cz/`, *Beta Sekce*). Nemáte-li zájem o testování a chcete-li mít na svém počítači vždy plně funkční (finální) verzi, pak tuto volbu nezapínejte.

Povolit režim internetové brány Tato volba přepíná firewall do speciálního režimu ochrany internetové brány (tj. směrovače nebo směrovače s překladem IP adres).

Po zapnutí volby *Povolit režim internetové brány* bude *Kerio Personal Firewall* propouštět pakety s cílovými porty, na kterých neběží žádná lokální aplikace, případně pakety s cílovými IP adresami, které nejsou lokální.

Není-li *Kerio Personal Firewall* skutečně nasazen na internetové bráně, pak by tato volba měla být vypnuta, jinak degraduje ochranu lokálního počítače!

Poznámky:

1. Volbu *Povolit režim internetové brány* lze také využít pro povolení síťové komunikace operačního systému, který je provozován v rámci programu *VMWare* (`http://www.vmware.com/`), jestliže *Kerio Personal Firewall* chrání hostitelský systém. Bude-li tato volba vypnuta, bude *Kerio Personal Firewall* blokovat pakety určené operačnímu systému uvnitř *VMWare*.

2. Je-li *Kerio Personal Firewall* použit k ochraně proxy serveru, není třeba tuto volbu zapínat (proxy server se chová jako klient na lokálním počítači).

Vytvářet výpis paměti při pádu Zapnutí/vypnutí vytváření ladicích informací pro případ havárie *Kerio Personal Firewallu*. Dojde-li po zapnutí této volby k pádu *Personal Firewall Engine* nebo *Personal Firewall GUI*, vytvoří se soubor s výpisem paměti a následně automaticky spustí nástroj *Assist*, který nabídne odeslání informací o pádu (komprimovaného výpisu paměti a vybraných záznamů) k analýze do firmy *Kerio Technologies*.

V případě, že došlo k havárii operačního systému, může *Kerio Personal Firewall* po opětovném startu odeslat k analýze výpis paměti jádra (resp. úplný výpis paměti v případě Windows NT 4.0). 1 minutu po startu služby *Personal Firewall Engine* se provede kontrola, zda se na disku nenalézá nový výpis paměti. Pokud ano, spustí se nástroj *Assist*. Ten se nejprve uživatele dotáže, zda se domnívá, že tento výpis má souvislost s pádem aplikace firmy *Kerio Technologies*. V případě kladné odpovědi nabídne jeho odeslání k analýze. Výpis paměti je odesílán v komprimované podobě.

Poznámka: Odeslané informace budou použity výhradně pro účely ladění aplikace *Kerio Personal Firewall*. Nebudou použity k žádnému jinému účelu ani poskytnuty třetí straně.

Konfigurace Tato sekce obsahuje tlačítka pro zálohování konfigurace *Kerio Personal Firewall* a její obnovení, případně načtení konfigurace aplikace *Kerio Personal Firewall 2.1.x*.

Po stisku tlačítka *Importovat* se zobrazí systémový dialog pro otevření souboru. *Kerio Personal Firewall* dokáže otevřít a načíst konfigurační soubor ve formátu:

- *Kerio Personal Firewall 4.x* v nešifrované podobě (formát XML, přípona `.cfg`)
- *Kerio Personal Firewall 2.1.x* (přípona `.conf`) — import konfigurace ze starší verze

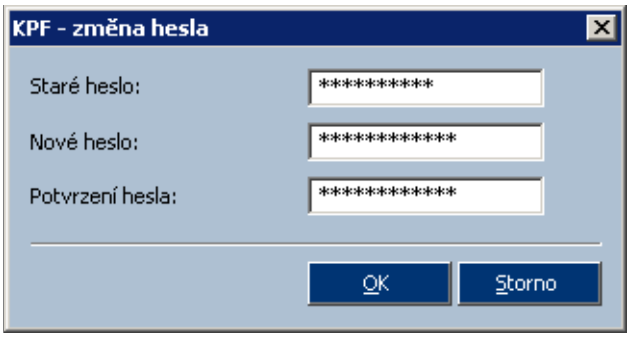
Tlačítko *Exportovat* otevírá systémový dialog pro uložení souboru. Takto je možné uložit konfigurační soubor (v nešifrované podobě) pro pozdější použití či pro přenos na jiný počítač.

Poznámka: Konfigurační soubor verze *4.x* nelze v šifrované podobě importovat.

Povolit ochranu heslem Nastavení hesla pro přístup ke konfiguraci *Kerio Personal Firewallu*. Je-li konfigurace chráněna heslem, pak je možné si ji pouze prohlížet. Při prvním pokusu o změnu je vyžadováno ověření uživatele zadáním hesla. Po úspěšném ověření je uživatel přihlášen a má právo konfiguraci měnit. Podrobné informace naleznete v kapitole 4.1.

Tlačítko *Odhlásit* slouží k odhlášení uživatele — při dalším pokusu o změnu konfigurace bude opět vyžadováno zadání hesla. Odhlášení je možné také volbou z kontextového menu ikony na nástrojové liště (viz kapitola 2.2)

Tlačítko *Nastavit heslo...* otevírá dialog pro zadání nebo změnu hesla.



Do položky *Staré heslo* je třeba zadat aktuální heslo (změnu hesla smí provést pouze oprávněný uživatel). Pokud nebylo dosud žádné heslo definováno (bezprostředně po

instalaci *Kerio Personal Firewallu*, po smazání konfigurace apod.), je tato položka neaktivní. Do položky *Nové heslo* zadejte požadované heslo a v položce *Potvrzení hesla* jej pro kontrolu zopakujte.

Poznámka: Vzdálená správa *Kerio Personal Firewallu* je možná pouze po ověření uživatele heslem. Je-li volba *Povolit ochranu heslem* vypnuta, pak není možné se připojit k *Personal Firewall Engine* z jiného počítače.

Preferovaný jazyk Volba jazyka uživatelského rozhraní *Kerio Personal Firewallu*. Po stisknutí tlačítka *OK* nebo *Použít* dojde k restartu uživatelského rozhraní. Při dalším otevření konfiguračního okna, resp. kontextového menu na nástrojové liště, se již uživatelské rozhraní zobrazí v požadovaném jazyce.

Jednotlivé jazykové verze (lokalizace) jsou uloženy v podadresáři `trans` adresáře, kde je *Kerio Personal Firewall* nainstalován.

Kapitola 5

Pravidla pro síťovou komunikaci

Klíčovým bodem konfigurace *Kerio Personal Firewallu* jsou pravidla pro síťovou komunikaci. K dispozici jsou tři typy pravidel:

- *Pravidla pro aplikace* — jednoduchá pravidla definující chování firewallu při síťové komunikaci s počítači v důvěryhodné zóně a v Internetu. Tato pravidla jsou vytvářena automaticky na základě reakce uživatele při zachycení dosud neznámé síťové komunikace. Podrobnosti viz kapitola 5.2.
- *Rozšířený paketový filtr* — detailní pravidla pro síťovou komunikaci (možnost nastavení IP adres, protokolu, portů, aplikace atd.). Pravidla paketového filtru mohou být definována buď ručně (v konfiguračním okně *Kerio Personal Firewallu*) nebo automaticky na základě reakce uživatele (viz kapitola 3.2)

  Nastavení rozšířeného paketového filtru je popsáno v kapitole 6.
- *Předdefinovaná pravidla pro síťovou komunikaci* — *Kerio Personal Firewall* obsahuje sadu přeedefinovaných pravidel, která jsou nezávislá na aplikacích. U předdefinovaných pravidel může uživatel nastavovat pouze akci (tj. povolit nebo zakázat příslušnou komunikaci). Předdefinovaná pravidla lze jednoduše zapnout nebo vypnout (jedna volba pro všechna pravidla). Podrobnosti viz kapitola 5.3.

Modul firewallu pro kontrolu síťové komunikace lze zapnout/vypnout volbou *Povolit modul síťové bezpečnosti* v sekci *Síťová bezpečnost*, záložka *Aplikace*. Je-li tato volba vypnuta, pak jsou všechny uvedené typy pravidel neaktivní.

5.1 Aplikace pravidel pro síťovou komunikaci

Při zachycení síťové komunikace aplikují jednotlivé moduly firewallu definovaná pravidla v určeném pořadí. Jestliže komunikace vyhovuje určitému pravidlu, provede se odpovídající akce a vyhodnocování se ukončí.

Pravidla jednotlivých modulů *Kerio Personal Firewallu* se aplikují v tomto pořadí:

1. Systém detekce útoků (IDS — viz kapitola 8)
2. Interní pravidla pro komponenty *Kerio Personal Firewallu* — např. povolení přístupu na WWW server firmy *Kerio Technologies* pro kontrolu a stahování nových verzí programu

3. Pravidla rozšířeného paketového filtru (viz kapitola 6)

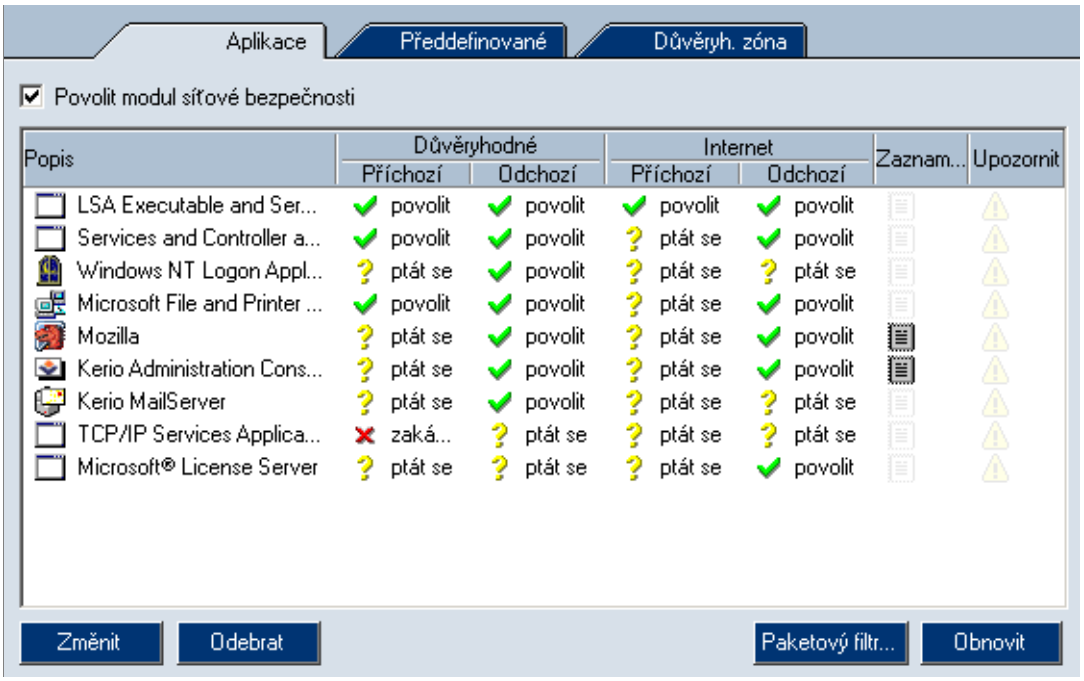
4. Předdefinovaná pravidla pro síťovou komunikaci (viz kapitola 5.3)

5. Pravidla pro síťovou komunikaci aplikací (viz kapitola 5.2)

Poznámka: Je-li vypnut modul síťové bezpečnosti a/nebo detekce útoků (viz kapitola 8), pak se příslušná pravidla na zachycenou komunikaci neaplikují. Interní pravidla firewallu vypnout nelze.

5.2 Pravidla pro aplikace

K zobrazení a úpravě pravidel pro aplikace slouží sekce *Síťová bezpečnost*, záložka *Aplikace*.



Každé pravidlo sestává z následujících částí:

Popis Ikona a popis aplikace. Nemá-li aplikace ikonu, bude použita systémová ikona pro spustitelné soubory. Není-li k dispozici popis aplikace, zobrazí se jméno souboru bez přípony.

Poznámka: Ikonu a popis aplikace nelze v *Kerio Personal Firewallu* změnit (tyto informace jsou dány tvůrcem konkrétní aplikace).

Důvěryhodné, Internet Nastavení chování firewallu při komunikaci dané aplikace s počítačem v důvěryhodné zóně a v Internetu v každém směru (*Příchozí*, *Odchozí*).

Pro každou zónu a každý směr komunikace lze zvolit jednu z těchto akcí:

- *povolit* — povolení komunikace
- *zakázat* — zákaz komunikace
- *ptát se* — *Kerio Personal Firewall* se dotáže uživatele, zda chce komunikaci povolit či zakázat. Při zachycení odpovídající komunikace se zobrazí dialog *Upozornění na spojení* (tento dialog je podrobně popsán v kapitole 3.2) a uživatel musí rozhodnout, jak se má firewall zachovat.

  Poznámka: V dialogu *Upozornění na spojení* může uživatel pravidlo změnit (zaškrtne-li volbu *Vytvořit pravidlo pro tuto komunikaci...*, pak se akce *Ptát se* v pravidle změní na akci, kterou uživatel zvolil).

Příklad: Pravidlo pro WWW prohlížeč *Mozilla*

Popis	Důvěryhodné		Internet		Zaznamenat	Upozornit
	Příchozí	Odchozí	Příchozí	Odchozí		
LSA Executable and Ser...	povolit	povolit	povolit	povolit		
Services and Controller a...	povolit	povolit	ptát se	povolit		
Windows NT Logon App...	ptát se	povolit	ptát se	ptát se		
Microsoft File and Printer...	povolit	povolit	ptát se	povolit		
Mozilla	ptát se	povolit	ptát se	povolit	✓	
Kerio Administration Con...	ptát se	povolit	ptát se	povolit	✓	

WWW prohlížeč je typická klientská aplikace — navazuje spojení s WWW servery. Odchozí komunikaci tedy můžeme povolit. WWW server ale nikdy nenavazuje spojení zpět na klienta: taková komunikace je podezřelá (může to být pokus o útok). Příchozí komunikaci s aplikací *Mozilla* tedy zakážeme, případně nastavíme akci *ptát se*, aby byl uživatel na takovou komunikaci upozorňován.

Zaznamenat Po zapnutí této volby bude veškerá komunikace vyhovující danému pravidlu zaznamenána do záznamu *Network* (viz kapitola 11.4), a to bez ohledu na nastavenou akci (zaznamenána bude tedy povolená i zakázaná komunikace).

Upozornit Zapnutím této volby bude při detekci komunikace vyhovující tomuto pravidlu zobrazeno upozornění — okno *Alert* (viz kapitola 3.4). Nezáleží na tom, zda je komunikace povolena či zakázána.

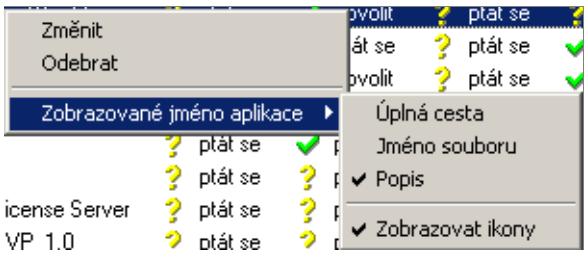
Tuto funkci lze využít např. v případě, kdy zakážeme nežádoucí komunikaci a chceme být informováni o tom, zda a kdy vzdálený počítač pokus o navázání spojení zopakuje.

Tlačítko *Změnit* otevírá dialog pro úpravu vybraného pravidla (viz dále). Tlačítko *Odebrat* odstraní vybrané pravidlo. Tlačítko *Obnovit* slouží k obnovení seznamu pravidel (po dobu otevření záložky *Aplikace* může dojít k interakci firewallu s uživatelem a v důsledku toho k přidání či změně pravidel).

Volby pro pravidla

V poli se seznamem pravidel jsou dostupné následující volby:

1. Kliknutím pravým tlačítkem myši ve sloupci *Popis* se zobrazí kontextové menu s těmito funkcemi:



   - *Změnit* — otevření dialogu pro úpravu pravidla (viz níže)
   - *Odebrat* — odstranění vybraného pravidla
   - *Zobrazované jméno aplikace* — volba, jakým způsobem bude zobrazován název aplikace:
     - úplná cesta k souboru
     - jméno souboru bez cesty
     - popis aplikace

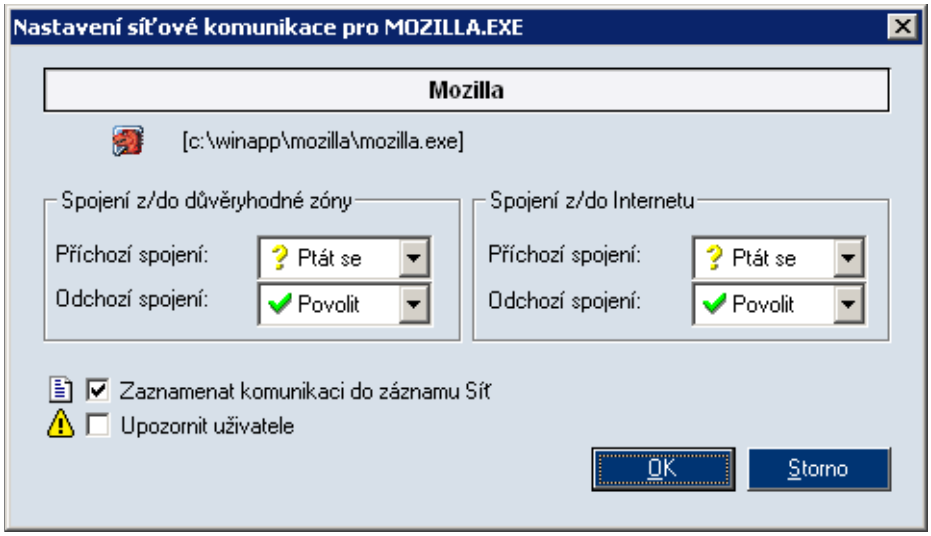
     Volba *Zobrazovat ikony* zapíná/vypíná zobrazování ikon aplikací před jménem souboru nebo popisem aplikace.

2. Kliknutím myší na akci (ve sloupci *Důvěryhodné* nebo *Internet*):
   - levým tlačítkem se akce cyklicky přepíná: *Povolit* — *Zakázat* — *Ptát se*
   - pravým tlačítkem se zobrazí kontextové menu, z něhož lze vybrat požadovanou akci.

3. Kliknutím levým tlačítkem myši ve sloupci *Zaznamenat* nebo *Upozornit* lze zapnout, resp. vypnout záznam komunikace vyhovující tomuto pravidlu do záznamu *Síť* nebo zobrazování upozornění uživateli při zachycení takové komunikace.

Dialog pro úpravu pravidla

Stisknutím tlačítka *Změnit* nebo volbou *Změnit* z kontextového menu se otevře dialog pro úpravu vybraného pravidla. V tomto dialogu lze nastavit akci pro každou zónu a směr komunikace, záznam komunikace odpovídající tomuto pravidlu a zobrazování upozornění uživateli.



V horním poli dialogu se zobrazuje popis aplikace a v dalším řádku ikona aplikace a plná cesta k spustitelnému souboru aplikace. Tyto informace nelze měnit.

Střední část dialogu umožňuje nastavení požadovaných akcí pro každou zónu a každý směr komunikace.

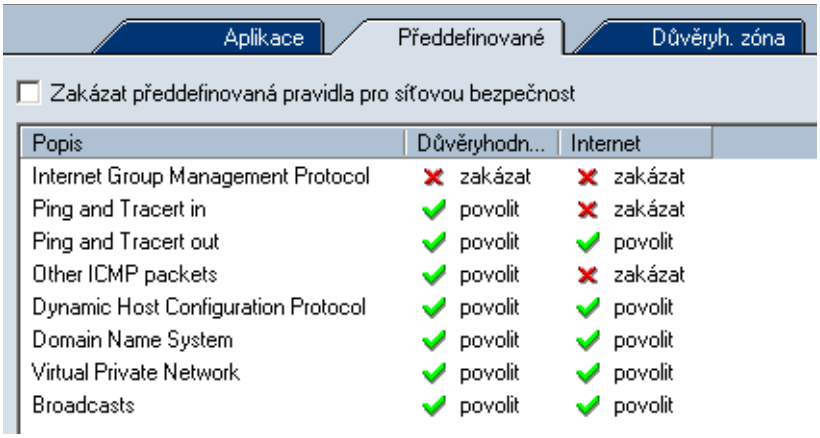
Volba *Zaznamenat komunikaci do záznamu Síť* zapíná záznam komunikace vyhovující tomuto pravidlu do záznamu *Síť* (viz kapitola 11.4).

Volba *Upozornit uživatele* zapíná zobrazování upozornění uživateli (viz kapitola 3.4) při zachycení komunikace vyhovující tomuto pravidlu.

5.3 Předdefinovaná pravidla pro síťovou komunikaci

Pro zjednodušení konfigurace obsahuje *Kerio Personal Firewall* sadu předdefinovaných pravidel pro síťovou komunikaci. Tato pravidla nejsou závislá na aplikacích (platí globálně). Uživatel se může rozhodnout, zda předdefinovaná pravidla použije či nikoliv, případně může upravit jejich nastavení.

Předdefinovaná pravidla pro síťovou komunikaci se nacházejí v sekci *Síťová bezpečnost*, záložka *Předdefinované*.



Pravidla v této záložce nelze přidávat ani odebírat. U každého pravidla lze pouze nastavit akci pro důvěryhodnou zónu a Internet. Nastavení akce se provádí kliknutím levým tlačítkem myši na příslušné místo (tj. v řádce vybraného pravidla ve sloupci *Důvěryhodné* nebo *Internet*). Opakovaným klikáním se střídavě přepínají akce *Povolit* a *Zakázat*.

Poznámka: U předdefinovaných pravidel nelze nastavit akci *Ptát se* (tj. dotázání se uživatele při zachycení odpovídající komunikace — viz kapitoly 5.2 a 3.2).

Volba *Zakázat předdefinovaná pravidla pro síťovou bezpečnost* zakazuje/povoluje předdefinovaná pravidla pro síťovou komunikaci. Je-li tato volba zaškrtnuta, pak jsou předdefinovaná pravidla ignorována a *Kerio Personal Firewall* pracuje pouze s pravidly pro aplikace (viz kapitola 5.2) a s rozšířeným paketovým filtrem (viz kapitola 6).

Tlačítko *Výchozí* obnovuje výchozí nastavení akcí v předdefinovaných pravidlech.

Popis předdefinovaných pravidel

Kerio Personal Firewall obsahuje tato předdefinovaná pravidla pro síťovou komunikaci:

Internet Group Management Protocol Protokol *IGMP* se používá k přihlašování a odhlašování do/ze skupiny příjemců multicastových zpráv. Tento protokol lze poměrně

snadno zneužít, a proto je ve výchozím nastavení zakázán. Povolte jej pouze v případě, provozujete-li aplikace, které využívají technologie multicast zpráv (typicky přenos zvuku či videa po Internetu).

Ping and Tracert in, Ping and Tracert out Programy *Ping* a *Tracert* (*Traceroute*) slouží ke zjištění odezvy vzdáleného počítače, resp. trasování cesty v síti. K tomuto účelu používají zprávy řídicího protokolu *ICMP* (*Internet Control Message Protocol*).

Případný útočník zpravidla nejprve zkouší, zda vybraná IP adresa „žije“ — tj. zda odpovídá na uvedené řídicí zprávy. Blokováním těchto zpráv se počítač stává „neviditelným“, což může snížit pravděpodobnost útoku.

Ve výchozím nastavení jsou blokovány příchozí *Ping* a *Tracert* zprávy z Internetu. Z důvěryhodné zóny jsou tyto zprávy povoleny (předpokládá se, že např. správce sítě bude programem *Ping* testovat dostupnost dané pracovní stanice).

Odchozí *Ping* a *Tracert* zprávy jsou povoleny pro obě zóny. Tyto nástroje jsou totiž velmi často používány pro ověření funkčnosti síťového připojení či dostupnosti vzdáleného počítače.

Other ICMP packets Pravidlo pro ostatní zprávy řídicího protokolu *ICMP* (např. přesměrování, cíl nedostupný apod.).

Dynamic Host Configuration Protocol *DHCP* slouží k automatickému nastavování parametrů TCP/IP (IP adresa, maska subsítě, výchozí brána atd.).

Upozornění: Zakázání *DHCP* může způsobit nefunkčnost síťového připojení vašeho počítače, pokud jsou parametry TCP/IP konfigurovány tímto protokolem!

Domain Name System *DNS* slouží k převodu jmen počítačů na IP adresy. Aby bylo možné zadávat cílové počítače jmény, musí být povolena komunikace alespoň s jedním DNS serverem.

Virtual Private Network Virtuální privátní síť (VPN) je bezpečné propojení dvou lokálních sítí (resp. připojení vzdáleného klienta do lokální sítě) přes Internet šifrovaným kanálem (tzv. tunelem). Pravidlo *Virtual Private Network* kontroluje vytváření VPN protokoly *PPTP* a *IPSec*.

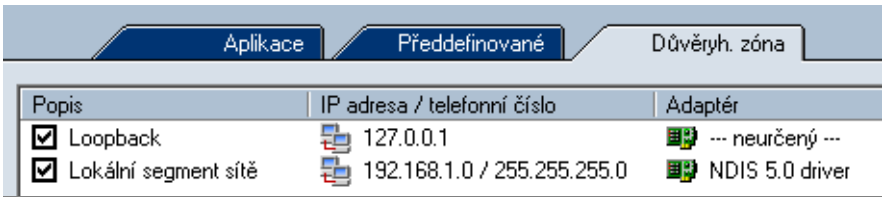
Broadcasts Pravidlo pro pakety se všeobecnou adresou. V zóně *Internet* platí toto pravidlo také pro pakety se skupinovou adresou (multicasts).

5.4 Definice důvěryhodné zóny

Při definici pravidel pro aplikace *Kerio Personal Firewall* rozlišuje dvě skupiny IP adres: důvěryhodnou zónu a Internet. Akce pro příchozí a odchozí komunikaci lze nastavit odděleně pro každou zónu. Důvěryhodná zóna je uživatelsky definovaná skupina IP adres

— jaké adresy budou považovány za důvěryhodné, záleží čistě na rozhodnutí uživatele. Všechny IP adresy, které nepatří do důvěryhodné zóny, jsou automaticky zařazeny do zóny *Internet*.

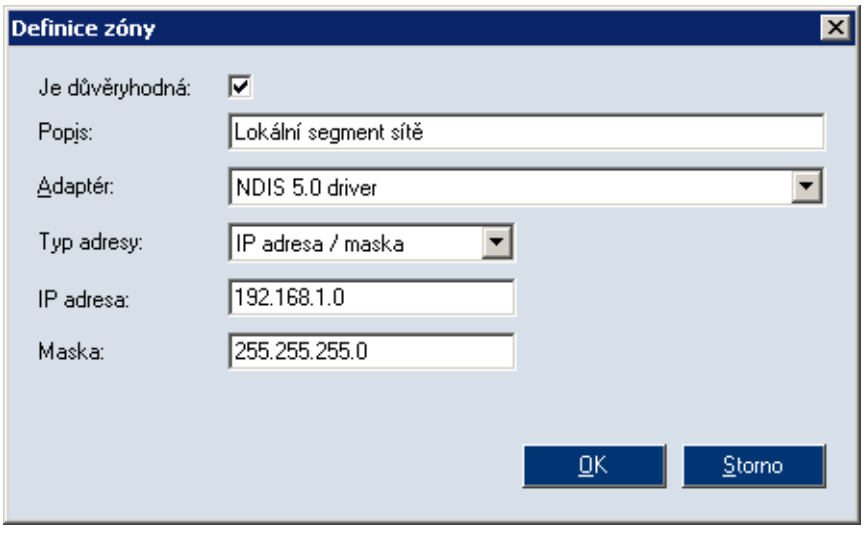
K definici důvěryhodné zóny slouží záložka *Důvěryhodná zóna* v sekci *Síťová bezpečnost*.



Důvěryhodná zóna může obsahovat libovolný počet položek typu IP adresa, rozsah IP adres, subsíť nebo síť připojená k danému rozhraní (podrobnosti viz dále). U každé položky lze volitelně specifikovat rozhraní, na kterém jsou zadané IP adresy povoleny (toto je mj. ochrana proti falšování IP adres).

Důvěryhodná zóna vždy obsahuje jednu předdefinovanou položku *Loopback*, kterou nelze zrušit. Jedná se o lokální zpětnovazební adresu (loopback) — tato adresa je vždy považována za důvěryhodnou.

Tlačítko *Přidat*, resp. *Změnit* otevírá dialog pro přidání, resp. změnu položky důvěryhodné zóny (stejný účinek jako tlačítko *Změnit* má také dvojité kliknutí na vybrané položce).



Je důvěryhodná Tato volba zařazuje/vyřazuje danou položku do/z důvěryhodné zóny. Je-li volba *Je důvěryhodná* vypnuta, uvedené IP adresy (rozsah adres, subsíť atd.) nejsou součástí důvěryhodné zóny (a jsou automaticky zařazeny do zóny *Internet*).

Volbu *Je důvěryhodná* lze využít např. pro explicitní specifikaci IP adres, které do důvěryhodné zóny nepatří. *Kerio Personal Firewall* bude příslušné rozhraní znát a nebude se dotazovat uživatele při zachycení komunikace přes toto rozhraní (viz kapitola 1.7).

Popis Slouží pro zvýšení přehlednosti — doporučujeme uvést stručnou charakteristiku přidávaného rozsahu adres, subsítě atd., případně důvod, proč byly tyto IP adresy do důvěryhodné zóny zařazeny.

Adaptér Výběr adaptéru (rozhraní), na kterém jsou zadané IP adresy platné.

Tato volba je také ochranou proti falšování IP adres — je-li paket s důvěryhodnou IP adresou přijat z jiného rozhraní, než ke kterému je daná síť připojena, pak je považován za nedůvěryhodný.

Speciální volba — *Libovolný* — (libovolný adaptér) znamená, že *Kerio Personal Firewall* nebude kontrolovat, z jakého rozhraní byl paket s danou IP adresou přijat.

Typ adresy Typ položky důvěryhodné zóny:

- *Počítač* — konkrétní IP adresa jednoho počítače (resp. síťového zařízení)
- *IP adresa / mask* — subsíť zadaná IP adresou sítě s odpovídající maskou
- *IP adresa / rozsah* — rozsah IP adres zadaný počáteční a koncovou IP adresou (včetně)
- *Všechny adresy* — libovolná IP adresa

Poznámka: Volbu *Všechny adresy* lze použít pouze ve spojení s konkrétním adaptérem („síť připojená k tomuto rozhraní“). V kombinaci s volbou — *Libovolný* — v položce *Adaptér* bychom totiž nastavili, že všechny IP adresy v Internetu patří do důvěryhodné zóny. Toto nastavení nemá smysl a *Kerio Personal Firewall* jej nepovoluje (tlačítko *OK* je v tomto případě neaktivní).

Kapitola 6

Rozšířený paketový filtr

Paketový filtr umožňuje definovat detailní pravidlo pro určitou síťovou komunikaci. Kromě lokální aplikace a směru komunikace lze určit také protokol, vzdálené IP adresy, vzdálené a lokální porty a další parametry.

Pravidla paketového filtru lze definovat dvěma způsoby:

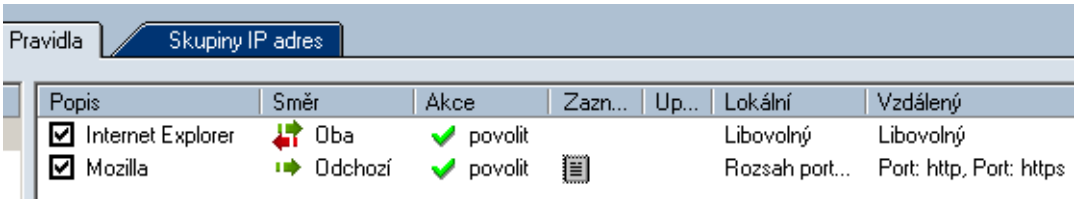
- Ručně — stisknutím tlačítka *Paketový filtr...* v sekci *Síťová bezpečnost*, záložka *Aplikace* se otevře okno *Rozšířený paketový filtr*, ve kterém lze prohlížet, upravovat a rušit pravidla paketového filtru (podrobnosti viz dále).
- Automaticky, resp. poloautomaticky — při zachycení komunikace, pro kterou nebylo nalezeno odpovídající pravidlo, je zobrazen dialog *Upozornění na spojení* (viz kapitola 3.2); zaškrtnutím volby *Vytvořit pravidlo rozšířeného paketového filtru* se namísto standardního pravidla pro aplikace vytvoří pravidlo paketového filtru.

Poznámka: Rozšířený paketový filtr nerozlišuje mezi důvěryhodnou zónou a Internetem (v pravidle je vždy uvedena konkrétní IP adresa, subsíť, skupina IP adres atd.).

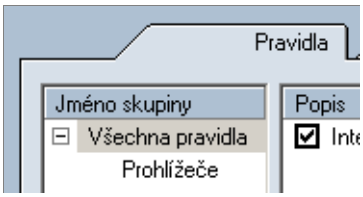
6.1 Pravidla paketového filtru

Pravidla rozšířeného paketového filtru se zobrazují v záložce *Pravidla* okna *Rozšířený paketový filtr*.

Pravidla tvoří uspořádaný seznam. Při zachycení síťové komunikace se seznam prochází shora dolů a použije se první pravidlo, kterému daná komunikace vyhoví. Tlačítky se šipkami nahoru a dolů v pravé části okna lze pořadí pravidel v seznamu upravit dle potřeby. Díky těmto vlastnostem je možno vytvářet složitější kombinace filtrovacích pravidel.



Pro zvýšení přehlednosti lze pravidla paketového filtru řadit do skupin. Členství ve skupině nemá žádný vliv na vyhodnocování pravidel — vždy jsou procházena pravidla ve všech skupinách. Skupiny pravidel se zobrazují v levé části záložky *Pravidla*.



Po kliknutí na jméno skupiny se ve střední části okna zobrazí seznam pravidel patřících do této skupiny.

Následující dvě skupiny jsou předdefinované a nelze je zrušit:

- *Všechna pravidla* („nadřazená skupina“) — obsahuje všechna pravidla paketového filtru
- *Výchozí* (výchozí skupina) — do této skupiny je automaticky zařazeno každé nově vytvořené pravidlo, pokud uživatel nezvolí jinou skupinu.

Poznámka: Skupiny pravidel nelze explicitně vytvářet a rušit. Skupinu lze vytvořit zadáním názvu nové (dosud neexistující) skupiny při definici pravidla. Zaniká automaticky při odstranění posledního pravidla.

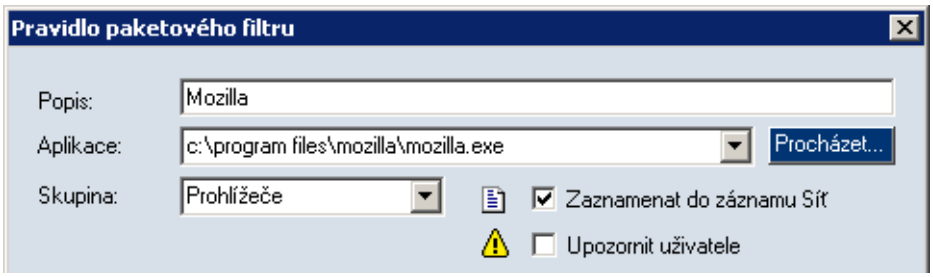
K manipulaci s pravidly paketového filtru slouží tlačítka pod seznamem skupin:

- *Změnit* — úprava vybraného pravidla
- *Přidat* — přidání nového pravidla na konec seznamu
- *Vložit* — přidání (vložení) nového pravidla na aktuální pozici (nad označené pravidlo)
- *Odebrat* — smazání označeného pravidla

Poznámka: Není-li označeno žádné pravidlo, je aktivní pouze tlačítko *Přidat*.

Vytvoření nebo změna pravidla

Po stisknutí tlačítka *Přidat*, *Vložit* nebo *Změnit* se otevře dialog pro definici pravidla paketového filtru. Pravidlo má tyto parametry:



Popis Název/popis pravidla. Do této položky doporučujeme vyplnit stručný popis pravidla (účel pravidla, název aplikace atd.) — výrazně se tím zlepší přehlednost seznamu pravidel. Do automaticky vytvářených pravidel se jako popis vkládá název lokální aplikace, která se účastní dané komunikace.

Aplikace Lokální aplikace, pro kterou pravidlo platí. Aplikaci lze zadat ručně (jméno spustitelného souboru včetně plné cesty), vybrat ze seznamu (při rozbalení této položky se nabídne seznam aplikací použitých v jiných pravidlech) nebo vyhledat na disku počítače (po stisknutí tlačítka *Procházet...* se zobrazí standardní systémový dialog pro otevření souboru).

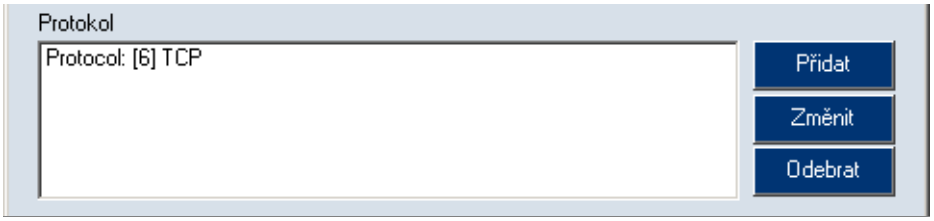
Filtrovací pravidlo může být i obecné, tj. bude platit pro libovolnou aplikaci. Toho dosáhneme výběrem speciální volby *any*, příp. ponecháme pole *Application* prázdné.

Skupina Skupina pravidel, do které má být pravidlo zařazeno. Zařazení do skupiny nemá žádný vliv na funkci pravidla, slouží pouze pro zpřehlednění seznamu pravidel.

V položce *Skupina* lze vybrat některou z již existujících skupin nebo zadat název nové skupiny — tím dojde k vytvoření skupiny, do které bude pravidlo zařazeno. Při vytváření nového pravidla je vždy nastavena výchozí skupina *Výchozí*. Totéž platí pro pravidla vytvářená automaticky (viz výše nebo kapitola 3.2).

Zaznamenat do záznamu Síť Zapnutí/vypnutí záznamu komunikace vyhovující tomuto pravidlu do záznamu *Síť* (viz kapitola 11.4).

Upozornit uživatele Zapnutí/vypnutí zobrazení upozornění uživateli (viz kapitola 3.4) při zachycení komunikace vyhovující tomuto pravidlu.

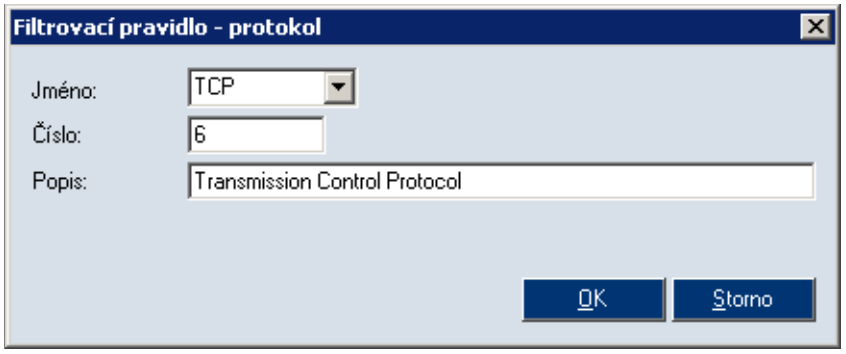


Protokol Nastavení komunikačních protokolů, pro které má pravidlo platit. Typicky je při komunikaci používán jeden protokol (např. TCP nebo UDP), některé aplikace však mohou využívat více protokolů současně (např. TCP a UDP na stejných portech).

Zůstane-li pole *Protocol* prázdné (tj. nezadáme žádný komunikační protokol), bude pravidlo platit pro libovolný komunikační protokol.

Poznámka: Komunikuje-li aplikace protokolem TCP i UDP, přičemž každý protokol používá jiné porty, je třeba v paketovém filtru definovat dvě různá pravidla.

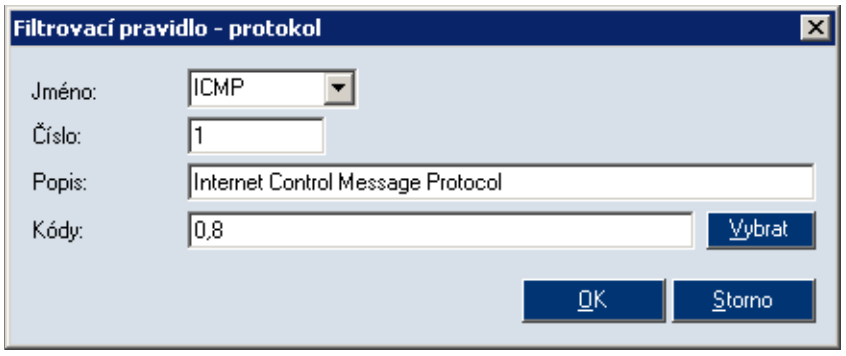
Po stisknutí tlačítka *Přidat* nebo *Změnit* se otevře dialog pro definici protokolu.



Protokol je specifikován číslem protokolu v hlavičce IP paketu. Toto číslo lze přímo zadat do položky *Číslo*. V položce *Jméno* je možno vybrat některý z předdefinovaných standardních protokolů.

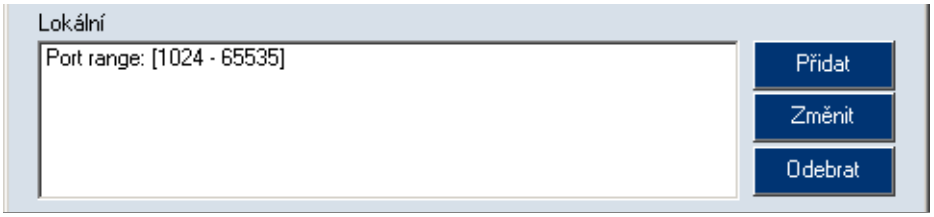
Položka *Popis* slouží k zadání popisu protokolu (pro zvýšení přehlednosti). Zobrazuje se pouze v tomto dialogu.

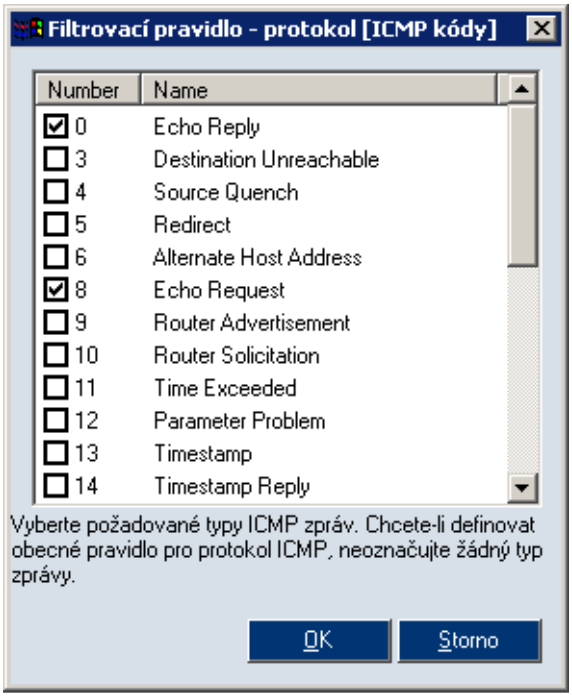
Při výběru protokolu ICMP se v dialogu zobrazí speciální položka *Kódy*. V ní lze nastavit typy ICMP zpráv, pro které bude pravidlo platit.



Typy zpráv se zadávají jejich číselnými kódy (jednotlivé kódy musí být odděleny čárkou). Zůstane-li položka *Kódy* nevyplněna, bude pravidlo platit pro všechny typy ICMP zpráv.

K snadnému nastavení typů ICMP zpráv slouží speciální dialog, který se zobrazí stisknutím tlačítka *Vybrat*. V tomto dialogu je možné vybrat požadované typy ICMP zpráv. Jejich kódy budou po stisknutí tlačítka *OK* automaticky dosazeny do položky *Kódy*.

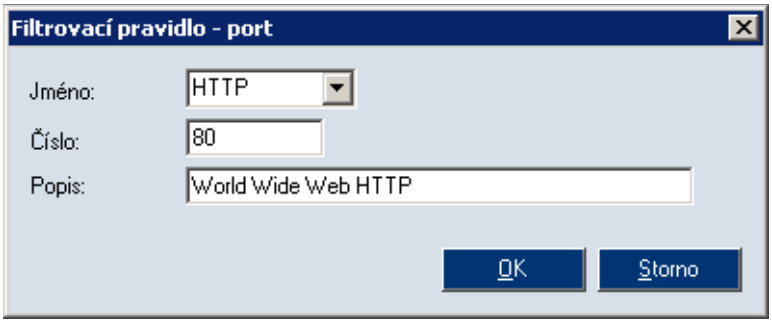




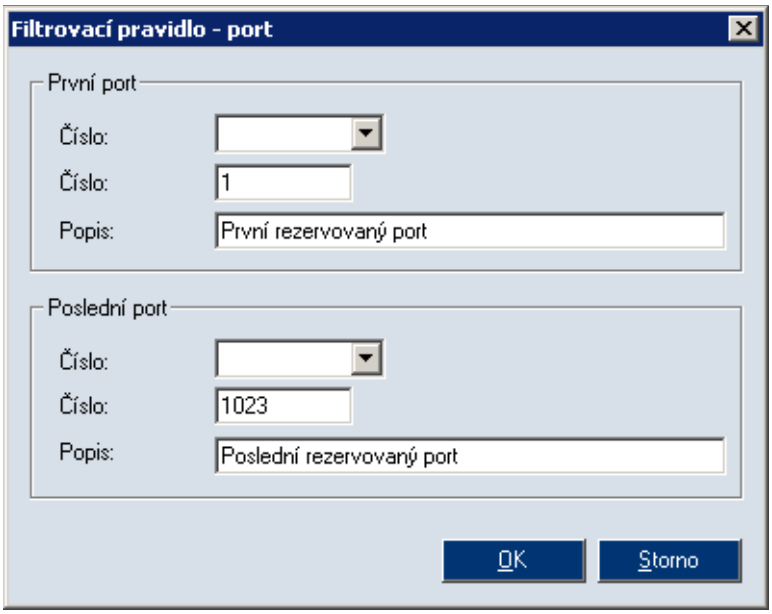
Lokální Specifikace lokální strany spojení. *Kerio Personal Firewall* implicitně používá všechny lokální IP adresy včetně zpětnovazebních (loopback). Z tohoto důvodu lze pro lokální stranu spojení specifikovat pouze porty.

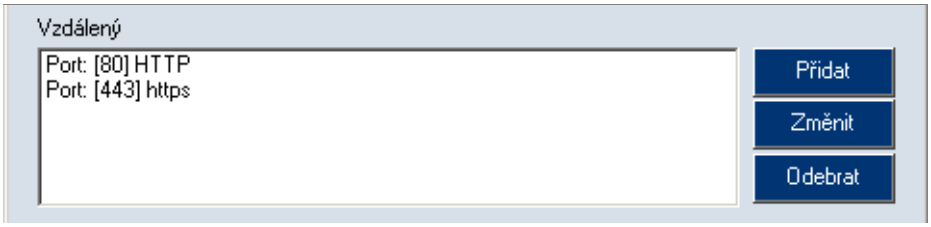
Tlačítkem *Přidat* lze přidat jeden port (*Přidat port*) nebo rozsah portů (*Přidat rozsah portů*). Jednotlivých portů i rozsahů portů může být zadáno více — takto lze pokrýt libovolnou množinu portů.

Port může být zadán číslem v položce *Číslo* (platné jsou pouze hodnoty z rozsahu `1-65535`) nebo výběrem předdefinované standardní služby v položce *Jméno*. Položka *Popis* slouží k zadání popisu portu, resp. služby (pro zvýšení přehlednosti).



V případě rozsahu portů dialog obsahuje dvě části: *První port* (počáteční port rozsahu) a *Poslední port* (koncový port rozsahu).





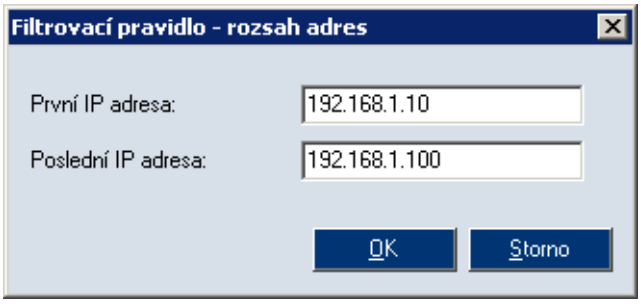
Vzdálený Specifikace vzdálené strany spojení. Dle potřeby je možno zadat IP adresu, port, případně obojí. Pravidlo se pak uplatní, jestliže zachycený paket bude obsahovat některou z IP adres a zároveň některý z portů uvedených v poli *Vzdálený*.

Vzdálený port může být opět zadán jednotlivě (*Přidat port*) nebo jako rozsah portů (*Přidat rozsah portů*).

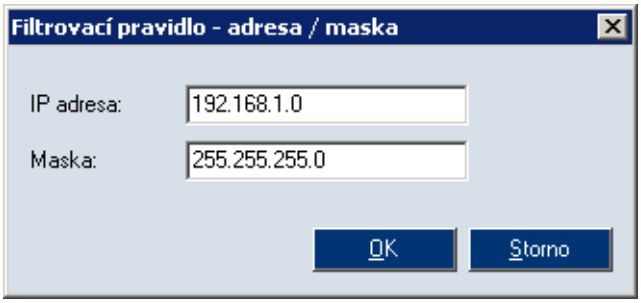
IP adresa může být zadána jako:

- jedna IP adresa (*Přidat adresu*)

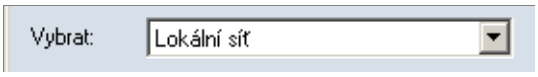
- rozsah IP adres (*Přidat rozsah adres*) — zadáme počáteční a koncovou adresu požadovaného rozsahu



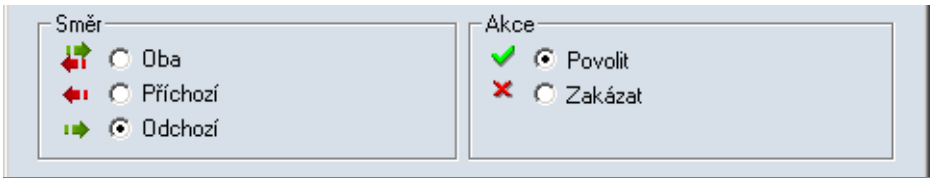
- subsíť (*Přidat adresu / masku*) — zadáme adresu subsítě a odpovídající masku



- skupina IP adres (*Přidat skupinu IP adres*) — v položce *Vybrat* vybereme některou ze skupin IP adres definovaných v záložce *Skupiny IP adres*



Jednotlivé možnosti zadání portů a IP adres lze libovolně kombinovat.



Směr Směr komunikace, pro který má pravidlo platit: oba směry, příchozí komunikace nebo odchozí komunikace.

Směrem komunikace je v tomto případě míněn směr navazování spojení (resp. směr prvního paketu, který zahajuje komunikaci).

Akce Akce, kterou má *Kerio Personal Firewall* provést při zachycení komunikace odpovídající tomuto pravidlu:

- *Povolit* komunikaci
- *Zakázat* komunikaci

Logika vytváření pravidel paketového filtru

Při definici filtrovacího pravidla je třeba znát logické vztahy mezi jednotlivými částmi pravidla a položkami v nich obsaženými.

- Vztah mezi poli *Protokol*, *Lokální* a *Vzdálený* je „a zároveň“. Pravidlu tedy vyhoví komunikace, která splní podmínky ve všech těchto polích.
- Mezi položkami stejného typu (tj. protokoly, IP adresy a porty) v jednom poli platí vztah „nebo“.

  Příklad: Pole *Vzdálený* obsahuje dva rozsahy portů: `80–88` a `8000–8080`. Podmínka bude splněna, bude-li vzdálený port patřit do jednoho z těchto rozsahů.
- Mezi položkami typu „IP adresa“ a „port“ v poli *Vzdálený* platí vztah „a zároveň“.

  Příklad: Pole *Vzdálený* obsahuje IP adresu `65.131.55.1` a port `80`. Tuto podmínku splní komunikace se vzdáleným počítačem s IP adresou `65.131.55.1` na portu `80`.

Poznámky k definici pravidel

Položky *Protocol*, *Lokální* a *Vzdálený* spolu úzce souvisejí. Při definici filtrovacích pravidel by měl uživatel dodržovat několik základních zásad:

1. Porty mají smysl pouze v případě komunikačních protokolů TCP a UDP. U ostatních protokolů jsou ignorovány.

   Platí-li pravidlo pro libovolný protokol (pole *Protokol* je prázdné), pak se porty uplatní v případě, kdy je zachycena komunikace protokolem TCP nebo UDP.
2. Aplikační služba je dána čísly portů a protokoly. V dialogu pro definici filtrovacího pravidla však název služby představuje pouze port — odpovídající protokol je třeba doplnit ručně.

   Příklad: Chceme vytvořit pravidlo pro příchozí HTTP komunikaci (např. povolit přístup na WWW server na počítači, který je chráněn *Kerio Personal Firewallem*).

   - V sekci *Lokální* přidáme jeden port (*Přidat port*), zvolíme službu *HTTP* — tím se nastaví port `80`.
   - V sekci *Protokol* musíme nastavit protokol TCP, který služba HTTP používá.
3. Velmi rošířený je model komunikace klient-server, kdy server čeká na známém (dohodnutém) portu na příchozí spojení. Klient při navazování spojení požádá operační systém o přidělení volného lokálního portu (který není předem znám). Z toho vyplývá, že zatímco port serveru musí být znám, port klienta může být (téměř) libovolný.

Tyto skutečnosti je třeba brát v úvahu při definici pravidel paketového filtru. Pro ilustraci uveďme dva příklady:

Příklad 1: Chceme povolit přístup k WWW serveru na lokálním počítači z počítače s IP adresou `60.80.100.120`. Definujeme pravidlo:

- *Protokol* — `[6] TCP` (služba HTTP využívá transportní protokol TCP)
- *Lokální* — `Port: [80] HTTP` (na lokálním počítači běží WWW server)
- *Vzdálený* — `Address: 60.80.100.120` (na vzdáleném počítači bude provozován klient — WWW prohlížeč; port předem neznáme, proto v pravidle uvedeme pouze IP adresu)

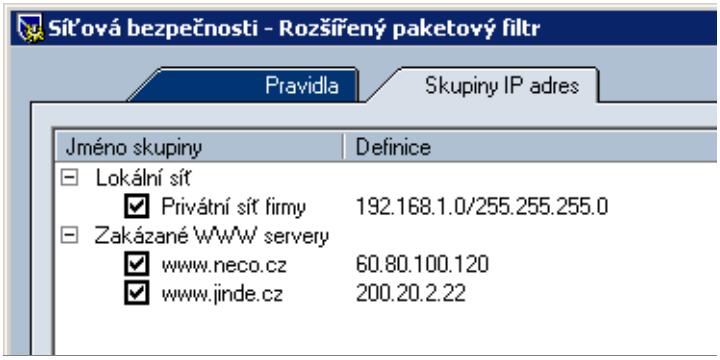
Příklad 2: Z lokálního počítače chceme zakázat přístup k WWW serveru s IP adresou `90.80.70.60`. Pravidlo definujeme takto:

- *Protokol* — `[6] TCP`
- *Lokální* — toto pole ponecháme nevyplněné (port klienta nelze předem určit)
- *Vzdálený* — `Port: [80] HTTP`, `Address: 90.80.70.60` (specifikujeme vzdálený server)

6.2 Skupiny IP adres

Pro snazší definici pravidel paketového filtru je možno vytvářet skupiny IP adres, které pak lze v pravidlech použít v sekci *Remote* dialogu pro editaci pravidel paketového filtru (viz výše).

Skupiny adres se zobrazují a definují v záložce *Skupiny IP adres* okna *Rozšířený paketový filtr*.

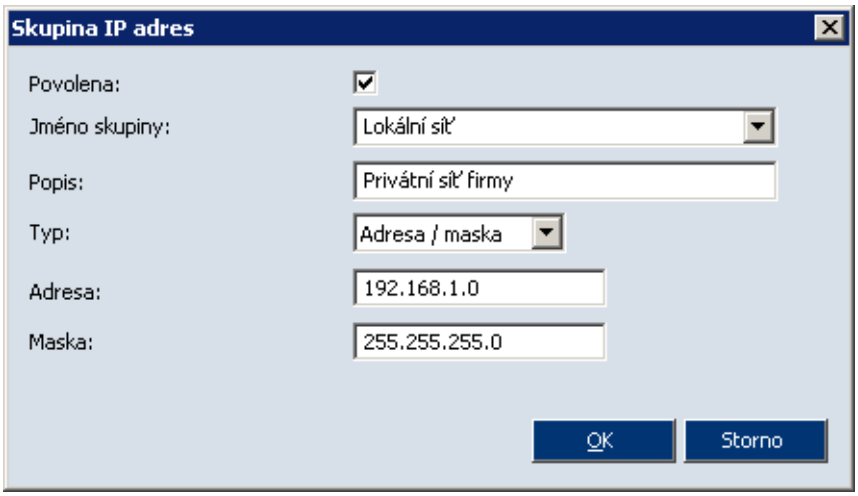


Okno obsahuje dva sloupce:

- *Jméno skupiny* — jméno skupiny IP adres, při rozbalení se pod jménem skupiny zobrazí položky obsažené v této skupině
- *Definice* — obsah (definice) jednotlivých položek skupiny

Zaškrtávací pole vedle popisu položky slouží k dočasnému vyřazení položky ze skupiny. Toho lze využívat např. při experimentování a odhalování chyb — položku není třeba odstraňovat a poté znovu přidávat.

Po stisknutí tlačítka *Přidat* (resp. *Změnit*, je-li vybrána nějaká položka) se otevře dialog pro definici skupiny IP adres.



Povolena Povolení / zakázání položky. Tato volba koresponduje se zaškrtávacím polem vedle názvu položky v záložce *Skupiny IP adres* (viz výše). Je-li volba *Povolena* vypnuta, položka je neaktivní, tzn. není součástí dané skupiny.

Jméno skupiny Jméno skupiny, do které má být položka zařazena. V tomto poli lze:

- vybrat jméno již definované skupiny — položka bude přidána do této skupiny
- zadat jméno nové (dosud neexistující) skupiny — tím dojde k vytvoření nové skupiny a zařazení položky do této skupiny

Typ Typ přidávané položky:

- *Počítač* — IP adresa jednoho počítače
- *Rozsah adres* — rozsah IP adres zadaný počáteční (*První adresa*) a koncovou (*Poslední adresa*) adresou

- *Adresa / maska* — subsíť zadaná adresou sítě s odpovídající maskou
- *Skupina adres* — jiná skupina IP adres (skupiny IP adres lze do sebe libovolně vnořovat).

Kapitola 7

Kontrola spouštěných aplikací (bezpečnost systému)

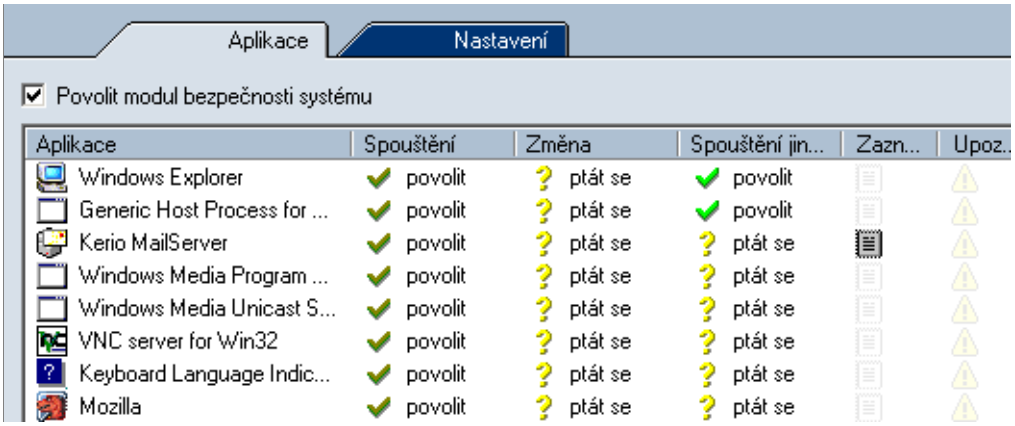
Kerio Personal Firewall má kontrolu nad všemi aplikacemi v operačním systému, bez ohledu na to, zda síťově komunikují či nikoliv. Takto např. dokáže okamžitě odhalit infikaci aplikace novým virem či trojským koněm — narozdíl od antivirového programu, kde vždy existuje určitá prodleva mezi objevením nového viru a příslušnou aktualizací virové databáze.

K nastavení parametrů kontroly aplikací slouží sekce *Bezpečnost systému*.

Volba *Povolit modul bezpečnosti systému* zapíná/vypíná kontrolu spouštěných aplikací. Je-li tato volba vypnuta, pak *Kerio Personal Firewall* spouštění aplikací nesleduje.

7.1 Pravidla pro aplikace

Záložka *Aplikace* v sekci *Bezpečnost systému* obsahuje pravidla pro spouštění a záměnu konkrétních aplikací.

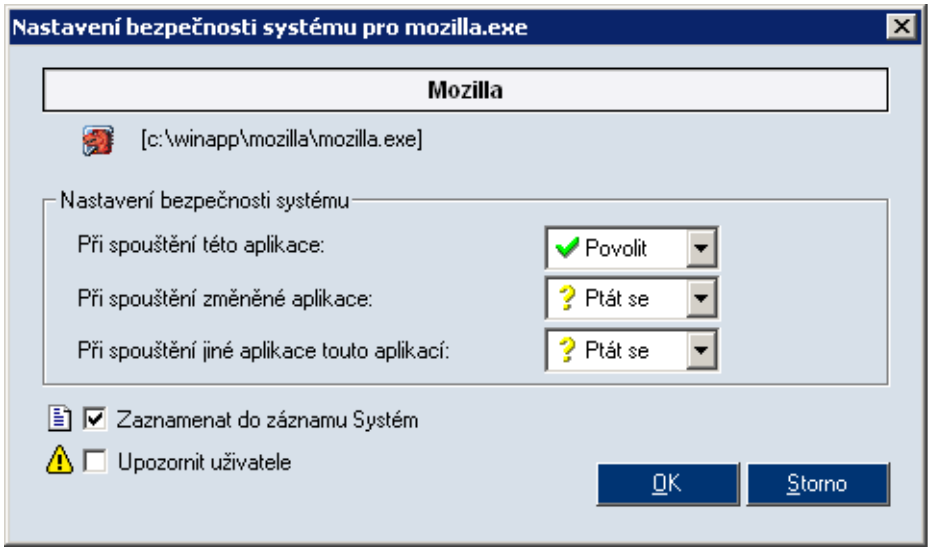


Tato pravidla se vytvářejí na základě interakce s uživatelem při spuštění dosud neznámé aplikace. Pravidla nelze vytvářet ručně, lze pouze měnit jejich nastavení nebo je odstranit.

Pro každou aplikaci může uživatel nastavit akci, kterou má firewall provést při spuštění aplikace, při změně spustitelného souboru aplikace a při spuštění jiné aplikace touto aplikací. Akci lze nastavit:

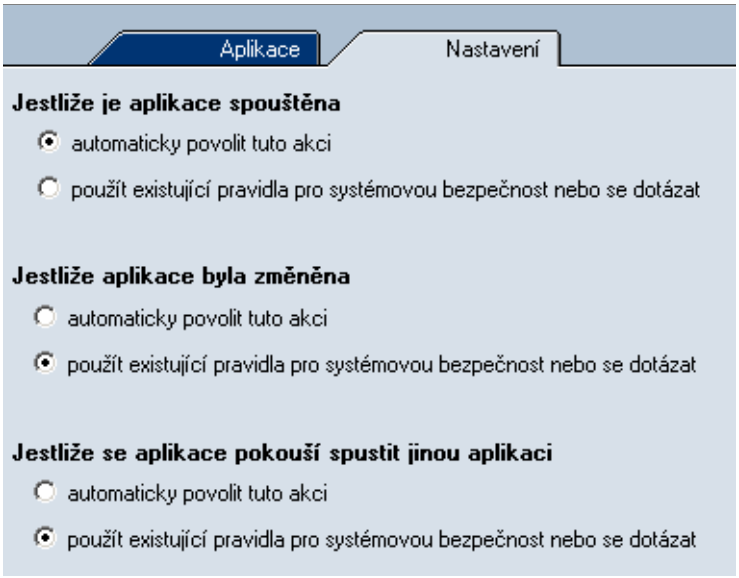
1. přímo v seznamu aplikací — klikáním levým tlačítkem na vybranou akci se cyklicky přepíná: *povolit*, *zakázat* a *ptát se* (dotázat se uživatele)
2. v kontextovém menu, které se zobrazí po kliknutí pravým tlačítkem na vybranou akci

3. v dialogu pro úpravu pravidla. Tento dialog se otevírá tlačítkem *Změnit*, příp. volbou *Změnit* z kontextového menu vybraného pravidla.



- V záhlaví dialogu je zobrazen popis aplikace, ikona a úplná cesta k spustitelnému souboru aplikace.
- Pole *Nastavení bezpečnosti systému* umožňuje nastavení akcí pro výše popsané tři případy.
- Volba *Zaznamenat do záznamu Systém* zapíná/vypíná záznam aktivity příslušné aplikace (tj. spuštění, změna spustitelného souboru nebo spuštění jiné aplikace touto aplikací)
- Volba *Upozornit uživatele* zapíná/vypíná zobrazování upozornění uživateli (viz kapitola 3.4) při aktivitě příslušné aplikace.

7.2 Obecná pravidla



Pravidla v záložce *Nastavení* určují základní chování firewallu v následujících situacích:

- *Jestliže je aplikace spouštěna*
- *Jestliže aplikace byla změněna* — změna spustitelného souboru aplikace (při spuštění aplikace se vytvoří kontrolní součet spustitelného souboru a porovná se s kontrolním součtem, který má *Kerio Personal Firewall* uložen ve své databázi)
- *Jestliže se aplikace pokouší spustit jinou aplikaci*

Pro každý z uvedených případů lze nastavit jednu z těchto možností:

- *automaticky povolit tuto akci* — *Kerio Personal Firewall* neblokuje spouštění aplikace, resp. akceptuje záměnu spustitelného souboru)
- *použít existující pravidla pro systémovou bezpečnost nebo se dotázat* — *Kerio Personal Firewall* použje pravidlo pro danou aplikaci (pokud existuje) nebo se dotáže uživatele, zda tuto akci povolí či nikoliv (viz kapitola 3.3)

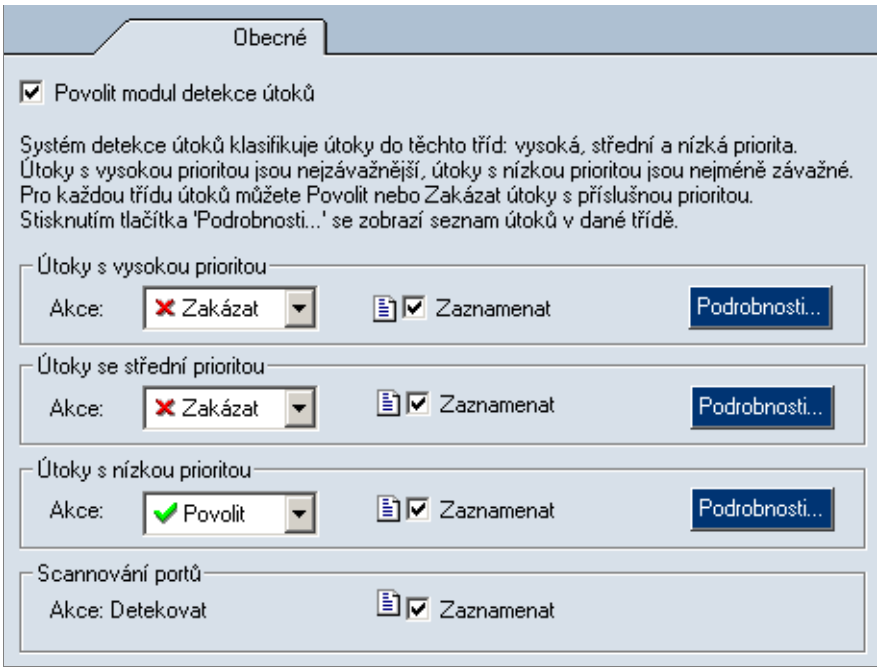
Kapitola 8

Detekce útoků

Kerio Personal Firewall dokáže rozpoznat a blokovat řadu známých typů útoků. K tomuto účelu má vlastní databázi útoků, která je aktualizována s každou novou verzí programu (z tohoto důvodu doporučujeme provádět aktualizaci *Kerio Personal Firewallu* vždy, když se automaticky nabídne).

8.1 Nastavení systému detekce útoků

Parametry systému detekce útoků (*IDS — Intrusion Detection System*) lze nastavit v sekci *Útoky*.



Volba *Povolit modul detekce útoků* zapíná/vypíná systém detekce útoků.

Kerio Personal Firewall rozlišuje tři skupiny útoků:

- *Útoky s vysokou prioritou* — kritické útoky — např. poškození operačního systému, pokusy o ovládnutí systému či únik dat

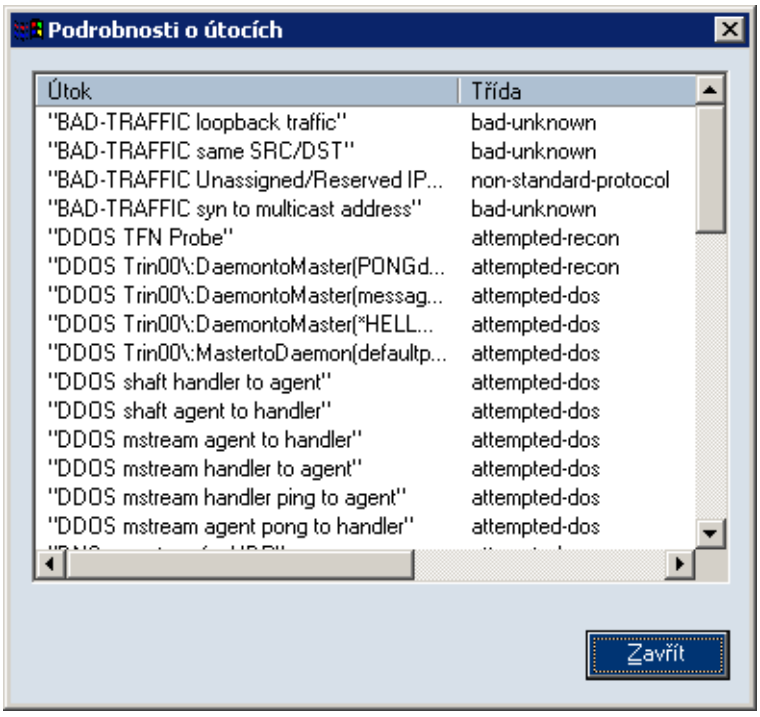
- *Útoky se střední prioritou* — útoky, které způsobují např. blokování určitých služeb, nefunkčnost síťového připojení apod.
- *Útoky s nízkou prioritou* — méně závažné útoky (podezřelé síťové aktivity, chyby v protokolech, neplatný formát dat apod.)

Pro každou z těchto skupin lze odděleně nastavit chování firewallu:

- *Akce* — reakce firewallu na útoky z této skupiny (*Povolit* nebo *Zakázat*, tj. blokovat).

  Obecně je doporučeno blokovat útoky skupin *Útoky s vysokou prioritou* a *Útoky se střední prioritou* — nepovolujte útoky těchto skupin, pokud si nejste skutečně jisti, co a proč děláte (např. experimentální účely). *Útoky s nízkou prioritou* jsou ve výchozím nastavení povoleny — jejich blokování by mohlo způsobovat nefunkčnost určitých služeb.
- *Zaznamenat* — záznam všech detekovaných útoků z této skupiny do logu *Útoky* (viz kapitola 11.6).

Tlačítko *Podrobnosti* zobrazí okno se seznamem útoků v dané skupině.



Okno obsahuje název (popis) útoku (sloupec *Útok*) a třídu útoku (sloupec *Třída*). *Kerio Personal Firewall* používá IDS typu *Snort* — podrobné informace naleznete na WWW stránkách `http:/www.snort.org/`.

Speciálním případem útoku je tzv. *Scannování portů* (vyhledávání otevřených portů na daném počítači). Z definice scannování portů vyplývá, že jej není možné zcela blokovat, pokud má uživatel otevřené nějaké porty (uzavřené porty se automaticky blokují). *Kerio Personal Firewall* jej pouze detekuje — volba *Zaznamenat* zapíná/vypíná záznam o scannování portů do logu *Útoky*.

Kapitola 9

Filtrování obsahu WWW stránek

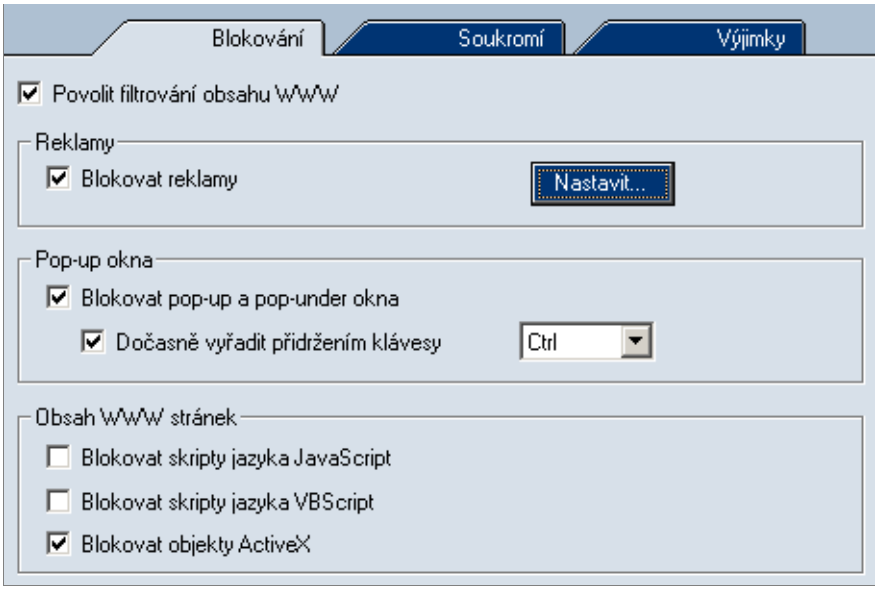
Filtr obsahu WWW stránek v *Kerio Personal Firewallu* má dvě hlavní funkce:

- blokování reklam (tj. bannerů, pop-up oken, skriptů atd.)
- ochrana soukromí (tj. kontrola odesílaných dat a ukládaných cookies)

K nastavení parametrů filtrování obsahu slouží sekce *WWW* konfiguračního okna *Kerio Personal Firewallu*.

Volba *Povolit filtrování obsahu WWW* v záložce *Blokování* zapíná/vypíná filtrování obsahu. Je-li tato volba vypnuta, pak neprovádí *Kerio Personal Firewall* kontrolu obsahu WWW stránek.

9.1 Blokování reklam, skriptů a pop-up oken



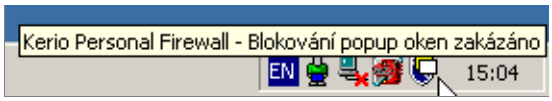
Kerio Personal Firewall má tyto možnosti filtrování nežádoucích prvků WWW stránek:

Blokovat reklamy Blokování reklam podle definovaných pravidel. Tlačítko *Nastavit* otevírá dialog pro definici těchto pravidel (viz dále).

Blokovat pop-up a pop-under okna Zákaz otevírání nevyžádaných oken prohlížeče (*pop-up* = okno otevřené nad aktuálním oknem, *pop-under* = okno otevřené pod aktuálním oknem — uživatel reklamu spatří po uzavření okna s navštívenou stránkou).

Dočasně vyřadit přidržením klávesy Po zapnutí této volby bude uživatel moci přidržením zvolené klávesy (*Ctrl* nebo *F12*) vyřadit funkci blokování pop-up a pop-under oken dle potřeby (např. po dobu otevírání konkrétní WWW stránky).

Vyřazení blokování pop-up oken je indikováno ikonou *Kerio Personal Firewallu* na nástrojové liště.



Upozornění: Klávesa *F12* může vykazovat kolize v debuggeru firmy *Microsoft*. Používáte-li vývojový nástroj *Microsoft Visual Studio*, doporučujeme pro dočasné vyřazení blokování pop-up oken nastavit klávesu *Ctrl*.

Blokovat skripty jazyka JavaScript, VBScript Filtrování všech příkazů příslušného skriptovacího jazyka z WWW stránek.

Blokovat objekty ActiveX Filtrování všech ActiveX komponent z WWW stránek.

Poznámka: Výše uvedené tři volby mohou v určitých případech způsobit nesprávné zobrazování některých stránek. Pokud taková situace nastane, je třeba definovat výjimky pro konkrétní stránky v záložce *Výjimky*, případně tyto volby nezapínat a filtrovat reklamy jiným způsobem (např. volbou *Blokovat reklamy*).

Pravidla pro filtrování reklam

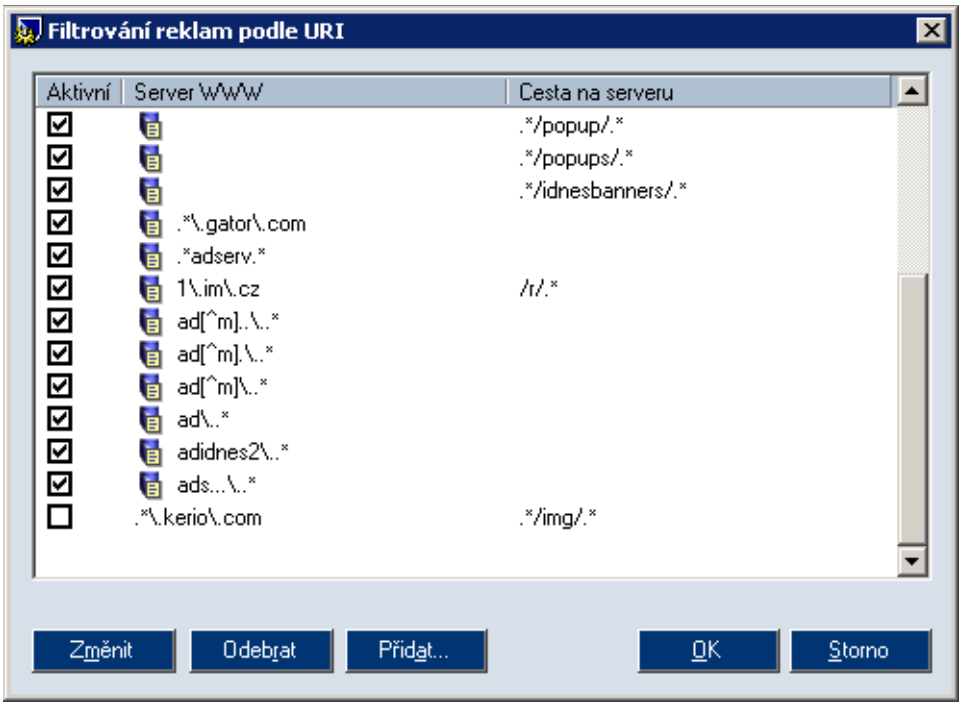
Tlačítko *Nastavit* otevírá okno s pravidly pro filtrování reklam.

Každé pravidlo je složeno ze dvou částí: *Serverová část* (jméno nebo IP adresa WWW serveru) a *Lokální část* (relativní adresa objektu na daném serveru).

Pokud je vyplněna pouze jedna z těchto položek, pak:

- je-li položka *WWW server* prázdná, platí pravidlo pro uvedenou relativní adresu na libovolném serveru
- je-li položka *Cesta na serveru* prázdná, pak pravidlo platí pro libovolný objekt na uvedeném serveru (de facto blokování přístupu na tento WWW server)

Zaškrtávací pole ve sloupci *Aktivní* zapíná/vypíná příslušné pravidlo. Takto lze pravidlo dočasně „vyřadit“ bez nutnosti jej odstraňovat a poté znovu přidávat.



Tlačítka *Změnit*, *Odebrat* a *Přidat* slouží pro úpravu či odstranění vybraného pravidla, resp. přidání nového pravidla.

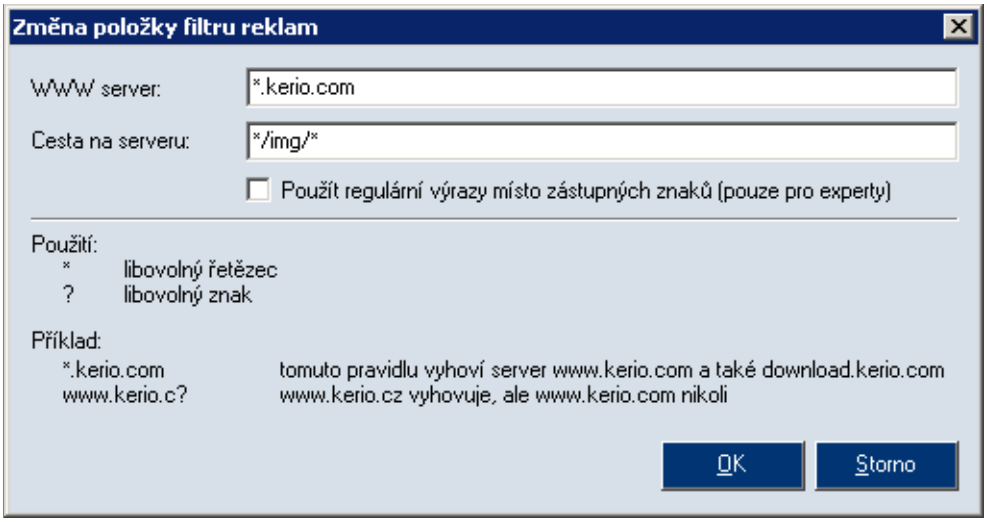
Kerio Personal Firewall má vlastní databázi předdefinovaných pravidel, která jsou označena ikonou. Předdefinovaná pravidla nelze změnit ani odstranit, lze je pouze aktivovat a deaktivovat. Databáze předdefinovaných pravidel je aktualizována při instalaci nové verze *Kerio Personal Firewallu*. Při aktualizaci zůstane zachováno nastavení sloupce *Aktivní* (tzn. při aktualizaci se neaktivují pravidla, která uživatel vypnul).

Tlačítko *Přidat* nebo *Změnit* otevírá dialog pro definici pravidla filtru reklam. Pravidlo sestává ze dvou částí:

- *WWW server* — jméno WWW serveru
- cesta na serveru — cesta k objektu (umístění objektu) na tomto serveru

Při definici serverová a lokální část mohou být použity buď zástupné znaky (jednodušší definice) nebo regulární výrazy (komplexní definice, pro zkušené uživatele).

Definice pravidla pomocí zástupných znaků



Je-li volba *Použít regulární výrazy místo zástupných znaků* vypnuta, pak lze v položkách *WWW server* a *Cesta na serveru* použít tyto dva zástupné znaky:

- * (hvězdička) — nahrazení libovolného (i nulového) počtu znaků
- ? (otazník) — nahrazení právě jednoho znaku

Příklady:

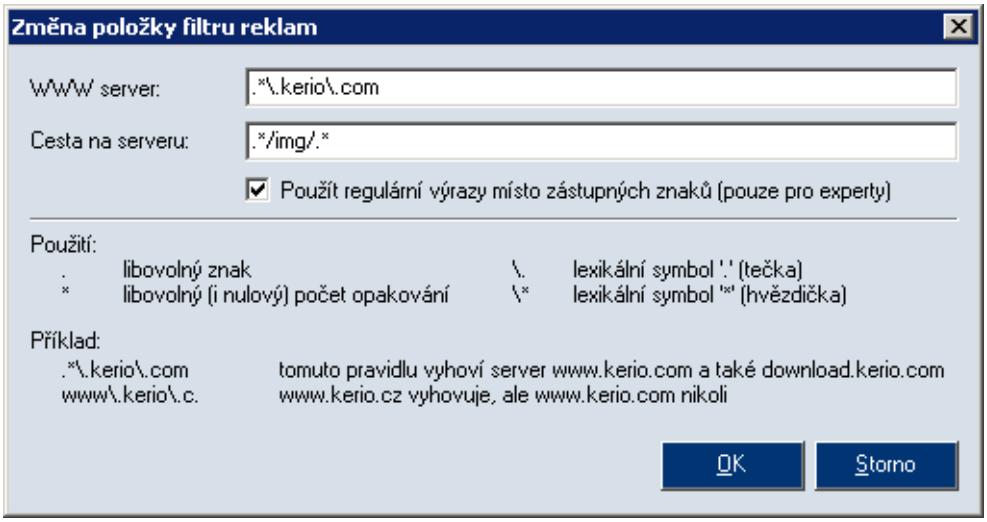
- Položka *WWW server* obsahuje řetězec `*.kerio.com`. Tomuto pravidlu vyhoví WWW servery `www.kerio.com` nebo `download.kerio.com`, ale nevyhoví např. `www.akerio.com`.
- Položka *WWW server* obsahuje řetězec `www.kerio.c?`. Tomuto pravidlu vyhoví WWW servery `www.kerio.cz` nebo `www.kerio.cx`, ale nevyhoví `www.kerio.com`.

Definice pravidla pomocí regulárních výrazů

Je-li zapnuta volba *Použít regulární výrazy místo zástupných znaků*, musít být položky *WWW server* a *Cesta na serveru* zadány formou tzv. regulárních výrazů standardu POSIX. Regulární výrazy umožňují popsat libovolný řetězec pomocí speciální symboliky.

Při definici adres WWW serverů a objektů pravděpodobně vystačíme s několika základními symboly:

- `.` (tečka) — nahrazuje libovolný znak v řetězci.
- * (hvězdička) — znamená libovolný (i nulový) počet opakování předchozího symbolu.



Př.: Výraz `.*` představuje libovolný počet libovolných znaků, tj. jakýkoliv (i prázdný) řetězec (text).

- \ (zpětné lomítko) — slouží k zadání znaku, který má v regulárním výrazu speciální význam.

  Př.: Výraz `\.` představuje znak „tečka“.

Příklad (viz obrázek):

- Položka *WWW server* obsahuje výraz `.*\.kerio\.com`.

  Tento výraz znamená, že jméno serveru musí obsahovat podřetězec `.kerio.com` — tedy např. `www.kerio.com`, `download.kerio.com`, `www.kpf.kerio.com` apod.

- Položka *Cesta na serveru* obsahuje výraz `.*/img/.*`.

  To znamená, že relativní adresa objektu na serveru musí obsahovat podřetězec `/img/` — tedy např. `/img/banner.gif`, `/data/img/bar.jpg` nebo pouze `/img/`.

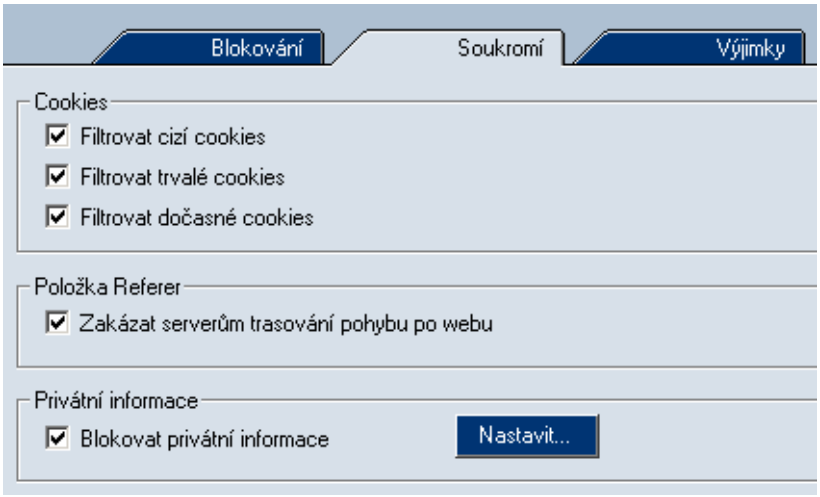
Podrobné informace o regulárních výrazech lze nalézt např. na adrese:

`http://www.gnu.org/software/grep/`

9.2 Ochrana soukromí uživatele

Záložka *Soukromí* obsahuje tyto volby pro ochranu soukromí uživatele:

Filtrovat cizí cookies Filtrování trvalých i dočasných cookies z jiných serverů (*3rd party cookies*).



Jedná se o cookies načítané z jiných WWW serverů než vlastní stránka (typickým příkladem jsou cookies reklam).

Filtrovat trvalé cookies Filtrování trvale ukládaných cookies.

Tyto cookies obsahují informace, které mohou být odeslány na WWW server při příští návštěvě dané stránky — server tak získá informaci o tom, že uživatel v minulosti tuto stránku již navštívil, o jeho uživatelském nastavení nebo libovolné jiné údaje.

Filtrovat dočasné cookies Filtrování dočasných cookies (ukládaných pouze po dobu jedné relace, tj. do ukončení WWW prohlížeče). Tyto cookies se používají při návratu na příslušnou stránku (resp. WWW server či server v dané doméně) v rámci této relace. Po uzavření všech oken WWW prohlížeče jsou všechny dočasné cookies smazány.

Zakázat serverům trasování pohybu po webu Blokování položky `Referer` v hlavičce protokolu HTTP.

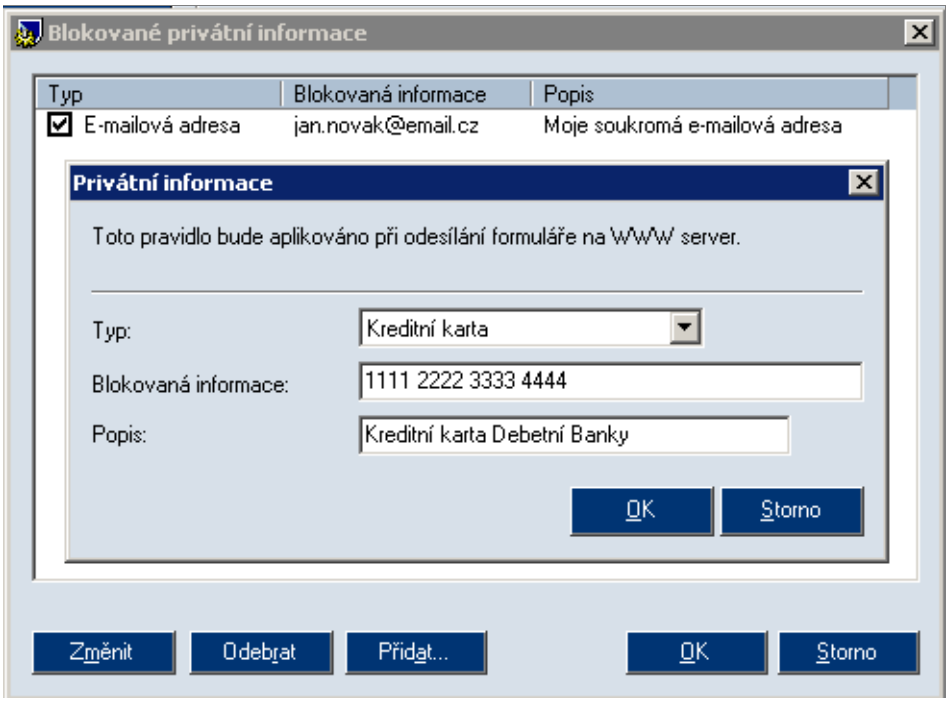
Tato položka obsahuje URL stránky, ze které uživatel na danou stránku přišel. Sledováním položky `Referer` lze mapovat pohyb uživatelů po Internetu.

Blokovat privátní informace Zákaz odesílání definovaných privátních informací z formulářů na WWW stránkách.

Tlačítko *Nastavit* otevírá okno pro definici privátních informací, jejichž odesílání má *Kerio Personal Firewall* blokovat.

Privátní informace se v *Kerio Personal Firewallu* definuje takto:

- *Typ* — výběr typu informace (např. e-mailová adresa, číslo kreditní karty atd.).

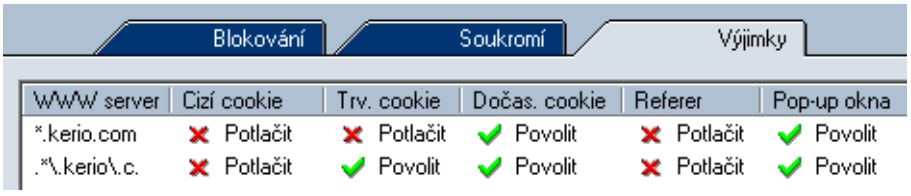


Tato položka má pouze informativní charakter a nesouvisí s typem pole na WWW stránce.

- *Blokovaná informace* — vlastní informace, tj. řetězec, jehož odeslání bude *Kerio Personal Firewall* blokovat.
- *Popis* — popis privátní informace (libovolný text, slouží pro zvýšení přehlednosti).

9.3 Výjimky pro jednotlivé WWW servery

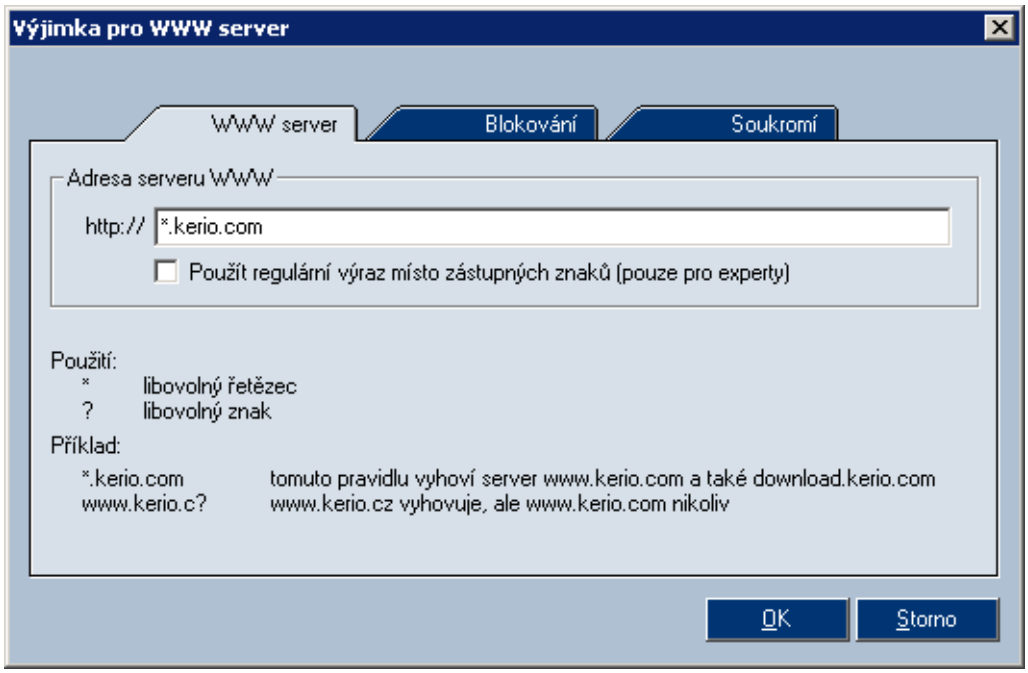
Záložka *Výjimky* umožňuje specifikovat WWW servery, pro které budou nastavena vlastní pravidla filtrování obsahu WWW stránek.



Výjimky pro jednotlivé WWW servery jsou užitečné zejména v případech, kdy obecná pravidla pro obsah WWW stránek (v záložkách *Blokování* a *Soukromí*) způsobují nefunkčnost určitých stránek (např. otevírání nových oken, přihlašování pomocí e-mailové

adresy apod.) nebo jejich úplné zablokování (v důsledku pravidel pro filtrování reklam). Při definici výjimky pro konkrétní server doporučujeme zvážit, zda se jedná o důvěryhodný server a které typy objektů (skripty, cookies, privátní informace) jsou skutečně nutné pro správnou funkci stránek na tomto serveru.

Tlačítko *Přidat*, resp. *Změnit* otevírá dialog pro definici výjimky.



Záložka *WWW server* slouží k zadání jména WWW serveru. Ve jméně serverů lze použít zástupné znaky nebo jej zadat formou regulárního výrazu (podrobnosti viz blokování reklam — viz kapitola 9.1).

Záložky

Blokování a *Soukromí* jsou téměř identické s odpovídajícími záložkami sekce *WWW*. Zde však jednotlivé volby platí pouze pro uvedený WWW server.

Kapitola 10

Stavové informace

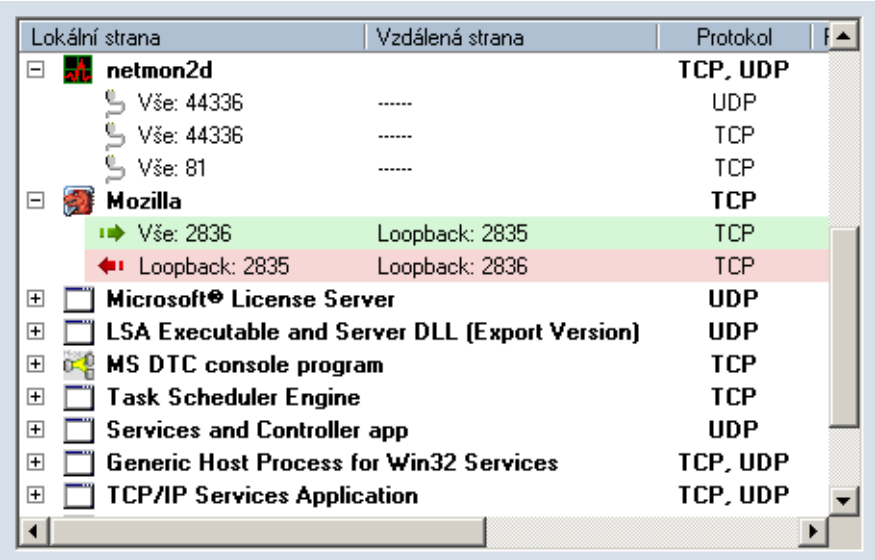
10.1 Přehled spojení a otevřených portů

V sekci *Přehled*, záložka *Spojení*, se zobrazuje seznam spojení a portů otevřených jednotlivými aplikacemi. Uživatel tak má kompletní přehled, jaké aplikace na jeho počítači síťově komunikují nebo čekají na navázání spojení.

Port označujeme jako otevřený, jestliže je v jednom z následujících stavů:

- navázané odchozí spojení (zelené podbarvení)
- navázané příchozí spojení (červené podbarvení)
- čeká na navázání spojení — serverový režim (bez podbarvení)

V záložce *Spojení* se zobrazuje seznam aplikací, které mají otevřen alepoň jeden port.



Na prvním řádku je vždy uvedena ikona a název (popis) aplikace (nemá-li aplikace ikonu, použije se systémová ikona pro spustitelný soubor; není-li k dispozici popis aplikace, zobrazí se jméno souboru bez přípony). Kliknutím na tlačítko [+] nebo [–] vedle ikony aplikace lze zobrazit, resp. skrýt seznam portů otevřených touto aplikací.

V dalších řádcích jsou pak zobrazena jednotlivá otevřená spojení. Jedná-li se o odchozí spojení, řádek je zvýrazněn světle zelenou barvou; příchozí spojení jsou zvýrazněna světle červenou barvou. Jednotlivé sloupce zobrazují podrobné informace o každém spojení:

Lokální strana Lokální IP adresa (příp. odpovídající DNS jméno) a port (příp. název služby, jedná-li se o standardní službu).

Namísto DNS jména počítače mohou být uvedena tato speciální jména:

- *Vše* — port je otevřen na všech lokálních IP adresách (IP adresa `0.0.0.0`)
- *Loopback* — lokální zpětnovazební IP adresa (`127.0.0.1`)

Vzdálená strana IP adresa (resp. DNS jméno) a číslo portu (resp. název služby) vzdáleného počítače. Platí totéž jako pro lokální adresu a port (viz výše).

Protokol Použitý transportní protokol (*TCP* nebo *UDP*, příp. oba).

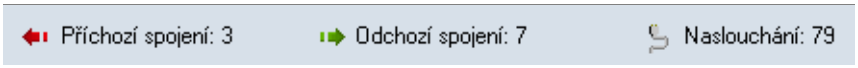
Rychlost příchozí, Rychlost odchozí Aktuální rychlost přijímaných (příchozích) a odesílaných (odchozích) dat v rámci daného spojení. Rychlost je uváděna v kilobytech za sekundu (KB/s).

Přijato bytů, Vysláno bytů Celkový objem dat přijatých a vyslaných v rámci daného spojení.

Poznámka: Jedná-li se o port, na kterém aplikace čeká na příchozí spojení, pak je známa pouze lokální IP adresa, lokální port a protokol.

Otevřené porty a navázaná spojení

V dolní části záložky *Spojení* (stavovém řádku) se zobrazuje aktuální počet spojení a otevřených portů:



- *Příchozích spojení* — počet navázaných příchozích spojení (tj. ze vzdáleného počítače na lokální počítač)
- *Odchozí spojení* — počet navázaných odchozích spojení (tj. z lokálního počítače na vzdálený počítač)
- *Naslouchání* — počet portů, na kterých aplikace čekají na navázání spojení

10.2 Statistiky

V sekci *Přehled / Statistiky* lze zobrazit statistiky systému detekce útoků a filtru obsahu WWW stránek za zvolené časové období.

Položka *Zobrazit statistiky za poslední ...* slouží k výběru časového období, za které budou statistiky zobrazovány:

- poslední hodina
- poslední den
- poslední týden
- poslední měsíc

Statistiky jsou rozděleny do skupin:

Reklamy Blokované reklamy a komponenty WWW stránek:

- *Reklamy* — počet objektů blokovaných pravidly pro filtrování reklam
- *Pop-up okna* — počet blokovaných pop-up a pop-under oken

Skripty

- *Skripty JavaScript* — počet filtrovaných skriptů v jazyce *JavaScript*
- *Skripty VBScript* — počet filtrovaných skriptů v jazyce *Visual Basic Script*
- *Objekty ActiveX* — počet filtrovaných ActiveX komponent

Útoky Počet detekovaných útoků:

- *Vysoká priorita* — kritické útoky
- *Střední priorita* — útoky se střední prioritou (např. blokování služeb)
- *Nízká priorita* — útoky s nízkou prioritou (např. podezřelé aktivity)
- *Scan portů* — zjišťování otevřených portů (*Port Scanning*)

Soukromí Počet objektů blokovaných ochranou soukromí uživatele:

- *Položky Referer* — počet filtrovaných položek `Referer` z hlavičky protokolu HTTP
- *Privátní informace* — počet zablokovaných odesílaných privátních informací

Cookies Počet blokovaných cookies jednotlivých typů:

- *Trvalé cookies* — počet filtrovaných trvalých cookies
- *Dočasné cookies* — počet filtrovaných dočasných cookies
- *Cizí cookies* — počet filtrovaných cizích cookies

Kapitola 11

Záznamy

Záznamy jsou soubory, které uchovávají historii určitých událostí.

Kerio Personal Firewall má samostatný záznam pro každý modul (*Síť*, *Systém*, *Útoky* a *WWW*).

Dále existují záznamy *Error* (chybová hlášení), *Warning* (varovná hlášení) a *Debug* (ladicí informace), do kterých se zapisují informace vztahující se k běhu programu *Kerio Personal Firewall*. Informace v těchto záznamech mohou být užitečné například při řešení problémů s technickou podporou firmy *Kerio Technologies*.

Soubory záznamů jsou uloženy v podadresáři `logs` adresáře, kde je *Kerio Personal Firewall* nainstalován (typicky `C:\Program Files\Kerio\Personal Firewall 4\logs`). Vlastní soubor záznamu má příponu `.log` (např. `network.log`). Ke každému záznamu přísluší tzv. indexový soubor (pro vyhledávání). Tento soubor má příponu `.idx` (např. `network.log.idx`).

11.1 Prohlížení záznamů

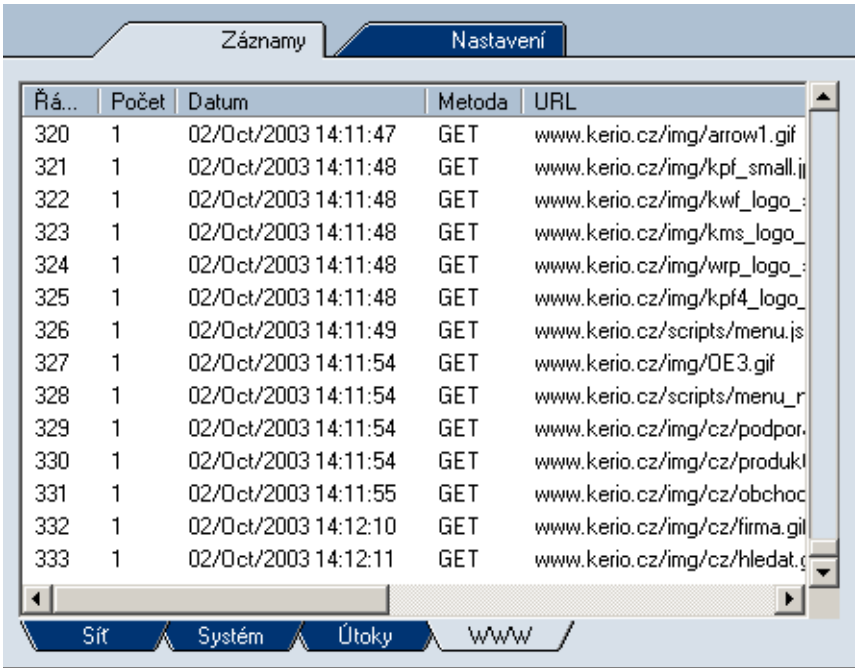
K prohlížení záznamů jednotlivých modulů firewallu a nastavení záznamů slouží sekce *Záznamy*.

Záložka *Záznamy* obsahuje v dolní části podzáložky se záznamy jednotlivých modulů firewallu. V každé záložce se zobrazuje vždy určitá část příslušného souboru záznamu. Kliknutím na název sloupce lze zobrazenou část záznamu seřadit podle vybraného sloupce.

Z technických důvodů (objem dat) nejsou soubory záznamů načítány celé do paměti. Ze souboru se načte pouze část, která má být zobrazena. Proto při prohlížení záznamů dochází k následujícím jevům:

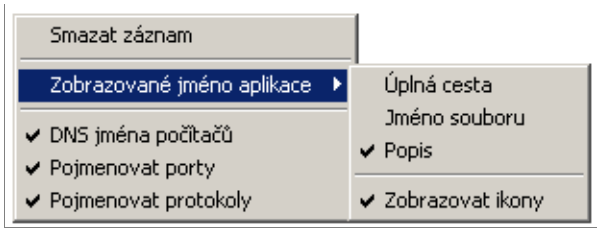
- Zobrazování je při pohybu v záznamu relativně pomalé.
- Při řazení podle vybraného sloupce je seřazena pouze aktuálně zobrazená část záznamu. Po přesunu na jinou část záznamu je třeba zobrazené informace znovu seřadit.

Poznámka: Záznamy *Error*, *Warning* a *Debug* nejsou z uživatelského rozhraní *Kerio Personal Firewall* přístupné — lze je prohlížet pouze jako soubory.



11.2 Kontextové menu pro záznamy

Při stiskutí pravého tlačítka v záložce se záznamem se zobrazí kontextové menu s volbami pro daný záznam:



Smazat záznam Tato volba smaže veškeré informace z příslušného souboru — smazaný záznam již nelze obnovit.

Zobrazované jméno aplikace Způsob zobrazování jmen aplikací:

- *Úplná cesta* ke spustitelnému souboru aplikace
- *Jméno* spustitelného souboru aplikace
- *Popis* aplikace (je-li k dispozici, jinak je zobrazeno jméno spustitelného souboru bez přípony)

Volba *Zobrazovat ikony* zapíná/vypíná zobrazování ikon aplikací (nemá-li aplikace ikonu, použije se systémová ikona pro spustitelný soubor).

DNS jména počítačů Zobrazování jmen počítačů namísto IP adres.

Jména počítačů se zjišťují z DNS (asynchronně). Dokud se nepodaří nalézt odpovídající jméno, je zobrazena IP adresa.

Pojmenovat porty Zobrazování jmen služeb namísto čísel portů (pouze pro standardní služby definované v systémovém souboru `services`).

Pojmenovat protokoly Zobrazování názvů (zkratek) protokolů namísto čísla protokolu (pouze pro standardní protokoly definované v systémovém souboru `protocols`).

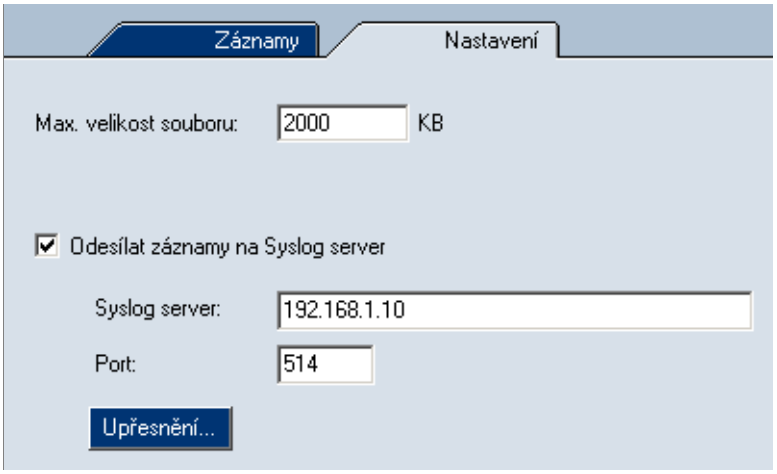
Poznámky:

1. V některých záznamech neobsahuje kontextové menu všechny výše popsané položky — např. v záznamu *Systém* se nezobrazuje žádná síťová komunikace, a proto zde nejsou volby *DNS jména počítačů*, *Pojmenovat porty* a *Pojmenovat protokoly*.

2. Volby *Zobrazované jméno aplikace*, *DNS jména počítačů* a *Pojmenovat porty/protokoly* mají globální platnost — jejich nastavení ovlivňuje všechny záznamy, sekci *Přehled / Spojení* (viz kapitola 10.1), dialogy *Upozornění na spojení* (kap. 3.2) a *Spouštění/Záměna/Spouštění jiné aplikace* (kap. 3.3) a okno s upozorněním (kap. 3.4). Nastavení zobrazování je rovněž popsáno v příslušných kapitolách.

11.3 Volby pro záznamy

V záložce *Nastavení* sekce *Záznamy* lze nastavit následující parametry a volby pro záznamy (nastavení platí pro všechny záznamy *Kerio Personal Firewallu*):

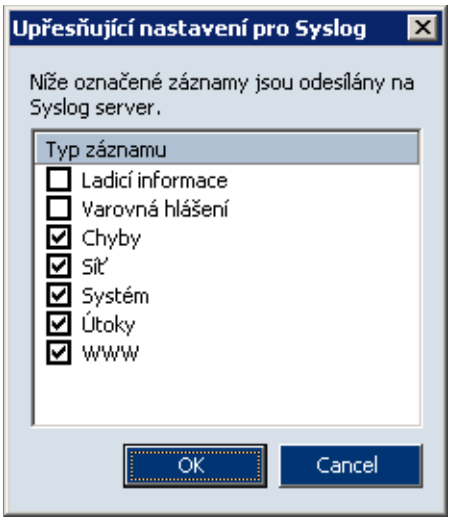


Max. velikost souboru Maximální velikost souboru záznamu (v kilobytech). Dosáhne-li soubor záznamu této velikosti, bude smazán a zapisován opět od začátku.

Odesílat záznamy na Syslog server Tato volba zapíná/vypíná odesílání vybraných záznamů na *Syslog* server.

Do položky *Syslog server* je třeba zadat jméno nebo IP adresu *Syslog* serveru a do položky *Port* číslo portu, na kterém *Syslog* server běží (standardně 514).

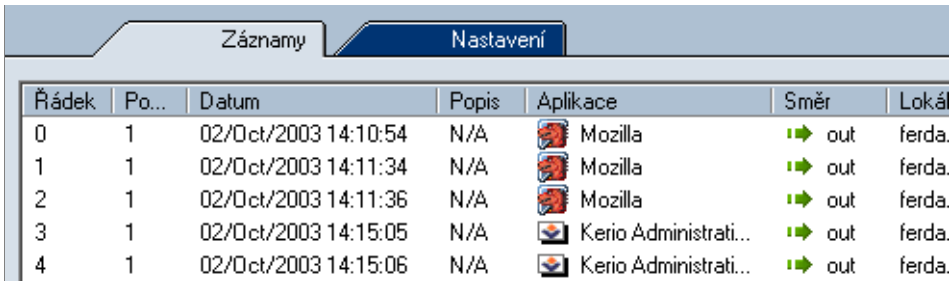
Tlačítko *Upřesnění...* otevírá dialog pro výběr záznamů *Kerio Personal Firewallu*, které mají být na *Syslog* server odesílány.



11.4 Záznam Síť

Do záznamu *Network* se ukládají informace o síťové komunikaci, která vyhověla určitému pravidlu pro aplikaci (viz kapitola 5.2) nebo pravidlu paketového filtru (viz kapitola 6). Komunikace se zaznamenává pouze tehdy, pokud je v příslušném pravidle zapnuta volba *Zaznamenat komunikaci do záznamu Síť*.

Záznam *Síť* obsahuje tyto informace:



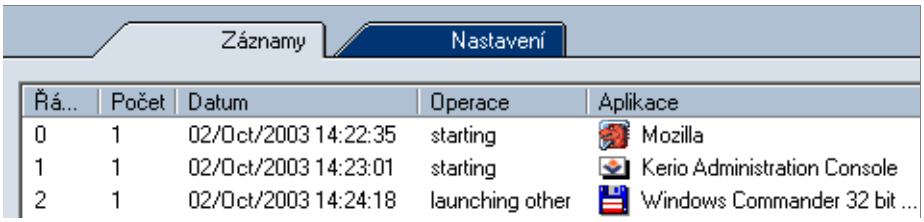
- *Řádek* — číslo řádku záznamu
- *Počet* — počet zpráv (opakuje-li se stejná zpráva vícekrát bezprostředně za sebou, uloží se do záznamu pouze jednou a uvede se počet opakování)
- *Datum* — datum a čas zápisu zprávy do záznamu
- *Popis* — v případě pravidla paketového filtru popis pravidla
- *Aplikace* — název lokální aplikace (dle volby *Zobrazované jméno aplikace*) příslušné k zachycené síťové komunikaci

  Poznámka: Do souboru záznamu je ukládán jak popis aplikace, tak úplná cesta ke spustitelnému souboru. Proto lze v okně záznamu způsob zobrazení aplikace libovolně přepínat.
- *Směr* — směr navázání spojení (*in* = na lokální počítač, *out* = z lokálního počítače)
- *Lokální strana* — lokální IP adresa (jméno počítače)
- *Vzdálená strana* — IP adresa (jméno) vzdáleného počítače
- *Protokol* — použitý komunikační protokol transportní úrovně (TCP, UDP apod.)
- *Akce* — akce, která byla provedena:
  - *permitted* — komunikace povolena
  - *denied* — komunikace zakázána
  - *asked* → *permitted* — zobrazen dotaz uživateli (tj. dialog *Upozornění na spojení*), uživatel komunikaci povolil
  - *asked* → *denied* — zobrazen dotaz uživateli, uživatel komunikaci zakázal

11.5 Záznam Systém

Do záznamu *Systém* se zapisují informace o spouštění aplikací, které vyhovují určitým pravidlům v sekci *Bezpečnost systému / Aplikace*. Záznam se provádí pouze tehdy, je-li v příslušném pravidle zapnuta volba *Zaznamenat do záznamu Systém*.

Záznam *Systém* obsahuje tyto informace:



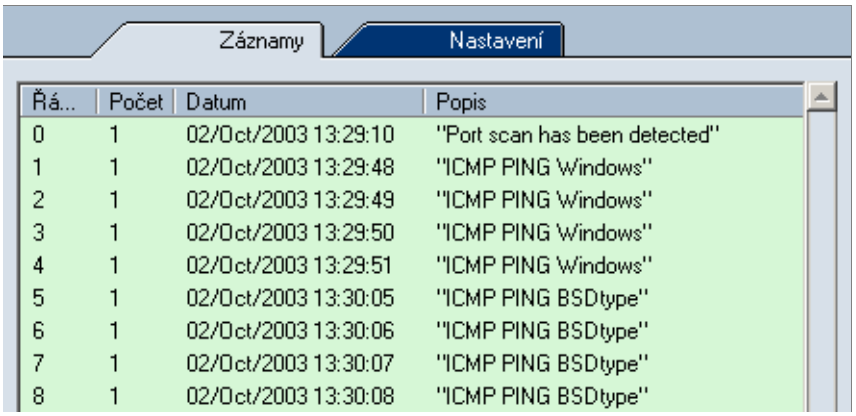
- *Řádek* — číslo řádku záznamu
- *Počet* — počet identických zpráv
- *Datum* — datum a čas zápisu zprávy do záznamu
- *Operace* — typ operace:
  - *starting* — spouštění aplikace
  - *starting modified* — změna ve spustitelném souboru aplikace
  - *launching other* — aplikace spouští jinou aplikaci
- *Aplikace* — název aplikace (dle volby *Zobrazované jméno aplikace*)
- *Předmět* — v případě spouštění jiné aplikace název této aplikace (dle volby *Zobrazované jméno aplikace*)
- *Akce* — akce, která byla provedena:
  - *permitted* — spuštění aplikace povoleno
  - *denied* — spuštění aplikace zakázáno
  - *asked* → *permitted* — zobrazen dotaz uživateli

    (tj. dialog *Spouštění/Záměna/Spouštění jiné aplikace*), uživatel spuštění povolil
  - *asked* → *denied* — zobrazen dotaz uživateli, uživatel spuštění zakázal

11.6 Záznam Útoky

Do záznamu *Útoky* se zapisují informace o detekovaných útocích. Zaznamenávány jsou útoky těch skupin, u nichž je zapnuta volba *Zaznamenat* (viz kapitola 8).

Záznam *Útoky* obsahuje tyto informace:

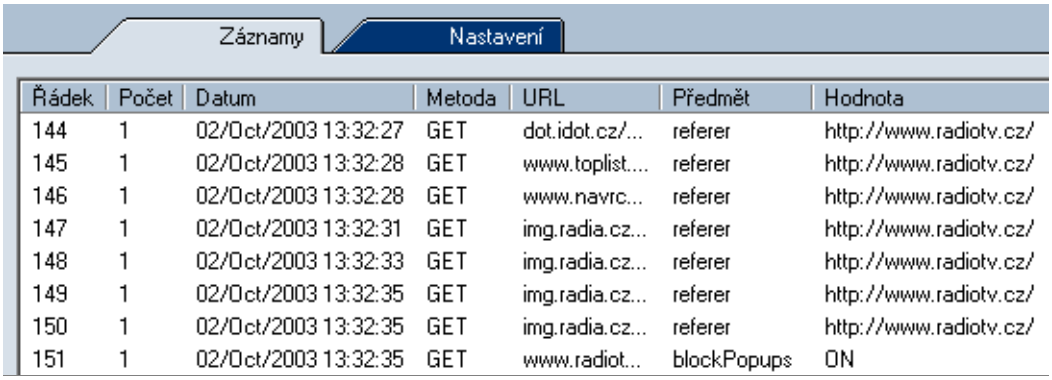


- *Řádek* — číslo řádku záznamu
- *Počet* — počet identických zpráv
- *Datum* — datum a čas zápisu zprávy do záznamu
- *Popis* — název (popis) zachyceného útoku (viz kapitola 8.1)
- *Směr* — směr útoku (útok může být veden i z lokálního počítače)
- *Vzdálená adres* — IP adresa (jméno) vzdáleného počítače (pokud je zjistitelná — útok může být veden z falšované IP adresy)
- *Odkazované URL* — URL stránky s bližšími informacemi o útoku (jsou-li k dispozici)
- *Třída útoku* — třída, do které je útok klasifikován (viz kapitola 8.1)
- *Priorita* — prioritní skupina, do které je útok zařazen v *Kerio Personal Firewallu* (vysoká, střední nebo nízká priorita)
- *Akce* — akce, kterou *Kerio Personal Firewall* provedl při zachycení tohoto útoku (*permitted* — útok povolen, *denied* — útok zakázán)

11.7 Záznam WWW

Do záznamu *WWW* se zapisují informace o objektech blokovaných filtrem obsahu WWW stránek. Tento záznam není konfigurovatelný — je-li modul filtrování obsahu aktivní (viz kapitola 9), zaznamenávají se všechny filtrované objekty.

Záznam *WWW* obsahuje tyto informace:



Řádek	Počet	Datum	Metoda	URL	Předmět	Hodnota
144	1	02/Oct/2003 13:32:27	GET	dot.idot.cz/...	referer	http://www.radiotv.cz/
145	1	02/Oct/2003 13:32:28	GET	www.toplist....	referer	http://www.radiotv.cz/
146	1	02/Oct/2003 13:32:28	GET	www.navrc...	referer	http://www.radiotv.cz/
147	1	02/Oct/2003 13:32:31	GET	img.radia.cz...	referer	http://www.radiotv.cz/
148	1	02/Oct/2003 13:32:33	GET	img.radia.cz...	referer	http://www.radiotv.cz/
149	1	02/Oct/2003 13:32:35	GET	img.radia.cz...	referer	http://www.radiotv.cz/
150	1	02/Oct/2003 13:32:35	GET	img.radia.cz...	referer	http://www.radiotv.cz/
151	1	02/Oct/2003 13:32:35	GET	www.radiot...	blockPopups	ON

- *Řádek* — číslo řádku záznamu
- *Počet* — počet identických zpráv
- *Datum* — datum a čas zápisu zprávy do záznamu
- *Metoda* — použitá metoda protokolu HTTP (*GET* nebo *POST*)
- *URL* — adresa objektu (resp. stránky), kterého se metoda týká
- *Předmět* — blokovaný prvek WWW stránky (*Advertisement* — reklama, *Referer* — odkaz `Referer` v HTTP hlavičce, *cookie* — trvalé nebo dočasné cookie,

  blockPopups — pop-up nebo pop-under okno)
- *Hodnota* — hodnota blokovaného prvku (viz níže)
- *Akce* — akce, která byla provedena (*removed* — odstraněný prvek z WWW stránky, *blocked* — blokováno pravidly pro reklamy)

Informace v položce *Hodnota* závisí na typu blokovaného objektu (viz položka *Předmět*):

- reklama (*Advertisement*) — sloupec *Hodnota* obsahuje pravidlo, které bylo uplatněno (viz kapitola 9.1)
- položka `Referer` — sloupec *Hodnota* obsahuje URL stránky, na kterou bylo v této položce odkazováno
- skripty (*Script*) — ve sloupci *Hodnota* je uveden typ skriptu nebo objektu, který byl filtrován (*JavaScript*, *VBScript* nebo *ActiveX*).
- pop-up a pop-under okna (*blockPopups*) — výraz *ON* ve sloupci *Hodnota* znamená, že pro danou stránku bylo aktivováno blokování pop-up a pop-under oken.

11.8 Záznamy Debug, Error a Warning

Záznam *Debug* obsahuje podrobné informace o běhu programu *Kerio Personal Firewall*.

Do záznamu *Error* se zapisují závažné chyby, které mají zásadní vliv na chod *Kerio Personal Firewallu* (např. nepodaří-li se z nějakého důvodu spustit službu *Personal Firewall Engine*).

Do záznamu *Warning* jsou zapisovány nekritické chyby (např. chyba při zjišťování nové verze programu).

Kapitola 12

Slovníček pojmů

Aplikační protokol 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.

Cookie Textové informace, které server ukládá ke klientovi (WWW prohlížeči). Slouží pro pozdější identifikaci klienta při opětovné návštěvě daného serveru/stránky. Cookies mouhou být zneužívány pro sledování, které stránky uživatel navštívil, případně k počítání přístupů.

Firewall Prostředek (zpravidla softwarový produkt) k ochraně před útoky a únikem dat. Existují dva základní typy firewallů:

- síťový firewall — chrání počítače v určité subsíti. Typicky bývá nasazen na bránu (směrovač), který připojuje tuto subsíť do Internetu.
- personální (osobní) firewall — chrání jeden konkrétní počítač (pracovní stanici uživatele). Oproti síťovému firewallu může navíc vztáhnout síťovou komunikaci ke konkrétní aplikaci, měnit své chování na základě interakce s uživatelem atd.

Poznámka: V tomto manuálu je výrazem *firewall* označován produkt *Kerio Personal Firewall*.

ICMP *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*).

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

Port 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.

TCP *TCP* (Transmission Control Protocol) 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.

TCP/IP *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 úrovní. Přitom platí, že pakety protokolů nižších úrovní obsahují (zapouzdřují) ve své datové části pakety protokolů vyšších úrovní (např. pakety protokolu TCP jsou neseny v IP paketech).

UDP *UDP* (User Datagram Protocol) 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.

Kapitola 13

Rejstřík